ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Ασφάλεια Σε Ευρυζωνικά Δορυφορικά Πολυμεσικά Δίκτυα Επικοινωνιών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Βασιλική Μ. Παπασωτηρίου

Επιβλέπων : Αθανάσιος Δ. Παναγόπουλος
Λέκτορας Ε.Μ.Π.

Αθήνα, Οκτώβριος 2012

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ
ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Ασφάλεια Σε Ευρυζωνικα Πολυμεσικά Δίκτυα Επικοινωνιών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Βασιλική Μ. Παπασωτηρίου

Επιβλέπων: Αθανάσιος Δ. Παναγόπουλος
Λέκτορας Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την .....η Οκτωβρίου2012.

.....	.....	.....
Α. Παναγόπουλος	Ι. Κανελλόπουλος	Φ. Κωνσταντίνου
Λέκτορας Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.

Αθήνα, Οκτώβριος 2012

.....

Βασιλική Μ. Παπασωτηρίου

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Η συνεχώς αυξανόμενη χρήση των δορυφορικών τηλεπικοινωνιακών συστημάτων καθώς και των υπηρεσιών που βασίζονται σε αυτά καθιστούν την ασφάλεια αναγκαίο και σημαντικό κομμάτι της αρχιτεκτονικής τους. Η ανάγκη παροχής ασφαλών τηλεπικοινωνιακών υπηρεσιών εξαιτίας και της συνεργασίας τους με τα υπόλοιπα τηλεπικοινωνιακά δίκτυα για την παροχή ολοκληρωμένων υπηρεσιών οδηγεί στην ανάπτυξη διαφόρων λειτουργικών οντοτήτων για τη διαχείριση της ασφάλειας.

Τα δορυφορικά τηλεπικοινωνιακά συστήματα απειλούνται με διάφορους τρόπους και δέχονται έυκολα επιθέσεις, τόσο εξωτερικές όσο κι εσωτερικές, οι οποίες σχετίζονται και με τα χαρακτηριστικά των συστημάτων αυτών. Στην παρούσα διπλωματική εργασία, αρχικά, κατηγοριοποιούνται αυτές οι απειλές κι επιθέσεις, αναλύονται τα χαρακτηριστικά των δορυφορικών συστημάτων και προτείνονται κάποια αντιμέτρα ασφάλειας. Στη συνέχεια καθορίζονται οι λειτουργίες διαχείρισης της ασφάλειας που αφορούν στο χειρισμό των δεδομένων, τη διαχείριση κλειδιών και την εδραίωση κι ενδυνάμωση της πολιτικής ασφάλειας. Η ανάλυση επικεντρώνεται στην ασφάλεια End-to-End και την ασφάλεια μεταξύ των δορυφορικών τερματικών και των επιγείων σταθμών , τη σουίτα πρωτοκόλλων IP και τα συστήματα ασφάλειας ανώτερων στρωμάτων. Περαιτέρω, ερευνάται πως τα προηγούμενα μέτρα μπορούν να εφαρμοστούν στα δορυφορικά συστήματα και να γίνουν διαφανή ως προς αυτά.

Η παραπάνω ανάλυση γίνεται τόσο για unicast όσο και για multicast μετάδοση πληροφορίας που μεταδίδεται μέσω δορυφόρου, δίνοντας ιδιαίτερη έμφαση στη multicast, θεωρώντας πως η κρυπτογράφηση γίνεται σε μεγάλες επιλεγμένες ομάδες, το μέγεθος και η δυναμική των οποίων παίζουν σημαντικό ρόλο. Τέλος, αναλύεται το κόστος του κύκλου ζωής της διαχείρισης κλειδιών για multicast συνδέσεις, δείχνοντας πως για τη λογική ιεραρχία κλειδιών (LKH), η προεγγραφή κι η περιοδική είσοδος είναι η πιο αποδοτική λύση. Καταλήγουμε πως μια λύση διασυνεργασίας μεταξύ της πολυεπίπεδης ασφάλειας IP (IPSec) και του LKH βελτιώνει την απόδοση και μειώνει την κυκλοφορία της διαχείρισης κλειδιών.

Λέξεις κλειδιά

Δορυφορικά Δίκτυα, IP Δορυφορικά Πολυμεσικά Δίκτυα, Διαχείριση Κλειδιών για Δορυφορικές Επικοινωνίες , Κρυπτογραφία.

Abstract

The increasing use of satellite networks and the provided satellite services make security a necessary and important part of their architecture. The need to provide secure services to satellite users and due to the interworking with other telecommunication networks we are leading to the development of various functional entities for security management.

Satellite communication systems are threatened in various ways and readily accept attacks, both external and internal, which are related to the characteristics of these systems. In this thesis, we initially categorize these threats and attacks, analyze the characteristics of satellite systems and propose some countermeasures. Then we specify the security management functions related to the handling of data, key management andthe consolidation and strengthening security policy. The analysis is focused on the End-to-End security between satellite terminals and gateways, the IP suite of protocols and systems and the security overburden. Moreover,we nvestigate how the well-known security techniques can be applied to satellite systems and make them transparent to these measures.

The above analysis is valid for both unicast and multicast satellite communication networks, with particular emphasis on multicast, assuming the encryption is done in large multicast groups, the size and dynamics of which play an important role. Finally, we analyze the life cycle costs of key management for multicast connections, showing how the logical key hierarchy (LKH), and the periodic subscription entrance is the most efficient solution. We conclude that an interworking solution between multilevel security IP (IPSec) and LKH improves efficiency and reduces the release of key management.

Keywords

Satellite Networks, IP-based Satellite Multimedia Networks, Keys management for Satellite Communications, Cryptography.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον κ. Α. Παναγόπουλο, ο οποίος μου εμπιστεύθηκε το συγκεκριμένο θέμα διπλωματικής εργασίας κι όλους όσους με στήριξαν.

Πίνακας περιεχομένων

Ευρετήριο σχημάτων

Ευρετήριο πινάκων

Εισαγωγή

Τα τελευταία χρόνια η ανάγκη για ασφάλεια στις επικοινωνίες γίνεται περισσότερο εντονότερη κι αναγκαία ευρέως. Οι δορυφόροι χρησιμοποιούνται για να επιτρέπουν και να υποστηρίζουν μια σειρά από σημαντικές υπηρεσίες, μεταξύ των οποίων είναι κι η επικοινωνία. Η σημασία της παροχής επαρκών μέτρων ασφαλείας για την προστασία της διαθεσιμότητας και της λειτουργίας των υπηρεσιών δεν πρέπει να υποτιμάται.

Καθώς η ζήτηση για ασφάλεια στις δορυφορικές επικοινωνίες αυξάνεται, η αναζήτηση επικεντρώνεται στις πιο αποδοτικές (συγκριτικά με το κόστος) και ευέλικτες λύσεις, οι οποίες μπορούν να ικανοποιήσουν τις ανάγκες ποικίλων αποστολών και οι οποίες μπορούν επίσης να ενσωματωθούν τόσο στα νέα όσο και στα υπάρχοντα συστήματα.

Η ανάπτυξη ωστόσο των προϊόντων ασφάλειας μπορεί να είναι πολύπλοκη και συχνά παρεξηγημένη. Η παροχή ασφάλειας απαιτεί πολλά περισσότερα από την απλή εφαρμογή κάποιων λειτουργιών ή από ένα επιπλέον "μαύρο κουτί" μέσα στο σύστημα. Η ασφάλεια απαιτεί τη συγκέντρωση των ανθρώπων, της τεχνολογίας και της λειτουργίας μέσα στα πλαίσια ολόκληρου του συστήματος.

Χωρίς τη σαφή κατανόηση αυτών των εννοιών, θα υπάρχει πάντα μια τάση επικέντρωσης στις πιο απλουστευμένες λύσεις. "do-it-yourself", οι οποίες όμως μπορούν να παρέχουν περιορισμένη αποτελεσματικότητα και μπορούν να κάνουν μια συνεκτική προσέγγιση σχετικά με την ασφάλεια να φαίνεται ακόμα πιο ακριβή από ότι είναι.

Οι πολλών εκατομμυρίων επενδύσεις για τα δορυφορικά συστήματα σε συνδυασμό με τη συνεχώς αυξανόμενη διαθεσιμότητα της τεχνολογίας των δορυφορικών επικοινωνιών έχουν φέρει το θέμα της ασφάλειας στο προσκήνιο. Οι δορυφόροι λειτουργούν σε ανοιχτό περιβάλλον όπου εξουσιοδοτημένοι και μη εξουσιοδοτημένοι άνθρωποι έχουν πρόσβαση στα δεδομένα που μεταδίδονται μεταξύ των δορυφόρων και των επίγειων σταθμών. Για τη προφύλαξη των επενδύσεων τους οι εταιρίες αυξάνουν την απαιτούμενη ασφάλεια στα δορυφορικά συστήματα.

Τα σημαντικότερα αντιμέτρα για την ασφάλεια των δορυφορικών συστημάτων είναι κρυπτογραφικά και παρουσιάζονται στην παρούσα διπλωματική εργασία.

Στο πρώτο κεφάλαιο καθορίζεται η αρχιτεκτονική διαχείρισης της ασφάλειας με βάση τη γενική αρχιτεκτονική των Ευρυζωνικών Δορυφορικών Πολυμέσων (Broadband Satellite Multimedia – BSM). Αρχικά αναλύονται οι απειλές κατά των δικτύων BSM, καθορίζονται τα αναγκαία μέτρα που απαιτούνται για την αντιμετώπισή τους και παρουσιάζονται τα χαρακτηριστικά των δορυφορικών συστημάτων που έχουν άμεση επίδραση στις υπηρεσίες ασφάλειας. Στη συνέχεια παρουσιάζονται τέσσερα παραδείγματα συνδυασμών των Συνδέσμων Ασφαλείας, υποθέτοντας τέσσερα σενάρια σχετικά με την ασφάλεια. Τα σενάρια αυτά είναι: Η ασφάλεια End-to-End, η ασφάλεια Gateway-to-Gateway, η ασφάλεια μεταξύ host και πύλης και η ασφάλεια μεταξύ απομακρυσμένου host και πύλης. Έπειτα παρουσιάζονται οι συστάσεις της Διεθνούς

Ένωσης Τηλεπικοινωνιών (ITU) για την αρχιτεκτονική ασφάλειας. Στην επόμενη παράγραφο του κεφαλαίου αναπτύσσεται το πλαίσιο αναφοράς της ασφάλειας, το οποίο ενσωματώνει τις κύριες οντότητες και λειτουργίες που σχετίζονται με την ασφάλεια BSM. Στη συνέχεια περιγράφεται ο Σύνδεσμος ασφαλείας, τα λειτουργικά στοιχεία της ασφάλειας BSM και το γενικό πρωτόκολλο της αρχιτεκτονικής BSM. Έπειτα παρουσιάζονται οι αλληλεπιδράσεις μεταξύ της ασφάλειας κι άλλων μη BSM policy οντοτήτων, με τη χρήση του πρωτοκόλλου COPS, RADIUS/ DIAMETER, καθώς και οι αλληλεπιδράσεις της ασφάλειας BSM Network με το Address Translation (NAT), όπως επίσης και οι αλληλεπιδράσεις μεταξύ της ασφάλειας και των εξυπηρετητών Performance Enhancing Proxies (PEP). Τελικά, ορίζεται η λεπτομερής λειτουργική αρχιτεκτονική της ασφάλειας BSM, παρουσιάζοντας κάποιες περιπτώσεις ασφάλειας οι οποίες εφαρμόζονται εξίσου σε BSM τοπολογίες αστέρα και πλέγματος.

Στο 2ο Κεφάλαιο παρουσιάζονται κάποιες λύσεις ασφάλειας BSM για τα διάφορα επίπεδα της στοίβας πρωτοκόλλου BSM. Αρχικά παρουσιάζονται οι υπηρεσίες ασφάλειας σε επίπεδο σύνδεσης, όπως είναι το επίπεδο Ασύγχρονου Τρόπου Μεταφοράς (Asychronous Transfer Mode – ATM) κελιών, το MPEG-TS για τα συστήματα DVB-S και DVB-RCS. Στη συνέχεια παρουσιάζονται οι υπηρεσίες ασφάλειας που παρέχονται σε επίπεδο δικτύου, όπως είναι η ασφάλεια του Internet Protocol (IPSec). Έπειτα παρουσιάζονται οι υπηρεσίες ασφάλειας σε επίπεδο μεταφοράς, όπως είναι το πρωτόκολλο Transport Layer Security (TLS), το πρωτόκολλο Ασφαλούς Μεταφοράς σε Πραγματικό Χρόνο - Secure Real Time Transport Protocol (SRTP) και το πρωτόκολλο reliable multicast. Τέλος παρουσιάζεται η ασφάλεια σε επίπεδο εφαρμογής, όπως είναι η ασφάλεια στην eXtensible Markup Language (XML, το Digital Rights Management (DRM), το Secure Shell (SSH) και το Pretty Good Privacy (PGP). Στην παράγραφο 2.3 παρουσιάζονται πέντε παραδείγματα διαχείρισης κλειδιών (Key management), η υπό όρους πρόσβαση DVB-S, η ασφάλεια DVB-RCS, η ασφάλεια IP unicast έλεγχος πρόσβασης με τη χρήση firewalls κι η διαχείριση ασφάλειας IP multicast. Στο τέλος της παραγράφου παρουσιάζονται κάποια πρόβλημα, κίνδυνοι κι απειλές που προκύπτουν, αιτήματα σχετικά με το εύρος ζώνης και την ανάθεση του και κάποιες λύσεις για τα προηγούμενα. Στην τελευταία παράγραφο του 2ου Κεφαλαίου παρουσιάζονται οι προτεινόμενες προδιαγραφές που προέρχονται από το ETSI.

Στο 3ο και τελευταίο Κεφάλαιο αναπτύσσεται η ασφάλεια των multicast δορυφορικών συνδέσεων, επικεντρώνοντας την ανάλυση στη διαχείριση κλειδιών. Αρχικά παρουσιάζεται η ασφάλεια IP multicast, αναλύοντας τους παράγοντες που επηρεάζουν το σχεδιασμό του ασφαλούς συστήματος multicast. Παρουσιάζονται επίσης η κλιμακωτή αρχιτεκτονική διανομής κλειδιού, αναλύοντας το μηχανισμό Logical Key Hierarchy (LKH) και το Group Traffic Encrypting Key (GTEK), τα πρωτόκολλα multicast key management, αναλύοντας το Group Secure Association Key Management Protocol (GSAKMP), το Multimedia Internet KEYing (MIKEY), το Group Domain of Interpretation (GDOI) και το Flat Multicast Key Exchange (FMKE). Στη συνέχεια

περιγράφεται ο κύκλος ζωής του LKH και τέλος το ML-IPSec, καθώς επίσης και η διασυνεργασία μεταξύ των ML-IPSec και LKH.

1. Τεχνικές Προδιαγραφές Προδιαγραφές Ασφάλειας για Ευρυζωνικά Δορυφορικά Δίκτυα

1.1. Εισαγωγή

Με βάση τα αποτελέσματα της αναφοράς για θέματα ασφάλειας στο BSM TR 102 287 [1] και την ανάγκη για παροχή υπηρεσιών ασφάλειας στα συστήματα BSM και τις διασυνεργασίες (interworking) με τον εξωτερικό κόσμο, είναι εξίσου αναγκαία η διαχείριση ασφάλειας των λειτουργικών οντοτήτων BSM. Αυτές οι οντότητες μπορεί να βρίσκονται πάνω ή κάτω από το Σημείο Πρόσβασης Υπηρεσίας Ανεξάρτητο του Δορυφόρου (SI – SAP) και καθορίζουν τον τρόπο με τον οποίο τα δεδομένα ασφαλίζονται μέσω του BSM.

Παρόλο που κάποια συστήματα σχετικά με την ασφάλεια των δορυφόρων υπάρχουν σήμερα, όπως τα DVB–S και DVB–RCS, ο κύριος στόχος του ορισμού της αρχιτεκτονικής είναι η ασφάλεια end-to-end καθώς κι η ασφάλεια μεταξύ των δορυφορικών τερματικών και πυλών κι επιπλέον η αλληλεπίδραση με συστήματα ανεξάρτητα των δορυφόρων όπως το πρωτόκολλο IPsec και τα συστήματα ασφαλείας σε ανώτερα επίπεδα.

Το παρόν κείμενο καθορίζει την αρχιτεκτονική διαχείρισης ασφάλειας με βάση τη γενική BSM αρχιτεκτονική TS 102 292 [2].

Το παρόν κείμενο καθορίζει τη λειτουργική αρχιτεκτονική BSM που απαιτείται για την παροχή υπηρεσιών ασφάλειας στον τελικό χρήστη και τα δορυφορικά δίκτυα. Αυτού του είδους η αρχιτεκτονική αναγνωρίζει τα λειτουργικά στοιχεία που επιτρέπουν την παροχή ασφάλειας σε BSM συστήματα ενσωματωμένα με ετερογενή δίκτυα. Τέτοια στοιχεία θα περιλαμβάνουν ασφαλή επεξεργασία δεδομένων, διαχείριση κλειδιών και χειρισμό της πολιτικής για ασφάλεια. Οι αλληλεπιδράσεις με Proxies Ενίσχυσης Απόδοσης (PEPs) και το πρωτόκολλο IPsec συναντώνται επίσης.

1.2.1. Απαιτήσεις των Υπηρεσιών Ασφαλείας BSM

Στην παράγραφο αυτή αναλύονται οι απειλές κατά των δικτύων BSM και καθορίζονται τα αναγκαία μέτρα που απαιτούνται για την αντιμετώπιση των απειλών αυτών. Επιπλέον, αναλύονται τα χαρακτηριστικά ενός δορυφορικού δικτύου σε σχέση με την επίπτωση που έχουν στην ασφάλεια και τελικά καθορίζονται οι απαιτήσεις ασφαλείας.

Η *ευπάθεια* είναι η επιδεκτικότητα μια κατάστασης κατά την οποία βρίσκεται κάτι εκτεθειμένο. Πρόκειται για ένα ενδεχόμενο, μια πιθανότητα και μια αδυναμία, ένα άνοιγμα. Η ευπάθεια από μόνη της μπορεί, αλλά μπορεί κι όχι, να δημιουργήσει σοβαρά προβλήματα, ανάλογα με ποιά εργαλεία είναι διαθέσιμα για την εκμετάλλευση αυτής

της αδυναμίας. Για παράδειγμα, η χρήση του δημόσιου internet για τη μεταφορά των δεδομένων του χρήστη και της διαχείρισης της κίνησης του δικτύου είναι μια κατάσταση ευπάθειας.

Η *απειλή* είναι μια ενέργεια ή ένα εργαλείο, που μπορεί να εκμεταλλευτεί και να εκθέσει την ευπάθεια κι έτσι να διακυβευθεί η ακεραιότητα ενός συστήματος. Δεν είναι όλες οι απειλές ισοδύναμες σχετικά με την ικανότητα τους να εκθέσουν και να εκμεταλλευτούν την ευπάθεια.

Μια *επίθεση* καθορίζει τις λεπτομέρειες για το πως μια συγκεκριμένη απειλή μπορεί να εκμεταλλευτεί την ευπάθεια. Είναι εξ ολοκλήρου πιθανό να υπάρχουν καταστάσεις κατά τις οποίες είναι γνωστές οι ευπάθειες κι οι απειλές αναπτύσσονται, αλλά καμία λογική επίθεση δεν μπορεί να σχεδιαστεί έτσι ώστε να χρησιμοποιήσει τη συγκεκριμένη απειλή κατά της ευπάθειας του συστήματος.

Τα *αντιμέτρα* είναι εκείνες οι ενέργειες που γίνονται για την προστασία του συστήματος από τις επιθέσεις, οι οποίες απειλούν συγκεκριμένες ευπάθειες. Στον κόσμο της ασφάλειας του δικτύου, τα αντιμέτρα αποτελούνται από εργαλεία όπως είναι ο εντοπισμός και καθαρισμός των ιών, το φιλτράρισμα των πακέτων, η πιστοποίηση του κωδικού πρόσβασης κι η κρυπτογράφηση.

Οποιοδήποτε σχέδιο ασφάλειας πρέπει να αναγνωρίζει τις ευπάθειες και τις απειλές, να προβλέπει ενδεχόμενες επιθέσεις, να εκτιμά αν είναι πιθανό να επιτύχουν ή όχι, να αξιολογεί ποια θα είναι η πιθανή ζημιά που θα προκαλέσουν οι επιτυχημένες επιθέσεις κι έπειτα να εφαρμόσει αντιμέτρα για τις επιθέσεις αυτές οι οποίες θεωρούνται πως είναι αρκετά σημαντικές ώστε να πρέπει να αντιμετωπιστούν. Οι απειλές κατά των συστημάτων BSM μπορούν γενικά να κατηγοριοποιηθούν σε απειλές δικτύου, λογισμικού, υλικού κι ανθρώπινες (από τον χρήστη).

1.2.1.1. Απειλές Δικτύου

Οι πιο απλή μορφή των απειλών δικτύου είναι οι *παθητικές* απειλές κατά τις οποίες οι παθητικοί εισβολείς προσπαθούν να υποκλέψουν ή να παρακολουθήσουν τις μεταδόσεις με σκοπό να αποκτήσουν την πληροφορία που μεταδίδεται. Οι δύο τύποι των παθητικών απειλών είναι η απελευθέρωση του μηνύματος περιεχομένου και της ανάλυσης της κίνησης. Οι παθητικές απειλές δεν ανιχνεύονται εύκολα διότι δεν προκαλούν κάποια αλλαγή στα δεδομένα κι επίσης ο εισβολέας δε χρειάζεται εξελιγμένα εργαλεία ή γνώση για την εκτέλεση των απειλών αυτών.

Οι *ενεργές* απειλές είναι γενικά πιο δύσκολο να εκτελεστούν με επιτυχία σε σχέση με τις παθητικές και συνήθως απαιτούν πιο εξελιγμένους πόρους. Παραδείγματα των απειλών αυτών δίνονται στη συνέχεια:

Μεταμφίεση (Πλαστοπροσωπία)

Η *μεταμφίεση* συμβαίνει όταν μια οντότητα προσποιείται πως είναι κάποια άλλη οντότητα. Η μεταμφίεση συνήθως χρησιμοποιείται μαζί με άλλους τύπους ενεργών απειλών, ειδικά μαζί με την *επανάληψη* και *τροποποίηση* των μηνυμάτων. Για παράδειγμα, οι ακολουθίες πιστοποίησης μπορεί να συλληφθούν και να παιχτούν ξανά μετά από μια έγκυρη ακολουθία πιστοποίησης. Μια εξουσιοδοτημένη οντότητα με μερικά προνόμια μπορεί να χρησιμοποιήσει τη *μεταμφίεση* έτσι ώστε να κερδίσει περισσότερα προνόμια παριστάνοντας την οντότητα που έχει αυτά τα προνόμια. Τυπικά αυτό μπορεί να συμβεί με κλοπή του κωδικού πρόσβασης και των πιστοποιητικών των άλλων προσώπων. Για παράδειγμα οι επιθέσεις *επανάληψης* είναι μια μορφή *μεταμφίεσης* κατά την οποία ένα έγκυρο μήνυμα που περιέχει την πληροφορία της πιστοποίησης μπορεί να παίζεται ξανά από κάποια άλλη οντότητα με σκοπό να πιστοποιήσει τον εαυτό της στην οντότητα πιστοποίησης.

Τροποποίηση του μηνύματος (χειραγώγηση)

Η τροποποίηση των μηνυμάτων συμβαίνει όταν το περιεχόμενο των δεδομένων αλλάξει χωρίς ανίχνευση κι έχει ως αποτέλεσμα μη εξουσιοδοτημένη επίδραση. Αυτή είναι η περίπτωση όπου για παράδειγμα το μήνυμα "Επέτρεψε στην Αλίκη να διαβάσει το εμπιστευτικό αρχείο Λογαριασμοί" τροποποιείται στο "Επέτρεψε στον Πέτρο να διαβάσει το εμπιστευτικό αρχείο Λογαριασμοί".

Άρνηση αναγνώρισης από ένα μέρος

Η *άρνηση της αναγνώρισης* από ένα μέρος μπορεί να συμβεί είτε από την πηγή είτε από τον προορισμό. *Άρνηση αναγνώρισης από την πηγή* συμβαίνει όταν το μέρος αρνείται πως είναι ο συντάκτης του μηνύματος κι *άρνηση αναγνώρισης από τον προορισμό* συμβαίνει όταν το μέρος αυτό αρνείται την αποδοχή του μηνύματος. Για παράδειγμα, όταν ένας πελάτης "κατεβάζει" μια ταινία από μια υπηρεσία pay per view, τότε ο πελάτης αυτός δε θα πρέπει να αρνηθεί το "κατέβασμα¨ αυτής της ταινίας με σκοπό να μην πληρώσει αυτό που είναι υποχρεωμένος.

Άρνηση παροχής υπηρεσιών (DoS)

Οι επιθέσεις *άρνησης παροχής υπηρεσιών* συμβαίνουν όταν μια οντότητα αποτυγχάνει να εκτελέσει σωστά τη λειτουργία της ή ενεργεί με τέτοιο τρόπο ο οποίος εμποδίζει τις άλλες οντότητες να εκτελέσουν τις δικές τους λειτουργίες.

Η επίθεση DoS μπορεί να είναι γενική, δηλαδή μια οντότητα να καταστέλλει όλα τα μηνύματα, ή μπορεί να υπάρχει συγκεκριμένος στόχος, όταν δηλαδή μια οντότητα καταστέλλει όλα τα μηνύματα που προορίζονται για ένα συγκεκριμένο προορισμό, για παράδειγμα την υπηρεσία ελέγχου της ασφάλειας. Η επίθεση μπορεί να περιλαμβάνει την καταστολή της κίνησης όπως περιγράφηκε σε αυτό το παράδειγμα ή να παράγει επιπλέον κίνηση. Είναι επίσης πιθανό να παράγει καινούρια μηνύματα με σκοπό τη διατάραξη της λειτουργίας του δικτύου, ειδικά όταν το δίκτυο έχει οντότητες

αναμετάδοσης που παίρνουν αποφάσεις δρομολόγησης βασισμένες στις αναφορές καταστάσεις που παίρνουν από άλλες οντότητες αναμετάδοσης.

Οι απαιτήσεις ασφαλείας για την αντιμετώπιση των απειλών δικτύου είναι:

- Πιστοποίηση της πηγής.
- Εμπιστευτικότητα κι ακεραιότητα των δεδομένων από την πηγή στους τελικούς χρήστες.
- Ικνηλασιμότητα (χρησιμοποιώντας για παράδειγμα συστήματα ανίχνευσης εισβολής) για την παρακολούθηση του δικτύου κι αρχεία καταγραφής (log files) για την καταγραφή της δραστηριότητας του δικτύου.
- Προστασία έναντι της άρνησης παροχής υπηρεσιών.

1.2.1.2. Απειλές Λογισμικού

Πολλά συστήματα αποτυγχάνουν εξαιτίας λαθών στην εφαρμογή. Κάποια συστήματα δεν διασφαλίζουν πως το plaintext (ακρυπτογράφητο κείμενο) καταστρέφεται μετά την κρυπτογράφηση του. Άλλα σύστημα χρησιμοποιούν προσωρινά αρχεία για να προστατευτούν από την απώλεια δεδομένων κατά τη διάρκεια κατάρρευσης του συστήματος ή εικονική μνήμη για να αυξήσουν τη διαθέσιμη μνήμη. Αυτά τα χαρακτηριστικά μπορεί να αφήσουν κατά λάθος το plaintext στο σκληρό δίσκο. Επιπλέον απόρρητες πληροφορίες μιας εταιρίας ή των πελατών πρέπει να αποθηκεύονται με ασφάλεια στο site του παρόχου διαφορετικά δημιουργείται σοβαρή απειλή αφού ο πάροχος θα έχει όλες τις απόρρητες πληροφορίες των πελατών κι αυτό να οδηγήσει σε κακή χρήση.

Κάποια παραδείγματα απειλών λογισμικού είναι:

Trapdoor
Όταν μια οντότητα του συστήματος μεταβάλλεται με σκοπό να επιτρέψει στον εισβολέα να προκαλέσει μη εξουσιοδοτημένη επίδραση είτε στην εντολή είτε σε ένα προκαθορισμένο γεγονός ή σε ακολουθία γεγονότων, τότε το αποτέλεσμα καλείται trapdoor. Για παράδειγμα, ο κωδικός επικύρωσης μπορεί να τροποποιηθεί έτσι ώστε εκτός από την κανονική του ενέργεια να επικυρώσει και τον κωδικό του εισβολέα.

Trojan Horse
Όταν εισάγεται στο σύστημα, ένα Trojan Horse δημιουργεί μια μη εξουσιοδοτημένη λειτουργία προσθετικά στην εξουσιοδοτημένη λειτουργία. Για παράδειγμα, ένας αναμεταδότης που αντιγράφει επίσης μηνύματα σε ένα μη εξουσιοδοτημένο κανάλι είναι ένα Trojan Horse.

Απειλή από τον κρυπτογραφικό σχεδιασμό
Ένα κρυπτογραφικό σύστημα μπορεί να είναι τόσο ισχυρό όσο ισχυροί είναι οι κρυπτογραφικοί αλγόριθμοι, οι αλγόριθμοι ψηφιακής υπογραφής, οι μονόδρομες συναρτήσεις κατακερματισμού (one-way hash functions) και οι κώδικες μηνύματος πιστοποίησης στα οποία βασίζεται. Σπάσιμο έστω κι ενός από τα παραπάνω σημαίνει είσοδος στο σύστημα.

Τα σύστημα συχνά δεν χρησιμοποιούν την κρυπτογράφηση σωστά με αποτέλεσμα να "χάνουν την εγγύηση" τους: παραλείποντας να ελέγξουν το μέγεθος των τιμών, επαναχρησιμοποιώντας παραμέτρους που δε θα έπρεπε να επαναχρησιμοποιηθούν κι άλλα. Οι κρυπτογραφικοί αλγόριθμοι δεν εξασφαλίζουν απαραίτητα ακεραιότητα στα δεδομένα. Τα πρωτόκολλα ανταλλαγή κλειδιών (key exchange) δε διασφαλίζουν πως και τα δύο μέρη θα λάβουν το ίδιο κλειδί. Οι γεννήτριες τυχαίων αριθμών είναι ένα άλλο σημείο μέσα από το οποίο μπορούν τα κρυπτογραφικά σύστημα να σπάσουν. Καλές γεννήτριες τυχαίων αριθμών είναι πολύ δύσκολο να σχεδιαστούν γιατί η ασφάλεια τους βασίζεται στα στοιχεία του λογισμικού και του υλικού. Παρόλο που η κρυπτογράφηση μπορεί να είναι ισχυρή, αν η γεννήτρια τυχαίων αριθμών δημιουργεί αδύναμα κλειδιά, τότε το σύστημα είναι πολύ εύκολο να σπάσει.

Απειλή από την πλήρη εξάρτηση του λειτουργικού συστήματος (OS)
Όταν η ασφάλεια της εφαρμογής λογισμικού εξαρτάται μόνο από την ασφάλεια του λειτουργικού συστήματος κι όχι να την συμπληρώνει τότε αυτή η κατάσταση θα εξελιχθεί σε απειλή.

Οι απαιτήσεις ασφαλείας για τις απειλές λογισμικού είναι:

- Προστασία έναντι των ιών λογισμικού.
- Καλός σχεδιασμός του λογισμικού για τις εμπορικές εφαρμογές έτσι ώστε να μην επιτρέπεται η μη εξουσιοδοτημένη πρόσβαση στο σύστημα και η τυχαία καταστροφή από μη έμπειρους χρήστες.
- Καλή ασφάλεια στο λογισμικό με ισχυρή κρυπτογράφηση κι αλγόριθμους με ψηφιακή υπογραφή, καλές γεννήτριες τυχαίων αριθμών κι ασφαλή αποθήκευση των εσωτερικών δεδομένων και των κλειδιών.

1.2.1.3. Απειλές στην εφαρμογή υλικού

Πολλά συστήματα, ειδικά τα εμπορικά συστήματα βασίζονται σε tamper-resistant υλικό για την ασφάλεια τους: έξυπνες κάρτες, ηλεκτρονικά πορτοφόλια, dongles, κ.α. Η ασφάλεια του υλικού είναι πολύ σημαντικό κομμάτι των περισσοτέρων συστημάτων ασφαλείας καθώς η ασφάλεια στηρίζεται μόνο σε υποθέσεις πως η ενδογενής ασφάλεια από την κατασκευή του (tamper-resistant) δεν είναι αρκετή. Κατά τον σχεδιασμό συστημάτων που χρησιμοποιούν tamper-resistant είναι καλύτερο να δημιουργηθούν

συμπληρωματικοί μηχανισμοί ασφάλειας σε περίπτωση που η τεχνική του tamper-resistant αποτύχει.

Όλα τα συστήματα hardware συμπεριλαμβανομένων των σταθμών πελατών, των δορυφορικών τερματικών και τον εξοπλισμό του δικτύου, όπως είναι τα routers και τα firewalls αν δεν είναι σωστά ρυθμισμένα μπορούν να αποτελέσουν απειλή, αφού θα γίνουν τα σημεία εισόδου της επίθεσης. Η μη εξουσιοδοτημένη πρόσβαση σε αυτά τα μηχανήματα αποτελεί απειλή επίσης διότι σημαίνει είσοδο στο σύστημα. Αν όλα τα βασικά συστήματα hardware δεν έχουν δημιουργήσει αντίγραφα ασφαλείας σε περίπτωση έκτακτης ανάγκης όπως είναι η διακοπή ρεύματος ή οι επιθέσεις άρνησης παροχής υπηρεσιών τότε δημιουργείται σοβαρή απειλή καθώς τα δεδομένα που είναι αποθηκευμένα σε αυτά τα συστήματα όπως επίσης κι η διαθεσιμότητα της υπηρεσίας θα χαθούν.

Οι απαιτήσεις ασφαλείας για τις απειλές υλικού είναι:

- Δημιουργία αντιγράφων ασφαλείας για την αποφυγή απώλειας δεδομένων εξαιτίας αποτυχίας του συστήματος ή σε περίπτωση λανθασμένης διαγραφής των δεδομένων.
- Προστασία από κλοπή υλικού.

1.2.1.4. Ανθρώπινες απειλές (από τον χρήστη)

Εσωτερικές επιθέσεις
Οι εσωτερικές επιθέσεις συμβαίνουν όταν οι νόμιμοι χρήστες ενός συστήματος συμπεριφέρονται απρομελέτητα ή με μη εγκεκριμένους τρόπους. Τα πιο γνωστά ηλεκτρονικά εγκλήματα προήλθαν από εσωτερικές επιθέσεις που εξέθεσαν την ασφάλεια του συστήματος. Για παράδειγμα, οι χρήστες ενός συστήματος δε θα πρέπει να αποκαλύπτουν απόρρητες πληροφορίες των πόρων της εταιρίας δίνοντας το όνομα χρήστη/ κωδικό πρόσβασης σε άλλους οι οποίοι δεν ανήκουν στην εταιρία.
Άλλη μία πολύ σοβαρή εσωτερική επίθεση είναι η πειρατεία, δηλαδή όταν ένας από τα νόμιμα μέλη μιας ομάδας δώσει την εφαρμογή BSM σε άλλους χωρίς η ομάδα να το γνωρίζει.

Τα περισσότερα συστήματα σπάνε διότι βασίζονται σε κωδικούς που δημιουργούν οι ίδιοι οι χρήστες, οι οποίοι συνήθως δεν επιλέγουν ισχυρούς κωδικούς. Ακόμα κι όταν το σύστημα είναι ασφαλές όταν χρησιμοποιείται σωστά, κάθε χρήστης του μπορεί κατά λάθος να ανατρέψει την ασφάλεια, ειδικά όταν το σύστημα δεν είναι πολύ καλά σχεδιασμένο. Το κλασικό παράδειγμα είναι ένας χρήστης ο οποίος δίνει τον κωδικό του σε ένα συνάδελφό του για να του διορθώσει κάποιο πρόβλημα όταν λείπει εκτός γραφείου. Οι χρήστες πολύ συχνά δεν αναφέρουν αμέσως την απώλεια μια έξυπνης κάρτας, θεωρώντας πως θα τη βρουν, κάτι που μπορεί να αποτελέσει εσωτερική επίθεση. Άλλα παραδείγματα είναι τα εξής: οι χρήστες δεν ελέγχουν προσεκτικά το

όνομα του ψηφιακού πιστοποιητικού, χρησιμοποιούν τον ίδιο κωδικό σε άλλα συστήματα, με μικρότερη ασφάλεια, δεν αλλάζουν τις αρχικές αδύναμες ρυθμίσεις του λογισμικού και διάφορα άλλα. Αν δεν υπάρχει εκπαιδευμένο προσωπικό, (διαχειριστές/ administrators) να παρακολουθούν και να ρυθμίζουν τα συστήματα και το δίκτυο τότε αυτό μπορεί να εξελιχθεί σε σοβαρή απειλή.

Εξωτερικές επιθέσεις
Οι εξωτερικές επιθέσεις διενεργούνται με σκοπό την απόκτηση εισόδου στο σύστημα από άτομα που δεν είναι μέλη της επιχείρησης ή δεν είναι πελάτες του παρόχου. Για το σκοπό αυτό χρησιμοποιούνται τεχνικές όπως υποκλοπή παρακολούθηση, αναπαραγωγή, τροποποίηση του μηνύματος ή διάλυση των υπηρεσιών χρησιμοποιώντας επιθέσεις άρνησης παροχής υπηρεσιών κ.α. με σκοπό να προχωρήσουν στις επιθέσεις δικτύου όπως περιγράφηκαν προηγουμένως.

Οι απαιτήσεις ασφαλείας για τις ανθρώπινες απειλές είναι:

- Τόσο οι χρήστες όσο και οι διαχειριστές πρέπει να έχουν πιστοποίηση, να μπορούν να ανιχνευθούν οι ενέργειες τους και να λογοδοτούν για αυτές.
- Security Event Management – Η ικανότητα παρακολούθησης κι αναφοράς γεγονότων σχετικών με την ασφάλεια μέσω κατάλληλου συνδέσμου των καταχωρήσεων και των γεγονότων.
- Προστασία των συστημάτων BSM από μη εξουσιοδοτημένους ανθρώπους.
- Εσωτερικά εμπόδια ανάμεσα στη διαχείριση των συνδρομητών και το δίκτυο των διαχειριστών.
- Κατάλληλη εκπαίδευση των χρηστών και των διαχειριστών όσον αφορά τις καλές πρακτικές ασφαλείας για την επιλογή κωδικών και τον έλεγχο της πρόσβασης σε υπολογιστές και κτήρια.

1.2.2. Ορισμός των υπηρεσιών ασφαλείας

Εξετάζοντας τις παραγράφους 1.2.1.1. έως 1.2.1.4. βλέπουμε πως η υποκλοπή (παθητικές επιθέσεις) μπορεί να θεωρηθεί ως μεγάλη απειλή στα συστήματα BSM, ειδικά για τις υπηρεσίες broadcast. Υπάρχουν κι άλλες σοβαρές απειλές. Όπως είναι η μεταμφίεση ή πλαστοπροσωπία, οι τροποποιήσεις μηνυμάτων κι η άρνηση παροχής υπηρεσιών. Αυτές οι απειλές απαιτούν κατάλληλα μέτρα για την αντιμετώπιση τους. Άλλα ζητήματα, όπως οι απειλές λογισμικού, υλικού ή οι ανθρώπινες χρειάζονται άλλα μέτρα όπως ο καλός σχεδιασμός και καλή συντήρηση του λογισμικού και του υλικού, σωστός έλεγχος του δορυφορικού εξοπλισμού και τέλος σωστή εκπαίδευση του προσωπικού των δορυφόρων και των πελατών σχετικά με τα θέματα ασφάλειας.

Για την αντιμετώπιση των απειλών που αναφέρθηκαν προηγουμένως, μπορούν να εφαρμοστούν κάποιες θεμελιώδεις υπηρεσίες ασφαλείας, στις οποίες περιλαμβάνεται η

πιστοποίηση, η ακεραιότητα, η εμπιστευτικότητα, η εξουσιοδότηση κι η αποδοχή αναγνώρισης.

- **Εμπιστευτικότητα/ ιδιωτικότητα/ μυστικότητα (Confidentiality/ privacy/ secrecy)** είναι μια υπηρεσία που χρησιμοποιείται για τη πραγματοποίηση ιδιωτικής συνεδρίας. Παρόλο που συνήθως χρησιμοποιείται η κρυπτογράφηση για την παροχή αυτής της υπηρεσίας, μια πιο αδύναμη μορφή της εμπιστευτικότητας μπορεί να επιτευχθεί με τον περιορισμό της δρομολόγησης της συνεδρίας datagrams. Η εμπιστευτικότητα χρησιμοποιείται ως αντιμέτρο κατά της υποκλοπής, της πλαστοπροσωπίας, της ανάλυσης της κυκλοφορίας και της διαρροής σημαντικών πληροφοριών αξιοποιώντας τις διαδικασίες με νόμιμη πρόσβαση στα δεδομένα.
- **Ακεραιότητα (Integrity)**, υπηρεσία που εγγυάται πως τα μηνύματα λαμβάνονται χωρίς τροποποιήσεις από μη εξουσιοδοτημένες οντότητες. Για την παροχή αυτής της υπηρεσίας οι μηχανισμοί που συνήθως χρησιμοποιούνται είναι η κρυπτογράφηση, οι Message Authentication Codes (MAC) ή οι ψηφιακές υπογραφές. Αυτό συμβάλει στην αποφυγή της επαναφοράς στο traffic stream πακέτων που έχουν προηγούμενα πιστοποιηθεί. Η υπηρεσία της ακεραιότητας αποτρέπει τον κακοχειρισμό των μηνυμάτων καθώς τα μηνύματα μπορούν σκοπίμως να τροποποιηθούν, να αντικατασταθούν ή και να διαγραφούν από κάποιον εισβολέα.
- **Πιστοποίηση (Authentication),** είναι μια υπηρεσία που χρησιμοποιείται για την επαλήθευση της ταυτότητας των οντοτήτων που παίρνουν μέρος σε μια μετάδοση. Η πιο απλή τεχνική είναι η ταυτότητα χρήστη (ID) κι ο κωδικός. Η πιστοποίηση μπορεί να είναι αμοιβαία (κι από τις δύο οντότητες που συμμετέχουν) ή μονόδρομη (μόνο από το δημιουργό). Οι κατάλληλοι μηχανισμοί για την παροχή αυτής της υπηρεσίας είναι η κρυπτογράφηση της πληροφορίας κι οι ψηφιακές υπογραφές. Κάποια παραδείγματα των ψηφιακών υπογραφών είναι το Digital Signature Standard (DSS), το Rivest, Shamir και Adleman (RSA) που βασίζονται στην τεχνολογία public key. Πιστοποιητικά υπογεγραμμένα από το Certification Authority (CA) χρησιμοποιούνται για να δεσμεύσουν την ταυτότητα μιας οντότητας με το αντίστοιχο public key.
- **Εξουσιοδότηση (Authorization) κι Έλεγχος Πρόσβασης (Access Control),** είναι μια υπηρεσία με την οποία επαληθεύονται τα προνόμια του εκάστοτε χρήστη. Η υπηρεσία αυτή συνήθως απαιτείται σε συνδυασμό με τη πιστοποίηση για την απόκτηση άδειας πρόσβασης. Αυτό αποτρέπει τη μη εξουσιοδοτημένη χρήση από κάποια πηγή, όπως για παράδειγμα οι εισβολείς που μπορούν να έχουν πρόσβαση σε υπηρεσία μέσω της πλαστοπροσωπίας. Επίσης αποτρέπει τις επιθέσεις άρνησης παροχής υπηρεσίας όπως τη διακοπή ή την κακή χρήση των υπηρεσιών δικτύου ή την εξάντληση των πόρων και την υπερφόρτωση.
- **Αποδοχή Ανανγνώρισης (Non-repudiation)** είναι μια υπηρεσία που αποτρέπει τον αποστολέα ή τον δέκτη την άρνηση των πράξεων του. Ο κύριος μηχανισμός που χρησιμοποιείται σε αυτές τις υπηρεσίες είναι οι ψηφιακές υπογραφές.

1.2.3. Δορυφορικά χαρακτηριστικά σχετικά με την ασφάλεια

Όπως παρουσιάστηκε στο TR 102 287 [1], υπάρχουν κάποια χαρακτηριστικά των δορυφόρων που έχουν άμεση επίδραση στις υπηρεσίες ασφάλειας. Κάποια από τα χαρακτηριστικά αυτά είναι τα εξής:

Καθυστέρηση (Delay)
Κάθε υπηρεσία BSM είναι σχεδιασμένη με μια τοπολογία με συγκεκριμένη καθυστέρηση κι απόκλιση καθυστέρησης. Στα BSM δεν καθορίζεται το ανώτατο όριο καθυστέρησης ούτε το εύρος της απόκλισης καθυστέρησης, αλλά αυτό το ζήτημα απασχολεί τους εκάστοτε σχεδιαστές των υπηρεσιών και τους χειριστές.

Γενικά, μια καθυστέρηση σε ένα δορυφορικό κόμβο (hop) κυμαίνεται μεταξύ των 240 με 280 ms κι έτσι ο χρόνος που απαιτείται για την ασφάλεια πρέπει να είναι ο λιγότερος δυνατός για να μην μειωθεί η ολική απόδοση της δορυφορικής σύνδεσης. Αν ο αριθμός των κόμβων είναι αρκετά μεγάλος δε συνίσταται η χρήση ασφάλειας Hop-by-Hop.

Ρυθμός Λαθών (Bit Error Rates – BER)
Οι συνδέσεις BSM γενικά θεωρούνται πως είναι Quasi-Error-Free κατά τη διάρκεια της διαθέσιμης σύνδεσης. Πάρα ταύτα, ο υψηλός ρυθμός λαθών (Bit Error Rates, BER) σε συνδέσεις BSM μπορεί να οδηγήσει σε απώλεια στο συγχρονισμό ασφάλειας και να μειώσει την αποδοτικότητα των υπηρεσιών ασφαλείας όπως το privacy και την ακεραιότητα, το οποίο επηρεάζει την απόδοση του δικτύου BSM. Επιπλέον, τα μηνύματα με Key Management είναι ευαίσθητα σε λάθη μετάδοσης. Για το λόγο αυτό τα πρωτόκολλα Key Management χρειάζονται συναρτήσεις αξιοπιστίας για να μην επηρεάζονται από τέτοια λάθη.

Εύρος Ζώνης (Bandwidth)
Γενικά στις BSM οντότητες το διαθέσιμο εύρος ζώνης είναι περιορισμένο. Για το λόγο αυτό η προσθήκη ασφάλειας αυξάνει τα overheads (επιβαρύνσεις λειτουργίας και συντήρησης) του δορυφορικού δικτύου. Τα overheads ασφαλείας ποικίλουν ανάλογα τις διάφορες τεχνολογίες κι έτσι ποικίλει κι η επίδραση που έχουν στην απόδοση του δικτύου BSM.

Ασυμμετρία Ζεύξης (Link Asymmetry)
Πολλά πρωτόκολλα υποθέτουν συμμετρικά μονοπάτια δικτύου. Πάρα ταύτα χρησιμοποιούνται συχνά ασύμμετρα μονοπάτια δικτύου ειδικά όταν πρόκειται για δορυφορικές ζεύξεις. Η ασυμμετρία αυτή απαιτεί ειδικό σχεδιασμό αν στο μονοπάτι δικτύου υπάρχουν συσκευές ασφαλείας.

Η επίδραση που έχουν τα χαρακτηριστικά της δορυφορικής ζεύξης στην ασφάλεια συνοψίζεται στα εξής:

- Λόγω των μεγάλων καθυστερήσεων της δορυφορικής ζεύξης, η καθυστέρηση στη διαδικασία της ασφάλειας θα πρέπει να είναι η μικρότερη δυνατή.
- Λόγω του περιορισμένου εύρους ζώνης και της ασυμμετρίας της ζεύξης, τα overheads της ασφάλειας θα πρέπει να είναι ελάχιστα.
- Λόγω του σχετικά υψηλού ρυθμού λαθών (BER) στα δορυφορικά δίκτυα, πρέπει να υπάρχει αξιοπιστία στις ανταλλαγές κλειδιών ασφαλείας (security key exchanges).

1.2.4 Σενάρια σχετικά με την ασφάλεια

Η ασφάλεια BSM μπορεί να χρησιμοποιηθεί ανάμεσα στους hosts και τις πύλες ασφαλείας (μαζί με τα STs ή τις πύλες) με διάφορους συνδυασμούς. Τα endpoints των υπηρεσιών ασφαλείας καθορίζονται από τους συνδέσμους ασφαλείας (Security Associations - SAs).

Σε αυτή την παράγραφο παρουσιάζονται τέσσερα παραδείγματα συνδυασμών των SAs. Αν το πρωτόκολλο IPsec χρησιμοποιείται (για παράδειγμα), τότε κάθε SA μπορεί να είναι είτε πρωτόκολλο Authentication Header (AH) είτε πρωτόκολλο Encapsulation Security Payload (ESP). Στην περίπτωση των host-to-host SAs μπορεί να έχουμε είτε κατάσταση μεταγωγής (transport mode) είτε tunneling, διαφορετικά είναι μόνο tunneling. Κάποια από αυτά τα σενάρια έχουν εφαρμογή σε συστήματα ATM και DVB-RCS. Για την ασφάλεια των στρωμάτων εφαρμογών και μεταφοράς, οι ενδιάμεσες πύλες ασφαλείας και τα δορυφορικά τερματικά δεν παίζουν κάποιο ρόλο. Σε επόμενη παράγραφο παρέχονται περισσότερες πληροφορίες για αυτού του είδους τα συστήματα.

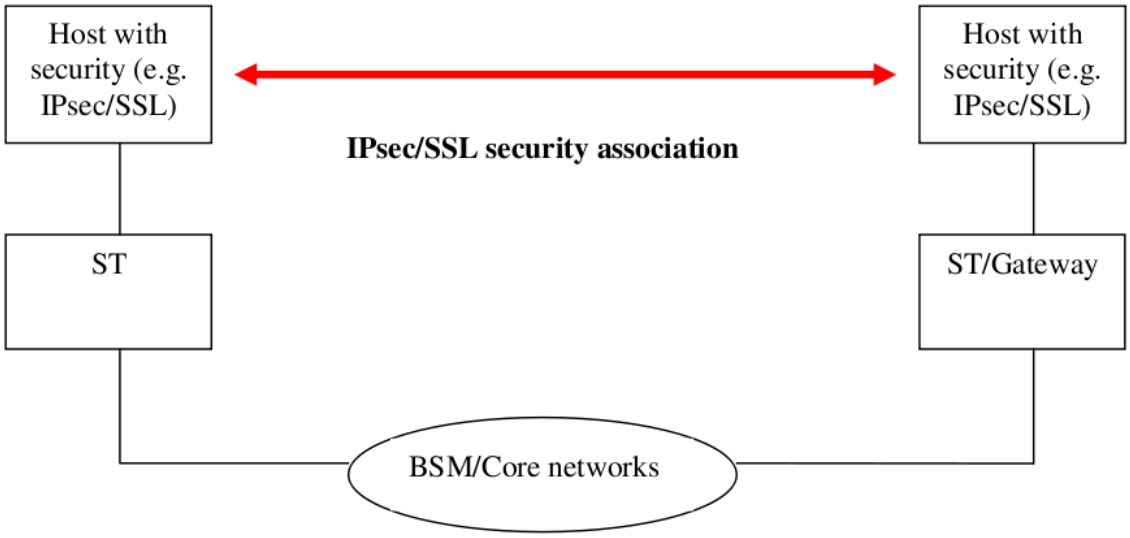
Όλα αυτά τα σενάρια προϋποθέτουν υβριδικά δορυφορικά/επίγεια δίκτυα εκτός από το σενάριο 2 (βλέπε παρακάτω: ασφάλεια Gateway-to-Gateway), το οποίο αναφέρεται μόνο σε δορυφόρους. Στο σενάριο 2, η χρήση του πρωτοκόλλου IPsec ή της ασφάλειας του στρώματος σύνδεσης (όπως τα DVB-RCS) είναι και τα δύο καλοί υποψήφιοι για τη διασφάλιση των υπηρεσιών BSM. Για όλα τα υπόλοιπα σενάρια που περιλαμβάνουν μέρος επίγειου δικτύου, το πρωτόκολλο IPsec είναι η καλύτερη λύση όταν η δορυφορική ζεύξη έχει μόνο μία αναπήδηση (hop) σε μια σύνδεση που αποτελείται από πολλούς κόμβους.

1.2.4.1. Ασφάλεια End-to-End

Όλη η ασφάλεια παρέχεται μεταξύ των end hosts κι εκτελείται τεχνολογία ασφάλειας όπως το πρωτόκολλο IPsec και SSL (Σχήμα 1). Αυτή η ρύθμιση είναι διάφανη στα BSM.

Για παράδειγμα, το IPsec στην κατάσταση μεταφοράς (transport mode) ή το TLS/ SSL μπορούν εξίσου να χρησιμοποιηθούν παρέχοντας προστασία στα δεδομένα κι

ακεραιότητα μεταξύ των πελατών κι αυτό είναι ασφάλεια end-to-end. Οι χρήστες μπορούν επίσης να αναγνωρίσουν τις απαιτήσεις ασφαλείας και να επιλέξουν τις κατάλληλες μεθόδους. Πάρα ταύτα, η λύση του IPsec δεν είναι διάφανη στην προσαρμογή του πρωτοκόλλου και τη συμπίεση των δεδομένων αν εκτελείται από Performance Enhancing Proxies (PEP) μέσα στα δίκτυα BSM.



Σχήμα 1: *Σύνδεσμος ασφάλειας μεταξύ των end hosts.*

1.2.4.2. Ασφάλεια Gateway-to-Gateway

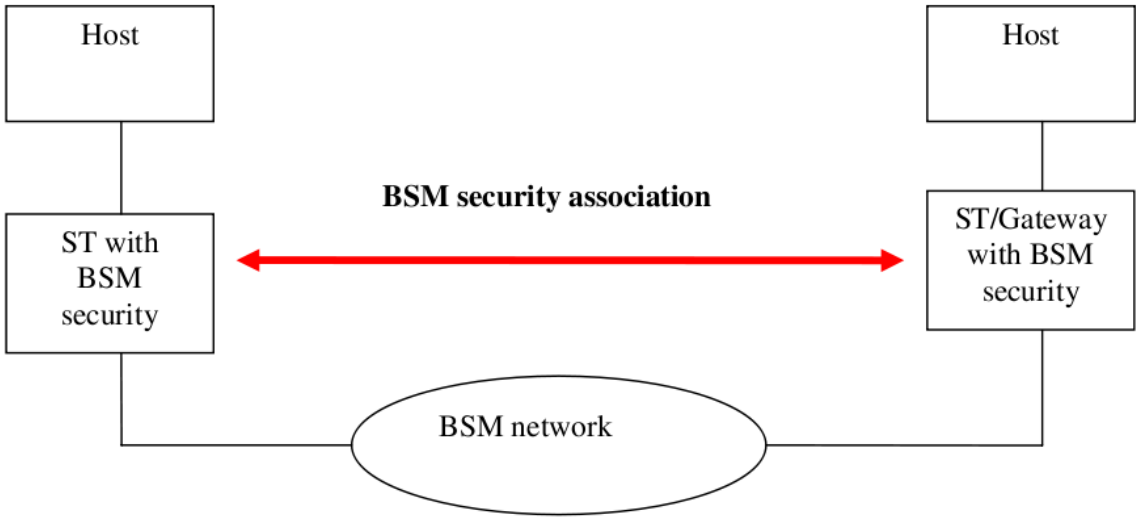
Εδώ η ασφάλεια παρέχεται μόνο μεταξύ των πυλών ασφαλείας (μπορεί να είναι μαζί με τα BSM ST ή την πύλη, βλέπε Σχήμα 2). Αυτό το σενάριο χρησιμοποιείται για τη δημιουργία των Εικονικών Ιδιωτικών Δικτύων (Virtual Private Networks - VPNs).

Για παράδειγμα, μπορεί να χρησιμοποιηθεί ασφάλεια στο επίπεδο σύνδεσης (όπως το DVB-RCS). Σε αυτή την περίπτωση οι απαιτήσεις είναι διαφανείς όπως η συμπίεση του δικτύου, το πρωτόκολλο, η συμπίεση των δεδομένων και το NAT.

Επίσης, το πρωτόκολλο IPsec μπορεί να χρησιμοποιηθεί από επιλογή του χρήστη του mode tunnel για να δημιουργήσει VPN με το IPsec παρέχοντας ασφάλεια σε ένα εταιρικό δίκτυο, για παράδειγμα. Ο χρήστης/ εταιρία αποφασίζει να το κάνει αυτό βασιζόμενος στην πολιτική ασφαλείας. Το κύριο θέμα εδώ είναι η διασφάλιση της πιστοποίησης/ αναγνώρισης των STs όπως επίσης και της ακεραιότητας της σύνδεσης, κάτι που μπορεί να επιτευχθεί πιο εύκολα με ασφάλεια σε επίπεδο σύνδεσης.

Οι απαιτήσεις αυτού του σεναρίου είναι η συμπίεση του δικτύου, το πρωτόκολλο, η συμπίεση των δεδομένων, το NAT αν αναπτυχθούν στα σωστά σημεία στα δίκτυα BSM

(χρησιμοποιώντας το IPsec μετά τη συμπίεση ή το TCP PEP κοντά στο BSM ST/ πύλες).

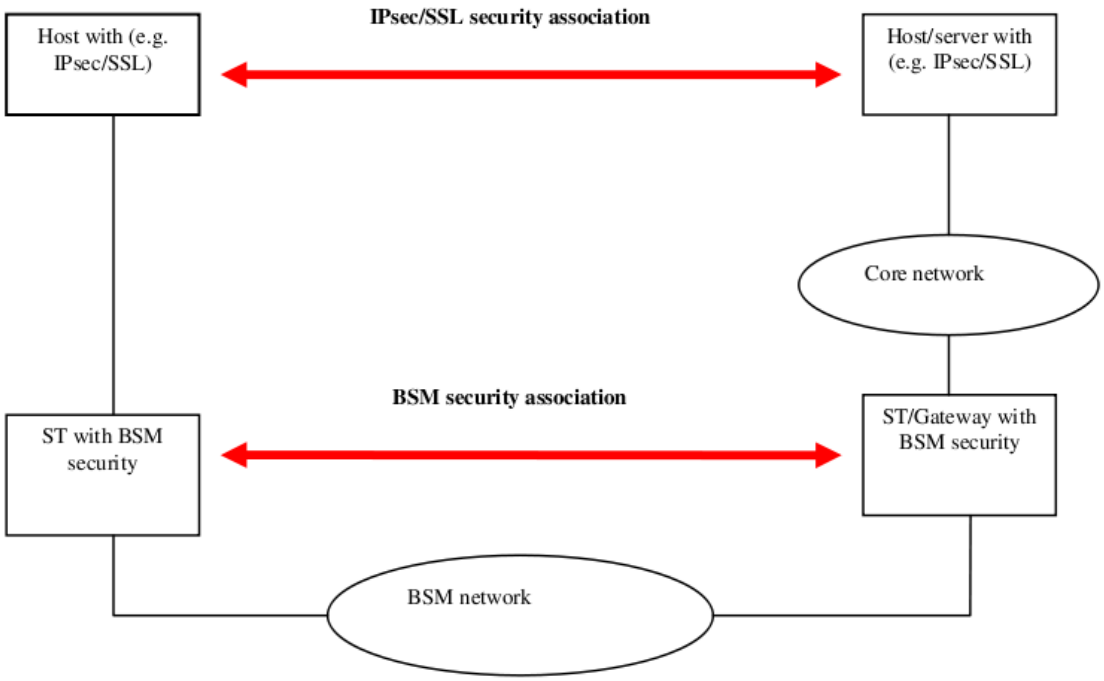


Σχήμα 2: *Σύνδεσμος ασφάλειας μεταξύ των BSM STs/ Πυλών.*

1.2.4.3. Συνδυασμός ασφάλειας του host και της πύλης

Το παράδειγμα αυτό επεκτείνει το Σχήμα 2 προσθέτοντας ασφάλεια end-to-end, όπως φαίνεται στο Σχήμα 3. Το tunnel gateway-to-gateway παρέχει είτε πιστοποίηση είτε εμπιστευτικότητα ή και τα δύο σε όλη την κυκλοφορία μεταξύ των πυλών. Οι ανεξάρτητοι hosts μπορούν να εφαρμόσουν πρόσθετες υπηρεσίες IPsec/ SSL.

Πάρα ταύτα, η χρήση των δύο τεχνολογιών μπορεί να είναι μια πιθανή αιτία καθυστέρησης και κακής απόδοσης.

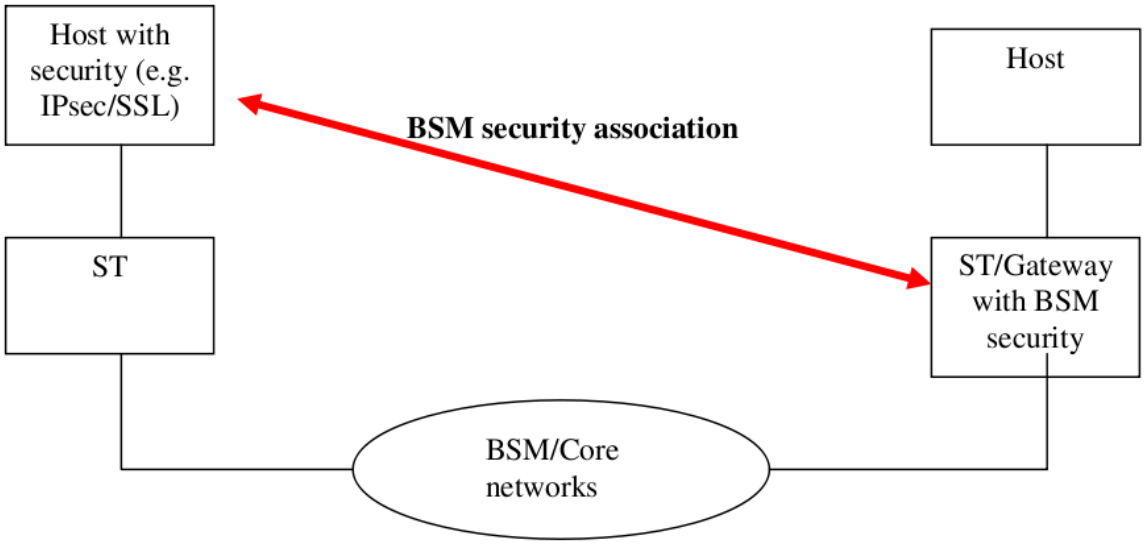


Σχήμα 3: *Σύνδεσμος συνδυαστικής ασφάλειας (BSM κι end host).*

1.2.4.4. Ασφάλεια μεταξύ απομακρυσμένου host και πύλης

Η ασφάλεια αυτή παρέχει στήριξη σε έναν απομακρυσμένο host που χρησιμοποιεί το Internet για να προσεγγίσει το δίκτυο του οργανισμού του (Σχήμα 4). Το tunnel mode απαιτείται μεταξύ του απομακρυσμένου host και της πύλης ασφαλείας (secure gateway). Αν είναι απαραίτητη η ασφάλεια end-to-end τότε ο απομακρυσμένος host μπορεί να χρησιμοποιήσει ένα πρόσθετο SA σε ένα αντίστοιχο host.

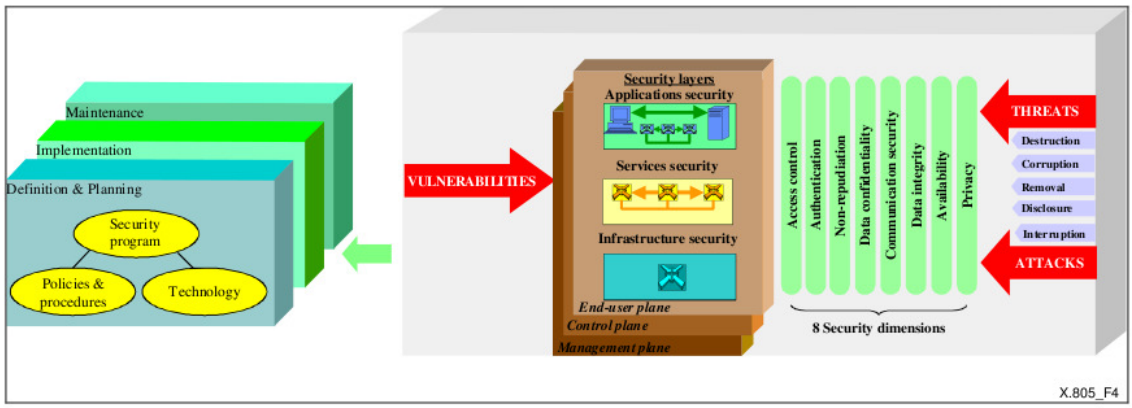
Οι πιο κοινές ρυθμίσεις είναι τα VPNs κι οι απομακρυσμένοι χρήστες (remote users). Για παράδειγμα, αν ο πάροχος επιλέξει VPN μέσω IPsec, τότε χρησιμοποιείται το tunnel mode για την παροχή ασφάλειας για παράδειγμα πάνω σε ένα δίκτυο BSM. Σε αυτό το παραπλήσιο στο end-to-end σενάριο δεν είναι προφανής η προσαρμογή του πρωτοκόλλου ούτε η συμπίεση των δεδομένων εφόσον εκτελείται από Performance Enhancing Proxies (PEP) μέσα στα δίκτυα BSM.



Σχήμα 4: *Σύνδεσμος ασφάλειας για απομακρυσμένη πρόσβαση.*

1.2.5. Συστάσεις του ITU-T – Αρχιτεκτονική ασφάλειας X.805

Η σύσταση αυτή καθορίζει την αρχιτεκτονική για την ασφάλεια του δικτύου παρέχοντας ασφάλεια end-to-end [3]. Αυτή η αρχιτεκτονική έχει εφαρμογή σε πολλά είδη δικτύων στα οποία το βασικό ζήτημα είναι η ασφάλεια end-to-end κι η οποία δεν εξαρτάται από την υποκείμενη τεχνολογία του κάθε δικτύου. Καθορίζει τα γενικά αρχιτεκτονικά στοιχεία που σχετίζονται με την ασφάλεια τα οποία είναι απαραίτητα για την ασφάλεια end-to-end, όπως φαίνεται στο Σχήμα 5. Ο σκοπός εδώ είναι να παρέχει, ως Ίδρυμα για την ανάπτυξη, τις λεπτομερείς συστάσεις για το δίκτυο ασφαλείας end-to-end.



Σχήμα 5: *ITU - X.805 Αρχιτεκτονική ασφάλειας για συστήματα μέσω End-to-End μεταδόσεων.*

Το έγγραφο ορισμού της αρχιτεκτονικής ασφαλείας για τα BSM εφαρμόζει παρόμοια μεθοδολογία με το X.805 αλλά είναι περισσότερη εξειδικευμένη για τα δορυφορικά συστήματα κι υπηρεσίες. Εκτός από την X.805 προσέγγιση end-to-end λαμβάνει υπόψη και την ασφάλεια gateway-to-gateway.

Υπάρχουν αρκετά αρχιτεκτονικά κομμάτια στο X.805 [3] (Σχήμα 5), όπως οι διαστάσεις ασφάλειας, τα στρώματα ασφάλειας, τα επίπεδα ασφάλειας κι η ανάλυση των απειλών και των επιθέσεων σε αυτά τα κομμάτια όπως επίσης κι η ανάπτυξη προγράμματος ασφάλειας. Η αρχιτεκτονική ασφάλειας των BSM αντιμετωπίσει τα περισσότερα από τα παραπάνω ζητήματα με διαφορετική προσέγγιση εστιάζοντας στα δορυφορικά δίκτυα και δίνοντας λιγότερη σημασία στην ασφάλεια end-to-end.

1.2.6. Περίληψη των απαιτήσεων των υπηρεσιών ασφάλειας

- Η ασφάλεια end-to-end (όπως το πρωτόκολλο IPsec) κι η ασφάλεια σε επίπεδο σύνδεσης μπορούν να υπάρχουν παράλληλα χωρίς η μία να εμποδίζει τη λειτουργία της άλλης.
- Η εμπιστευτικότητα των δεδομένων είναι βασική απαίτηση για την αντιμετώπιση των παθητικών απειλών (χρησιμοποιώντας κρυπτογράφηση).
- Εναλλακτική προστασία με τη χρήση της διεύθυνση MAC σε επίπεδο σύνδεσης.
- Πιστοποίηση των τερματικών BSM (επίπεδο σύνδεσης). Αυτό είναι μέρος του key management κι εκτελείται κατά την ανταλλαγή αρχικών κλειδιών και τη φάση της πιστοποίησης.
- Για τις ενεργές απειλές: Απαιτείται η πιστοποίηση της πηγής κι η ακεραιότητα των δεδομένων, χρησιμοποιώντας τεχνικές όπως τον κωδικό πιστοποίησης του μηνύματος (MAC) και τις ψηφιακές υπογραφές. Οι ενεργές επιθέσεις είναι πιο δύσκολο να εκτελεστούν και για το λόγο αυτό η υπηρεσία της ακεραιότητας ή της πιστοποίησης σε ένα δίκτυο BSM δεν είναι υποχρεωτική, αλλά παραμένει σημαντική σε περιβάλλοντα στα οποία πολλά διαφορετικά τερματικά μοιράζονται μια πηγή εκπομπής.
- Αποσύνδεση των λειτουργιών του key management στα BSM από την κρυπτογράφηση των δεδομένων στα BSM, το οποίο εξασφαλίζει τον ανεξάρτητο καθορισμό των συστημάτων αυτών όπως για παράδειγμα την επαναχρησιμοποίηση των υπαρχόντων συστημάτων διαχείρισης της ασφάλειας (για παράδειγμα τα GDOI RFC 3547 [4] και τα GSAKMP RFC 4535 [5]) και/ ή την ανάπτυξη νέων συστημάτων εφόσον αυτό απαιτείται.

Επιπρόσθετα υπάρχουν κάποιες γενικές απαιτήσεις:

- Υποστήριξη των υπηρεσιών χρήστη: Η λύση που θα επικρατήσει για την ασφάλεια πρέπει να χρησιμοποιεί ίδιους μηχανισμούς τόσο για υπηρεσίες μονής εκπομπής (unicast) όσο και πολλαπλής (multicast) (όπως η διαπραγμάτευση, η πιστοποίηση κι οι διαδικασίες keying και re-keying). Όμως στην παρούσα εργασία δεν ασχολούμαστε με αρχιτεκτονική πολλαπλής εκπομπής (multicast).
- Λειτουργικά θέματα: Εξαιτίας της μεγάλης δορυφορικής κάλυψης, τα δορυφορικά συστήματα λειτουργούν σε πολλές διαφορετικές χώρες οι οποίες διέπονται από διαφορετικές νομοθεσίες (σχετικές με την εξουσιοδοτημένη κρυπτογράφηση των αλγορίθμων και με το μήκος των κλειδιών). Επιπλέον, το

δορυφορικό σύστημα θα υπάρχει για πολλά χρόνια και μάλλον θα πρέπει να λειτουργήσει με διαφορετικές εκδόσεις firmware του τερματικού. Έτσι τα συστήματα ασφάλειας BSM πρέπει να υποστηρίζουν ένα πλατύ εύρος για διαφορετικές παραμέτρους κατά τη διάρκεια της φάσης διαπραγμάτευσης με σκοπό να παρέχουν ευελιξία στους χειριστές τους.

- Παροχή συμβατότητας με άλλες υπηρεσίες ή λειτουργίες για την ασφάλεια των συνδρομητών: Λαμβάνοντας υπόψη τους διαφορετικούς ρόλους που έχουν οι διάφοροι παράγοντες (Access Network Operator, Internet Service Provider), είναι πιθανό να υπάρχουν ταυτόχρονα διαφορετικά σενάρια ασφάλειας. Για παράδειγμα, ο ISP (πάροχος) ή ο συνδρομητής μπορεί να χρησιμοποιούν τα δικά τους συστήματα ασφάλειας πάνω στη σύνδεση δεδομένων (όπως κάποιοι χρήστες έχουν την τάση να εφαρμόζουν το πρωτόκολλο IPsec κι άλλοι όχι). Για το λόγο η επιλαχούσα λύση για την ασφάλεια στα BSM δε θα πρέπει να συγκρούεται με τη λύση που προτείνεται από τον πάροχο της υπηρεσίας ή από τον συνδρομητή.
- Συμβατότητα με άλλες λειτουργίες του δικτύου: Σε ένα δορυφορικό σύστημα μπορεί να χρησιμοποιούνται κι άλλες λειτουργίες δικτύου, όπως το Network Address Translation (NAT) ή η επιτάχυνση TCP. `Η λύση για την ασφάλεια στα BSM θα πρέπει να είναι συμβατή με τέτοιες λειτουργίες όπως είναι το NAT/ NAPT, IPsec, SSL, κ.α.
- Προώθηση της ασφάλειας και κανάλι επιστροφής: Η προώθηση της σύνδεσης με privacy είναι σημαντική, όμως η ασφάλεια στη σύνδεση επιστροφής δεν είναι απαραίτητη.
- Εδραίωση εμπιστοσύνης μεταξύ των οντοτήτων που παίρνουν μέρος στην επικοινωνία: Όταν χρησιμοποιείται κρυπτογράφηση για την παροχή προστασίας των δεδομένων, έρχεται στο προσκήνιο το ζήτημα της εμπιστοσύνης. Αυτό το πρόβλημα αφορά τις οντότητες που παράγουν, διανέμουν και διαχειρίζονται τα κρυπτογραφικά κλειδιά και τις πολιτικές ασφάλειας. Η απαίτηση αυτή αφορά τα ζητήματα στα οποία οι οντότητες πρέπει να αναγνωρίζουν την εμπιστοσύνη κατά την εκτέλεση των λειτουργιών αυτών, την πηγή της αρχής κι άλλα σχετικά θέματα.

Όσον αφορά τις σχετικές με την ασφάλεια τεχνολογίες, το IPsec κι η ασφάλεια στο επίπεδο σύνδεσης ικανοποιούν περισσότερο από κάθε άλλο τις απαιτήσεις των υπηρεσιών ασφάλειας για τα BSM.

Το μεγάλο πλεονέκτημα του πρωτοκόλλου IPsec είναι η ευρεία εφαρμογή σε IP routers και hosts. Η απόφαση για χρησιμοποίηση του IPsec στο στρώμα μεταφοράς είναι μια απόφαση που μπορεί να παρθεί από συγκεκριμένο ζεύγος end-hosts. Η χρησιμοποίηση σε επίπεδο tunnel είναι μια επιλογή που γίνεται από τον χρήστη ή τον χειριστή του δικτύου. Το πρωτόκολλο IPsec σε επίπεδο tunnel παρέχει ασφάλεια στα δίκτυα BSM, με το μειονέκτημα όμως πως υπάρχουν overheads. Επιπλέον, αυτή η μέθοδος δεν παρέχει υπηρεσίες ασφάλειας και σε άλλα πρωτόκολλα δικτύου που μπορεί να χρησιμοποιούνται μαζί με το ULE (όπως το MPLS και Ethernet Bridging), απαιτώντας την εφαρμογή κι άλλων μεθόδων. Άλλο ένα ζήτημα στο οποίο η μέθοδος του IPsec δεν πετυχαίνει είναι η ανάγκη προστασίας της ταυτότητας του χρήστη ή δέκτη σε μια μετάδοση.

Η ασφάλεια σε επίπεδο σύνδεσης θεωρείται ένας πρόσθετος μηχανισμός στο IPsec, έχοντας παρόμοιες λειτουργίες, αλλά παρέχει επιπλέον εμπιστευτικότητα και προαιρετική προστασία στις διευθύνσεις MAC των τερματικών BSM. Η ασφάλεια End-to-End, το πρωτόκολλο IPsec κι η ασφάλεια σύνδεσης BSM μπορούν να εφαρμοστούν παράλληλα, με το IPsec να παρέχει ασφάλεια End-to-End μεταξύ των hosts και το επίπεδο σύνδεσης να παρέχει ασφάλεια στη σύνδεση εκπομπής BSM. Ο διαχειριστής της ασφάλειας BSM θα προσπαθήσει να χρησιμοποιήσει μαζί το IPsec με το επίπεδο σύνδεσης έτσι ώστε να παρέχει υπηρεσίες ασφάλειας με τον πιο αποδοτικό τρόπο αποφεύγοντας ταυτόχρονα, όσο είναι δυνατόν, την επικάλυψη των υπηρεσιών αυτών στα διάφορα επίπεδα.

Στα υβριδικά δορυφορικά/ επίγεια σενάρια, όπου ο δορυφορικός κόμβος είναι ένα μέρος του συνολικού επικοινωνιακού μονοπατιού, η ασφάλεια End-to-End (όπως το IPsec) θεωρείται καλύτερη λύση, μπορεί όμως να χρησιμοποιηθεί και το επίπεδο δορυφορικής σύνδεσης ως προσθετικό μέτρο για την ενίσχυση της ασφάλειας των υπηρεσιών BSM.

1.3. Λειτουργικές Απαιτήσεις της Αρχιτεκτονικής Ασφάλειας BSM

Αυτή η εργασία βασίζεται στις υπηρεσίες κι αρχιτεκτονικές BSM όπως ορίζονται από την τελική αναφορά του IABG και το TR 101 985 [6]. Υπάρχει όμως παρόμοια εργασία της ομάδας ETSI TISPAN για τις προδιαγραφές της αρχιτεκτονικής ασφάλειας στα Next Generation Networks (NGN), TR 187 002 [7]. Αυτές οι προδιαγραφές καθορίζουν τις απαραίτητες λειτουργικότητες της ασφάλειας, περιγράφουν τις κατάλληλες λειτουργίες ασφάλειας, τα συστατικά και δομικά μέρη των NGN. Πολλές έννοιες εδώ είναι κοινές με εκείνες των δικτύων BSM.

Η παράγραφος αυτή περιγράφει τα δομικά λειτουργικά μέρη της ασφάλειας BSM και τις αλληλεπιδράσεις με οντότητες που δεν είναι BSM, όπως τα COPS, RADIUS, DIAMETER και PEPs.

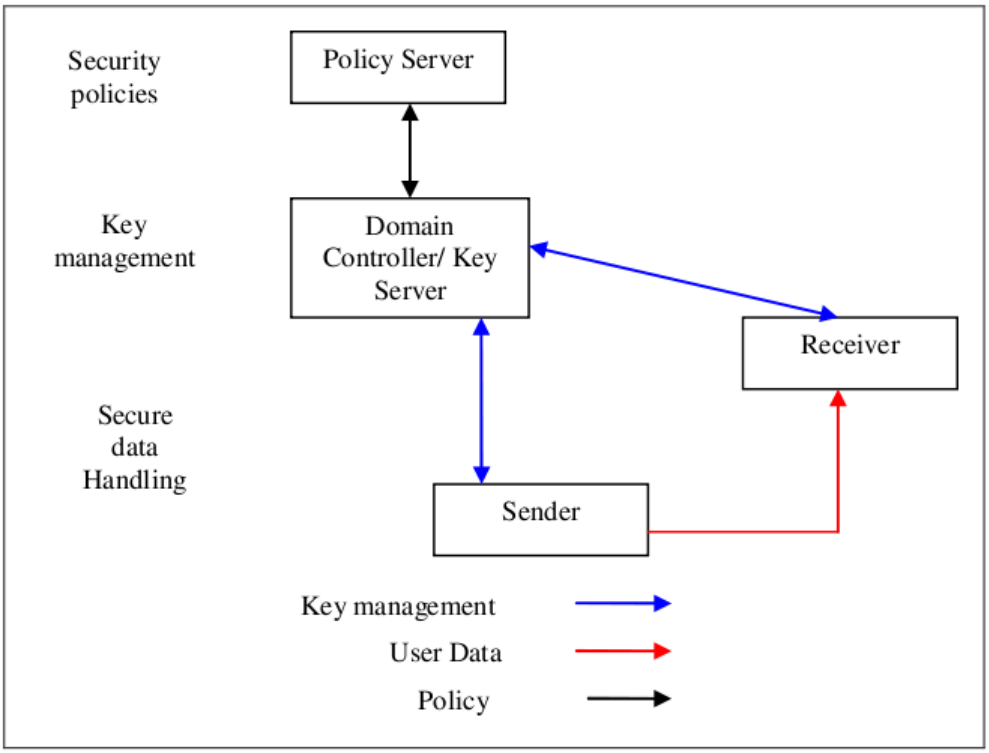
1.3.1. Πλαίσιο Αναφοράς της Ασφάλειας

Το πλαίσιο αναφοράς για την ασφάλεια BSM ακολουθεί το πλαίσιο αναφοράς του IETF κι έχει τρείς ευρύτερες λειτουργικές περιοχές: τον ασφαλή χειρισμό των δεδομένων, το key management και την πολιτική ασφάλειας, όπως φαίνεται στο Σχήμα 6. Το πλαίσιο αυτό ενσωματώνει τις κύριες οντότητες και λειτουργίες που σχετίζονται με την ασφάλεια BSM. Τέτοιες οντότητες ασφάλειας μπορούν να αναπτυχθούν κάτω ή πάνω από το SI-SAP (Σχήμα 6).

Ο στόχος του πλαισίου αναφοράς είναι να παρέχει κάποιο γενικό πλαίσιο σχετικά με τις λειτουργικές περιοχές και τις σχέσεις των περιοχών αυτών. Κάποια ζητήματα

καλύπτουν περισσότερες από μία λειτουργική περιοχή. Ένα παράδειγμα αυτής της περίπτωσης είναι η έκφραση των πολιτικών που αφορούν στα κλειδιά BSM, το οποίο περιέχει τις λειτουργικές περιοχές του key management στα BSM και τις πολιτικές ασφάλειας.

Στα διαγράμματα του πλαισίου αναφοράς, τα μονά "κουτιά" δε αντιστοιχούν σε μια μοναδική οντότητα που εκτελεί μια δεδομένη λειτουργία. Αντίθετα, ένα "κουτί" στο πλαίσιο αναφοράς θα πρέπει να ερμηνεύεται χαλαρά όπως αναφέρεται σε μια δεδομένη λειτουργία σχετικά με τη λειτουργική περιοχή. Αν η λειτουργία εκτελείται στην πραγματικότητα ως μία ή περισσότερες οντότητες αυτό εξαρτάται από τη συγκεκριμένη λύση. Για παράδειγμα, το "κουτί" με την ετικέτα "Key Server" πρέπει να ερμηνευτεί σε γενικούς όρους ως κάτι σχετικό με τις λειτουργίες του key management.



Σχήμα 6: *Λειτουργικές Περιοχές του Συγκεντρωτικού Πλαισίου Αναφοράς της Ασφάλειας BSM.*

Το πλαίσιο αναφοράς μπορεί να είναι είτε συγκεντρωτικό είτε κατανεμημένο. Το συγκεντρωτικό σενάριο είναι αυτό που φαίνεται στο Σχήμα 6. Τα κουτιά είναι οι λειτουργικές οντότητες και τα βέλη είναι οι διεπαφές μεταξύ τους. Τα πρότυπα πρωτόκολλα είναι απαραίτητα για τις διεπαφές αυτές υποστηρίζοντας τις υπηρεσίες μονής/ πολλαπλής εκπομπής μεταξύ των λειτουργικών οντοτήτων. Υπάρχουν τρείς ομάδες των λειτουργικών οντοτήτων:

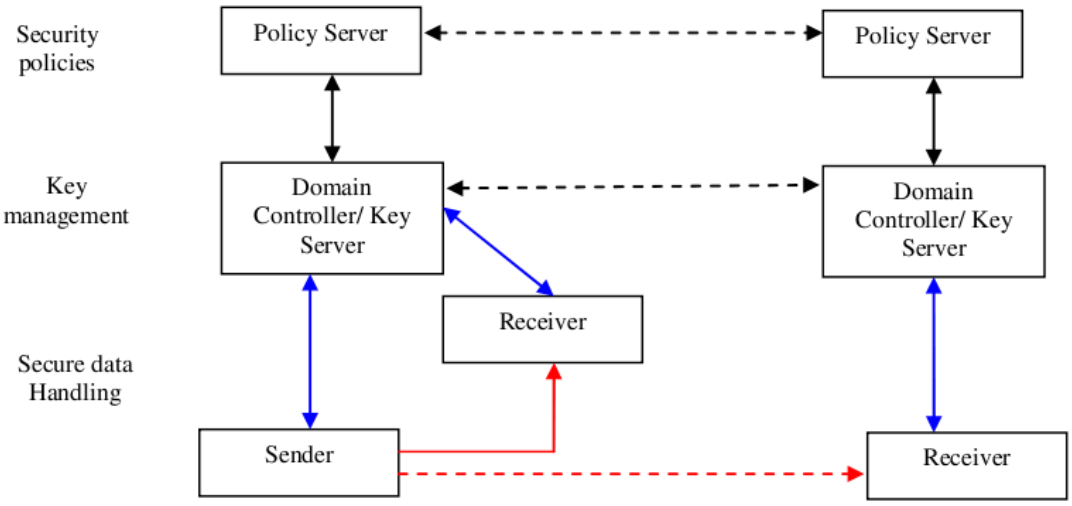
Domain Controller και Key Server

Το Domain Controller και το Key Server (DCKS) αντιπροσωπεύουν τόσο την οντότητα όσο και τις λειτουργίες που σχετίζονται την έκδοση και τη διαχείριση των κρυπτογραφικών κλειδιών που χρησιμοποιούνται από μια περιοχή (domain) μέσα στο δίκτυο BSM. Το DCKS οδηγεί στους ελέγχους για την πιστοποίηση του χρήστη και την εξουσιοδότηση στα υποψήφια μέλη.

Αποστολέας (Sender) και Δέκτης (Receiver)

Τόσο ο αποστολέας (Sender) όσο κι ο δέκτης (Receiver) πρέπει να αλληλεπιδρούν με την οντότητα DCKS για λόγους σχετικούς με το key management. Σε αυτό περιλαμβάνεται η πιστοποίηση/ εξουσιοδότηση του χρήση ή και του τερματικού (όπως τα STs), η απόκτηση των υλικών κρυπτογράφησης (keying) σύμφωνα με τις πολιτικές του key management, η απόκτηση νέων κλειδιών κατά τη διάρκεια των ενημερώσεων των κλειδιών (key updates) και η απόκτηση άλλων μηνυμάτων σχετικά με τη διαχείριση των υλικών κρυπτογράφησης (keying) και με τις παραμέτρους ασφάλειας.

Το κατανεμημένο πλαίσιο αναφοράς (Σχήμα 7) χρειάζεται για τις λύσεις που είναι επεκτάσιμες σε σενάρια που καλύπτουν περισσότερες από μία διαχειριστική περιοχή ή περιοχή ασφάλειας του BSM. Ένα απλό παράδειγμα διαχειριστικής περιοχής ή περιοχής ασφάλειας είναι μια εταιρία VPN που χρησιμοποιεί δίκτυο BSM. Πάρα ταύτα, οι πύλες BSM μπορούν να χρησιμοποιηθούν για προώθηση δεδομένων (όπως η μεταφορά αρχείων από ένα επίγειο ISP) σε STs που ανήκουν σε διαφορετικά VPN με διάφορες πολιτικές ασφάλειας και κανόνες.



Σχήμα 7: *Λειτουργικές Περιοχές του Κατανεμημένου Πλαισίου Αναφοράς της ασφάλειας BSM.*

Στο κατανεμημένο σχέδιο, η οντότητα DCKS έρχεται σε επαφή με άλλες οντότητες DCKS έτσι ώστε να επιτευχθεί επεκτασιμότητα στις υπηρεσίες που είναι σχετικές με το key management). Οι οντότητες DCKS απαιτούν ένα μέσο πιστοποίησης των αντίστοιχων οντοτήτων DCKS, ένα μέσο εξουσιοδότησης κι ένα μέσο για την ασφαλή

αλληλεπίδραση για να διανέμουν τα κλειδιά και η πολιτική ασφαλείας. Παρόμοια, οι Policy Servers πρέπει να αλληλεπιδρούν μεταξύ τους με ασφάλεια και να επιτρέπουν την επικοινωνία και την ενδυνάμωση των πολιτικών ασφάλειας μέσα από το internet.

1.3.1.1. Χειρισμός των Δεδομένων (Ιδιωτικότητα κι Ακεραιότητα)

Ο ασφαλής χειρισμός των δεδομένων καλύπτει όλες τις σχετικές με την ασφάλεια κατεργασίες των δεδομένων τόσο από τον αποστολέα όσο κι από τον δέκτη. Σε μια τυπική ασφαλή συνεδρία, τα δεδομένα πρέπει να είναι:

- Κρυπτογραφημένα, χρησιμοποιώντας ένα κλειδί, κυρίως για τον έλεγχο πρόσβασης και πιθανών για τη εμπιστευτικότητα.
- Πιστοποιημένα, για την επαλήθευση της πηγής και της ακεραιότητας των δεδομένων.

1.3.1.2. Διαχείριση κλειδιού (Key Management)

Η υπηρεσία ασφάλειας περιγράφει τη λειτουργικότητα της διανομής κι ενημέρωσης του κρυπτογραφικού υλικού (key material) μέσω της διάρκειας μιας ενεργούς συνεδρίας. Ανάμεσα στα στοιχεία αυτή της υπηρεσίας ασφαλείας είναι και τα εξής:

- DCKS στην ειδοποίηση των μελών (αποστολέα ή δέκτη) σχετικά με το τρέχον κρυπτογραφημένο υλικό (keying material) (για παράδειγμα κλειδιά κρυπτογράφησης και πιστοποίησης, βοηθητικά κλειδιά για τη διαχείριση της ασφάλειας, κλειδιά για την πιστοποίηση της πηγής, κ.α.).
- Ενημέρωση του τρέχοντος υλικού κρυπτογράφησης ανάλογα με τις συνθήκες και τις πολιτικές.
- Τερματισμός της συνεδρίας με ασφαλή τρόπο.

Τα Key Servers και τα μέλη μπορούν να εκμεταλλευτούν το κοινό Public Key Infrastructure (PKI) για να αυξήσουν την επεκτασιμότητα της πιστοποίησης και της εξουσιοδότησης. Για να καταστεί διαλειτουργικό κι ασφαλές το πρωτόκολλο ασφαλείας IP, αυτή η υπηρεσία ασφαλείας πρέπει να συγκεκριμενοποιήσει τα host abstractions όπως είναι το Security Association Database (SAD) και το Security Policy Database (SPD) παρόμοια με το πρωτόκολλο IPsec. Για το λόγο αυτό, αυτή η υπηρεσία ασφαλείας λαμβάνει υπόψη της τις απαιτήσεις του key management για το πρωτόκολλο IP.

Η υπηρεσία αυτή περιγράφει επίσης τη λειτουργικότητα της επικοινωνίας σχετικά με το key management ανάμεσα σε διάφορους DCKS servers στο κατανεμημένο σχέδιο. Το key management εμφανίζεται τόσο στο συγκεντρωτικό όσο και στο κατανεμημένο σχέδιο όπως μας δείχνει το Σχήμα 7.

1.3.1.3. Καθιέρωση κι Ενδυνάμωση της Πολιτικής Ασφαλείας

Οι πολιτικές ασφαλείας BSM πρέπει να παρέχουν τους κανόνες για τη λειτουργία και των υπόλοιπων στοιχείων του Πλαισίου Αναφοράς. Οι πολιτικές ασφαλείας μπορούν να διανεμηθούν με τρόπο ad-hoc σε κάποιες περιπτώσεις. Πάρα ταύτα, ο καλύτερος συντονισμός και τα μεγαλύτερα επίπεδα ασφάλειας μπορούν να επιτευχθούν αν το Policy Controller διανέμει πολιτικές ασφαλείας στα μέλη του BSM. Για παράδειγμα, η πολιτική πρέπει να καθορίσει το απαραίτητο επίπεδο εξουσιοδότησης που απαιτείται για τη συμμετοχή μιας οντότητας σε μια συνεδρία.

Η μετάφραση των κανόνων πολιτικής από ένα μοντέλο δεδομένων σε ένα άλλο είναι πολύ πιο δύσκολη σε ένα κατανεμημένο περιβάλλον ασφάλειας. Αυτό ισχύει ιδιαίτερα τα μέλη των υπηρεσιών εκτείνονται σε πολλές διαχειριστικές περιοχές. Οι πολιτικές που καθορίζονται σε ανώτερο επίπεδο από το ένα εργαλείο Policy Management πρέπει να μεταφράζονται σε πιο ακριβείς κανονισμούς τους οποίους οι μηχανισμοί ασφαλείας μπορούν να καταλάβουν και να εφαρμόσουν.

Η διαχείριση της πολιτικής ασφαλείας περιλαμβάνει το σχεδιασμό του Policy Server, τους ορισμούς της συγκεκριμένης πολιτικής που θα χρησιμοποιηθεί από τις υπηρεσίες IP κι από την ασφάλεια σε επίπεδο εφαρμογής και την επικοινωνία των πρωτοκόλλων μεταξύ του Policy Server και του Key Server. Η υπηρεσία ασφάλειας μπορεί να αναγνωριστεί χρησιμοποιώντας διάφορους μηχανισμούς:

- Χρησιμοποιώντας μια πρότυπη υποδομή πολιτικής , όπως είναι η αρχιτεκτονική του Policy Decision Point και του Policy Enforcement Point (RFC 2748 και RFC 3084) [8] [9].
- Χρησιμοποιώντας το πρωτόκολλο key management για τη μεταφορά της πολιτικής ασφαλείας.
- Χρησιμοποιώντας άλλα πρωτόκολλα όπως είναι το Session Initiation Protocol (SIP) για τη μεταφορά της πολιτικής ασφαλείας ή ακόμα και μέσω των διαδικτυακών υπηρεσιών.

Στο ελάχιστον όμως αυτή η υπηρεσία ασφαλείας αναγνωρίζεται από διάφορους ορισμούς πολιτικής, όπως είναι οι συνθήκες και οι λειτουργίες τις εκάστοτε συνεδρίας ασφαλείας.

1.3.1.4. Περιγραφή του Συνδέσμου Ασφαλείας (Security Association)

Ο Σύνδεσμος Ασφαλείας (Security Association – SA) είναι ένας πολύ διαδεδομένος όρος στα κρυπτογραφικά συστήματα. Ο μηχανισμός SA συνήθως έχει τα εξής χαρακτηριστικά:

- Selectors: όπως οι διευθύνσεις της πηγής και του προορισμού.

- Ιδιότητες: όπως είναι ο Security Parameter Index (SPI), το cookie pair και οι ταυτότητες.
- Πολιτική κρυπτογράφησης: όπως είναι οι αλγόριθμοι, η διάρκεια των κλειδιών, το μήκος των κλειδιών που χρησιμοποιούνται για την πιστοποίηση ή την εμπιστευτικότητα.
- Κλειδιά, όπως είναι η πιστοποίηση, η κρυπτογράφηση, και τα κλειδιά υπογραφής.

Οι τρεις κατηγορίες των SA είναι:

Registration SA (REG)
Είναι μια ξεχωριστή unicast SA μεταξύ του DCKS και κάθε μέλους (αποστολείς και δέκτες). Αυτό το SA απαιτείται για (αμφίδρομες) unicast επικοινωνίες μεταξύ του DCKS κι ενός μέλους (μπορεί να είναι αποστολέας ή δέκτης). Αυτή η κατηγορία SA μπορεί να υπάρξει μόνο μεταξύ του DCKS κι ενός μέλους. Δίνεται στην οντότητα DCKS έλεγχος πρόσβασης στα κλειδιά, με διανομή πολιτικής στα μέλη (ή στα πιθανά μέλη) και με διάδοση κλειδιών ασφαλείας στα μέλη.

Το Registration SA εισάγεται από ένα μέλος για να πάρει πληροφορίες SA από την οντότητα DCKS. Με αυτό τον τρόπο το μέλος αιτεί τη συμμετοχή του στην ασφαλή συνεδρία, ή αρχικοποιεί ξανά τα κλειδιά SA αφού έχει αποσυνδεθεί από το δίκτυο (για παράδειγμα όταν ένας υπολογιστής host απενεργοποιείται κατά τη διάρκεια των λειτουργιών re-key). Η πληροφορία SA που μπορεί να προέλθει από την οντότητα DCKS σχετίζεται (και χρησιμοποιείται για να προστατεύσει) τη διαδικασία re-key και τα δεδομένα δύο Sass (βλέπε παρακάτω).

Πάρα ταύτα, η απαίτηση για Registration SA δεν υποδηλώνει την ανάγκη ύπαρξης πρωτοκόλλου εγγραφής (registration protocol) για τη δημιουργία του Registration SA. Το Registration SA μπορεί αντ' αυτού να στηθεί με χειροκίνητους τρόπους, όπως να αναπτυχθεί πάνω σε μια smart card. Έτσι, αυτό που είναι σημαντικό είναι η ύπαρξη του Registration SA κι ότι χρησιμοποιείται για να την προστασία άλλων SAs.

Re-key SA (REKEY)
Είναι ένα μοναδικό SA ανάμεσα στο διαχειριστή ασφάλειας και τα μέλη. Σε κάποιες περιπτώσεις, μια οντότητα DCKS χρειάζεται να έχει τη δυνατότητα να "σπρώξει" νέα κλειδιά κατά τη διάρκεια μιας ασφαλούς συνεδρίας. Το τελευταίο ικανοποιείται με το Re-key SA.

Data Security SA (DATA)
Είναι ένα SA δεδομένων μεταξύ των πηγών και των προορισμών. Το Data Security SA προστατεύει τα δεδομένα μεταξύ του αποστολέα και του δέκτη. Από την οπτική του αποστολέα υπάρχει τουλάχιστον ένα Data Security SA για τον δέκτη.

1.3.1.5. Λειτουργικά Στοιχεία της Ασφάλειας BSM

Για το χειρισμό των δεδομένων, αποστολείς και δέκτες BSM μπορούν να είναι οι τελικοί χρήστες ή τα BSM τερματικά (ST ή πύλες). Η ιδιωτικότητα/ ακεραιότητα των δεδομένων επιτυγχάνεται χρησιμοποιώντας μεθόδους ασφάλειας που συμφωνούνται κατά τη διάρκεια της ανταλλαγής μηνυμάτων key management και σύμφωνα με τους κανονισμούς της πολιτικής ασφαλείας BSM.

Για τη λειτουργία του key management, η οντότητα DCKS αναφέρεται ως BSM Network manager κι έχει την ευθύνη της δημιουργίας και της διανομής των κλειδιών στους BSM αποστολείς και δέκτες. Οι κατηγορίες του Συνδέσμου Ασφαλείας (Security Association): REG (εγγραφή), REKEY και DATA μπορεί να χρησιμοποιηθούν ξεχωριστά ή και συνδυασμένα ανάλογα με τις υπηρεσίες BSM και τους κανονισμούς της πολιτικής ασφάλειας.

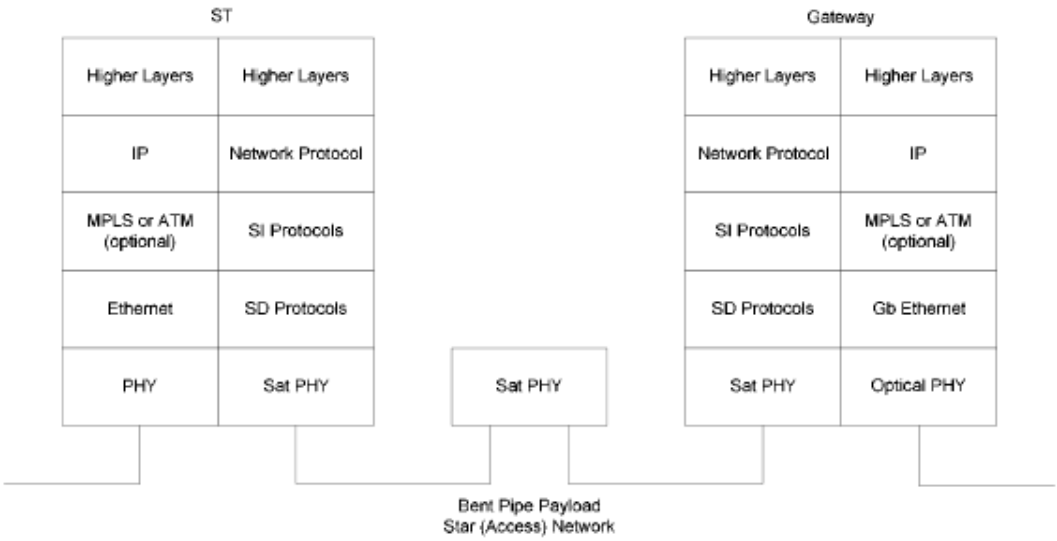
Για την πολιτική ασφαλείας BSM, μπορεί να δημιουργηθεί από το BSM Network manager ή από άλλη οντότητα (όπως είναι η NCC). Τέτοιου είδους πολιτική πρέπει να διανέμεται σε όλες τις οντότητες ασφάλειας στα BSM, χρησιμοποιώντας ασφαλείς μηχανισμούς όπως είναι ο COPS ή το πρωτόκολλο key management.

1.3.2. Γενικό Πρωτόκολλο Αρχιτεκτονικής BSM

Το γενικό πρωτόκολλο αρχιτεκτονικής BSM συμπεριλαμβανομένων και των λειτουργιών ασφαλείας παρουσιάζεται στο Σχήμα 10. Το σχήμα δείχνει τις οντότητες ασφάλειας πάνω και κάτω από το SI – SAP. Το μήνυμα ασφάλειας περνάει μέσα από το SI-U-SAP ή το SI-C-SAP ή το SI-M-SAP ανάλογα από τη φύση του μηνύματος. Περισσότερες λεπτομέρειες για αυτό παρουσιάζονται σε επόμενη παράγραφο.

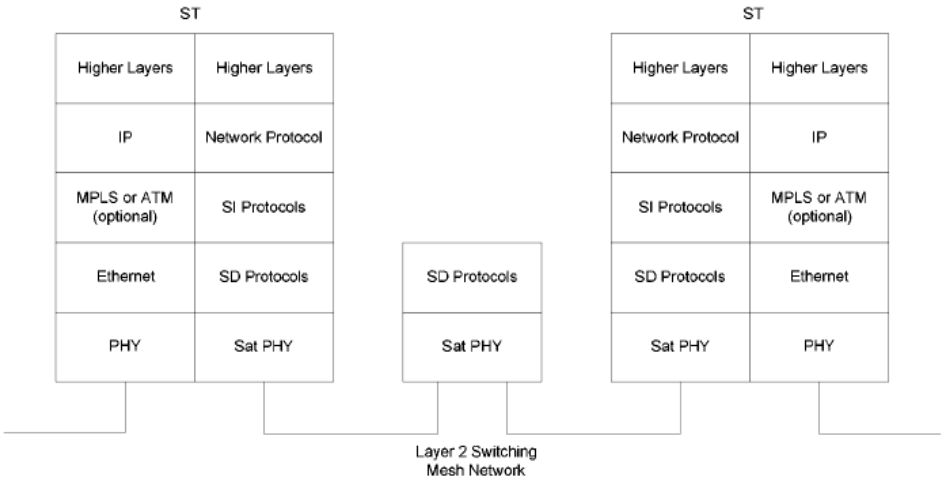
Η αρχιτεκτονική BSM καθορίζει τους σχηματισμούς αστέρα (star) και πλέγματος (mesh):

- *Δίκτυο Πρόσβασης* (σχηματισμός αστέρα) χρησιμοποιώντας μη αναγεννητικά δορυφορικά συστήματα. Σε αυτή την τοπολογία το Internet είναι προσβάσιμο με μία αναπήδηση (hop) μέσω μιας πύλης. Το Σχήμα 8 παρουσιάζει τη στοίβα πρωτοκόλλου για το δίκτυο αστέρα και το μη αναγεννητικό payload.



Σχήμα 8: *Τοπολογία αστέρα: παράδειγμα στοίβας πρωτοκόλλου.*

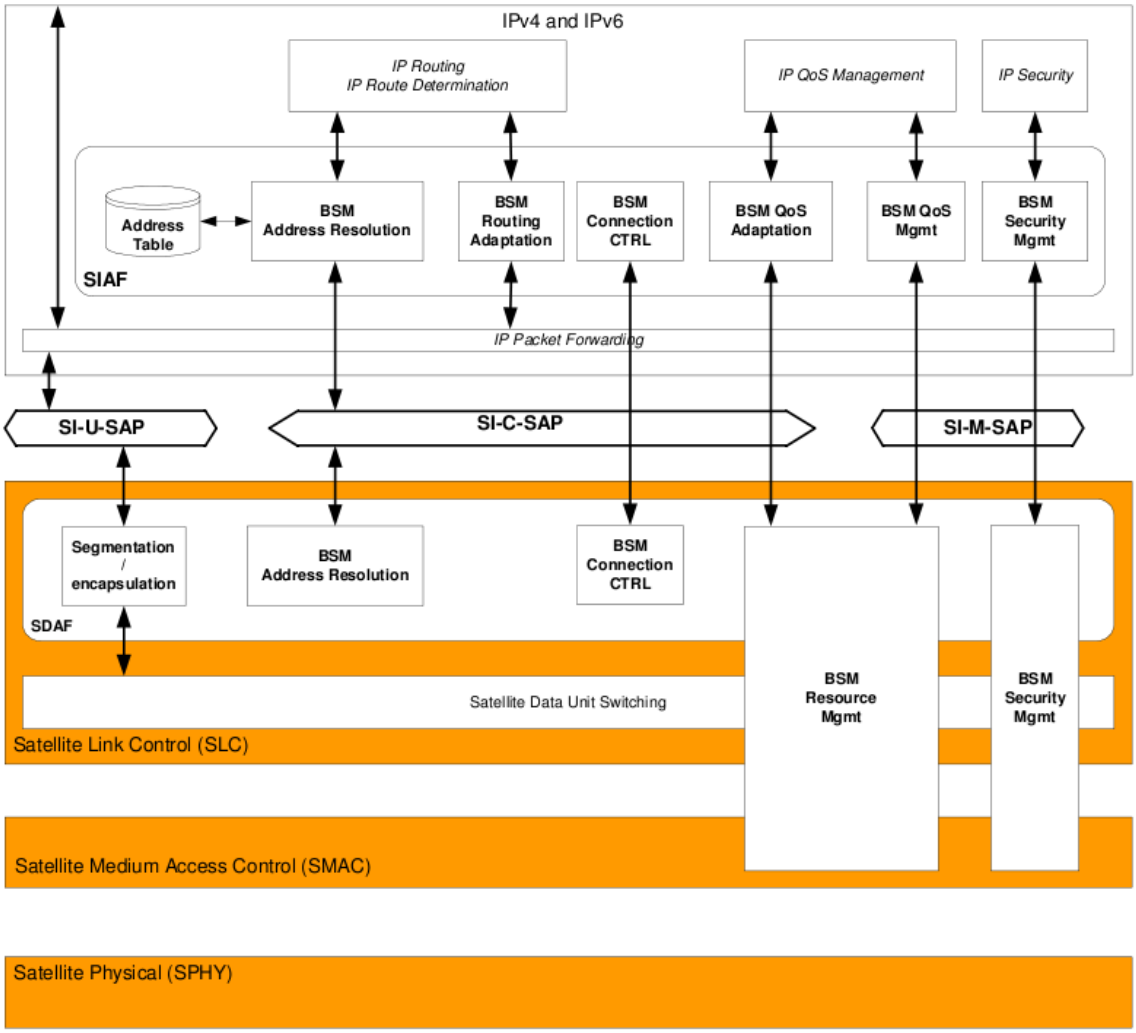
- *Δίκτυο Πλέγματος* χρησιμοποιώντας peer-to-peer τρόπο επικοινωνίας μεταξύ τερματικών/ πυλών. Όταν η σύνδεση peer-to-peer παρέχεται με μία αναπήδηση (ST σε ST), ο σχηματισμός αυτός χρησιμοποιεί μια on-board συσκευή επεξεργασίας. Αυτή η τοπολογία συχνά συσχετίζεται με σενάρια γεφύρωσης (bridging) και μεταγωγής (switching) (βλέπε Σχήμα 9). Η τοπολογία πλέγματος μπορεί επίσης να υποστηρίζεται μέσω ενός μη αναγεννητικού payload με διπλή αναπήδηση: Τα δεδομένα πηγαίνουν από τη πηγή ST σε μια πύλη κι από μια πύλη σε ένα προορισμό ST, Μια ειδική περίπτωση της τοπολογίας πλέγματος είναι όταν ένα BSM χρησιμοποιείται για σύνδεση μεταξύ τομέων, ένα πιθανό σενάριο τόσο για την περίπτωση της πολυεκπομπής όσο και της γεφύρωσης.



Σχήμα 9: *Τοπολογία πλέγματος: παράδειγμα στοίβας πρωτοκόλλου με Επίπεδο 2 μεταγωγής σε δορυφόρο.*

Αναφορικά με την ασφάλεια, και στις δύο τοπολογίες η διαδικασία της ασφάλειας μπορεί να χωριστεί σε δύο φάσεις:

- Καθιέρωση της ασφάλειας: όπως είναι η οντότητα πιστοποίησης κι η ανταλλαγή κλειδιών. Αυτή είναι συνήθως μια επίπεδη λειτουργία ελέγχου στο επίπεδο σύνδεσης (για παράδειγμα DVB-RCS, παρόμοια με την ιδέα εκτός ζώνης σηματοδοσίας (out of band signaling) κι επίπεδος χρήστης στα ανώτερα επίπεδα (παρόμοια με την ιδέα εντός ζώνης σηματοδοσία in-band signaling).
- Ασφαλής ανταλλαγή δεδομένων: όπως χρησιμοποιώντας κωδικοποίηση κι ακεραιότητα στα δεδομένα. Αυτή είναι συνήθως μια επίπεδη λειτουργία χρήστη.



Σχήμα 10: *BSM στοίβα πρωτοκόλλου για υπηρεσίες unicast.*

1.3.3. Αλληλεπιδράσεις μεταξύ της ασφάλειας κι άλλων μη BSM Policy οντοτήτων

1.3.3.1. Χρήση COPS για την παροχή της πολιτικής ασφαλείας

Ο οργανισμός IETF ορίζει το πρωτόκολλο (RFC 2748) [8] Common Open Policy Server (COPS) ως επεκτάσιμο πρωτόκολλο που επιτρέπει στους policy servers (Policy PDPs) να μεταφέρουν αποφάσεις πολιτικής στις συσκευές δικτύου. Το COPS είναι σχεδιασμένο με τέτοιο τρόπο ώστε να υποστηρίζει πολλαπλούς τύπους πελατών πολιτικής.
Στα δίκτυα BSM, το COPS μπορεί να χρησιμοποιηθεί για να πετύχει QoS ή να μεταφέρει πληροφορίες ασφάλειας μεταξύ των οντοτήτων διαχείρισης BSM και των δορυφορικών τερματικών (πυλών/ ST).

Στο RFC 3084 [9], περιγράφεται η χρήση του πρωτοκόλλου COPS στην υποστήριξη της παροχής της πολιτικής (COPS-PR). Αυτή η προδιαγραφή είναι ανεξάρτητη από το είδος της πολιτικής που προβλέπεται (QoS, Ασφάλεια, κ.α.). Το μοντέλο δεδομένων που υποθέτεται σε αυτό το κείμενο βασίζεται στην ιδέα του Policy Information Bases (PIBs) το οποίο καθορίζει τα δεδομένα της πολιτικής. Με στόχο την υποστήριξη του μοντέλου που περιλαμβάνει πολλαπλούς Policy – PDPs ελέγχοντας μη επικαλυπτόμενες περιοχές της πολιτικής με ένα μόνο Policy Enforcement Point (Policy – PEP), ο τύπος πελάτη που καθορίζεται από το Policy – PEP στον Policy PDP είναι μοναδικός για τη συγκεκριμένη περιοχή της πολιτικής που διαχειρίζεται. Ένας μόνο τύπος πελάτη για μια δεδομένη περιοχή της πολιτικής (για παράδειγμα η ασφάλεια) θα χρησιμοποιηθεί για όλα τα PIBs που υπάρχουν στην περιοχή αυτή. Ο πελάτης θα πρέπει να μεταχειριστεί όλους τους τύπους COPS-PR που υποστηρίζει ως μη επικαλυπτόμενα κι ανεξάρτητα namespaces που τα instances δε θα πρέπει να μοιράζονται.

1.3.3.2. Πρωτόκολλο Radius/ Diameter

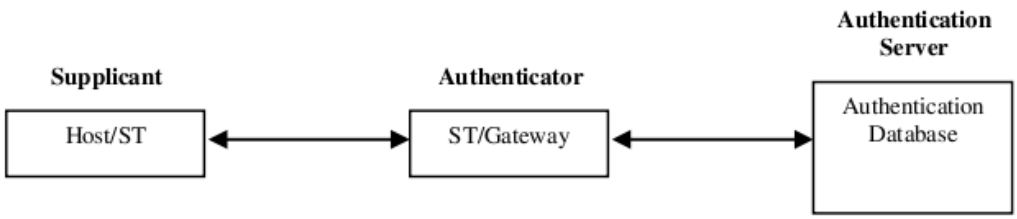
Τα πρωτόκολλα AAA, Πιστοποίηση (Authentication), Εξουσιοδότηση (Authorization) και Λογιστική Καταγραφή (Accounting), όπως είναι το RADIUS (RFC 2865) [10] αναπτύχθηκαν αρχικά για να παρέχουν dial-up υπηρεσίες με τη χρήση του πρωτοκόλλου Point-to-Point (PPP) καθώς επίσης και πρόσβαση στους τερματικούς servers. Αυτό επιτυγχάνεται χρησιμοποιώντας το πρωτόκολλο Remote Authentication Dial-In User Service (RADIUS).

Το RADIUS client είναι υπεύθυνο να μεταφέρει τις πληροφορίες για το χρήστη στους RADIUS servers που έχουν ορισθεί και μετά να ενεργήσει ανάλογα με το περιεχόμενο που επιστέφεται. Οι RADIUS servers είναι υπεύθυνοι να δεχθούν τις αιτήσεις του χρήστη για σύνδεση, να πιστοποιήσουν τον χρήστη και να επιστρέψουν όλες τις απαραίτητες πληροφορίες για τις ρυθμίσεις στον πελάτη έτσι ώστε να μπορέσει να

παρέχει τις ανάλογες υπηρεσίες στον χρήστη. Ένας RADIUS server μπορεί να λειτουργήσει ως διαμεσολαβητής πελάτης (proxy client) για άλλους RADIUS servers ή για άλλου είδους servers πιστοποίησης. Για να είναι εφικτό αυτό, ο πελάτης δημιουργεί ένα "Αίτημα προσπέλασης" που περιέχει τέτοιες ιδιότητες όπως είναι το όνομα χρήστη, ο κωδικός χρήστη, η ταυτότητα του πελάτη και τη θύρα της ταυτότητας (Port ID) από την οποία ο χρήστης θα έχει πρόσβαση. Όταν χρησιμοποιείται κωδικός, αυτός παραμένει κρυφός με τη βοήθεια της μεθόδου RSA Message Digest Algorithm MD5.

Το πρωτόκολλο αυτό εφαρμόζεται και χρησιμοποιείται ευρέως. Η εμπειρία έχει δείξει πως όταν χρησιμοποιείται σε μεγάλης κλίμακας συστήματα μπορεί να οδηγήσει σε μειωμένη απόδοση και σε απώλεια δεδομένων, κυρίως γιατί δεν υπάρχει πρόβλεψη για τον έλεγχο συμφόρησης. Ως αποτέλεσμα αυτών το RFC 3588 [11] προτείνει ως εναλλακτικό του RADIUS το πρωτόκολλο DIAMETER. Για παράδειγμα στο RFC 3162 [12], δεν απαιτείται στο RADIUS υποστήριξη IPsec, η οποία όμως υποστήριξη IPsec είναι υποχρεωτική για το DIAMETER ενώ η υποστήριξη TLS είναι προαιρετική.
Στα δίκτυα BSM, η επικοινωνία μεταξύ DIAMETER πελάτη – εξυπηρετητή (client-server) είναι διάφανη για την ασφάλεια BSM. Πάρα ταύτα όταν γίνεται χρήση του RADIUS θα πρέπει να χρησιμοποιείται είτε το πρωτόκολλο IPsec είτε ασφάλεια σε επίπεδο σύνδεσης έτσι ώστε να μεταδίδονται τα μηνύματα πιστοποίησης/ εξουσιοδότησης.
Στην παρούσα εργασία οι έννοιες των πρωτοκόλλων RADIUS/ DIAMETER έχουν αφαιρεθεί κι αντ'αυτών ορίζονται παρακάτω τρείς οντότητες πιστοποίησης και στο Σχήμα 11 περιγράφεται η διαδικασία πιστοποίησης:

- *Supplicant*: Ο πελάτης ή το μηχάνημα που αιτείται πρόσβασης στο δίκτυο
- *Authenticator*: Το δεύτερο στοιχείο της αρχιτεκτονικής είναι η συσκευή πρόσβασης ή η πύλη, που είναι συνήθως διακόπτης ή σημείο πρόσβασης (access-point) λη κόμβος. Η συσκευή είναι ένα σύστημα πιστοποίησης που επιτρέπει ή μπλοκάρει την πρόσβαση στο δίκτυο.
- *Authentication Server*: Τυπικά πρόκειται για RADIUS/DIAMETER server από τον οποίο οι χρήστες θα πρέπει να πιστοποιηθούν κι από τον οποίο θα πάρουν εξουσιοδότηση.



Σχήμα 11: *Διαδικασία Πιστοποίησης.*

1.3.3.3. Αλληλεπιδράσεις της ασφάλειας BSM Network με το Address Translation (NAT)

Η πιο συχνή χρήση του πρωτοκόλλου IPsec (RFC 2401) [13] είναι ίσως η παροχή δυνατοτήτων Εικονικού Ιδιωτικού Δικτύου (Virtual Private Networking- VPN). Μια πολύ δημοφιλής εφαρμογή των VPNs είναι η εργασία εξ αποστάσεως με πρόσβαση στο εταιρικό Intranet. Στις μέρες μας, τα Network Address Translations (NATs) όπως ορίζονται στο RFC 3022 [14], αναπτύσσονται ευρέως στις οικιακές πύλες, όπως επίσης και σε άλλες τοποθεσίες που είναι πιθανό να υπάρχει ανάγκη για εργασία εξ αποστάσεως, όπως τα ξενοδοχεία για παράδειγμα. Όμως το θέμα της συμβατότητας των IPsec – NAT είναι ένα μεταβατικό πρόβλημα και σχετίζεται με το περιορισμένο χώρο διευθύνσεων στο IPv4. Στο IPv6 η αντιμετώπιση της έλλειψης διευθύνσεων δεν είναι πρόβλημα. Για το λόγο αυτό, μια χρήσιμη λύση για τη συμβατότητα των IPsec – NAT θα πρέπει να αναπτύσσεται σε μικρότερη χρονική κλίμακα από το IPv6. Παρακάτω παρουσιάζονται κάποια από τα θέματα συμβατότητα μεταξύ του IPsec και του NAT (3715) [15]:

- Ασυμβατότητα μεταξύ του πρωτοκόλλου AH (RFC 2402) [16] στο IPsec και του NAT, διότι η επικεφαλίδα (header) AH ενσωματώνει τις IP διευθύνσεις της πηγής και του προορισμού κατά τον έλεγχο της ακεραιότητας του κωδικοποιημένου μηνύματος.
- Ασυμβατότητα μεταξύ των αθροισμάτων ελέγχου (checksums) και του NAT. Τα αθροίσματα ελέγχου (checksums) TCP και UDP εξαρτώνται από τις IP διευθύνσεις πηγής και προορισμού κατά την περίληψη της ψευδοεπικεφαλίδας (pseudo-header) στον υπολογισμό. Ως αποτέλεσμα, όταν τα αθροίσματα ελέγχου (checksums) υπολογίζονται κι ελέγχονται μετά την παραλαβή, θα ακυρώνονται κατά το πέρασμα από το NAT ή κάποια αντίστροφη συσκευή NAT.

Σύμφωνα με τα παραπάνω, όταν χρησιμοποιείται το IPsec στα δίκτυα BSM προκύπτουν θέματα NAT κατά την απομακρυσμένη πρόσβαση, σε σενάρια terminal-to-terminal και end-to-end. Μια λύση είναι η χρήση του Realm Specific IP (RSIP, RFC 3103, RFC 3104) [17] [18]. Η λύση αυτή λειτουργεί μόνο για ένα NAT κι όχι για πολλαπλά NATs. Μια πιο γενικευμένη λύση είναι εκείνη που προτείνει το IETF για τα δίκτυα BSM, η οποία επιλύει τα θέματα συμβατότητας εφαρμόζοντας τα παρακάτω:

- Ενσωμάτωση του πρωτοκόλλου UDP στα πακέτα ESP στο IPsec όπως καθορίζεται στο RFC 3948 [19].
- Διαχείριση κλειδιών του IPsec και διάσχιση NAT όπως καθορίζεται στο RFC 3947 [20].
- Η μορφή AH του IPsec δε θα πρέπει να χρησιμοποιείται.

1.3.4. Αλληλεπιδράσεις μεταξύ της ασφάλειας και των εξυπηρετητών Performance Enhancing Proxies (PEP)

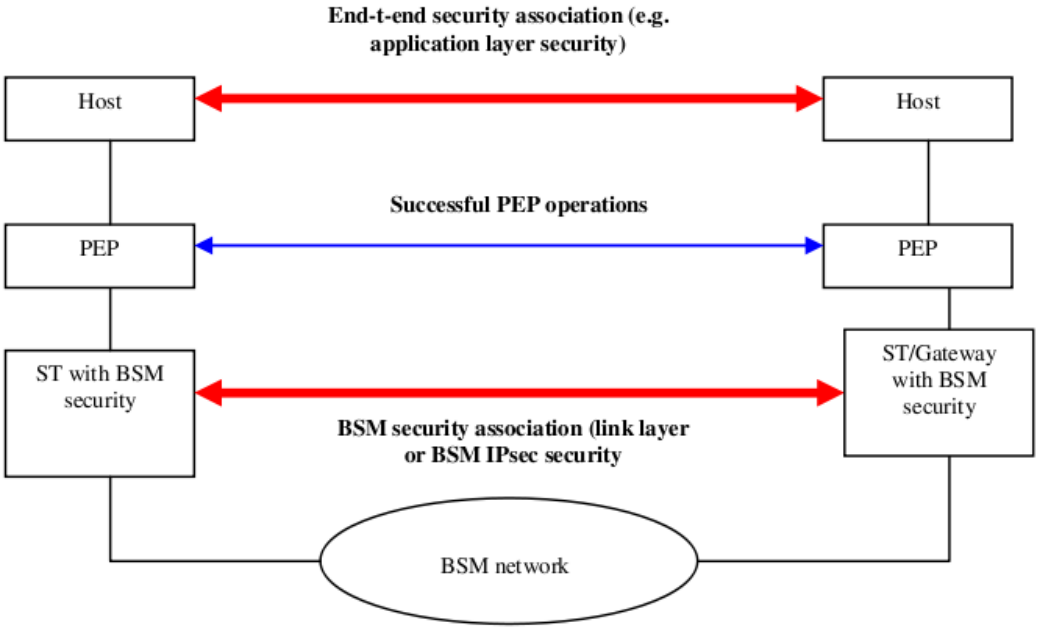
Το Transmission Control Protocol (RFC 0793) [21] (TCP) χρησιμοποιείται ως το πρωτόκολλο στο επίπεδο μεταφοράς από πολλές εφαρμογές του internet και του intranet. Πάρα ταύτα, σε συγκεκριμένα περιβάλλοντα, το TCP κι άλλα πρωτόκολλα ανωτέρων επιπέδων έχουν περιορισμένη απόδοση λόγω των χαρακτηριστικών σύνδεσης του συγκεκριμένου περιβάλλοντος. Ο εξυπηρετητής Performance Enhancing Proxy (PEP) μπορεί να εκτελέσει τεχνικές μετριασμού (mitigation) (RFC 3135) [22]. Ο PEP χρησιμοποιείται για να βελτιώσει την απόδοση των πρωτοκόλλων του internet στα δικτυακά μονοπάτια όπου η απόδοση υστερεί λόγω των χαρακτηριστικών της επικοινωνίας (για παράδειγμα στη δορυφορική επικοινωνία) ή ενός υποδικτύου του μονοπατιού. Υπάρχει ένα μεγάλο φάσμα συσκευών PEP (RFC 3449) [23], που κυμαίνονται από απλές συσκευές (για παράδειγμα φιλτράρισμα ACK) σε πιο προηγμένες συσκευές (για παράδειγμα stateful συσκευές που χωρίζουν μια TCP σύνδεση σε δύο ξεχωριστά μέρη).

Πάρα ταύτα η χρήση PEP σε δορυφορικό περιβάλλον έχει κάποιες επιπτώσεις στην ασφάλεια. Η πιο επιβλαβής επίπτωση του τερματισμού της end-to-end σημασιολογίας μιας σύνδεσης είναι η απενεργοποίηση της end-to-end χρήσης του IPsec. Γενικότερα, ένας χρήστης ή ένας διαχειριστής δικτύου θα πρέπει να επιλέξει ανάμεσα στην χρήση των PEPs και του IPsec. Αν το IPsec χρησιμοποιείται end-to-end, οι PEPs που εφαρμόζονται ή οι ενδιάμεσοι κόμβοι στο δίκτυο δεν μπορούν να εξετάσουν τις επικεφαλίδες μεταφοράς ή εφαρμογής των IP πακέτων λόγω της κρυπτογράφησης των IP πακέτων μέσω της επικεφαλίδας ESP του IPsec (είτε στο επίπεδο μεταφοράς είτε στο tunnel) που καθιστά την επικεφαλίδα TCP και το payload ακατάληπτο για τους PEPs. Χωρίς να μπορεί να εξετάσει τις επικεφαλίδες μεταφοράς ή εφαρμογής, ένας PEP δε μπορεί να λειτουργήσει με το βέλτιστο δυνατό τρόπο ή μπορεί να μην λειτουργήσει και καθόλου.

Αν η εφαρμογή του PEP δεν είναι διάφανη στους χρήστες και οι χρήστες μπορούν να εμπιστευτούν το PEP, τότε το IPsec μπορεί να χρησιμοποιηθεί ξεχωριστά μεταξύ κάθε τερματικού συστήματος και PEP. Πάρα ταύτα, στις περισσότερες περιπτώσεις αυτή η εναλλακτική δεν είναι επιθυμητή ή δεν είναι αποδεκτή καθώς τα τερματικά συστήματα δεν μπορούν να εμπιστευτούν τα PEPs γενικά. Με μια διάφανη εφαρμογή του PEP, είναι δύσκολο για το τερματικό σύστημα να εμπιστευτεί το PEP διότι δεν είναι σε θέση να γνωρίζει την ύπαρξη του. Ακόμα κι αν ο χρήστης είναι ενήμερος για το PEP, είναι προβληματική (αν όχι ακατόρθωτη) σύσταση αποδεκτών συνδέσμων ασφαλείας με το PEP, διατηρώντας παράλληλα τη μη αναγεννητική φύση των PEPs.

Για την συνύπαρξη του IPsec και των PEPs απαιτούνται κάποια βήματα. Αν ένας τερματικός χρήστης επιλέξει να χρησιμοποιήσει το IPsec για κάποια μεταφορά, κι όχι για κάποια άλλη, ο μηχανισμός PEP μπορεί να εφαρμοστεί σε εκείνη τη μεταφορά

χωρίς το IPsec. Άλλη μία εναλλακτική είναι η εφαρμογή του IPsec μεταξύ δύο PEPs σε μια κατανεμημένη εφαρμογή PEP, κάτι που τουλάχιστον προστατεύει τη μεταφορά μεταξύ των δύο PEPs (το πρόβλημα εμπιστοσύνης των PEPs παραμένει).



Σχήμα 12: *Κατάλληλοι σύνδεσμοι ασφάλειας για τη διασυνεργασία των PEPs.*

Στα δίκτυα BSM κι όπως φαίνεται και στο Σχήμα 12, οι PEPs μπορούν να χρησιμοποιηθούν με επιτυχία με τις ακόλουθες ρυθμίσεις:

- Με ασφάλεια σε επίπεδο σύνδεσης που λειτουργεί μόνο σε δορυφορική ζεύξη (όπως είναι η ασφάλεια DVB – RCS)
- Με το πρωτόκολλο IPsec, εξασφαλίζοντας πως το IPsec χρησιμοποιείται ανάμεσα σε BSM ST/ πύλη, όπου η κρυπτογράφηση IPsec γίνεται στην εισερχόμενη κίνηση μετά τις λειτουργίες PEP κι η αποκρυπτογράφηση γίνεται στην εξερχόμενη κίνηση πριν τις λειτουργίες PEP.

Βλέπουμε πως η απαίτηση είναι η ασφάλεια να εφαρμόζεται με τέτοιο τρόπο που να επιτρέπει στις οντότητες PEP την πρόσβαση στις επικεφαλίδες του πρωτοκόλλου μεταφοράς (όπως το TCP). Έτσι η ασφάλεια σε επίπεδο σύνδεσης κι εφαρμογής είναι διάφανη στους PEPs. Όταν χρησιμοποιείται το IPsec, τότε οι λειτουργίες PEP θα πρέπει να εκτελούνται έξω από τη διαδικασία IPsec, όπως δείχνει και το Σχήμα 12. Η τελική αναφορά του IABG για το πρόγραμμα ESA [24] δίνει περισσότερες πληροφορίες σχετικά με τους PEPs και τα θέματα ασφάλειας στους δορυφόρους.

1.3.5. Περίληψη των απαιτήσεων της αρχιτεκτονικής ασφάλειας

Η αρχιτεκτονική της ασφάλειας BSM θα πρέπει να καλύπτει τις παρακάτω λειτουργικές απαιτήσεις:

- Η αρχιτεκτονική ασφάλειας BSM θα πρέπει να ακολουθεί μια σπονδυλωτή προσέγγιση, έτσι ώστε διαφορετικά υποσύνολα των λειτουργιών της ασφάλειας να μπορούν να εφαρμοστούν (όχι όλα ή τίποτα).
- Είτε να υποστηρίζονται υπηρεσίες ασφαλείας πάνω από το σημείο SI – SAP (όπως το IPsec) είτε κάτω από το SI – SAP (όπως η ασφάλεια σε επίπεδο σύνδεσης χρησιμοποιώντας το DVB – RCS).
- Οι υπηρεσίες ασφαλείας θα πρέπει να περιέχουν ιδιωτικότητα των δεδομένων, πιστοποίηση της πηγής BSM, ενώ η πιστοποίηση του τερματικού BSM είναι προαιρετική.
- Μια λειτουργία διαχείρισης της ασφάλειας του δικτύου BSM πρέπει να μπορεί να εφαρμοστεί για να παρέχεται συνολικός έλεγχος στις διαδικασίες ασφάλειας και στις πολιτικές.
- Η εφαρμογή των λειτουργιών της διαχείρισης των κλειδιών ασφαλείας (συμφωνία κλειδιών και διανομή) και του χειρισμού των δεδομένων (κρυπτογράφηση κι ακεραιότητα) πρέπει να διασφαλίζει τη μη ύπαρξη αρνητικών επιπτώσεων στην απόδοση του δικτύου BSM.
- Δυνατότητα να εφαρμοστεί το μεγάλο εύρος των μεθόδων για την ασφάλεια έτσι ώστε να μπορεί να προσπεραστεί το εμπόδιο των διαφορετικών νόμων σχετικών με την κρυπτογράφηση στις διάφορες χώρες.

1.4. Ορισμός της λειτουργικής αρχιτεκτονικής της ασφάλειας BSM

Σε αυτή την παράγραφο ορίζονται τα στοιχεία της αρχιτεκτονικής BSM μαζί με τις λεπτομερείς αλληλεπιδράσεις γύρω από τη διεπαφή SI – SAP.

1.4.1. Λεπτομερής λειτουργική αρχιτεκτονική της ασφάλειας BSM

Η παράγραφος αυτή παρουσιάζει το λεπτομερές σύστημα ασφάλειας σε διάφορες αρχιτεκτονικές περιπτώσεις. Αυτές οι περιπτώσεις ασφάλειας επικεντρώνονται στην τοποθέτηση των λειτουργιών ασφάλειας πάνω ή κάτω από το σημείο SI – SAP. Για παράδειγμα οι οντότητες ασφάλειας του key management και της κρυπτογράφησης των δεδομένων μπορούν να είναι κι οι δύο πάνω ή κάτω από το σημείο SI – SAP ή μία πάνω κι η άλλη κάτω. Όλες αυτές οι περιπτώσεις εξετάζονται σε αυτή την παράγραφο.

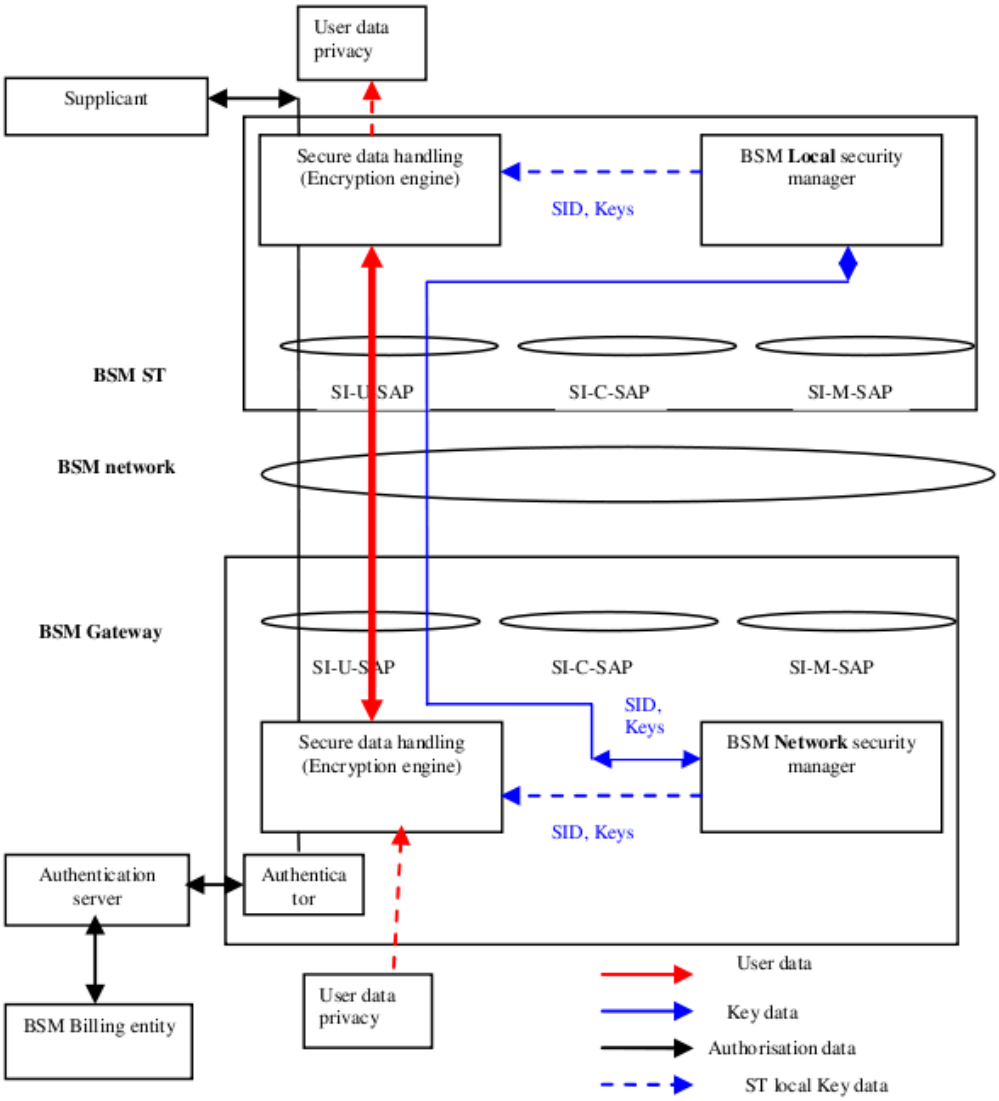
Επιπρόσθετα, παρουσιάζεται η ιδέα του Security Association Identity (SID) του BSM. Για παράδειγμα, αν υπάρχει ασφαλής σύνδεση μεταξύ ενός ST και μιας πύλης, τότε το SID είναι ο αριθμός αναφοράς που θα χρησιμοποιηθεί για να μεταφέρει τις πληροφορίες ασφαλείας μεταξύ των διαχειριστών ασφάλειας του τοπικού δικτύου BSM όπως είναι τα

κλειδιά κρυπτογράφησης, οι μέθοδοι των ψηφιακών υπογραφών κι ανταλλαγή πολιτικών ασφαλείας.

Αν υπάρχει μόνο ένας διαχειριστής ασφάλειας του δικτύου BSM, τότε το SID θα είναι μοναδικό για ολόκληρο το δίκτυο BSM. Στην αντίθετη περίπτωση, που υπάρχουν αρκετοί διαχειριστές ασφάλειας του δικτύου (για παράδειγμα ένας για κάθε ISP), τότε το SID πρέπει να χρησιμοποιείται σε συνδυασμό με τα BSM-ID των οντοτήτων πηγής και προορισμού, με σκοπό την αναγνώριση των συνδέσμων ασφαλείας μεταξύ δύο οντοτήτων BSM.

Οι περιπτώσεις ασφάλειας που παρουσιάζονται σε αυτή την παράγραφο εφαρμόζονται εξίσου σε BSM τοπολογίες αστέρα και πλέγματος. Στην τοπολογία πλέγματος χωρίς On-Board Processor (OBP), τα STs επικοινωνούν μεταξύ τους μέσω μιας πύλης BSM (hub). Στην τοπολογία πλέγματος με OBP, τα STs επικοινωνούν απευθείας μεταξύ τους χωρίς την ανάγκη της πύλης BSM (hub). Με σεβασμό στις περιπτώσεις ασφαλείας που παρουσιάζονται εδώ, οι τοπολογίες αστέρα και πλέγματος (χωρίς OBP) θεωρούνται ίδιες, όπου η λειτουργία του διαχειριστή ασφάλειας του δικτύου BSM είναι πιθανό να τοποθετείται στην πύλη BSM (hub). Πάρα ταύτα, για την τοπολογία πλέγματος με OBP, η κύρια διαφορά είναι πως η λειτουργία του διαχειριστή ασφάλειας του δικτύου BSM μπορεί να βρίσκεται σε οποιοδήποτε ST του BSM.

1.4.1.1. Περίπτωση 1: IPsec κι οντότητες ασφάλειας στα BSM



Σχήμα 13: *Περίπτωση 1.IPsec κι οντότητες ασφάλειας BSM.*

Όπως φαίνεται στο Σχήμα 13, η περίπτωση αυτή περιγράφει τη χρήση του IPsec πάνω σε ένα δίκτυο BSM με ρύθμιση ασφάλειας gateway-to-gateway όπως είναι το σενάριο της VPN πάνω σε δορυφόρους. Το πρωτόκολλο IPsec λειτουργεί πάνω από το σημείο SI – SAP.

Η ασφάλεια παρέχεται μεταξύ των πυλών ασφαλείας (που μπορεί να συνυπάρχουν με το ST ή πύλη του BSM). Η πύλη ασφάλειας αποτελείται από δύο λειτουργικές οντότητες:

- Την οντότητα του ασφαλούς χειρισμού των δεδομένων (μηχανισμός ιδιωτικότητας/ ακεραιότητας): Το IPsec πρέπει να λειτουργεί σε tunnel mode.
- Την οντότητα διαχείρισης κλειδιών: Σε μια τοπολογία αστέρα, θα υπάρχει ένας διαχειριστής ασφάλειας δικτύου για ολόκληρο το δίκτυο BSM (βρίσκεται μαζί

με την πύλη/ κόμβο του BSM). Επιπλέον σε κάθε ST υπάρχει ένας τοπικός διαχειστής ασφάλειας.

Το Σχήμα 13 δείχνει πως όλες οι οντότητες ασφάλειας βρίσκονται πάνω από το σημείο SI – SAP. Το διάγραμμα δείχνει επίσης πως το SI – SAP (η διεπαφή χρήστη) χρησιμοποιείται μόνο για τη μετάδοση των πληροφοριών ασφαλείας (μηνύματα δεδομένων του χρήστη και διαχείρισης κλειδιών).

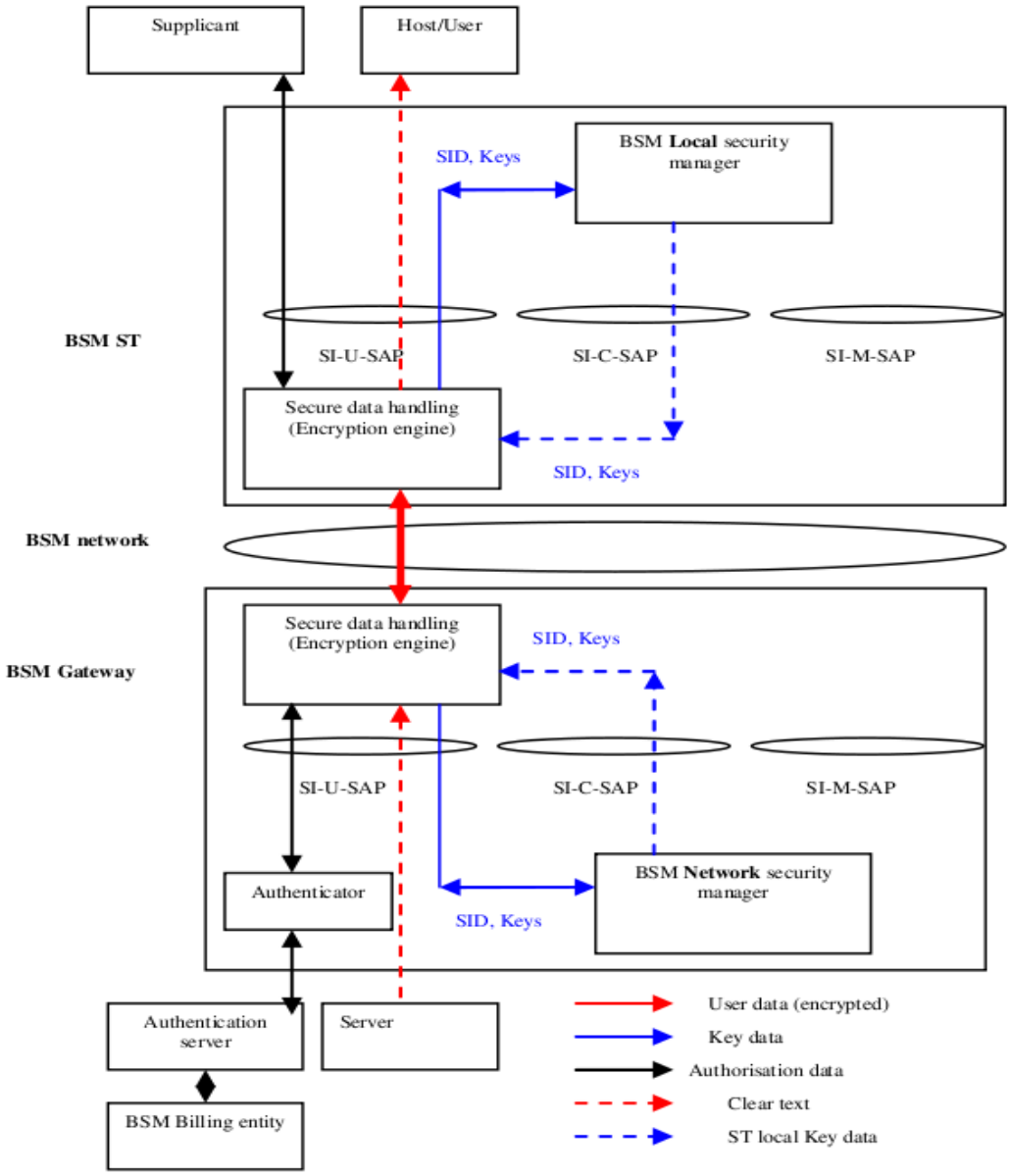
Η διαδικασία πιστοποίησης του πελάτη (οντότητες Suplicant, Authenticator και Authentication server) φαίνεται επίσης στο σχήμα, όπου το IPsec χρησιμοποιείται για να μεταφέρει πληροφορίες πιστοποίησης (όπως είναι το όνομα χρήστη και ο κωδικός) μεταξύ του Suplicant και του Authentication server.

Τόσο ο Authentication server όσο κι ο διαχειριστής δικτύου BSM επικοινωνούν με το BSM NCC σχετικά με την ασφάλεια και την εξουσιοδότηση. Για λόγους απλοποίησης του διαγράμματος αυτές οι αλληλεπιδράσεις δε φαίνονται εδώ. Όπως περιγράφηκε στην παράγραφο 1.3.2., οι σύνδεσμοι ασφαλείας registration και re-key θα πρέπει να αναπτύσσονται ανάμεσα στο διαχειριστή ασφάλειας δικτύου BSM και του τοπικούς διαχειριστές ασφάλειας σε κάθε ST. Στην περίπτωση του IPsec, το πρωτόκολλο IETF Internet Key Exchange (IKE) (RFC 4109) [25] πρέπει να χρησιμοποιείται για την καθιέρωση όλων των συνδέσμων ασφαλείας. Αυτό θα εξασφαλίσει την αμοιβαία πιστοποίηση μεταξύ όλων των οντοτήτων ασφαλείας, καθιερώνοντας τα κλειδιά που χρησιμοποιούνται μεταγενέστερα για να διασφαλίσουν τα δεδομένα του χρήστη. Η χρήση του IKE διασφαλίζει επίσης τη συμβατότητα μεταξύ των BSM των γενικών (επίγειων) συστημάτων ασφαλείας του Internet.

Όμως η χρήση του IPsec για multicast είναι μία πρόκληση διότι τα tunnel IPsec πρέπει να ρυθμιστούν από τις πύλες BSM για κάθε ST, το οποίο είναι αποτελεσματικό για unicast ρύθμιση και τα πλεονεκτήματα της IP πολυεκπομπής χάνονται.

Το έγγραφο για την αρχιτεκτονική ασφαλείας του Internet Protocol (RFC 4301) [26] περιγράφει τις υπηρεσίες ασφαλείας για την κίνηση στο επίπεδο IP. Η αρχιτεκτονική αυτή ορίζει κυρίως τις υπηρεσίες των unicast πακέτων του Internet Protocol (IP), όπως επίσης και για τα χειροκίνητα ρυθμισμένα multicast πακέτα IP.

1.4.1.2 Περίπτωση 2: Οντότητες ασφάλειας BSM μεικτών επιπέδων σύνδεσης (διαχειριστής ασφαλείας πάνω από το SI-SAP και μηχανισμοί ασφάλειας κάτω από το SI-SAP)



Σχήμα 14: *Περίπτωση 2.Οντότητες ασφαλείας BSM μεικτών επιπέδων σύνδεσης.*

Όπως φαίνεται στο Σχήμα 14, η περίπτωση αυτή περιγράφει τη χρήση της ασφάλειας σε επίπεδο σύνδεσης (κάτω από το SI-SAP) με key management (διαχειριστής ασφαλείας) ως εφαρμογή (πάνω από το SI-SAP σε τοπολογία αστέρα) με ένα συγκεντρωτικό διαχειριστή ασφαλείας δικτύου (μπορεί να συνυπάρχει με την πύλη/ κόμβο BSM). Τυπικά παραδείγματα των συστημάτων αυτών είναι τα DVB – RCS με MPE ή με Unidirectional Lightweight Encapsulation (ULE) RFC 4326 [27] ενθυλάκωση IP.

Παρόμοια με την περίπτωση 1, η ασφάλεια παρέχεται μεταξύ των πυλών ασφαλείας (μπορεί να βρίσκεται μαζί με τα ST ή τις πύλες του BSM). Η πύλη ασφάλειας αποτελείται από δύο λειτουργικές οντότητες:

- Την οντότητα ασφαλούς χειρισμού των δεδομένων (μηχανισμός ιδιώτικότητας/ ακεραιότητας): για παράδειγμα η ασφάλεια DVB-RCS που εκτελεί κρυπτογράφηση δεδομένων κάτω από το SI-SAP.
- Την οντότητα key management: Με μια τοπολογία αστέρα, υπάρχει ένας διαχειριστής δικτύου για ολόκληρο το δίκτυο BSM (τοποθετείται μαζί με την πύλη/ κόμβο του BSM). Πρόσθετα υπάρχει ένα διαχειριστής ασφαλείας τοπικού δικτύου για κάθε ST.

Η διαδικασία πιστοποίησης του πελάτη (οντότητες Suplicant, Authenticator και Authentication server) φαίνεται επίσης στο σχήμα, όπου η ασφάλεια σε επίπεδο σύνδεσης χρησιμοποιείται για να μεταφέρει πληροφορίες πιστοποίησης (όπως είναι το όνομα χρήστη και ο κωδικός) μεταξύ του Suplicant και του Authentication server.

Στο Σχήμα 14 φαίνονται επίσης οι οντότητες ασφαλείας πάνω και κάτω από το SI-SAP. Το διάγραμμα δείχνει επίσης πως το SI-U-SAP (η διεπαφή χρήστη) χρησιμοποιείται για να μεταφέρει με ασφάλεια τις πληροφορίες του χρήστη, ενώ η ασφαλής πληροφορία του key management μεταφέρεται μέσω της διεπαφής SI-U-SAP. Τα μηνύματα πιστοποίησης του πελάτη χρησιμοποιούν τη διεπαφή SI-U-SAP.

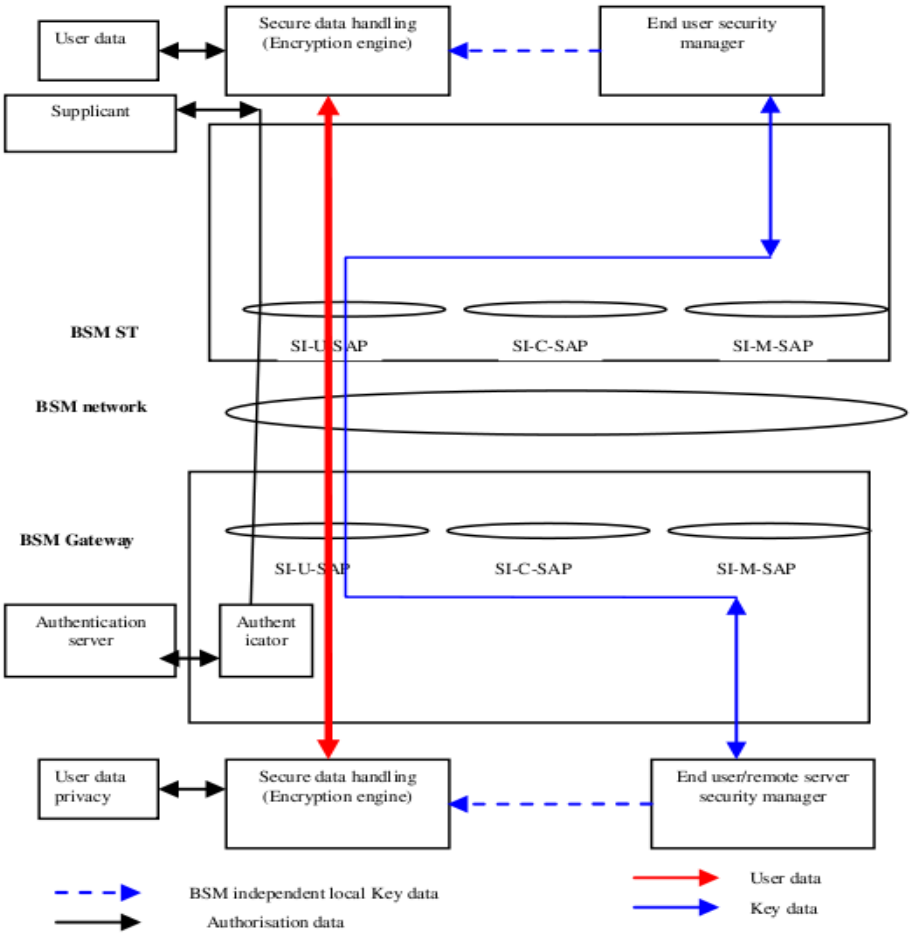
Τόσο ο Authentication server όσο κι ο διαχειριστής δικτύου BSM επικοινωνούν με το BSM NCC σχετικά με την ασφάλεια και την εξουσιοδότηση. Για λόγους απλοποίησης του διαγράμματος αυτές οι αλληλεπιδράσεις δε φαίνονται εδώ. Όπως περιγράφηκε στην παράγραφο 1.3.2, οι σύνδεσμοι ασφαλείας registration και re-key θα πρέπει να αναπτύσσονται ανάμεσα στο διαχειριστή ασφάλειας δικτύου BSM και του τοπικούς διαχειριστές ασφάλειας σε κάθε ST. Στην περίπτωση της ασφάλειας στο επίπεδο σύνδεσης, πρέπει να χρησιμοποιείται η συγκεκριμένη ασφάλεια δορυφορικών συστημάτων. Για παράδειγμα, για τα δορυφορικά συστήματα DVB-RCS, οι διαδικασίες της σύνδεσης και της ανταλλαγής κλειδιών, σύμφωνα με τις συστάσεις του DVB-RCS, πρέπει να χρησιμοποιούνται για την εδραίωση των συνδέσμων ασφαλείας. Για τα συστήματα BSM που λειτουργούν με ULE πρέπει να χρησιμοποιούνται οι συγκεκριμένες διαδικασίες key management για το ULE. (RFC 4326) [27].

Το τελευταίο διασφαλίζει την αμοιβαία πιστοποίηση μεταξύ των οντοτήτων ασφαλείας, εδραιώνοντας τα κλειδιά που χρησιμοποιούνται μεταγενέστερα για τη διασφάλιση των δεδομένων χρήστη. Η χρήση της ασφάλειας σε επίπεδο σύνδεσης πιστοποιεί επίσης και τα τερματικά BSM (STs και πύλες), το οποίο δεν είναι δυνατό με τη χρήση του IPsec (Περίπτωση 1).

Ο σύνδεσμος ασφαλείας SID πρέπει να χρησιμοποιείται σε όλες τις ανταλλαγές μηνυμάτων διαχείρισης ασφάλειας.

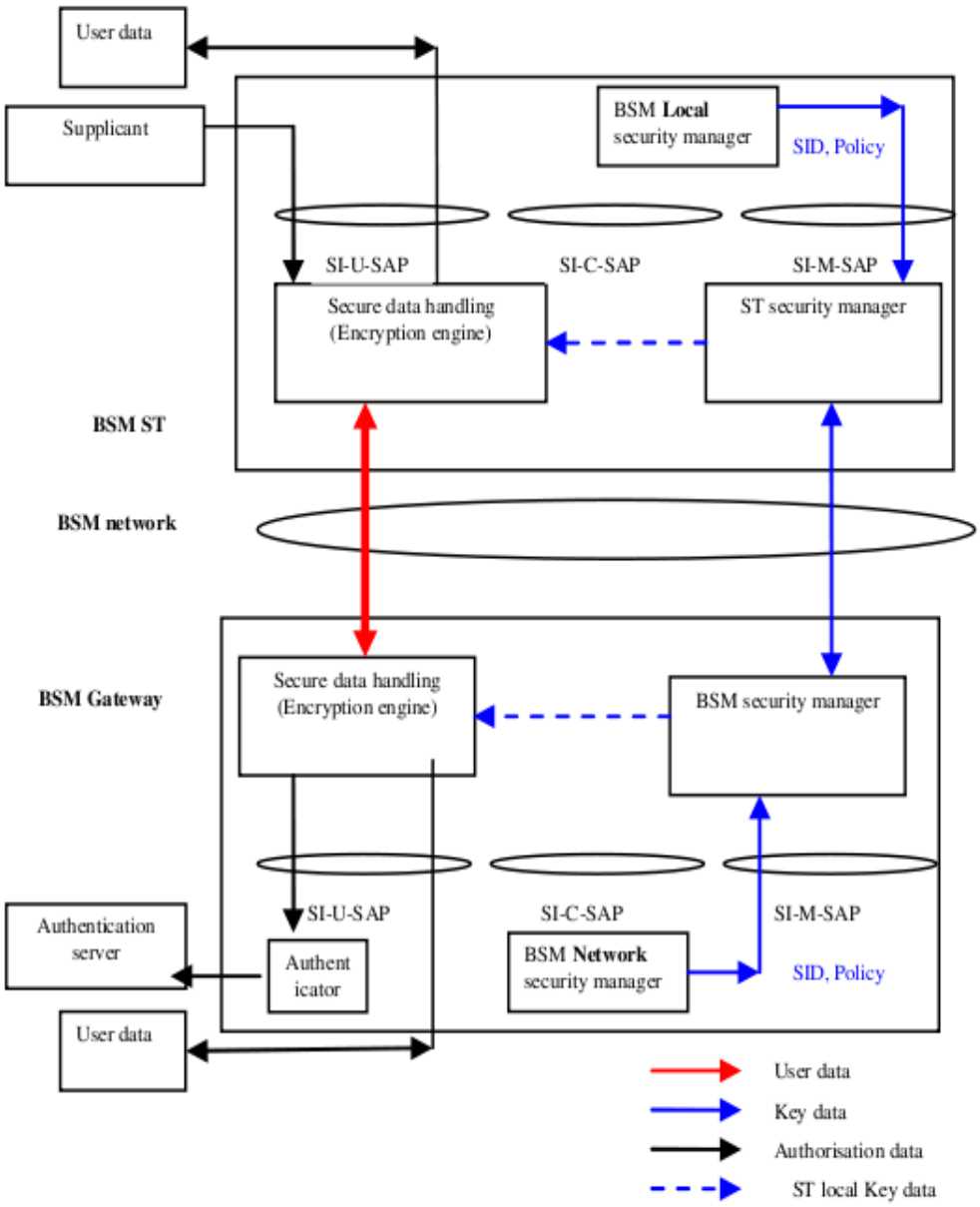
1.4.1.3. Περίπτωση 3: Ασφάλεια End-to-End

Η περίπτωση αυτή είναι εφαρμόσιμη στο IPsec, TLS/SSL και την ασφάλεια σε επίπεδο εφαρμογής (Σχήμα 15). Αυτό είναι χρήσιμο σε σενάρια end-to-end κι απομακρυσμένης πρόσβασης που περιγράφηκαν στις παραγράφους 1.2.4.1 και 1.2.4.4. Η περίπτωση αυτή είναι διαφανής στο δίκτυο BSM. Αν οι περιπτώσεις 1,2 ή 4 χρησιμοποιούνται ταυτόχρονα με την περίπτωση 3 τότε πρέπει να δοθεί ιδιαίτερη προσοχή στη μείωση της απόδοσης του δικτύου BSM εξαιτίας της διπλής διαδικασίας ασφάλειας.



Σχήμα 15: *Περίπτωση 3. Ασφάλεια End-to-End, διαφανής στο BSM.*

1.4.1.4. Περίπτωση 4: Ασφάλεια σε επίπεδο καθαρής σύνδεσης



Σχήμα 16: *Περίπτωση 4. Ασφάλεια σε επίπεδο σύνδεσης, διαφανής στο BSM.*

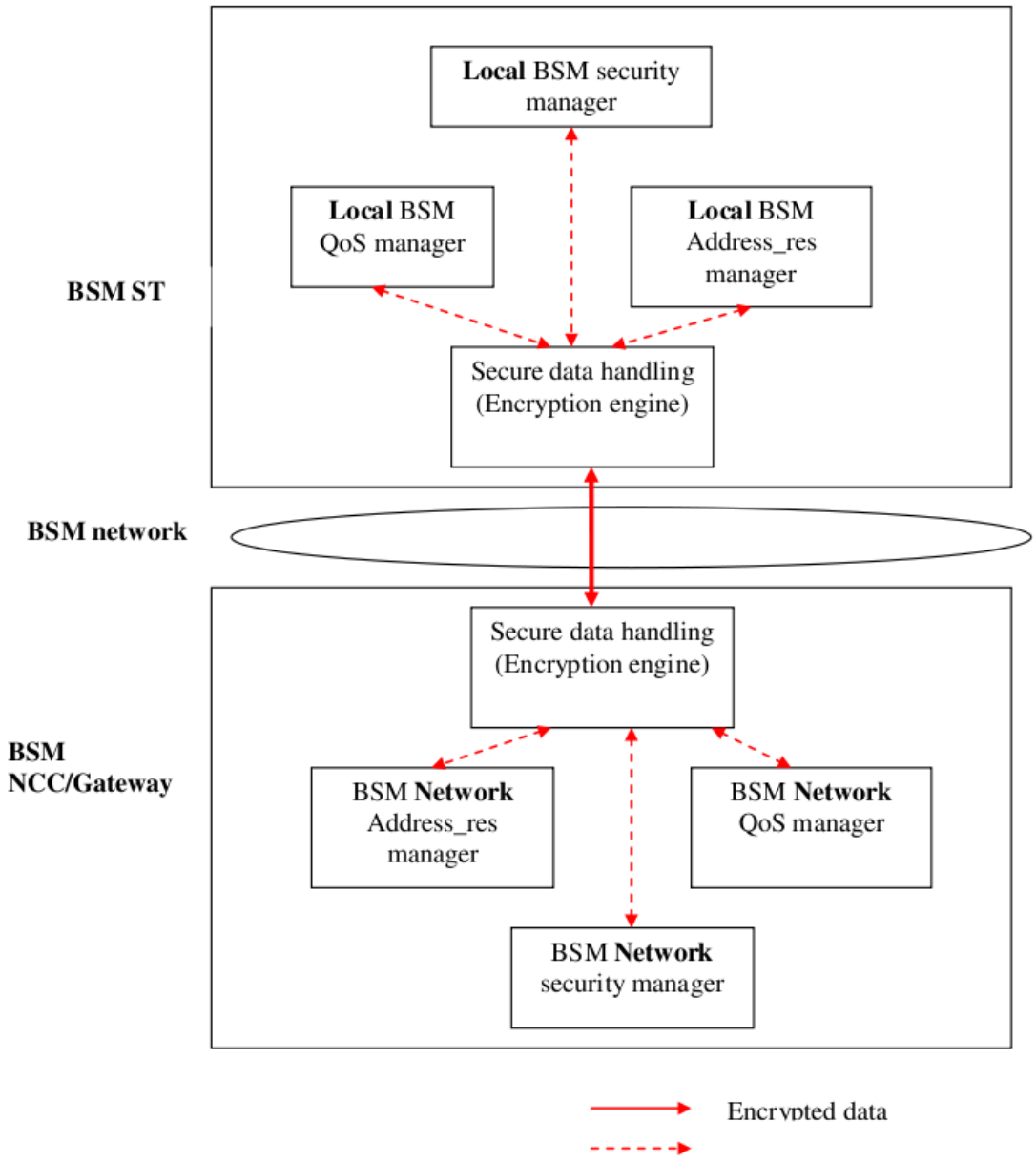
Η περίπτωση αυτή (Σχήμα 16) είναι εφαρμόσιμη στα συστήματα ασφαλείας ATM, DVB-RCS και ULE που εφαρμόζονται στο δίκτυο BSM μόνο σε επίπεδο δορυφορικής σύνδεσης. Αυτό είναι εφαρμόσιμο και στο σενάριο gateway-to-gateway που περιγράφηκε στην παράγραφο 1.2.4.2.

Η περίπτωση αυτή είναι διαφανής στο BSM, όμως οι διαχειριστές ασφαλείας του τοπικού δικτύου και το δικτύου BSM θα πρέπει να είναι σε θέση να επιβάλουν τους κανονισμούς πολιτικής ασφαλείας BSM σε αυτή την περίπτωση και για επικοινωνία πρέπει να χρησιμοποιούν τη διεπαφή SI-M-SAP. Ο σύνδεσμος ασφαλείας SID πρέπει να χρησιμοποιείται σε όλες τις ανταλλαγές μηνυμάτων διαχείρισης ασφάλειας.

1.4.2. Γενικευμένες αλληλεπιδράσεις μεταξύ της ασφάλειας κι άλλων οντοτήτων BSM

Η παράγραφος αυτή ασχολείται με την αλληλεπίδραση και τη διασυνεργασία με το QoS στα BSM, τη διαχείριση address resolution.

Όταν χρησιμοποιείται το QoS τότε τα μηνύματα key management πρέπει να χρησιμοποιούν μεγάλης προτεραιότητας κλάσεις QoS για να διασφαλιστούν γρήγορες κι ασφαλείς ανταλλαγές κλειδιών. Αυτό συνεπάγεται ανάθεση QIDs με υψηλή κλάση υπηρεσίας στις ανταλλαγές μηνυμάτων ασφαλείας. Αυτό έχει εφαρμογή στις περιπτώσεις ασφαλείας 1, 2 και 3.



Σχήμα 17: *Αλληλεπιδράσεις μεταξύ των οντοτήτων ασφάλειας, QoS και address resolution.*

Το σχήμα 17 περιγράφει τη χρήση της ασφάλειας BSM για την κρυπτογράφηση/ πιστοποίηση QoS και τις αιτήσεις/ ανταποκρίσεις address resolution μεταξύ των ST/ πυλών και NCC. Οι διεπαφές SI-SAP δε φαίνονται εδώ διότι το διάγραμμα επικεντρώνεται στις διασφάλιση της ανταλλαγής μηνυμάτων, πάνω στο δίκτυο BSM, μεταξύ των διαχειριστών δικτύου BSM (QoS και address resolution) και των τοπικών

διαχειριστών σε κάθε ST/ πύλη του BSM. Ο μηχανισμός κωδικοποίησης μπορεί να είναι πάνω ή κάτω από το SI-SAP.

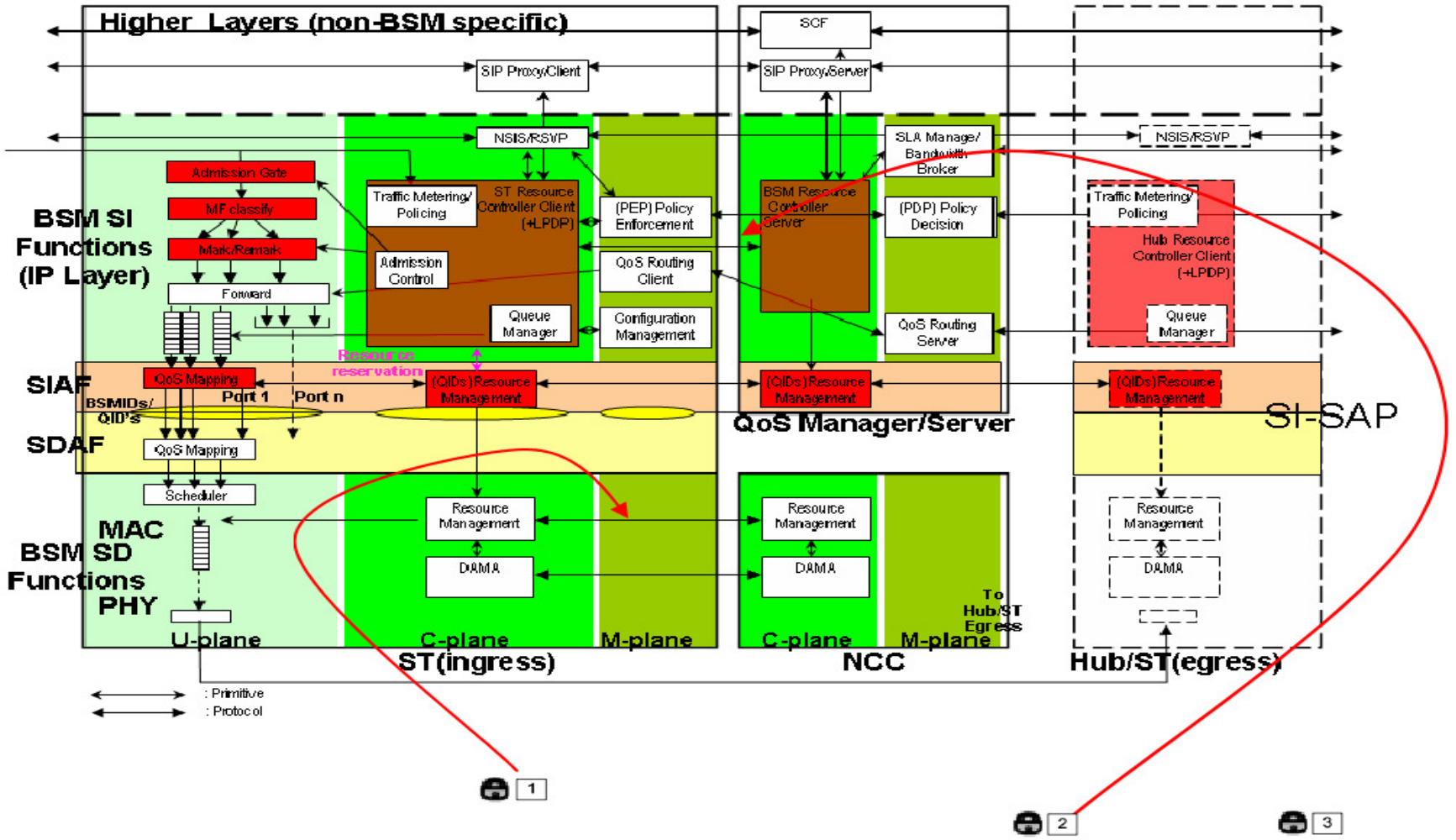
1.4.3. Αλληλεπιδράσεις μεταξύ των οντοτήτων ασφάλειας και QoS

1.4.3.1. Ασφάλεια του QoS signaling στα δίκτυα BSM

Στο έγγραφο της λειτουργικής αρχιτεκτονικής QoS (TS 102 462) [28] παρουσιάζονται περιπτώσεις QoS. Σε όλες αυτές τις περιπτώσεις υποθέτεται πως το σύστημα BSM παρέχει διαφορετικά επίπεδα του φορέα QoS μέσω συγκεκριμένου αριθμού QIDs, κάτι που καθορίζει τη φύση του QoS που προσφέρεται στο SI-SAP. Αυτό που διαφοροποιεί τις περιπτώσεις είναι ο τρόπος με τον οποίο τα QIDS προσεγγίζονται ή τροποποιούνται από το επίπεδο IP και πέρα. Σε όλες τις περιπτώσεις τα θέματα ασφαλείας είναι κοινά.

Τα σχέδια του χρήστη και της διαχείρισης δεν παρουσιάζονται σε αυτή την παράγραφο. Σε επίπεδο ελέγχου, οι επικοινωνίες μεταξύ της διαχείρισης πόρων στα ST/ GW και τα NCC πρέπει να διασφαλίζονται. Αυτά τα μηνύματα QoS μεταξύ των ST/ GW και τα NCC πρέπει να πιστοποιούνται κι εναλλακτικά να κρυπτογραφούνται (αυτό εξαρτάται από την πολιτική ασφαλείας του δικτύου BSM.

Στο σχήμα 18 (αντιγραμμένο από το έγγραφο για τη λειτουργική αρχιτεκτονική QoS (TS 102 462) [28]. Περίπτωση QoS 3), όταν η ασφάλεια εφαρμόζεται κάτω από το σημείο SI-SAP, τότε η σύνδεση με τον αριθμό 1 πρέπει να ασφαλίζεται χρησιμοποιώντας επίπεδο σύνδεση όπως είναι οι διαδικασίες ασφαλείας DVD-RCS. Αν η ασφάλεια εφαρμόζεται κάτω από το σημείο SI-SAP, τότε πρέπει να ασφαλίζεται η σύνδεση με αριθμό 2 χρησιμοποιώντας τις διαδικασίες ασφάλειας IPsec ή TLS. Τόσο η σύνδεση 1 όσο και η 2 θα πρέπει να ασφαλίζονται. Παρόλο που είναι πολύ πιθανό να ασφαλιστούν και οι δύο συνδέσεις, 1 και 2, ταυτόχρονα, θα πρέπει να δοθεί προσοχή η επίπτωση που θα έχει η διαδικασία ασφάλειας στην απόδοση του δικτύου BSM.



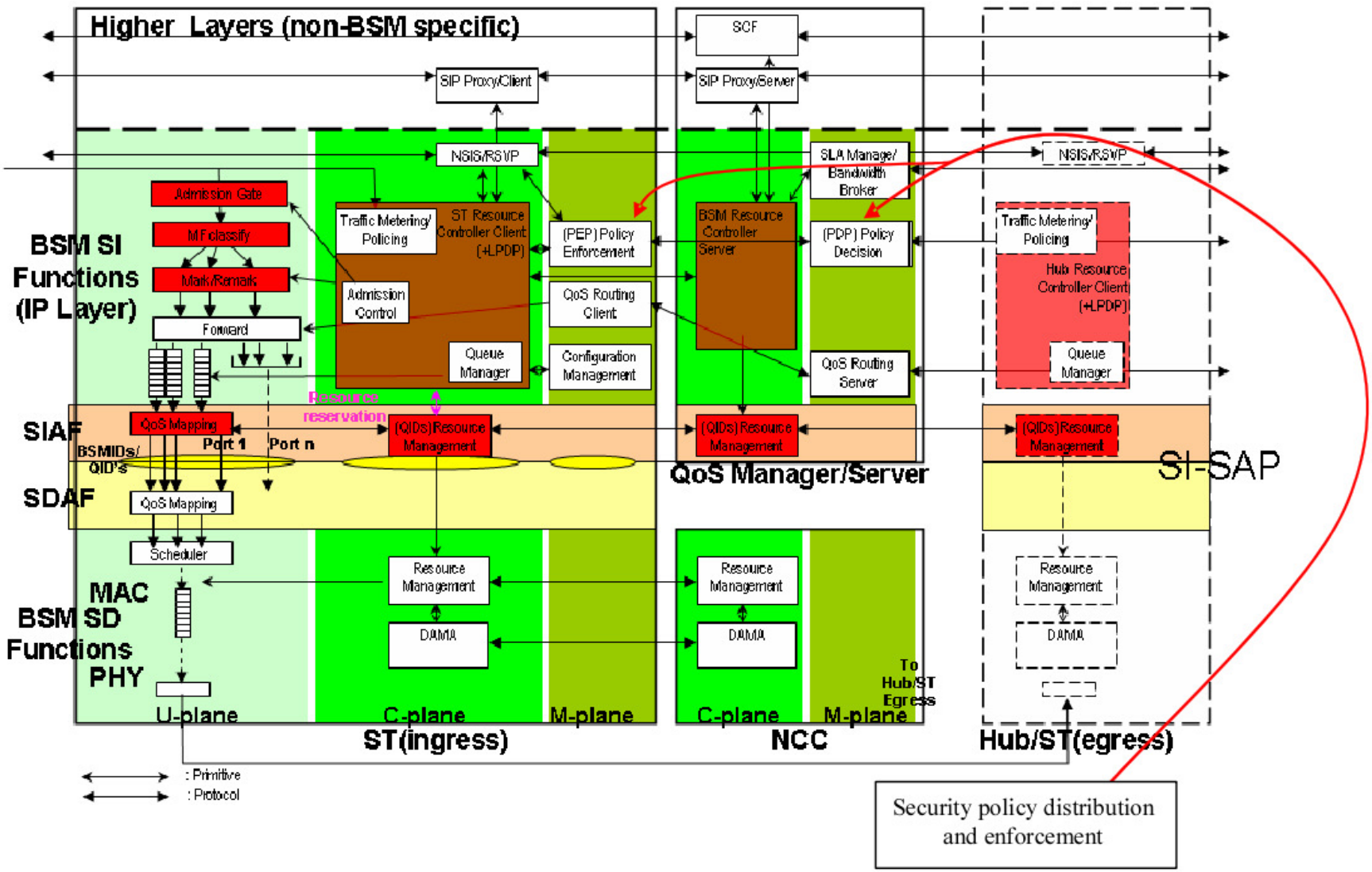
Σχήμα 18: *Διασφάλιση των μηνυμάτων διαχείρισης πόρων μεταξύ των NCC και ST/*

Στο σχήμα 18 φαίνεται επίσης η σύνδεση με αριθμό 3 μεταξύ των οντοτήτων NSIS/ SIP στο ST/ GW και των NCC. Τα θέματα ασφαλείας αυτών των οντοτήτων είναι έξω από το πεδίο δράσης των δικτύων BSM. Όμως αν χρησιμοποιείται SIP ή NSIS signaling στα BSM, τότε πρέπει να δοθεί προσοχή στις συστάσεις ασφαλείας του IETF και για τα δύο πρωτόκολλα (όπως είναι το RFC 4081 για τα NSIS και το RFC 3893 και RFC 3329 για την ασφάλεια SIP) [29] [30] [31].

1.4.3.2 Χρήση των πρωτοκόλλων COPS για την παροχή της πολιτικής ασφαλείας

Στα δίκτυα BSM. όπως περιγράφθηκε στην παράγραφο 1.3.4., μπορεί να χρησιμοποιηθεί το πρωτόκολλο Common Open Policy Service (COPS) για να μεταφέρει QoS ή πληροφορία ασφαλείας μεταξύ των οντοτήτων διαχείρισης του BSM και των δορυφορικών τερματικών (πύλες/ ST) (RFC 2748) [8]. Πρόσθετα, αν χρησιμοποιείται το COPS για την παροχή του QoS, τότε το πρωτόκολλο COPS Policy Provisioning (COPS-PR) πρέπει επίσης να χρησιμοποιείται για τη μεταβίβαση πολιτικής ασφαλείας (RFC 3084) [9].Το Σχήμα 19 (αντιγραμμένο από το έγγραφο για τη λειτουργική αρχιτεκτονική του QoS (TS 102 462) [28]. Περίπτωση QoS 3) δείχνει τις αλληλεπιδράσεις μεταξύ των οντοτήτων COPS στην μεταφορά QoS και πληροφορίες σχετικές με την ασφάλεια. Στο ST/ Πύλη, το Policy Enforcement Point (Policy-PEP) αλληλεπιδρά με τον τοπικό διαχειριστή ασφαλείας. Στο NCC το Policy Decision Point (Policy- PDP) αλληλεπιδρά με το διαχειριστή ασφαλείας του δικτύου BSM. Για λόγους απλότητας αυτές οι αλληλεπιδράσεις δε φαίνονται στο παρακάτω σχήμα.

Το σχέδιο διαχείρισης χρησιμοποιείται για να μεταφέρεις επικοινωνίες σχετικές με την πολιτική ασφαλείας. Τέτοιες επικοινωνίες δεν απαιτούν κάποια ειδική μεταχείριση QoS εκτός κι αν ορίζεται από το QoS ή τους κανονισμούς της πολιτικής ασφαλείας.



Σχήμα 19: *Διασφάλιση της διανομής ασφάλειας με τη χρήση COPS.*

1.4.3.3. Χρήση αξιόπιστων μηχανισμών μεταφοράς (QoS) για τη μεταφορά μηνυμάτων διαχείρισης κλειδιών

Στις περιπτώσεις ασφάλειας 1 και 3 τα μηνύματα διαχείρισης ασφάλειας μεταφέρονται σε επίπεδο χρήστη μέσω της διεπαφής SI-SAP. Ως εκ τούτου, οι ουρές για πληροφορία ασφάλειας διαχειρίζονται με τον ίδιο τρόπο που διαχειρίζεται κάθε άλλο δεδομένο χρήστη. Όμως στα μηνύματα διαχείρισης ασφάλειας θα πρέπει να δίνεται σχετικά υψηλή προτεραιότητα. Αυτή η κατανομή θα πρέπει να είναι στατική και να αποφασίζεται από της πολιτική ασφαλείας του δικτύου BSM ή μπορεί να είναι δυναμική εξαρτώμενη από τη φύση του QoS που προσφέρεται στο SI-SAP.

Η περίπτωση 2 είναι παρόμοια με τις 1 και 3, εκτός του ότι τα μηνύματα διαχείρισης κλειδιών ασφαλείας μεταφέρονται σε επίπεδο ελέγχου μέσω της διεπαφής SI-SAP. Για το λόγο αυτό, απαιτείται παρόμοια διαχείριση QoS σε αυτό το επίπεδο για τα μηνύματα ασφαλείας.

Στην περίπτωση 4, όλα τα μηνύματα διαχείρισης ασφαλείας βρίσκονται κάτω από το SI-SAP κι έτσι δεν υπάρχει ανάγκη διαχείρισης QoS πάνω από το SI-SAP για αυτά τα μηνύματα ασφάλειας.

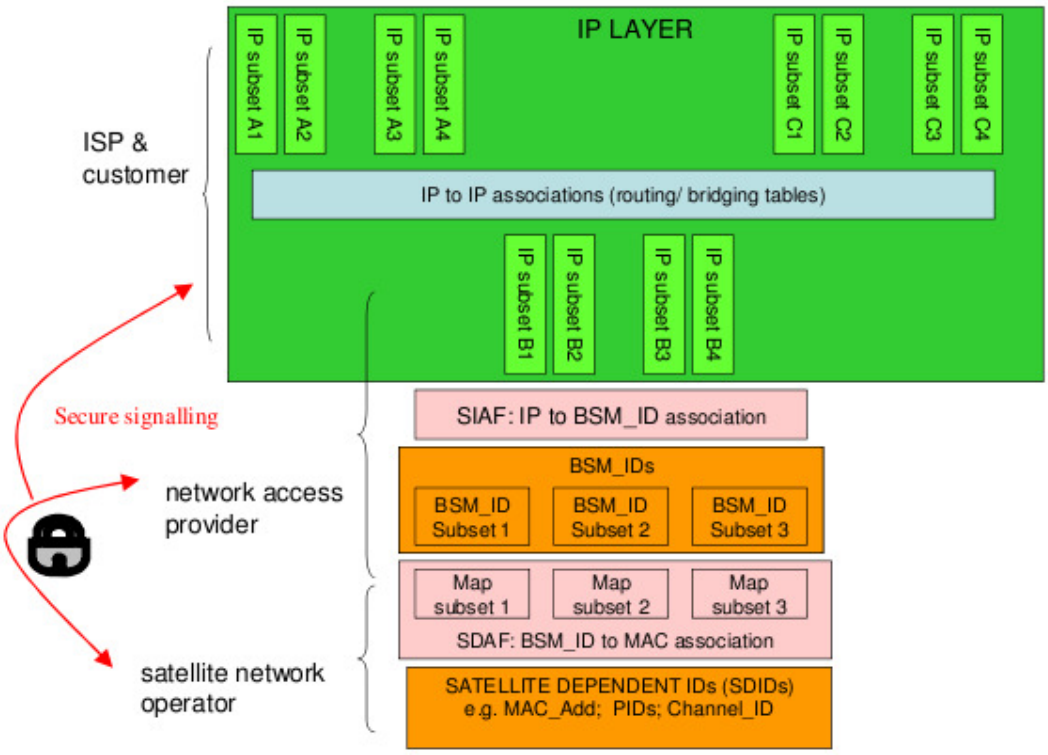
1.4.4. Αλληλεπιδράσεις μεταξύ των οντοτήτων ασφαλείας και του address resolution

1.4.4.1. Ασφάλεια του address resolution signaling στο δίκτυο BSM

Το πρωτόκολλο address resolution του BSM ορίζεται στο SI-SAP spec (TS 102 357) και το έγγραφο Address Management στο SI-SAP (TS 102 460) [3]. Τα βασικά θέματα είναι πως να σχεδιαστούν οι διευθύνσεις IP στα BSM-IDs κι έπειτα οι δορυφορικές διευθύνσεις MAC.

Ένα γενικευμένο μοντέλο παρουσιάζεται στο Σχήμα 20. Αναφορικά με την ασφάλεια, κάθε address resolution signaling γύρω από τη διεπαφή SI-SAP με ένα ST/ πύλη ή στο NCC δεν έχει καμία επίπτωση στην ασφάλεια.

Πάρα ταύτα, οι επικοινωνίες μεταξύ των οντοτήτων address resolution (στα ST/ GW και NCC) πρέπει να διασφαλιστούν μεταξύ των ISPs, των πελατών, των παροχών πρόσβαση στο δίκτυο και των χειριστών του δορυφορικού δικτύου (όπως φαίνεται στο Σχήμα 20). Αυτά τα μηνύματα address resolution μεταξύ των ST/ GW και NCC πρέπει να
πιστοποιούνται κι εναλλακτικά να κρυπτογραφούνται (αυτό εξαρτάται από την πολιτική ασφαλείας του δικτύου BSM).



Σχήμα 20: *Γενικευμένο μοντέλο διαχείρισης διευθύνσεων σε δίκτυο BSM.*

1.4.4.2. Χρήση του RADIUS με DHCP servers

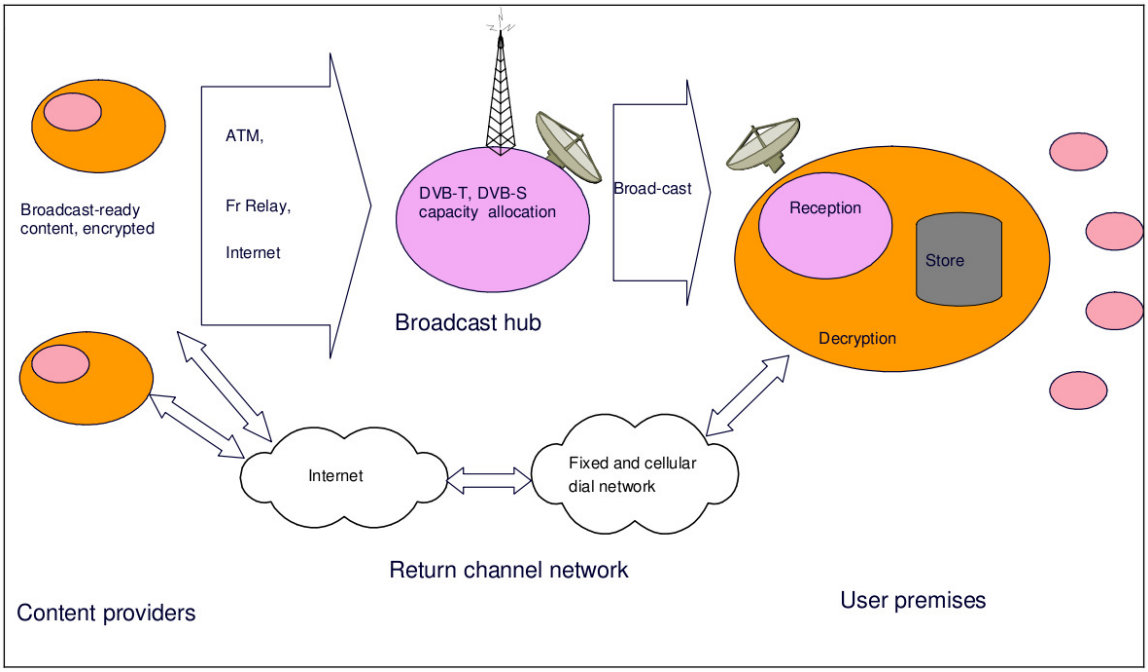
Όταν χρησιμοποιείται DHCP στο BSM τότε οι ιδιότητες του RADIUS ενεργοποιούν ένα στοιχείο του δικτύου για να μεταφερθούν οι ιδιότητες της ταυτοποίησης κι εξουσιοδότησης που λαμβάνονται κατά την πιστοποίηση RADIUS σε ένα DHCP server (RFC 4014) [32]. Όταν ο DHCP server λαμβάνει ένα μήνυμα από ένα εφεδρικό agent (Network Access Server, NAS) που περιέχει τις ιδιότητες του RADIUS εξάγει τα περιεχόμενα του sub option και χρησιμοποιεί τις πληροφορίες για την επιλογή των παραμέτρων ρύθμισης για τον πελάτη.

2. Ευρυζωνικά Δορυφορικά Πολυμεσικά IP Δίκτυα: Προδιαγραφές Ασφάλειας.

2.1. Εισαγωγή στην ασφάλεια BSM

Παρά το γεγονός πως το internet έχει αναπτυχθεί ως μία point-to-point υπηρεσία δικτύου, υπάρχουν κάποιοι περιορισμοί στην προσαρμογή σε μεγάλους όγκους, συντηρώντας τις προσδοκίες των χρηστών για απόδοση και κρατώντας χαμηλά το κόστος. Τα μέσα broadcast προσφέρουν τρόπους για την αντιμετώπιση αυτών των προβλημάτων καθώς επίσης και για την αύξηση της αφομοίωσης των υπηρεσιών multicast με τέτοιο τρόπο που δεν έχει αξιοποιηθεί ποτέ από το επίγειο internet.

Ο σχηματισμός ενός broadcast συστήματος φαίνεται στο Σχήμα 21, το οποίο είτε επίγειο είτε δορυφορικό, έχει το πλεονέκτημα της κάλυψης της υπηρεσίας σε αγροτικές κι απομακρυσμένες περιοχές και μια απλή τοπολογία με τον ελάχιστον αριθμό ενδιάμεσων κόμβων μεταγωγής μεταξύ του πυρήνα του δικτύου και του χρήστη. Ένα κανάλι επιστροφής απαιτείται γενικά, το οποίο παρέχεται μέσω dial-up ενσύρματης σύνδεσης ή ασύρματου δικτύου το οποίο υποστηρίζει ήδη πρόσβαση στο στενοζωνικό (narrowband) internet.



Σχήμα 21: *Ευρυζωνικό σύστημα broadcast*

Για το λόγο αυτό τα έσοδα των δορυφόρων τα επόμενα χρόνια είναι όλο και περισσότερο πιθανό ότι θα προέρχονται από εφαρμογές κι υπηρεσίες βασισμένες στο IP

είτε για να συμπληρώσουν τις επίγειες υπηρεσίες broadcast είτε για να παρέχουν υπηρεσίες προστιθέμενης αξίας σε κάποιες εξειδικευμένες αγορές. Η πρόκληση για την επόμενη γενιά δορυφορικών συστημάτων είναι συνεπώς να καθορίσουν μια κοινή βάση για την αποτελεσματική ολοκλήρωση των δορυφόρων με ασφαλή τηλεπικοινωνιακά δίκτυα γύρω από το IP. Η δορυφορική πρόσβαση, σε αντίθεση με τη μεταγωγή μεγάλων αποστάσεων, θεωρείται ως ιδιαίτερα βολικό στοιχείο της συνολικής τηλεπικοινωνιακής υποδομής, δεδομένου πως παρέχει οπουδήποτε ευρυζωνική πρόσβαση σε όλους αναπτύσσοντας ένα δορυφορικό τερματικό τόσο για τους οικιακούς χρήστες όσο και για τα SOHO/ εταιρικά δίκτυα.

Πρόσθετα, η ασφάλεια γίνεται ένα σημαντικό θέμα για την επιτυχία κάθε υπηρεσίας που προσφέρεται από τα δορυφορικά συστήματα. Όμως το δορυφορικό περιβάλλον έχει τις δικιές του προκλήσεις σχετικά με την ασφάλεια, όπως είναι:

- Οι υποκλοπές κι οι ενεργές εισβολές είναι πολύ πιο εύκολες σε σχέση με τα επίγεια ή κινητά δίκτυα εξαιτίας της ευρυζωνικής φύσης των δορυφόρων.
- Τα δορυφορικά κανάλια μπορεί να χρειάζονται εύρωστο συγχρονισμό ασφαλείας. Αυτό απαιτεί μια προσεκτική αξιολόγηση των κρυπτογραφικών συστημάτων για να αποτρέψουν την υποβάθμιση της Ποιότητας Υπηρεσιών (Quality of Service – QoS) κατά τη διαδικασία της ασφάλειας.

Για του λόγους αυτούς, το σύστημα ασφαλείας BSM πρέπει να είναι αποδοτικό και να έχει την ελάχιστη επίπτωση στην απόδοση του συστήματος BSM. Άλλος ένας λόγος για την παροχή ασφάλειας είναι πως η προστασία του περιεχομένου πρέπει να θεωρείται σημαντικό κομμάτι της αξίας των BSM και θα πρέπει εύκολα να γίνεται μέσα από το BSM.

Η παροχή της δομής ασφάλειας BSM δεν ισοδυναμεί με μια λύση πλήρους ασφάλειας. Αναμένεται πως κάποια συγκεκριμένα στοιχεία συμπεριλαμβανομένων των κρυπτογραφικών αλγορίθμων, κλειδιών και των διαδικασιών παραγωγή κλειδιών και κάποιων υλικών κομματιών, θα παραμείνουν εξωτερικά ή ιδιόκτητα. Οι τοπολογίες των BSM είναι ποικίλες κι υποστηρίζουν ένα ευρύ φάσμα εφαρμογών στις οποίες αντιστοιχεί ένα εξίσου ευρύ φάσμα απαιτήσεων ασφάλειας. Κάποια παραδείγματα υπηρεσιών που προσφέρονται από τα δίκτυα BSM είναι:

- Μια εφαρμογή τηλεδιάσκεψης (video conference) με ασφάλεια που εφαρμόζεται στην εφαρμογή του λογισμικού, τα emails προστατεύονται μέσω SMIME κι η σύνδεση στο internet για πληρωμή με πιστωτική κάρτα προστατεύεται από το Secure Socket Layer (SSL).
- Μια σύνδεση VPN αποκλειστικά για έναν εργοδότη εταιρικού δικτύου με τη χρήση του IPsec και γεννήτριας κλειδιού πράκτορα (Key generator agent) ειδικά ορισμένου για τον εργοδότη.
- Παράδοση ενός περιεχομένου βασισμένου στη συνδρομή, με τη μορφή αρχείου ή streaming, προστατευμένο από το CA.

Η δομή του κεφαλαίου αυτού είναι οργανωμένη με τέτοιο τρόπο έτσι ώστε να παρέχει μια εισαγωγή στα θέματα ασφαλείας της αρχιτεκτονικής BSM στο υποκεφάλαιο αυτό. Η παράγραφος 2.2. παρέχει μια σύντομη ανάλυση των απειλών ασφαλείας στα δίκτυα BSM και των μέτρων που απαιτούνται για την αντιμετώπιση τους. Στην παράγραφο 2.3. παρουσιάζονται οι λύσεις για την ασφάλεια σε διάφορα επίπεδα της στοίβας πρωτοκόλλου BSM, όπως είναι η ασφάλεια σε επίπεδο σύνδεσης (DVB-S, DVB-RCS και ATM), η ασφάλεια σε επίπεδο δικτύου (IPsec), σε επίπεδο μεταγωγής (όπως το SSL) κι η ασφάλεια σε επίπεδο εφαρμογής (όπως είναι το XML και το DRM). Η παράγραφος 2.4. παρουσιάζει τα θέματα της διαχείρισης ασφάλειας και της διαχείρισης του κλειδιού και τις πιθανές λύσεις στα δίκτυα BSM. Η παράγραφος 2.5. παρέχει τις προτεινόμενες από το ETSI προδιαγραφές για την ασφάλεια.

2.1.1. Σχέση μεταξύ των χαρακτηριστικών της δορυφορικής ζεύξης και της ασφάλειας

Υπάρχουν πτυχές των συνδέσεων BSM, οι οποίες διαφέρουν από τις ισοδύναμες επίγειες. Οι πάροχοι υπηρεσίας (Service Providers – SP) θα πρέπει να έχουν επίγνωση αυτών των πτυχών και να κάνουν βήματα τα οποία να διασφαλίζουν πως κάθε λύση ασφάλειας που επιλέγεται από τον χρήστη θα λειτουργεί σε οποιαδήποτε υπηρεσία BSM που προσφέρεται.

Καθυστέρηση (Delay)
Κάθε υπηρεσία BSM είναι σχεδιασμένη με μια τοπολογία με συγκεκριμένη καθυστέρηση κι απόκλιση καθυστέρησης. Δεν ορίζεται άνω όριο καθυστέρησης ή εύρος απόκλισης της καθυστέρησης στα BSM, κάτι που απασχολεί τους μεμονωμένους σχεδιαστές την υπηρεσίας και τους διαχειριστές.

Αναφορικά με την ασφάλεια, η καθυστέρηση της διαδικασίας κρυπτογράφησης θα πρέπει να είναι η ελάχιστη δυνατή.

Αριθμός των αναπηδήσεων (hops)
Δεν υπάρχει κανένας περιορισμός στον αριθμό των δορυφορικών hops σε μια συγκεκριμένη υπηρεσία BSM, ή ανώτατο όριο στη συνολική καθυστέρηση της σύνδεσης. Έγκειται στο ενδιαφέρον του παρόχου να ελαχιστοποιήσει τον αριθμό για να εξασφαλίσει την ελάχιστη καθυστέρηση, αλλά η ευελιξία των BSM σημαίνει πως σε κάποιες περιπτώσεις μερικά μόνο hops είναι η καλύτερη λύση. Έτσι ο πάροχος θα πρέπει να γνωρίζει των αριθμό των hops σε μια υπηρεσία για να εξασφαλίσει την κατάλληλη παροχή για να ελέγχει τη λειτουργία ασφαλείας. Η κρυπτογράφηση hop-by-hop ή οι πιστοποιήσεις δεν είναι επιθυμητές αν ο αριθμός των hops είναι μεγάλος.

Σφάλμα απόδοσης (Error Performance)
Οι συνδέσεις BSM γενικά θεωρούνται πως είναι Quasi-Error-Free κατά τη διάρκεια της διαθέσιμης σύνδεσης. Η χρήση της συνεχόμενης ή turbo Πρόσθιας Διόρθωσης Σφαλμάτων (Forward Error Correction - FEC) δείχνει πως υπάρχουν περίπου 8 δεκάδες ανά dB της απόκλισης BER ανά dB του λόγου C/N, εννοώντας πως η διάρκεια των περιόδων με σημαντικό ρυθμό λαθών είναι πολύ μικρή και μπορεί να αμεληθεί. Εξασθένηση μπορεί να υπάρχει λόγω της ατμόσφαιρας ή από άλλες αιτίες και μπορεί να προκαλέσει σημαντικές περιόδους διακοπής. Πάρα ταύτα, τα σφάλματα σύνδεσης στα BSM μπορεί να οδηγήσουν σε απώλεια συγχρονισμού της ασφάλειας, το οποίο μπορεί να έχει επίπτωση στην ρυθμόαποδοση (throughput) του δικτύου BSM.

Γεγονότα εξασθένισης
Τα BSM δεν έχουν συγκεκριμένες προδιαγραφές για την εξασθένιση της απόδοσης, κάτι που είναι αντικείμενο του ορισμού της μεμονωμένης υπηρεσίας. Κάποιες ζεύξεις είναι σχεδιασμένες να λειτουργούν κατά 99,99% ή και καλύτερα, ενώ άλλες μπορεί να είναι σχεδιασμένες να δουλεύουν με τρόπο εξασθένισης της συχνότητας, όπως για παράδειγμα να περιλαμβάνει πολύ μικρά σταθερά δορυφορικά πιάτα ή κινητά τερματικά. Το κατάλληλο επίπεδο ανοχής σε διακοπές πρέπει να είναι σχεδιασμένο κατά την εφαρμογή της υπηρεσίας και μέσα στο σύστημα ασφαλείας που το χρησιμοποιεί.

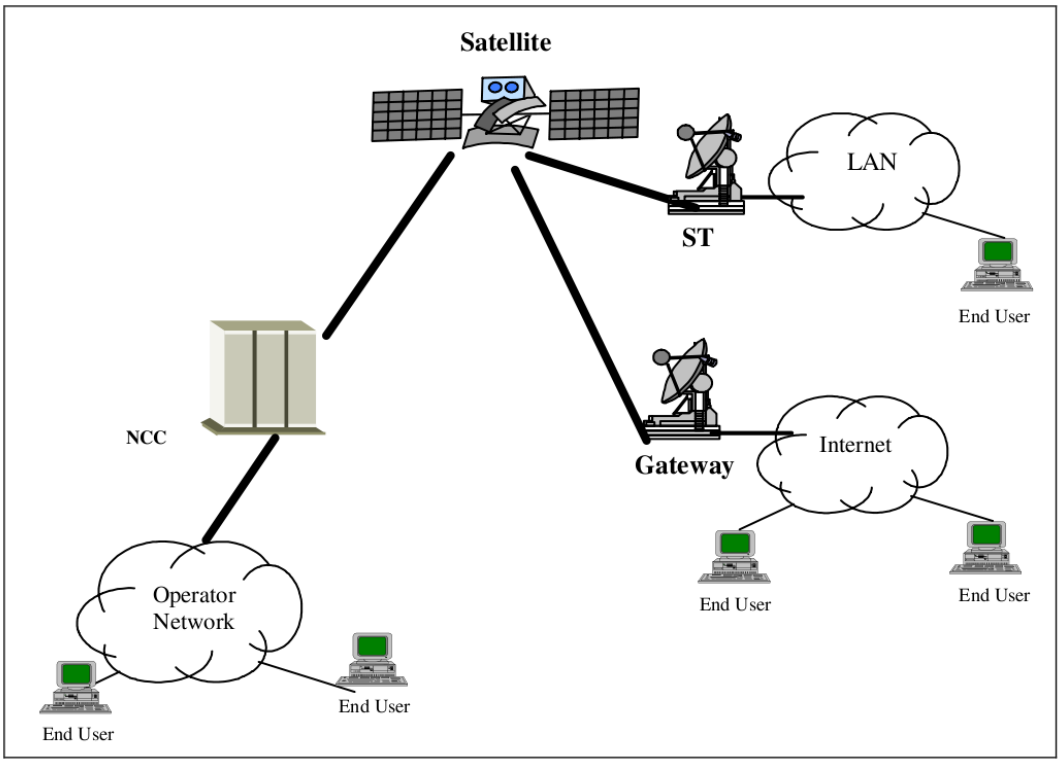
Τοπολογία Δικτύου κι Επιλογές συνδεσιμότητας
Υπάρχει μικρός αριθμός τοπολογιών κι έτσι η ασφάλεια Satellite Independent θα είναι άσχετη με το BSM. Όπου ο τύπος του συστήματος παίζει ρόλο στο ανεξάρτητο δορυφορικό κομμάτι τότε πρέπει να χρησιμοποιείται το SI-SAP.

Performance Enhancing Proxies (PEPs) κι οι λειτουργίες του δικτύου στα 4 άλλα επίπεδα
Οι PEPs χρησιμοποιούνται σε κάποια δορυφορικά συστήματα υψηλής ταχύτητας για να υπερπηδήσουν την επίδραση της καθυστέρησης στη σύνδεση σε μια λειτουργία TCP. Το BSM δεν ορίζει συγκεκριμένους PEPs ούτε βάζει περιορισμούς στη λειτουργία τους. Αφού συμμετέχουν στην παρεμβολή της λειτουργίας TCP στους τελικούς κι ενδιάμεσους κόμβους του δικτύου, είναι πιθανό να παρέμβουν στη λειτουργία κάποιων συστημάτων ασφαλείας. Για το λόγο αυτό ο πάροχος πρέπει να επιβεβαιώσει τη λειτουργία του συστήματος BSM σε σχέση με οποιαδήποτε χρήση των PEPs, και να επιβεβαιώσει επίσης τη λειτουργία της ασφάλειας.

Αναφορικά με την ασφάλεια, υπάρχουν προβλήματα στη χρήση των PEPs με Internet Security (IPsec) όπου το end-to-end IPsec μπορεί να αποτρέψει τη σωστή λειτουργία του δορυφορικού PEP.

2.1.2. Αρχιτεκτονική συστήματος BSM

Τα συστήματα BSM αποτελούνται από ένα διαστημικό τμήμα, από ένα ή περισσότερους δορυφόρους κι από ένα επίγειο τμήμα που αποτελείται από το Κέντρο Ελέγχου του Δικτύου (Network Control Centre - NCC), ή από πύλες και μεμονωμένα δορυφορικά τερματικά (Satellite Terminals – STs) (βλέπε Σχήμα 20). Ανάλογα με τον τύπο του payload στους δορυφόρους είναι πιθανές διάφορες αρχιτεκτονικές δικτύου.



Σχήμα 22: *Γενικευμένο σύστημα BSM*

Όπως ορίστηκε στο TR 101 984 [33], το BSM προσφέρει μια γενική υπηρεσία IP η οποία πρέπει να εξελίσσεται με τις αλλαγές του internet. Για την εργασία αυτή οι περιπτώσεις χρήσης περιλαμβάνουν αλλά δεν περιορίζονται στις παρακάτω:

- Point-to-point συνδεσιμότητα,
- πρόσβαση στο internet
- διανομή περιεχομένου και
- streaming πολυμέσων σε πραγματικό χρόνο

Αυτές οι περιπτώσεις χρήσης είναι κοινές σε όλα τα τρέχοντα projects του Special Task Force (STF), όπως επίσης έχουν αντιμετωπιστεί στα TRs σχετικά τόσο με την Αρχιτεκτονική [33] όσο και με το Internet Protocol [34]. Οι περιπτώσεις χρήσης

παρέχονται από τα BSMs χρησιμοποιώντας τρείς κύριες αρχιτεκτονικές δικτύου που υποστηρίζουν υπηρεσίες point-to-point, multicast και broadcast και είναι οι εξής:

- πρόσβαση στο δίκτυο
- διανομή περιεχομένου στην άκρη
- πυρήνας δικτύου

Ένα δίκτυο BSM μπορεί να υποστηρίζει και τα τρία σενάρια. Πάρα ταύτα, η παρούσα εργασία δίνει προτεραιότητα σε θέματα σχετικά με τα δύο πρώτα σενάρια, δηλαδή τα σενάρια για την πρόσβαση στο δίκτυο και για τη διανομή περιεχομένου στην άκρη. Κι αυτό διότι εδώ δεν αντιμετωπίζονται συγκεκριμένα οι υπηρεσίες multicast όπου το BSM μπορεί να παίξει σημαντικό ρόλο πυρήνα. Στις υπηρεσίες unicast οι ρυθμοί των δεδομένων που συνήθως σχετίζονται με δίκτυα πυρήνα είναι πιο χαμηλοί από εκείνους που προσφέρουν τα BSMs με τη σειρά των μεγεθών (terabits ανά δευτερόλεπτα σε οπτικά δίκτυα πυρήνα).

Τα δορυφορικά συστήματα BSM μπορούν να διαχωριστούν στους παρακάτω τύπους:

Μη αναγεννητικό (transparent) σύστημα
Ένα BSM με ένα μη-ανατροφοδοτούμενο payload (έναν επαναλήπτη) καλείται συχνά "bent-pipe σύστημα" ή "μη αναγεννητικό σύστημα" . Αυτό το σύστημα δεν τερματίζει κανένα επίπεδο της στοίβας πρωτοκόλλου του BSM σε ένα δορυφόρο. Ο δορυφόρος πολύ απλά επαναλαμβάνει τα σήματα από τις συνδέσεις του χρήστη στις συνδέσεις του τροφοδότη με μη αναγεννητικό τρόπο. Με αυτο το σύστημα (το οποίο χρησιμοποιεί global και spot beams) οι επικοινωνίες μεταξύ των δορυφορικών τερματικών (ST) και του internet γίνονται μέσω μια τερματικής πύλης συνδεδεμένης στο internet. Το κανάλι προώθησης χρησιμοποιεί τη δορυφορική εκπομπή, σε αντίθεση με το κανάλι επιστροφής που μπορεί να χρησιμοποιήσει αρκετές τεχνολογίες (για παράδειγμα δορυφόρο, τηλέφωνο ή δίκτυο DSL, κλπ). Το σύστημα αυτό κυρίως χρησιμοποιείται για πρόσβαση αφού απαιτεί διπλά hops δορυφόρου για επικοινωνίες ST σε ST. Σε αυτό το σύστημα όλες οι λειτουργίες δικτύου εκτελούνται από το NCC.

Αναφορικά με την ασφάλεια, η σύνδεση των μη αναγεννητικών δορυφόρων πρέπει να διασφαλίζεται είτε σε επίπεδο δορυφορικής σύνδεσης είτε σε κάποιο ανώτερο επίπεδο.

Αναγεννητικοί (regenerative) δορυφόροι (OBP)
Ένας αναγεννητικός δορυφόρος παρέχει γεφύρωση ή λειτουργικότητα δικτύου σε ένα δορυφόρο. Συνήθως, αυτή η πρόσθετη λειτουργικότητα είναι για να μεγιστοποιεί την αποδοτικότητα των multi-beams δορυφόρων και να βελτιώνει την κατανομή των πόρων του ραδιοφάσματος στην άνω ζεύξη. Γενικά, ο On-Board-Processor (OBP) χρησιμοποιεί ένα On-Board Switch (OBS) για να στείλει κυψέλες BSM από beam σε beam (ψηφιακή μεταγωγή). Ένας On-Board Controller (OBC) διαχειρίζεται τους πόρους της άνω και κάτω ζεύξης καθώς επίσης κάποια διαχείριση της επίδοσης onboard. Σε αυτό το σύστημα το Network Control Centre (NCC) χρησιμοποιείται για τον καθολικό

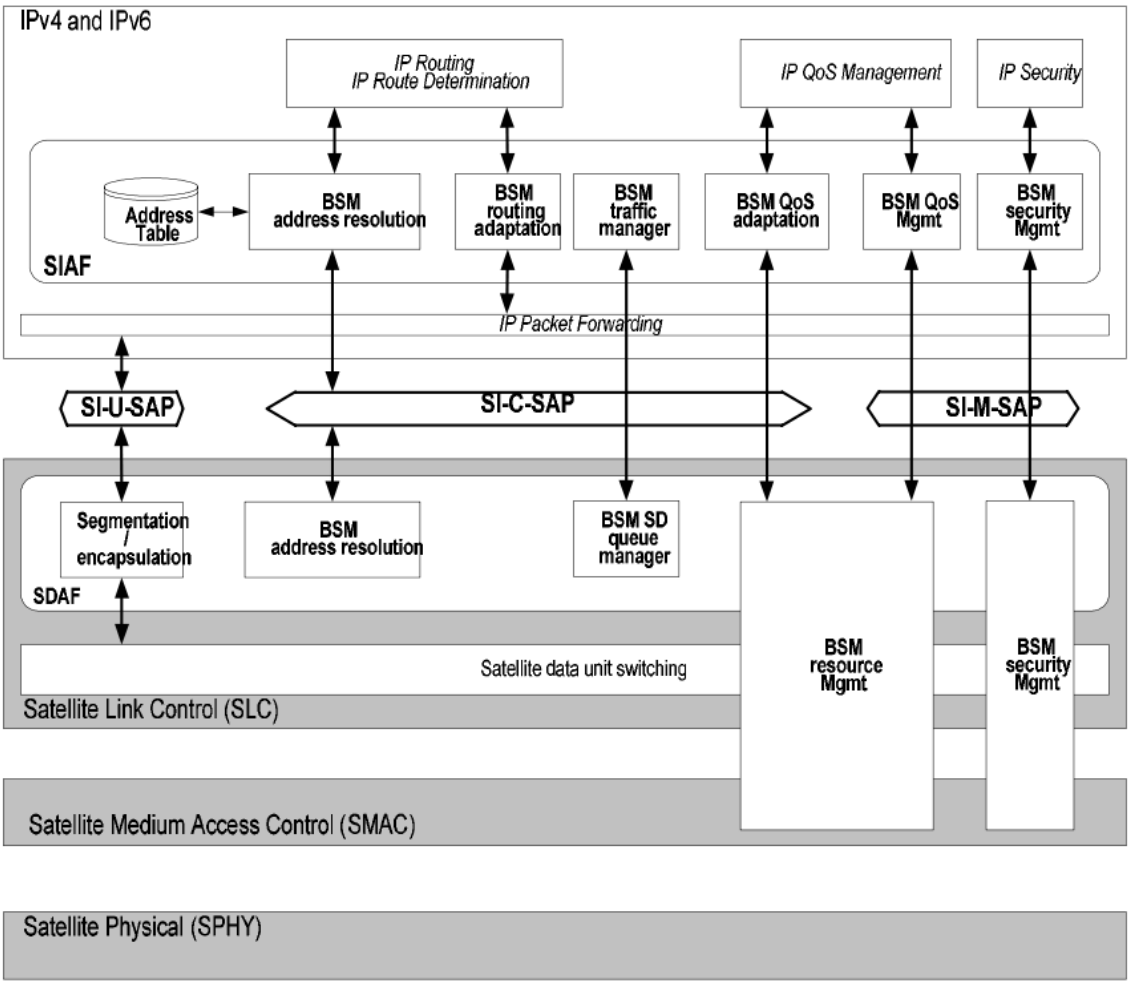
συντονισμό, τη διαχείριση πόρων σε μη πραγματικό χρόνο και τη διαχείριση δικτύου. Το σύστημα αυτό ενεργοποιεί επικοινωνίες single-hop ST-to-ST (peer to peer) και καθιστά εφικτή την πρόσβαση όπου χρειάζεται.

Αναφορικά με την ασφάλεια, οι απαιτήσεις των δορυφόρων OBP είναι παρόμοιες με εκείνες των μη αναγεννητικών κι επιπλέον υπάρχει η ανάγκη διασφάλισης των επικοινωνιών μεταξύ του NCC και του OBP.

Κάθε μία από τις παραπάνω περιπτώσεις χρήσης έχει κάποιες απαιτήσεις ασφαλείας που πρέπει να διευθετηθούν. Παραδείγματα αυτών των απαιτήσεων είναι η εμπιστευτικότητα κι η ακεραιότητα των δεδομένων από την πηγή στους τελικούς χρήστες, η πιστοποίηση της πηγής, η προστασία της διαχείρισης των υποδομών από μη εξουσιοδοτημένους ανθρώπους κι η προστασία έναντι της επίθεσης άρνησης παροχής υπηρεσιών. Πιο λεπτομερής ανάλυση παρουσιάζεται στην παράγραφο 2.2. Μια πολύ σημαντική απαίτηση είναι η διαφάνεια, όπου τα δίκτυα BSM πρέπει να υποστηρίζουν οποιαδήποτε υπηρεσία κρυπτογράφησης και να λειτουργούν με τέτοιο τρόπο που δε δημιουργεί συγκεκριμένες απαιτήσεις ή περιορισμούς στο δίκτυο. Κάθε τέτοια υπηρεσία πρέπει να είναι σε θέση να λειτουργεί στις συνθήκες μετάδοσης της κάθε τύπου υπηρεσίας BSM που έχει επιλεγεί και πρέπει να συμμορφώνεται με τις νομικές διατάξεις που ισχύουν.

2.2. Επιπεδοποίηση της ασφάλειας στη στοίβα πρωτοκόλλου BSM

Η στοίβα πρωτοκόλλου του BSM ορίζεται στο TR 102 292 [2] και φαίνεται στο Σχήμα 23.



Σχήμα 23: *Στοίβα πρωτοκόλλου BSM*

Η ασφάλεια μπορεί να παρέχεται σε κάθε επίπεδο της στοίβας πρωτοκόλλου BSM όπως είναι τα επίπεδα σύνδεσης, δικτύου, μεταφοράς κι εφαρμογής. Κατά την παρουσίαση αυτή για λόγους απλότητας αγνοούμε τα επίπεδα παρουσίασης και συνόδου του κλασικού μοντέλου OSI κι επικεντρωνόμαστε στο μοντέλο που παρέχεται από τα Internet Protocols. Γενικά, υπάρχει η ανάγκη να εδραιωθεί μια αξιόπιστη σχέση μεταξύ των χρηστών του συστήματος ασφάλειας end-to-end μέσω ενός συστήματος διαχείρισης της ασφάλειας. Οι λειτουργίες ασφάλειας μπορεί να είναι ορατές στους τελικούς χρήστες και τις εφαρμογές αν εφαρμόζονται σε επίπεδο εφαρμογής, διαφορετικά μπορεί να είναι διαφανείς αν εφαρμόζονται σε κατώτερα επίπεδα. Η παράγραφος αυτή ασχολείται με τα πλεονεκτήματα και τα μειονεκτήματα της καθεμιάς ασφάλειας.

2.2.1. Ασφάλεια σε επίπεδο σύνδεσης

Οι υπηρεσίες ασφαλείας μπορούν να παρέχονται σε επίπεδο σύνδεσης όπως είναι το επίπεδο Ασύγχρονου Τρόπου Μεταφοράς (Asychronous Transfer Mode – ATM) κελιών, το MPEG-TS για τα συστήματα DVB-S και DVB-RCS. Η ασφάλεια σε επίπεδο σύνδεσης έχει τα παρακάτω πλεονεκτήματα:

- Η ασφάλεια παρέχεται ανεξάρτητα από τα πρωτόκολλα ανωτέρων επιπέδων (IP, TCP, UDP, RTP ή αξιόπιστο multicast)
- Μπορεί να προστατεύσει τη δορυφορική ζεύξη έναντι της ανάλυσης της κίνησης και των παράνομων αλλαγών στις ρυθμίσεις του δορυφορικού δικτύου.
- Μπορεί να παρέχει προστασία σε όλες τις εφαρμογές πραγματικού χρόνου και μη πραγματικού χρόνου.

Τα μειονεκτήματα της ασφάλειας σε επίπεδο σύνδεσης είναι τα παρακάτω:

- Μόνο τα δορυφορικά τερματικά πιστοποιούνται
- Μόνο η κίνηση της δορυφορικής ζεύξης μπορεί να κρυπτογραφηθεί και να υπογραφεί ψηφιακά.

2.2.1.1. Ασφάλεια ATM

Το ATM Forum έχει ορίσει τέσσερις υπηρεσίες ασφαλείας στις προδιαγραφές ATM [34] όπως παρουσιάζονται παρακάτω:

- Ασφάλεια στο επίπεδο χρήστη: η ασφάλεια στο επίπεδο χρήστη ορίζει τους μηχανισμούς που επιτρέπουν την ασφαλή επικοινωνία μεταξύ των κόμβων ενός δικτύου ATM. Η ασφάλεια σε επίπεδο χρήστη όπως ορίστηκε από το ATM Forum έχει τις εξής υποκατηγορίες: έλεγχος πρόσβασης, πιστοποίηση, εμπιστευτικότητα δεδομένων κι ακεραιότητα δεδομένων.
- Ασφάλεια στο επίπεδο ελέγχου: το επίπεδο ελέγχου ορίζει το απαιτούμενο call control signaling για να εγκατασταθεί, να συντηρηθεί και τελειώσει μια εικονική σύνδεση (Virtual Connection – VC). Έτσι, η αρχική σηματοδότηση έχει οριστεί ως ο κύριος στόχος της ασφάλειας σε επίπεδο ελέγχου για κάθε σηματοδότηση endpoin to endpoint, switch to switch και endpoint to switch.
- Υπηρεσίες στήριξης: οι υπηρεσίες στήριξης καθορίζουν τις υποδομές πιστοποίησης, τους μηχανισμούς ανταλλαγής κλειδιών και τη βασική διαπραγμάτευση των απαιτήσεων και δυνατοτήτων ασφάλειας.
- Ασφάλεια στο επίπεδο διαχείρισης: το επίπεδο διαχείρισης είναι υπεύθυνο τόσο για τις λειτουργίες διαχείρισης ενός συστήματος ως σύνολο (plane management) όσο για τη λειτουργία του δικτύου και του συστήματος διαχείρισης των λειτουργιών όπως είναι η διαχείριση των πόρων (layer management).

Οι προδιαγραφές ασφαλείας του ATM Forum αναφέρουν πως το payload ενός ATM κελιού είναι κρυπτογραφημένο κι η επικεφαλίδα του κελιού είναι αμετάβλητη. Μια

μελέτη στα διαθέσιμα ολοκληρωμένα κυκλώματα (ICs) ATM δείχνει πως η αιχμή της τεχνολογίας Segmentation And Reassembly (SAR) controllers ενσωματώνει στη μονάδα τόσο το επίπεδο AAL όσο και το επίπεδο ATM. Έτσι για να διατηρηθεί η συμβατότητα μεταξύ του υπάρχοντος υλικού (hardware) ATM και του κρυπτογραφικού υλικού, η πρόσβαση στο κελί ATM μπορεί μόνο να γίνει από τη διεπαφή υλικού μεταξύ του SAR controller και της μονάδας Transmission Convergence (TC). Αυτή η διεπαφή έχει τυποποιηθεί από το ATM Forum ως Universal Test and Operations Physical Interface για το επίπεδο 2 ATM (UTOPIA). Διακόπτοντας τη διεπαφή UTOPIA η κρυπτογράφηση του payload του ATM κελιού με ένα πρότυπο, συμβατό κι ευέλικτο κλειδί είναι εφικτή σε υψηλές ταχύτητες μετάδοσης (για παράδειγμα 155 Mbps). Προσθετικά της πιθανής υψηλής ταχύτητας μετάδοσης, ένα άλλο πλεονέκτημα της διακοπής της ροής του κελιού στη UTOPIA είναι πως η λύση είναι ανεξάρτητη του υλικού αφού οι περισσότεροι κατασκευαστές υλικών ATM υποστηρίζουν τη UTOPIA. Διακόπτοντας τη τυποποιημένη UTOPIA αποσυνδέεται το υλικό κρυπτογράφησης από το φυσικό μέσο και ολοκληρώνει το στόχο να είναι εφαρμόσιμο σε όλα τα μέσα. Ακόμη κι αν αυτή η αρχιτεκτονική υλικού μοιάζει να είναι απλή, υπάρχουν δύο σημαντικές θεωρήσεις σχετικά με την απόδοση που πρέπει να γίνουν:

- ATM ρυθμαπόδοση (throughput): η κρυπτογραφική μονάδα πρέπει να διαχειριστεί το συνολικό αμφίδρομο εύρος ζώνης.
- Στατιστική πολυπλεξία: η κρυπτογράφηση για κάθε VC (εικονική σύνδεση) με μοναδικό κλειδί συνεδρίας για κάθε χρήστη πρέπει να υποστηρίζεται. Για να συμβεί αυτό θα πρέπει η κρυπτογραφική μονάδα να αλλάζει κλειδιά αρκετά γρήγορα (για παράδειγμα ένα ευέλικτο σύστημα κλειδιών). Η έρευνα για την ευελιξία των κλειδιών δείχνει πως μια κρυπτογραφική μονάδα για κάθε κατεύθυνση είναι αποτελεσματική εφόσον το key memory ενσωματώνεται στη κρυπτογραφική μονάδα χρησιμοποιώντας τεχνικές γρήγορης Content Addressable Memory (CAM).

Οι προδιαγραφές του ATM Forum ασχολούνται με τα θέματα ασφαλείας που αφορούν επίγεια δίκτυα μόνο. Αρκετά λίγη εργασία έχει γίνει σχετικά με την ασφάλεια των δορυφόρων ATM. Υπάρχουν αρκετές τεχνικές προκλήσεις που πρέπει να αξιολογηθούν προσεκτικά για τη ασφάλιση των δορυφόρων ATM, όπως είναι ο συγχρονισμός της κρυπτογράφησης σε περιβάλλοντα με υψηλότερους ρυθμούς λαθών (BER), τα οποία λάθη οφείλονται στην εκρηκτική φύση. Για το λόγο αυτό, είναι σημαντικό να εξεταστεί η επίδραση των λαθών αυτών στην απόδοση της κρυπτογράφησης του payload του ATM κελιού. Άλλο ένα ζήτημα είναι ο ρυθμός μετάδοσης κι η αναβάθμιση του κρυπτογραφικού κλειδιού όταν το ATM έχει σχεδιαστεί για υψηλούς ρυθμούς δεδομένων. Έτσι υπάρχει η ανάγκη να αλλάζει το κρυπτογραφικό κλειδί συχνά αλλά αυτή η πρόκληση δεν είναι συγκεκριμένη στους δορυφόρους και περιλαμβάνει επίσης επίγεια δίκτυα ATM.

2.2.1.2. Υπό όρους πρόσβαση στο DVB-S

Η πρόσβαση υπό συνθήκη (Conditional Access-CA) είναι μια υπηρεσία που επιτρέπει στους broadcasters να περιορίσουν συγκεκριμένα προγραμματιστικά προϊόντα σε συγκεκριμένους θεατές. Το CA το πετυχαίνει αυτό κρυπτογραφώντας τα προγράμματα των broadcasters. Συνεπώς, τα προγράμματα αυτά θα πρέπει να αποκρυπτογραφούνται στο τελικό στάδιο της λήψης πριν αποκωδικοποιηθεί για θέαση. Το CA προσφέρει δυνατότητες όπως την Pay-Per-View (PPV), διαδραστικές λειτουργίες όπως είναι το Video-on-Demand (VoD) και παιχνίδια, την ικανότητα να περιορίσει την πρόσβαση σε συγκεκριμένο υλικό (ταινίες για ενήλικες για παράδειγμα) και την ικανότητα των άμεσων μηνυμάτων σε set-top boxes (πιθανώς βασισμένα στη γεωγραφική περιοχή).

Το σύστημα Conditional Access χρησιμοποιείται στο σύστημα DVB [35], [36] περιλαμβάνει τις εξής τρείς κύριες λειτουργίες:
Κρυπτογράφηση/αποκρυπτογράφηση (scrambling/ descrambling), έλεγχος των δικαιωμάτων και διαχείριση των δικαιωμάτων.

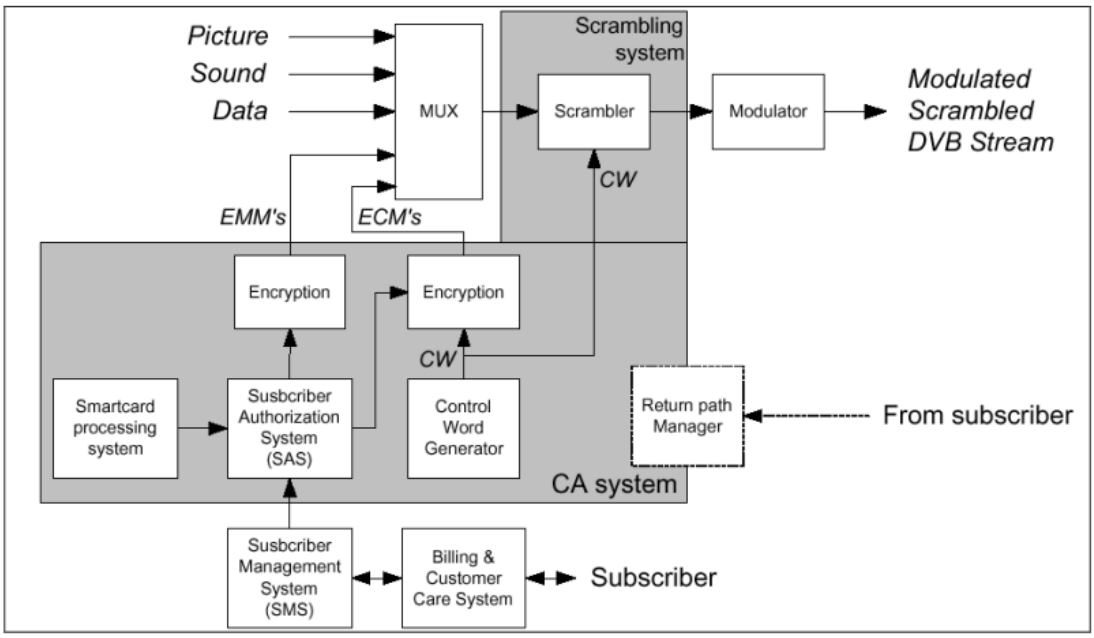
Η λειτουργία την κρυπτογράφησης/αποκρυπτογράφησης (scrambling/ descrambling) στοχεύει στο να κάνει την υπηρεσία δυσνόητη σε μη εξουσιοδοτημένους χρήστες. Η αποκρυπτογράφηση (descrambling) μπορεί να επιτευχθεί από κάθε δέκτη ο οποίος έχει τον κατάλληλο descrambler και ένα μυστικό Control Word (CW). Η κρυπτογράφηση (scrambling) μπορεί να εφαρμοστεί σε κομμάτια της υπηρεσίας είτε χρησιμοποιώντας ένα κοινό Control Word (CW) είτε ξεχωριστά Control Word για κάθε κομμάτι.

Η λειτουργία του ελέγχου των δικαιωμάτων αποτελείται από την εκπομπή των συνθηκών που απαιτούνται για την πρόσβαση σε μια υπηρεσία, μαζί με τους κρυπτογραφικούς μυστικούς κωδικούς για την ενεργοποίηση της αποκρυπτογράφησης (descrambling) σε εξουσιοδοτημένους δέκτες. Αυτοί οι κώδικες στέλνονται μέσα σε ειδικά μηνύματα που λέγονται Entitlement Checking Messages (ECMs) κι αυτά μεταφέρονται ως σύνολο.

Η λειτουργία της διαχείρισης των δικαιωμάτων αποτελείται από τη διανομή των δικαιωμάτων στους δέκτες. Αυτά είναι μερικά είδη δικαιωμάτων που αντιστοιχούν σε διαφορετικές μορφές εγγραφής σε μια υπηρεσία: εγγραφή ανά θέμα, επίπεδο ή τάξη, προκρατημένα pay-per programme ή αυθόρμητα pay-per programme, ανά υπηρεσία ή ανά διάρκεια. Η πληροφορία αυτή στέλνεται μέσα από ειδικά μηνύματα που λέγονται Entitlement Management Messages (EMMs) και μπορεί να μεταφέρονται ως σύνολο όπως οι υπηρεσίες κρυπτογράφησης ή με κάποια άλλα μέσα. Οι λειτουργίες ελέγχου και διαχείρισης απαιτούν τη χρήση μυστικών κλειδιών και κρυπτογραφικών αλγορίθμων.

Για να κατανοήσουμε πως χρησιμοποιείται το CA, αρχικά πρέπει να δούμε τα δεδομένα που κρυπτογραφεί. Κάθε ξεχωριστό πρόγραμμα που παρέχει ένας broadcaster αποτελείται από πολλά στοιχεία, όπως είναι το video, ο ήχος και το κείμενο. Στην

ψηφιακή τηλεόραση, αυτά τα στοιχεία μετατρέπονται σε ψηφιακή μορφή χρησιμοποιώντας τον κωδικοποιητή MPEG-2. Τα δεδομένα MPEG-2 που σχετίζονται με κάθε πρόγραμμα χωρίζονται σε πολλά πακέτα και το συνολικό άθροισμα αυτών των πακέτων για κάθε πρόγραμμα ονομάζεται Program Elementary Stream (PES). Το PES για κάθε πρόγραμμα πολυπλέκεται μαζί με άλλα PES άλλων προγραμμάτων. Αυτή η ροή των πολυπλεγμένων προγραμμάτων σπάει σε πακέτα των 188 byte για μετάδοση και στο σημείο αυτό ονομάζεται Digital Video Broadcast (DVB) MPEG-2 Transport Stream (TS). Η υπηρεσία CA μπορεί να κρυπτογραφήσει τα δεδομένα των προγραμμάτων είτε στο επίπεδο PES είτε στο επίπεδο TS, με τη τελευταία να είναι η προτιμώμενη επιλογή.



Σχήμα 24: *Αρχιτεκτονική του Conditional Access συστήματος*

Μια γενική αρχιτεκτονική τέτοιου συστήματος φαίνεται στο Σχήμα 22. Τα κύρια στοιχεία του συστήματος είναι: ένας πολυπλέκτης (MUX) που συνδυάζει το video stream, το audio stream και τα EMMs και ECMs σε ένα μόνο DVB stream. Αυτός ο πολυπλέκτης είναι μια ειδική off-the-shelf συσκευή. Άλλο ένα στοιχείο είναι ο ρυθμιστής (modulator) που παίρνει το σήμα που προκύπτει και το ρυθμίζει για τη μετάδοση του στο δορυφόρο. Το τρίτο στοιχείο είναι ένα conditional access σύστημα που αποτελείται από συγκεκριμένες ενότητες:

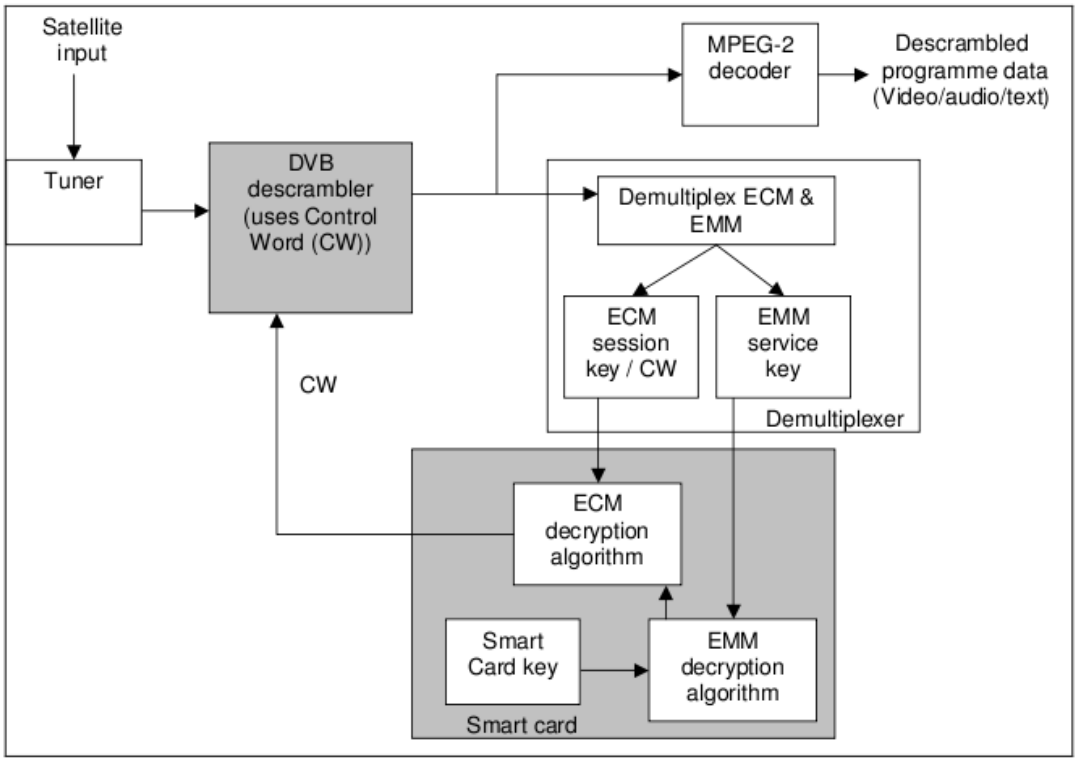
- Το scrambler: Κρυπτογραφεί το payload των πακέτων που αποτελούν τη ροή μεταφοράς, χρησιμοποιώντας ένα Common Word που παράγεται από τη γεννήτρια Control Word. Το scrambler συνήθως κρυπτογραφεί τα πακέτα που περιέχουν τις πληροφορίες εικόνας και ήχου και κάποιες φορές μερικά πακέτα που περιέχουν δεδομένα. Τα πακέτα που περιέχουν EMMs και ECMs δεν κρυπτογραφούνται. Η προτιμώμενη εφαρμογή του scrambler είναι στη συσκευή πολυπλέκτη. Επίσης υπάρχουν και stand-alone scramblers.

- Το σύστημα Subscriber Authorization System (SAS): Επεξεργάζεται τις διαφορετικές εξουσιοδοτήσεις προβολής που δίνονται στους συνδρομητές και τις χρησιμοποιεί για να παράγει επαρκή EMMs και ECMs.
- Τη γεννήτρια Control Word η οποία δημιουργεί τα control words: Δύο μηχανές κρυπτογράφησης (συνήθως εφαρμοσμένες από το ίδιο πρόγραμμα) χρησιμοποιούνται για την κρυπτογράφηση του περιεχομένου των EMMs και των Control Words που αποθηκεύονται στα ECMs.
- Το σύστημα επεξεργασίας των smart cards: Περιέχει πληροφορίες σχετικά με τις απόρρητες πληροφορίες που αποθηκεύονται στις smart cards του καταναλωτή ή set-top boxes του. Αυτή η ενότητα αρκετά συχνά ενσωματώνεται στο SAS.

Το conditional access σύστημα χρειάζεται πληροφορίες από άλλες ενότητες του συστήματος, όπως είναι οι παρακάτω:

- Το Subscriber Management System (SMS) έχει όλα τα δεδομένα σχετικά με τους συνδρομητές, τις τρέχουσες συνδρομές και πληρωμές. Αυτό το σύστημα αλληλεπιδρά με το σύστημα τιμολόγησης και προσοχής του χρήστη για να υπολογίσει τα έξοδα. Το SMS ορίζει για ποια προγράμματα έχουν εξουσιοδότηση να δουν οι συνδρομητές.
- Ο return path manager (αν υπάρχει το return path): η ενότητα αυτή μπορεί να χρησιμοποιηθεί από το conditional access σύστημα για την εκτέλεση λειτουργιών πιστοποίησης και για να πάρει feedback για την κατάσταση και την συμπεριφορά των set-top boxes.

Στο τελικό σημείο λήψης, είναι η δουλειά του Set-Top Box (STB) να αποκρυπτογραφήσει την κρυπτογράφηση CA και να αποκωδικοποιήσει τα δεδομένα MPEG-2 για προβολή. Το Σχήμα 25 είναι ένα μπλοκ διάγραμμα ενός τυπικού STB. Οι κύριες περιοχές του STB που συμμετέχουν στο conditional access παρουσιάζονται με γκρι χρώμα. Το μπλοκ με την ετικέτα CA μπορεί να είναι ειδικό, ενσωματωμένο στην ενότητα CA ή μπορεί να είναι ένα από τα πρότυπα descramblers.



Σχήμα 25: *Conditional access σε ένα τυπικό set-top box*

Το κομμάτι του δέκτη του STB δέχεται το εισερχόμενο σήμα, το αποδιαμορφώνει και το στέλνει στη γεννήτρια ροής μεταφοράς. Αυτό το μέρος του STB ανασυνθέτει τη ροή μεταφοράς, η οποία περιέχει πολλά πακέτα πληροφορίας. Κάθε πακέτο συσχετίζεται με το δικό του (στην επικεφαλίδα του) Program Identifier (PID). Όλα τα πακέτα με τιμή του PID hex 1 δεν έχουν κρυπτογραφηθεί και χρησιμοποιούνται από τον επεξεργαστή αποπολυπλέκτη (demux processor) για την κατασκευή του Conditional Access Table (CAT). Αυτός ο πίνακας αναγνωρίζει όλες τις τιμές PID των πακέτων μεταφοράς που περιέχουν EMMs. Ο demux processor κατασκευάζει επίσης το Program Map Table (PMT) από μη κρυπτογραφημένα πακέτα και δίνει τις τιμές PID για όλες τις ροές μεταφοράς που σχετίζονται με το συγκεκριμένο πρόγραμμα. Τα ιδιωτικά δεδομένα που αφορούν το πρόγραμμα μπορούν επίσης να περιλαμβάνονται σε αυτό τον πίνακα. Για παράδειγμα, η τιμή PID ενός πακέτου που περιέχει το Entitlement Control Message (ECM). Τα δεδομένα που περιέχονται σε αυτά τα δύο μηνύματα (τα EMM και ECM) είναι ζωτικά για την αποκρυπτογράφηση του κρυπτογραφημένου υλικού του προγράμματος.

Πάρα ταύτα, πρέπει να σημειωθεί πως τα πρότυπα δεν ορίζουν λεπτομερώς τις ηλεκτρονικές smart-cards ούτε τους αλγορίθμους. Έτσι, το σύστημα που περιγράφηκε εδώ είναι ένα τυπικό παράδειγμα, Τα απαιτούμενα EMM από τον demur processor σχετίζονται με την εξουσιοδότηση των υπηρεσιών. Επιτρέπει σε ένα set-top box ή μια συγκεκριμένη γεωγραφική περιοχή την πρόσβαση στις υπηρεσίες και περιλαμβάνει το κρυπτογραφικό κλειδί της υπηρεσίας. Τυπικά, το κλειδί αυτό πρέπει να αλλάζει κάθε λίγους μήνες για να αποθαρρύνονται με αυτό τον τρόπο οι hackers.

Το κρυπτογραφημένο κλειδί πολλαπλής συνεδρίας, μεταφέρεται από το ECM και σχετίζεται με συγκεκριμένο υλικό του προγράμματος. Αυτό το κλειδί, μόλις αποκρυπτογραφηθεί, γίνεται στην πραγματικότητα το control word για το DVB descrambler, επιτρέποντας τη ροή μεταφοράς να αποκρυπτογραφηθεί έτσι ώστε ο θεατής να μπορεί να δει ένα συγκεκριμένο πρόγραμμα ή να δει το υλικό του προγράμματος για μια συγκεκριμένη συνεδρία. Όπως δείχνει το Σχήμα 5, το κλειδί της υπηρεσίας (EMM) στέλνεται σε μια smart card, οπού αποκρυπτογραφείται με τη βοήθεια του κλειδιού του χρήστη που βρίσκεται μέσα στην κάρτα. Η αποκρυπτογράφηση παραχωρεί το Control Word (CW) που είναι το κλειδί για DVB descrambler της ροής μεταφοράς.

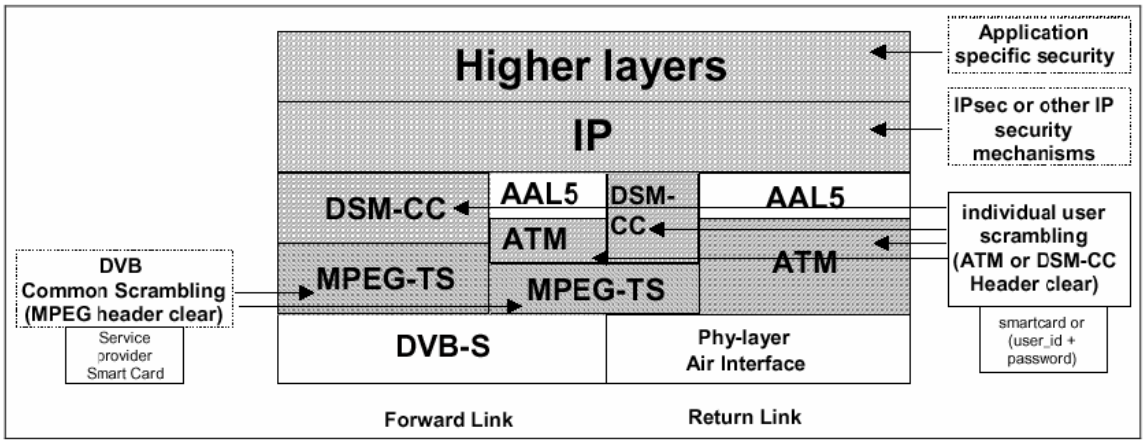
Η κύρια αδυναμία του DVB-S CA είναι οι μονόδρομος (broadcast) μεταδόσεις. Έτσι είναι πολύ δύσκολο να σταματήσει η απάτη κι η κλωνοποίηση των TV smart cards χωρίς το αποτελεσματικό κανάλι επιστροφής και έναν αποτελεσματικό τρόπο αναβάθμισης των κλειδιών των smart cards.

2.2.1.3. Ασφάλεια DVB-RCS

Όπως ορίστηκε στο EN 301 790 [37], η ασφάλεια που προορίζεται για την προστασία της ταυτότητας του χρήστη συμπεριλαμβάνοντας την ακριβή τοποθεσία, την κίνηση σηματοδότησης από και προς τον χρήστη, την κίνηση των δεδομένων από και προς τον χρήστη και τον χειριστή έναντι οποιασδήποτε χρήσης του δικτύου χωρίς την κατάλληλη εξουσία και συνδρομή. Τρία επίπεδα ασφάλειας μπορούν να εφαρμοστούν στα διαφορετικά στρώματα:

- Κοινή κρυπτογράφηση DVB στη ζεύξη προώθησης (μπορεί να απαιτείται από τον πάροχο της υπηρεσίας)
- Κρυπτογράφηση του δορυφορικού διαδραστικού δικτύου του μεμονωμένου χρήστη στη ζεύξη προώθησης κι επιστροφής.
- Μηχανισμοί ασφάλειας στο επίπεδο IP ή και σε κάποιο υψηλότερο (μπορεί να χρησιμοποιηθεί από τον πάροχο της υπηρεσίας, τον πάροχο του περιεχομένου).

Παρόλο που ο χρήστης/ πάροχος της υπηρεσίας μπορεί να χρησιμοποιήσει τα δικά του συστήματα ασφαλείας πάνω από το επίπεδο σύνδεσης δεδομένων, είναι επιθυμητή η παροχή ενός συστήματος ασφάλειας στο επίπεδο σύνδεσης των δεδομένων έτσι ώστε το σύστημα να ασφαλίζει εγγενώς τη δορυφορική συνεδρία χωρίς τη βοήθεια προσθετικών μέτρων. Επίσης, αφού η δορυφορική ζεύξη προώθησης του δικτύου βασίζεται στα πρότυπα DVB/ MPEG-TS , ο μηχανισμός της κοινής κρυπτογράφησης DVB μπορεί να εφαρμοστεί, χωρίς όμως να είναι απαραίτητος (θα προσθέσει απλά μια επιπλέον προστασία στη συνολική ροή ελέγχου για του μη συνδρομητές). Αυτή η ιδέα παρουσιάζεται στο Σχήμα 26.



Σχήμα 26: *Επίπεδα ασφάλειας του δορυφορικού διαδραστικού δικτύου*

Στα παρακάτω υποθέτεται πως μπορεί να υπάρχουν περισσότεροι από έναν χρήστες ανά Return Channel Satellite Terminal (RCST) και πως τέτοιοι χρήστες θα έχουν ασφάλεια με δική τους πρωτοβουλία. Οι όροι RCST και ST (Satellite Terminal) έχουν την ίδια σημασία στο παρόν κείμενο. Η ασφάλεια συνεπώς ορίζεται σε πιο υψηλό επίπεδο από το μεμονωμένο ST. Στη βάση του χρήστη, ένας αλγόριθμος πιστοποίησης μπορεί είτε να ελέγξει τον όνομα χρήστη και τον κωδικό σε μια συσκευή του πελάτη είτε να χρησιμοποιήσει μια smart cart μέσα στο ST. Όλα τα δεδομένα κι ο έλεγχος από και προς τον χρήστη μπορούν να κρυπτογραφηθούν σε μια μεμονωμένη βάση του χρήστη. Κάθε χρήστης μπορεί να έχει το control word για τη ζεύξη επιστροφής και προώθησης, κάτι που δεν επιτρέπει σε κανέναν άλλο παρά μόνο στο NCC/ Πύλη ή τον ίδιο τον χρήστη να αποκρυπτογραφήσει τα δεδομένα, εκτός βέβαια από τη νόμιμη άρση απορρήτου που πραγματοποιείται από τις αρχές μιας χώρας.

2.2.2. Ασφάλεια σε επίπεδο δικτύου

Οι υπηρεσίες ασφαλείας μπορούν επίσης να παρέχονται σε επίπεδο δικτύου. Το IPsec (RFCs 2401 [40], 2408 [43] και 2406 [38]) είναι ένα πρωτόκολλο που λειτουργεί πάνω από το IP και κάτω από τα πρωτόκολλα επιπέδου 4 όπως είναι το TCP και το UDP.

Η ασφάλεια σε επίπεδο δικτύου έχει τα εξής πλεονεκτήματα:

- Η ασφάλεια παρέχεται ανεξάρτητα από τα πρωτόκολλα ανώτερων επιπέδων (TCP, UDP, RTP ή multicast).
- Μπορεί να προστατεύει τη κίνηση του δικτύου από αναδρομολόγηση και παράνομες αλλαγές στις ρυθμίσεις δικτύου.
- Μπορεί να παρέχει προστασία σε όλες τις εφαρμογές πραγματικού και μη χρόνου.

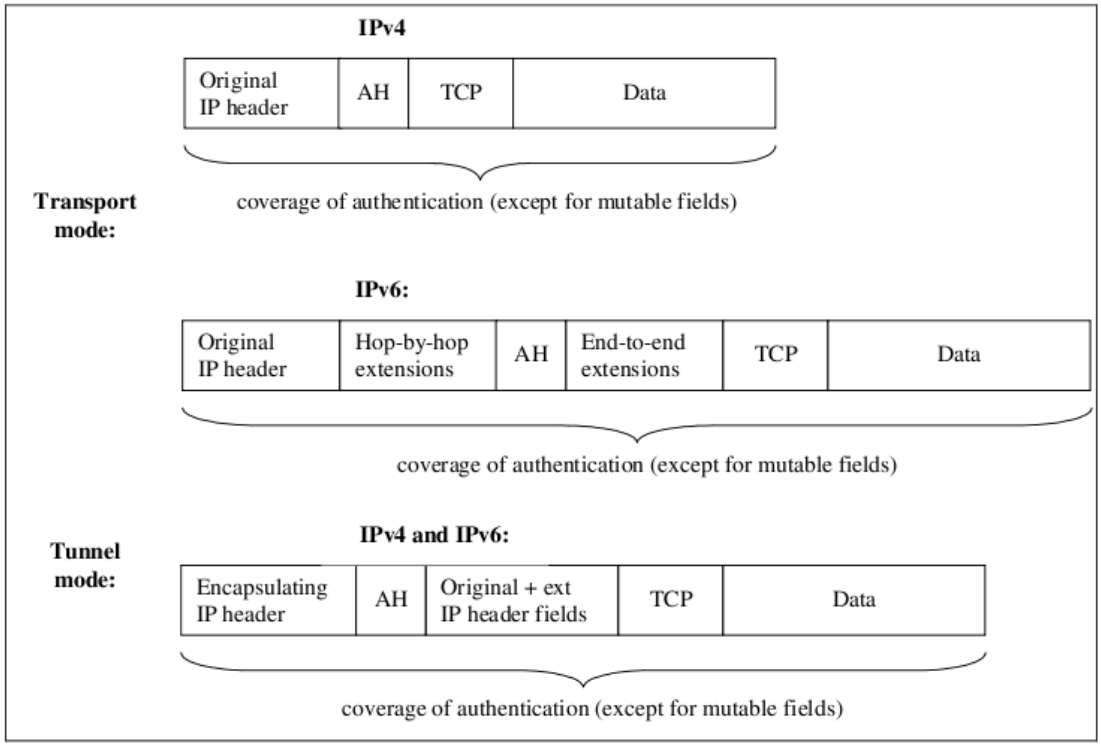
Τα μειονεκτήματα αυτή της ασφάλειας είναι τα εξής:

- Μόνο η απομακρυσμένη τελική διεύθυνση δικτύου (για παράδειγμα, η διεύθυνση IP) πιστοποιείται.
- Στην περίπτωση του IPsec, η εφαρμογή υπηρεσιών ασφαλείας στο επίπεδο IP μπορεί να προκαλέσει προβλήματα στη διασυνεργασία με τα σχετικά πρωτόκολλα. Δύο παραδείγματα είναι: Το Network Address Translations (NAT) δεν μπορεί να χρησιμοποιηθεί (αφού η διεύθυνση IP δεν μπορεί να αλλάξει στο δρόμο) και τα PEPs (RFC 3135 [22]) χρησιμοποιούνται για να ενισχύσουν την απόδοση των ζεύξεων όπως είναι οι κινητές και οι δορυφορικές θα αποτύχουν αφού τα περιεχόμενα των datagrams (όπως ένα κομμάτι TCP) είναι κρυπτογραφημένα.

2.2.2.1. Ασφάλεια Internet (IPSec)

Η αρχιτεκτονική ασφαλείας του Internet Protocol γνωστό ως IP Security (IPSec) είναι η πιο προηγμένη προσπάθεια της τυποποίησης της ασφάλειας του Internet. Το πρωτόκολλο IPSec χρησιμοποιείται για να παρέχει διαλειτουργικές υπηρεσίες ασφάλειας βασισμένες στην κρυπτογράφηση (για παράδειγμα εμπιστευτικότητα, πιστοποίηση, ακεραιότητα κι αποδοχή αναγνώρισης) στο επίπεδο IP. Αποτελείται από ένα πρωτόκολλο πιστοποίησης: Authentication Header (AH), από ένα πρωτόκολλο εμπιστευτικότητας: Encapsulated Security Payload (ESP) κι επίσης περιλαμβάνει ένα Internet Security Association Establishment και το Key Management Protocol (ISAKMP). Αυτά τα πρωτόκολλα ασφαλείας σχεδιάστηκαν και για τα δύο περιβάλλοντα του IP version 4 (IPv4) και του IP version 6 (IPv6).

Όπως φαίνεται στο Σχήμα 27, το IP Authentication Header (AH) παρέχει connectonless (χωρίς συνδέσεις) ακεραιότητα και πιστοποίηση στην πηγή των δεδομένων για τα IP datagrams. Παρέχει επίσης ασφάλεια έναντι των επαναλήψεων. Το Authentication Header μπορεί να χρησιμοποιηθεί είτε μόνο του είτε σε συνδυασμό με το ESP. Το AH πιστοποιεί ελαφρώς περισσότερες πληροφορίες στο IP datagram σε σχέση με το ESP (Η επικεφαλίδα του IP datagram δεν περιλαμβάνεται στον υπολογισμό του κρυπτογραφικού checksum του ESP). Το πρωτόκολλο Authentication Header έχει δύο τύπους: transport ή tunnel.

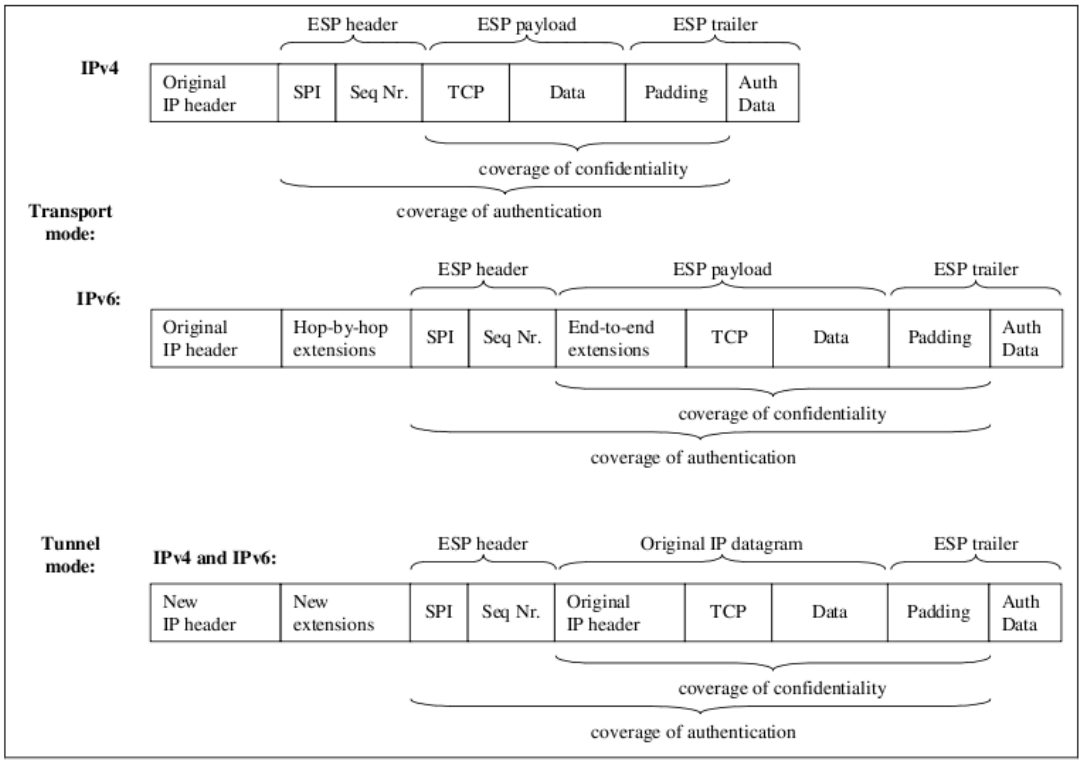


Σχήμα 27: *Authentication Header στις καταστάσεις transport και tunnel*

Στην κατάσταση λειτουργίας transport χρησιμοποιείται μόνο στην πιστοποίηση host-to-host ενώ στην κατάσταση λειτουργίας tunnel μπορεί να χρησιμοποιηθεί μεταξύ δύο hosts, σε ένα host-to-gateway και σε gateway-to-gateway. Το tunnel επιτρέπει στο host να αναθέσει την υπηρεσία ασφάλειας στην πύλη, κάτι που είναι ιδιαίτερα ενδιαφέρον για τις εταιρίες με δύο ιδιωτικά μακρινά δίκτυα που συνδέονται μέσω του δημόσιου Internet. Σε αυτή την κατάσταση, η επικεφαλίδα IP του host/gateway που είναι υπεύθυνη για τον υπολογισμό/ έλεγχο του AH προστίθεται ενώ η παλιά επικεφαλίδα IP κρατιέται στο νέο IP datagram και μετακινείται μετά το AH.

Το Authentication Header περιέχει αρκετά πεδία για την αναγνώριση της υπηρεσίας πιστοποίησης που παρέχεται και επιπλέον για τα κρυπτογραφικά checksums. Το πεδίο της επικεφαλίδας “Next” αναγνωρίζει το επόμενο payload ακολουθούμενο από την επικεφαλίδα AH (IANA αριθμοί πρωτοκόλλων IP). Το πεδίο “Length” δίνει το μήκος της συνολικής επικεφαλίδας AH -2 (σε μονάδα των 32 bits). Το πεδίο του Security Parameter Index (SPI) αναγνωρίζει το σύνδεσμο ασφαλείας για αυτό το datagram (μοναδική τιμή για ένα δεδομένο προορισμό IP. Το SPI κι ο προορισμός αναγνωρίζουν μοναδικά ένα σύνδεσμο ασφαλείας). Τέλος, το “Sequence Number” είναι ένα προαιρετικό πεδίο, που περιλαμβάνεται μόνο όταν η υπηρεσία για την αποτροπή της επανάληψης επιλέγεται. Το AH δεν προστατεύει μεταβλητά πεδία των IP datagrams (για παράδειγμα τις επιλογές της καταγραφής του μονοπατιού, timestamp, της χαλαρής δρομολόγησης της πηγής και της αυστηρής δρομολόγησης της πηγής).

Όπως φαίνεται στο Σχήμα 28, η επικεφαλίδα του Encapsulated Security Payload (ESP) παρέχει μια μείξη υπηρεσιών ασφαλείας: εμπιστευτικότητα των δεδομένων, πιστοποίηση της προέλευσης των δεδομένων, ακεραιότητα χωρίς συνδέσεις, μηχανισμούς για την αποφυγή της επανάληψης κι εμπιστευτικότητα σε περιορισμένη ροή κίνησης. Ο συνδυασμός των υπηρεσιών εξαρτάται από τις επιλογές που γίνονται κατά τη διάρκεια της εδραίωσης του συνδέσμου ασφαλείας. Το ESP μπορεί να χρησιμοποιηθεί μόνο του ή σε συνδυασμό με το AH. Είναι σχεδιασμένο να λειτουργεί είτε στην κατάσταση transport είτε στην tunnel.



Σχήμα 28: *Encapsulated Security Payload (ESP) στις καταστάσεις transport και tunnel*

2.2.3. Ασφάλεια στο επίπεδο μεταφοράς

Οι υπηρεσίες ασφαλείας παρέχονται εναλλακτικά στο επίπεδο μεταφοράς. Παραδείγματα αυτού είναι τα TLS (RFC 2246 [39]) ή το πρωτόκολλο reliable multicast που περιλαμβάνει υπηρεσίες ασφαλείας. Ένα πρωτόκολλο όπως είναι το TLS υποθέτει ένα πρωτόκολλο αξιόπιστης μεταφοράς όπως είναι το TCP κι έτσι λειτουργεί αποτελεσματικά πάνω από το επίπεδο 4 της στοίβας πρωτοκόλλου ISO. Η ασφάλεια σε επίπεδο μεταφοράς που είναι ενσωματωμένη στο επίπεδο μεταφοράς, όπως είναι το πρωτόκολλο reliable multicast έχει τα ακόλουθα πλεονεκτήματα:

- Στην περίπτωση των περιβαλλόντων που είναι βασισμένα σε Unix, η ασφάλεια εφαρμόζεται στο χώρο του χρήστη κι όχι στον πυρήνα, απλοποιώντας τις ρυθμίσεις των hosts.
- Τα κλειδιά μπορούν να είναι κοινά για κάθε host, απλοποιώντας το key management.

Τα αντίστοιχα μειονεκτήματα είναι:

- Οι διευθύνσεις IP των τελικών host είναι γνωστές κι έτσι είναι επιδεκτικές στην ανάλυση της κίνησης.
- Σε σύγκριση με τη λειτουργία του TLS με TCP, δεν υπάρχει κανένα γενικευμένο σύστημα ασφάλειας για πρωτόκολλα αναξιόπιστης μεταφοράς όπως είναι το UDP, το οποίο χρησιμοποιείται ευρέως για να μεταφέρει multicast και κίνηση σε πραγματικό χρόνο.

2.2.3.1. Transport Layer Security (TLS)

Το πρωτόκολλο TLS παρέχει ιδιωτικότητα στις επικοινωνίες μέσα από το Internet. Το πρωτόκολλο επιτρέπει στις εφαρμογές του πελάτη/ server να επικοινωνούν με τέτοιο τρόπο που είναι σχεδιασμένος για να αποτρέπει την υποκλοπή, την αλλοίωση και την πλαστογραφία των μηνυμάτων. Το πρωτόκολλο αποτελείται από δύο επίπεδα: το TLS Record Protocol και το TLS Handshake Protocol. Στο χαμηλότερο επίπεδο, τοποθετημένο στη κορυφή μερικών πρωτοκόλλων αξιόπιστης μεταφοράς (για παράδειγμα το TCP) βρίσκεται το TLS Record Protocol. Το TLS Record Protocol παρέχει ασφάλεια στη σύνδεση που έχει δύο βασικές ιδιότητες:

- Η σύνδεση είναι ιδιωτική. Η συμμετρική κρυπτογράφηση χρησιμοποιείται για να κρυπτογραφηθούν τα δεδομένα (για παράδειγμα το DES (Digital Encryption Standard), το AES (Advanced Encryption Standard), κ.α.). Τα κλειδιά για αυτή τη συμμετρική κρυπτογράφηση παράγονται μοναδικά για κάθε σύνδεση και βασίζονται σε μια μυστική διαπραγμάτευση με ένα άλλο πρωτόκολλο (όπως είναι το TLS Handshake Protocol). Το Record Protocol χρησιμοποιείται επίσης και χωρίς κρυπτογράφηση.
- Η σύνδεση είναι αξιόπιστη. Η μεταφορά του μηνύματος περιλαμβάνει επίσης έναν έλεγχο ακεραιότητας του μηνύματος χρησιμοποιώντας ένα keyed MAC. Ασφαλείς συναρτήσεις κατακερματισμού (hash functions), όπως είναι οι SHA και MD5, χρησιμοποιούνται για τους υπολογισμούς MAC. Το Record Protocol μπορεί να λειτουργήσει και χωρίς MAC, αλλά γενικά σε αυτή τη μορφή χρησιμοποιείται μόνο όταν κάποιο άλλο πρωτόκολλο χρησιμοποιεί το Record Protocol ως μεταφορά των διαπραγματευτικών παραμέτρων ασφάλειας.

Το TLS Record Protocol χρησιμοποιείται για την ενθυλάκωση διαφόρων πρωτοκόλλων υψηλότερων επιπέδων. Ένα τέτοιο πρωτόκολλο ενθυλάκωσης είναι το TLS Handshake Protocol, το οποίο επιτρέπει στον server και τον πελάτη να πιστοποιήσουν ο ένας τον

άλλο και να διαπραγματευτούν τον κρυπτογραφικό αλγόριθμο καθώς και τα κρυπτογραφικά κλειδιά προτού το πρωτόκολλο εφαρμογής μεταδώσει ή λάβει τα πρώτα byte δεδομένων.

Το TLS Handshake Protocol παρέχει ασφάλεια στη σύνδεση που έχει τις εξής τρεις ιδιότητες:

- Η ταυτότητα της ισότιμης οντότητας μπορεί να πιστοποιηθεί με τη χρήση ασύμμετρου ή δημόσιου κλειδιού κρυπτογράφησης (για παράδειγμα το RSA). Αυτή η πιστοποίηση είναι προαιρετική αλλά γενικά απαιτείται για τουλάχιστον μία από τις ισότιμες οντότητες.
- Η φάση της διαπραγμάτευσης ενός κοινόχρηστου μυστικού μηνύματος είναι ασφαλής: Το διαπραγματευόμενο μυστικό μήνυμα δεν είναι διαθέσιμο στους υποκλοπείς και για κάθε πιστοποιημένη σύνδεση το μήνυμα δεν μπορεί να αποκτηθεί, ακόμα κι αν ο επιτιθέμενος μπορεί να βρεθεί στη μέση της σύνδεσης.
- Η διαπραγμάτευση είναι αξιόπιστη: κανένας επιτιθέμενος δεν μπορεί να τροποποιήσει την επικοινωνία διαπραγμάτευσης χωρίς να ανιχνευθεί από τα μέρη της επικοινωνίας.

2.2.3.2. Πρωτόκολλο Ασφαλούς Μεταφοράς σε Πραγματικό Χρόνο - Secure Real Time Transport Protocol (SRTP)

Το SRTP είναι ένα προφίλ του Real Time Transport Protocol (RTP), το οποίο παρέχει εμπιστευτικότητα και προστασία έναντι της επανάληψης στην κίνηση (στον έλεγχο της κίνησης) RTP/RTCP.

Το SRTP μπορεί να πετύχει υψηλό throughput και χαμηλή επέκταση πακέτων. Το SRTP αποδεικνύεται πως παρέχει την κατάλληλη προστασία σε ετερογενή περιβάλλοντα, για παράδειγμα περιβάλλοντα που περιλαμβάνουν τόσο ενσύρματες όσο κι ασύρματες ζεύξεις. Για να έχουμε αυτά τα χαρακτηριστικά, περιγράφονται προκαθορισμένοι μετασχηματισμοί, βασισμένοι σε μια προσθετική ροή κρυπτογραφήματος για την κρυπτογράφηση, μια keyed συνάρτηση κατακερματισμού (hash function) για την πιστοποίηση του μηνύματος κι ένα "σιωπηλό" δείκτη για την αλληλουχία/ συγχρονισμό βασισμένο στο RTP sequence number για το SRTP και σε ένα δείκτη για το Secure RTCP (SRTCP). Τα βασικά χαρακτηριστικά της ασφάλειας του SRTP υπάρχουν για να διασφαλίζουν:

- Την εμπιστευτικότητα των RTP και RTCP payloads
- Την ακεραιότητα ολόκληρων των RTP και RTCP πακέτων, μαζί με την προστασία έναντι των πακέτων που αναπαράγονται ξανά.

Άλλοι λειτουργικοί στόχοι για το πρωτόκολλο είναι:

- Ένα πλαίσιο που επιτρέπει την αναβάθμιση με νέους κρυπτογραφικούς μετασχηματισμούς.
- Χαμηλό κόστος εύρους ζώνης, για παράδειγμα ένα πλαίσιο που διατηρεί την αποδοτικότητα της συμπίεσης της επικεφαλίδας RTP.
- Χαμηλό υπολογιστικό κόστος.
- Μικρό μέγεθος κώδικα και μνήμης δεδομένων για της πληροφορίες keying και τις λίστες αναπαραγωγής.
- Περιορισμένη επέκταση πακέτων για την υποστήριξη του στόχου εξοικονόμησης εύρους ζώνης.
- Ανεξαρτησία από τα βασικά επίπεδα μεταφοράς, δικτύου και το φυσικό επίπεδο που χρησιμοποιούνται από το RTP, συγκεκριμένα υψηλή ανοχή στην απώλεια πακέτων και στην αναδιοργάνωση κι αντοχή στα λάθη μετάδοσης του κρυπτογραφημένου payload.
- Πρόσθετα, το SRTP παρέχει κάποια πρόσθετα χαρακτηριστικά, τα οποία έχουν παρουσιαστεί για να ελαφρύνουν το φόρτο του key management και για την αύξηση της ασφάλειας. Σε αυτά περιλαμβάνονται:

    ~ Ένα μοναδικό κλειδί, που καλείται master key, και παρέχει το υλικό του keying για την προστασίας της εμπιστευτικότητας και της ακεραιότητας, και οι δύο για τη ροή SRTP και την αντίστοιχη ροή SRTCP. Αυτό επιτυγχάνεται μέσω της συνάρτησης key derivation (προέλευση κλειδιού), που παρέχει τα αποκαλούμενα session keys (κλειδιά συνεδρίας) για την αντίστοιχη πρωταρχική ασφάλεια, προερχόμενα με ασφάλεια από το master key.
    ~ Πρόσθετα, το key derivation μπορεί να ρυθμιστεί έτσι ώστε να ανανεώνει περιοδικά τα session keys, κάτι που περιορίζει το μέγεθος του κρυπτογραφήματος που παράγεται από ένα καθορισμένο κλειδί κι είναι διαθέσιμο στον επιτιθέμενο να το κρυπταναλύσει.
    ~ Τα αποκαλούμενα salting keys που χρησιμοποιούνται για την προστασία έναντι των εκτός σύνδεσης επιθέσεων προ-υπολογισμού.

Αυτές οι ιδιότητες εξασφαλίζουν πως το SRTP είναι η καλύτερη προστασία για το RTP/RTCP τόσο για το ενσύρματο όσο και για το ασύρματο σενάριο.

2.2.4. Ασφάλεια σε επίπεδο εφαρμογής

Κατ'αρχήν, το σύστημα ασφάλειας θα πρέπει να είναι όσο κοντά γίνεται στον τελικό χρήστη ή στην τελική οντότητα και για το λόγο αυτό η ασφάλεια σε επίπεδο εφαρμογής προσφέρει μια καλή λύση. Στην ασφάλεια σε επίπεδο εφαρμογής, οι υπηρεσίες ασφάλειας παρέχονται σε κάθε εφαρμογή κι είναι ενσωματωμένες στον κώδικα της εφαρμογής. Η ασφάλεια σε επίπεδο εφαρμογής έχει τα εξής πλεονεκτήματα:

- Οι υπηρεσίες ασφάλειας είναι ανεξάρτητες των διέποντων πρωτοκόλλων.

- Οι υπηρεσίες ασφάλειας παρέχουν ένα επίπεδο διαβεβαίωσης που είναι ανεξάρτητο της κυριότητας του διέποντος δικτύου (για παράδειγμα το δημόσιο Internet, τα VPNs, κι άλλα τμήματα μιας εταιρίας).
- Τα δεδομένα δεν τίθενται σε κίνδυνο αν παραδοθούν σε λάθος host ή εφαρμογή.

Παρόλαυτα, η ασφάλεια σε επίπεδο εφαρμογής έχει τα παρακάτω μειονεκτήματα:

- Η ασφάλεια πρέπει να κατασκευάζεται μεμονωμένα σε κάθε εφαρμογή, αυξάνοντας την ανάπτυξη του λογισμικού και τη δοκιμή του χρονοδιαγράμματος, με ενδεχομένως μειωμένα επίπεδα της ασφάλειας λογισμικού.
- Τα κλειδιά επομένως χωρίζονται για κάθε εφαρμογή, με διπλασιασμό της προσπάθειας στο key management.
- Η ανάλυση της κίνησης μπορεί εύκολα να εκτελεστεί από ένα ενδεχόμενο επιτιθέμενο: οι διευθύνσεις του τελικού σημείου (για παράδειγμα η θύρα TCP και η διεύθυνση IP του host) είναι ορατές στο ακρυπτογράφητο κείμενο. Συνεπώς, ένας επιτιθέμενος γνωρίζει ποιος επικοινωνεί, ακόμα κι αν δεν μπορεί να καθορίσει τι ακριβώς λέγεται.
- Οι επιθέσεις άρνησης παροχής υπηρεσιών είναι πολύ πιθανές, κατά τις οποίες ένας ενεργός εισβολέας εισάγει ένα μεγάλο αριθμό ψεύτικων πακέτων τα οποία η ασφάλεια σε επίπεδο εφαρμογής θα εντοπίσει και θα απορρίψει, καταναλώνοντας όμως αρκετό χρόνο CPU στο τελικό σύστημα.

2.2.4.1. Ασφάλεια στην eXtensible Markup Language (XML)

Κατά τη διάρκεια των δύο τελευταίων χρόνων, η extensible Markup Language (XML) έχει γρήγορα αναδειχθεί στο πρότυπο για την ηλεκτρονική ανταλλαγή δεδομένων στις επιχειρηματικές εφαρμογές. Παράλληλα, συνεχίζει να επεκτείνεται η υιοθέτηση του Public Key Infrastructure (PKI) και των ψηφιακών υπογραφών από τις αγορές, τους εμπόρους του Internet, και τους προμηθευτές ως το de facto ισχυρό θεμέλιο για την πιστοποίηση των χρηστών, των ιστοτόπων και των επιχειρηματικών εταίρων.

Εξαιτίας της ταχύτητας που απέκτησε η XML ως η προτεινόμενη μορφή για την ανταλλαγή εταιρικών πληροφοριών στο Web, μεγαλώνει η ανάγκη για πρότυπους μηχανισμούς για τις εφαρμογές ώστε να παρέχουν πιστοποίηση κι ιδιωτικότητα στα κείμενα XML. Οι σημερινές αγορές είναι πρόθυμες στο να δουλεύουν μαζί η XML και το PKI με σκοπό να καλυφθούν οι ευρείες προσδοκίες για κρυπτογραφικά ασφαλείς, XML συζευγμένες εταιρικές εφαρμογές. Όλες οι εφαρμογές ηλεκτρονικού εμπορίου απαιτούν εμπιστοσύνη κι ασφάλεια, κάνοντας έτσι το έργο της επινόησης κοινών XML μηχανισμών για την πιστοποίηση μεταξύ των εμπόρων, των αγοραστών και των προμηθευτών και των ψηφιακών υπογραφών και της κρυπτογράφησης των κειμένων XML όπως τα συμβόλαια κι οι συναλλαγές πληρωμών.

Επιπρόσθετα, η ένωση των οργανισμών IETF-W3C σε μια ομάδα εργασίας έχει μόλις ολοκληρώσει ένα προτεινόμενο πρότυπο για τις XML Digital Signatures, αλλά κάθε

καταστατικό ρητών περιορίζει κάθε εργασία σε συγκεκριμένη περιοχή. Πρόσφατα, μια νέα ομάδα εργασίας μέσα στον οργανισμό W3C έχει επωμιστεί με την ευθύνη της ανάπτυξης των προτύπων για την XML Encryption.

2.2.4.2. Digital Rights Management (DRM)

Η μεταφορά αρχείων είναι αυτή τη στιγμή ο μεγαλύτερος καταγεγραμμένος καταναλωτής της χωρητικότητας του Internet, με τη μορφή των συνδέσεων peer-to-peer για το διαμοιρασμό μουσικών αρχείων. Η βιομηχανία παραγωγής μουσικής φαίνεται να είναι διστακτική στη multicast διανομή μουσικής, εξαιτίας της πιθανότητας να μοιράζονται απευθείας τα αρχεία οι χρήστες μεταξύ τους. Αυτές είναι εκτιμήσεις για την ανάπτυξη της βιομηχανίας Digital Right Management (DRM) [40] να προτρέψει τους ιδιοκτήτες πνευματικών δικαιωμάτων να συνειδητοποιήσουν τα έσοδα κάθε μεταφοράς, είτε μέσω μιας κεντρικής διανομής είτε peer-to-peer. Το μοντέλο BSM broadcast για το Internet θα πρέπει να επιτρέπει να επανέλθει ο έλεγχος στους ιδιοκτήτες δικαιωμάτων έτσι ώστε να μειωθούν οι συνδέσεις peer-to-peer.

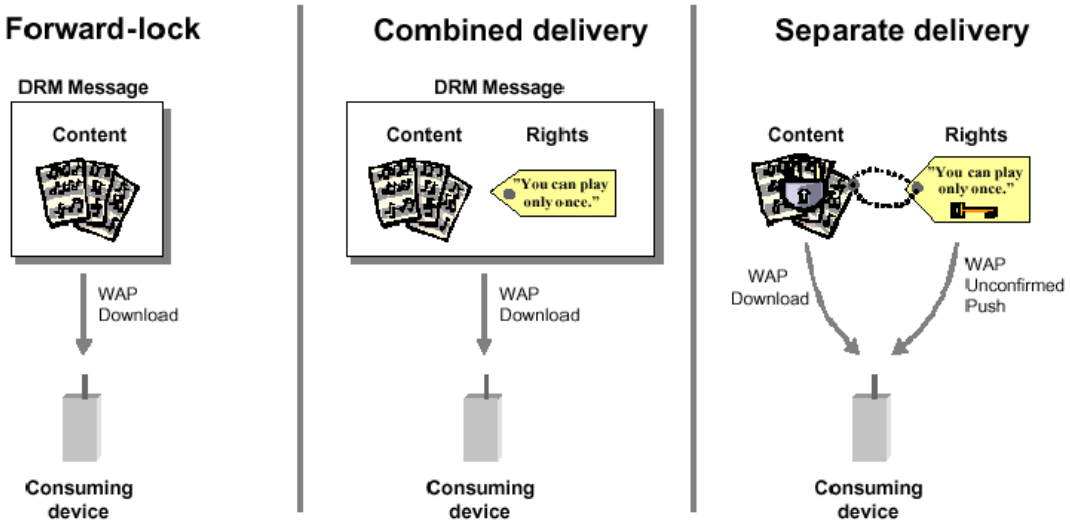
Το DRM είναι ένας τρόπος κρυπτογράφησης των αρχείων πριν τη μετάδοση τους και την τοπική αποθήκευση τους από το χρήστη, έτσι ώστε τα αρχεία να αποκρυπτογραφούνται από τους κατόχους ενός έγκυρου κλειδιού κάτω από καθορισμένες εμπορικές συνθήκες. Θέτει έτσι σε κίνδυνο τόσο τη διαδικασία κρυπτογράφησης/ αποκρυπτογράφησης όσο και τη διαδικασία του key management που είναι συνδεδεμένο με το subscription management.

Ο κύριος σκοπός του DRM είναι να ενδυναμώσει την αφορά περιεχομένου στη μαζική αγορά επιτρέποντας τις νόμιμες αγορές και κάνοντας παράνομη την αντιγραφή και την προώθηση μη ασφαλή και καθόλου συμφέρουσα από οικονομική σκοπιά. Από την πλευρά των ιδιοκτητών, διανομέων και κομιστών του περιεχομένου αναμένεται πως μόνο οι νόμιμες διαδικασίες θα χρησιμοποιούνται στην προστασία του υλικού από την πηγή.

Κάθε αρχείο κρυπτογραφείται με ένα κλειδί, που επιτρέπει τους χρήστες να το αποκρυπτογραφήσουν και παρέχεται μέσα από ένα πακέτο άδειας το οποίο εφαρμόζεται στο λογισμικό και περιλαμβάνει τους όρους χρήσης, για παράδειγμα τις ημερομηνίες ισχύος, τις φορές που έχει παιχτεί ή το σύνολο των χαρακτηριστικών ενός προγράμματος υπολογιστή. Οι όροι μπορούν να επεκταθούν σε ρήτρα μιας διαδικασίας όταν ένα αρχείο αντιγράφεται ή προωθείται, ένα πρόστιμο μπορεί να πληρώνεται στους ιδιοκτήτες των δικαιωμάτων. Αυτό μπορεί να είναι ένας τρόπος νομιμοποίησης της προώθησης peer-to-peer και μπορεί να είναι χρήσιμο σε πολλές περιπτώσεις στις οποίες το υλικό δεν είναι απευθείας διαθέσιμο από τον διανομέα.

2.2.4.2.1. Open Mobile Alliance (OMA) DRM

Οι στόχοι του Open Mobile Alliance (OMA) DRM είναι να προτρέψει την ελεγχόμενη κατανάλωση των αντικειμένων ψηφιακών μέσων επιτρέποντας τους παρόχους περιεχομένου να εκδηλώσουν δικαιώματα χρήσης, όπως για παράδειγμα την ικανότητα προεπισκόπησης του DRM περιεχομένου, την εμπόδιση της παράνομης προώθησης του κατεβασμένου DRM περιεχομένου σε άλλους χρήστες. Στα μέλη του OMA περιλαμβάνονται κυρίαρχες εταιρίες λογισμικού και πάροχοι κινητού δικτύου όπως η Microsoft, η IBM,η Nokia κι η Ericsson.



Σχήμα 29: *OMA DRM μέθοδοι παράδοσης*

Τα δικαιώματα μπορούν να παραδοθούν στη συσκευή κατανάλωσης κατεβάζοντας τους μαζί με το περιεχόμενο ή στέλνοντας τα δικαιώματα χωριστά από το περιεχόμενο (βλέπε Σχήμα 29). Η πρώτη περίπτωση (συνδυασμένη παράδοση) είναι πιο απλή ενώ η δεύτερη περίπτωση (ξεχωριστή παράδοση) παρέχει μεγαλύτερη ασφάλεια κάνοντας πιο δύσκολη την κλοπή του περιεχομένου.

Για κλείδωμα της προώθησης και συνδυασμένη παράδοση ο πάροχος του περιεχομένου πρέπει να το κάνει σε μορφή πακέτων, εναλλακτικά με ένα αντικείμενο δικαιωμάτων μέσα στο DRM μήνυμα. Αυτό το μήνυμα μπορεί να παραδίδεται στη συσκευή χρησιμοποιώντας για παράδειγμα το μηχανισμό OMA Download. Στη μέθοδο της ξεχωριστής παράδοσης ο πάροχος του περιεχομένου χρειάζεται να μετατρέψει το αντικείμενο του ακρυπτογράφητου μέσου σε DRM Content Format (DCF) όπως ορίζεται στις προδιαγραφές “DRM Content Format (DCF)”. Αυτή η μετατροπή περιλαμβάνει συμμετρική κρυπτογράφηση του περιεχομένου κάνοντας το DRM προστατευμένο περιεχόμενο άχρηστο σε άλλους που δεν έχουν πρόσβαση στο κρυπτογραφικό κλειδί του περιεχομένου. Έτσι το περιεχόμενο σε μορφή DRM μπορεί να διανέμεται μέσω μιας μη ασφαλούς μεταφοράς και μια πιο ασφαλής (από την οπτική

του DRM) μεταφορά χρησιμοποιείται για την παράδοση των όρων χρήσης με το κρυπτογραφικό κλειδί.

Για τον χειρισμό αρχείων δεδομένων συνεχόμενης ροής χρησιμοποιούνται οι μηχανισμοί OMA DRM σε έμμεσου ελέγχου αντικείμενα πολυμέσων μέσω ελέγχου των μετα-δεδομένων. Για παράδειγμα, μπορεί να είναι μια καταγραφή Session Description Protocol (SDP) ως περιγραφή της συνεδρίας των αρχείων δεδομένων συνεχόμενης ροής. Για να υπάρχει το ίδιο επίπεδο ασφάλειας για τις ροές με τα κατεβασμένα αντικείμενα, προτείνεται ο streaming player να μην επιτρέπεται να αποθηκεύει ροές πολυμέσων. Περαιτέρω, οι ροές πολυμέσων πραγματικού χρόνου πρέπει να προστατεύονται με τη χρήση μηχανισμών ισχυρής κρυπτογράφησης κατάλληλης για ασύρματο περιβάλλον, όπως είναι το Secure Real-Time Protocol (SRTP) που περιγράφηκε στην παράγραφο 2.2.3.2.

2.2.4.3. Secure Shell (SSH)

Το Secure Shell αναπτύχθηκε από το SSH Communication Security που έχει μεγάλο εύρος χαρακτηριστικών μεταξύ των οποίων είναι η προστασία όλων των κωδικών και δεδομένων, η πλήρως ενσωματωμένη ασφαλής μεταφορά αρχείων κι αντιγραφής αρχείων κι η αυτόματη πιστοποίηση των χρηστών. Πρόκειται για ένα πρόγραμμα για τη σύνδεση σε άλλο υπολογιστή μέσω του δικτύου, για την εκτέλεση εντολών σε απομακρυσμένο υπολογιστή και τη μεταφορά αρχείων από τον ένα υπολογιστή στον άλλο. Παρέχει ισχυρή πιστοποίηση κι ασφαλείς επικοινωνίες μέσω μη ασφαλών καναλιών. Προορίζεται για τον αντικαταστάτη των rlogin, rash και rap.

Το SSH είναι ένα πρωτόκολλο για ασφαλή απομακρυσμένη είσοδο κι άλλες ασφαλείς υπηρεσίες δικτύου πάνω σε ένα μη ασφαλές δίκτυο. Το Internet Draft περιγράφει την αρχιτεκτονική του πρωτοκόλλου SSH όπως επίσης τη σημειογραφία και την ορολογία που χρησιμοποιείται στα έγγραφα του πρωτοκόλλου SSH. Αναφέρει επίσης το αλγοριθμικό σύστημα SSH που επιτρέπει τοπικές επεκτάσεις. Το πρωτόκολλο SSH αποτελείται από τρία κύρια στοιχεία: Το Transport Layer Protocol παρέχει πιστοποίηση του server, μυστικότητα κι ακεραιότητα με τέλεια προώθηση της μυστικότητας. Το User Authentication Protocol πιστοποιεί τον πελάτη του server. Το Connection Protocol πολυπλέκει το κρυπτογραφημένο tunnel σε πολλά λογικά κανάλια.

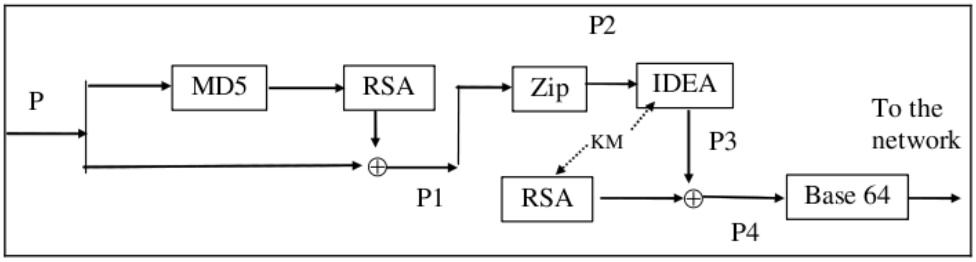
2.2.4.4. Pretty Good Privacy (PGP)

Το Pretty Good Privacy είναι ένα ολοκληρωμένο πακέτο ασφάλειας email που προσφέρει ιδιωτικότητα, πιστοποίηση, ψηφιακές υπογραφές και συμπίεση. Το PGP

βασίζεται στο σύστημα δημόσιου κλειδιού RSA και MD5 και στο σύστημα μυστικού κλειδιού IDEA.

Όπως φαίνεται στο Σχήμα 30, η Alice θέλει να στείλει το ακρυπτογράφητο μήνυμα P στον Bob με ασφαλή τρόπο. Υποθέτοντας πως τόσο η Alice όσο κι ο Bob γνωρίζουν ο ένας του άλλου το δημόσιο κλειδί. Η Alice αρχικά κατακερματίζει το μήνυμα P χρησιμοποιώντας το MD5 και μετά κρυπτογραφεί το αποτέλεσμα με το δικό της ιδιωτικό κλειδί RSA. Οι κρυπτογραφημένες τιμές κατακερματισμού και το αρχικό μήνυμα ενώνονται τώρα στο μήνυμα P1 και συμπιέζονται στο μήνυμα P2 χρησιμοποιώντας το πρόγραμμα ZIP. Έπειτα το PGP προτρέπει την Alice για μια τυχαία είσοδο να παράγει ένα 128-bit IDEA κλειδί KM. Το session key KM χρησιμοποιείται για την κρυπτογράφηση του P2 και το KM κρυπτογραφείται χρησιμοποιώντας το δημόσιο κλειδί του Bob. Αυτά τα δύο στοιχεία ενώνονται και μετατρέπονται στο base64 για να το κάνουν συμβατό με το RFC 822 [41] και το MIME.

Όταν ο Bob παίρνει το μήνυμα, αντιστρέφει την κωδικοποίηση base64 κι αποκρυπτογραφεί το κλειδί IDEA χρησιμοποιώντας το ιδιωτικό κλειδί RSA. Χρησιμοποιώντας αυτό το κλειδί, αποκρυπτογραφεί το μήνυμα για να πάρει το P2. Μετά την αποσυμπίεση του ο Bob αποκρυπτογραφεί τη τιμή του κατακερματισμού χρησιμοποιώντας το δημόσιο κλειδί της Alice. Αν η τιμή του κατακερματισμού συμφωνεί με το δικό του MD5, τότε ξέρει πως το P είναι το σωστό μήνυμα από την Alice.



P: Plaintext
P1: P + signed hash of P (using source's RSA private key)
P2: Ziped P1
P3: Encrypted P2 (with IDEA"s secret key KM)
P4: P3 + secret key KM for IDEA (encrypted with destination's RSA public key)

Σχήμα 30: *PGP σύστημα ασφάλειας email*

Το RFC 2015 [42] περιγράφει πως το Pretty Good Privacy (PGP) μπορεί να χρησιμοποιηθεί για την ασφάλεια των emails στη μορφή Multipurpose Internet Mail Extensions (MIME).

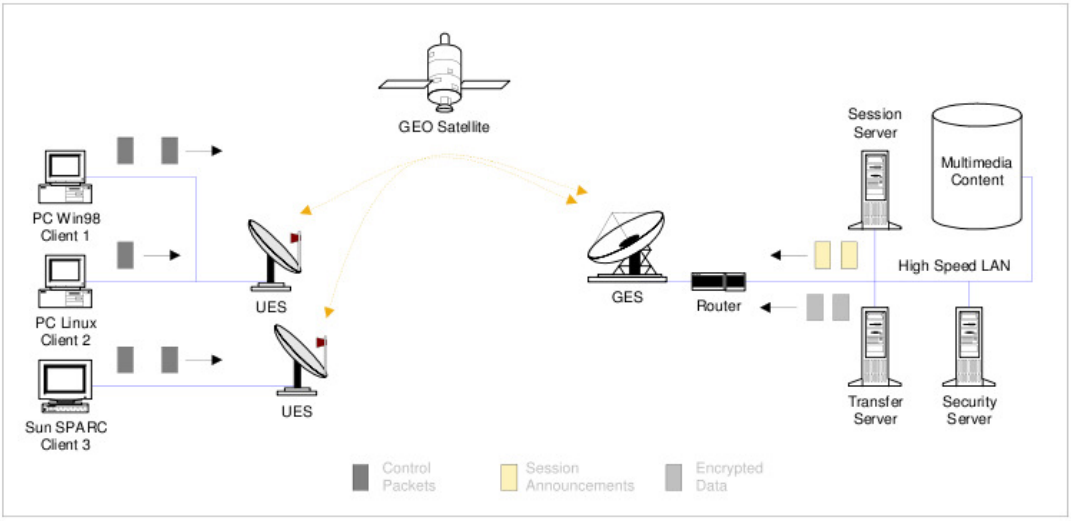
2.2.4.5. Κατάλληλα διαμορφωμένη ασφάλεια για τις δορυφορικές εφαρμογές

Είναι αρκετά πιθανή η ανάπτυξη ασφαλών κι αξιόπιστων εφαρμογών μεταφοράς που λαμβάνουν υπόψη τους τα χαρακτηριστικά της δορυφορικής ζεύξης. Ένα παράδειγμα είναι το ασφαλές Satellite Reliable Multicast Transport Protocol (SAT-RMTP) που ανά πτύχθηκε ως μέρος του GEOCAST project (Ένα Ευρωπαϊκό IST project). Το SAT-RMTP παρέχει παράδοση του περιεχομένου του δικτύου μέσω ενός multicast δικτύου. Αυτό το πρωτόκολλο μεταφοράς αναπτύχθηκε για να μετριάσει τη ζήτηση στο server/ δίκτυο και για να ανέχεται την απώλεια πακέτων εξαιτίας τόσο της συμφόρησης στο στένεμα του δικτύου όσο και των βλαβών της ζεύξης (fading).

Κωδικοποιημένα clip πολυμέσων αποθηκεύονται στον server περιεχομένου. Χρησιμοποιώντας το εργαλείο περιεχομένου, αυτά τα αρχεία κρυπτογραφούνται και δημιουργείται η πληροφορία της συνεδρίας. Μπορεί να χρησιμοποιηθεί μορφή MPEG-1, MPEG-2 ή QuickTime. Κάθε χρήστης χρησιμοποιεί ένα εργαλείο συνεδρίας πελάτη για να επιλέξει το απαραίτητο περιεχόμενο πολυμέσων. Ένα πρωτόκολλο συνεδρίας (Session Directory Revised (SDR)) χρησιμοποιείται το οποίο έχει μια menu-driven interface. Το πρωτόκολλο συνεδρίας περιγράφει τα αντικείμενα (αρχεία) που είναι διαθέσιμα για κατέβασμα.

Το πρωτόκολλο ασφαλείας αναγνωρίζει τους ξεχωριστούς τελικούς χρήστες και συσχετίζει καταστάσεις (κλειδιά) ασφαλείας με τους πελάτες. Η κρυπτογράφηση κι η αποκρυπτογράφηση παρέχεται σε επίπεδο εφαρμογής, κι όταν χρειάζεται η κρυπτογράφηση το πρωτόκολλο μεταφοράς διανέμει κρυπτογραφημένο περιεχόμενο.

Το Σχήμα 31 δείχνει την αλληλεπίδραση μεταξύ του session server και κάθε πελάτη του. Η εφαρμογή έχει κατασκευαστεί με τέτοιο τρόπο ώστε να επιτρέπει τη διαδικασία session server κι έναν αριθμό πρωτοκόλλων μεταφοράς/ ασφάλειας να βρίσκονται σε μια κοινή πλατφόρμα server ή εναλλακτικά να κατανέμονται μεταξύ ενός αριθμού πλατφόρμων server.



Σχήμα 31: *SATRMTP περιγραφή της επικοινωνίας των πρωτοκόλλων μεταφοράς και συνεδρίας*

Αναφορικά με την ασφάλεια, όλοι οι πελάτες θα έχουν ένα Secure Association (SA) με τον server ασφάλειας. Αυτός ο SA μπορεί να βασίζεται είτε σε ένα μυστικό κλειδί είτε σε δημόσιο κλειδί. Στον SA με μυστικό κλειδί, κάθε πελάτης μοιράζεται ένα μυστικό κλειδί με τον server. Στον SA με δημόσιο κλειδί, κάθε πελάτης έχει ένα πιστοποιητικό, το οποίο αποθηκεύεται στον server κι ένα δικό του ιδιωτικό κλειδί που αποθηκεύεται τοπικά. Στον SA με το δημόσιο κλειδί κάθε πελάτης επίσης αποθηκεύει το δημόσιο πιστοποιητικό του server ασφάλειας.

Στην εφαρμογή SATRMTP, ο server ασφάλειας διατηρεί δύο βάσεις δεδομένων: μια βάση με τις πληροφορίες του χρήστη (περιέχει άδειες πρόσβασης του πελάτη) και μια βάση ασφάλειας (όπου αποθηκεύονται τα κλειδιά). Ένα πρωτόκολλο ασφάλειας πελάτη/ server αναπτύσσεται κι εφαρμόζεται έτσι ώστε να παρέχει πιστοποίηση και πρόσβαση και την ασφαλή διανομή των κλειδιών στους πελάτες (χρησιμοποιώντας τον σύνδεσμο ασφαλείας). Ακολουθώντας τη μεταφορά του αρχείου, το εργαλείο αποκρυπτογράφησης του περιεχομένου, από πλευράς πελάτη, θα αποκρυπτογραφήσει κάθε αντικείμενο. Το εργαλείο ελέγχει επίσης τη ψηφιακή υπογραφή του αποστολέα για να τον πιστοποιήσει. Το αποκρυπτογραφημένο αρχείο περνάει μετά σε ένα multimedia player. Ακολουθώντας την επιτυχημένη αποκρυπτογράφηση, ο πελάτης ασφάλειας πρέπει να στείλει μια βεβαίωση στο server ασφάλειας για να του επιβεβαιώσει την επιτυχημένη αποκρυπτογράφηση.

2.2.5. Ασφάλεια end-to-end κι ασφάλεια δορυφορικού δικτύου

Η ασφάλεια end-to-end μπορεί να παρέχεται σε κάθε επίπεδο της στοίβας πρωτοκόλλου όπως είναι το επίπεδο εφαρμογής, μεταφοράς ή δικτύου, όπως παρουσιάστηκαν στις παραγράφους 2.3.2 έως 2.3.4. Γενικά, υπάρχει η ανάγκη καθιέρωσης μιας σχέσης

εμπιστοσύνης μεταξύ των χρηστών του συστήματος ασφάλειας end-to-end μέσω ενός συστήματος διαχείρισης της ασφάλειας. Οι λειτουργίες ασφαλείας μπορεί να είναι ορατές στους τελικούς χρήστες και τις εφαρμογές αν εφαρμόζονται στο επίπεδο εφαρμογής, ή μπορεί να είναι transparent, αν εφαρμόζονται σε κατώτερα επίπεδα.

Σε αντίθεση, η ασφάλεια του δορυφορικού δικτύου επικεντρώνεται στον έλεγχο πρόσβασης και σε μηχανισμούς κρυπτογράφησης/ ακεραιότητας των δεδομένων μέσα στα όρια του BSM δορυφορικού δικτύου. Η ασφάλεια σε επίπεδο σύνδεσης είναι η καλύτερη λύση εδώ, όπως παρουσιάστηκε στην παράγραφο 2.3.1. Το δορυφορικό δίκτυο μπορεί να έχει τοπολογία αστέρα και πλέγματος με αναγεννητικούς ή bent pipe δορυφόρους. Οι διαδικασίες ασφάλειας DVB και ATM μπορούν να χρησιμοποιηθούν για να ασφαλίζουν τις δορυφορικές ζεύξεις. Το IPSec μπορεί να χρησιμοποιηθεί για να παρέχει ασφάλεια στο δορυφορικό δίκτυο εφαρμόζοντας IPSec tunnels.

2.2.6. Υπηρεσίες ασφάλειας στα επίπεδα του BSM πρωτόκολλου

Ο πίνακας 1 παρέχει μια περίληψη των κύριων πλεονεκτημάτων και μειονεκτημάτων της ασφάλειας σε κάθε επίπεδο της BSM στοίβας πρωτοκόλλου.

Πίνακας 1: Σύγκριση της ασφάλειας στα διάφορα επίπεδα

	Επίπεδο σύνδεσης	**Επίπεδο δικτύου**	**Επίπεδο μεταφοράς**	**Επίπεδο εφαρμογής**
Κύρια πλεονεκτήματα	Πλήρης έλεγχος της ασφάλειας της δορυφορικής ζεύξης.	Το IPSec είναι η καλύτερη λύση για την ασφάλεια του Internet.	Χρησιμοποιείται ευρέως για την ασφάλεια των TCP συνδέσεων.	Μπορεί να ικανοποιήσει τις απαιτήσεις των εφαρμογών πολύ καλά.
Κύρια μειονεκτήματα	Μόνο το δορυφορικό hop είναι ασφαλές.	Το IPSec λειτουργεί μόνο για δίκτυα IP.	Καμία ασφάλεια για UDP και multicast.	Καμία διαφάνεια, όπου οι εφαρμογές χρειάζονται τροποποίηση για να προσαρμοστούν στην ασφάλεια.

Επίσης οι υπηρεσίες ασφάλειας μπορεί να παρέχονται σε επίπεδο της BSM στοίβας πρωτοκόλλου όπως συνοψίζεται παρακάτω:

Πίνακας 2: Υπηρεσίες ασφαλείας στα διάφορα επίπεδα πρωτοκόλλου

	Επίπεδο σύνδεσης	**Επίπεδο δικτύου IP**	**Επίπεδο μεταφοράς**	**Επίπεδο εφαρμογής**
Πιστοποίηση του δορυφορικού τερματικού	Ναι	Ναι (διεύθυνση IP)	Όχι	Όχι
Πιστοποίηση του τερματικού χρήστη	Όχι	Ναι (διεύθυνση IP)	Όχι	Όχι
Πιστοποίηση του χρήστη	Όχι	Όχι	Ναι	Ναι
Ιδιωτικότητα στη δορυφορική ζεύξη	Ναι	Ναι (IPSec IP tunnel)	Όχι	Όχι
Ιδιωτικότητα end-to-end	Όχι	Ναι	Ναι	Ναι
Ακεραιότητα δεδομένων στη δορυφορική ζεύξη	Ναι	Ναι (IPSec IP tunnel)	Όχι	Όχι
Ακεραιότητα δεδομένων end-to-end	Όχι	Ναι	Ναι	Ναι

Εξετάζοντας τον Πίνακα 2, βλέπουμε πως εφαρμόζοντας ασφάλεια σε επίπεδο δικτύου όπως είναι το IPSec, υπάρχει ευελιξία στη στενότερη ενοποίηση με το Internet και ικανοποιείται η απαίτηση κάποιων υπηρεσιών πολυμέσων για δορυφορική ασφάλεια ή ασφάλεια end-to-end.

2.3. Επισκόπηση της διαχείρισης ασφάλειας

Κάθε σύστημα ασφάλειας που απαιτεί τα δύο μέρη να έχουν το ίδιο key material χρειάζεται σύστημα key management για να διασφαλίσει πως και τα δύο μέρη συμφωνούν για το ποιούς κρυπτογραφικούς αλγόριθμους θα χρησιμοποιήσουν και ποια κρυπτογραφικά κλειδιά χρειάζονται. Σε όλες τις περιπτώσεις το πιο δύσκολο πρόβλημα ασφάλειας είναι η διαχείριση ασφάλειας και η διανομή του κλειδιού. Πέντε παραδείγματα key management παρουσιάζονται στις επόμενες παραγράφους: υπό όρους πρόσβαση DVB-S, ασφάλεια DVB-RCS, ασφάλεια IP unicast έλεγχος πρόσβασης με τη χρήση firewalls και διαχείριση ασφάλειας IP multicast.

2.3.1. Key Management της υπό όρους πρόσβασης DVB-S

Βλέπε την παράγραφο 2.3.1.2. για περισσότερες λεπτομέρειες.

2.3.2. Πρωτόκολλα ανταλλαγής κλειδιών DVB-RCS

Main key exchange
Το Main Key Exchange (MKE) χρησιμοποιεί το πρωτόκολλο των Diffie-Hellman για να δημιουργήσει ένα κοινόχρηστο μυστικό μεταξύ του NCC και του ST, το οποίο είναι ανεξάρτητο από τη τιμή cookie. Περαιτέρω χρησιμοποιεί τη τιμή cookie για να πιστοποιήσει το ST και το NCC. Χρησιμοποιεί εναλλακτικά το πρόσφατα δημιουργημένο κοινόχρηστο μυστικό για να ενημερώσει τη τιμή cookie. Τελικά, εξάγει ένα κοινόχρηστο μυστικό κλειδί που χρησιμοποιείται στην ασφάλεια περιεχομένου και στην επεξεργασία του payload της ροής δεδομένων.

Η ανταλλαγή ξεκινάει από το NCC στέλνοντας ένα μήνυμα που περιέχει τις τιμές Diffie-Hellman m, g, X κι ένα nonce string, το nonce1. Το ST ανταποκρίνεται με ένα μήνυμα που περιέχει τη τιμή Diffie-Hellman, Y, μια τυχαία nonce string, τη nonce2 κι ένα string πιστοποίησης, το auth. Το NCC και ST χρησιμοποιεί την ίδια φόρμουλα για τον υπολογισμό του string πιστοποίησης

auth= H (cookie, nonce1 ~ nonce2)

το οποίο γνωστοποιείται από το ST κι ελέγχεται από το NCC. Αυτό αποδεικνύει τη ταυτότητα του ST, αφού απαιτεί τη γνώση του cookie για το σωστό υπολογισμό του auth. Το ST και το NCC χρησιμοποιούν τις τιμές Diffie-Hellman για να καταλήξουν στην ίδια κρυφή τιμή, s:

s = g^(x × y)modm

Αυτή η τιμή του μη προσημασμένου ακεραίου κωδικοποιείται ως ένα byte string, το μήκος του οποίου καθορίζεται από την παράμετρο μεγέθους Diffie-Hellman, χρησιμοποιώντας την ιεράρχηση byte big endian. Χρησιμοποιείται μετά στον υπολογισμό του προσωρινού κοινόχρηστου κρυφού string, temp:

temp = H (encode (s), nonce2 ~ nonce1)

Αν το cookie πρόκειται να ενημερωθεί, η νέα τιμή υπολογίζεται για τα τμήματα από n = 1,2,… :

newcookie(n) = H (temp ~ (unsigned char)1 ~ (unsigned char)n, " ")

Αυτά τα string τιμών υπολογίζονται και συνενώνονται μέχρι το συνολικό μέγεθος να φτάσει ή να υπερβεί το μήκος του cookie. Τότε το cookie επικρατεί παίρνοντας τα πρώτα 20 bytes από τα συνενωμένα τμήματα, ξεκινώντας από την αρχή. Το session key που χρησιμοποιείται για την κρυπτογράφηση της ροής payload υπολογίζεται παρομοίως σε τμήματα:

key(n) = H (temp ~ (unsigned char)2 ~ (unsigned char)n, " ")

όπου και πάλι, ένας ικανοποιητικός αριθμός τμημάτων υπολογίζεται για να παράγει αρκετά bytes για να καλυφθεί το μήκος του κλειδιού. Το session key επικρατεί, με τον ίδιο τρόπο που επικράτησε και το cookie, παίρνοντας τον απαραίτητο αριθμό bytes έξω από τα συνενωμένα κομμάτια, ξεκινώντας από την αρχή.

Quick Key Exchange

Το Quick Key Exchange (QKE) χρησιμοποιεί την υπάρχουσα τιμή του cookie για να πιστοποιήσει το ST στο NCC, κι έπειτα εξάγει ένα κοινόχρηστο μυστικό κλειδί για την ασφάλεια του περιεχομένου που χρησιμοποιείται στη διαδικασία του payload της ροής δεδομένων. Η ανταλλαγή ξεκινάει από το NCC στέλνοντας ένα μήνυμα που περιέχει ένα τυχαίο nonce string, το nonce1.

Το ST ανταποκρίνεται με ένα μήνυμα που περιέχει ένα τυχαίο nonce string, το nonce2 και μια παράμετρο πιστοποίησης, την auth. Η τιμή της auth υπολογίζεται με τον ίδιο τρόπο που γίνεται και στο Main Key Exchange και μπορεί να χρησιμοποιηθεί για την επιβεβαίωση της ταυτότητας του ST. Το ST και το NCC υπολογίζουν ένα προσωρινό κοινόχρηστο μυστικό string, το temp:

temp = H (cookie ~ (unsigned char)3, nonce2 ~ nonce1)

Αυτή η τιμή χρησιμοποιείται για να παράγει το κρυπτογραφικό κλειδί του payload με τον ίδιο τρόπο που γίνεται και στο Main Key Exchange.

Explicit Key Exchange

Το Explicit Key Exchange (EKE) χρησιμοποιείται από το NCC για να παραδώσει ένα προκαθορισμένο session key στο ST. Το session key κρυπτογραφείται με ένα προσωρινό κλειδί που προκύπτει από την τιμή cookie και χρησιμοποιείται για την ασφάλεια περιεχομένου που χρησιμοποιείται στη διαδικασία payload της ροής δεδομένων.

Η παράδοση πραγματοποιείται από το NCC στέλνοντας ένα μήνυμα που περιέχει ένα τυχαίο nonce string, το nonce1 κι ένα byte string, κρυπτογραφημένου κλειδιού, το οποίο έχει το ίδιο μέγεθος με το κλειδί που χρησιμοποιείται για την κρυπτογράφηση του payload. Το ST ανταποκρίνεται με ένα μήνυμα που περιέχει ένα τυχαίο nonce string, το nonce2 και μια παράμετρο πιστοποίησης, την auth. Η τιμή της auth υπολογίζεται με τον

ίδιο τρόπο όπως και στο Main Key Exchange και μπορεί να χρησιμοποιηθεί για να βεβαιώσει την ταυτότητα του ST. Τόσο το NCC όσο και το ST υπολογίζουν ένα προσωρινό κοινόχρηστο μυστικό string, το temp:

temp = H (cookie ~ (unsigned char)4, nonce1)

το οποίο χρησιμοποιείται για να δημιουργήσει τμήματα σε ένα προσωρινό κλειδί, με τον ίδιο τρόπο που γίνεται και στο Main Key Exchange. Το NCC χρησιμοποιεί αυτό το string των τμημάτων του προσωρινού κλειδιού σε μία XOR με ένα session key για να αποκτήσει τη τιμή του κρυπτογραφημένου κλειδιού και το ST εκτελεί μια δεύτερη XOR για να αποκρυπτογραφήσει τη τιμή του session key.

2.3.3. Διαχείριση IPSec

Το IP Security (IPSec) παρέχει εμπιστευτικότητα, ακεραιότητα, έλεγχο πρόσβασης και πιστοποίηση της πηγής στα IP datagrams. Αυτές οι υπηρεσίες παρέχονται διατηρώντας μία κοινόχρηστη κατάσταση μεταξύ της πηγής και της καταβόθρας ενός IP datagram. Η κατάσταση αυτή καθορίζει εκτός των άλλων, τις συγκεκριμένες υπηρεσίες που παρέχονται στο datagram, ποιοί κρυπτογραφικοί αλγόριθμοι θα χρησιμοποιηθούν για την παροχή των υπηρεσιών και τα κλειδιά που θα έχουν ως είσοδο οι κρυπτογραφικοί αλγόριθμοι. Η εδραίωση αυτής της κοινόχρηστης κατάστασης με χειροκίνητο τρόπο δεν κλιμακώνεται καλά και για το λόγο αυτό χρειάζεται ένα πρωτόκολλο.

Για unicast κίνηση το IPSec Key Management Protocol καλείται Internet Key Exchange (IKE). Το IKE έχει αναπτυχθεί για να διασφαλίσει πως όταν δύο μέλη επιθυμούν να επικοινωνήσουν με ασφάλεια μπορούν να συμφωνήσουν για όλες τις απαραίτητες πληροφορίες με έναν ασφαλή τρόπο ακόμα κι αν δεν έχουν επικοινωνήσει ποτέ ξανά. Ένα δομικό στοιχείο είναι το Internet Security Association και Key Management Protocol (ISAKMP) (RFC 2408 [43]). Το ISAKMP καθορίζει τις διαδικασίες και τη μορφή των πακέτων για να καθιερώσει, να διαπραγματευθεί, να τροποποιήσει και διαγράψει το Security Association (SA). Δε δεσμεύεται για κανένα κρυπτογραφικό αλγόριθμο, καμιά τεχνική παραγωγής κλειδιών ή ανταλλαγής κλειδιών. Το ISAKMP είναι σχεδιασμένο έτσι ώστε να είναι ανεξάρτητο της ανταλλαγής κλειδιών και να μπορεί να υποστηρίξει διάφορα πρωτόκολλα ανταλλαγής κλειδιών. Το προσχέδιο του Internet Key Exchange (IKE) περιγράφει ένα συγκεκριμένο πρωτόκολλο ανταλλαγής κλειδιών.

Το IKE είναι το πρωτόκολλο, που εκτελεί αμοιβαία πιστοποίηση κι εδραιώνει τους συνδέσμους ασφαλείας (SAs) για το IPSec. Η βάση του πρωτοκόλλου για τη πρώτη μορφή του IKE τεκμηριώθηκε στα RFCs 2407 [44], 2408 [43] και 2409 [45]. Ο σκοπός του IKE είναι να διαπραγματευθεί και να παρέχει τα πιστοποιημένα κρυπτογραφημένα

δεδομένα (keying material) για τους συνδέσμους ασφαλείας με ένα προστατευμένο τρόπο. Μπορεί να χρησιμοποιηθεί για να διαπραγματευθεί Virtual Private Network (VPNs) κι επίσης για να παρέχει σε ένα απομακρυσμένο χρήστη ενός απομακρυσμένου site (του οποίου η διεύθυνση IP δε χρειάζεται να είναι γνωστή εκ των προτέρων) πρόσβαση σε ένα ασφαλές host ή δίκτυο. Υποστηρίζεται επίσης η διαπραγμάτευση πελάτη. Η λειτουργία πελάτη τίθεται όταν τα διαπραγματευτικά μέρη δεν είναι τελικά σημεία για κάθε διαπραγμάτευση συνδέσμου ασφαλείας συμβαίνει. Όταν χρησιμοποιείται με λειτουργία πελάτη, οι ταυτότητες των τελικών μερών παραμένουν μυστικές.

Περαιτέρω, το IKE ενσωματώνει ένα μηχανισμό που αποτρέπει τις επιθέσεις άρνησης παροχής υπηρεσιών κατά τις οποίες οι servers πλημμυρίζουν από ψευδή αιτήματα μηνυμάτων. Ο στόχος του επιτιθέμενου που διαπράττει αυτές τις απειλές, είναι να κρατήσει ένα server απασχολημένο με την επιβεβαίωση ενός μεγάλου αριθμού ψευδών αιτημάτων με σκοπό να προκαλέσει υπερβολική χρήση της CPU και συνεπώς να υποβαθμίσει την υπηρεσία που παρέχεται από το server στους νόμιμους χρήστες. Ο μηχανισμός του IKE για την αποτροπή αυτών των επιθέσεων βασίζεται στην τεχνική anti-clogging. Η αρχή λειτουργίας του anti-clogging είναι η εκτέλεση της ανταλλαγής ενός ζεύγους από "cookies" στην αρχή της κάθε σύνδεσης μεταξύ πελάτη και server πριν από την έναρξη οποιασδήποτε επαλήθευσης πόρων. Η αρχική ανταλλαγή παρέχει μια αδύναμη πιστοποίηση κι επιτρέπει την επιβεβαίωση της παρουσίας του πελάτη στην διεκδικούμενη διεύθυνση IP παρεμποδίζοντας έτσι τις προσπάθειες για πλημμύρισμα χρησιμοποιώντας ψευδείς διευθύνσεις IP από ένα μοναδικό host. Ο υπολογισμός του cookie από τον server βασίζεται σε μια απλή συνάρτηση κατακερματισμού (hash function) απαιτώντας χαμηλή χρήση της CPU, σε αντίθεση με την ισχυρή πιστοποίηση που χρειάζεται έντονη χρήση της CPU και τις λειτουργίες της παραγωγής κλειδιών, και καμία δέσμευση πόρων δεν χρειάζεται πριν από την ολοκλήρωση της επιτυχημένης ανταλλαγής του cookie.

Το IKE πολλές φορές καλείται και IKEv1 κι οι εφαρμογές του ενσωματώνουν πρόσθετη λειτουργικότητα συμπεριλαμβανομένων πολύπλοκων χαρακτηριστικών για τη Network Address Translation (NAT) διάσχιση, πιστοποίηση κι απόκτηση της απομακρυσμένης διεύθυνσης, που δεν καταγράφονται στα βασικά κείμενα. Μια νέα έκδοση του IKE έχει οριστικοποιηθεί από το IPSec WG στο IETF. Ο στόχος της προδιαγραφής του IKEv2 είναι να ορίσει όλη αυτή τη λειτουργικότητα σε ένα έγγραφο, όπως επίσης και να απλοποιήσει και να βελτιώσει το πρωτόκολλο και να διορθώσει διάφορα προβλήματα του IKEv1 τα οποία βρέθηκαν κατά την ανάπτυξη ή την ανάλυση του. Το IKEv2 διατηρεί τα περισσότερα χαρακτηριστικά του αρχικού IKE, μεταξύ των οποίων είναι η απόκρυψη της ταυτότητας, η τέλεια προώθηση της μυστικότητας, δύο φάσεις και την κρυπτογραφική διαπραγμάτευση, ενώ σε μεγάλο βαθμό επανασχεδιάζει το πρωτόκολλο σχετικά με την αποτελεσματικότητα, την ασφάλεια, την ευρωστία και την ευελιξία του.

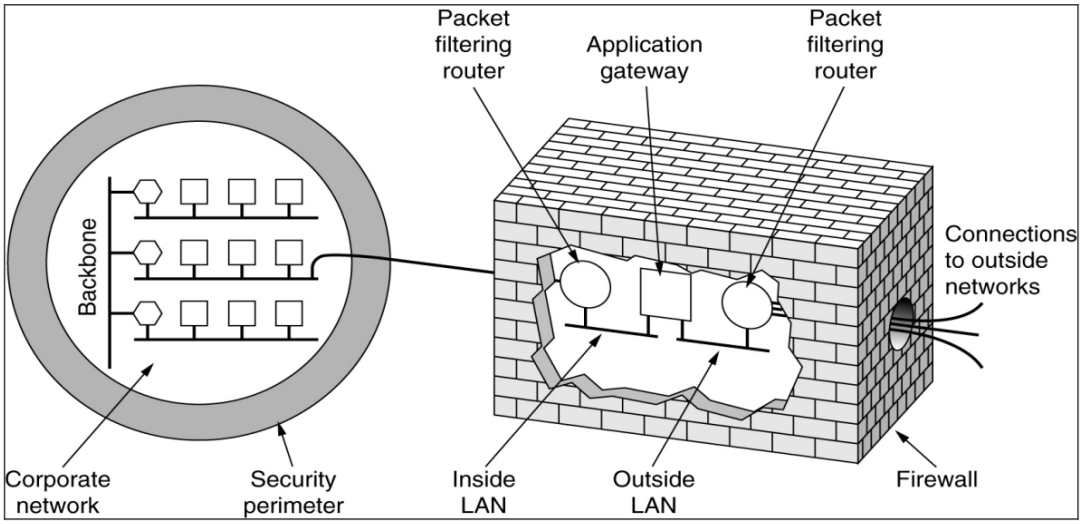
2.3.4. Έλεγχος πρόσβασης

Λειτουργικά ο έλεγχος πρόσβασης μπορεί να χωριστεί σε δύο διαφορετικά θέματα: Το πρώτο θέμα είναι η προστασία της συστάδας από πιο χαλαρά παρεχόμενα μηχανήματα που βρίσκονται κρυμμένα πίσω από τους hackers. Η λύση βρίσκεται σε μια αφιερωμένη μηχανή πύλης με ξεχωριστές προφυλάξεις ασφαλείας, που χρησιμοποιείται για να εξυπηρετήσει το εξωτερικό δίκτυο, ειδικά το Internet, συνδέσεις και γραμμές εισερχομένων κλήσεων. Αυτό καλείται τοίχος προστασίας (Firewall).

Το δεύτερο ζήτημα περιορίζεται σε πιο προηγμένα δορυφορικά συστήματα, όπου κυριαρχούν δορυφόροι με αυξανόμενης επεξεργασίας ευθύνες. Αυτό καλείται προστασία χωρητικότητας και περιγράφεται στην παράγραφο 2.4.5.2. Επίσης θέματα πρωτοκόλλων που σχετίζονται με την αίτηση/ εκχώρηση εύρους ζώνης παρουσιάζονται στην παράγραφο 2.4.5.3.

2.3.4.1. Firewalls

Τα Firewalls είναι ένα βασικό μέσο παροχής ασφάλειας στο δίκτυο, που λειτουργούν όπως μία τάφρος γύρω από ένα μεσαιωνικό κάστρο (βλέπε Σχήμα 32). Τα Firewalls περιορίζουν την είσοδο και την έξοδο πληροφορίας σε προσεκτικά ελεγχόμενα σημεία κι αποτρέπουν μη αποδεκτές προσπάθειες για πρόσβαση στους πόρους μέσα από το τοίχος προστασίας. Παρόλο που μια σημαντική χρήση των Firewalls είναι η ενεργοποίηση της ασφαλούς πρόσβασης στο Internet από εταιρικά δίκτυα, χρησιμοποιούνται επίσης για να περιορίσουν την πρόσβαση σε ιδιωτικές και κρίσιμες πληροφορίες.



Σχήμα 32: *Προστασία με firewall από μη αξιόπιστα δίκτυα*

Τα Firewalls δεν είναι η λύση για όλα τα προβλήματα σχετικά με την ασφάλεια που αντιμετωπίζει ένας οργανισμός. Τα ίδια τα Firewalls είναι ευάλωτα σε παραβιάσεις ασφαλείας. Γενικά ένα Firewall μπορεί να εκτελέσει τα παρακάτω:

- Το φιλτράρισμα των πακέτων είναι μία από τις βασικές λειτουργίες που εκτελείται από ένα Firewall. Αυτή είναι η λειτουργία κατά την οποία επιτρέπεται σε συγκεκριμένα πακέτα και datagrams να περάσουν μέσα από το τοίχος προστασίας, ενώ σε άλλα όχι. Το φιλτράρισμα μπορεί να γίνεται:
  I. Στην πηγή της διεύθυνσης IP,
  II. στον προορισμό της διεύθυνσης IP,
  III. στον αριθμό της θύρας TCP ή UDP της πηγής,
  IV. στον αριθμό της θύρας TCP ή UDP του προορισμού,
  V. στον αριθμό (ID) του πρωτοκόλλου IP.

- Το Network Address Translations (NAT) μεταφράζει τις εσωτερικές ή ιδιωτικές διευθύνσεις IP σε δημόσιες διευθύνσεις IP ή σε διευθύνσεις IP που μπορούν να δρομολογηθούν σε παγκόσμιο επίπεδο. Αυτή η μετάφραση επιτρέπει στους χρήστες να μπορούν να κρύβουν τις δικές τους εσωτερικές διευθύνσεις δικτύου και να μπορο΄πυν όμως να επικοινωνούν με δίκτυα που χρησιμοποιούν δημόσιες διευθύνσεις IP.
- Την ασφάλεια IP (IPSec) όπως περιγράφηκε στα προηγούμενα.
- Οι proxy servers ή οι εφαρμογές των firewalls είναι κάποιοι τρόποι για να υπάρχουν περισσότερα από ένα Firewall στα οποία κάποια από τα φιλτραρίσματα εκτελούνται σε αυτό που αναφέρεται ως proxy firewall ή εφαρμογή gateway. Για παράδειγμα όλα τα πακέτα TELNET και FTP ενός συγκεκριμένου host (server προορισμού) σε ένα μη αξιόπιστο δίκτυο περνάνε από την εφαρμογή gateway μόνο αν είναι συμβατά με τη λίστα ελέγχου πρόσβασης του Firewall. Με αυτό τον τρόπο, η πηγή της εφαρμογής TELNET/ FTP (για παράδειγμα ο απομακρυσμένος πελάτης που συνδέεται σε ένα μη αξιόπιστο δίκτυο) δεν συνδέεται ποτέ απευθείας με τον server προορισμού.

2.3.4.2. Ασφάλεια χωρητικότητας σε ένα αναγεννητικό δορυφορικό σύστημα

Τα αναγεννητικά δορυφορικά συστήματα με εκτεταμένη ενσωματωμένη επεξεργασία και πολύπλοκο οικοδόμημα μεταγωγέων που υποστηρίζουν την τοπολογία πλέγματος με ένα μεγάλο αριθμό δεσμών κεραιών κι ενδο-δορυφορικές ζεύξεις μοιράζονται μια ανησυχία σχετικά με την ασφάλεια άγνωστη σε συμβατικά κι απλούστερα σχέδια δορυφορικών συστημάτων. Μέσα στη δομή της οικογένειας BSM αυτά σχηματίζουν την αναγεννητική δορυφορική οικογένεια πλέγματος (RSM) των δορυφορικών συστημάτων.

Τοποθετώντας τη λειτουργία του εύρους ζώνης ανάλογα με τη ζήτηση (Bandwidth in Demand – BoD) πάνω στο δορυφόρο επιτυγχάνεται η μείωση της καθυστέρησης που σχετίζεται με αναθέσεις πόρων στην άνω ζεύξη. Το ST απαιτεί εύρος ζώνης και το

δίκτυο ικανοποιεί το αίτημα από το πηγάδι των διαθέσιμων πόρων κι έτσι συμβαίνουν τουλάχιστον δύο καθυστερήσεις μετ' επιστροφής (round trip delays) στο συμβατικό σύστημα αλλά μόνο μία τέτοια καθυστέρηση όταν η επεξεργασία είναι ενσωματωμένη. Πάρα ταύτα, ο δορυφόρος έχει περιορισμένη δυνατότητα επεξεργασίας και περιορισμένη χωρητικότητα σε μνήμη και δεν μπορεί να έχει πρόσβαση στην πληροφορία της ST εγγραφής ή στις συμφωνίες σε επίπεδο υπηρεσίας όταν επεξεργάζεται τα αιτήματα για εύρος ζώνης και δεν μπορεί να αποθηκεύσει τη χωρητικότητα χρήσης δεδομένων. Από την άλλη πλευρά, το κεντρικό σημείο (hub) έχει πλήρη πρόσβαση σε όλες τις πληροφορίες των συνδρομητών και μπορεί να καταγράψει όλη τη χρήση πληροφορίας αν τα αιτήματα BoD επεξεργάζονται σε αυτό το σημείο.

Το πρόβλημα επιδεινώνεται από την τοπολογία πλέγματος των RSM δορυφορικών συστημάτων με εκατοντάδες στενές δέσμες. Αφού τα δεδομένα του χρήστη μπορούν να ρέουν με μια αναπήδηση μεταξύ οποιωνδήποτε δύο STs κι όχι μέσα από ένα κομβικό σημείο, όπως στην περίπτωση της τοπολογίας αστέρα, το κομβικό σημείο ή το Κέντρο Ελέγχου των Λειτουργιών του Δικτύου (Network Operations Control Centre – NOCC) δεν μπορεί να δει τις ροές των δεδομένων χρήστη και δεν μπορεί να καταγράψει τη χρήση δεδομένων. Αυτό μπορεί να είναι ένα βάρος για τους πόρους του δορυφόρου, να απαιτεί δηλαδή από το δορυφόρο να καταγράφει τη χρήση της πληροφορίας.

Η προστασία της χωρητικότητας είναι ο μηχανισμός ασφάλειας που είναι υπεύθυνος για όλες τις πτυχές της προστασίας της δορυφορικής χωρητικότητας από κακή χρήση. Είναι ειδικά υπεύθυνη για την προστασία από τις επόμενες ST παραβιάσεις:

- Εκπομπή σε μη εξουσιοδοτημένα slots ή συχνότητες
- Εκπομπή με πλαστές ταυτότητες πηγής (Source IDs)
- Μίμηση άλλου ST
- Πρόσβαση σε μη εξουσιοδοτημένες υπηρεσίες
- Πρόσβαση στις δέσμες της κάτω ζεύξης και στις ενδο-δορυφορικές ζεύξεις χωρίς εξουσιοδότηση
- Μικρότερη αναφορά της χρήσης του
- Υπέρβαση της εξουσιοδοτημένης χρήσης.

Η προστασία χωρητικότητας πρέπει να είναι αρκετά ισχυρή έτσι ώστε μια απάτη να μην είναι οικονομικά αποτελεσματική. Αυτό σημαίνει πως μια υπηρεσία που λαμβάνεται μέσω απάτης πρέπει να κοστίζει λιγότερο από το κόστος της διαπέρασης της ασφάλειας του συστήματος.

Μια συγκεντρωτική και πολύ απλή λύση για την ασφάλεια της χωρητικότητας δουλεύει πολύ καλά σε τοπολογία αστέρα όπου η λειτουργία BoD εκτελείται στο κομβικό σημείο αφού όλα τα αιτήματα έρχονται μέσω του κομβικού αυτού σημείου κι όλη η κίνηση των δεδομένων του χρήστη ρέει μέσα στο κομβικό σημείο. Μια κατανεμημένη και σχετικά πιο πολύπλοκη λύση για τη ασφάλεια της χωρητικότητα προτιμάται στην τοπολογία πλέγματος κι όταν η BoD εκτελείται πάνω στο δορυφόρο.

2.3.4.2.1. Προβλήματα, κίνδυνοι κι απειλές

Από την άποψη της ασφάλειας το δορυφορικό σύστημα είναι για πολλούς λόγους παρόμοιο με τα παλιότερα, ασύρματα, δημόσια δίκτυα. Όλα αυτά τα δίκτυα έχουν απαιτήσεις για να προστατευθούν έναντι της μη εξουσιοδοτημένης χρήσης. Το σύστημα πρέπει να είναι προστατευμένο έναντι της μεταφοράς κυκλοφορίας είτε από μη εξουσιοδοτημένα STs, που μεταφέρουν κυκλοφορία η οποία με κάποιους τρόπους υπερβαίνει τα εξουσιοδοτημένα όρια του Set είτε από STs με τέτοιο τρόπο ώστε ο πραγματικός τελικός χρήστης δε χρεώνεται για τη χρήση.

Τα δορυφορικά συστήματα RSM διαφέρουν από τα προηγούμενα ασύρματα, δημόσια δίκτυα υπό την έννοια πως είναι ένα δίκτυο με μοναδική αναπήδηση και πακέτα μεταγωγής των οποίων οι πόροι βρίσκονται στο διάστημα κι είναι υπερβολικά περιορισμένοι. Χωρίς ειδικά μέτρα, ένα μη εξουσιοδοτημένο ST μπορεί εύκολα να χρησιμοποιήσει το σύστημα απλά εκπέμποντας πακέτα μέσα από τα TDMA slots στον μεταγωγέα από όπου δρομολογούνται για τον επιθυμητό προορισμό, ενδεχομένως χωρίς να το γνωρίζει το NOCC. Ένα ST το οποίο εκπέμπει με υψηλότερη από την κανονική ισχύ πρέπει να είναι σε θέση να εκπέμπει μέσω οποιωνδήποτε TDMA slots και να υπερπηδά τα STs στα οποία έχουν κατανεμηθεί τα slots.

2.3.4.2.2. Εξάρτηση σε άλλους μηχανισμούς ασφάλειας

Η προστασία χωρητικότητας εξαρτάται από τρεις άλλους μηχανισμούς ασφαλείας:

I. Ασφάλεια στο κομμάτι του διαστήματος
II. Ασφάλεια στο ST
III. Ασφάλεια σηματοδότησης

Η ασφάλεια στο κομμάτι του διαστήματος είναι υπεύθυνη για την προστασία του payload έναντι της μη εξουσιοδοτημένης πρόσβασης. Είναι επίσης υπεύθυνη για την προστασία του δορυφορικού διαύλου έναντι της μη εξουσιοδοτημένης πρόσβασης όπως είναι οι επικοινωνίες Telemetry Tracking and Command (TT & C).

Η προστασία χωρητικότητας εξαρτάται από την ασφάλεια στο κομμάτι του διαστήματος υπό την έννοια πως το κομμάτι του διαστήματος μπορεί να λάβει από το NOCC το υλικό κωδικοποίησης που χρειάζεται για να εφαρμόσει το κομμάτι του στην προστασία της χωρητικότητας. Η ασφάλεια στο κομμάτι του διαστήματος παρέχει προστασία στο υλικό κωδικοποίησης κατά τη διάρκεια της εκπομπής στο payload.

Οι μηχανισμοί της ασφάλειας στο κομμάτι του διαστήματος εφαρμόζονται με συμβατικούς τρόπους κι είναι εσωτερικοί στα κομμάτια του διαστήματος και του NOCC αντίστοιχα. Η ασφάλεια στο κομμάτι του διαστήματος δεν εμπίπτει στο πεδίο μελέτης αυτής της εργασίας.

Η ασφάλεια στο ST είναι υπεύθυνη για την προστασία ενός ST έναντι οποιασδήποτε με εξουσιοδοτημένης χρήσης.

Η προστασία της χωρητικότητας εξαρτάται από την ασφάλεια στο ST υπό την έννοια πως το παραποιημένο λογισμικό του ST παρέχει κάποια περιορισμένη ικανότητα για να υπερβεί την εξουσιοδοτημένη χωρητικότητα παρακάμπτοντας το λογισμικό ST που επιβάλλεται για τον έλεγχο της εισόδου, τη διαχείριση της ενέργειας στην άνω ζεύξη κι άλλες πολιτικές για τον περιορισμό της χωρητικότητας.

Η προστασία χωρητικότητας εξαρτάται από την ασφάλεια στο ST σε μεγαλύτερο βαθμό υπό την έννοια πως ένα παραβιασμένο ST επιτρέπει κάποιες παραβιάσεις στην ασφάλεια οι οποίες ανιχνεύονται μόνο μέσω του ελέγχου της χρήσης.

Η ασφάλεια της σηματοδότησης είναι υπεύθυνη για:

I. Το κομμάτι της ασφάλειας ενός Set που εισέρχεται στο σύστημα, δηλαδή την εγγραφή ST.
II. Την παροχή ιδιωτικότητας και tamper resistance για τη διαχείριση των επικοινωνιών του δικτύου μεταξύ του NOCC και του ST.
III. Την ασφαλή διανομή του υλικού κωδικοποίησης της προστασίας χωρητικότητας στα STs.

Η προστασία χωρητικότητας εξαρτάται από την ασφάλεια σηματοδότησης για την ασφαλή διανομή του κάθε υλικού κωδικοποίησης στα STs.

2.3.4.3. Ζητήματα σχετικά με το πρωτόκολλο προστασίας της χωρητικότητας

Το υπόλοιπο αυτής της παραγράφου περιγράφει την ασφάλεια χωρητικότητας από την άποψη:

- της πιστοποίησης των πακέτων – πως ένας δορυφόρος πιστοποιεί την κυκλοφορία των πακέτων που λαμβάνονται από τα STs στα κανάλια κυκλοφορίας και πως ο δορυφόρος αποφασίζει αν επιτρέπεται η ζητούμενη δρομολόγηση ή μεταγωγή.
- Των αιτημάτων για εύρος ζώνης – πως ο δορυφόρος πιστοποιεί ένα αίτημα για εύρος ζώνης.

- Των χορηγήσεων εύρους ζώνης – πως ένας δορυφόρος πιστοποιεί μια χορήγηση εύρους ζώνης.

2.3.4.3.1. Πιστοποίηση των πακέτων

Η πιστοποίηση των πακέτων κι ο έλεγχος των αλγορίθμων:

- Πρέπει να ελαχιστοποιούν τους απαιτούμενους δορυφορικούς πόρους για την εκτέλεση του ελέγχου
- Δεν πρέπει να απαιτούν άκαμπτο συγχρονισμό διανομής κλειδιών.
- Πρέπει να παρέχουν υλικό κωδικοποίησης στο ST που μπορεί να χρησιμοποιηθεί για να πιστοποιήσει τη ταυτότητα του ST, περιορίζοντας τη ζημιά που μπορεί να προκληθεί στο σύστημα από ένα παραβιασμένο ST.
- Πρεπει να παρέχουν μηχανισμούς εκπομπής σύμφωνα με τους οποίους ένα μη καταχωρημένο ή μη εξουσιοδοτημένο ST ή ένα ST που δεν έχει έγκυρα κλειδιά να μπορεί να έχει πρόσβαση στο NOCC για τις λειτουργίες διαχείρισης, όπως είναι η εγγραφή, το αίτημα για τις πληροφορίες του συστήματος ή η διανομή του κλειδιού ασφαλείας μέσα από το δορυφόρο.
- Πρέπει να στηρίζουν την ικανότητα του συστήματος για την ενδυνάμωση των περιορισμών στο payload του εύρους ζώνης όπως είναι ο έλεγχος ροής, οι μετρήσεις της ποιότητας υπηρεσιών κι η συμφόρηση των πολιτικών διαχείρισης.
- Πρέπει να επιτρέπουν ενδυνάμωση της πιστοποίησης, κάτι που περιορίζει τη χρήση πόρων του ST μόνο για συγκεκριμένους σκοπούς.
- Το NOCC θα πρέπει να είναι σε θέση να ελέγχει την πρόσβαση στο ST στους ακόλουθους πόρους:

    - εκπομπή που φέρει κυκλοφορία μέσω ανταγωνισμού των καναλιών
    - ειδικές δέσμες κάτω ζεύξης (γεωγραφικές, παγκόσμιες, κτλ που μπορεί να χρησιμοποιούν μεγαλύτερη ενέργεια δορυφορικής εκπομπής) και πόρους
    - multicast εκπομπή, για παράδειγμα πρόσβαση στους πόρους αντιγραφής των δορυφορικών πακέτων
    - εκπομπή Διαδορυφορικών Ζεύξεων (Inter-Satellite Link - ISL)
    - ειδικές ομάδες καναλιών, για παράδειγμα οι πόροι της άνω ζεύξης που προορίζονται για χρήση από μια υποομάδα των STs ή των χρηστών (συχνότητες ή χρονικά slots).

2.3.4.3.2. Αιτήματα εύρους ζώνης

Τυπικά, όταν το υπόστρωμα Ελέγχου Πρόσβασης Μέσου (Medium Access Control – MAC) έχει πακέτα να μεταδώσει, στέλνει ένα αίτημα εύρους ζώνης στο δίκτυο. Αν το αίτημα εύρους ζώνης επεξεργάζεται στο HUB ή το NOCC τότε το αίτημα αυτό μπορεί εύκολα να συγκριθεί με οποιοδήποτε SLA ή οποιαδήποτε πληροφορία του συνδρομητή κι ανάλογα θα χορηγείται ή θα απορρίπτεται. Η απάτη ή κακή χρήση μπορεί εύκολα να

εντοπιστεί. Όταν η λειτουργία BoD μετακινείται στο δορυφόρο, δεν είναι χρήσιμη η πρόσβαση στην πληροφορία του συνδρομητή. Για το λόγο αυτό, απαιτείται ένας διαφορετικός μηχανισμός αιτήματος εύρους ζώνης.

Ο μηχανισμός αιτήματος εύρους ζώνης πρέπει να είναι σε θέση να απορρίπτει αιτήματα εύρους ζώνης τα οποία παραβιάζουν ένα SLA ή μια συνδρομή του ST. Ο μηχανισμός πρέπει επίσης να προστατεύει το δορυφόρο από πολλά αιτήματα εύρους ζώνης προερχόμενα από ένα ή μια μικρή ομάδα ST. Αφού το αρχικό αίτημα εύρους ζώνης πιθανότατα θα χρησιμοποιήσει ανταγωνισμό καναλιών, ο μηχανισμός αιτήματος εύρους ζώνης πρέπει να περιορίσει τη πρόσβαση σε αυτούς τους πόρους. Ένας αλγόριθμος προστασίας του αιτήματος εύρους ζώνης παρέχει ένα μηχανισμό που επιτρέπει το ST να εγκρίνει κάθε αίτημα εύρους ζώνης πριν μεταδοθεί στο δορυφόρο. Ο αλγόριθμος πρέπει να παρέχει στο δορυφόρο τα μέσα για την πιστοποίηση των αιτημάτων έτσι ώστε να διασφαλίσει πως δε θα παραβιαστούν μετά την έγκριση. Ο αλγόριθμος πρέπει να είναι σχεδιασμένος να είναι αρκετά ισχυρός κι αρκετά ευέλικτος για να υποστηρίζει μεγάλο εύρος σχεδίων της προστασίας της χωρητικότητας κι αλγορίθμους για εύρος ζώνης ανάλογα με τη ζήτηση για όλα τη διάρκεια ζωής του συστήματος.

2.3.4.3.3. Ανάθεση εύρους ζώνης

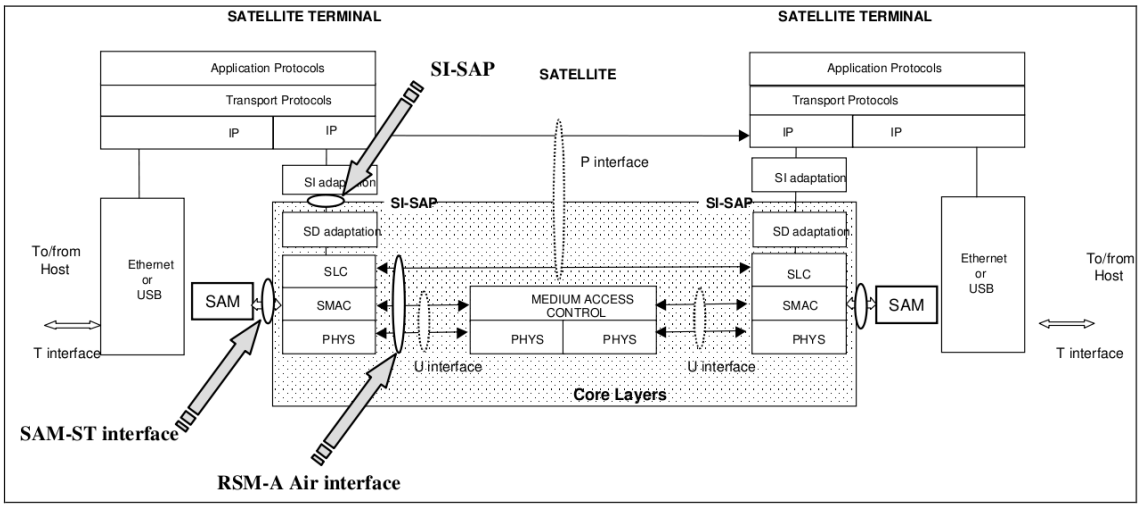
Μέσα στο μηχανισμό ασφαλείας για την προστασία της χωρητικότητας, το ST πρέπει να είναι σε θέση να πιστοποιεί τις αναθέσεις εύρους ζώνης που λαμβάνονται από το payload. Για να συμβεί αυτό, το ST πρέπει να μπορεί να βεβαιώνει πως η συγκεκριμένη ανάθεση εύρους ζώνης (συμπεριλαμβανομένου του αριθμού πλαισίου για το οποίο ισχύει η ανάθεση) λήφθηκε χωρίς να παραποιηθεί από το payload.

Οι αλγόριθμοι που χρησιμοποιούνται για να επιτευχθεί αυτό πρέπει να ελαχιστοποιούν τους απαιτούμενους πόρους του δορυφόρου, όπως είναι η ενέργεια, η επεξεργασία και η μνήμη.

2.3.4.4. Η λύση RSM-A

Το SAM είναι ένα στοιχείο ασφάλειας του δορυφορικού τερματικού. Φυσικώς είναι ένα ολοκληρωμένο κύκλωμα ενσωματωμένο στο τερματικό. Το SAM περιλαμβάνει μυστικό υλικό κωδικοποίησης και πιστοποιεί κάθε πακέτο Αναγεννητικού Δορυφορικού Πλέγματος(Regenerative Satellite Mesh), τύπου Α (RSM – A) που στέλνεται έξω από το τερματικό παράγοντας ένα πεδίο ελέγχου πρόσβασης (Access Control Field – ACF), το οποίο μπορεί να επιβεβαιωθεί από άλλα εξουσιοδοτημένα στοιχεία του συστήματος. Το SAM θα υπογράψει μόνο εκείνα τα αιτήματα που είναι έγκυρα με βάση τις πολιτικές που καθορίζονται για το συγκεκριμένο ST. Από την πλευρά της λήψης, βεβαιώνει πως

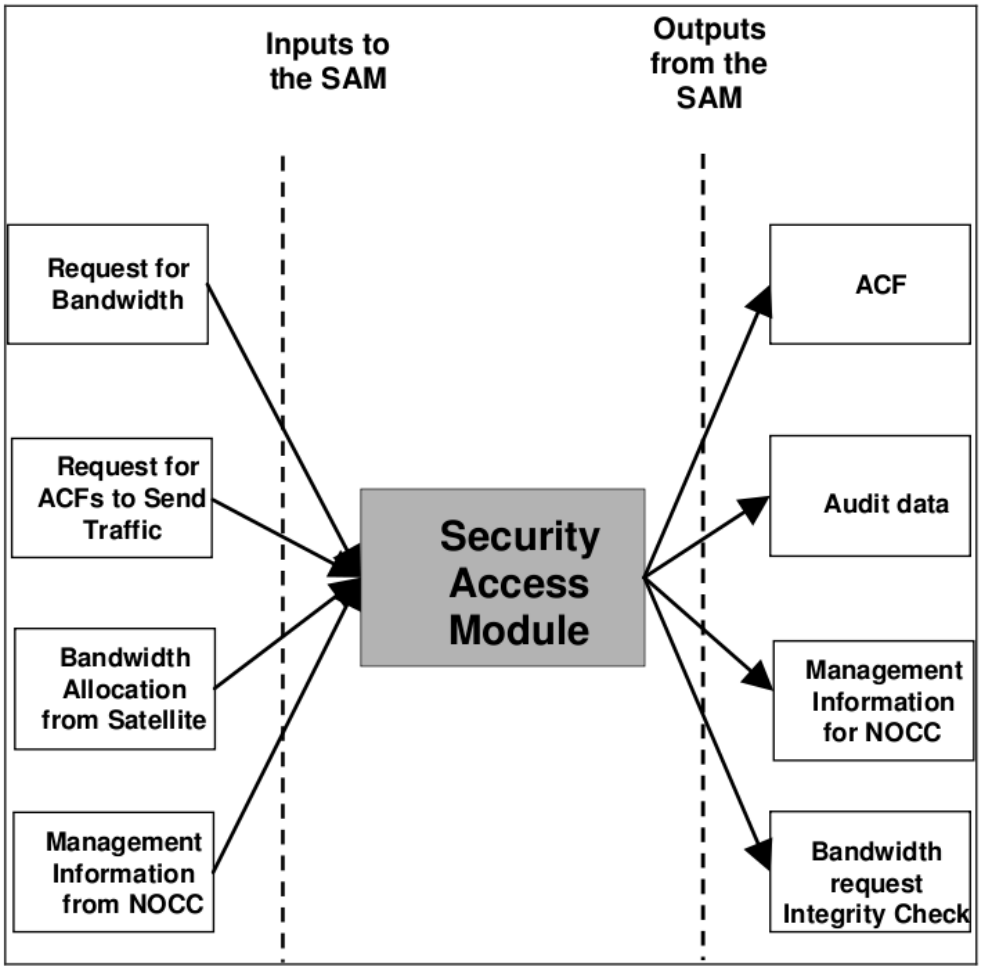
τα μηνύματα διαχείρισης είναι αυθεντικά μηνύματα προερχόμενα από το NOCC. Το σύστημα αυτό περιγράφεται στο TS 102 189-3 [49] και φαίνεται στα Σχήματα 33 και 34.



Σχήμα 33: *Πρωτόκολλο αρχιτεκτονικής και διεπαφή SAM-ST*

Οι περιοχές του SAM της ευθύνης του συστήματος RSM-A είναι οι ακόλουθες:

- πιστοποίηση
- προστασία εξουσιοδότησης
- καταχώρηση
- έλεγχος χρήσης.



Σχήμα 34: *Αλληλεπιδράσεις μεταξύ του SAM και του ST σχετικά με τις λειτουργίες ασφάλειας*

Μια σημαντική λειτουργικότητα για το SAM είναι η επιβεβαίωση του αιτήματος εύρους ζώνης. Το ST απαιτεί εύρος ζώνης από το δορυφόρο βασιζόμενο στις πολιτικές που υπέγραψε κι έλαβε από το NOCC κατά τη διάρκεια της διαδικασίας καταχώρησης. Το SAM διασφαλίζει πως το ST εμμένει σε αυτές τις πολιτικές κι έτσι δε θα υπογράψει αιτήματα που δεν είναι μέσα στα όρια αυτών των οδηγιών. Το SAM θα εγκρίνει αιτήματα που συμφωνούν με την πολιτική απαγορεύοντας στο ST να στείλει κάποιο μήνυμα στο δορυφόρο απαιτώντας διανομή εύρους ζώνης. Το SAM θα επιστρέψει ένα κώδικα Ελέγχου της Ακεραιότητας (Integrity Check) μαζί με το μήνυμα ανταπόκρισης στο αίτημα εύρους ζώνης αν δεν επιτρέπεται στο ST να απαιτήσει εύρος ζώνης. Το SAM θα επιστρέψει επίσης ένα μήνυμα αποτυχία του αιτήματος για εύρος ζώνης στο ST με κώδικα αποτυχίας αν το SAM απορρίψει το αίτημα του ST για εύρος ζώνης. Το ST δεν απαιτεί εύρος ζώνης από το δορυφόρο χωρίς ένα έγκυρο κώδικα ακεραιότητας από το SAM.

Επίσης το SAM επικοινωνεί με κάποια μηνύματα διαχείρισης με το NOCC μέχρι και το ST. Αυτά τα μηνύματα τυπικά είναι διαφανή στο ST κι είναι πάντα κρυπτογραφημένα από το SAM. Το NOCC στέλνει μηνύματα στο SAM μέσω του ST κι αυτά τα μηνύματα είναι επίσης πάντα κρυπτογραφημένα. Το ST θα αφαιρέσει την επικεφαλίδα ST-SAM

από αυτά τα μηνύματα που λαμβάνονται από το SAM και προορίζονται για το NOCC. Το ST θα προσθέσει επικεφαλίδες UDP/ IP κι επικεφαλίδες πρωτοκόλλου διαχείρισης όπως απαιτείται.

2.3.5. Επιλογές διαχείρισης κλειδιών για τα συστήματα BSM

Όπως παρουσιάστηκε στις παραγράφους 2.3.1. έως 2.3.4., οι λύσεις για τη διαχείριση της ασφάλειας και του ελέγχου πρόσβασης εξαρτώνται από τα επίπεδα στα οποία εφαρμόζεται η ασφάλεια.

Το IPsec και η σχετικές με αυτό αρχιτεκτονικές unicast και multicast διαχείρισης/ διανομής κλειδιών είναι αρκετά κατάλληλα για εφαρμογή στα δίκτυα BSM.

Ο έλεγχος πρόσβασης του δορυφορικού τερματικού με τη χρήση ενός σχεδίου όπως είναι το SAM είναι άλλο ένα κατάλληλο εργαλείο που αποτρέπει τη πρόσβαση σε μη εξουσιοδοτημένους χρήστες.

Όταν χρησιμοποιούνται τα συστήματα DVB-RCS και DVB-S τότε ένας συνδυασμός της ασφάλειας IPSec και DVB-S CA ή DVB-RCS μπορεί να εφαρμοστεί για να καλύψει όλες τις πλευρές των απαιτήσεων ασφαλείας του δορυφόρου και της ασφάλειας end-to-end.

2.4. Προτεινόμενες προδιαγραφές που προέρχονται από το ETSI

2.4.1. Συζήτηση

Στο προηγούμενο κεφάλαιο παρουσιάστηκαν οι γενικές απειλές κατά του δικτύου BSM, των παρόχων υπηρεσιών και των χρηστών με μια ανάλυση των απαιτούμενων υπηρεσιών ασφαλείας για την αποτροπή αυτών των απειλών. Επίσης στην παράγραφο 2.2. δόθηκε μια επισκόπηση των επιλογών για λύσεις ασφαλείας που είναι διαθέσιμες για τα δίκτυα BSM στη στοίβα πρωτοκόλλου σε σύγκριση με τα πλεονεκτήματα των λύσεων για την ασφάλεια end-to-end και ασφάλεια δορυφόρου. Επιπρόσθετα, στην παράγραφο 2.3. παρουσιάστηκαν διάφορες λύσεις στα πιο δύσκολα προβλήματα στην ασφάλεια, όπως είναι η διαχείριση της ασφάλειας κι ο έλεγχος πρόσβασης. Οι λύσεις της διαχείρισης ασφάλειας συμπεριλαμβάνουν τις επιλογές multicast, DVB-S (broadcast), DVB-RCS (διαδραστικός δορυφόρος) και το IPSec.

Το IPsec και η σχετικές με αυτό αρχιτεκτονικές unicast και multicast διαχείρισης/ διανομής κλειδιών είναι αρκετά κατάλληλα για εφαρμογή στα δίκτυα BSM κι αυτή η λύση εφαρμόζεται κυρίως στο ανεξάρτητο του δορυφόρου (Satellite Independent – SI)

κομμάτι της στοίβας πρωτοκόλλου. Κάποιες από τις επιλογές διαχείρισης της ασφάλειας BSM σχετίζονται με τη ασφάλεια των συνδέσεων unicast και one-to-one. Πάρα ταύτα, ένα μεγάλο κομμάτι της ασφάλειας σχετίζεται με το multicast και broadcast. Η διαδικασία της ασφάλειας και της εκτέλεσης της διαχείρισης των κλειδιών για multicast και broadcast είναι πολύ πιο πολύπλοκη σε σχέση με το unicast. Η παράγραφος 2.3.4. εισήγαγε κάποιους παράγοντες που επηρεάζουν το σχεδιασμό της ομάδας συστήματος ασφαλείας για τα BSM. Παραδείγματα αυτών των παραγόντων είναι οι εφαρμογές multicast, η δυναμική της ομάδας, η επεκτασιμότητα και το μοντέλο της υποκείμενης εμπιστοσύνης, Ο συνδυασμός κάποιων από αυτούς τους παράγοντες θα είναι ο αποφασιστικός παράγοντας για τις παραμέτρους της πολιτικής ασφαλείας, όπως είναι:

- οι διαδικασίες για την ίδρυση, τη λειτουργία και την περάτωση της ομάδας
- οι μέθοδοι διανομής κλειδιών. Για παράδειγμα, το σύστημα διανομής επίπεδου κλειδιού ή LKH μπορεί να επιλεγεί για να καλύψει τις απαιτήσεις της ομάδας
- η ισχύς των απαιτούμενων κρυπτογραφικών αλγορίθμων και των ψηφιακών υπογραφών, όπως είναι η χρήση του DES, του τριπλού DES ή του AES για ιδιωτικότητα και των συστημάτων υπογραφής RSA ή DSS
- τι πρέπει να γίνει όταν κάτι πάει λάθος: όπως είναι η αποτυχία του δικτύου, οι επιθέσεις DoS, τα προβλήματα με την οντότητα πιστοποίησης κι εξουσιοδότησης. Οι διαδικασίες συνήθως καθορίζονται από την πολιτική ασφαλείας. Πρέπει να υπάρχει ξεκάθαρος τρόπος για τη δημιουργία, τη διάδοση και την ενδυνάμωση των πολιτικών ασφαλείας.

Οι παράγοντες αυτοί, επίσης, επηρεάζουν την επιλογή του πρωτοκόλλου διαχείρισης κλειδιών όπως είναι το GDOI, το FMKE, το GSAKMP ή το MIKEY, όπως παρουσιάστηκαν στην παράγραφο 2.4.4.

Για υπηρεσίες broadcasting η ιδιαίτερη προσοχή στις απαιτήσεις ασφαλείας και στις ρυθμίσεις του δικτύου θα είναι ο αποφασιστικός παράγοντας για την επιλογή των συστημάτων διαχείρισης της ασφάλειας, όπως είναι το DVB-S CA, το DVB-RCS ή το IPSec και τα σχετικά πρωτόκολλα διαχείρισης της ομάδας.

Ο έλεγχος πρόσβασης του δορυφορικού δικτύου, που παρουσιάστηκε στην παράγραφο 2.3.4., επικεντρώνεται σε δύο τύπους συστημάτων: ο ένας είναι το τοίχος προστασίας (firewall) κι ο άλλος ένα ολοκληρωμένο κύκλωμα ή έξυπνη κάρτα, όπως είναι το SAM. Τα firewalls κυρίως προστατεύουν το ιδιωτικό δίκτυο από εξωτερικές επιθέσεις, Τα ολοκληρωμένα κυκλώματα ή οι έξυπνες κάρτες προφυλάσσουν από εσωτερικές επιθέσεις ή από κακή χρήση, όπου τα θέματα σχετικά με την προστασία της χωρητικότητας περιγράφηκαν στην παράγραφο 2.3.4.2. και τα ζητήματα πρωτοκόλλου που σχετίζονται με το αίτημα/ ανάθεση εύρους ζώνης παρουσιάστηκαν στην παράγραφο 2.3.4.3. Έτσι, ο έλεγχος πρόσβασης θα παίξει ένα κύριο ρόλο στην κάλυψη κάποιων απαιτήσεων ασφαλείας για πολλές υπηρεσίες πάνω στα δίκτυα BSM.

Υπάρχουν επίσης κι άλλα ζητήματα που πρέπει να ληφθούν υπόψη κατά την εφαρμογή ενός συστήματος ασφαλείας για τα δίκτυα BSM, όπως είναι:

- η διαφάνεια: όπως είναι η λεπτομερής αναφορά των συνθηκών κάτω από τις οποίες το IPSec μπορεί να υποστηριχθεί με διαφάνεια στα δίκτυα BSM. Επίσης η ασφάλεια σε επίπεδο εφαρμογής μπορεί να λειτουργήσει με διαφάνεια πάνω στα δίκτυα BSM όπως το σχέδιο DRM που αναφέρθηκε στην παράγραφο 2.3.4.2.
- η DVB-S πρόσβαση υπό συνθήκη: κριτική εξέταση της DVB-S πρόσβαση υπό συνθήκη και της χρησιμότητας της για της υπηρεσίες BSM
- οι λύσεις ασφαλείας multicast: κριτική ανάλυση των λύσεων ασφαλείας multicast στην ομάδα IETF Multicast SECurity (MSEC) και της συσχετιζόμενης αρχιτεκτονικής διανομής κλειδιού προτείνοντας μερικές διακριτές λύσεις για τα δίκτυα BSM
- τα χαρακτηριστικά της ασφάλειας: τα προτεινόμενα χαρακτηριστικά της ασφάλειας που παρέχονται από τα συστήματα BSM, για παράδειγμα τα χαρακτηριστικά που παρέχονται σε επίπεδο σύνδεσης, επίπεδο δικτύου, κτλ.
- η πολιτική ασφάλειας: καθορισμός της πολιτικής ασφαλείας BSM για συγκεκριμένες απειλές (όπως είναι η άρνηση παροχής υπηρεσιών, η μεταμφίεση κι οι επιθέσεις επανάληψης του μηνύματος)
- η αλληλεπίδραση μεταξύ των στρωμάτων: η αντιστοιχία μεταξύ των λειτουργιών διαχείρισης της ασφάλειας και των χαμηλότερων στρωμάτων όπως είναι σχέση της multicast διαχείρισης ασφάλειας και του IPSec (επίπεδο IP), του DVB-S, του DVB-RCS (επίπεδο σύνδεσης, όπως το MPEG-TS).

2.4.2. Διαχειριστής ασφάλειας BSM (BSM Security Manager – BSM – SM)

Από τις προηγούμενες παραγράφους προκύπτει εύκολα πως για τη διατήρηση της ασφάλειας και την αξιολόγηση της απόδοσης της ιδιωτικότητας/ ακεραιότητας των δεδομένων των BSM στον κόσμο του Internet, υπάρχει η ανάγκη για κάποιον "διαχειριστή". Η στοίβα πρωτοκόλλου από το BSM οδηγεί την ανάπτυξη του BSM Security Manager (BSM-SM). Ο "διαχειριστής" βρίσκεται πάνω από το σημείο πρόσβασης υπηρεσίας (SAP) και καθορίζει πω τα πρωτόκολλα IP και τα πακέτα ασφαλίζονται μέσα από το BSM, όπου τα πρωτόκολλα Satellite Independent (SI) χρησιμοποιούνται και το τρόπο με τον οποίο με τη σειρά τους προκαλούν τις λειτουργίες Satellite Dependent (SD).

Ο BSM-SM πρέπει να έχει την ευελιξία να υποστηρίζει διάφορους τύπους χειριστών BSM από ένα πάροχο εύρους ζώνης μέχρι ένα χειριστή δικτύου. Τοποθετείται τόσο στην είσοδο όσο και την έξοδο του BSM κι έχει εφαρμογή ST καθώς κι εφαρμογές NCC. Για το λόγο αυτό, ο BSM-SM μπορεί να περιγραφεί ως ένας "έξυπνος" διαχειριστής που επιβλέπει τις διαδικασίες ασφάλειας με αναφορά στις πολιτικές ασφαλείας και τις διαδικασίες ελέγχου πρόσβασης.

Η διαχείριση της ασφάλειας μπορεί να κυμαίνεται από την "αδιαφορία' (για παράδειγμα πλήρης διαφάνεια) μέχρι τις πλήρεις ικανότητες για τη διαχείριση της ασφάλειας και της

πολιτικής. Έτσι η αρχιτεκτονική του BSM-SM πρέπει να είναι σπονδυλωτή και πλήρως αναβαθμίσιμη. Επίσης, εξαιτίας της φύσης του BSM, ο διαχειριστής ασφάλειας μπορεί να χρειάζεται να αλληλεπιδρά με διαφορετικά επίπεδα της στοίβας OSI. Ο BSM-SM πρέπει να είναι σχεδιασμένος ως αυτόνομος, στην πραγματικότητα όμως σχετίζεται με άλλες οντότητες ελέγχου και διαχείρισης του BSM. Έτσι η εφαρμογή του βασίζεται πάνω στη λειτουργική μονάδα και στις εδραιωμένες επικοινωνίες.

Ο BSM-SM έχει πολλά κοινά στοιχεία με τις λειτουργίες διαχείρισης ασφάλειας IPSec και MSEC, όπως είναι η unicast διαχείριση κλειδιών, η ίδρυση/ διατήρηση/ απομάκρυνση της multicast ομάδας κι η multicast διανομή κλειδιού της ομάδας. Πάρα ταύτα, ο BSM-SM μπορεί να έχει κάποιες συγκεκριμένες λειτουργίες έτσι ώστε να ικανοποιεί τις απαιτήσεις των υπηρεσιών BSM. Για παράδειγμα, αν χρησιμοποιείται το SAM για τον έλεγχο πρόσβασης, τότε πρέπει να καθορίζονται οι αλληλεπιδράσεις μεταξύ του BSM-SM και του SAM. Επίσης όταν επιλέγεται η ασφάλεια σε επίπεδο σύνδεσης (όπως είναι οι συστάσεις ασφαλείας DVB-RCS) τότε ο BSM-SM αλληλεπιδρά μέσω του SAP με χαμηλότερα στρώματα. Μια επισκόπηση της αρχιτεκτονικής αυτού του συστήματος περιγράφεται στο [36] και φαίνεται στο Σχήμα 3. Ο BSM-SM μπορεί να επικοινωνεί με διαφορετικά επίπεδα της στοίβας BSM.

2.4.3. Προτεινόμενη ασφάλεια TSs

Στο Σχήμα 35 παρουσιάζεται η δομή των προτεινόμενων τεχνικών προδιαγραφών (TSs), που διαχωρίζονται σε multicast και unicast. Όλες οι προτεινόμενες TSs έχουν τα εξής χαρακτηριστικά:

- τη χρήση ανοιχτών προδιαγραφών: όπου είναι απαραίτητο οι προτεινόμενες TSs βασίζονται στις διαθέσιμες ανοιχτές προδιαγραφές (για παράδειγμα τα προϊόντα των ομάδων IETF MSEC και IPSec)
- όλες οι προδιαγραφές πρέπει να βρίσκονται στα ανεξάρτητα του δορυφόρου επίπεδα και πρέπει να είναι ανεξάρτητες από τις ιδιαιτερότητες των εξαρτώμενων από το δορυφόρο χαμηλότερων επιπέδων ανάλογα με την περίπτωση
- όλες οι προδιαγραφές πρέπει να διασυνεργάζονται με τις λειτουργίες IP.

Στα επόμενα ακολουθεί μια σύντομη παρουσίαση όλων των προτεινόμενων TSs:

- TS1: Γενική αρχιτεκτονική ασφαλείας: Αυτή η προδιαγραφή καλύπτει την αρχιτεκτονική του διαχειριστή ασφαλείας, όπως περιγράφηκε λεπτομερώς στην παράγραφο 2.4.2., βασισμένη στην αρχιτεκτονική BSM [2]. Η αρχιτεκτονική θα κάνει μια λειτουργική αποσύνθεση δείχνοντας ποιές λειτουργίες τοποθετούνται πάνω και κάτω από το SI-SAP [50]

    ~ TS1.1: Παράμετροι απόδοσης: Αυτή η προδιαγραφή ορίζει ένα συγκεκριμένο σετ παραμέτρων της απόδοσης ασφάλειας BSM που είναι μετρήσιμες στο ST, στην NCC/ πύλη κι από τον πάροχο της υπηρεσίας.

Αυτό βασίζεται στο τρέχον έργο του IETF σχετικά με τις ομάδες IPSec και MSEC. Παραδείγματα τέτοιων παραμέτρων είναι η επεξεργασία των αναγκών ενέργειας για την ασφάλεια, τα επιπλέον έξοδα δεδομένων, ο χρόνος αποκατάστασης από καταστάσεις μικρής/ μεγάλης αποτυχίας, η επιλογή των αλγορίθμων ασφάλειας και τα μέτρα προστασίας έναντι των επιθέσεων άρνησης παροχής υπηρεσιών.

- TS2: Ασφάλεια unicast. Αυτή η προδιαγραφή καλύπτει όλες τις πλευρές της unicast πολιτικής ασφάλειας για το χειρισμό των δεδομένων και την ανταλλαγή κι αποθήκευση κλειδιών.

  ~ TS2.1: Πολιτικές unicast ασφαλείας. Αυτή η προδιαγραφή καλύπτει πτυχές της πολιτικής στο πλαίσιο της unicast ασφάλειας, λαμβάνοντας υπόψη το γεγονός πως τέτοιες πολιτικές μπορεί να εκφράζονται με διαφορετικούς τρόπους και μπορεί να υπάρχουν για διαφορετικά επίπεδα σε δεδομένη αρχιτεκτονική unicast ασφάλειας
  ~ TS2.2: Unicast χειρισμός δεδομένων. Αυτή η προδιαγραφή καλύπτει τις σχετικές με την ασφάλεια μεταχειρίσεις των unicast δεδομένων από τον αποστολέα κι από τον παραλήπτη όπως είναι η κρυπτογράφηση/ αποκρυπτογράφηση των δεδομένων κι η επιβεβαίωση των ψηφιακών υπογραφών

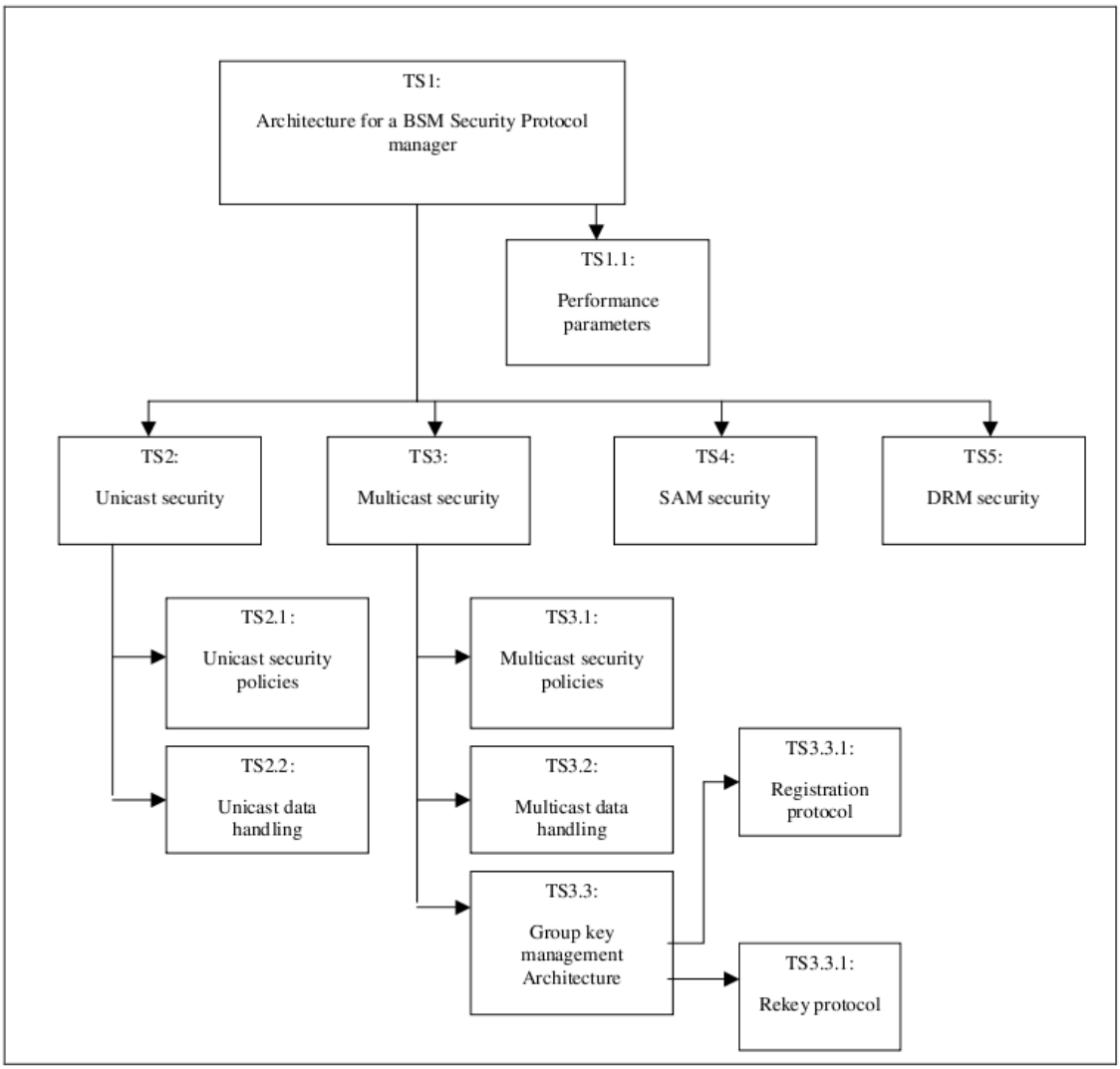
- TS3: Ασφάλεια multicast. Η προδιαγραφή αυτή παρέχει μια επισκόπηση κι αιτιολογία της αρχιτεκτονικής multicast ασφάλειας που χρησιμοποιείται για μικρές και μεγάλες multicast ομάδες. Καθορίζει το πλαίσιο αναφοράς της multicast ασφάλειας και τις υπηρεσίες ασφάλειας που μπορεί να είναι μέρος της ασφαλούς multicast λύσης

  ~ TS3.1: Πολιτικές multicast ασφάλειας. Αυτή η προδιαγραφή καλύπτει πτυχές της πολιτικής στο πλαίσιο της multicast ασφάλειας, λαμβάνοντας υπόψη το γεγονός πως τέτοιες πολιτικές μπορεί να εκφράζονται με διαφορετικούς τρόπους και μπορεί να υπάρχουν για διαφορετικά επίπεδα σε δεδομένη αρχιτεκτονική multicast ασφάλειας
  ~ TS3.2: Multicast χειρισμός δεδομένων. Αυτή η προδιαγραφή καλύπτει τις σχετικές με την ασφάλεια μεταχειρίσεις των multicast δεδομένων από τον αποστολέα κι από τον παραλήπτη όπως είναι η κρυπτογράφηση/ αποκρυπτογράφηση των δεδομένων κι η επιβεβαίωση των ψηφιακών υπογραφών
  ~ TS3.3: Διαχείριση ομαδικού κλειδιού. Αυτή η προδιαγραφή ασχολείται με την ασφαλή διανομή κι ανανέωση του υλικού κωδικοποίησης

    ° TS3.3.1: Πρωτόκολλο καταχώρησης. Αυτό είναι ένα πρωτόκολλο για την αμοιβαία πιστοποίηση μεταξύ του group controller/ key server κι ενός νέου μέλους της ομάδας
    ° TS3.3.2: Πρωτόκολλο rekey. Είναι ένας μηχανισμός που χρησιμοποιείται από το group controller/ key server για να ανανεώσει περιοδικά ή να αλλάξει το Σύνδεσμο Ασφαλείας (Security Association – SA) των δεδομένων στέλνοντας πληροφορίες rekey στα μέλη της ομάδας. Τα μηνύματα rekey

μπορεί να προέρχονται από αλλαγές στις συμμετοχές της ομάδας, αλλαγές στην πολιτική ασφαλείας της ομάδας, τη δημιουργία νέων κλειδιών για την προστασία της κυκλοφορίας ή από τη λήξη του κλειδιού

- TS4: Ασφάλεια της προστασίας της χωρητικότητας: η προδιαγραφή αυτή καλύπτει τον συνεκτικό έλεγχο πρόσβασης και την ασφαλή αίτηση/ εκχώρηση εύρους ζώνης στα δορυφορικά τερματικά
- TS5: Ασφάλεια DRM. Τα DRMs (Digital Rights Management – Διαχείριση Ψηφιακών Δικαιωμάτων) είναι συστήματα ασφαλείας στο επίπεδο της εφαρμογής. Η προδιαγραφή αυτή καλύπτει θέματα σχετικά με την αλληλεπίδραση μεταξύ του BSM-Security Manager και του DRM.



Σχήμα 35: *Προτεινόμενες Τεχνικές Προδιαγραφές*

3. Η Δυναμική Διαχείριση Κλειδών σε Ασφαλή Δορυφορικά Κανάλια Επιλεγμένης Εκπομπής.

3.1. Εισαγωγή

Τα ευρυζωνικά δορυφορικά δίκτυα που βασίζονται στο Internet Protocol (IP) έχουν τη δυνατότητα να προσφέρουν τις multicast υπηρεσίες με ικανοποιητικό κόστος. Πάρα ταύτα, οι δορυφόροι παρουσιάζουν κάποιες σημαντικές προκλήσεις ασφάλειας.

- Η υποκλοπή κι η ενεργή εισβολή είναι πολύ πιο εύκολες σε σχέση με τα επίγεια ή κινητά δίκτυα εξαιτίας της ευρυζωνικότητας των δορυφόρων.
- Τα δορυφορικά συστήματα έχουν περιορισμένους πόρους, συγκεκριμένα σε περιοχές με περιορισμένη ισχύ εκπομπής (κι έτσι χωρητικότητα καναλιού), και περιορισμένη ικανότητα επεξεργασίας και μεταγωγής για δορυφόρους με ενσωματωμένο σύστημα επεξεργασίας.
- Τα δορυφορικά κανάλια έχουν υψηλό ρυθμό λαθών ανά bit (BER), το οποίο έχει ως αποτέλεσμα σε απώλεια πακέτων κι σε απώλεια του συγχρονισμού της ασφάλειας.

Τα συστήματα ασφάλειας για τα δορυφορικά δεδομένα πρέπει, για τους παραπάνω λόγους, να βελτιστοποιούνται λαμβάνοντας υπόψη αυτούς τους περιορισμούς και συγκεκριμένα την ανάγκη για εμπιστευτικότητα και την απαίτηση να χρησιμοποιούνται οι δορυφορικοί πόροι αποτελεσματικά. Οι γεωστατικοί δορυφόροι υποφέρουν επίσης από μεγάλη καθυστέρηση διάδοσης κι ως εκ τούτου τα δορυφορικά συστήματα πρέπει να προσθέτουν μικρές καθυστερήσεις στην κυκλοφορία.

Στο κεφάλαιο αυτό θεωρούμε την επεκτασιμότητα των multicast υπηρεσιών ασφάλειας, εστιάζοντας σε θέματα σχετικά με την εμπιστευτικότητα στις δορυφορικές ζεύξεις, ελαχιστοποιώντας παράλληλα τη χρήση των δορυφορικών πόρων. Ένα συγκεκριμένο ζήτημα στη διασφάλιση των multicast συνδέσεων είναι αυτό της διαχείρισης κλειδιού, το οποίο χρειάζεται να κλιμακώνεται αποτελεσματικά, ιδιαίτερα εξαιτίας του μεγάλου αριθμού των multicast αποδεκτών (ενδεχομένως της τάξης των εκατομμυρίων) που

αναμένονται στα δορυφορικά δίκτυα. Προτείνεται, στο κεφάλαιο αυτό, ένας αριθμός κλιμακωτών προσεγγίσεων και συγκεκριμένα αναλύεται λεπτομερώς η Λογική Ιεραρχία Κλειδιών (Logical Key Hierarchy – LKH).

Οι λειτουργικές μονάδες ενίσχυσης απόδοσης (PEMs) χρησιμοποιούνται για να ενισχύσουν την απόδοση των δορυφορικών ζεύξεων. Ένας τύπος PEM είναι ο proxy ενίσχυσης απόδοσης (Performance Enhancing Proxy – PEP) [22], που χρησιμοποιείται για να βελτιώσει την απόδοση των πρωτοκόλλων στα μονοπάτια του δικτύου όπως είναι οι δορυφορικές ή οι ασύρματες ζεύξεις, όπου η τοπική απόδοση υποφέρει εξαιτίας των χαρακτηριστικών της ζεύξης ή του υποδικτύου. Οι PEMs συνήθως θεωρούνται στο πλαίσιο της ροής κυκλοφορίας του πρωτοκόλλου ελέγχου της unicast μετάδοσης (TCP), αλλά ισχύουν και για multicast κυκλοφορία. Για παράδειγμα, μια multicast ροή ήχου μπορεί να μεταδοθεί χρησιμοποιώντας το πρωτόκολλο μετάδοσης σε πραγματικό χρόνο (RTP) πάνω στο πρωτόκολλο datagram του χρήστη (UDP): Αφού το περιεχόμενο δεδομένων του κάθε πακέτου είναι μικρό, η μετάδοση μπορεί να αυξηθεί αποτελεσματικά με τη χρήση των PEMs για να συμπιεστεί η επικεφαλίδα στη δορυφορική ζεύξη. Άλλο ένα παράδειγμα είναι η εφαρμογή των μηχανισμών της Πρόσθιας Διόρθωσης Σφαλμάτων (FEC) στα PEMs για να μειωθεί ο ρυθμός λαθών της δορυφορικής ζεύξης για το multicast κανάλι. Οι PEMs γενικά διαβάζουν κι αλλάζουν το περιεχόμενο της επικεφαλίδας στο επίπεδο μεταφοράς κι έτσι μπορούν να χρησιμοποιηθούν συνήθως μόνο όταν η επικεφαλίδα δεν είναι κρυπτογραφημένη. Για το λόγο αυτό, οι μηχανισμοί ασφάλειας στο επίπεδο δικτύου, όπως είναι το Internet Protocol Security (IPSec), που κρυπτογραφούν ολόκληρο το πακέτο στο επίπεδο μεταφοράς δεν είναι συμβατοί με τη χρήση αυτών των PEMs σε επικοινωνίες που βασίζονται σε δορυφόρους: Το IPSec κρύβει όλες τις λεπτομέρειες των πρωτοκόλλων των ανώτερων επιπέδων και κάνει εφικτό σε κάθε ενδιάμεσο κόμβο να μπορεί να επεξεργαστεί αυτή την πληροφορία. Συνεπώς, κάθε υπηρεσία που απαιτεί να γνωρίζει το περιεχόμενο της επικεφαλίδας σε επίπεδο μεταφοράς οπουδήποτε αλλού πέρα του τελικού host δεν μπορεί να λειτουργήσει αν τα πακέτα IP είναι κρυπτογραφημένα.

Στο κεφάλαιο αυτό θεωρούμε τη διαχείριση κλειδιών και συγκεκριμένα τα κόστη του κύκλου ζωής της διανομής κλειδιού. Λαμβάνουμε υπόψη όχι μόνο το κόστος της επανακρυπτογράφησης όταν οι χρήστες εισέρχονται ή εγκαταλείπουν μια εδραιωμένη ομάδα, αλλά θεωρούμε επίσης, τα κόστη κατασκευής ενός δέντρου κατά τη διάρκεια

της αρχικοποίησης μιας multicast ομάδας. Δείχνουμε για το LKH πως η προεγγραφή του χρήστη κι η περιοδική είσοδος μειώνουν το κόστος της αρχικοποίησης και πως ο βέλτιστος βαθμός εξόδου (outdegree) ενός ιεραρχικού δέντρου ποικίλει ανάλογα με την αναμενόμενη μεταβλητότητα των χρηστών και τον παράγοντα επανακρυπτογράφησης. Άλλες εργασίες [51] δείχνουν πως όταν η επανακρυπτογράφηση συμβαίνει μετά την είσοδο ή την αναχώρηση, το κατώτερο όριο στη χειρότερη περίπτωση κόστους της ανανέωσης του κλειδιού είναι μια λογαριθμική μεταβολή με συμμετοχή N στην ομάδα. Στην εργασία αυτή, από την άλλη πλευρά, σύμφωνα με την παρούσα λογαριθμική συνάρτηση, δείχνεται πως η βέλτιστη τιμή του βαθμού εξόδου (outdegree) k του δέντρου ποικίλει ανάλογα με την αναμενόμενη συχνότητα επανακρυπτογράφησης, λαμβάνοντας υπόψη τόσο το κόστος της αρχικής κατασκευής του δέντρου όσο και το κόστος της επανακρυπτογράφησης μέσα στη διάρκεια ζωής της multicast ομάδας. Σε άλλη εργασία [52], ο βέλτιστος αριθμός των κλειδιών που έχουν ανατεθεί σε κάθε μέλος της ομάδας σχετίζεται με την πιθανότητα διαγραφής του μεμονωμένου μέλους. Εδώ, υποθέτουμε πως κάθε μέλος είναι εξίσου πιθανό να εισέλθει ή να εγκαταλείψει την ομάδα, δεδομένου πως το δέντρο έχει ίσους αριθμούς κλειδιών για κάθε μέλος.

Όπως περιγράφθηκε παραπάνω, οι PEMs μπορεί να μην είναι συμβατοί με τα συστήματα ασφάλειας end-to-end και να παρουσιάζουν συγκεκριμένο πρόβλημα για τα δορυφορικά συστήματα. Το IPSec σε πολλαπλά επίπεδα έχει προταθεί σαν μια προσέγγιση που επιτρέπει στις εξουσιοδοτημένες συσκευές του δικτύου την πρόσβαση στις επικεφαλίδες των πακέτων, διατηρώντας ταυτόχρονα την end-to-end ιδιωτικότητα των δεδομένων που μεταφέρονται σε αυτά τα πακέτα. Στην εργασία αυτή, προτείνουμε κι αναλύουμε μια λύση διασυνεργασίας μεταξύ του IPSec σε πολλαπλά επίπεδα (ML-IPSec) και του LKH και δείχνουμε πως η κυκλοφορία της διαχείρισης κλειδιών στις δορυφορικές ζεύξεις μπορεί να μειωθεί περαιτέρω με τη χρήση αυτής της προσέγγισης. Τελικά, λαμβάνεται υπόψη η επίδραση του ML-IPSec και του LKH στο κόστος του κύκλου ζωής.

3.2. Ασφάλεια IP multicast

Στην αρχιτεκτονική BSM το IP multicast είναι ένας αποτελεσματικός τρόπος διανομής δεδομένων από ένα server σε μια ομάδα πελατών. Το IP multicast είναι ένα πρωτόκολλο Internet που ενεργοποιεί τη μετάδοση πακέτων δεδομένων σε μια ομάδα παραληπτών. Το IP multicast κάνει αποτελεσματική τη χρήση του εύρους ζώνης θέτοντας ένα μέσο σημείο μεταξύ της unicast κίνησης (one-to-one) και της broadcast IP κίνησης (one-to-all σε ένα δίκτυο). Αυτό ταιριάζει καλά στη one-to-many ή many-to-many μεταφορά μεγάλων δεδομένων ή στη μετάδοση ροής πολυμέσων (ήχος ή video) σε ένα μεγάλο αριθμό ετερογενών παραληπτών. Το IP multicast υποστηρίζει αυτού του τύπου τη μετάδοση επιτρέποντας στους πόρους να μεταδίδουν ένα μοναδικό αντίγραφο του μηνύματος σε μια ομάδα ενδιαφερομένων παραληπτών.

Το μοντέλο του ανώνυμου παραλήπτη που διέπει το IP multicast είναι ελκυστικό ειδικά διότι το δέντρο διανομής είναι εύκολα επεκτάσιμο, υποκείμενο στους διαθέσιμους πόρους του πρωτοκόλλου δρομολόγησης multicast. Κάθε host σε ένα υποδίκτυο μπορεί να συμμετέχει σε μια ομάδα multicast χωρίς ο δρομολογητής του υποδικτύου να δίνει πληροφορίες ταυτοποίησης για τον host σε άλλους δρομολογητές αντίθετα της ροής του δέντρου διανομής. Αυτό επιτρέπει στο IP multicast να επεκτείνεται σε ένα μεγάλο αριθμό συμμετεχόντων hosts. Η επεκτασιμότητα του δέντρου διανομής στο IP multicast κάνει το μοντέλο IP multicast πολύ ελκυστικό από τη σκοπιά της κλιμάκωσης.

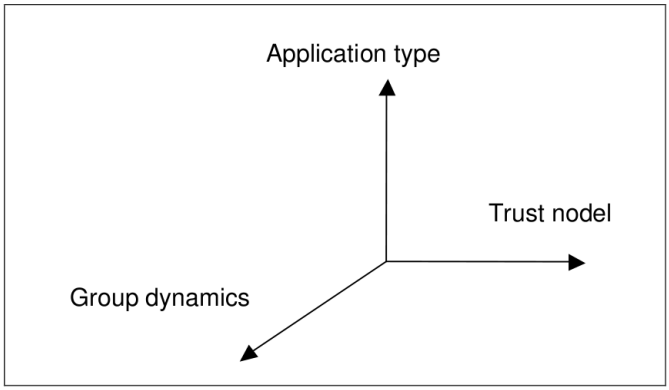
Πάρα ταύτα, από τη σκοπιά της ασφάλειας, πρόσθετοι μηχανισμοί κι υπηρεσίες πρέπει να αναπτυχθούν στην κορυφή του βασικού μοντέλου IP multicast. Αυτή η αποσύνδεση της ασφάλειας από το μοντέλο του IP multicast είναι επωφελής αφού επιτρέπει διαφορετικά μοντέλα κι αρχιτεκτονικές ασφαλείας να αναπτυχθούν χωρίς να επηρεάζουν το δέντρο διανομής multicast που παραδίδει τα multicast δεδομένα end-to-end. Αυτή η αποσύνδεση είναι επίσης σημαντική από τη σκοπιά των εφαρμογών, αφού κάθε εφαρμογή απαιτεί διαφορετική μορφή της πληροφορίας του host κι άλλες παραμέτρους ασφαλείας και μπορεί να αναπτύσσει διάφορους μηχανισμούς ταυτοποίησης και πιστοποίησης του χρήστη. Στο έγγραφο Functional BSM Multicast Architectures [46] ορίζεται η ομάδα διαχείρισης του BSM multicast καθώς κι η δρομολόγηση του multicast. Από τη σκοπιά της ασφάλειας, η ομάδα διαχείρισης και η δρομολόγηση πρέπει να είναι transparent στην ασφάλεια. Έτσι, το μοντέλο της ασφάλειας BSM πρέπει να λειτουργεί με κάθε ομάδα διαχείρισης και κάθε πρωτόκολλο δρομολόγησης.
Όπως φαίνεται στο Σχήμα 36, υπάρχουν αρκετοί αλληλένδετοι παράγοντες ή όψεις του IP multicast που επηρεάζουν τις προσεγγίσεις και τους μηχανισμούς που χρησιμοποιούνται για την ασφάλεια του. Από αυτούς, κάποιοι ευρείς και περισσότερο σχετικοί περιλαμβάνουν:

- Multicast τύπο εφαρμογής
- δυναμική της ομάδας

- θέματα επεκτασιμότητας
- υποκείμενο μοντέλο εμπιστοσύνης.

Ο συνδυασμός αυτών των παραγόντων θα είναι ο αποφασιστικός παράγοντας για τις παραμέτρους της ομάδας πολιτικής ασφάλειας, όπως είναι:

- διαδικασίες για την εγκαθίδρυση, το τρέξιμο και το τερματισμό της ομάδας
- μεθόδους διανομής κλειδιών. Για παράδειγμα το σύστημα διανομής επίπεδου κλειδιού (flat key) ή LKH μπορεί να επιλεγεί για να καλύψει τις απαιτήσεις αυτής της ομάδας. Για εφαρμογές one-to-many με μεγάλες και δυναμικές ομάδες, η πολιτική του rekeying πρέπει να καθορίζεται προσεκτικά έτσι ώστε να μειωθεί το εύρος ζώνης που απαιτείται για την κίνηση του key management.
- ισχυρότητα των κρυπτογραφικών αλγορίθμων και των ψηφιακών υπογραφών που απαιτούνται, όπως είναι η χρήση του DES, τριπλού DES ή του AES για ιδιωτικότητα και RSA ή συστήματα υπογραφής DSS
- τι πρέπει να γίνει όταν κάτι πάει στραβά: όπως είναι η βλάβη του δικτύου, οι επιθέσεις DoS, προβλήματα με την πιστοποίηση κι εξουσιοδότηση της οντότητας. Οι διαδικασίες συνήθως καθορίζονται από την πολιτική ασφαλείας. Πρέπει να υπάρχει ένας ξεκάθαρος τρόπος ή δημιουργία, η διάδοση κι ενδυνάμωση των πολιτικών ασφαλείας.



Σχήμα 36: *Παράγοντες που επηρεάζουν το σχεδιασμό του ασφαλούς συστήματος multicast*

Αναμένεται πως οι ομάδες BSM multicast μπορεί να είναι μεγάλες κι αρκετά δυναμικές. Έτσι είναι σημαντικό να εξεταστούν διάφοροι μέθοδοι για τη διαχείριση της ασφάλειας για τέτοιες μεγάλες ομάδες. Στις επόμενες παραγράφους υπάρχουν δύο ιδέες: η μία είναι η αποτελεσματική αρχιτεκτονική για την ασφάλεια στη διανομή κλειδιών (διάδοση) σε μεγάλες και δυναμικές ομάδες, κι η άλλη ιδέα είναι συστήματα διαχείρισης ασφάλειας που καθορίζουν τους κανονισμούς για την εδραίωση ασφαλών ομάδων, τον έλεγχο των μελών που συμμετέχουν κι εγκαταλείπουν την ομάδα με ασφάλεια.

3.2.1. Κλιμακωτή αρχιτεκτονική διανομής κλειδιού

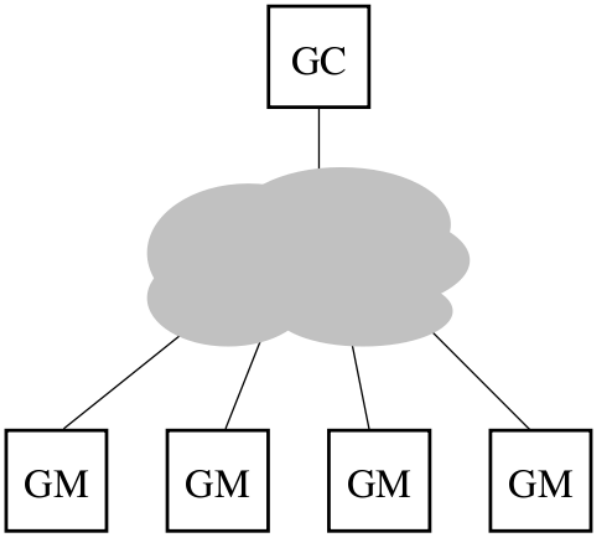
Το Logical Key Hierarchy (LKH) είναι ένας μηχανισμός για την ασφάλεια της διαχείρισης κλειδιών σε μία ομάδα από οντότητες, παρέχοντας τη δυνατότητα να αρχικοποιήσει την ομάδα με ένα κοινό κλειδί κι έπειτα να κάνει rekey ην ομάδα όπως απαιτείται (RFC 2627 [47]). Είναι επομένως συγκεκριμένη εφαρμογή σε ασφαλείς multicast επικοινωνίες. Στο IETF αυτή η αρχιτεκτονική είναι ο προτιμώμενος τρόπος για τη διάδοση του κλειδιού σε μεγάλες ομάδες. Το LKH μπορεί να χρησιμοποιηθεί με οποιοδήποτε από τα πρωτόκολλα διαχείρισης ασφάλειας που αναφέρονται στην επόμενη παράγραφο.

Το LKH απαιτεί δύο τύπους οντοτήτων όπως φαίνεται στο Σχήμα 37: έναν ελεγκτή της ομάδας (Group Controller - GC) κι ένα ή περισσότερα μέλη της ομάδας (Group Members - GMs). Το πρώτο είναι υπεύθυνο για τη δημιουργία και διανομή των κλειδιών και για rekeying (για τη διατήρηση της ασφάλειας) ανάλογα με την περίσταση. Τα Group Members είναι οντότητες που έχουν πρόσβαση στις ομάδες κλειδιών. Για να υποστηρίξει το LKH το GC επικοινωνεί με κάθε GM, αλλά τα GMs δεν χρειάζεται να επικοινωνούν μεταξύ τους. Σε μια ασφαλή multicast επικοινωνία δεν είναι απαραίτητο για το GC να τοποθετείται στο ίδιο μέρος με την πηγή των multicast δεδομένων. Το LKH παρέχει τα εξής πλεονεκτήματα:

- επεκτασιμότητα: οι πόροι που απαιτούνται για τη διαχείριση των κλειδιών μέσα σε μια ομάδα αναπτύσσονται πιο αργά από το μέγεθος της ομάδας, N. Αυτοί οι πόροι περιλαμβάνουν τις απαιτήσεις για τη μετάδοση στο δίκτυο, τη χωρητικότητα GC, τη χωρητικότητα GM, τη προσπάθεια κρυπτογράφησης GC και την προσπάθεια αποκρυπτογράφησης GM.
- Απόδειξη συνεννόησης: καμία ομάδα οντοτήτων δεν μπορεί να αποκτήσει ως σύνολο κάποιο κλειδί εκτός κι αν μια ή περισσότερες από αυτές τις οντότητες το απέκτησε μεμονωμένα.

Το κέρδος του LKH είναι φαινομενικό συγκεκριμένα όταν μια ομάδα χρειάζεται να γίνει rekeyed.

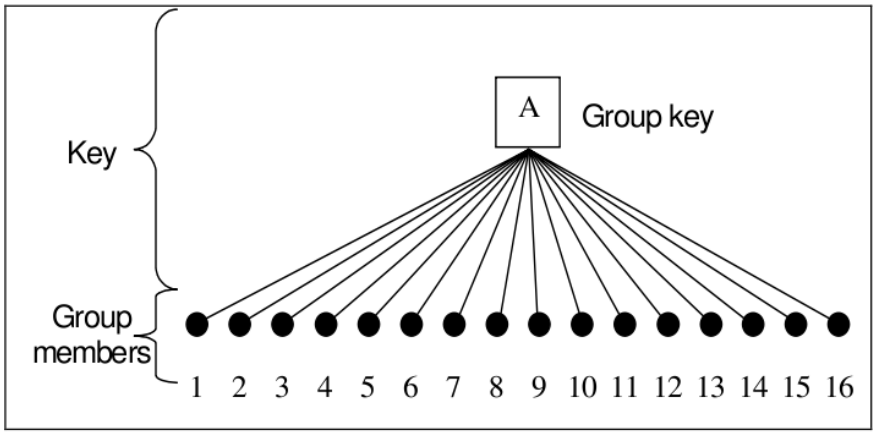
Το LKH δεν ορίζει τους μηχανισμούς για τη μετάδοση των κλειδιών μεταξύ του group controller και των group members: αυτή είναι λειτουργία μιας ομάδας πρωτοκόλλου key management όπως είναι το GSAKMP. Το LKH είναι ανεξάρτητο από οποιοδήποτε αλγόριθμο κρυπτογράφησης ή αποκρυπτογράφησης.



Σχήμα 37: *Λογική δομή της οντότητας LKH*

Κάθε GM θεωρείται πως έχει ένα αρχικό σύνδεσμο ασφαλείας κατά ζεύγη μαζί με το GC, δηλαδή το GM και το GC μοιράζονται ένα μυστικό κλειδί γνωστό μόνο σε αυτές τις δύο οντότητες. Ο μηχανισμός με τον οποίο αυτός ο ασφαλής σύνδεσμος συμβαίνει είναι έξω από το πεδίο έρευνας του LKH, αλλά τυπικά μπορεί να περιλαμβάνει τη χρήση μιας τεχνικής όπως είναι η Diffie-Hellman για να δημιουργήσει ένα κοινόχρηστο μυστικό κλειδί γνωστό μόνο σε αυτά τα δύο μέρη, ή ένα προδιανεμημένο μυστικό ή μια μυστική ανταλλαγή χρησιμοποιώντας το σύστημα του δημόσιου κλειδιού.

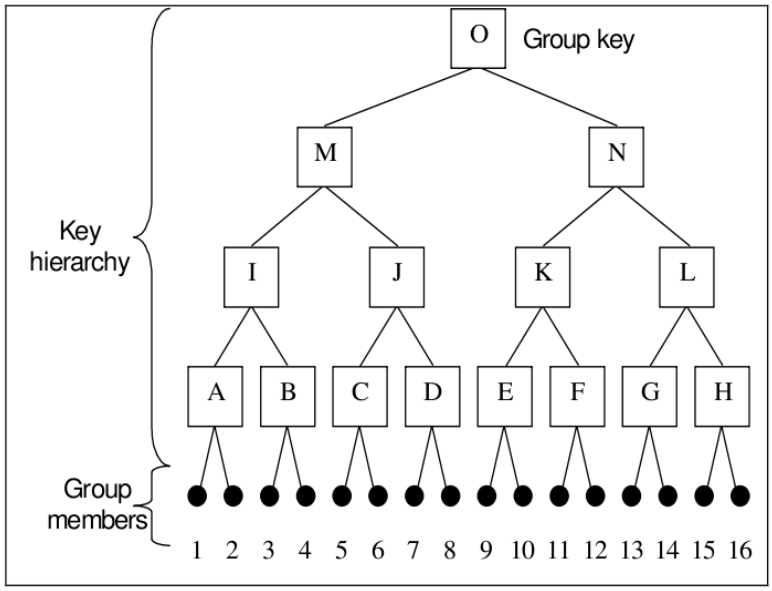
Παρουσιάζουμε το LKH θεωρώντας ένα σύστημα flat key management που μπορεί να χρησιμοποιηθεί για το διαμοιρασμό ενός μοναδικού κλειδιού, "A", έτσι ώστε να είναι γνωστό στο GC και σε όλα τα GMs αλλά όχι σε άλλες οντότητες. Το σύστημα flat key management αποτελείται από N ζεύγη κλειδιών καθένα από τα οποία μοιράζεται μεταξύ του group controller κι ενός από τα N group members (βλέπε επίσης το Σχήμα 38). Κάθε ένα από αυτά τα ζεύγη των ασφαλών συνδέσμων παρουσιάζεται με κύκλο και η ομάδα κλειδών παρουσιάζεται με ένα κουτί με τίτλο "A". Αν η ομάδα κλειδιών αλλάξει η νέα ομάδα κλειδιών πρέπει να κρυπτογραφηθεί με το μοναδικό ζεύγος κλειδιών του κάθε χρήστη και μετά να γίνει unicast σε αυτό το χρήστη. Κάθε ένα από αυτά τα κρυπτογραφημένα κλειδιά παρουσιάζεται με μια γραμμή στο Σχήμα 38. Έτσι για N χρήστες ένας συνολικός αριθμός N κρυπτογραφημένων κλειδιών παράγεται και μεταδίδεται μέσα από το δίκτυο.



Σχήμα 38: *Ιεραρχία κλειδιών: Ν ζεύγη κλειδιών*

Αντιπαραθέτουμε αυτό με το LKH, όπου ένα δέντρο κλειδιών χρησιμοποιείται για το διαμοιρασμό του μοναδικού κλειδιού "Ο" έτσι ώστε να είναι γνωστό στο GC και σε όλα τα GMs αλλά όχι σε άλλες οντότητες. Στο Σχήμα 39 τα κλειδιά έχουν τον τίτλο Α μέχρι Ο, οι κύκλοι και πάλι παριστάνουν τα ζεύγη κλειδιών και η κάθε γραμμή αντιπροσωπεύει τα κρυπτογραφημένα κλειδιά που στέλνονται στο δίκτυο. Ας υποθέσουμε τώρα πως ο Χρήστης 11 χρειάζεται να διαγραφεί από την ομάδα multicast. Τότε όσα κλειδιά κατέχει ο Χρήστης 11 (κλειδιά F, K, N, O) πρέπει να αλλάξουν και να διανεμηθούν στους χρήστες που τα χρειάζονται, χωρίς να επιτρέπεται στον Χρήστη 11 να κατέχει αυτά τα κλειδιά ή σε κάποιον άλλο που δεν έχει το δικαίωμα τους. Για να συμβεί αυτό, πρέπει τα κλειδιά που έχει ο Χρήστης 11 να αντικατασταθούν, προχωρώντας από κάτω προς τα πάνω.

Ο server επιλέγει ένα νέο κλειδί για τον πιο χαμηλό κόμβο (όχι το φύλλο, για το οποίο υπάρχει ένας μοναδικός unicast ασφαλής σύνδεσμος μεταξύ του GC και του GM), μετά μεταδίδει το κλειδί κρυπτογραφημένο με τα κατάλληλα κλειδιά. Έτσι για παράδειγμα, το πρώτο κλειδί που αντικαθίσταται είναι το Κλειδί F, κι αυτό το νέο κλειδί θα σταλεί κρυπτογραφημένο μαζί με το μοναδικό ζεύγος κλειδιών του Χρήστη 12. Το δεύτερο κλειδί που θα αντικατασταθεί είναι το Κλειδί Κ, το οποίο στέλνεται κρυπτογραφημένο μαζί με το πρόσφατα αντικατεστημένο Κλειδί F (για το Χρήστη 12) κι επίσης μαζί με το κλειδί Ε (για τους Χρήστες 9 και 10). Το κλειδί Ν στέλνεται μετά κρυπτογραφημένο στο πρόσφατα αντικατεστημένο Κλειδί Κ (για τους Χρήστες 9, 10 και 12) κι επίσης κρυπτογραφημένο στο Κλειδί L (μοιράζεται από τους Χρήστες 13 έως 16). Τελικά, το Κλειδί Ο αντικαθίσταται κι αυτό το νέο κλειδί στέλνεται κρυπτογραφημένο στο πρόσφατα αντικατεστημένο Κλειδί Ν (για τους Χρήστες 9, 10 και 12 μέχρι 16) κι επίσης κρυπτογραφείται χωριστά στο Κλειδί Μ (μοιράζεται από τους Χρήστες 1 έως 8). Αφού προχωράμε από το τέλος προς την αρχή, κάθε ένα από τα αντικατεστημένα κλειδιά έχει αντικατασταθεί πριν χρησιμοποιηθεί για να κρυπτογραφήσει άλλο κλειδί.



Σχήμα 39: *Λογική ιεραρχία κλειδιών*

Τα επτά κλειδιά που στέλνονται αντιπροσωπεύουν μια σημαντική εξοικονόμηση στα 16 κλειδιά που θα χρειαστεί να μεταδοθούν χρησιμοποιώντας το σύστημα flat key του Σχήματος 39. Σύντομα γράφουμε αυτά τα κλειδιά ως $\{F\}_{12}$ $\{K\}_E$ $\{K\}_F$ $\{N\}_K$ $\{N\}_L$ $\{O\}_M$ $\{O\}_N$. Γενικά, ο αριθμός των μεταδόσεων που απαιτούνται είναι το άθροισμα των βαθμών των αντικατεστημένων κόμβων. Σε ένα δέντρο k-ary βάθους d, αυτό είναι το σύνολο των $kd - 1 = k\log_k N - 1$ μεταδόσεων.

Το Group Traffic Encrypting Key (GTEK), που χρησιμοποιείται για την κρυπτογράφηση της κίνησης των δεδομένων, ανάλογα με την πολιτική ασφαλείας, μπορεί είτε να είναι το Κλειδί Ο (βλέπε Σχήμα 39) είτε να είναι ξεχωριστά κρυπτογραφημένο χρησιμοποιώντας το Κλειδί Ο και να μεταδίδεται σε όλα τα group members.

3.2.2. Πρωτόκολλα multicast key management

3.2.2.1. Group Secure Association Key Management Protocol (GSAKMP)

Το GSAKMP είναι ένα πρωτόκολλο τριών μηνυμάτων multicast key management το οποίο δεν απαιτεί κάποιο βασικό unicast σύνδεσμο ασφαλείας, θεωρείται πως χρησιμοποιείται ένας μη ασφαλής μηχανισμός για τη μετάδοση μη ευαίσθητης πληροφορίας σχετικά με τους μηχανισμούς ασφάλειας που χρησιμοποιείται για την εδραίωση της ομάδας.

Το πρωτόκολλο GSAKMP περιλαμβάνει μηχανισμούς για την πολιτική διάδοσης της ομάδας και για τη λειτουργία rekeying της ομάδας. Η μετάδοση μιας πλήρως καθορισμένης πολιτικής, που πάρθηκε σε όλα τα συμμετέχοντα group members, είναι αυτό που επιτρέπει ρο GSAKMP να υποστηρίζει τις διαμοιρασμένες αρχιτεκτονικές και τις πολλαπλές πηγές δεδομένων μέσα σε μία μοναδική κρυπτογραφική ομάδα. Οι διαμοιρασμένες αρχιτεκτονικές υποστηρίζονται διότι η αποφασισμένη πολιτική επιτρέπει τη βασισμένη σε κανόνες κατανομή των ενεργειών του Group Security Association στους πόρους του δικτύου. Οι πολλαπλές πηγές δεδομένων υποστηρίζονται διότι η συμπερίληψη της αποφασισμένης πολιτικής και των payloads της πολιτικής επιτρέπει στα group members να επανεξετάσει τις παραμέτρους της πρόσβασης της ομάδας και της εξουσιοδότησης.

Στην ομάδα GSAKMP υπάρχουν δύο τύποι οντοτήτων, ένα Group Member κι ένα Group Controller, που καθορίζονται παρακάτω.

Group Member: Το Group Member (GM) είναι μια οντότητα με πρόσβαση στις ομάδες κλειδιών. Ανεξάρτητα από τον τρόπο με τον οποίο ένας μέλος παίρνει μέρος στην ομάδα ή τον τρόπο με τον οποίο δομείται η ομάδα, τα GMs εκτελούν τις παρακάτω ενέργειες:

- Επικύρωση των εξουσιοδοτήσεων για ενέργειες σχετικές με την ασφάλεια
- αποδοχή της ομάδας κλειδιών από το Group Controller
- αίτημα για ομάδα κλειδιών από το Group Controller
- διατήρηση των τοπικών Certificate Revocation Lists (CRLs)
- ενδυνάμωση των πολιτικών των συνεργαζόμενων ομάδων όπως ορίζεται στην αποφασισμένη πολιτική ομάδας
- εκτέλεση ομότιμης αξιολόγησης των ενεργειών του key management και
- διαχείριση των τοπικών τους κλειδιών.

Group Controller: Το Group Controller (GC) είναι μια ομάδα με άδεια να εκτελέσει οποιαδήποτε σημαντική ενέργεια πρωτοκόλλου από τις παρακάτω:

- Δημιουργία και διανομή κλειδιών
- διατήρηση της υποδομής Rekey
- δημιουργία και διατήρηση των πινάκων Rekey.

Η ακολουθία των γεγονότων του GSAKMP είναι απλή κι είναι η εξής:

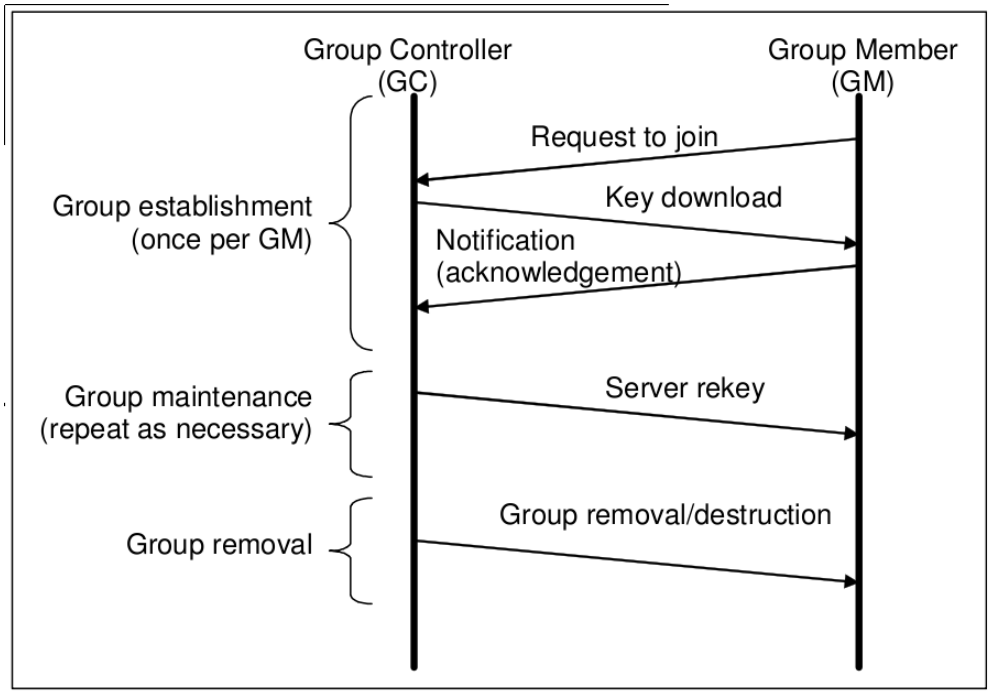
- ο ορισμός της σουίτας ασφάλειας μεταδίδεται έξω από το πρωτόκολλο
- η φάση της εδραίωσης της ομάδας που περιλαμβάνει τα εξής:
  - ~ Request To Join (RTJ)
  - ~ Κατέβασμα του κλειδιού
  - ~ Ενημέρωση
- το Security Association (SA) έτοιμα και να λειτουργεί
- η διαχείριση της ομάδας

Η ανακοίνωση περιλαμβάνει τουλάχιστον τη σουίτα ασφάλειας, που είναι οι τύποι των κρυπτογραφικών αλγορίθμων που χρησιμοποιούνται κι ο αναμενόμενος τύπος κλειδιών.

Ενώ η αρχική ακολουθία που μια οντότητα χρησιμοποιεί για να εισέλθει στην ομάδα είναι unicast μεταξύ της οντότητας και του GC, τα μηνύματα διαχείρισης της ομάδας είναι multicast από τη φύση τους και περιλαμβάνουν το rekey, αλλαγές στην πολιτική και διαγραφή της ομάδας.

Κύκλος ζωής του GSAKMP

Ο κύκλος ζωής μιας GSAKMP ομάδας ασφαλών συνδέσμων μπορεί να χωριστεί σε τρείς φάσεις που παρουσιάζονται στη συνέχεια. Στο Σχήμα 40 το αριστερό κομμάτι του διαγράμματος απεικονίζει τις ενέργειες του GC και το αριστερό τις ενέργειες των GMs.



Σχήμα 40: *GSAKMP ανταλλαγή μηνύματος*

Εγκαθίδρυση GSAKMP ομάδας

Τα ενδεχόμενα GMs μπορούν να ενταχθούν σε μία ομάδα με έναν από τους παρακάτω δύο τρόπους:

- Με πρόσκληση (push)
- Με αίτημα (pull)

Το Σχήμα 40 περιγράφει ένα αίτημα ένταξης στην ομάδα (Request to Join – RTJ), ένα μήνυμα "pull" που στέλνεται από ένα ενδεχόμενο GM. Κατά την παραλαβή του RTJ, το GC πρέπει είτε να αποδεχτεί είτε να αρνηθεί το αίτημα. Αν γίνει αποδοχή, το GC

ελέγχει το μήνυμα RTJ κι ακολουθεί η επιτυχημένη εξουσιοδότηση κι επιβεβαίωση δημιουργώντας το κλειδί download payload. Αυτό περιλαμβάνει την πολιτική payload, την κίνηση του κρυπτογραφικού κλειδιού payload κι επίσης το γεγονός rekey payload, που βοηθάει στην επεκτάσιμη συντήρηση της ομάδας. Το GM γνωστοποιεί το GC για την επιτυχημένη παραλαβή του μηνύματος του download του κλειδιού.

Το μέλος της ομάδας θα κινήσει τις ακολουθίες τριών μηνυμάτων για την εγκαθίδρυση της ομάδας, οι οποίες είναι:

- Το Request To Join (RTJ) ξεκινά το κομμάτι της εγκαθίδρυσης της ομάδας GSAKMP του πρωτοκόλλου. Το RTJ περιέχει ένα πεδίο δημιουργίας κλειδιού για χρήση στην εγκαθίδρυση της ομάδας.
- Το key download περιλαμβάνει ένα πεδίο δημιουργίας κλειδιού και μια κρυπτογραφημένη πολιτική και key download payloads.
- Το μήνυμα της γνωστοποίησης ολοκληρώνει την πιστοποίηση του μέλους.

GSAKMP ομάδα συντήρησης

Η φάση της ομάδας συντήρησης περιλαμβάνει τα παρακάτω:

Το μέλος εντάσσεται και φεύγει

Η προσθήκη μελών σε μια ήδη εγκατεστημένη ομάδα θα ακολουθήσει ακριβώς τη διαδικασία που παρουσιάστηκε σε προηγούμενη παράγραφο. Με εξαίρεση τις καθαρές αποστολές της ομάδας (όπως η δημιουργία πολιτικής, GTEK, πίνακας Rekey), μια οντότητα γίνεται GM χρησιμοποιώντας τις ίδιες ανταλλαγές μηνυμάτων που περιγράφηκαν στην προηγούμενη παράγραφο.

Το μέλος μιας ομάδας που αποφασίζει εθελοντικά να εγκαταλείψει την ομάδα είναι υπεύθυνο για την καταστροφή των κλειδιών του. Οποιαδήποτε άλλη πράξη απαιτείται για την εθελοντική απομάκρυνση από την ομάδα πρέπει να αντιμετωπίζεται συγκεκριμένα από την πολιτική ασφαλείας της ομάδας.

Γεγονότα Επανακτυπτογράφησης (Rekey)

Ένα γεγονός Rekey είναι οποιαδήποτε ενέργεια, συμπεριλαμβανομένων των συμβιβασμών, η οποία συνεπάγεται τη δημιουργία και τη διάδοση ενός νέου ομαδικού κλειδιού (group key) και/ ή της πληροφορίας Rekey. Από τη στιγμή που έχει αναγνωριστεί, με τη χρήση της πολιτικής ασφαλείας της ομάδας, πως έχει συμβεί ένα γεγονός Rekey, το GC πρέπει να δημιουργήσει και να στείλει στην ομάδα ένα προσημασμένο μήνυμα που να περιέχει το GTEK και τον πίνακα Rekey.

Κάθε GM που λαμβάνει αυτό το μήνυμα πρέπει να επιβεβαιώσει την υπογραφή σε αυτό το μήνυμα για να διασφαλίσει τη γνησιότητά του. Αν η υπογραφή του μηνύματος δεν επιβεβαιωθεί η διαδικασία τερματίζεται. Το GSAKMP στέλνει ένα κατάλληλα πιστοποιημένο μήνυμα με ένα Notification Payload τύπου NACK για να υποδείξει τη

λήψη από το GM. Αν γίνει η επιβεβαίωση το GM θα βρει το κατάλληλο πακέτο Rekey download και θα αποκρυπτογραφήσει την πληροφορία μαζί με το αποθηκευμένο κλειδί Rekey.

Απομάκρυνση/ καταστροφή της ομάδας GSAKMP

Η τελική φάση του κύκλου ζωής της ομάδας είναι η απομάκρυνση της ομάδας. Αν αποφασιστεί η καταστροφή της ομάδας, η ειδοποίηση μπορεί είτε να γίνει broadcast μέσω ενός καναλιού key management είτε μέσω μιας υπηρεσίας καταλόγου.

Rekey Management

Η χρήση προηγμένων τεχνικών rekey management, όπως είναι το Logical Key Hierarchy (LKH), μειώνει το overhead που προκαλείται από το key management κατά τη διάρκεια των γεγονότων Rekey. Αυτό επιτρέπει να εδραιωθούν υπερβολικά μεγάλες ομάδες (100.000 – 1.000.000 χρήστες) και να ελέγχονται με αποτελεσματικό τρόπο.

3.2.2.2. Multimedia Internet KEYing (MIKEY)

Το πρωτόκολλο MIKEY χρησιμοποιείται για peer-to-peer, απλές one-to-many και μικρές σε μέγεθος (διαδραστικές) ομάδες και προορίζεται για χρήση εφαρμογών σε πραγματικό χρόνο. Ένα από τα κύρια σενάρια πολυμέσων είναι το σενάριο πολυμέσων συνομιλίας, κατά το οποίο οι χρήστες μπορεί να αλληλεπιδρούν και να συνομιλούν σε πραγματικό χρόνο. Σε αυτά τα σενάρια αναμένεται πως οι peers θα στήσουν συνεδρίες πολυμέσων μεταξύ τους, όπου η συνεδρία πολυμέσων θα αποτελείται από μία ή περισσότερες ροές πολυμέσων (για παράδειγμα SRTP streams).

Το πρωτόκολλο MIKEY είναι σχεδιασμένο έτσι ώστε να έχει τα παρακάτω χαρακτηριστικά:

- Ασφάλεια end-to-end: μόνο οι συμμετέχοντες έχουν πρόσβαση στα παραγόμενα κλειδιά
- Απλότητα
- Αποτελεσματικότητα: σχεδιασμένο να έχει:
  - ~ Χαμηλή κατανάλωση έυρους ζώνης
  - ~ Χαμηλό φόρτο εργασίας για τους υπολογισμούς
  - ~ Μικρό μέγεθος κώδικα
  - ~ Μικρό αριθμό round-trips
  - ~ Tunneling, δυνατότητα να κάνει“tunnel” στο MIKEY στα πρωτόκολλα εδραίωσης συνεδρίας (όπως το SIP και το RTSP)
  - ~ Ανεξαρτησία μιας συγκεκριμένης λειτουργίας ασφάλειας από την υποκείμενη μεταφορά.

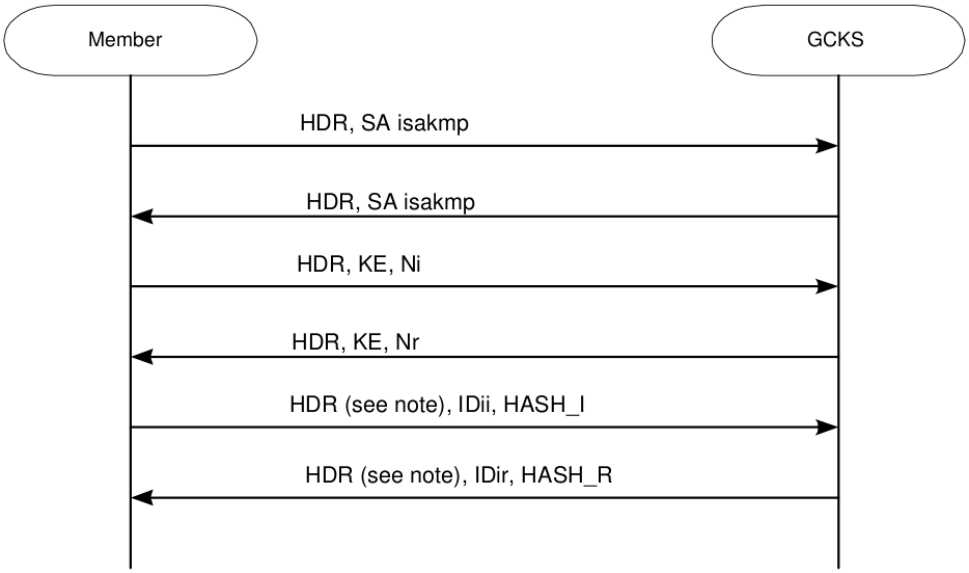
Το MIKEY μπορεί να χρησιμοποιηθεί με συμμετρικά κλειδιά, δημόσια κλειδιά ή με ανάπτυξη κοινόχρηστου κλειδιού χρησιμοποιώντας το πρωτόκολλο Diffie-Hellaman. Όταν τα μηνύματα MIKEY γίνονται tunneled με τη χρήση του SIP, τα χαρακτηριστικά ασφάλειας του SIP μπορούν να χρησιμοποιηθούν για την ασφάλεια των μηνυμάτων MIKEY.

Το MIKEY προσφέρει μόνο εγγραφή των χρηστών και διανομή του αρχικού κλειδιού. Αντίθετα από το GSAKMP, δεν παρέχει μηχανισμούς rekeying ούτε επιτρέπει διάδοση της πολιτικής ασφαλείας της ομάδας. Το πρωτόκολλο βελτιστοποιείται κυρίως για απόδοση σε πραγματικό χρόνο και δεν είναι επεκτάσιμο σε μεγάλες ομάδες.

3.2.2.3. Group Domain of Interpretation (GDOI)

Το GDOI (RFC 3547 [4]) είναι ένα ISAKMP Domain of Interpretation (DOI) της ομάδας key management για την υποστήριξη των ασφαλών επικοινωνιών της ομάδας. Προτείνει νέες ανταλλαγές σύμφωνα με τα πρότυπα του ISAKMP και του IKE. Όλα τα μηνύματα GDOI χρησιμοποιούνται για τη δημιουργία, τη συντήρηση και τη διαγραφή των συνδέσμων ασφαλείας για μια ομάδα. Αυτοί οι σύνδεσμοι ασφαλείας προστατεύουν ένα ή περισσότερα Key-Encrypting Keys (KEK), Traffic-Encrypting Keys (TEK) ή δεδομένα που μοιράζονται τα μέλη της ομάδας. Το GDOI αποτελείται από 3 διαφορετικές ανταλλαγές.

IKE phase 1
Το GDOI επαναχρησιμοποιεί την IKE phase 1 για δημιουργήσει ISAKMP SA μεταξύ ενός πιθανού μέλους και των Group Controller και Key Server (GCKS), που παρέχει εμπιστευτικότητα κι ακεραιότητα. Αυτό το ασφαλές κανάλι χρησιμοποιείται για να προστατεύσει μια νέα Phase 2 ανταλλαγής που λέγεται “GROUPKEY-PULL” κι ορίζεται παρακάτω.



NOTE: Protected by the IKE Phase 1 SA, encryption occurs after HDR.

Σχήμα 41: *GDOI ανταλλαγή "IKE Phase 1"*

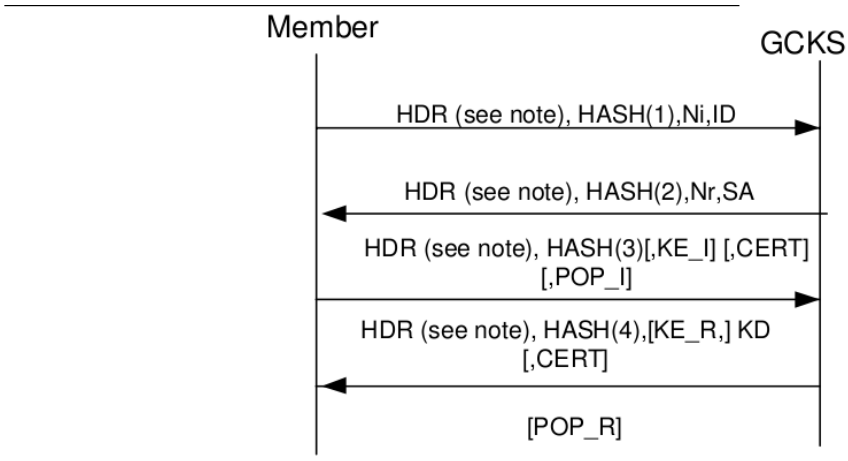
Ανταλλαγή GROUPKEY-PULL

Το GDOI προτείνει μια νέα ανταλλαγή Phase 2, που λέγεται GROUPKEY-PULL, της οποίας ο στόχος είναι να εγκαθιδρύσει ένα Re-Key SA και/ή Data Security SAs στο μέλος μιας συγκεκριμένης ομάδας. Αυτή η ανταλλαγή ξεκινά από ένα ενδεχόμενο μέλος προς το GCKS. Ο IKE Phase 1 SA προστατεύει το GROUPKEY-PULL. Μπορεί να υπάρχουν πολλαπλές ανταλλαγές GROUPKEY-PULL για ένα δεδομένο Phase 1 SA.

Το πιθανό μέλος στέλνει το αρχικό μήνυμα μαζί με το αναγνωριστικό της ομάδας (περιέχεται στο ID payload) στην οποία θέλει να πάρει μέρος.

Ο GCKS Responder ενημερώνει το πιθανό μέλος για τις πολιτικές κρυπτογράφησης της ομάδας στο SA payload. Ένα Re-Key SA μπορεί να καθοριστεί κι ένα ή περισσότερα Data Security SAs καθορίζονται.

Το τελευταίο μήνυμα κατεβάζει το KD (Key Download) payload. Αν ο Re-Key SA ορίζεται στο SA payload, τότε το KD θα περιέχει το KEK. Αν ένας ή περισσότεροι Data SAs ορίζονται στο SA payload, το KD θα περιέχει τα TEKs. Εκτός των άλλων, αν ένα Re-Key SA ορίζεται στο SA payload, πρέπει να υπάρχει το SEQ payload (το SEQ payload περιέχει τη τρέχουσα τιμή της αριθμητικής ακολουθίας που διατάσσει τα Group-Key Push datagrams.

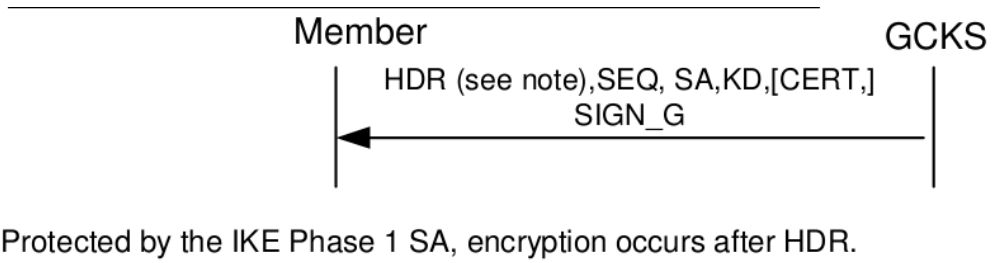


Σχήμα 42: *GDOI ανταλλαγή "GROUPKEY-PULL"*

Τα HASH payloads αποδεικνύουν πως ο peer γνωρίζει το μυστικό κλειδί της Phase 1 κι εγγυάται "ζωτικότητα" (εμποδίζει κάποιον από την αναπαραγωγή της πρόσφατης ανταλλαγής GROUPKEY-PULL). Στην πραγματικότητα, οι παράμετροι των συναρτήσεων κατακερματισμού πάντοτε εξαρτώνται από τυχαίους αριθμούς (Ni και Nr), που εγγυάται ένα μοναδικό HASH payload για κάθε μήνυμα. Με το HASH του δεύτερου μηνύματος, το Group Member είναι σίγουρο πως το μήνυμα προέρχεται από το GCKS, και δεν πρόκειται για κάποιο επαναλαμβανόμενο μήνυμα. Το HASH του τρίτου μηνύματος εγγυάται πως η ανταλλαγή GROUPKEY-PULL ξεκίνησε από το πιθανό Group Member κι όχι από κάποιο εισβολέα που επαναλαμβάνει μια πρόσφατη ανταλλαγή GROUPKEY-PULL.

Στα τελευταία δύο μηνύματα περιλαμβάνονται (προαιρετικά) τα Proof-of-Prossession (POP) και "Cerificate" (CERT) payloads. Το POP payload περιέχει την ψηφιακή υπογραφή του μηνύματος, που μπορεί να υπολογιστεί με το ιδιωτικό κλειδί του αποστολέα. Το Cerificate" περιλαμβάνει το αντίστοιχο δημόσιο κλειδί πιστοποιημένο από τον ιδιοκτήτη της ομάδας. Αν αυτά τα payloads σταλούν από τα μέλη, αυτό αποδεικνύει πως είναι εξουσιοδοτημένα να έχει πρόσβαση σα ομαδικά κλειδιά (ο ιδιοκτήτης της ομάδας του έδωσε ένα ζευγάρι δημόσιων/ ιδιωτικών κλειδιών). Αν σταλούν από το GCKS αυτό δείχνει πως είναι εξουσιοδοτημένο να δώσει τα κλειδιά για την ομάδα.

GROUPKEY PUSH



Σχήμα 43: *GDOI ανταλλαγή "GROUPKEY-PUSH"*

Το GDOI χρησιμοποιεί το GROUPKEY-PUSH datagram για να αντικαταστήσει ένα Re-Key SA KEK, και/ ή να δημιουργήσει ένα νέο Sata Security SA. Το GROUPKEY-PUSH μήνυμα "ωθείται" από το GCKS στα μέλη (στο multicast). Τα GROUPKEY-PUSH μηνύματα είναι κρυπτογραφημένα με το Re-Key SA κι υπογεγραμμένα από το GCKS.

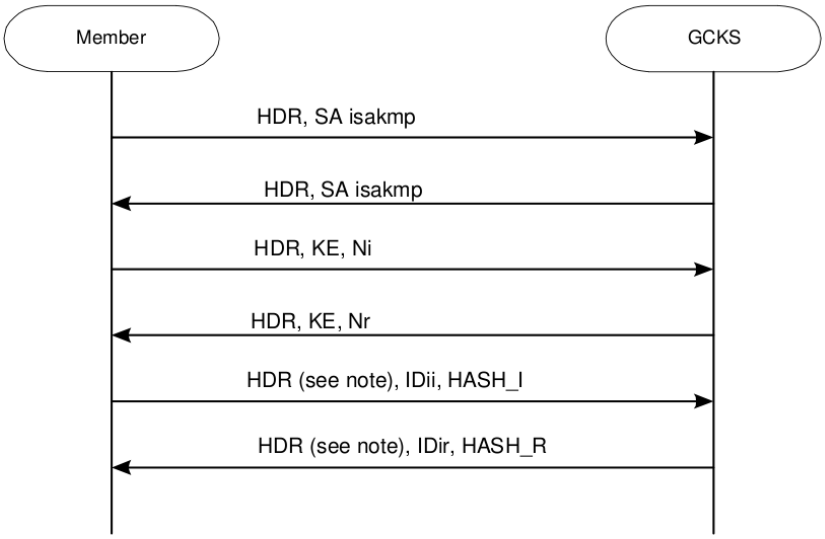
Το KD payload περιέχει τα νέα κλειδιά.

Το SEQ payload περιέχει μια αριθμητική ακολουθία, η οποία αντιστοιχεί στην αριθμητική ακολουθία η οποία έχει αρχικοποιηθεί στην ανταλλαγή GROUPKEY-PULL. Το μέλος αποδέχεται μόνο τα GROUPKEY-PUSH μηνύματα με μια αριθμητική ακολουθία κατώτερη της ακολουθίας του προηγούμενου μηνύματος (αυτός ο μηχανισμός αποτρέπει τις επιθέσεις επανάληψης).

3.2.2.4. Flat Multicast Key Exchange (FMKE)

Το FMKE (Flat Multicast Key Exchange [48]) είναι ένα νέο πρωτόκολλο ομαδικού key management. Το αντικείμενο του είναι να διαχειριστεί με ασφάλεια τα ομαδικά Security Associations (SA), για παράδειγμα να εγκαθιδρύσει και να ανανεώσει το Data Security και τα Re-Key SAs στα Group Members. Το FMKE αποτελείται από 3 διαφορετικές ανταλλαγές.

FMKE Phase 1 (IKE Phase 1)
Το FMKE επαναχρησιμοποιεί την IKE Phase 1 για να δημιουργήσει ένα ISAKMP SA μεταξύ του πιθανού μέλους και του Group Controller και Key Server (GCKS), που παρέχει εμπιστευτικότητα κι ακεραιότητα. Αυτό το ασφαλές κανάλι χρησιμοποιείται για να προστατεύσει τη νέα ανταλλαγή Phase 2, που ορίζεται παρακάτω.



NOTE: Protected by the IKE Phase 1 SA, encryption occurs after HDR.

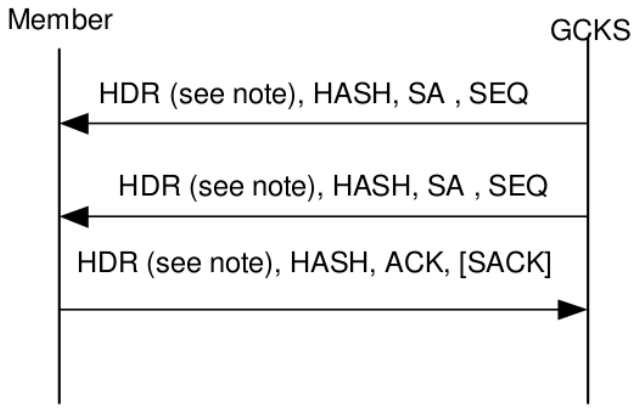
Σχήμα 44: *FMKE ανταλλαγή Phase 1*

FMKE Phase 2

Ο στόχος της ανταλλαγής Phase 2 είναι να εγκαθιδρύσει Re-Key SAs και/ ή Data-Security SAs στο μέλος. Τα μεταδιδόμενα SAs ανήκουν στις ίδιες ή διαφορετικές ομάδες. Κατά τη διάρκεια αυτή της φάσης, το μέλος μπορεί να λαμβάνει όλα τα Data Security SAs και Re-Key SAs για τα οποία έχει εξουσιοδοτημένη πρόσβαση. Η ανταλλαγή Phase 2 συμβαίνει μια φορά, μετά τη Phase 1 κι αρχικοποιείται από το GCKS και προστατεύεται από το Phase 1 SA.

Η ανταλλαγή Phase 2 αποτελείται από δύο τύπους μηνυμάτων: τα μηνύματα που στέλνονται από το GCKS, που περιέχουν τα SA χαρακτηριστικά στα οποία έχει πρόσβαση το μέλος και τα μηνύματα που στέλνονται από το μέλος, τα οποία χρησιμοποιούνται για να αναγνωρίσουν τα προηγούμενα μηνύματα.

Τα μηνύματα αναγνώρισης στέλνονται περιοδικά από το μέλος.



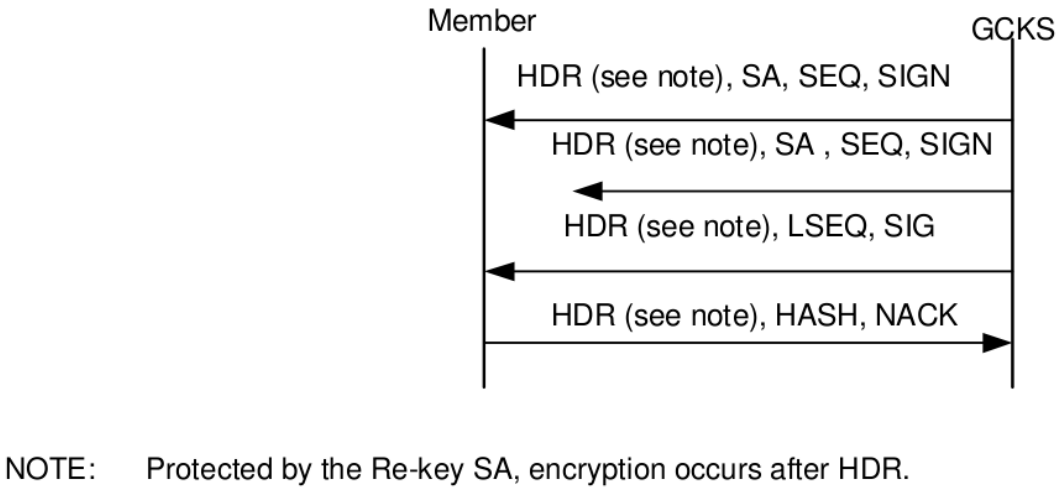
NOTE: Protected by the phase 1 SA, encryption occurs after HDR.

Σχήμα 45: *FMKE ανταλλαγή Phase 2*

Στα GCKS μηνύματα το SEQ payload περιέχει την τρέχουσα τιμή της αριθμητικής ακολουθίας, η οποία διατάσσει αυτά τα μηνύματα. Στα μηνύματα των μελών η τιμή του ACK (Acknowledgement) payload αναφέρει την αριθμητική ακολουθία του τελευταίου μηνύματος που λήθφηκε σωστά. Το SACK (Selective Acknowledment) payload μπορεί εναλλακτικά να περιλαμβάνεται στα Phase 2 μηνύματα μελών. Όταν ένα ή περισσότερα GCKS μηνύματα λείπουν επιτρέπει την αναφορά μερικών από τα ήδη ληφθέντα αριθμητικά μηνύματα.

Το HASH payload δείχνει πως τα μηνύματα δεν έχουν τροποποιηθεί κατά τη διάρκεια της μετάδοσης και πως ο peer γνωρίζει το Phase 1 μυστικό. Το HASH payload εγγυάται επίσης πως τα μηνύματα δε θα παιχτούν ξανά από μια παλιά συνεδρία, αφού απαιτείται το μυστικό της τελευταίας Phase 1. Το SEQ payload στα GCKS μηνύματα επιτρέπει στο μέλος να διαγράψει όλα τα μηνύματα που έχουν ήδη ληφθεί στη Phase 2, αφού πρέπει να ελέγξει αν η αριθμητική ακολουθία είναι μεγαλύτερη από εκείνη των προηγούμενων SEQ payloads.

FMKE Phase 3



Σχήμα 46: *FMKE ανταλλαγή Phase 3*

Ο στόχος της Phase 3 είναι να δημιουργήσει, να ανανεώσει και/ ή να αντικαταστήσει τα Data Security SAs και/ ή να ανανεώσει το Re-key SA στα Group Members (που ανήκουν στην ίδια ομάδα). Η Phase 3 προστατεύεται από το Re-Key SA της ομάδας. Το GCKS ωθεί τις ιδιότητες του νέου SA.

Στην Phase 3 το GCKS στέλνει δύο τύπους μηνυμάτων. Ο πρώτος τύπος περιέχει το SA payload και χρησιμοποιείται για να δημιουργήσει, να ανανεώσει και/ ή να αντικαταστήσει τα νέα SAs (περιλαμβάνονται τα TEKs και τα KEKs). Σε αυτά τα μηνύματα, όπως στη Phase 2, ένα SEQ payload περιλαμβάνεται που περιέχει μια αριθμητική ακολουθία που τα διατάσσει. Ο δεύτερος τύπος μηνυμάτων, που στέλνονται περιοδικά, περιλαμβάνει ένα LSEQ (Last Sequence Number) payload του οποίου η τιμή αναφέρει την τελευταία αριθμητική ακολουθία που χρησιμοποιήθηκε από το GCKS. Αυτά απαιτούνται για να εξασφαλίσουν την αξιοπιστία.

Το Group Member στέλνει μόνο ένα τύπο μηνυμάτων. Αυτά τα μηνύματα χρησιμοποιούνται ως μηνύματα μη αναγνώρισης, δηλαδή απαιτούν την επαναμετάδοση, σε multicast, των μηνυμάτων, των οποίων η αριθμητική ακολουθία αναφέρεται στο NACK (Negative Acknowledgement) payload. Ένα Group Member μπορεί να προσδιορίσει αν έχει λάβει ένα ή περισσότερα μηνύματα εξαιτίας των SEQ και LSEQ payloads που περιλαμβάνονται στα μηνύματα που στέλνονται από το GCKS. Για μια ομάδα, η ανταλλαγή Phase 3 μπορεί να ξεκινήσει από το GCKS αμέσως μόλις το Re-Key SA εδραιωθεί σε ένα τουλάχιστον από τα Group Member.

Το SIG payload περιέχει την ψηφιακή υπογραφή ολόκληρου του μηνύματος πριν την κρυπτογράφηση (συμπεριλαμβανομένης της επικεφαλίδας και εξαιρουμένου του ίδιου του SIG payload). Η υπογραφή εγγυάται πιστοποίηση της πηγής δεδομένων, για παράδειγμα η πηγή αυτών των μηνυμάτων είναι το GCKS.

Το SEQ payload των μηνυμάτων GCKS επιτρέπει στα Group Members να ανιχνεύσουν μηνύματα που παίζονται ξανά: διαγράφουν όλα τα μηνύματα που έχουν ήδη ληφθεί.

Το HASH payload των μηνυμάτων του Group Member αποδεικνύει πως τα μηνύματα δεν έχουν τροποποιηθεί κατά τη διάρκεια της μετάδοσης και πως η πηγή τους είναι ένα από τα Group Members.

Rekeying
Ορίζονται δύο μορφές rekeying: η μία σε multicast, βασισμένη στη Phase 3 (ίδια μηνύματα εκτός του ότι ένα Key download payload προστίθεται στα GCKS μηνύματα) και μία σε unicast βασισμένη στη Phase 2 (ίδια μηνύματα εκτός του ότι ένα Key download payload προστίθεται στα GCKS μηνύματα).

Το FMKE μπορεί να θεωρηθεί μια περίπτωση χρήσης του GDOI. Οι κύριες διαφορές μεταξύ του GDOI και του FMKE είναι:

- Το FMKE προσφέρει αξιόπιστη ανταλλαγή διανομής κλειδιών.
- Το FMKE Phase 2 απαιτεί λιγότερα μηνύματα για ένα ίσο αριθμό SAs για τη μετάδοση σε σχέση με το GDOI GROUPKEY PULL.
- Στο FMKE τα μέλη δεν απαιτούν να έχουν πρόσβαση σε μια ομάδα, λαμβάνουν απευθείας όλα τα SAs που έχουν εξουσιοδότηση να ξέρουν.

3.3. Σχετικές εργασίες με τη multicast διαχείριση κλειδιών

Η διαδικασία της διασφάλισης και της εκτέλεσης της διαχείρισης κλειδιών για unicast συνδέσεις είναι πλήρως κατανοητή [43], [45], [53], αλλά η multicast ασφάλεια είναι πιο πολύπλοκη. Κατ' αρχήν, μια multicast σύνδεση πρέπει να θεωρείται, από την πλευρά της ασφάλειας, σαν ένα σετ από unicast συνδέσεις, αλλά αυτή η προσέγγιση δεν επεκτείνεται καλά σε μεγάλες ομάδες, ειδικά στην κλίμακα που αναμένεται για τα δορυφορικά συστήματα. Τα πρωτόκολλα που διαχειρίζονται τη διαδικασία της διανομής κλειδιών σε ένα multicast περιβάλλον βρίσκονται υπό κατασκευή [54], [55], [56].

Οι κύριοι παράγοντες για τη multicast διαχείριση κλειδιών είναι ο ελεγκτής της ομάδας (Group Controller – GC) και τα μέλη της ομάδας (Group Members – GMs). Το πρώτο είναι υπεύθυνο για τη δημιουργία και διανομή των κλειδιών και της επανακρυπτογράφησης (για τη διατήρηση της ασφάλειας) όπου χρειάζεται, ενώ το

δεύτερο είναι οντότητες που έχουν πρόσβαση στα ομαδικά κλειδιά. Το GC δεν είναι απαραίτητο να βρίσκεται στον ίδιο χώρο με τη multicast πηγή δεδομένων. Κάθε GM έχει ένα αρχικό one-to-one σύνδεσμο ασφάλειας με το GC (χρησιμοποιώντας τεχνικές όπως είναι η Deffie-Hellman για να δημιουργήσει ένα κοινόχρηστο μυστικό γνωστό μόνο στα δύο αυτά μέρη ή ένα προμοιρασμένο μυστικό ή μια μυστική ανταλλαγή με τη χρήση του συστήματος του δημοσίου κλειδιού [57]). Αυτοί οι σύνδεσμοι ασφάλειας χρησιμοποιούνται μετά για να δημιουργήσουν και να μοιράσουν την πληροφορία σχετικά με τον ομαδικό σύνδεσμο ασφάλειας μεταξύ του GC κι όλων των GMs. Ο υπέρτατος στόχος του ομαδικού συνδέσμου ασφάλειας είναι να διασφαλίσει πως το μοναδικό κλειδί, συνήθως ονομάζεται ομαδικό κρυπτογραφικό κλειδί κυκλοφορίας (Group Traffic Encryption Key - GTEK) είναι γνωστό στο GC και σε όλα τα GMs αλλά σε καμία οντότητα έξω από την ομάδα: Αυτό το κλειδί μπορεί μετά να χρησιμοποιηθεί για να κρυπτογραφήσει τα δεδομένα multicast μέσα στην ομάδα.

Η multicast ομάδα μπορεί να χρειάζεται να επανακρυπτογραφηθεί για οποιονδήποτε από τους εξής λόγους:

1) Το ομαδικό κλειδί συνήθως ανανεώνεται τακτικά (τυπικά κάθε λίγα δευτερόλεπτα ή λεπτά) για να μειωθεί η πιθανότητα μια επιτυχημένης κρυπτανάλυσης της κρυπτογραφημένης κυκλοφορίας.
2) Το ομαδικό κλειδί μπορεί να χρειάζεται να αλλάξει κατά παραγγελία εφόσον διαπιστωθεί πως το κλειδί έχει παραβιαστεί.
3) Η επανακρυπτογράφηση μπορεί να απαιτείται όταν ένα νέο μέλος εισέρχεται στη multicast ομάδα. Αυτό διασφαλίζει πως το μέλος δεν μπορεί να αποκρυπτογραφήσει την κωδικοποιημένη κυκλοφορία που είχε σταλεί πριν εισέλθει στην ομάδα (backward secrecy).
4) Η επανακρυπτογράφηση μπορεί να απαιτείται όταν ένα υπάρχον μέλος φεύγει από την multicast ομάδα. Αυτό διασφαλίζει πως το μέλος δεν μπορεί να αποκρυπτογραφήσει την κωδικοποιημένη κυκλοφορία που στέλνεται αφού φύγει (forward secrecy).

Για μεγάλες multicast ομάδες που έχουν συχνές αλλαγές στα μέλη τους, το κόστος της επανακρυπτογράφησης μπορεί να είναι σημαντικό, αφού οι δορυφορικοί πόροι είναι ακριβοί. Η επεκτάσιμη επανακρυπτογράφηση είναι, για το λόγο αυτό, ένα σημαντικό πρόβλημα που χρειάζεται να ληφθεί υπόψη για να μπορούν να υποστηριχθούν οι

ασφαλείς επικοινωνίες στις μεγάλες δυναμικές ομάδες. Στη συνέχεια παρουσιάζονται τεχνικές επανακρυπτογράφησης για κάθε μία από τις τέσσερις λειτουργίες που περιγράφηκαν παραπάνω.

Αρκετές τεχνικές υπάρχουν για την επανακρυπτογράφηση 1) και 3): Δύο επιλογές υπάρχουν για να κρυπτογραφηθεί το νέο ομαδικό κλειδί με είτε α) το παλιό ομαδικό κλειδί είτε β) ένα ξεχωριστό κλειδί "ελέγχου" που διαπραγματεύεται κατά τη σύνοδο δημιουργίας. Για τις περιπτώσεις 2) και 4), μια διαφορετική προσέγγιση επανακρυπτογράφησης απαιτείται αφού το παλιό κλειδί είναι γνωστό σε τουλάχιστον ένα χρήστη που δεν είναι πια παραλήπτης της multicast εκπομπής.

Έχει αναπτυχθεί ένας αριθμός προσεγγίσεων για τη multicast διαχείριση κλειδιών με στόχο τη βελτίωση της επεκτασιμότητας των ομαδικών συνδέσμων ασφάλειας διασφαλίζοντας πως οι παράμετροι αναπτύσσονται λιγότερο γρήγορα από το μέγεθος της ομάδας N. Οι παράμετροι που θεωρούνται περιλαμβάνουν την προσπάθεια κρυπτογράφησης GC και τις απαιτήσεις σε μνήμη. Οι τεχνικές διαχείρισης κλειδιών περιλαμβάνουν ένα επίπεδο σύστημα, το Iolus [58], το LKH [47] [59] και το Kronos [60].

Στην πιο απλή προσέγγιση, που είναι ένα επίπεδο σύστημα, το GC μοιράζεται ένα μοναδικό κλειδί με κάθε ξεχωριστό GM. Το GTEK μπορεί μετά να σταλεί στα μέλη κρυπτογραφώντας το N φορές με κάθε ένα από τα N μοναδικά κλειδιά. Συνεπώς, τόσο το φορτίο του GC κρυπτογραφικού κλειδιού όσο κι η επανακρυπτογράφηση της κυκλοφορίας αυξάνονται γραμμικά με N. Αξίζει να σημειωθεί πως για αυτό το επίπεδο σύστημα η ευρυζωνική φύση του δορυφόρου δεν παρέχει κάποιο πλεονέκτημα σε σύγκριση με το επίγειο δίκτυο, αφού τα κρυπτογραφημένα μηνύματα που στέλνονται στα N GMs είναι όλα διαφορετικά.

Στο Iolus [58], μια multicast ομάδα χωρίζονται σε αρκετές υποομάδες. Το GC διαχειρίζεται ένα δέντρο από ομάδα υποελεγκτών, καθένας από τους οποίους διαχειρίζεται ένα υποσύνολο της συμμετοχής της ομάδας. Το πλεονέκτημα αυτού του μηχανισμού είναι πως η προσπάθεια επανακρυπτογράφησης μοιράζεται μεταξύ των υποελεγκτών, αλλά τα μειονεκτήματα αυτής της προσέγγισης είναι ο μεγάλος αριθμός των υποελεγκτών που απαιτούνται σε μεγάλες ομάδες, η ανάγκη εμπιστοσύνης των

υποελεγκτών, κι η καθυστέρηση που προκαλείται από την ανάγκη να επανακρυπτογραφηθεί η κυκλοφορία καθώς περνά από κάθε υποελεγκτή.

Το LKH, που περιγράφεται πιο λεπτομερώς παρακάτω, χρησιμοποιεί ένα σύνολο κλειδιών διατεταγμένα σε μια δομή δέντρου για να μειωθεί το κόστος της επανακρυπτογράφησης. Για ένα πλήρες δέντρο με βαθμό εξόδου k και βάθος d, ο αριθμός των κλειδιών επανακρυπτογράφησης που μεταδίδονται σε ένα μέλος σε συμβιβασμό είναι $k\log_k N - 1$, το οποίο συγκρίνεται ευνοϊκά με το κόστος του $N = k^d$ του επίπεδου συστήματος. Το σύστημα είναι επίσης ισχυρό έναντι στη συμπαιγνία, υπό την έννοια πως δεν υπάρχει κάποιο σύνολο χρηστών που να μπορεί να διαβάσει μαζί οποιοδήποτε μήνυμα εκτός εάν ένας από αυτούς μπορεί να το διαβάσει μεμονωμένα. Βελτιώσεις του LKH για τη συγκεκριμένη περίπτωση των δυαδικών δέντρων ($k = 2$) έχουν επίσης προταθεί με μονόδρομες συναρτήσεις δέντρων (One-way Function Trees) [61], [62] και [63]: Και οι δύο αυτές προσεγγίσεις μειώνουν τον αριθμός των κλειδιών επανακρυπτογράφησης που απαιτούνται στην περίπτωση του συμβιβασμού ενός χρήστη από $2\log_2 N - 1$ σε $\log_2 N$.

Το Kronos είναι μια επιπλέον προσπάθεια για να μειωθεί η κρυπτογράφηση της κυκλοφορίας σε μεγάλες δυναμικές multicast ομάδες. Αυτή η προσέγγιση αναγνωρίζει αν δύο χρήστες αναχωρήσουν και προκαλέσουν δύο γεγονότα επανακρυπτογράφησης, κάποια από τα κλειδιά που αλλάζουν θα είναι κοινά στα δύο γεγονότα επανακρυπτογράφησης. Η επανακρυπτογράφηση της κυκλοφορίας μπορεί να σωθεί από τις ομαδικές αλλαγές και να επανακρυπτογραφεί πιθανώς κάθε λίγα δευτερόλεπτα.

3.4. Κόστος του κύκλου ζωής του LKH

3.4.1. Κόστη κύκλου ζωής

Υπάρχει μια σιωπηρή παραδοχή στη βιβλιογραφία σχετικά με το LKH, πως ο χρήστης που προσέρχεται ή αποχωρεί από τη διαδικασία της επανακρυπτογράφησης είναι το κύριο κόστος της διαχείρισης κλειδιών, με τα κόστη της αρχικοποίησης του δέντρου να είναι αμελητέα. Πάρα ταύτα, υπάρχουν εφαρμογές (όπως η μεταφορά αρχείων), όπου ο πληθυσμός των χρηστών έχει μικρή μεταβλητότητα κι έτσι τα κόστη της αρχικοποίησης του δέντρου γίνονται σημαντικά. Επίσης, κι ευδιάκριτα, μπορεί να υπάρχουν multicast ομάδες (π.χ. pay-per-view) όπου οι συνδρομητές εισέρχονται στην ομάδα στην ίδια περίπου χρονική στιγμή με αυξημένη απαίτηση για την εγκαθίδρυση συνδέσμου ασφάλειας στην ομάδα.

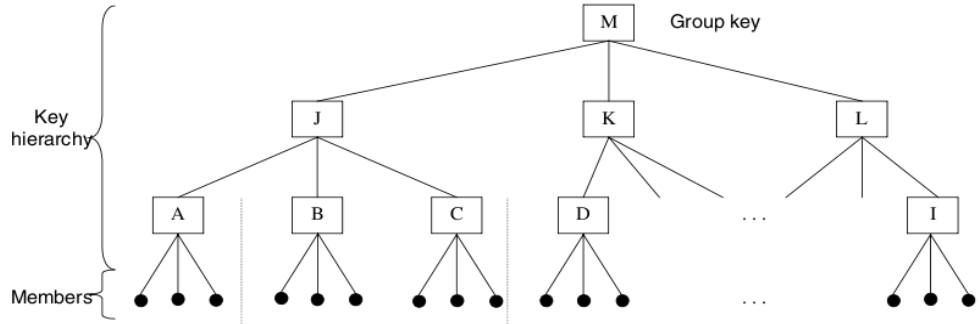
Για την ανάλυση μας χωρίζουμε τον κύκλο ζωής μιας ασφαλούς ομαδικής σύνδεσης στις εξής φάσεις:

- Αρχικοποίηση: Τα μέλη πιστοποιούνται στο GC και χορηγούνται με κλειδιά, μεταξύ των οποίων το ομαδικό κλειδί που χρησιμοποιείται για την κρυπτογράφηση των δεδομένων.
- Μεταφορά δεδομένων: Αυτό περιλαμβάνεις δύο δραστηριότητες επανακρυπτογράφησης:
    - ~ Το GTEK ανανεώνεται τακτικά έτσι ώστε να μειωθεί η πιθανότητα μιας επιτυχημένης κρυπτανάλυσης του κρυπτογραφημένου κειμένου.
    - ~ Η διαδικασία της επανακρυπτογράφησης συμβαίνει όταν μέλη εισέρχονται ή αποχωρούν για να διασφαλιστεί η τέλεια μυστικότητα προς τα πίσω ή προς τα εμπρός, αντίστοιχα, ή όταν ένα κλειδί ή μέλος έχει παραβιαστεί.
- Τερματισμός: Μόλις τα δεδομένα μεταφερθούν η ασφαλής σύνδεση τερματίζεται. Υποθέτουμε πως τα κλειδιά απλά απορρίπτονται αφού δε γίνεται πλέον κάποια χρήση.

Σε αυτή την ανάλυση υποθέτουμε πως ολόκληρο το LKH δέντρο γεμίζει κατά τη διάρκεια της φάσης της αρχικοποίησης, πως όταν η φάση της αρχικοποίησης ολοκληρωθεί το LKH δέντρο παραμένει ισοσταθμισμένο [64] και πως παραμένει σχεδόν γεμάτο καθώς τα μέλη εισέρχονται κι αποχωρούν.

3.4.2 Ανάλυση

Καθώς κάθε GM εισέρχεται σε μια ομάδα το μέλος πιστοποιείται και δημιουργείται ένα ζεύγος κλειδιών για την ασφαλή επικοινωνία με το GC χρησιμοποιώντας ένα μηχανισμό ο οποίος όμως είναι έξω από το αντικείμενο αυτής της εργασίας. Η μετρική μας είναι ο αριθμός των κρυπτογραφημένων κλειδιών που εκπέμπονται από την πηγή: Αγνοώντας τα overheads των πρωτοκόλλων, αυτό είναι ανάλογο της κυκλοφορίας του κλειδιού του δικτύου. Για ασφαλές multicast πάνω σε δορυφόρο, όπου οι πόροι είναι περιορισμένοι, είναι συγκεκριμένα σημαντικό να ελαχιστοποιηθούν τα κόστη κυκλοφορίας της διαχείρισης κλειδιών.



DYNAMIC TREE: generic tree of outdegree *k* and depth *d*

Member number:	1	2	..	*k*	*k*+1	*k*+2	..	2*k*	..	k^2	k^2+1	..	...	k^d-*k*+1	..	k^d
Perfect memory:	1	1	..	1	3	1	1		..	1	4	..	...	2	..	1
Tr'mit keys as required:	1	1	..	1	3	2	2		..	2	4	..	...	*d*	..	*d*
Perfect backward sec:	1	2	..	*k*	3	4	..	2+*k*	..	2*k*	4	..	...	*kd*-*k*+1	..	*kd*

DYNAMIC TREE: example join costs (for *k*=*d*=3)

Member number:	1	2	3	4	5	6	7	8	9	10	11	12	...	25	26	27
Perfect memory:	1	1	1	3	1	1	2	1	1	4	1	1	...	2	1	1
Tr'mit keys as required:	1	1	1	3	2	2	2	2	2	4	3	3	...	3	3	3
Perfect backward sec:	1	2	3	3	4	5	4	5	6	4	5	6	...	7	8	9

STATIC TREE: generic tree of outdegree *k* and depth *d*

Member number:	1	2	..	*k*	*k*+1	*k*+2	..	2*k*	..	k^2	k^2+1	..	...	k^d-*k*+1	..	k^d
Perfect memory:	*d*	1	..	1	2	1	1		..	1	3	..	...	2	..	1
Tr'mit keys as required:	*d*	*d*	..	*d*	*d*	*d*	*d*		..	*d*	*d*	..	...	*d*	..	*d*
Perfect backward sec:	*d*	*d*+1	..	*d*+*k*-1	*d*+1	..			..	*d*+2*k*-2	4	..	...	*kd*-*k*+1	..	*kd*

STATIC TREE: example join costs (for *k*=*d*=3)

Member number:	1	2	3	4	5	6	7	8	9	10	11	12	...	25	26	27
Perfect memory:	3	1	1	2	1	1	2	1	1	3	1	1	...	2	1	1
Tr'mit keys as required:	3	3	3	3	3	3	3	3	3	3	3	3	...	3	3	3
Perfect backward sec:	3	4	5	4	5	6	5	6	7	4	5	6	...	7	8	9

Σχήμα 47: *Προσεγγίσεις για την αρχικοποίηση του δέντρου*

Θεωρούμε τώρα το κόστος της αρχικοποίησης. Παίρνουμε υπόψη τρεις προσεγγίσεις, σε αύξουσα σειρά κόστους, με τις γενικευμένες περιπτώσεις και τα αριθμητικά παραδείγματα που φαίνονται στο Σχήμα 47. Για καθεμία από τις τρεις προσεγγίσεις μπορούμε είτε να θεωρήσουμε ένα *στατικό* δέντρο, που έχει βάθος d υποτίθεται προκαθορισμένο είτε να θεωρήσουμε ένα *δυναμικό* δέντρο, του οποίου το βάθος μεγαλώνει όσο αυξάνεται ο αριθμός των μελών, με το βάθος να είναι 1 όταν δεν υπάρχουν περισσότερα από k μέλη, 2 όταν ο αριθμός των μελών κυμαίνεται από k + 1 μέχρι k^2 και ούτω καθεξής. Τα κόστη αρχικοποίησης για κάθε μία από τις τρεις προσεγγίσεις είναι ακολούθως:

Περίπτωση 1

Υποθέτουμε πως κάθε παραλήπτης έχει τέλεια μνήμη: Μόλις ένα δοσμένο κλειδί μεταδίδεται, οποιοσδήποτε παραλήπτης που το έχει δοθεί το κλειδί κρυπτογράφησης (ακόμα και σε επόμενο χρόνο) μπορεί να αποκρυπτογραφήσει το κωδικοποιημένο

κλειδί. Παρόλο που αυτή η υπόθεση δεν αναμένεται να είναι έγκυρη στην πράξη, παρέχει μια χρήσιμη σύγκριση σε αυτή την ανάλυση αφού έχει το χαμηλότερο κόστος αρχικοποίησης. Όπως θα φανεί παρακάτω, αντιστοιχεί επίσης σε μια χρήσιμη κατηγορία κατασκευής δέντρου. Τόσο για τα δυναμικά όσο και για τα στατικά δέντρα ο συνολικός αριθμός των κλειδιών που μεταδίδονται για να δέχονται N χρήστες στην ομάδα είναι

$$B_1 = \frac{k}{k-1}(N-1) \sim O(N) \qquad (1)$$

Περίπτωση 2

Όλα τα κλειδιά που θα χρειαστεί ένας παραλήπτης μεταδίδονται την ίδια στιγμή που ο παραλήπτης εισέρχεται στην ομάδα. Οι χρήστε δεν απαιτούν μνήμη των προηγούμενων μεταδόσεων και μπορεί ακόμα και να απενεργοποιηθούν πριν από την ένταξη τους στην ομάδα. Τα κλειδιά, για το λόγο αυτό, μπορεί να μεταδοθούν πολλές φορές, όταν διαφορετικοί χρήστες τα απαιτούν. Σε αυτή την περίπτωση, ο συνολικός αριθμός των κλειδιών που μεταδίδονται για να δέχονται N χρήστες στην ομάδα είναι $O(N\log_k N)$, με τις ακριβείς εκφράσεις για τα στατικά και δυναμικά δέντρα να είναι αντίστοιχα

$$B_{2static} = N\log_k N \qquad (2)$$

$$B_{2dynamic} = (N+1)\log_k N - \frac{N}{k-1} + \frac{1}{k-1} \qquad (3)$$

Περίπτωση 3

Επανακρυπτογράφηση σε κάθε είσοδο: Αυτό διασφαλίζει πως η τέλεια μυστικότητα προς τα πίσω διατηρείται καθώς το δέντρο αρχικοποιείται. Για τη διασφάλιση της τέλειας μυστικότητας προς τα πίσω όταν κάθε μέλος εισέρχεται στην ομάδα, δεν πρέπει μόνο το ομαδικό κλειδί να αλλάξει αλλά επίσης τα κλειδιά που ενεργοποιούν τον εισερχόμενο παραλήπτη να αποκρυπτογραφήσει προηγούμενα κλειδιά πρέπει να αλλάξουν: Αν αυτό δε συμβεί, τότε ένας μετέπειτα εισερχόμενος παραλήπτης με μνήμη μπορεί να αποκτήσει το προηγούμενο ομαδικό κλειδί και να μπορεί έτσι να αποκρυπτογραφήσει εκπομπές που συνέβησαν πριν την είσοδό του στην ομάδα. Ο

συνολικός αριθμός των κλειδιών που μεταδίδονται για να δέχονται N χρήστες είναι επίσης O($N\log_k N$), με τις εκφράσεις για τα στατικά και δυναμικά δέντρα να είναι

$$B_{3static} = \left(\frac{k+1}{2}\right) N \log_k N \tag{4}$$

$$B_{3dynamic} = \left(\frac{k+1}{2}\right) N \log_k N - \frac{N}{k-1} + \frac{k}{k-1} \tag{5}$$

3.4.3. Επιπτώσεις

Η προσέγγιση της τέλειας μνήμης έχει το χαμηλότερο κόστος αρχικοποίησης του δέντρου. Αντιστοιχεί επίσης σε ένα χρήσιμο τρόπο κατασκευής ενός multicast δέντρου: έστω μια multicast συνεδρία που ανακοινώνεται [ίσως χρησιμοποιώντας το πρωτόκολλο ανακοίνωσης συνεδρίας (Session Protocol Protocol – SAP)] και κάθε πιθανό μέλος που προσκαλείται (ή απαιτείται) να εγγραφεί προκαταβολικά. Τότε, τη στιγμή που η συνεδρία είναι υποχρεωμένη να ξεκινήσει, η πηγή γνωρίζει τον αριθμό N των μελών και κατασκευάζει το δέντρο με την εξής σειρά: Όλα τα κλειδιά χαμηλότερου επιπέδου (A,…,I, Σχήμα 47) στέλνονται κρυπτογραφημένα με το ζεύγος κλειδιών του κάθε παραλήπτη, μετά τα κλειδιά του δευτέρου επιπέδου (J,…,L, Σχήμα 48) και ούτω καθεξής. Κάθε παραλήπτης μπορεί να αποκρυπτογραφήσει κάθε κλειδί όπως λαμβάνεται και το κόστος αρχικοποίησης του δέντρου (1) είναι O(N).

Η δεύτερη προσέγγιση αντιστοιχεί σε μέλη που φτάνουν περιοδικά. Σε αυτή την περίπτωση η πηγή δεν μπορεί να υποθέσει πως ένας νεότερα εισερχόμενος παραλήπτης έχει οποιαδήποτε πληροφορία σχετική με τα κλειδιά κι όλα τα κλειδιά που απαιτούνται από κάθε παραλήπτη πρέπει να μεταδοθούν με το κόστος αρχικοποίησης να είναι O($N\log_k N$).

Το κόστος [(2), (3)] μπορεί όμως να μειωθεί αν οι εισερχόμενοι παραλήπτες ομαδοποιούνται (ίσως κάθε μερικά κλειδιά) έτσι ώστε τα κλειδιά να μεταδίδονται μαζί. Για παράδειγμα, εάν (Σχήμα 47) τα μέλη 25 και 26 εισέλθουν ξεχωριστά, στέλνονται έξι κλειδιά. Όμως, αν εισέλθουν ταυτόχρονα μόνο τέσσερα κλειδιά στέλνονται. Αυτό είναι παρόμοιο με την περιοδική επανακρυπτογράφηση [60], κι αφού εδώ κατά κύριο λόγο αρχικοποιούνται νέοι χρήστες, το απαιτούμενο σύνολο κλειδιών θα συσχετίζεται ιδιαίτερα και σημαντική εξοικονόμηση μπορεί να πραγματοποιηθεί. Το κέρδος εξοικονόμησης από την περιοδική επανακρυπτογράφηση ποσοτικοποιείται από το [65].

3.4.4. Μεταβλητότητα

Θεωρούμε τώρα το κόστος του κύκλου ζωής μιας ομαδικής σύνδεσης, που καθορίζεται σε αυτό το κομμάτι ως το άθροισμα του κόστους της αρχικοποίησης του LKH δέντρου και του κόστους της επανακρυπτογράφησης κατά τη διάρκεια της φάσης της μεταφοράς δεδομένων όταν τα GMs εισέρχονται ή αποχωρούν. Περαιτέρω, καθορίζουμε τη μεταβλητότητα α ως το μέσο αριθμό των επανακρυπτογραφήσεων ανά GM. Έτσι, μια τιμή του α=1 σημαίνει πως κατά μέσο όρο έγινε μία λειτουργία επανακρυπτογράφησης ανά GM κατά τη διάρκεια της ασφαλούς εκπομπής. Το κόστος κάθε επανακρυπτογράφησης είναι $R = k\log_k N - 1$ όταν ένα GM αποχωρεί και $R = k\log_k N$ όταν ένα GM εισέρχεται: οι συναρτήσεις αυτές έχουν μια ελάχιστη τιμή k = 3 (σημειώνουμε πως το k παίρνει μόνο ακέραιες τιμές). Όμως όταν συνυπολογίζουμε το κόστος της αρχικοποίησης και το κόστος της επανακρυπτογράφησης, η βέλτιστη τιμή του k που δίνει ένα ελάχιστος κόστος του κύκλου ζωής είναι διαφορετικό. Για κάθε προσέγγιση αρχικοποίησης, το κόστος του κύκλου ζωής ενός στατικού δέντρου είναι

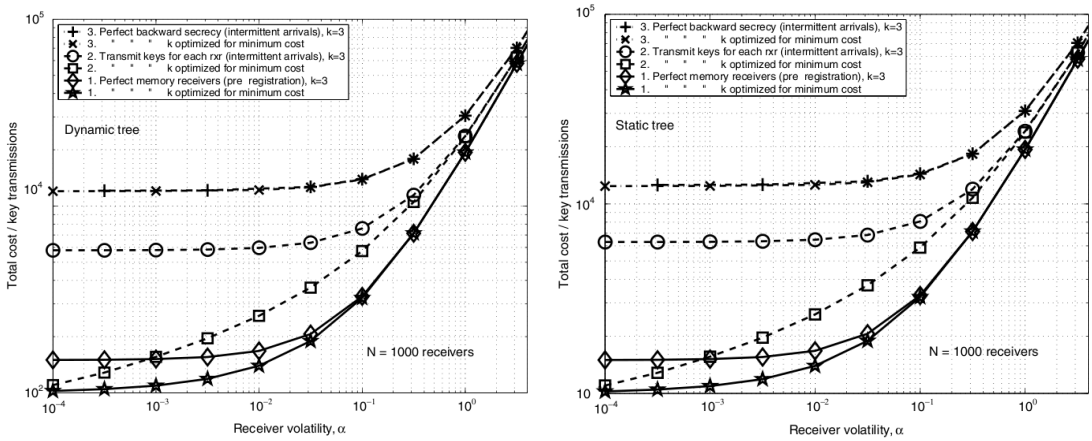
$$C_1 = B_1 + RNa = \frac{k}{k-1}(N-1) + aN(k\log_k N - 1) \qquad (6)$$

$$C_{2static} = B_{2static} + RNa = N\log_k N + aN(k\log_k N - 1) \qquad (7)$$

Για να διασφαλίσουμε τέλεια μυστικότητα προς τα πίσω, συμπεριλαμβάνουμε το κόστος επανακρυπτογράφησης στην είσοδο ενός χρήστη $k\log_k N$. Υποθέτοντας ίσο αριθμό εισόδων κι αποχωρήσεων

$$C_{3static} = B_{3static} + R'Na = \left(\frac{k+1}{2}\right) N \log_k N + aN(k \log_k N - 0.5) \qquad (8)$$

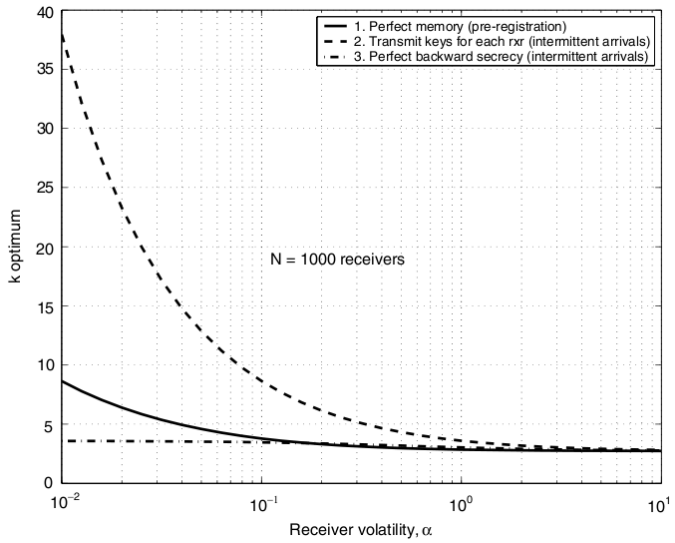
Διαφορίζουμε αυτές τις εκφράσεις και χρησιμοποιούμε τη μέθοδο Newton-Raphson για να βρούμε το ελάχιστο κόστος ως συνάρτηση του k για μια δοσμένη τιμή του α. Στο Σχήμα 48 φαίνεται κάθε κόστος ως συνάρτηση του α για δυναμικά και στατικά δέντρα.



(α) (β)

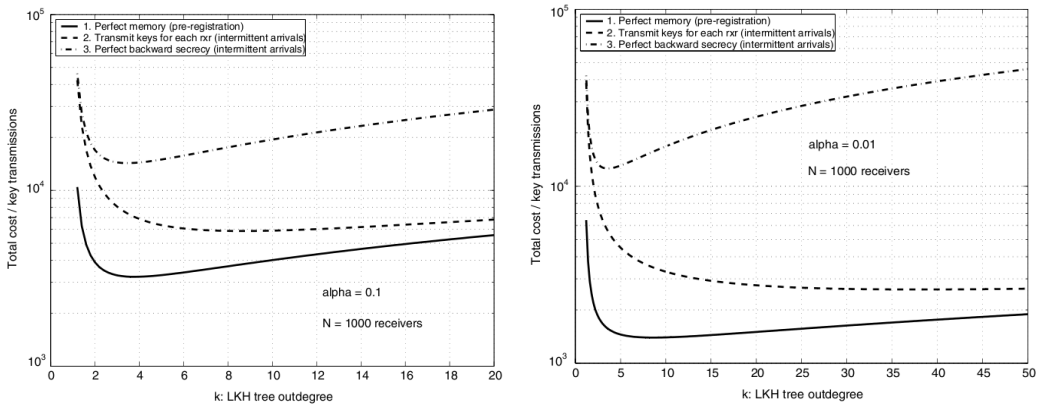
Σχήμα 48: *Κόστος κύκλου ζωής ως συνάρτηση του α. (α) Δυναμικό δέντρο (β) Στατικό δέντρο*

Για να παρουσιάσουμε την επίδραση του βελτιστοποιημένου k, σχεδιάσαμε καμπύλες τόσο για την περίπτωση ενός δέντρου με προκαθορισμένο βαθμό εξόδου k=3 όσο και για την περίπτωση που ο βαθμός εξόδου του δέντρου βελτιστοποιείται για τη δοσμένη μεταβλητότητα. Το Σχήμα 49 δείχνει ποιά είναι αυτή η βέλτιστη τιμή του k για κάθε τιμή της μεταβλητότητας α.



Σχήμα 49: *Βέλτιστη τιμή του βαθμού εξόδου k του δέντρου ως συνάρτηση της μεταβλητότητας α*

Το Σχήμα 50 δείχνει πως το συνολικό κόστος ποικίλει ως συνάρτηση του k για δύο παραδείγματα τιμών του α.



(α) (β)

Σχήμα 50*: Ευαισθησία κόστους για διάφορες τιμές της μεταβλητότητας α*

Παρατηρούμε τα εξής:

- Η προεγγραφή έχει το χαμηλότερο κόστος.
- Το κόστος της διακοπτόμενης άφιξης μπορεί να μειωθεί σημαντικά σε χαμηλή μεταβλητότητα βελτιστοποιώντας το k (οι βέλτιστες τιμές είναι k = 37 για α = 10^{-2} και k = 8 για α = 10^{-1} από N ~ 10^3 μέχρι 10^6, Σχήμα 50).
- Η μυστικότητα προς τα πίσω έχει το υψηλότερο κόστος.

- Τα κόστη του κύκλου ζωής είναι σχεδόν πανομοιότυπα για τα στατικά και δυναμικά δέντρα (στατικά δέντρα χρησιμοποιούνται για το λόγο αυτό στα σχήματα 49 και 50).
- Σε χαμηλή μεταβλητότητα, υπάρχουν σημαντικές διαφορές στο κόστος μεταξύ της βέλτιστης τιμής του k και της συμβατικής τιμής k = 2 ή k = 3, για την περίπτωση 1 (παραλήπτες με τέλεια μνήμη) και την περίπτωση 2 (μετάδοση κλειδιών τη στιγμή που ο παραλήπτης εισέρχεται στην ομάδα, Σχήμα 48).
- Για περιοδική επανακρυπτογράφηση (α >> 1), οι καμπύλες συγκλίνουν και το κόστος είναι ανεξάρτητο της προσέγγισης αρχικοποίησης.

Για παράδειγμα, χαμηλή μεταβλητότητα πληθυσμού είναι μια εταιρική συνεδρίαση με βίντεο που μεταδίδεται στους υπαλλήλους, οι οποίοι αναμένεται πως δε θα αφήσουν τη συνεδρίαση περιοδικά. Ένα σημαντικό παράδειγμα μηδενικής μεταβλητότητας είναι μια μεταφορά αρχείου: Δεν έχει νόημα να αποχωρήσει και να εισέλθει πάλι αφού τα δεδομένα θα χαθούν, Στην περίπτωση αυτή, η μεταβλητότητα είναι α = 0 και η βέλτιστη ιεραρχία κλειδιών είναι επίπεδη. Πράγματι, σε χαμηλή μεταβλητότητα η προεγγραφή στην περίπτωση 1 (= παραλήπτες με τέλεια μνήμη) και οι διακοπτόμενες αφίξεις στην περίπτωση 2 με βελτιστοποιημένο k συγκλίνουν σε ίδιο κόστος $C_1 = C_2 = N$ (Σχήμα 48).

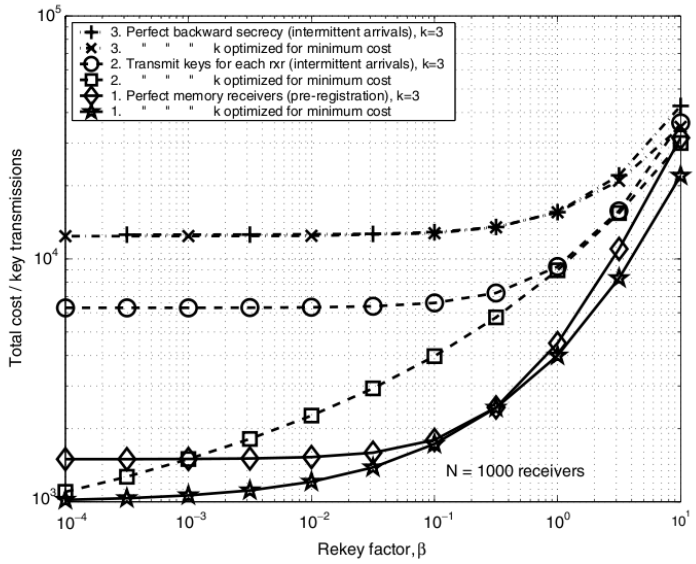
3.4.5. Ανανέωση του ομαδικού κλειδιού

Το κόστος του κύκλου ζωής μπορεί επίσης να υπολογιστεί λαμβάνοντας υπόψη την επανακρυπτογράφηση για την αποτροπή της κρυπτανάλυσης. Σε αυτή την παράγραφο θα επαναπροσδιορίσουμε το κόστος του κύκλου ζωής ως το άθροισμα του κόστους της αρχικοποίησης του LKH δέντρου και του κόστους των κανονικών ανανεώσεων GTEK κατά τη διάρκεια της φάσης της μεταφοράς δεδομένων. Έστω πως η διάρκεια ζωής μιας ομάδας είναι T κι η περίοδος ανανέωσης της ομάδας τ. Τότε, ο συνολικός αριθμός των αλλαγών του ομαδικού κλειδιού κατά τη διάρκεια ζωής της ομάδας είναι T/τ. Εάν κάθε νέο ομαδικό κλειδί κρυπτογραφείται με κάθε ένα από τα παιδιά του και μετά εκπέμπεται multicast (για παράδειγμα $\{M\}_{\Xi}$, $\{M\}_{K}$, $\{M\}_{\Lambda}$, Σχήμα 39), ο συνολικός αριθμός των κλειδιών που μεταδίδονται εξαιτίας των ανανεώσεων του ομαδικού κλειδιού είναι kT/τ.

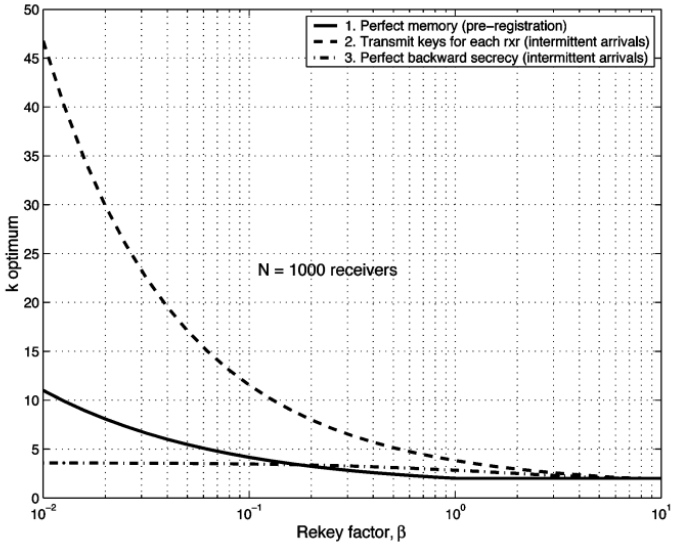
Ορίζουμε ένα κανονικοποιημένο παράγοντα επανακρυπτογράφησης β = T/Nτ. Έτσι μια ομάδα από 10^5 χρήστες με χρόνο ζωής τις 3 ώρες και περίοδο ανανέωσης του ομαδικού κλειδιού τα 10 δευτερόλεπτα, έχει $\beta = 10^{-2}$. Το κόστος της διάρκειας ζωής είναι τότε, για παράδειγμα για τέλεια μνήμη/ προεγγραφή

$$C_1^{'} = B_1 + kN\beta = \frac{k}{k-1}(N-1) + kN\beta \qquad (9)$$

το οποίο έχει ελάχιστο αναφορικά με το k όταν $k = 1 + (1/\sqrt{\beta})$. Τα κόστη του κύκλου ζωής φαίνονται ως συνάρτηση του β για στατικά δέντρα στο Σχήμα 51 και η βέλτιστη τιμή του k ως συνάρτηση του β φαίνεται στο Σχήμα 52.



Σχήμα 51: *Κόστος του κύκλου ζωής ως συνάρτηση του παράγοντα επανακρυπτογράφησης β*



Σχήμα 52: *Βέλτιστη τιμή του βαθμού εξόδου k του δέντρου ως συνάρτηση του παράγοντα επανακρυπτογράφησης β*

Σημειώνουμε τα παρακάτω:

- Για χαμηλό β, όταν ο αριθμός των επανακρυπτογραφήσεων ανά GM είναι μικρός, η βέλτιστη τιμή του k είναι >>3.
- Για υψηλό β, η επανακρυπτογράφηση με σκοπό την αποτροπή της κρυπτανάλυσης κυριαρχεί πάνω στα κόστη κατασκευής του δέντρου, κι έτσι η βέλτιστη τιμή του k είναι k = 2 (σημειώνοντας πως αυτό δεν έχει νόημα για k μικρότερο του 2).

3.5. ML-IPSec

Η ανάλυση της παραγράφου 3.3. δείχνει πως η κυκλοφορία της επανακρυπτογράφησης του δικτύου μπορεί να βελτιστοποιηθεί, αλλά όταν θεωρούμε multicast μετάδοση σε δορυφορικές ζεύξεις, η χρήση της κρυπτογράφησης της κυκλοφορίας σε επίπεδο δικτύου μπορεί να μην είναι συμβατοί με τα PEMs. Για το λόγο αυτό, θεωρούμε ένα μηχανισμό που επιτρέπει την κρυπτογράφηση της κυκλοφορίας σε επίπεδο δικτύου με δορυφορικά PEMs. Σε αυτή την παράγραφο περιγράφουμε το ML-IPSec και δείχνουμε πως υποστηρίζει την ασφάλεια multicast πάνω σε δορυφόρους παρέχοντας ταυτόχρονα αυξημένη αξιοποίηση των δορυφορικών πόρων. Στην επόμενη παράγραφο 3.5. θα

συνεχίσουμε με την περιγραφή μια λύσης που παρέχει διασυνεργασία μεταξύ του ML-IPSec και του LKH, ενώ μειώνει την κυκλοφορία της διαχείρισης κλειδιών.

3.5.1. IPSec

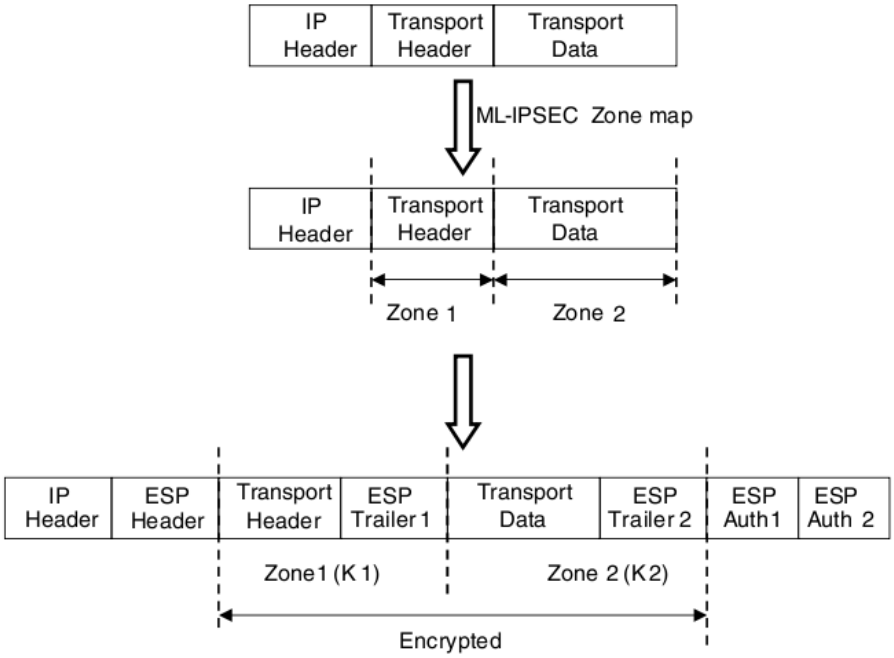
Η αρχιτεκτονική IPSec της ασφάλειας IP παρέχει τυποποιημένη ασφάλεια internet στο επίπεδο IP [13] κι υποστηρίζει υπηρεσίες ασφαλείας βασισμένες στη διαλειτουργική κρυπτογράφηση (για παράδειγμα, εμπιστευτικότητα, πιστοποίηση, ακεραιότητα κι αποδοχή αναγνώρισης). Αποτελείται από ένα πρωτόκολλο πιστοποίησης , μια επικεφαλίδα πιστοποίησης (AH) [16], ένα πρωτοκόλλο εμπιστευτικότητας ενθυλακωμένο με payload ασφάλειας (ESP) [38] και περιλαμβάνει επίσης ένα σύνδεσμο ασφάλειας internet κι ένα πρωτόκολλο διαχείρισης κλειδιών (ISAKMP) [43]. Αυτά τα πρωτόκολλα ασφάλειας είναι σχεδιασμένα και για τα δύο περιβάλλοντα, την IP έκδοση 4 (IPv4) και την IP έκδοση 6 (IPv6).

Το IPSec υποστηρίζει δύο τύπους: τη μεταφορά και το tunnel. Στην κατάσταση μεταφοράς, η επικεφαλίδα IP μεταδίδεται καθαρά και τα δεδομένα IP είναι κρυπτογραφημένα. Οι συσκευές δικτύου μπορούν έτσι να επεξεργαστούν το IP datagram. Στην κατάσταση tunnel, ολόκληρο το datagram (επικεφαλίδα και payload) είναι κρυπτογραφημένο και μια νέα επικεφαλίδα IP είναι μπροστά στο datagram. Και στις δύο καταστάσεις, η επικεφαλίδα του επιπέδου μεταφοράς είναι κρυπτογραφημένη. Έτσι αυτό περιλαμβάνει επικεφαλίδες μεταφοράς που περιέχουν την απαιτούμενη πληροφορία στην περίπτωση των δορυφορικών πυλών για να εκτελέσουν ενίσχυση της απόδοσης ή άλλες έξυπνες λειτουργίες δρομολόγησης.

Το επίπεδο μεταφοράς μπορεί να είναι είτε unicast (TCP ή UDP) είτε multicast είτε αξιόπιστο multicast. Κάποιοι βασικοί κανόνες για τις τεχνικές βελτιστοποίησης TCP που χρησιμοποιούνται στις δορυφορικές επικοινωνίες κι οι επιπτώσεις που μπορεί να έχουν στο IPSec έχουν επισημανθεί στο [66]. Όμως αν οι τεχνικές βελτιστοποίησης συμπεριλάβουν ενδιάμεσους δρομολογητές ή πύλες κι αυτά απαιτούν πρόσβαση ανάγνωσης ή εγγραφής στην επικεφαλίδα του επιπέδου μεταφοράς ή στα ενθυλακωμένα δεδομένα, το IPSec δεν μπορεί να χρησιμοποιηθεί χωρίς κάποιου είδους προσαρμογή.

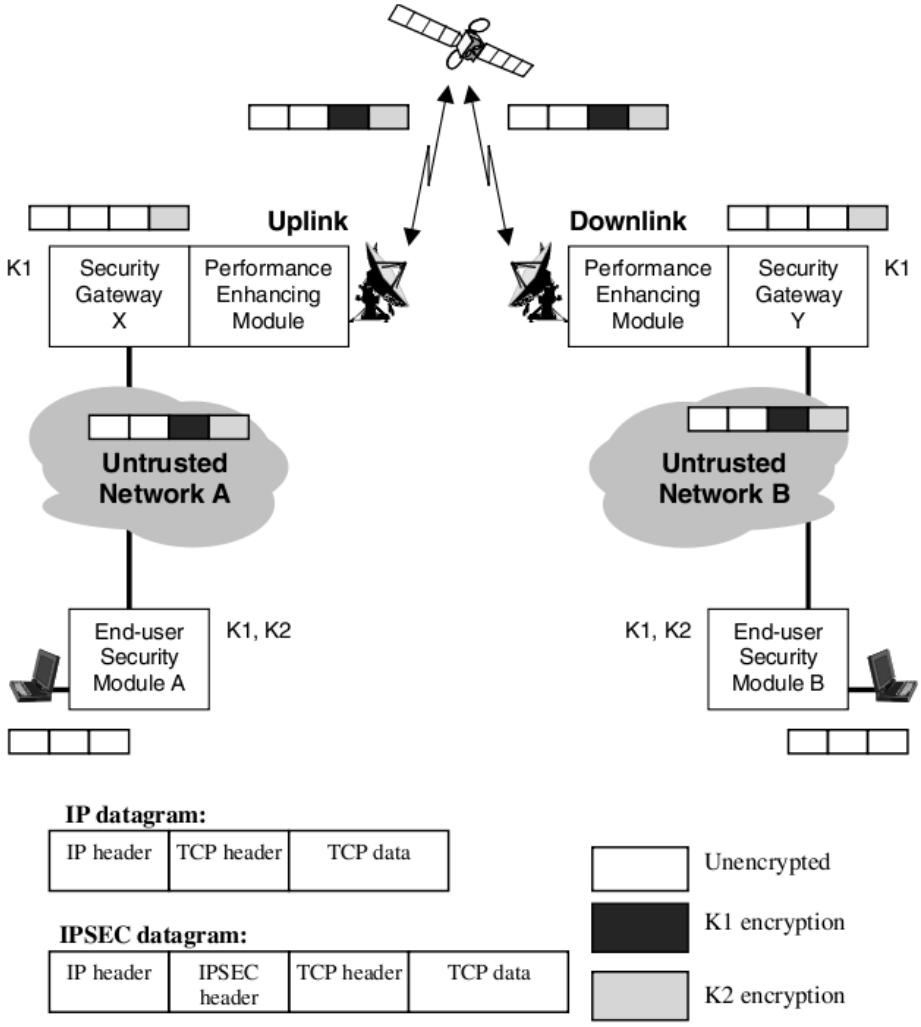
3.5.2. ML-IPSec

Εργασία σχετική με το ML-IPSec έχει γίνει, για παράδειγμα, από το Hughes Network Systems [67]. Έχει επίσης θεωρηθεί για κινητά δίκτυα [68] και η βελτιστοποίηση του multicast πάνω σε δορυφόρους είναι ακόμα αντικείμενο έρευνας. Το ML-IPSec καθορίζει μια σχέση ασφάλειας που περιλαμβάνει όχι μόνο τον αποστολέα και τον παραλήπτη μιας υπηρεσίας ασφάλειας αλλά κι επιλεγμένους ενδιάμεσους κόμβους στη ροή κυκλοφορίας. Το IP datagram χωρίζεται σε διάφορες ζώνες και διαφορετικά σχέδια ασφάλειας εφαρμόζονται σε κάθε ζώνη (παρουσιάζεται στο Σχήμα 53 για IPSec σε κατάσταση μεταφοράς). Ξεχωριστές σχέσεις ασφάλειας μπορούν να χρησιμοποιηθούν για να καλύψουν κάθε ζώνη του IP datagram και μετά να δημιουργηθεί ένας νέος τύπος συνδέσμου ασφάλειας (SA) που ονομάζεται σύνθετος SA (CSA). Έτσι στο Σχήμα 53, τα δεδομένα μεταφοράς είναι κρυπτογραφημένα χρησιμοποιώντας το κλειδί K2, ενώ η επικεφαλίδα μεταφοράς είναι κρυπτογραφημένη με το κλειδί K1.



Σχήμα 53: *Δομή του ML-IPSec datagram (κατάσταση μεταφοράς)*

3.5.3 ML-IPSec για δορυφόρους



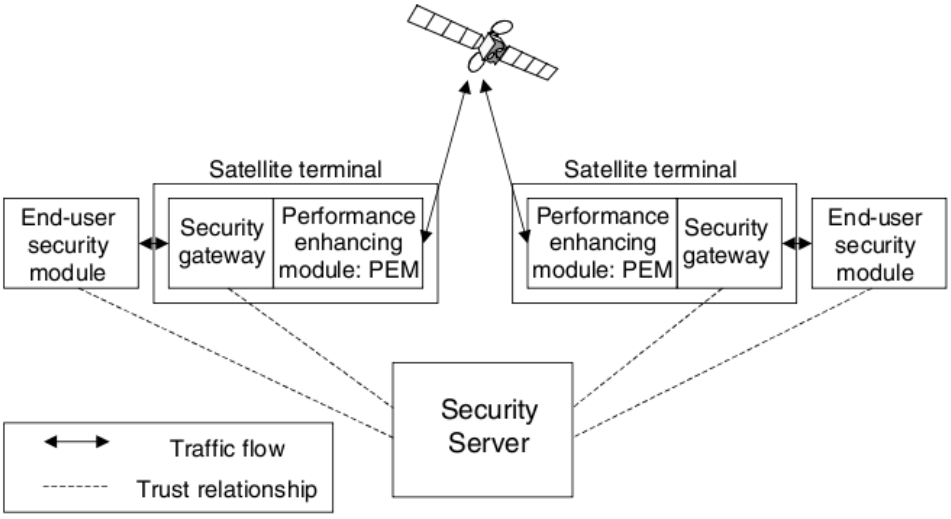
Σχήμα 54: *ML-IPSec σε ένα δορυφορικό πλαίσιο*

Το Σχήμα 54 περιγράφει τη χρήση του ML-IPSec σε ένα δορυφορικό περιβάλλον [69]. Για απλότητα, η ανάλυση περιγράφεται αρχικά από την άποψη της ασφαλούς unicast σύνδεσης. Για multicast, η ανάλυση είναι παρόμοια, παρόλο που υπάρχουν ενδεχομένως πολλές πύλες κάτω ζεύξης. Ένας χρήστης στο δίκτυο Α επιθυμεί να δημιουργήσει μια ασφαλή σύνδεση με ένα κόμβο στο δίκτυο Β. Η λειτουργική μονάδα ασφάλειας του τελικού χρήστη Α δημιουργεί συνδέσμους ασφάλειας με τη λειτουργική μονάδα ασφάλειας Β κι επίσης με τις δορυφορικές πύλες ασφάλειας Χ και Υ. Όταν ο χρήστης Α στέλνει ένα IP datagram, αυτό κρυπτογραφείται χρησιμοποιώντας το κλειδί Κ1 για να κρυπτογραφήσει την επικεφαλίδα μεταφοράς και το κλειδί Κ2 για να κρυπτογραφήσει το περιεχόμενο της μεταφοράς. Με την παραλαβή από το τερματικό της άνω ζεύξης η

επικεφαλίδα μεταφοράς μόνο αποκρυπτογραφείται από την πύλη ασφάλειας X, οποιαδήποτε λειτουργία ενίσχυσης απόδοσης, όπως είναι η συμπίεση της επικεφαλίδας ή η παραποίηση, εκτελείται κι η επικεφαλίδα μεταφοράς επανακρυπτογραφείται. Το datagram έπειτα μεταδίδεται μέσω της δορυφορικής ζεύξης, όπου η ασφάλεια εγγυάται από την κρυπτογράφηση. Στην κάτω ζεύξη του δορυφόρου (πύλη ασφάλειας Y), η επικεφαλίδα μεταφοράς αποκρυπτογραφείται χρησιμοποιώντας το κλειδί K1, κι οποιαδήποτε λειτουργία ενίσχυσης της απόδοσης μπορεί να εκτελεστεί. Η επικεφαλίδα επανακρυπτογραφείται από την πύλη ασφάλειας Y χρησιμοποιώντας το κλειδί K1 και προωθείται. Το datagram είναι πλήρως ασφαλισμένο κατά τη μεταφορά πάνω στο μη αξιόπιστο δίκτυο B. Στον τελικό χρήστη B το datagram αποκρυπτογραφείται χρησιμοποιώντας τα δύο κλειδιά K1 και K2.

Συνοπτικά, φαίνεται πως οι οντότητες ασφάλειας στο τέλος των συνδέσεων (π.χ. στην πηγή A και σε κάθε προορισμό B μιας multicast μετάδοσης) χρειάζονται και τα δύο ομαδικά κλειδιά K1 και K2. Πάρα ταύτα, ενδιάμεσες πύλες ασφάλειας που είναι υπεύθυνες για λειτουργίες ενίσχυσης της απόδοσης χρειάζονται πρόσβαση μόνο στο ομαδικό κλειδί K1 ώστε να μπορούν να διαβάσουν κι αν είναι απαραίτητο να αλλάξουν την επικεφαλίδα μεταφοράς.

Η προσέγγιση αυτή εγείρει ζητήματα εμπιστοσύνης, αφού υπάρχουν δύο διαφορετικές οντότητες οι οποίες έχουν πρόσβαση σε κοινή πληροφορία. Η πύλη ασφάλειας και το PEM είναι και τα δύο μέρη του διαχειριστή του δορυφορικού τερματικού (Σχήμα 55). Η λειτουργική μονάδα ασφάλειας του τελικού χρήστη από την άλλη πλευρά, είναι κομμάτι του τερματικού ή της εφαρμογής του τελικού χρήστη κι ελέγχεται από τον τελικό χρήστη. Η πύλη ασφάλειας χρειάζεται πρόσβαση στο κλειδί K1 κι οι τελικοί χρήστες να έχουν πρόσβαση στα κλειδιά K1 και K2. Για να επιτευχθεί αυτό, τόσο ο διαχειριστής του δορυφορικού τερματικού όσο κι ο τελικός χρήστης πρέπει να εμπιστεύονται ένα τρίτο ασφαλές μέρος (ο server ασφάλειας του Σχήματος 55). Το αξιόπιστο τρίτο μέρος είναι υπεύθυνο για την παραγωγή και διανομή κλειδιού κι αυτό δημιουργεί τις βάσεις για την ασφάλεια end-to-end μεταξύ του χρήστη και του διαχειριστή του δορυφορικού τερματικού, που στο τελευταίο δίνεται εμπιστοσύνη πρόσβασης στις επικεφαλίδες μεταφοράς.

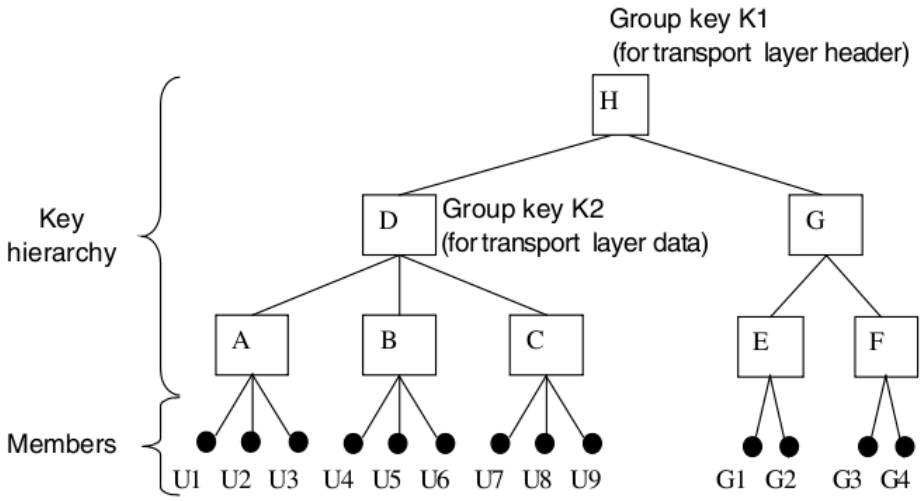


Σχήμα 55: *ML-IPSec αξιόπιστες σχέσεις*

3.6. Διασυνεργασία ML-IPSec και LKH

3.6.1. Ανάλυση

Παρουσιάζουμε τώρα μια προέκταση του LKH, που περιγράφθηκε στην παράγραφο 3.3., η οποία παρέχει ένα αποτελεσματικό και επεκτάσιμο σύστημα διαχείρισης κλειδιών για multicast ML-IPSec. Τα δύο ομαδικά κλειδιά K1 και K2 μπορούν να διαχειριστούν χρησιμοποιώντας δύο ξεχωριστά LKH δέντρα, αλλά εξοικονόμηση μπορεί να γίνει με την ένταξη τους σε μία ιεραρχία όπως ακολουθεί. Το Σχήμα 56 μας δείχνει την προτεινόμενη ιεραρχία κλειδιού για ένα σύνολο χρηστών U1 έως U9 κι ένα σύνολο ενδιάμεσων πυλών G1 έως G4. Όλοι οι χρήστες κι οι ενδιάμεσες πύλες είναι μέλη μιας multicast ομάδας. Σε αυτή την περιγραφή, οι εννέα χρήστες βρίσκονται σε ένα υποδέντρο με βαθμό εξόδου $k_U = 3$ κι οι τέσσερις πύλες είναι σε ένα υποδέντρο με βαθμό εξόδου $k_g = 2$.



Σχήμα 56: *Ολοκληρωμένο LKH δέντρο για ML-IPSec*

Η ρίζα (κλειδί H) έχει δύο παιδιά, ανεξάρτητα από τις τιμές των k_U και k_g. Όπως και στην παράγραφο 3.3., τα κλειδιά K1 και K2 μπορούν είτε να είναι τα LKH κλειδιά H και D, που φαίνονται στο Σχήμα 56, είτε μπορεί να είναι ξεχωριστά κλειδιά κρυπτογραφημένα χρησιμοποιώντας τα H και D αντίστοιχα που μεταδίδονται στα μέλη. Το ομαδικό κλειδί K1 που χρησιμοποιείται για να κρυπτογραφήσει την επικεφαλίδα του επιπέδου μεταφοράς βρίσκεται στη ρίζα του δέντρου και το ομαδικό κλειδί K2 που χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα είναι ένα από τα δύο παιδιά της ρίζας. Υπενθυμίζοντας πως στο LKH κάθε μέλος γνωρίζει μόνο τα κλειδιά που βρίσκονται στη διαδρομή του φύλλου από τον κόμβο του μέλους μέχρι τη ρίζα, φαίνεται πως οι χρήστες έχουν πρόσβαση και στα δύο K1 και K2, ενώ οι πύλες έχουν πρόσβαση μόνο στα κλειδί K1. Στην περίπτωση που μια πύλη εκτεθεί, ως μέρος της φυσιολογικής LKH επανακρυπτογράφησης μεταδίδεται το $\{K1\}_{K2}$, κι έτσι οι χρήστες μπορούν ακόμα να αποκρυπτογραφήσουν την επικεφαλίδα μεταφοράς. Για τους χρήστες που βρίσκονται πριν από την εκτεθειμένη πύλη, υποθέτεται πως υπάρχει ένα μονοπάτι ασφάλειας μέσω κάποιας από τις άλλες πύλες έτσι ώστε να μπορούν να λάβουν τη multicast κυκλοφορία.

Εάν υπάρχουν N_U χρήστες και N_G ενδιάμεσες πύλες τότε το κόστος της επανακρυπτογράφησης για αυτό το μοναδικό ολοκληρωμένο δέντρο είναι όπως

ακολουθεί παρακάτω. Για μια αναχώρηση χρήστη, υποθέτοντας ένα πλήρες δέντρο, το κόστος επανακρυπτογράφησης είναι

$$R_{U-\text{int}\,egrated} = k_U \log_{k_U} N_U + 1 \tag{10}$$

Για αναχώρηση της πύλης, το κόστος επανακρυπτογράφησης είναι

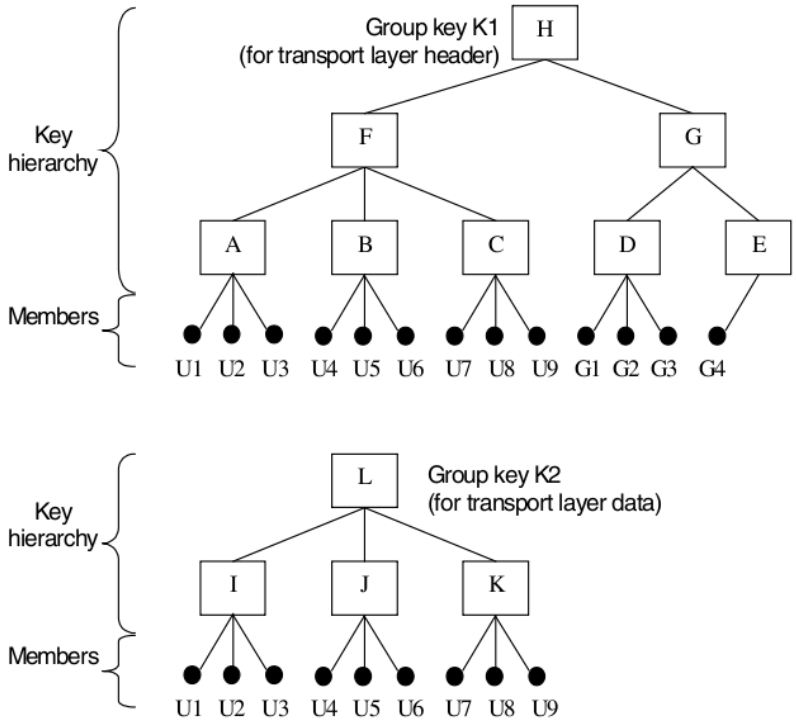
$$R_{G-\text{int}\,egrated} = k_G \log_{k_G} N_G + 1 \tag{11}$$

Αυτό συγκρίνεται με το κόστος επανακρυπτογράφησης για δύο ξεχωριστά δέντρα (Σχήμα 57), όπως ακολουθεί. Το συνδυασμένο LKH δέντρο για το κλειδί K1 έχει N_U + N_G μέλη και βαθμό εξόδου k_{comb}. Το LKH δέντρο για το K2 έχει N_U μέλη και υποθέτουμε πως ο βαθμός εξόδου του παραμένει k_U. Τότε, για μια αναχώρηση χρήστη, το κόστος επανακρυπτογράφησης και για τα δύο κλειδιά K1 και K2 είναι

$$R_{U-se\pi erate} = \{k_{comb} \log_{k_{comb}} (N_U + N_G) - 1\} + \{k_U \log_{k_U} N_U - 1\} \tag{12}$$

και για μια αναχώρηση πύλης, το κόστος επανακρυπτογράφησης (για την επανακρυπτογράφηση μόνο του K1) είναι

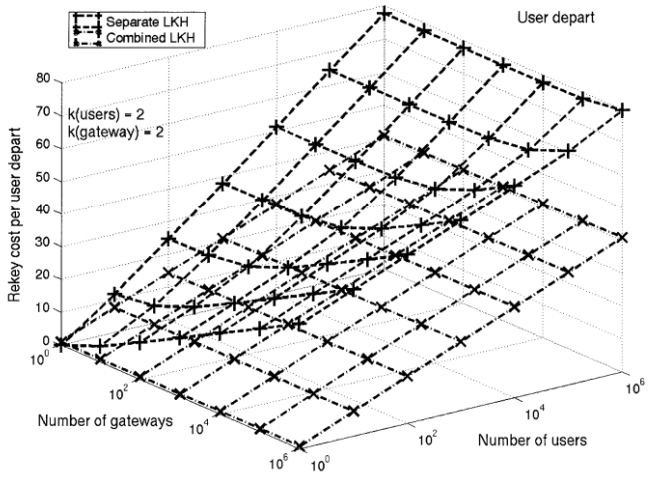
$$R_{U-se\pi erate} = k_{comb} \log_{k_{comb}} (N_U + N_G) - 1 \tag{13}$$



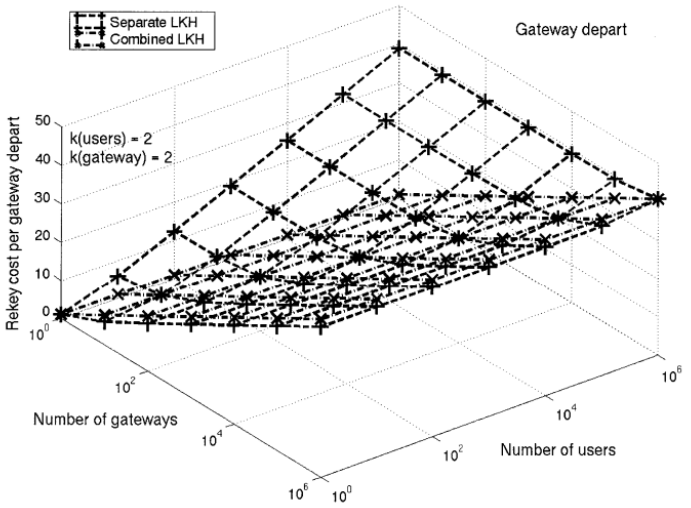
Σχήμα 57: *Ξεχωριστά LKH δέντρα για την επικεφαλίδα μεταφοράς και τα δεδομένα*

3.6.2. Επιπτώσεις

Τα κόστη επανακρυπτογράφησης για μια αναχώρηση χρήστη και για μια αναχώρηση πύλης φαίνονται αντίστοιχα στα Σχήμα 58 και 59. Αυτά δείχνουν πως για επανακρυπτογράφηση χρήστη, το κόστος είναι σχεδόν το μισό για τιμές $N_U \geq N_G$ και μειώνεται ακόμα περισσότερο στην πολύ απίθανη περίπτωση που ο αριθμός των πυλών ξεπεράσει τον αριθμό των χρηστών. Για αναχώρηση πύλης, η εξοικονόμηση του ολοκληρωμένου LKH δέντρου συγκριτικά με το ξεχωριστό κόστος της επανακρυπτογράφησης LKH είναι εξαιρετικά υψηλή για $N_U >> N_G$, δηλαδή όταν υπάρχει σχετικά μικρός αριθμό πυλών.



Σχήμα 58: *Διασυνεργασία ML-IPSec και LKH: Κόστος επανακρυπτογράφησης κατά την αναχώρηση χρήστη*

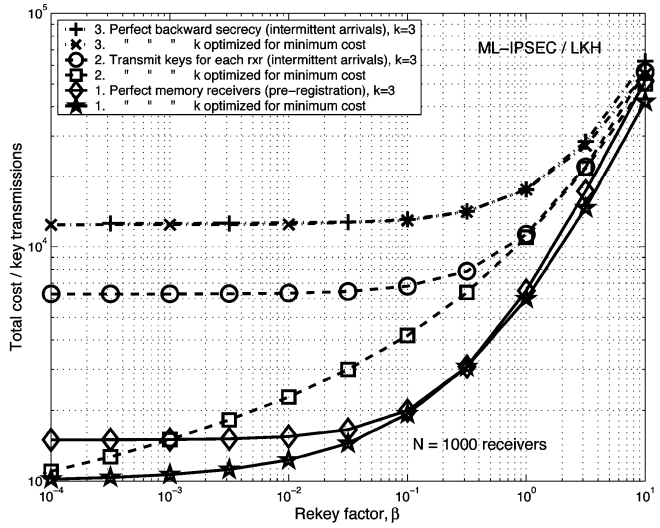


Σχήμα 59: *Διασυνεργασία ML-IPSec και LKH: Κόστος επανακρυπτογράφησης κατά την αναχώρηση πύλης*

Οι πύλες συνήθως αναμένεται να είναι λιγότερο ευμετάβλητες σε σχέση με τους χρήστες. Στην περίπτωση αυτή, ο βέλτιστος βαθμός εξόδου του υποδέντρου του χρήστη μπορεί να επιλεχθεί χρησιμοποιώντας την ανάλυση που περιγράφθηκε στην παράγραφο 3.3. χρησιμοποιώντας το βαθμό εξόδου του υποδέντρου του χρήστη να είναι k_U.

Η επανακρυπτογράφηση για την ανανέωση του ομαδικού κλειδιού μπορεί είτα να αλλάξει το κλειδί δεδομένων μεταφοράς K2, είτε να αλλάξει και τα δύο κλειδιά, K1 και

K2. Στην πρώτη περίπτωση, η ανάλυση της παραγράφου 3.3. και τα κόστη του κύκλου ζωής της επανακρυπτογράφησης που δίνονται στο Σχήμα 51 είναι εφαρμόσιμα για δέντρο από N_U χρήστες και βαθμό εξόδου k_U. Για την τελευταία περίπτωση, ο αριθμός των κλειδιών που μεταδίδονται για κάθε επανακρυπτογράφηση είναι $2 + k_U$, και το κόστος του κύκλου ζωής φαίνεται στο Σχήμα 60.



Σχήμα 60: *ML-IPSec και LKH: Κόστος του κύκλου ζωής ως συνάρτηση του παράγοντα επανακρυπτογράφησης β*

3.7. Επίλογος

Οι υπηρεσίες δικτύου που βασίζονται σε δορυφόρους παρουσιάζουν σημαντικά ζητήματα ασφάλειας και συγκεκριμένα την απαίτηση για ιδιωτικότητα και την ανάγκη για αποτελεσματική χρήση των δορυφορικών πόρων. Η εργασία αυτή προσφέρει δύο συνεισφορές για την περιοχή των multicast υπηρεσιών.

Στην πρώτη συνεισφορά, θεωρούμε τα κόστη του κύκλου ζωής της επανακρυπτογράφησης για multicast ομάδες που χρησιμοποιούν LKH για τη διαχείριση κλειδιών. Έχουμε δείξει πως η προεγγραφή μπορεί να μειώσει το κόστος αρχικοποίησης του ιεραρχικού δέντρου. Όταν η προεγγραφή δεν είναι εφικτή, η περιοδική είσοδος μπορεί τότε να μειώσει το κόστος. Για εφαρμογές με χαμηλή μεταβλητότητα α, όπου το

ποσοστό των χρηστών που εισέρχονται και εγκαταλείπουν την ομάδα κατά τη διάρκεια της σύνδεσης είναι χαμηλό, υπάρχει ένας βέλτιστος βαθμός εξόδου του δέντρου που ποικίλει ανάλογα με τη μεταβλητότητα και δίνει το ελάχιστο κόστος του κύκλου ζωής του κλειδιού. Παρόμοια, ο βέλτιστος βαθμός εξόδου ποικίλει ανάλογα με τον παράγοντα επανακρυπτογράφησης β που αντικατοπτρίζει τον αριθμό των ανανεώσεων του ομαδικού κλειδιού. Αυτή η ανάλυση, για το λόγο αυτό, ελαχιστοποιεί την κυκλοφορία της διαχείρισης κλειδιού που απαιτείται στον δορυφόρο κι έχει επίσης μεγάλη εφαρμογή στα επίγεια δίκτυα.

Στην δεύτερη συνεισφορά, παρουσιάσαμε μια λύση διασυνεργασίας μεταξύ του ML-IPSec και του LKH που υποστηρίζει την εφαρμογή των PEMs στους δορυφόρους. Στην προτεινόμενη προσέγγιση, οι τελικοί χρήστες τοποθετούνται στο ένα κλαδί του LKH δέντρου και τα δορυφορικά τερματικά ή πύλες στο άλλο κλαδί. Το κλειδί ρίζα του LKH δέντρου μπορεί να χρησιμοποιηθεί για την ασφάλεια της επικεφαλίδας μεταφοράς κι ένα κλειδί κλαδί ενεργεί ως GTECH κι ασφαλίζει το περιεχόμενο των δεδομένων για τους τελικούς χρήστες. Το προτεινόμενο σχέδιο είναι επεκτάσιμο, κατά του ότι η προσπάθεια επανακρυπτογράφησης ποικίλει με το logN κι είναι αποτελεσματικό, σε ότι δεδομένου ότι για τις αναχωρήσεις χρηστών ο αριθμός των επανακρυπτογραφήσεων που απαιτούνται είναι στο μισό σε σχέση με τις δύο ξεχωριστές ιεραρχίες δέντρου.

Παραπομπές:

[1] ETSI TR 102 287: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); IP Interworking over satellite; Security aspects.".
[2] ETSI TS 102 292: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; Functional architecture for IP interworking with BSM networks".
[3] ETSI TS 102 460: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); Address Management at SI-SAP".
[4] IETF RFC 3547: "The Group Domain of Interpretation".
[5] IETF RFC 4535: "Group Secure Association Key Management Protocol".
[6] ETSI TR 101 985: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP over Satellite".
[7] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN-SEC); Threat and Risk Analysis".
[8] IETF RFC 2748: "The COPS (Common Open Policy Service) Protocol".
[9] IETR RFC 3084: "COPS Usage for Policy Provisioning (COPS-PR)".
[10] IETF RFC 2865: "Remote Authentication Dial In User Service (RADIUS)".
[11] IETF RFC 3588: "Diameter Base Protocol".
[12] IETF RFC 3162: "RADIUS and IPv6".
[13] IETF RFC 2401: “Security Architecture for the Internet Protocol"
[14] IETF RFC 3022: "Traditional IP Network Address Translator (Traditional NAT)".
[15] IETF RFC 3715: "IPsec-Network Address Translation (NAT) Compatibility Requirements".
[16] IETF RFC 2402: "IP Authentication Header".
[17] IETR RFC 3103: "Realm Specific IP: Protocol Specification".
[18] IETF RFC 3104: "RSIP Support for End-to-end IPsec".
[19] IETF RFC 3948: "UDP Encapsulation of IPsec ESP Packets".
[20] IETF RFC 3947: "Negotiation of NAT-Traversal in the IKE2".
[21] IETF RFC 0793: "Transmission Control Protocol".
[22] IETF RFC 3135: "Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations".
[23] IETF RFC 3449: "TCP Performance Implications of Network Path Asymmetry".
[24] IABG final report. ESA project: "IP security over satellites". Contract No. 15555/01/NL/US. 2002.
[25] IETF RFC 4109: "Algorithms for Internet Key Exchange version 1 (IKEv1)".
[26] IETF RFC 4301: "Security Architecture for the Internet Protocol".
[27] IETF RFC 4326: "Unidirectional Lightweight Encapsulation (ULE) for Transmission of IP Datagrams over an MPEG-2 Transport Stream (TS)".
[28] ETSI TS 102 462: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM); QoS Functional Architecture".
[28] IETF RFC 4081: "Security Threats for Next Steps in Signaling (NSIS)".

[30] IETF RFC 3893: "Session Initiation Protocol (SIP) Authenticated Identity Body (AIB) Format".
[31] IETF RFC 3329: "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".
[32] IETF RFC 4014: "Remote Authentication Dial-In User Service (RADIUS) Attributes Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Information Option".
[33] ETSI TR 101 984: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; Services and Architectures".
[34] ATM Forum Technical Committee af-sec-0100.002 (March 2001): "ATM Security Specification Version 1.1".
[35] ETSI TS 103 197: "Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt".
[36] ETSI EN 301 192: "Digital Video Broadcasting (DVB); DVB specification for data broadcasting".
[37] ETSI EN 301 790: "Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems".
[38] IETF RFC 2406: "IP Encapsulating Security Payload (ESP)".
[39] IETF RFC 2246: "The TLS Protocol Version 1.0".
[40] Open Mobile Alliance OMA-Download-DRM-v1-0-20020905-C: "Digital Rights Management Version 1.0" Version 05-September-2002,
http://www.openmobilealliance.org/tech/docs/index.htm#DRM.
[41] IETF RFC 822: "Standard for the format of ARPA Internet text messages".
[42] IETF RFC 2015: "MIME Security with Pretty Good Privacy (PGP)".
[43] IETF RFC 2408: "Internet Security Association and Key Management Protocol (ISAKMP)".
[44] IETF RFC 2407: "The Internet IP Security Domain of Interpretation for ISAKMP".
[45] IETF RFC 2409: "The Internet Key Exchange".
[46] ETSI TS 102 293: "Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) services and architectures; IP Interworking over satellite; Multicast group management; IGMP adaptation".
[47] IETF RFC 2627: "Key Management for Multicast: Issues and Architectures".
[48] IETF draft-duquer-fmke-00.txt: "The Flat Multicast Key Exchange protocol".
[49] ETSI TS 102 189-3: "Satellite Earth Stations and Systems (SES); Regenerative Satellite Mesh - A (RSM-A) air interface; MAC/SLC layer specification; Part 3: SLC layer".
[50] ETSI. DTS/SES-00081: "Satellite Earth Stations and Systems (SES); BSM Air Interface Specification; Common Air interface specification; Satellite Independent Service Access Point SI-SAP".
[51] J. Snoeyink, S. Suri, and G. Varghese, “A lower bound for multicast key distribution,” in Proc. IEEE INFOCOM, Apr. 2001, pp. 422–431.
[52] R. Poovendran and J. S. Baras, “An information-theoretic approach for design and analysis of rooted-tree-based multicast key management schemes,” IEEE Trans. Inform. Theory, vol. 47, pp. 2824–2834, Nov. 2001.

[53] H. Orman, “The OAKLEY key determination protocol,” IETF, RFC2412, Nov. 1998.
[54] J. Arrko et al., “MIKEY: Multimedia Internet Keying,” IETF Internet Draft, work-in-progress, draft-ietf-msec-mikey-06.txt, Feb. 2003, expires Aug. 2003.
[55] M. Baugher et al., “The group domain of interpretation,” IETF Internet Draft, work-in-progress, draft-ietf-msec-gdoi-08.txt, May 2003, expires Nov. 2003.
[56] H. Harney, A. Schuett, and A. Colegrove, “GSAKMP Light,” IETF Internet Draft, work-in-progress, draft-ietf-msec-gsakmp-light-sec-01.txt, July 2002, expires Dec. 2002.
[57] B. Schneier, Applied Cryptography. New York: Wiley, 1996.
[58] S. Mittra, “Iolus: A framework for scalable secure multicasting,” in Proc. SIGCOMM, 1997, pp. 277–288.
[59] C. K. Wong, M. Gouda, and S. S. Lam, “Secure group communications using key graphs,” IEEE/ACM Trans. Networking, vol. 8, pp. 16–30, Feb. 2000.
[60] S. Setia et al., “Kronos: A scalable group re-keying approach for secure multicast,” in Proc. IEEE Symp. Research Security Privacy, May 2000, pp. 215–228.
[61] D. Balenson et al., “Key management for large dynamic groups: One-way function trees and amortized initialization,” IETF Draft, work-in-progress, draft-balenson-groupkeymgmt-oft-00.txt, Feb. 1999.
[62] M. J. Moyer et al., “A survey of security issues in multicast communications,” IEEE Network, vol. 13, pp. 12–23, Nov. 1999.
[63] R. Canetti et al., “Multicast security: A taxonomy and some efficient constructions,” in Proc. IEEE INFOCOM, 1999, pp. 708–716.
[64] M. J. Moyer et al., “Maintaining Balanced Key Trees for Secure Multicast,” IETF Internet-Draft, work-in-progress, draft-irtf-smug-key-tree-balance-00.txt, June 25, 1999.
[65] Y. R. Yang et al., “Reliable group rekeying: A performance analysis,” Comp. Commun. Rev., vol. 31, pp. 27–38, 2001.
[66] G. Noubir and L. von Allmen, “Security issues in Internet protocols over satellite links,” in Proc. 50th Vehicular Tech. Conf., 1999, pp.2726–2730.
[67] Y. Zhang, “Multi-layer Internet security for satellite & wireless networks,” Hughes Res. Lab., HRL Tech. Rep. 99-611, Dec. 1, 1999.
[68] N. Assaf et al., “Interworking between IP security and performance enhancing proxies for mobile networks,” IEEE Commun. Mag., vol. 40, pp. 138–144, May 2000.
[69] M. Annoni et al., “Interworking between multi-layer IPSEC and secure multicast services over GEO satellites,” presented at the COST-272 Symp., Thessaloniki, Greece, June, 20–21 2002. Doc. TD-02-016-P.