ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ

ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Ασφάλεια Δικτύων Κινητών Επικοινωνιών : Πρωτόκολλα και Επιθέσεις Ασφάλειας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αντώνιος Ι. Καλτσάς

Επιβλέπων: Αθανάσιος Δ. Παναγόπουλος

Αναπληρωτής Καθηγητής Ε.Μ.Π

Αθήνα, Ιούνιος 2017

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ

ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΣΥΣΤΗΜΑΤΩΝ ΜΕΤΑΔΟΣΗΣ ΠΛΗΡΟΦΟΡΙΑΣ

ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΥΛΙΚΩΝ

Ασφάλεια Δικτύων Κινητών Επικοινωνιών : Πρωτόκολλα και Επιθέσεις Ασφάλειας

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Αντώνιος Ι. Καλτσάς

Επιβλέπων: Αθανάσιος Δ. Παναγόπουλος

Αναπληρωτής Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την Ιουνίου 2017

.....	.....	.....
Αθ. Παναγόπουλος Αν. Καθηγητής Ε.Μ.Π	Π. Κωττής Καθηγητής Ε.Μ.Π	Γ. Φικιώρης Αν. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούνιος 2017

.....

Αντώνιος Ι. Καλτσάς

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

ΠΕΡΙΛΗΨΗ

Στο πλαίσιο της συγκεκριμένης διπλωματικής εργασίας παρουσιάζονται θέματα ασφάλειας των Δικτύων Κινητών Επικοινωνιών. Έτσι, πέρα από το τεχνικό κομμάτι, επικεντρωνόμαστε σε θέματα που αφορούν το δικαίωμα της ελεύθερης επικοινωνίας, το απόρρητο της επικοινωνίας. Στα παραπάνω θέματα αναφερόμαστε στο πρώτο κεφάλαιο μαζί με κάποιες έννοιες όπως η ιδιωτικότητα των δικτύων κινητών επικοινωνιών και κατά πόσο κάποιος χρήστης δικτύου κινητής τηλεφωνίας μπορεί να την διατηρήσει.

Στο δεύτερο κεφάλαιο, δίνουμε βάση σε ζητήματα που αφορούν την ασφάλεια και το απόρρητο σε κυψελωτά δίκτυα GSM και δίκτυα του 802.11. Ειδικότερα, εξειδικεύουμε τη μελέτη μας σε θέματα όπως η πιστοποίηση ενός χρήστη, η κρυπτογράφηση των στοιχείων ενός συνδρομητή και σε γενικότερα στοιχεία και χαρακτηριστικά ασφαλείας ενός ασύρματου δικτύου.

Στο τρίτο κεφάλαιο περνάμε σε ένα θέμα αιχμής και αναφερόμαστε στο Internet of Things. Έτσι, εστιάζουμε το ενδιαφέρον μας στη ραγδαία εξάπλωσή του και πώς το IoT μπορεί να επηρεάσει τη ζωή μας σε υψηλό βαθμό. Ακολουθεί στο ίδιο κεφάλαιο μία εκτενής αναφορά στα πρωτόκολλα που διέπουν τη λειτουργία του IoT με βαρύτητα στα θέματα ασφαλείας του IoT.

Όλο το τέταρτο κεφάλαιο είναι αφιερωμένο σε θέματα που αφορούν την Επικινδυνότητα σε Κρίσιμες Επικοινωνιακές Υποδομές (Critical Infrastructure-Critical Information Infrastructure). Ορίζονται οι κρίσιμες επικοινωνιακές υποδομές, τα πλεονεκτήματα και τα μειονεκτήματά τους, πότε αυτές θεωρούνται ευάλωτες, πότε παραβιάζονται. Ταυτόχρονα, γίνεται μία αναφορά σε θέματα όπως η αποτίμηση της επικινδυνότητας και στα επίπεδα που η τελευταία διεξάγεται. Παράλληλα, περιγράφονται μία σειρά από πλαίσια διαχείρισης επικινδυνότητας και τα βήματά τους.

Τέλος στο πέμπτο κεφάλαιο εστιάζουμε στις πολιτικές ασφαλείας στα δίκτυα υπολογιστών μαζί με μία αναφορά στη διαχείριση ασφαλείας του Ελληνικού Στρατού.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Δίκτυα Κινητών Επικοινωνιών, Ασύρματα Δίκτυα, GSM, 802.11, IoT, 6LoWPAN, Core COAP, Κρίσιμες Επικοινωνιακές Υποδομές.

SUMMARY

In the context of this thesis, the security issues of Mobile Communications Networks are presented. Thus, beyond the technical part, we focus on issues concerning the right of free communication, the confidentiality of communication. The above issues are referred to the first chapter along with some concepts such as the privacy of mobile communications networks and whether a mobile network user can maintain it.

In the second chapter, we focus on security and privacy issues in GSM cellular networks and 802.11 networks. Specifically, we specialize our study on issues such as user authentication, encryption of subscriber data, and more general security features of a wireless network.

In chapter three, we are talking about a very up-to-date topic and we refer to the Internet of Things. So we focus our attention on its rapid expansion and how IoT can affect our lives to a high degree. An extensive reference to the protocols governing the operation of IoT with regard to IoT security issues follows in the same chapter.

Fourth chapter is devoted to Critical Infrastructure and Critical Information Infrastructure. Critical communication infrastructures, their advantages and disadvantages are defined, when they are considered vulnerable and when they are violated. At the same time, a reference is made to issues such as risk assessment and the level at which it is being conducted. In addition to this, a series of risk management frameworks and their steps are outlined.

Finally, in the fifth chapter we focus on security policies on computer networks along with a reference to the security management of the Greek Army.

KEY WORDS: Mobile Communications Networks, Wireless Networks, GSM, 802.11, IoT, 6LoWPAN, Core COAP, Critical Communication Infrastructures.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ……...σελ.9
1.1 Το δικαίωμα της ελεύθερης επικοινωνίας……...σελ.9
1.2 Η προστασία του απορρήτου της επικοινωνίας……..σελ.9
1.3 Ζητήματα απορρήτου και ιδιωτικότητας στο τομέα των ηλεκτρονικών επικοινωνιών στη σύγχρονη εποχή……σελ.12
Βιβλιογραφία-Αναφορές……...σελ.16
ΚΕΦΑΛΑΙΟ 2: ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ GSM ΚΑΙ 802.11…….σελ.17
2.1Τα βασικότερα ζητήματα ασφαλείας του GSM……...σελ.17
2.1.1 Προστασία της ταυτότητας του συνδρομητή……σελ.19
2.1.2 Πιστοποίηση Ταυτότητας συνδρομητή…….....σελ.20
2.1.3 Η κρυπτογράφηση των δεδομένων του συνδρομητή……σελ.23
2.1.4 Κάρτα SIM και Έλεγχος IMEI…….σελ.25
2.2 Τα βασικότερα ζητήματα ασφαλείας του 802.11…….σελ.27
2.2.1 Εμπιστευτικότητα – Ιδιωτικότητα…….....σελ.29
2.2.2 Ακεραιότητα…….σελ.29
2.2.3 Αυθεντικοποίηση……...σελ.30
2.2.4 Active Attacks……...σελ.31
2.2.4.1 Masquerading…….....σελ32
2.2.4.2 Replay……....σελ.32
2.2.4.3 Message Modification……...σελ.32
2.2.4.4 Denial-of-Service……...σελ.32
2.2.5 Passive Attacks…….σελ.33
2.2.5.1 Eavesdropping……...σελ.33
2.2.5.2 Traffic Analysis…….....σελ.33
2.3 Απειλές Ασφαλείας……...σελ.33
2.3.1 Απώλεια εμπιστευτικότητας……..σελ.33
2.3.2 Απώλεια Ακεραιότητας…….....σελ.36
2.3.3 Απώλεια Διαθεσιμότητας Δικτύου……σελ.36
2.3.4 Άλλοι κίνδυνοι Ασφαλείας……σελ.37
Βιβλιογραφία-Αναφορές……...σελ.38
ΚΕΦΑΛΑΙΟ 3: ΤΟ IOT (INTERNET OF THINGS)……...σελ.39
3.1. Ορισμός του IoT…….....σελ.39
3.2. Το IoT στη ζωή μας……....σελ.40
3.3. Κύρια χαρακτηριστικά του IoT……..σελ.41
3.4 Ασφάλεια……σελ.43
3.4.1 Τα πρωτόκολλα του IoT……...σελ.43
3.4.2 Απαιτήσεις Ασφαλείας……σελ.46
3.4.3 Παρουσίαση του πρωτοκόλλου IoT……σελ.46
3.4.3.1 Επίπεδο PHY του IEEE 802.15.4……..σελ.48
3.4.3.2 Επίπεδο MAC του IEEE 802.15.4…….....σελ.50
3.4.3.3 Δομή SuperFrame……..…σελ.51
3.4.3.4 Μοντέλο Μεταφοράς Δεδομένων……σελ.52
3.4.3.5 Μηχανισμοί CSMA-CA……....σελ.54
3.4.3.6 Κατανάλωση Ισχύος……σελ.54
3.4.4 Τύποι Κόμβων Δικτύου στο 802.15.4……σελ.55
3.4.5 Δομή Πλαισίων……....σελ.56
3.4.6 Αξιοπιστία και Κρυπτογράφηση……σελ.58
3.5 Routing Over Low-power and Lossy networks (RoLL)…….....σελ.58

3.6 Το πρωτόκολλο CoAP…….σελ.60
3.7 Το πρωτόκολλο DTLS (Datagram Transport Layer Security)……....σελ.61
Βιβλιογραφία-Αναφορές:……..σελ.63
ΚΕΦΑΛΑΙΟ 4: ΕΠΙΚΙΝΔΥΝΌΤΗΤΑ ΣΕ ΚΡΊΣΙΜΕΣ ΕΠΙΚΟΙΝΩΝΙΑΚΈΣ ΥΠΟΔΟΜΈΣ (CRITICAL INFRASTRUCTURE-CRITICAL INFORMATION INFRASTRUCTURE)……..σελ.65
4.1 Εισαγωγή-Γενικά…….σελ.65
4.2 Κρίσιμες Υποδομές και Εξαρτήσεις……σελ.68
4.3 Πότε αποτυγχάνουν οι κρίσιμες υποδομές;…….σελ.70
4.4 Προστασία Κρίσιμων Υποδομών για να αποφευχθεί η αποτυχία τους……...σελ.71
4.5 Προστασία Κρίσιμων Υποδομών και Διαδίκτυο……σελ.73
4.6 Ανθεκτικότητα Κρίσιμων Υποδομών……..σελ.73
4.7 Λόγοι Αναγκαιότητας στις κρίσιμες υποδομές……...σελ.76
4.8 Πλαίσια και πολιτικές ανθεκτικότητας……...σελ.78
4.9 Αποτίμηση Επικινδυνότητας σε Κρίσιμες Υποδομές…….σελ.80
4.9.1 Σύγχρονες Προσεγγίσεις……..σελ.80
4.9.2 Βασική Προσέγγιση Αποτίμησης Επικινδυνότητας…….σελ.89
4.10 Μοντέλα αλληλοεξαρτήσεων……σελ.93
Βιβλιογραφία-Αναφορές……...σελ.96
ΚΕΦΑΛΑΙΟ5: ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝσελ.100
5.1 Η οργανωτική ασφάλεια……σελ.101
5.2 Περιεχόμενα Πολιτικής Ασφαλείας……..σελ.102
5.3 Οδηγίες για τη σωστή εφαρμογή της πολιτικής ασφαλείας……..σελ.106
5.4 Οι πολιτικές ασφαλείας στο στρατιωτικό περιβάλλον……..σελ.109
5.4.1 Εθνικός Κανονισμός Ασφαλείας……σελ.111
5.4.2 Στρατιωτικός Κανονισμός 80-20……σελ.113
5.4.3 Διαχείριση Ασφαλείας Ελληνικού Στρατού……...σελ.116
Βιβλιογραφία-Αναφορές:……σελ.118

ΚΕΦΑΛΑΙΟ 1: ΕΙΣΑΓΩΓΗ

1.1 Το δικαίωμα της ελεύθερης επικοινωνίας

Η ύπαρξη και η δράση ενός ανθρώπου εντός της κοινωνίας προϋποθέτει την επικοινωνία με τους άλλους. Η ζωή ενός ανθρώπου είναι στενότατα και αναπόδραστα συνδεδεμένη με την επικοινωνία.

Η ανάπτυξη της προσωπικότητας, η συμμετοχή στην κοινωνική, οικονομική, πολιτική ζωή, δικαιώματα που προστατεύονται από το Σύνταγμα προϋποθέτουν την ανεμπόδιστη ανταλλαγή ιδεών, πληροφοριών, μηνυμάτων.

Αλλά και αυτή η ιδιωτική ζωή του ανθρώπου περιλαμβάνει τη σχέση του με τον περιβάλλοντα κόσμο, τις ιδιωτικές σχέσεις του με άλλους ανθρώπους. Οι σχέσεις αυτές προϋποθέτουν, συνεπάγονται ή επιβάλλουν την επικοινωνία υπό τη μορφή της αποστολής μηνυμάτων (επιστολές, τηλεφωνήματα, φαξ, ηλεκτρονικά μηνύματα). Η ίδια η εσωτερική ολοκλήρωση ενός ανθρώπου προϋποθέτει την ελευθερία της επικοινωνίας, την ελευθερία στην παροχή και πρόσληψη πληροφοριών.

Η ικανότητα της επικοινωνίας και της συμμετοχής έχει από τη μια πλευρά ως προϋπόθεση και ταυτόχρονα συνέπεια την πρόσβαση στις πηγές της πληροφόρησης, την ελευθερία της πληροφορίας. Από την άλλη πλευρά η ικανότητα αυτή περιορίζεται ή και αναιρείται, εάν δεν διασφαλίζεται η εμπιστευτικότητα των επικοινωνιών, το γνωστό σε όλους απόρρητο.

Ο εμπιστευτικός χαρακτήρας που περιβάλλει μία επικοινωνία διευκολύνει την άσκηση και άλλων συνταγματικών ελευθεριών όπως π.χ. του ιδιωτικού βίου, της ελευθερίας της γνώμης ή ακόμη και της επαγγελματικής ελευθερίας.

Η καταγραφή προσωπικών πληροφοριών και η καταγραφή ή παρακολούθηση των επικοινωνιών προσβάλλει την αξία του ανθρώπου και την ελευθερία του αλλά και δυσχεραίνει ουσιαστικά την απόλαυση και άλλων δικαιωμάτων καθώς και την άσκηση και άλλων συνταγματικά προστατευόμενων ελευθεριών [1].

1.2 Η προστασία του απορρήτου της επικοινωνίας

Το απόρρητο των επικοινωνιών από την πλευρά του νομοθέτη αποτελεί την εξέλιξη του παραδοσιακού απορρήτου των επιστολών. Συγκεκριμένο άρθρο του Συντάγματος έχει μία ευρεία και ανοιχτή διατύπωση: Αναφέρεται στο απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο

τρόπο και το προσδιορίζει ως απόλυτα απαραβίαστο. Συνεπώς, πρόκειται για θεμελιώδες ατομικό δικαίωμα, η προστασία του οποίου αποτελεί υποχρέωση της πολιτείας, με υψηλό βαθμό προτεραιότητας για τις κρατικές υπηρεσίες και τα όργανά της.

Αντικείμενο της προστασίας δεν είναι το μήνυμα καθεαυτό, το οποίο προστατεύεται από την ελευθερία έκφρασης και διάδοσης της γνώμης, αλλά το απόρρητο του μηνύματος. Η προστασία του απορρήτου αφορά όχι μόνο το παραδοσιακό μέσο των επιστολών αλλά κάθε μορφή ιδιωτικής επικοινωνίας, ανεξάρτητα εάν πρόκειται για επικοινωνία με προσωπικό ή επαγγελματικό χαρακτήρα. Δεν υπάρχει διαβάθμιση στην προστασία. Το κρίσιμο στοιχείο είναι να πραγματώνεται η επικοινωνία, υπό συνθήκες εμπιστευτικότητας.

Η προστασία του απορρήτου αποσκοπεί στη διασφάλιση της ελεύθερης προσωπικής επικοινωνίας, το οποίο όμως δεν διαγράφει μόνο τα όρια της ιδιωτικής σφαίρας που προστατεύει η έννομη τάξη αλλά εγγυάται και το δικαίωμα των ατόμων στην ελεύθερη επικοινωνία με τους άλλους, ως προϋπόθεση αυτόνομων εκδηλώσεων, αποφάσεων και δράσεων και προϋποθέτει δύο τουλάχιστον πρόσωπα, τον αποστολέα και τον παραλήπτη του μηνύματος.

Το απαραβίαστο των επικοινωνιών που κατοχυρώνει το Σύνταγμα σημαίνει ότι απαγορεύεται κάθε ενέργεια των δημόσιων αρχών προς λήψη γνώσεως ή κοινοποίηση σε τρίτους (αδιάφορο εάν πρόκειται για δημόσιες αρχές ή ιδιώτες) του περιεχομένου ή και αυτού του γεγονότος της επικοινωνίας. Το άρθρο 19 προστατεύει την ελεύθερη επικοινωνία και ανταπόκριση. Η προστασία αφορά όχι μόνο τα γραπτά μηνύματα, αλλά και οποιαδήποτε άλλη μορφή ιδιωτικής, δηλαδή μη δημόσιας, επικοινωνίας. Έτσι προστατεύονται το απόρρητο οι επιστολές, τα τηλεγραφήματα, τα τηλεφωνήματα, τα φαξ, τα e-mails.

Μάλιστα για την προστασία του απορρήτου των επικοινωνιών, η Πολιτεία έχει αναλάβει και υλοποιήσει μια σειρά από σχετικές πρωτοβουλίες για την ενίσχυση του επιπέδου προστασίας του εν λόγω δικαιώματος και τη θεσμική του θωράκιση, πρωτίστως, στο ίδιο το Σύνταγμα.

Ειδικότερα, κατά την αναθεώρηση του 2001 ο συντακτικός νομοθέτης συμπεριέλαβε στα άρθρα 19 και 101Α διατάξεις, σύμφωνα με τις οποίες με

εκτελεστικό του Συντάγματος νόμο συγκροτείται Ανεξάρτητη Διοικητική Αρχή για την προστασία του εν λόγω δικαιώματος. Στο πλαίσιο αυτό, με το νόμο 3115/2003, ιδρύθηκε η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών, με σκοπό την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών.

Περαιτέρω, σημειώνεται ότι, προς τις ανωτέρω και λοιπές συναφείς συνταγματικές προβλέψεις και επιταγές εναρμονίστηκε και η κοινή νομοθεσία και σε ότι αφορά το ζήτημα της άρσης του απορρήτου των επικοινωνιών, πάντοτε υπό τις εγγυήσεις της αρμόδιας δικαστικής Αρχής. Ειδικότερα, η άρση του απορρήτου των τηλεφωνικών συνδιαλέξεων επιτρέπεται μόνο στις περιπτώσεις, που ορίζονται ρητά, στις διατάξεις του άρθρου 3 ν. 2225/1994 «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις», όπως ο νόμος αυτός τροποποιήθηκε, συμπληρώθηκε και ισχύει καθώς και του π.δ. 47/2005, ήτοι για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων [2].

Πέραν αυτών στο ν. 3674/2008 με τον τίτλο «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» έχουν συμπεριληφθεί πρόσθετες, προστατευτικές του εν λόγω εννόμου αγαθού, ρυθμίσεις (κατάρτιση ειδικού σχεδίου πολιτικής ασφάλειας παρόχου, καταγραφή διαχειριστικών λειτουργιών, έλεγχος των συστημάτων του παρόχου από την Α.Δ.Α.Ε. κ.λ.π.). Από το σύνολο των διατάξεων του εν λόγω νόμου προκύπτει ξεκάθαρα η πρόθεση της πολιτείας να ενισχύσει σημαντικά και αποτελεσματικά το θεσμικό πλαίσιο που περιβάλλει τη διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών.

Επιπλέον, με τον ως άνω νόμο επήλθαν τροποποιήσεις στις διατάξεις του Ποινικού Κώδικα. Ειδικότερα, αφενός μεν προστέθηκε το άρθρο 292 Α «Εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών» αφετέρου δε τροποποιήθηκε το άρθρο 370 Α «Παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας». Με την τελευταία αυτή τροποποίηση αυστηροποιήθηκαν οι ποινικές κυρώσεις των παραβατών των διατάξεων του εν λόγω άρθρου, καθότι μετετράπησαν από πλημμεληματικές σε κακουργηματικές και η δίωξη των σχετικών εγκλημάτων ασκείται αυτεπαγγέλτως. Παράλληλα, προβλέφθηκε η επιβολή

διοικητικών κυρώσεων ως και η έγερση αστικών αξιώσεων σε βάρος των παραβατών της σχετικής νομοθεσίας.

Επιπροσθέτως, ιδρύθηκε στην Ελληνική Αστυνομία, ειδική Υπηρεσία για την πρόληψη και καταστολή των εγκλημάτων παραβίασης του απορρήτου των ηλεκτρονικών επικοινωνιών, η οποία συνεργάζεται με την Α.Δ.Α.Ε. και τελεί υπό την εποπτεία του αρμόδιου Εισαγγελέα [3].

1.3 Ζητήματα απορρήτου και ιδιωτικότητας στο τομέα των ηλεκτρονικών επικοινωνιών στη σύγχρονη εποχή

Η συνεχώς αυξανόμενη πρόοδος της τεχνολογίας, ιδίως στο τομέα των ηλεκτρονικών επικοινωνιών και η δυνατότητα αντλήσεως πληροφοριών από την επεξεργασία των δεδομένων που προκύπτουν από τη χρήση ηλεκτρονικών δικτύων και επικοινωνιών, θέτει σε κίνδυνο τον ιδιωτικό βίο του ατόμου.

Κίνδυνοι υφίστανται και είναι υπαρκτοί τόσο για τον ιδιωτικότητα των χρηστών τηλεπικοινωνιακών δικτύων, όσο και χρηστών του διαδικτύου (κυβερνοχώρου).

Συχνά περιπτώσεις υποκλοπών και παραβίασης του απορρήτου των επικοινωνιών τόσο στον τηλεπικοινωνιακό τομέα όσο και στο διαδίκτυο, έρχονται στο φως της δημοσιότητας. Η υποκλοπή μπορεί να εκδηλώνεται και να περιλαμβάνει την ακρόαση, έλεγχο ή επιτήρηση του περιεχομένου των επικοινωνιών και την παροχή του περιεχομένου των δεδομένων, είτε άμεσα, μέσω της πρόσβασης και χρήσης των συστημάτων πληροφοριών, είτε έμμεσα μέσω της χρήσης ηλεκτρονικής συνακρόασης ή συσκευών παγίδευσης με τεχνικά μέσα [4].

Μια άλλη διάσταση που αναδεικνύεται από την χρήση των δικτύων ηλεκτρονικών επικοινωνιών είναι η αυτόματη παραγωγή και αποθήκευση δεδομένων, η επεξεργασία των οποίων αποσκοπεί, κατ' αρχήν, στη μετάδοση της επικοινωνίας, καθιστά δε περαιτέρω δυνατή τη δημιουργία ενός ηλεκτρονικού ή ψηφιακού πορτραίτου του κάθε χρήστη, με βάση τις πληροφορίες που αντλούνται από την επεξεργασία των δεδομένων αυτών.

Από την αποκάλυψη των προσωπικών στοιχείων, αλλά και από την επεξεργασία των τηλεφωνικών κλήσεων ή των προσβάσεων του χρήστη σε

ιστοσελίδες του διαδικτύου, είναι δυνατόν να δημιουργηθεί ένα ψηφιακό αρχείο, αντίστοιχο με αυτό του τηλεφωνικού καταλόγου, από το οποίο μπορεί κανείς να αντλήσει προσωπικές πληροφορίες για το άτομο και να εξάγει μια σειρά από συμπεράσματα (για τις γνωριμίες, τις φιλικές, επαγγελματικές σχέσεις του χρήστη κ.τ.λ.)

Επιπλέον, από τη χρήση των υπηρεσιών της κινητής τηλεφωνίας, αλλά και του ίδιου του κινητού τηλεφώνου πέραν των ανωτέρω, είναι δυνατόν να πληροφορηθούμε τη γεωγραφική θέση του χρήστη, την κατεύθυνσή του καθώς και τη μετάβαση και παραμονή του στην αλλοδαπή.

Η τεχνολογία, ιδιαίτερα στο πλαίσιο της παροχής υπηρεσιών κινητής τηλεφωνίας, έχει εξελιχθεί τόσο, ώστε δικαιολογημένα υποστηρίζεται ότι η κατοχή ενός κινητού τηλεφώνου ταυτίζεται με την ύπαρξη ενός «κατασκόπου στη τσέπη» του χρήστη εξαιτίας των πληροφοριών που μπορούν να αποκτηθούν από τα δεδομένα που προκύπτουν από τη χρήση της συσκευής, καθιστώντας παράλληλα ευάλωτη την ιδιωτική ζωή του χρήστη.

Θετική προοπτική βέβαια της ως άνω δυνατότητας αποτελεί η αξιοποίηση της για τον εντοπισμό και τη σύλληψη επικίνδυνων εγκληματιών ή την υπεράσπιση κατηγορουμένου (λ.χ. άλλοθι, απόδειξη αναληθών ισχυρισμών).

Σε πολλές περιπτώσεις η έννοια της προστασίας των προσωπικών δεδομένων ταυτίζεται με την έννοια της προστασίας της ιδιωτικής ζωής ή αλλιώς της ιδιωτικότητας, καθώς τα προσωπικά δεδομένα αποτελούν στοιχεία της ιδιωτικότητας ενός ατόμου. Ο όρος ιδιωτικότητα αναφέρεται ως “το δικαίωμα στην απομόνωση” (the right to be let alone) και σχετίζεται με την απομόνωση, την μυστικότητα και την αυτονομία. Αλλιώς, η ιδιωτικότητα χρησιμοποιείται για να περιγράψει την κατάσταση του να μπορεί κάποιος να είναι μόνος και να μην μπορεί κάποιος να τον δει ή να τον ακούσει, καθώς και την κατάσταση του να είναι κάποιος ελεύθερος από τη δημόσια προσοχή. Ο όρος αυτός χρησιμοποιείται στις ΗΠΑ χωρίς διάκριση από την έννοια των προσωπικών δεδομένων για ζητήματα που άπτονται της προστασίας τους. Ο όρος προσωπικά δεδομένα (personal data) χρησιμοποιείται κυρίως στην ευρωπαϊκή νομική ορολογία, στην πράξη όμως οι δύο έννοιες συχνά ταυτίζονται [5].

Η διαδικτυακή ιδιωτικότητα (internet privacy) αναφέρεται στο δικαίωμα της διατήρησης της προσωπικής ιδιωτικότητας σε σχέση με την αποθήκευση, μετατροπή, διάθεση σε τρίτους και επίδειξη πληροφοριών οι οποίες αφορούν ένα άτομο, μέσω του διαδικτύου. Η ιδιωτικότητα στο διαδίκτυο αποτελεί μέρος της λεγόμενης ιδιωτικότητας των πληροφοριών (information privacy), η οποία αναφέρεται στη γενική απαίτηση των ατόμων να μην είναι διαθέσιμα τα προσωπικά τους δεδομένα σε άλλα άτομα και οργανισμούς. Στην περίπτωση που ένα τρίτο μέρος κατέχει τα προσωπικά δεδομένα κάποιου ατόμου, η ιδιωτικότητα αναφέρεται στη δυνατότητα του ατόμου να ασκεί ένα σημαντικό βαθμό ελέγχου σχετικά τη χρήση των προσωπικών του δεδομένων [6].

Τα προσωπικά δεδομένα στο διαδίκτυο ορίζονται ως οποιαδήποτε πληροφορία σχετίζεται με την ταυτοποίηση ενός ατόμου. Στα προσωπικά δεδομένα περιλαμβάνονται:

- Περιεχόμενο το οποίο έχει δημιουργηθεί από τον χρήστη, συμπεριλαμβανομένων των προσωπικών ιστολογίων (blogs) και ο σχολιασμός, οι φωτογραφίες, τα βίντεο

- Δραστηριότητα ή δεδομένα συμπεριφοράς, συμπεριλαμβανομένων των αναζητήσεων στον ιστό, τις διαδικτυακές αγορές. τα ποσά και τον τρόπο πληρωμής

- Κοινωνικά δεδομένα, συμπεριλαμβανομένων των επαφών και φίλων στα μέσα κοινωνικής δικτύωσης

- Δεδομένα τοποθεσίας, στα οποία περιλαμβάνονται η διεύθυνση κατοικίας, και ο προσδιορισμός της θέσης και τοποθεσίας του ατόμου (GPS), μέσω του κινητού τηλεφώνου ή της διεύθυνσης IP (IP address).

- Δημογραφικά δεδομένα στα οποία συμπεριλαμβάνεται η ηλικία, το φύλο, η φυλή, το εισόδημα, οι σεξουαλικές προτιμήσεις, οι πολιτικές πεποιθήσεις, κλπ.

- Αναγνώριση δεδομένων επίσημης φύσης, όπως το όνομα, οι οικονομικές πληροφορίες και οι αριθμοί τραπεζικών λογαριασμών, ο αριθμός μητρώου ασφαλισμένων και τα ποινικά μητρώα

Ωστόσο, η ταξινόμηση των διαδικτυακών προσωπικών δεδομένων μπορεί να γίνει και σύμφωνα με τα κοινωνικά δίκτυα [7]:

● Δεδομένα εξυπηρέτησης (service data), τα οποία καταχωρούνται για τη δημιουργία ενός λογαριασμού (π.χ. το όνομα, η διεύθυνση και ο αριθμός πιστωτικής κάρτας)

● Δεδομένα γνωστοποίησης (disclosed data), τα οποία καταχωρούνται εθελοντικά από τον χρήστη

● Εμπιστευτικά δεδομένα (entrusted data), για παράδειγμα τα σχόλια που γίνονται στις καταχωρήσεις άλλων προσώπων

● Συμπτωματικά δεδομένα (incidental data), τα οποία αφορούν κάποιον συγκεκριμένο χρήστη αλλά έχουν καταχωρηθεί από άλλο πρόσωπο

● Δεδομένα συμπεριφοράς (behavioural data), τα οποία περιλαμβάνουν πληροφορίες για τη δραστηριότητα των χρηστών μιας ιστοσελίδας και δύναται να χρησιμοποιηθούν για τη δημιουργία στοχοποιημένης διαφήμισης

● Συναγόμενα δεδομένα (inferred data), τα οποία προκύπτουν από τα δεδομένα

γνωστοποίησης κάποιου, το προφίλ ή τις διαδικτυακές του δραστηριότητες.

Τα προσωπικά δεδομένα συχνά κατηγοριοποιούνται και σύμφωνα με τη χρήση τους. Είναι κοινή τακτική η διάκριση ανάμεσα στα δεδομένα που συλλέγονται από έναν συγκεκριμένο φορέα προκειμένου να χρησιμοποιηθούν για μια τρέχουσα - προσωρινή διαδικτυακή εργασία και σε αυτά που τα οποία αποθηκεύονται για χρήση και ανάλυση και/ή πωλούνται σε τρίτα μέρη.

Στη δεύτερη κατηγορία, τα είδη των εμπλεκόμενων προσωπικών δεδομένων δύναται να ταξινομηθούν βάση της φύσης τους σε δύο μεγάλες κατηγορίες: από τη μία πλευρά, στις πληροφορίες που δεν αναμένεται να αλλάξουν δραματικά κατά την πάροδο του χρόνου, οι οποίες αναφέρονται ως στατικές προσωπικές πληροφορίες (static private information). Τέτοιες πληροφορίες αφορούν το οικονομικό ιστορικό, το ιατρικό ιστορικό, τα προσωπικά πιστεύω και η διασύνδεση με ομάδες ανθρώπων, καθώς και τα προσωπικά αρχεία. Από την άλλη πλευρά περιλαμβάνονται οι πληροφορίες οι οποίες αλλάζουν δραματικά με την πάροδο του χρόνου, παρόλα αυτά όμως δύναται να συλλεχθούν και να αναλυθούν κατά τρόπο που να μπορεί να δημιουργηθεί ένα καλά ενημερωμένο προφίλ του ατόμου. Οι πληροφορίες αυτές αναφέρονται ως δυναμικές προσωπικές πληροφορίες, όπως το ιστορικό δραστηριότητας (στο διαδίκτυο) και το ιστορικό περιεχομένου [8], [9], [10].

Βιβλιογραφία-Αναφορές:

[1] Ζαχαριουδάκη Δ., Εργασία με τίτλο: «Προστασία Προσωπικών Δεδομένων», Εθνική Σχολή Δημόσιας Διοίκησης, Μάρτιος 2001.

[2] http://www.hellenicparliament.gr/Vouli-ton-Ellinon/To-Politevma/Syntagma/ [Πρόσβαση: 27/3/17].

[3] Δαγτόγλου Π. (1991)., "Ατομικά Δικαιώματα", Συνταγματικό Δίκαιο, τεύχος. Β', Αθήνα 1991.

[4] Τμήμα Πληροφορικής Ιονίου Πανεπιστήμιο, Επιστημονικές Σημειώσεις Ασφάλειας, διαθέσιμες στην ηλεκτρονική διεύθυνση: di.ionio.gr/~emagos/security/Simeioseis-Asfaleia%20Part%20B.pdf [Πρόσβαση: 27/3/17].

[5] http://www.ldoceonline.com/ [Πρόσβαση: 27/3/2017]

[6] Clarke Roger "Information privacy on the Internet" (1998). http://www.rogerclarke.com/DV/IPrivacy.html [Πρόσβαση 27/3/2017]

[7] Schneier (2010), SecuritySchneier on Security, A blog covering security and security technology. http://www.schneier.com/blog/archives/2009/11/a_taxonomy_of_s.html [Πρόσβαση: 27/3/2017]

[8] Huaiqing Wang, Matthew K.O. Lee, and Chen Wang (1998): "Consumer Privacy Concerns about Internet Marketing". Communications of the Acm, 1998/Vol. 41, No. 3

[9] Μήτρου, Λ. Προστασία προσωπικών δεδομένων στο πεδίο των ηλεκτρονικών επικοινωνιών, Σημειώσεις - Διαλέξεις στο Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων, Πανεπιστήμιο Αιγαίου. 2012.

[10] Η προστασία της Ιδιωτικότητας στην Πληροφορική και τις Επικοινωνιες σε : Κ. Λαμπρινουδάκης, Στεφ. Γκρίτζαλης, Λίλιαν Μήτρου, Σωκρ. Κάτσικας, «Προστασία της Ιδιωτικότητας & Τεχνολογίες Πληροφορικής και Επικοινωνιών». s.l. : Παπασωτηρίου, 2010.

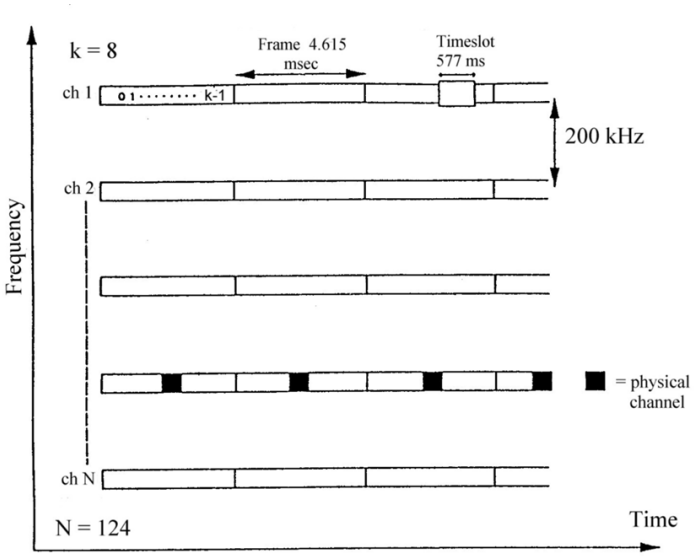
ΚΕΦΑΛΑΙΟ 2: ΖΗΤΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ GSM ΚΑΙ 802.11

2.1 Τα βασικότερα ζητήματα ασφαλείας του GSM

Το μειονέκτημα της ύπαρξης μεγάλου αριθμού αναλογικών συστημάτων στην Ευρώπη μαζί με την ανάγκη εξυπηρέτησης του διαρκώς αυξανόμενου αριθμού χρηστών και την καθιέρωση συμβατότητας των δικτύων κινητών επικοινωνιών με το σταθερό δίκτυο που ολοένα ψηφιακοποιείται , οδήγησαν τη CEPT στη σύσταση της ομάδας " Group Special Mobile " με σκοπό τη σύνταξη προδιαγραφών για ένα νέο σύστημα . Το έργο της ομάδας αυτής κατέληξε στο σύστημα GSM (Global System for Mobile communications) .

Το νέο σύστημα σχεδιάστηκε κυρίως για τη μετάδοση ομιλίας και λιγότερο για τη μετάδοση δεδομένων (fax , e-mail , αρχεία) και αναμενόταν να παρέχει καλύτερη ποιότητα ήχου , πανευρωπαϊκή περιαγωγή (roaming) , εφαρμογές με χαμηλότερο κόστος , δυνατότητα για αυξημένη φασματική απόδοση , υψηλή ευελιξία και ανοικτή αρχιτεκτονική που θα επιτρέπει την εισαγωγή νέων υπηρεσιών στο άμεσο μέλλον . Κρίθηκε , έτσι , απαραίτητο να ενσωματωθούν στο σύστημα και όλοι εκείνοι οι αναγκαίοι μηχανισμοί ασφαλείας προκειμένου αυτό να προστατευτεί σε ενδεχόμενες ανεπιθύμητες επιθέσεις .

Το GSM χρησιμοποιεί Πολλαπλή Πρόσβαση με Διαίρεση Χρόνου (TDMA) και Διαίρεση Συχνότητας (FDMA) . Έτσι , μπορούν να λαμβάνουν χώρα την ίδια χρονική στιγμή και στην ίδια συχνότητα πολλές συνδιαλλαγές χρησιμοποιώντας διαφορετικές χρονικές σχισμές (timeslots) , όπως φαίνεται στο σχήμα που ακολουθεί . Ένα πλαίσιο (frame) έχει διάρκεια 4.615ms και αποτελείται από οκτώ τέτοιες χρονοσχισμές (577ms διάρκεια η καθεμία) . Οι συχνότητες εκπομπής και λήψης είναι διαφορετικές με αποτέλεσμα οι μεταδόσεις της άνω ζεύξης (κινητό προς σταθμό βάσης) και της κάτω ζεύξης (σταθμό βάσης προς κινητό) να είναι ταυτόχρονες [1].



TDMA / FDMA

Το εύρος ζώνης του GSM είναι 25 MHz και παρέχει 125 φέρουσες , που καθεμία έχει εύρος ζώνης 200 kHz . Βέβαια λόγω φαινομένων παρεμβολής από άλλα συστήματα , η πρώτη φέρουσα συνήθως δε χρησιμοποιείται οπότε ο αριθμός των καναλιών μειώνεται σε 124 . Με δεδομένο ότι αντιστοιχούν 8 χρήστες ανά κανάλι , μπορούν να υπάρξουν περίπου 1000 πραγματικά κανάλια για ομιλία ή δεδομένα . Η χωρητικότητα αυτή μπορεί να διπλασιαστεί αν πέσει στο μισό ο ρυθμός κωδικοποίησης φωνής . Η περιοχή συχνοτήτων για την άνω ζεύξη είναι 890 MHz έως 915 MHz (με τις φέρουσες να βρίσκονται σε συχνότητες 890.2 , 890.4 ...) , ενώ για την κάτω ζεύξη είναι 935 MHz έως 960 MHz (με φέρουσες αντίστοιχα τις συχνότητες 935.2 , 935.4 ...) . Δηλαδή το εύρος διαχωρισμού εκπομπής και λήψης είναι 45 MHz.

Η διαμόρφωση , τώρα , που χρησιμοποιεί το GSM είναι η GMSK . Ο τύπος αυτός διαμόρφωσης θεωρείται ανθεκτικός σε παρεμβολές " συγγενούς καναλιού " , ενώ παράλληλα εξασφαλίζει ότι το μέγιστο ποσοστό της ακτινοβολούμενης ισχύος συγκεντρώνεται πλησίον της κεντρικής συχνότητας χωρίς να διασπείρεται σε μεγάλο εύρος . Ο ρυθμός εκπομπής είναι 270.833 Kbps (ισομοιράζεται ανάμεσα στους 8 χρήστες , οπότε αντιστοιχεί στον καθένα ρυθμός 33.85 Kbps) , ενώ για τη διόρθωση σφαλμάτων χρησιμοποιείται συνελικτική κωδικοποίηση με ρυθμό κωδικοποίησης 13 Kbps ή 6.5 Kbps .

Ένα σημαντικό πρόβλημα που εμφανίζεται στο GSM είναι η διασυμβολική παρεμβολή , η οποία αντιμετωπίζεται με έναν ισοσταθμιστή Viterbi . Η παρεμβολή λόγω πολλαπλών δρόμων αντιμετωπίζεται με διαφορική λήψη , η οποία , ανάλογα με το περιβάλλον μπορεί να περιορίσει σε μεγάλο βαθμό τις διαλείψεις. Σε μερικά περιβάλλοντα , όπως π.χ. στις πόλεις , τα 200 KHz του εύρους ζώνης δεν αρκούν πλέον για την επίλυση του θέματος των πολλαπλών διαδρομών , οπότε και τα αργά κινούμενα τερματικά αντιμετωπίζουν μεγάλης διάρκειας ριπές σφαλμάτων. Η κατάσταση αυτή μπορεί να βελτιωθεί σημαντικά μεταπηδώντας συχνότητα από σχισμή σε σχισμή (frequency hopping) [2].

Τέλος , αναφορικά με τη μετάδοση , ο σταθμός βάσης κατευθύνει το κινητό να χρησιμοποιήσει την ελάχιστη ισχύ που είναι απαραίτητη για μια αξιόπιστη μετάδοση. Τόσο ο κινητός όσο και ο σταθμός βάσης χρησιμοποιούν Ασυνεχή Μετάδοση , προκειμένου το μεν κινητό να διαφυλάξει τη μπαταρία του , ο δε σταθμός βάσης να μειώσει τη διακαναλική παρεμβολή .

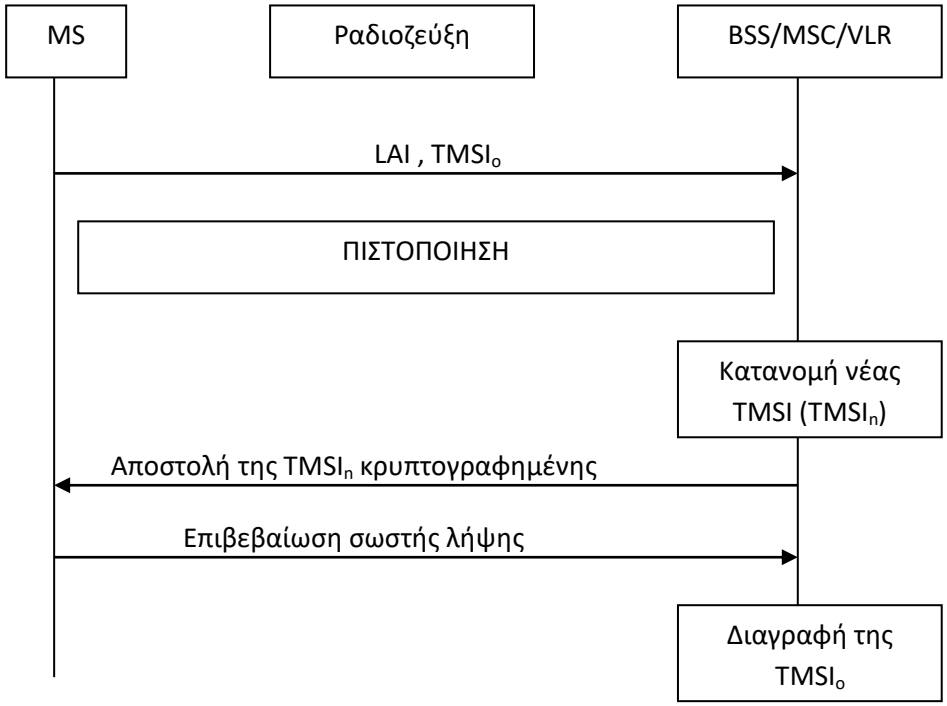
Το σύστημα ασφαλείας του GSM έχει σκοπό να παρέχει :

- Ανωνυμία στο συνδρομητή , μέσω της χρησιμοποίησης της ταυτότητας TMSI
- Πιστοποίηση της ταυτότητας του χρήστη στο δίκτυο , με τη χρήση τριπλετών .
- Κρυπτογράφηση των δεδομένων στη ραδιοζεύξη .
- Προστασία των ευαίσθητων πληροφοριών του χρήστη στην κάρτα SIM .

2.1.1 Προστασία της ταυτότητας του συνδρομητή

Με τη χρησιμοποίηση της προσωρινής ταυτότητας TMSI αποφεύγεται η συχνή εκπομπή της IMSI στη ραδιοζεύξη. Έτσι παρέχεται στο χρήστη ανωνυμία και δεν είναι δυνατή η αναγνώρισή του από κάποιον που “ακούει” το δίαυλο. Μία νέα ταυτότητα TMSI πρέπει να κατανέμεται στο κινητό από το VLR τουλάχιστον κάθε φορά που γίνεται ενημέρωση θέσης. Ο κινητός σταθμός όταν προσπαθεί να αποκτήσει πρόσβαση στο δίκτυο, χρησιμοποιεί την TMSI που του είχε τελευταία φορά κατανεμηθεί, αντί της IMSI. Το VLR βρίσκει μέσα από τους πίνακες που διαθέτει την αντιστοίχηση μεταξύ TMSI – IMSI και κατά συνέπεια τη μόνιμη ταυτότητα του κινητού . Έτσι, μετά από την επιτυχή πιστοποίηση και εγκατάσταση ενός καναλιού για επικοινωνία, το VLR καθορίζει νέα TMSI στο κινητό την οποία

και του αποστέλλει κρυπτογραφημένη. Μετά από μεταπομπή σε νέο VLR ή επαναπιστοποίηση με το ίδιο VLR , πάντα αποστέλλεται καινούρια TMSI στο MS. Τότε το τελευταίο αποθηκεύει το νέο αυτό αριθμό και διαγράφει τον προηγούμενο. Ομοίως το VLR αντιστοιχεί στην IMSI τη νέα TMSI που έχει καθορίσει, διαγράφοντας την παλιά από τη βάση δεδομένων του. Στο σχήμα που ακολουθεί φαίνεται η κατανομή καινούριας ταυτότητας TMSI στο MS από το VLR μετά από επιτυχή διαδικασία ενημέρωσης θέσης [3].

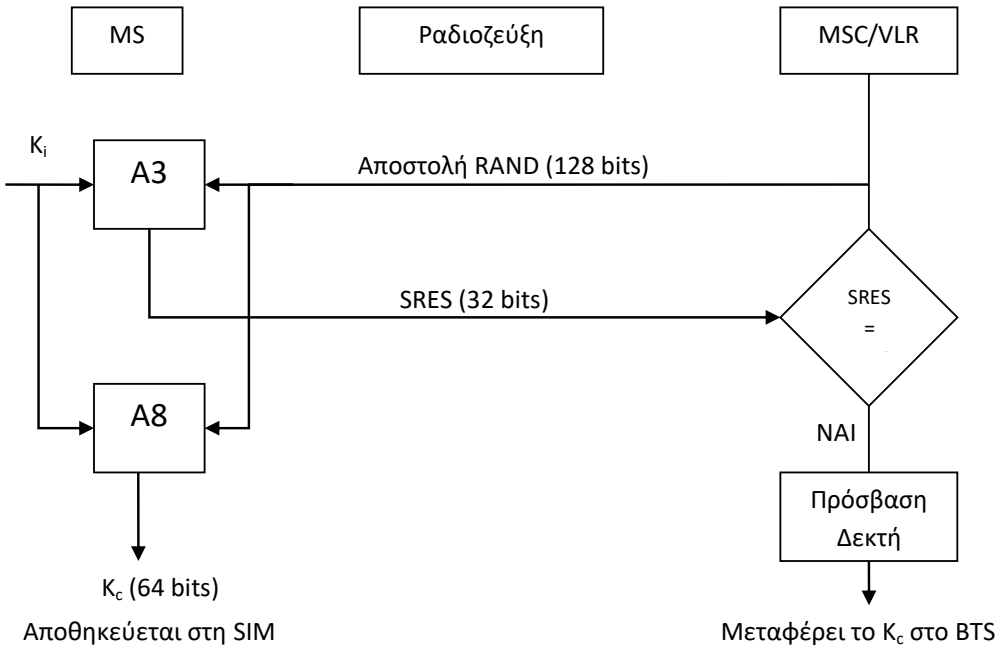


Προστασία της IMSI μέσω της χρησιμοποίησης της TMSI

2.1.2 Πιστοποίηση Ταυτότητας συνδρομητή

Γίνεται προκειμένου το PLMN να εξακριβώσει ότι η ταυτότητα που εστάλη από το MS είναι αληθινή . Πιστοποίηση πραγματοποιείται σε κάθε εγγραφή , ενημέρωση θέσης και πρόσβαση του κινητού στο δίκτυο για εισερχόμενη ή εξερχόμενη κλήση . Η διαδικασία εκτελείται αφού πρώτα γίνει γνωστή η ταυτότητα του συνδρομητή και πριν κρυπτογραφηθεί το κανάλι. Βασίζεται στην αποστολή από το MSC/VLR ενός τυχαίου αριθμού RAND το οποίο είναι 128 bits . Το MS μόλις λάβει τον αριθμό αυτό

υπολογίζει με τον αλγόριθμο A3, χρησιμοποιώντας ως είσοδο στον αλγόριθμο αυτό και το μυστικό κλειδί Ki που είναι επίσης 128 bits και είναι αποθηκευμένο στην κάρτα SIM , την ενυπόγραφη απάντηση SRES, που έχει μήκος 32 bits, και την αποστέλει στο VLR . Κατόπιν , με τον αλγόριθμο A8, και με εισόδους πάλι τα RAND και Ki , εξάγει το κλειδί κρυπτογράφησης Kc, που έχει μήκος μόλις 64 bits, το οποίο και αποθηκεύει για να χρησιμοποιήσει ύστερα κατά την κρυπτογράφηση/αποκρυπτογράφηση των δεδομένων. Με τη σειρά του το VLR μόλις αποκτήσει τη SRES , τη συγκρίνει με την XRES που έχει αποθηκευμένη στη βάση δεδομένων του και αν αυτές ταυτίζονται, ο κινητός σταθμός θεωρείται πιστοποιημένος. Σε κάθε πρόσβαση του κινητού στο δίκτυο πρέπει να αποστέλεται διαφορετικό RAND κάθε φορά, έτσι ώστε ακόμα και η απόκτησή του από κάποιον τρίτο κατά τη διάρκεια μιας σύνδεσης να καταστεί άχρηστη την επόμενη. Η χρησιμοποίηση κάθε φορά και άλλου RAND οδηγεί και στον υπολογισμό διαφορετικών σε κάθε περίπτωση SRES και Kc. Η διαδικασία πιστοποίησης των συνδρομητών φαίνεται στο σχήμα που ακολουθεί.



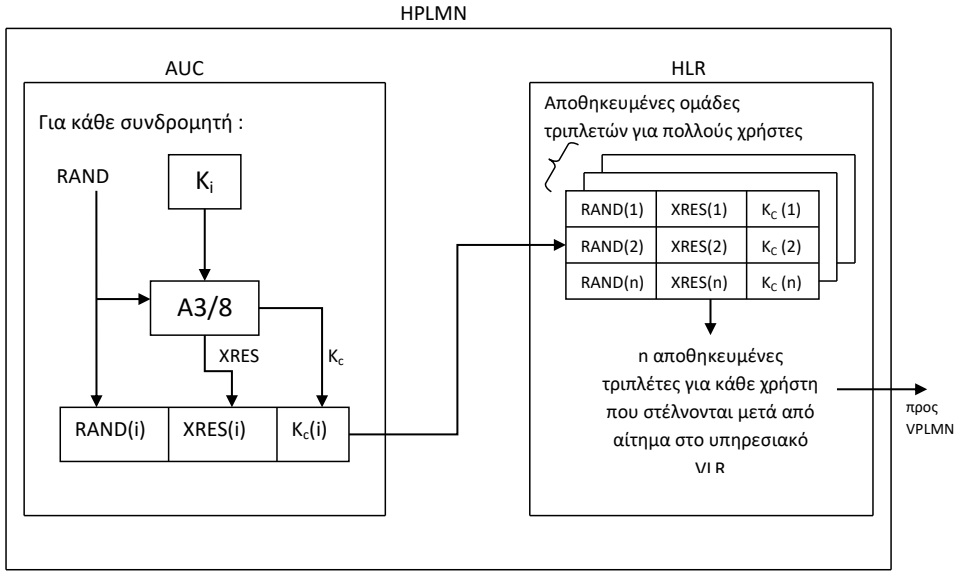
Διαδικασία Πιστοποίησης στο GSM

Μετά την επιτυχή πιστοποίηση του συνδρομητή το κλειδί Kc μεταβιβάζεται από την κάρτα SIM στον κινητό εξοπλισμό (ME) και από το MSC/VLR στο BTS

προκειμένου να πραγματοποιηθεί η κρυπτογράφηση/ αποκρυπτογράφηση . Οι αλγόριθμοι A3 και A8 δεν έχουν μέχρι τώρα δημοσιευτεί .

Χρήση των τριπλετών

Η παραγωγή των τριπλετών (RAND , SRES , Kc) γίνεται στο κέντρο πιστοποίησης AUC με τη χρήση των αλγορίθμων A3 και A8 . Το AUC παράγει μια ομάδα τριπλετών για ένα MS , κάθε φορά με διαφορετικό RAND , και την περνά στο HLR του οικείου PLMN (HPLMN) του χρήστη . Έτσι , όταν ένας κινητός σταθμός περιάγεται σε κάποιο επισκεπτόμενο δίκτυο PLMN (VPLMN) , το δίκτυο αυτό δε χρειάζεται να γνωρίζει τίποτα σχετικά με το μυστικό κλειδί Ki του χρήστη και τους αλγορίθμους πιστοποίησης παρά μόνο ζητάει από το οικείο HLR του συνδρομητή να στείλει στο υπηρεσιακό VLR τριπλέτες προκειμένου να γίνει η πιστοποίηση του χρήστη . Μετά από αίτημα , λοιπόν, του VPLMN το HLR παρέχει πέντε διαφορετικές τριπλέτες στο MSC/VLR για το συνδρομητή αυτό . Το VLR επιλέγει μία από αυτές και πιστοποιεί το χρήστη με τον τρόπο που περιγράψαμε παραπάνω . Όταν το VPLMN δεν έχει πλέον τριπλέτες για έναν χρήστη , ζητάει κατά τον ίδιο τρόπο μία ακόμα ομάδα τριπλετών από το HLR , αλλά σε περίπτωση που για κάποιο λόγο δεν μπορεί να αποκτήσει άλλες από το HPLMN επιτρέπεται να επαναχρησιμοποιήσει κάποιες ήδη χρησιμοποιημένες τριπλέτες. Η διαδικασία δημιουργίας τριάδων στο AUC και η αποθήκευση αυτών στο HLR φαίνεται στο σχήμα που ακολουθεί [4].



Δημιουργία τριπλετών στο AUC και αποθήκευση αυτών στο HLR

2.1.3 Η κρυπτογράφηση των δεδομένων του συνδρομητή

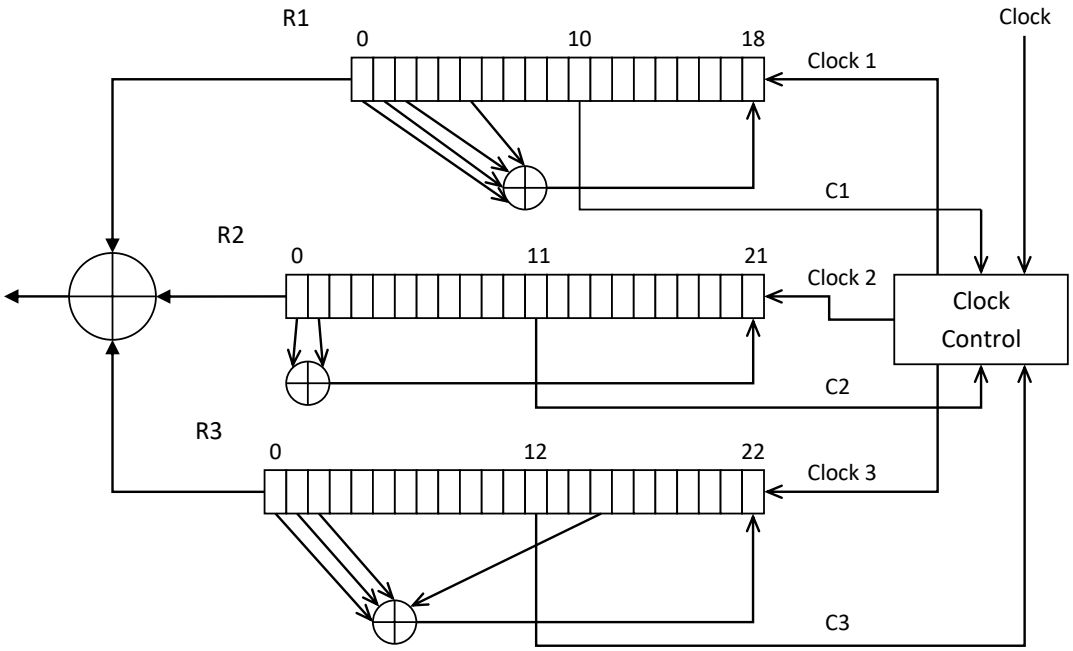
Με την κρυπτογράφηση επιτυγχάνεται προστασία των ευαίσθητων δεδομένων του χρήστη στη ραδιοζεύξη . Πραγματοποιείται μεταξύ του κινητού εξοπλισμού ΜΕ και του σταθμού βάσης BTS . Μετά την πιστοποίηση , το BTS ενημερώνει τον κινητό σταθμό σχετικά με το ποιους αλγορίθμους κρυπτογράφησης υποστηρίζει και δίνει εντολή για έναρξη της διαδικασίας (cipher command) . Ο αλγόριθμος που χρησιμοποιείται είναι ο A5 (με αρκετές εκδόσεις) και είναι ο μοναδικός που δε βρίσκεται στην SIM αλλά στη συσκευή του χρήστη σε μορφή hardware . Λαμβάνει ως εισόδους το κλειδί συνόδου Kc (64 bits) και τον αριθμό του πλαισίου (frame number -FN) που πρόκειται να εκπεμφθεί (αντίστοιχα να ληφθεί στην περίπτωση αποκρυπτογράφησης) (22 bits) και παράγει ως εξόδους μία κλειδική ακολουθία των 228 bits . Τα πρώτα 114 bits χρησιμοποιούνται για να κρυπτογραφήσουν τα δεδομένα που θα μεταδοθούν και τα υπόλοιπα 114 bits για να αποκρυπτογραφήσουν την ίδια στιγμή αυτά που θα ληφθούν καθώς στο GSM οι ζεύξεις είναι αμφίδρομες οπότε ο κινητός σταθμός και ο σταθμός βάσης μεταδίδουν και λαμβάνουν ταυτόχρονα . Ο αριθμός πλαισίου χρησιμοποιείται απλά και μόνο για την επίτευξη συγχρονισμού μεταξύ κινητού σταθμού και σταθμού βάσης κατά τη διάρκεια της διαδικασίας . Η κλειδική ακολουθία που προκύπτει μετά την εκτέλεση του αλγορίθμου γίνεται XOR με το "καθαρό" πλαίσιο κι έτσι παράγεται το προστατευμένο πλαίσιο το οποίο εν συνεχεία εκπέμπεται . Στην κατεύθυνση λήψης ακολουθούνται τα ίδια ακριβώς βήματα με αποτέλεσμα ο δέκτης να αποκτά μετά την αποκρυπτογράφηση τα δεδομένα στην αρχική μορφή τους . Να σημειώσουμε ότι κάθε "καθαρό" πλαίσιο GSM περιλαμβάνει 114 bits πληροφορίας , συνεπώς , η πράξη XOR γίνεται bit–by–bit .

Σε περίπτωση μεταπομπής κατά τη διάρκεια μιας κλήσης , το Kc και όλα τα στοιχεία ασφαλείας , μεταφέρονται στο καινούριο BTS που εξυπηρετεί τον κινητό σταθμό . Το κλειδί Kc παραμένει αναλλοίωτο παρά τη μεταπομπή.

Ο αλγόριθμος A5 χρησιμοποιεί τρεις καταχωρητές ολίσθησης (LSFR) διαφορετικού μήκους ο καθένας. Το συνδυασμένο μήκος των τριών καταχωρητών είναι 64 bits . Οι έξοδοί τους γίνονται XOR κι έτσι παράγεται ένα bit κλειδικής ακολουθίας . Οι καταχωρητές έχουν μήκος 19 , 22 και 23 bits αντίστοιχα ενώ αποτελούνται και από πολυώνυμα ανάδρασης (feedback polynomials) . Ένας

καταχωρητής θεωρείται clocked αν το μεσαίο του bit συμφωνεί με την τιμή του bit που έχει την πλειοψηφία μεταξύ των μεσαίων bits των τριών καταχωρητών . Για παράδειγμα αν τα μεσαία bits των τριών LSFR είναι 1 , 1 και 0 , τότε οι δύο πρώτοι είναι clocked ή αν τα μεσαία bits είναι 0 , 1 , 0 , ο πρώτος και ο τρίτος είναι clocked . Δηλαδή σε κάθε εκτέλεση τουλάχιστον δύο καταχωρητές είναι clocked . Στο σχήμα που ακολουθεί , φαίνονται οι τρεις καταχωρητές ολίσθησης του A5 καθώς και ο έλεγχος των συντονισμών (clock control) . Τα clock 1,2,3 που συντονίζουν τους LSFR προκύπτουν από τις συναρτήσεις :

$$clock1 = clock \cap ((C1 \cap (C2 \cup C3)) \cup \neg (C1 \cup (C2 \cap C3)))$$
$$clock2 = clock \cap ((C2 \cap (C1 \cup C3)) \cup \neg (C2 \cup (C1 \cap C3)))$$
$$clock3 = clock \cap ((C3 \cap (C1 \cup C2)) \cup \neg (C3 \cup (C1 \cap C2)))$$



Οι τρεις καταχωρητές του A5

Οι τρεις καταχωρητές αρχικοποιούνται με το κλειδί συνόδου Kc και τον αριθμό πλαισίου FN . Το κλειδί καθόλη τη διάρκεια της συνόδου είναι το ίδιο ενώ ο FN αυξάνεται κατά ένα για κάθε πλαίσιο . Έτσι για κάθε ένα frame παράγεται μία διαφορετική κλειδική ακολουθία . Με αυτόν τον τρόπο εξασφαλίζεται ότι δύο πλαίσια δεν πρόκειται να κρυπτογραφηθούν με την ίδια κλειδική ακολουθία .

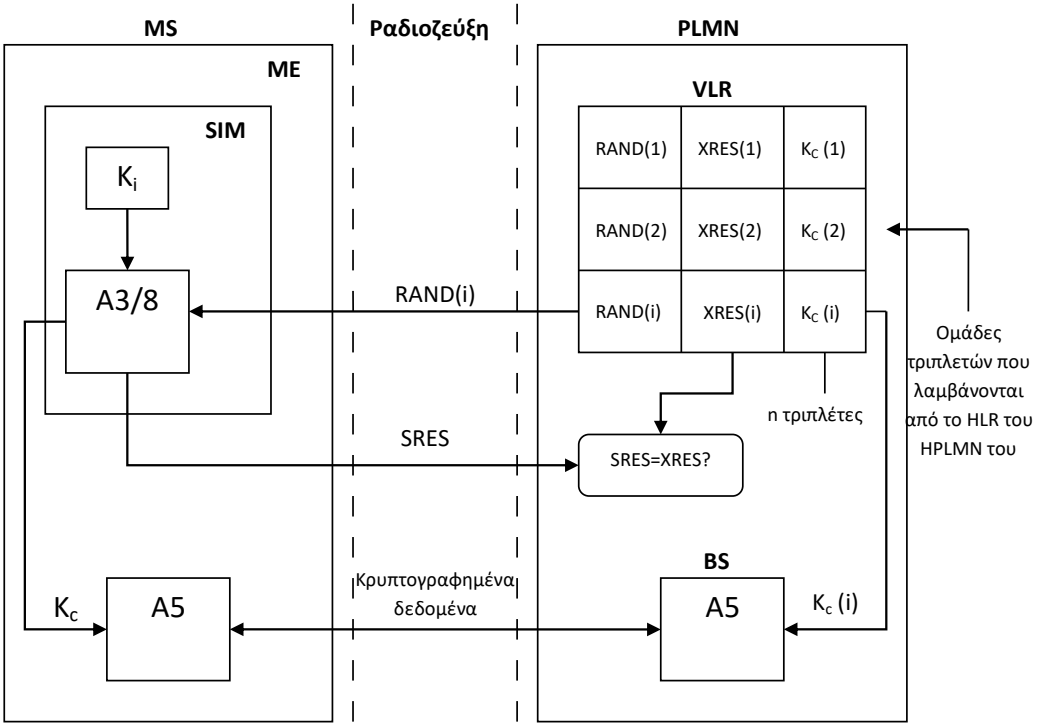
Στους καταχωρητές πρώτα φορτώνεται το 64-bit κλειδί Kc bit-by-bit . Κατά τη διάρκεια αυτής της διαδικασίας δεν ισχύει ο κανόνας της πλειοψηφίας των μεσαίων bits (the majority clocking rule) που περιγράφηκε παραπάνω . Κατόπιν φορτώνεται στους καταχωρητές ο 22-bit αριθμός πλαισίου κατά τον ίδιο τρόπο , ενώ και τώρα δεν ισχύει ο ανωτέρω κανόνας . Αφότου οι καταχωρητές έχουν αρχικοποιηθεί με το κλειδί Kc και τον τρέχοντα αριθμό πλαισίου , συντονίζονται εκατό φορές , χρησιμοποιώντας από εδώ και στο εξής το clock control , και τα παραγόμενα bits απορρίπτονται . Ύστερα από αυτό 228 bits κλειδικής ακολουθίας δημιουργούνται από τα οποία τα πρώτα 114 bits χρησιμοποιούνται για την κρυπτογράφηση του πλαισίου , που θα μεταδοθεί στη ζεύξη MS – BTS (BTS – MS αντίστοιχα) , ενώ τα υπόλοιπα 114 bits για την αποκρυπτογράφηση του πλαισίου , που θα ληφθεί από τη ζεύξη BTS – MS (MS – BTS αντίστοιχα) . Με το πέρας αυτής της διαδικασίας , οι καταχωρητές αρχικοποιούνται ξανά με το κλειδί Kc και τον αριθμό του επόμενου πλαισίου .

Ο αλγόριθμος A5 λειτουργεί σε πολλές εκδόσεις . Ο A5/0 δε χρησιμοποιεί καθόλου κρυπτογράφηση . Ο A5/1 χρησιμοποιείται σε πολλές συσκευές σήμερα και είναι ο πρώτος αλγόριθμος κρυπτογράφησης που σχεδιάστηκε για το GSM . Ο A5/2 αποτελεί την πιο αδύναμη έκδοση , ωστόσο χρησιμοποιείται αρκετά , ενώ ο A5/3 , που είναι δυνατός αλγόριθμος συγκριτικά με τους δύο προαναφερθέντες , τελευταία έχει αρχίσει να ενσωματώνεται στις κινητές συσκευές . Το GSM σκοπεύει να εισάγει και έναν τέταρτο αλγόριθμο , τον A5/4 , του οποίου ο σχεδιασμός όμως δεν έχει ακόμα ολοκληρωθεί. Να σημειώσουμε ότι οι αλγόριθμοι A5/1 και A5/2 δεν έχουν μέχρι τώρα γίνει δημόσια γνωστοί [5].

2.1.4 Κάρτα SIM και Έλεγχος IMEI

Η κάρτα SIM έχει σχεδιασθεί έτσι ώστε να μπορεί να μετακινείται από τον υπόλοιπο κινητό εξοπλισμό, αφού σε αυτήν είναι αποθηκευμένα τα ευαίσθητα προσωπικά δεδομένα του χρήστη. Επίσης είναι κατά τέτοιο τρόπο κατασκευασμένη που δύσκολα μπορεί κάποιος τρίτος να αποσπάσει τα απόρρητα αυτά στοιχεία ακόμα κι αν έχει τον κατάλληλο εξοπλισμό. SIM και ME (mobile equipment) συνεργάζονται προκειμένου να παρέχουν στο συνδρομητή όλους τους απαραίτητους μηχανισμούς ασφαλείας. Συγκεκριμένα στη SIM γίνεται η πιστοποίηση του χρήστη και η δημιουργία του κλειδιού Kc, ενώ στο ME λαμβάνει χώρα η

κρυπτογράφηση/αποκρυπτογράφηση . Στο σχήμα που ακολουθεί απεικονίζεται ολοκληρωμένο το μοντέλο ασφαλείας του GSM για την προστασία της ταυτότητας και των δεδομένων του χρήστη στη ραδιοζεύξη.



Το μοντέλο ασφαλείας του GSM στη ραδιοζεύξη

Ένας τελευταίος μηχανισμός ασφαλείας που εφαρμόζει το GSM είναι ο έλεγχος της ταυτότητας IMEI του συνδρομητή . Όπως σε κάθε κλήση το κλειδί Kc που χρησιμοποιείται πρέπει να είναι διαφορετικό , έτσι και ο έλεγχος της ταυτότητας του κινητού τερματικού (IMEI) πρέπει να γίνεται κάθε φορά που ο χρήστης προσπαθεί να αποκτήσει πρόσβαση στο δίκτυο προκειμένου να διεκπεραιώσει κάποια λειτουργία (κλήση , αποστολή δεδομένων κ.τ.λ.). Ο έλεγχος αυτός αποσκοπεί στο να βεβαιωθεί το σύστημα ότι κανένα κλεμμένο ή μη εξουσιοδοτημένο κινητό δε χρησιμοποιείται . Πραγματοποιείται με τη συνεργασία του κέντρου τεκμηρίωσης EIR, το οποίο μετά τον έλεγχο αποφαίνεται αν μια κλήση πρέπει να συνεχιστεί ή να διακοπεί . Η ανταλλαγή μηνυμάτων μεταξύ του κινητού σταθμού και του MSC/VLR γίνεται σε κρυπτογραφημένη μορφή (ο έλεγχος IMEI διεξάγεται αφού πρώτα έχουν ολοκληρωθεί οι διαδικασίες πιστοποίησης και έχει δοθεί εντολή για έναρξη της κρυπτογράφησης).

2.2 Τα βασικότερα ζητήματα ασφαλείας του 802.11

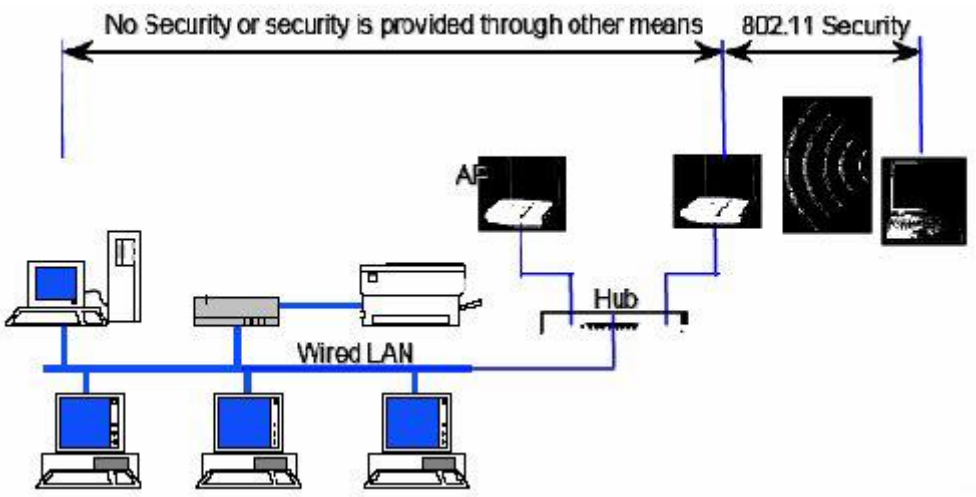
Τα ασύρματα δίκτυα τύπου 802.11 είναι αυτή τη στιγμή ο πιο διαδεδομένος τρόπος για ασύρματη διασύνδεση ηλεκτρονικών υπολογιστών και το πιο ραγδαία αναπτυσσόμενο κομμάτι στην αγορά των δικτύων. Μάλιστα, τα περιθώρια αύξησης του προβλεπόμενου ρυθμού ανάπτυξης του δεν έχουν ακόμα φτάσει στο πιθανό μέγιστο τους.

Το 1999 διανεμήθηκαν παγκοσμίως περίπου 1,4 εκατομμύρια ασύρματοι τοπικοί δικτυακοί αναμεταδότες(Access Points - APs). Το 2000 το ποσό αυτό τετραπλασιάστηκε φθάνοντας τα 4,9 εκατομμύρια. Οι μεσομακροπρόθεσμες προβλέψεις μιλάνε για σίγουρη αύξηση του αριθμού αυτού μέχρι το 2006, όπου και υπολογίζεται να φθάσει τα 56 εκατομμύρια. Αυτή η αύξηση θα έχει ως αποτέλεσμα το συνολικό μερίδιο της εν λόγω αγοράς να ανέρχεται στο τρομακτικό ποσό των $4,5 δισεκατομμυρίων, σύμφωνα με τις αναλύσεις της Allied Business Intelligence. Αν αναλογιστούμε δε την μείωση των τιμών και την τρομακτική αύξηση των πωλήσεων των φορητών υπολογιστών, μπορούμε να μιλάμε για μια παγκόσμια τάση που μας οδηγεί στην νομαδικότητα.

Συνεπώς, τα ασύρματα δίκτυα είναι μονόδρομος και ένα κομμάτι του συνόλου της σύγχρονης και μελλοντικής πραγματικότητας και όχι μια ξεχωριστή εναλλακτική οντότητα. Επίσης κατασκευάζονται και διαδίδονται συσκευές οι οποίες χρησιμοποιούν την τεχνολογία 802.11 λόγω των μεγάλων πλεονεκτημάτων της, όπως είναι η χρήση της τεχνολογίας IP και συνεπώς η εύκολη διασύνδεση αυτών των συσκευών με το διαδίκτυο, αλλά και το κόστος του εξοπλισμού που απαιτείται για την δημιουργία ενός δικτύου 802.11.

Έτσι είναι φανερό ότι η χρήση ασυρμάτων δικτύων αλλά και ειδικότερα η χρήση της τεχνολογίας 802.11, αν και είναι ήδη πολύ διαδεδομένη, έχει χώρο μπροστά της για μεγαλύτερη εξάπλωση και χρήση. Αυτή η εξάπλωση δημιουργεί νέες προκλήσεις για την προστασία αυτών των εφαρμογών, οι οποίες θα βασίζονται στην τεχνολογία 802.11, αλλά και για την φυσική λειτουργία των δικτύων αυτών. Η εμπειρία έχει δείξει ότι για κάθε διαδεδομένη τεχνολογία εμφανίζονται ολοένα και δυσκολότερες προκλήσεις ασφαλείας, ακριβώς λόγω αυτής της διάδοσης και της γνώσης για αυτή την τεχνολογία.

Το πρότυπο IEEE 802.11 προσδιόρισε διάφορες υπηρεσίες ασφαλείας ώστε να μπορέσει να λειτουργήσει σε ένα ασφαλές λειτουργικό περιβάλλον. Οι υπηρεσίες ασφαλείας οι οποίες παρέχονται, κατά ένα μεγάλο μέρος είναι συνδεδεμένες με το πρωτόκολλο Wired Equivalent Privacy (WEP) για να προστατευθούν τα δεδομένα κατά τη διάρκεια της ασύρματης μετάδοσης μεταξύ των πελατών και των σημείων πρόσβασης. Το WEP παρέχει μόνο ασφάλεια για την ασύρματη μετάδοση των πληροφοριών και όχι για όλη τη σύνδεση όπως φαίνεται και στο παρακάτω σχήμα:



Ασφάλεια στο WLAN

Οι τρεις βασικές υπηρεσίες ασφαλείας οι οποίες έχουν οριστεί στο πρότυπο 802.11 της IEEE είναι οι ακόλουθες :

- Εμπιστευτικότητα – Ιδιωτικότητα (Confidentiality - Privacy): Η εμπιστευτικότητα, ως ένας από τους κυριότερους στόχους του WEP, επιτεύχθηκε με την κρυπτογράφηση των δεδομένων ώστε η πρόσβαση σε αυτά να είναι αδύνατη.
- Ακεραιότητα (Integrity): Ένας άλλος στόχος του WEP ήταν η ακεραιότητα ώστε να μην είναι δυνατό να αλλαχθούν τα περιεχόμενα του μηνύματος κατά τη διάρκεια μετάδοσης χωρίς να γίνει αντιληπτό.
- Αυθεντικοποίηση (Authentication): Ο κυριότερος, ωστόσο, στόχος του WEP ήταν η υπηρεσία αυθεντικοποίησης του client στο access point αλλά όχι αντιστρόφως.

Έτσι επιτυγχάνεται η ελεγχόμενη σύνδεση με το δίκτυο το οποίο προστατεύεται. Εδώ πρέπει να αναφέρουμε ότι το πρότυπο 802.11 δεν αντιμετωπίζει θέματα

ασφαλείας όπως είναι ο έλεγχος, η μη αποποίηση(non repudiation) και οι εξουσιοδοτήσεις (authorization). Οι υπηρεσίες περιγράφονται πιο κάτω με μεγαλύτερη λεπτομέρεια [6], [7].

2.2.1 Εμπιστευτικότητα – Ιδιωτικότητα

Το πρότυπο 802.11 υποστηρίζει την ιδιωτικότητα μέσω χρήσης κρυπτογραφικών αλγόριθμων. Η κρυπτογραφική μέθοδος του WEP για την ιδιωτικότητα χρησιμοποιεί το συμμετρικό κλειδί τύπου RC4 για να δημιουργήσει μια σειρά από ψευδοτυχαίους αριθμούς. Σε αυτή τη "ροή" εφαρμόζεται και μια XOR ώστε τα δεδομένα να αποσταλούν. Μέσω αυτής της τεχνικής του WEP είναι δυνατόν να προστατευθούν τα δεδομένα από ανάγνωση από χρήστες οι οποίοι δεν έχουν το κατάλληλο κλειδί. Το WEP εφαρμόζεται σε όλα τα δεδομένα πάνω από το 802.11 WLAN ώστε να προστατευθούν δεδομένα τύπου Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX) και Hyper Text Transfer Protocol (HTTP). Όπως ορίζεται στο πρότυπο 802.11 το WEP υποστηρίζει μόνο κρυπτογραφικά κλειδιά μήκους 40-bit για το διαμοιραζόμενο κλειδί. Ωστόσο όλοι οι Providers υποστηρίζουν κλειδιά μήκους 104 bits και πολλοί και 128 bits. Το κλειδί WEP μήκους 104-bit, για παράδειγμα, με την προσθήκη ενός Initialization Vector (IV) μήκους 24-bit γίνεται ένα κλειδί RC4 μήκους 128-bit. Γενικά ανεβάζοντας το μήκους του κλειδιού αυξάνεται και η ασφάλεια. Η έρευνα έχει δείξει ότι για κλειδιά μεγαλύτερα από 80-bits η επίθεση brute-force είναι υπερβολικά δύσκολο να επιτύχει αφού χρειάζεται μεγάλη υπολογιστική δύναμη. Στην πράξη όμως η προστασία με το WEP είναι ξεπερασμένη και ευάλωτη για οποιουδήποτε μήκους κλειδί.

2.2.2 Ακεραιότητα

Το πρότυπο 802.11 περιγράφει επίσης τα μέσα με τα οποία μπορεί να προστατευθεί η ακεραιότητα των μηνυμάτων. Η υπηρεσία αυτή έχει σχεδιαστεί να απορρίπτει πακέτα τα οποία έχουν υποστεί επίθεση τύπου "in the middle". Η παραπάνω απλή τεχνική χρησιμοποιεί μια κρυπτογραφική Cyclic Redundancy Check (CRC). Ένα πλαίσιο ελέγχου CRC-32 υπολογίζεται για κάθε payload πριν από την μετάδοση. Το πακέτο κρυπτογραφείται χρησιμοποιώντας ένα κλειδί RC4 και προκύπτει το κρυπτογράφημα. Μόλις λαμβάνεται το παραπάνω αποκρυπτογραφείται καιπροκύπτει μετά από υπολογισμούς το CRC. Αν δεν είναι ίδια τότε υπάρχει λάθος στην μετάδοση. Ωστόσο, ομοίως με την ιδιωτικότητα, έτσι και για την ακεραιότητα ο

μηχανισμός δεν μπορεί να εγγυηθεί την ασφάλεια αφού η κρυπτογράφηση μέσω WEP περιέχει ένα σφάλμα στην κρυπτογράφηση μειώνοντας σοβαρά την αποτελεσματικότητά του.

Το πρότυπο 802.11, δυστυχώς, δεν προβλέπει μεθόδους διαχείρισης κλειδιών (όπως είναι ο κύκλος ζωής και άλλα) και έτσι η δημιουργία, η διάδοση, η αποθήκευση, ο έλεγχος και πολλές άλλες λειτουργίες αφήνονται στους διαχειριστές αυτών των δικτύων (αυτό ισχύει αν ακολουθούνται οι προδιαγραφές του αρχικού 802.11, κάτι το οποίο δεν ισχύει σήμερα). Σε περίπτωση όμως που το παραπάνω ισχύει, εισάγονται πολλές αδυναμίες στην ασφάλεια του δικτύου. Τέλος, λόγω του ότι οι αρχικές προδιαγραφές δεν αναφέρουν για διαχείριση κλειδιών, είναι πολύ δύσκολο έως ανέφικτο να γίνει αυτό σε ένα περιβάλλον εταιρικής κλίμακας, η οποία ίσως να απαιτεί την αλλαγή των κλειδιών τακτικά και την παραγωγή τυχαίων κλειδιών. Για παράδειγμα σε ένα πανεπιστημιακό χώρο μπορεί να υπάρχουν ακόμα και 15.000 APs. Η διαχείριση τόσων κλειδιών είναι ένα αρκετά πολύπλοκο σενάριο.

2.2.3 Αυθεντικοποίηση

Το πρότυπο IEEE 802.11 ορίζει δύο τρόπους με τους οποίους είναι δυνατόν να αυθεντικοποιηθεί ένας χρήστης σε έναν σταθμό πρόσβασης: α) Open System Authentication και β) Shared-Key Authentication. Ο δεύτερος είναι βασισμένος στην κρυπτογραφία ενώ ο πρώτος όχι. Η τεχνική Open System Authentication δεν είναι στην πραγματικότητα αυθεντικοποίηση αλλά είναι δυνατή η πρόσβαση σε ένα σταθμό πρόσβασης χωρίς περιορισμούς. Πρέπει επίσης να αναφερθεί ότι η αυθεντικοποίηση είναι μονόδρομη, μόνο ο χρήστης αυθεντικοποιήται στον σταθμό βάσης.

Με την τεχνική Open System Authentication, ένας χρήστης αυθεντικοποιήται απλώς απαντώντας με την MAC του κατά την διάρκεια της ανταλλαγής μηνυμάτων με τον Access Point. Κατά την ανταλλαγή ο χρήστης δεν είναι ουσιαστικά επικυρωμένος αλλά απλώς απαντά με το σωστό περιεχόμενο στην ανταλλαγή μηνυμάτων. Η χωρίς κρυπτογραφική επικύρωση τεχνική Open-System Authentication είναι ευάλωτη σε επιθέσεις.

Η τεχνική Shared-Key Authentication είναι μια κρυπτογραφική τεχνική η οποία εφαρμόζει ένα απλό σύστημα «ερώτησης - απάντησης» (challenge-response) ώστε να

διαπιστωθεί αν ο χρήστης έχει στην κατοχή του το κλειδί. Ο χρήστης χρησιμοποιώντας το κλειδί που έχει στην κατοχή του κρυπτογραφεί το challenge και το επιστρέφει. Ο σταθμός βάσης το αποκρυπτογραφεί και αν είναι ίδιο με το challenge που του έστειλε τότε τον επικυρώνει ως χρήστη.

Ο αλγόριθμος που χρησιμοποιείται για τη δημιουργία του 128-bit challenge είναι ο RC4 stream cipher. Πρέπει να προστεθεί ότι η μέθοδος αυτή είναι απλή και δεν αυθεντικοποιεί και τον σταθμό βάσης. Δηλαδή δεν υπάρχει εγγύηση ότι ο σταθμός βάσης είναι αυτός που εμπιστευόμαστε. Λόγω αυτής της αδυναμίας έχουν εμφανιστεί πολλές επιθέσεις γνωστές ως “man-in-the-middle Attacks” (MITM).

Όπως αναφέρθηκε πιο πάνω, η βιομηχανία 802.11 WLAN έχει αυτήν την περίοδο αυξητικές τάσεις στις προτιμήσεις του καταναλωτικού κοινού. Πολλές οργανώσεις, συμπεριλαμβανομένων και λιανικών καταστημάτων, νοσοκομείων, αερολιμένων και γενικότερα πολλών επιχειρήσεων, έχουν επενδύσει σε ασύρματο εξοπλισμό. Εντούτοις, αν και αναφορικά με το 802.11 έχει παρατηρηθεί τεράστια απήχηση και επιτυχία στην ασύρματη αγορά, υπάρχουν και ζητήματα, τα οποία δε βαίνουν θετικά. Έχουν υπάρξει πολυάριθμες εκθέσεις και έγγραφα περιγράφοντας επιθέσεις στα ασύρματα δίκτυα 802.11 που εκθέτουν την υποδομή του 802.11 σε κινδύνους ασφαλείας. Σε αυτήν την ενότητα θα καλύψουμε εν συντομία τους κινδύνους ασφαλείας που μπορεί να υπάρξουν αναλύοντας τις επιθέσεις με γνώμονα την απειλή της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δικτύων.

2.2.4 Active Attacks

Ενεργός (active) είναι μια επίθεση κατά την οποία ένα αναρμόδιο συμβαλλόμενο μέρος κάνει τροποποιήσεις σε ένα μήνυμα, ένα ρεύμα στοιχείων, ή ένα αρχείο. Είναι δυνατό να ανιχνευθεί αυτός ο τύπος επίθεσης αλλά μπορεί να μην είναι αναστρέψιμος. Οι ενεργές επιθέσεις μπορούν να λάβουν τη μορφή ενός από τους τέσσερις παρακάτω τύπους (ή ένα συνδυασμό από αυτούς): Masquerading, Replay, Message Modification και Denial-of-Service).

2.2.4.1 Masquerading

Ο επιτιθέμενος παρουσιάζεται ως εξουσιοδοτημένος χρήστης και με αυτόν τον τρόπο κερδίζει ορισμένα προνόμια.

2.2.4.2 Replay

Ο επιτιθέμενος ελέγχει τις μεταδόσεις (παθητική επίθεση) και αναμεταδίδει τα μηνύματα ως νόμιμος χρήστης.

2.2.4.3 Message Modification

Ο επιτιθέμενος αλλάζει ένα νόμιμο μήνυμα με τη διαγραφή, την προσθήκη, την αλλαγή, ή την εκ νέου αίτηση του.

2.2.4.4 Denial-of-Service

Ο επιτιθέμενος γενικότερα αποτρέπει ή απαγορεύει την κανονική χρήση ή τη διαχείριση των εγκαταστάσεων επικοινωνιών. Τα 802.11 ασύρματα δίκτυα μπορούν να αντιμετωπίσουν DoS επιθέσεις που χρησιμοποιούν το καθ' εαυτό 802.11 πρωτόκολλο και από παρεμβολή στην S-Band ISM περιοχή συχνοτήτων. Δηλαδή, αν θέλουμε να δημιουργήσουμε ένα RF σύστημα που χρησιμοποιεί την ISM μπάντα, δε χρειάζεται να έχουμε άδεια, αν και χρειάζεται να καταχωρήσουμε την συσκευή. Όλα τα 802.11 δίκτυα χρησιμοποιούν την ISM μπάντα στην περιοχή 2,4 – 2,5 GHz, η οποία είναι υπερβολικά φορτωμένη. Ασύρματα τηλέφωνα, συσκευές παιδικής παρακολούθησης, X10 κάμερες και πολλές άλλες συσκευές στην εν’ λόγω μπάντα μπορούν να προκαλέσουν απώλεια πακέτων ή παρεμβολή στην λειτουργία των 802.11 δικτύων.

Ένα άλλο εγγενές πρόβλημα των 802.11 συστημάτων είναι ότι η διαχείριση των frames, που ελέγχουν την σύνδεση στον client είναι τελείως μη αυθεντικοποιημένη και μπορεί να προσβληθεί από έναν κρυπταναλυτή. Ουσιαστικά, ένας εισβολέας μπορεί να προωθήσει ένα πακέτο έτσι ώστε να φαίνεται ότι είναι ένα access point, ζητώντας από τους clients να αποσυνδεθούν. Μάλιστα, δεν μπορεί τίποτα να γίνει, προκειμένου να αποτρέψουμε κάποιον πού θέλει να κάνει μια τέτοια επίθεση στο δίκτυό μας. Το εργαλείο WLAN Jack που περιέχει αυτού του είδους την επίθεση, εμπεριέχεται στο Air Jack.

Τέλος, ας μην ξεχνάμε, ότι οι clients μπορεί να είναι περιπλανώμενοι χρήστες με μηχανήματα χαμηλών δυνατοτήτων αλλά κυρίως συγκεκριμένης αυτονομίας ενέργειας. Για παράδειγμα, αν ένας φορητός υπολογιστής συνέχεια συνδέεται και αποσυνδέεται η διάρκεια της μπαταρίας του θα μειωθεί αισθητά.

2.2.5 Passive Attacks

Παθητική (passive) είναι μια επίθεση στην οποία ένα αναρμόδιο συμβαλλόμενο μέρος αποκτά πρόσβαση σε έναν πόρο και δεν τροποποιεί το περιεχόμενό του (π.χ. Eavesdropping Attack). Οι παθητικές επιθέσεις προκύπτουν είτε παρακολουθώντας κρυφά ένα δίκτυο είτε με ανάλυση της δικτυακής κυκλοφορίας. Αυτές οι δύο παθητικές επιθέσεις περιγράφονται πιο κάτω.

2.2.5.1 Eavesdropping

Ο επιτιθέμενος ελέγχει τις μεταδόσεις για το περιεχόμενο των μηνυμάτων. Ένα παράδειγμα αυτής της επίθεσης είναι ένα πρόσωπο που ακούει στις μεταδόσεις στο τοπικό LAN μεταξύ δύο τερματικών σταθμών ή που συντονίζει στις μεταδόσεις μεταξύ ενός μικρού ασύρματου τηλεφώνου και ενός σταθμού βάσεων.

2.2.5.2 Traffic Analysis

Ο επιτιθέμενος, με έναν πιο διακριτικό τρόπο, αποκτά πληροφορίες ελέγχοντας τις μεταδόσεις για επαναλαμβανόμενες ακολουθίες επικοινωνίας (patterns). Ένα μη αμελητέο ποσό πληροφοριών περιλαμβάνεται στη ροή των μηνυμάτων μεταξύ των επικοινωνούντων συμβαλλόμενων μερών.

2.3 Απειλές Ασφαλείας

Οι κίνδυνοι που συνδέονται με το 802.11 είναι το αποτέλεσμα μιας ή περισσότερων από αυτές τις επιθέσεις. Οι συνέπειες αυτών των επιθέσεων περιλαμβάνουν, αλλά δεν περιορίζονται, στην απώλεια ιδιόκτητων πληροφοριών, σε νομικές δαπάνες και δαπάνες αποκατάστασης, στην αμαυρωμένη εικόνα μιας επιχείρησης και την απώλεια δικτυακής υπηρεσίας.

2.3.1 Απώλεια εμπιστευτικότητας

Με τον όρο εμπιστευτικότητα εννοούμε την έννοια εκείνη με την οποία οι πληροφορίες δεν παρέχονται ή δεν αποκαλύπτονται σε αναρμόδια άτομα, οντότητες,

ή διαδικασίες. Αυτό είναι, γενικά, μια θεμελιώδης απαίτηση ασφαλείας για τους περισσότερους οργανισμούς. Λόγω της ραδιοφωνικής φύσης της ασύρματης τεχνολογίας, η εμπιστευτικότητα είναι μια απαίτηση ασφαλείας που πολύ δύσκολα επιτυγχάνεται σε ένα ασύρματο δίκτυο. Οι επιτιθέμενοι δεν είναι απαραίτητο να διαπεράσουν ένα UTP καλώδιο ώστε να έχουν πρόσβαση στους δικτυακούς πόρους. Επιπλέον, μπορεί να μην είναι δυνατό να ελεγχθεί η απόσταση από την οποία εμφανίζεται η μετάδοση. Αυτό καθιστά τα παραδοσιακά φυσικά αντίμετρα ασφαλείας λιγότερο αποτελεσματικά.

Η παθητική παρακολούθηση των ασύρματων επικοινωνιών του 802.11 μπορεί να προκαλέσει σημαντικό κίνδυνο για έναν οργανισμό. Ένας κρυπταναλυτής μπορεί ν είναι σε θέση να ακούσει και να λάβει ευαίσθητες πληροφορίες συμπεριλαμβανομένων των ιδιόκτητων πληροφοριών, των IDs του δικτύου, των κωδικών πρόσβασης και των στοιχείων διαμόρφωσης. Αυτός ο κίνδυνος είναι υπαρκτός επειδή τα σήματα του 802.11 μπορούν να ταξιδέψουν έξω από την περίμετρο του κτιρίου. Λόγω της εκτεταμένης εμβέλειας των ραδιοφωνικών μεταδόσεων, οι επιτιθέμενοι μπορούν ενδεχομένως να ανιχνεύσουν τη μετάδοση από ένα μέρος χώρου στάθμευσης ή από κοντινούς δρόμους.

Αυτό το είδος επίθεσης, που εκτελείται μέσω της χρήσης ενός ασύρματου εργαλείου ανάλυσης συσκευών δικτύου, ή ενός sniffer software, είναι ιδιαίτερα εύκολο για δύο λόγους: 1) συχνά τα χαρακτηριστικά γνωρίσματα της τεχνολογίας WLAN σχετικά με την εμπιστευτικότητα δεν είναι ενεργοποιημένα ακόμη και 2) λόγω των πολυάριθμων ευπαθειών του 802.11 στην ασφάλεια, όπως αναφέραμε πιο πάνω. Προγράμματα ανάλυσης ασύρματων πακέτων, όπως το AirSnort και το WEPcrack, είναι εργαλεία που είναι εύκολα διαθέσιμα στο διαδίκτυο σήμερα. Το AirSnort είναι ένα από τα πρώτα εργαλεία που δημιουργούνται για να αυτοματοποιήσουν τη διαδικασία αυτή. Δυστυχώς, το λογισμικό αυτό επίσης χρησιμοποιείται για το “σπάσιμο” αυτών των δικτύων. Το AirSnort μπορεί να εκμεταλλευθεί τις ρωγμές στον RC4, ο οποίος αποτελεί μέρος των αρχικών προτύπων WEP. Για να το επιτύχει αυτό, το AirSnort χρειάζεται μόνο έναν υπολογιστή που να τρέχει το λειτουργικό σύστημα Linux και μια ασύρματη κάρτα δικτύου. Το λογισμικό ελέγχει παθητικά τις μεταδόσεις του WLAN και υπολογίζει τα κλειδιά κρυπτογράφησης αφότου ανακτηθούν τουλάχιστον 100 MB δικτυακών πακέτων. Σε ένα δίκτυο με αυξημένη κίνηση, η συγκέντρωση αυτή μπορεί να πάρει μόνο τρεις ή

τέσσερις ώρες, ενώ εάν ο όγκος κυκλοφορίας είναι χαμηλός, μπορεί να πάρει ακόμ και μερικές ημέρες. Παραδείγματος χάριν, ένα πολυάσχολο σημείο πρόσβασης που διαβιβάζει 3.000 bytes με 11 Mbps θα εξαντλήσει το IV των 24-bit μετά από περίπου 10 ώρες. Εάν μετά από δέκα ώρες που ο επιτιθέμενος παρακολουθεί, ανακτήσει δύο κείμενα στα οποία έχει χρησιμοποιηθεί το ίδιο κλειδί, τόσο η ακεραιότητα όσο και η εμπιστευτικότητα μπορούν να βρίσκονται σε κίνδυνο. Αφότου έχουν παραληφθεί πακέτα δικτύων, τα θεμελιώδη κλειδιά μπορούν να αποκτηθούν σε λιγότερο από ένα δευτερόλεπτο. Μόλις το κλειδί WEP γίνει γνωστό, ο χρήστης μπορεί να διαβάσει οποιοδήποτε πακέτο ταξιδεύει πάνω στο WLAN. Η ευρεία διαθεσιμότητα, η ευκολία χρήσης και η δυνατότητα τέτοιων εργαλείων να υπολογίσουν κλειδιά, καθιστούν ουσιαστικό για τους διαχειριστές ασφαλείας να εφαρμόσουν ασφαλείς ασύρματες λύσεις. Το Airsnort μπορεί να μην είναι σε θέση να εκμεταλλευθεί τον ενισχυμένο αλγόριθμο RC4 μέσω μιας τυποποιημένης εφαρμογής.

Τα WLANs έχουν επίσης κίνδυνο απώλειας της εμπιστευτικότητας μετά από μια ενεργό επίθεση. Η παρακολούθηση μέσω λογισμικού όπως περιγράφεται πιο πάνω μπορεί να λάβει τα ονόματα χρηστών και τους κωδικούς πρόσβασης (καθώς επίσης και οποιαδήποτε άλλα στοιχεία που διαπερνούν το δίκτυο) καθώς στέλνονται μέσω μιας ασύρματης σύνδεσης. Κάποιος μπορεί να είναι σε θέση να υποδυθεί έναν νόμιμο χρήστη και να αποκτήσει πρόσβαση στο συνδεμένο ενσύρματο δίκτυο από ένα AP. Μόλις ο εισβολέας συνδεθεί στο δίκτυο, μπορεί να ανιχνεύσει τα δίκτυα μέσω αγορασμένων ή δημοσιών και εύκολα διαθέσιμων εργαλείων. Ο κακόβουλος ωτακουστής (eavesdropper) χρησιμοποιεί έπειτα το όνομα χρηστών, τον κωδικό πρόσβασης και τις πληροφορίες διευθύνσεων IP για να αποκτήσει πρόσβαση στους πόρους δικτύων και τα ευαίσθητα εταιρικά στοιχεία.

Τέλος, ένα ψεύτικο AP θέτει έναν κίνδυνο ασφαλείας. Ένας κακόβουλος ή ανεύθυνος χρήστης θα μπορούσε, λαθραία, να παρεμβάλει ένα ψεύτικο AP σε ένα ντουλάπι, στο πλαίσιο ενός πίνακα δωματίου διασκέψεων, ή οποιασδήποτε άλλη κρυμμένης περιοχή μέσα σε ένα κτίριο. Το ψεύτικο AP θα μπορούσε έπειτα να χρησιμοποιηθεί για να επιτρέψει σε αναρμόδια άτομα να αποκτήσουν πρόσβαση στο δίκτυο. Εφ' όσον είναι η θέση του κοντά στους χρήστες του WLAN και διαμορφώνεται έτσι ώστε να εμφανιστεί σαν ένα νόμιμο AP στους ασύρματους πελάτες, είναι δυνατόν το ψεύτικο AP να μπορέσει επιτυχώς να πείσει τους ασύρματους πελάτες για την νομιμότητά του και να τους αναγκάσει να στείλουν την

κυκλοφορία μέσω αυτού. Το ψεύτικο AP μπορεί να παρεμποδίσει την ασύρματη κυκλοφορία μεταξύ ενός εξουσιοδοτημένου AP και των ασύρματων πελατών. Χρειάζεται μόνο να διαμορφωθεί με ένα ισχυρότερο σήμα από το υπάρχον AP για να παρεμποδίσει την κυκλοφορία πελατών.

Ένας κακόβουλος χρήστης μπορεί επίσης να αποκτήσει πρόσβαση στο ασύρματο δίκτυο μέσω APs που διαμορφώνονται για να επιτρέψουν την πρόσβαση χωρίς αυθεντικοποίηση.

2.3.2 Απώλεια Ακεραιότητας

Τα ζητήματα ακεραιότητας των δεδομένων στα ασύρματα δίκτυα είναι παρόμοια με εκείνα στα ενσύρματα δίκτυα. Επειδή οργανισμοί εφαρμόζουν συχνά ασύρματα ή ενσύρματα δίκτυα χωρίς επαρκή κρυπτογραφική προστασία των δεδομένων, η ακεραιότητα μπορεί να είναι δύσκολο να επιτευχθεί. Ένας hacker, παραδείγματος χάριν, μπορεί να παραβιάσει την ακεραιότητα των δεδομένων με τη διαγραφή ή την τροποποίηση των δεδομένων σε ένα e-mail από ένα λογαριασμό στο ασύρματο σύστημα. Αυτό μπορεί να είναι καταστρεπτικό σε έναν οργανισμό εάν κάποιο σημαντικό e-mai διανέμεται ευρέως μεταξύ των παραληπτών ηλεκτρονικού ταχυδρομείου.

Επειδή τα χαρακτηριστικά γνωρίσματα ασφαλείας του 802.11 δεν προβλέπουν την ισχυρή ακεραιότητα των μηνυμάτων, άλλα είδη ενεργών επιθέσεων που παραβιάζουν την ακεραιότητα συστημάτων είναι δυνατά. Όπως αναφέρθηκε πριν, ο μηχανισμός ακεραιότητας βασισμένος στο WEP είναι απλά ένα CRC. Οι επιθέσεις τροποποίησης μηνυμάτων είναι δυνατές όταν δεν χρησιμοποιούνται κρυπτογραφικοί μηχανισμοί ελέγχου όπως κώδικες ή hashes επικύρωσης μηνυμάτων.

2.3.3 Απώλεια Διαθεσιμότητας Δικτύου

Μια παραβίαση της διαθεσιμότητας των δικτύων περιλαμβάνει κάποια μορφή επίθεσης DoS, όπως το μπλοκάρισμα. Το μπλοκάρισμα εμφανίζεται όταν μεταδίδει σκόπιμα ένας χρήστης ένα σήμα από μια ασύρματη συσκευή προκειμένου να καλυφθούν τα νόμιμα ασύρματα σήματα. Το μπλοκάρισμα μπορεί επίσης να προκληθεί ακούσια από τις ασύρματες εκπομπές φούρνων, τηλεφώνων ή μικροκυμάτων. Το μπλοκάρισμα οδηγεί σε μια διακοπή στις επικοινωνίες επειδή τα νόμιμα ασύρματα σήματα είναι ανίκανα να επικοινωνήσουν στο δίκτυο. Και οι απλοί

χρήστες μπορούν επίσης να προκαλέσουν ένα DoS. Ένας χρήστης, παραδείγματος χάριν, μπορεί ακούσια να μονοπωλήσει ένα ασύρματο σήμα με τη μεταφόρτωση μεγάλων αρχείων, εμποδίζοντας άλλους χρήστες να έχουν πρόσβαση στο δίκτυο. Κατά συνέπεια, οι πολιτικές ασφαλείας των αντιπροσωπειών πρέπει να περιορίσουν τους τύπους και τα ποσά δεδομένων τα οποία οι χρήστες είναι σε θέση να μεταφορτώσουν στα ασύρματα δίκτυα.

2.3.4 Άλλοι κίνδυνοι Ασφαλείας

Με την επικράτηση των ασύρματων συσκευών, περισσότεροι χρήστες επιδιώκουν τρόπους να συνδεθούν απομακρυσμένα με τα δίκτυα των οργανισμών τους. Μια τέτοια μέθοδος είναι η χρήση ενδιάμεσων δικτύων. Τα κέντρα διαλέξεων, παραδείγματος χάριν, συνήθως παρέχουν ασύρματα δίκτυα για τους χρήστες για να συνδεθούν με το διαδίκτυο και στη συνέχεια με τους οργανισμούς τους κατά τη διάσκεψη. Οι αερολιμένες, τα ξενοδοχεία και ακόμη και μερικά προνομιακά καφέ αρχίζουν να εγκαθιστούν δίκτυα 802.11 δημοσίως προσιτά για τους πελάτες τους, προσφέροντας ακόμη και την δικλείδα VPN, για επιπρόσθετη ασφάλεια.

Αυτά τα δημόσια δίκτυα εισάγουν τρεις αρχικούς κινδύνους:

1) επειδή είναι δημόσια, είναι προσιτά στον καθένα, ακόμη και σε κακόβουλους χρήστες,

2) χρησιμεύουν ως μια γέφυρα στο δίκτυο ενός χρήστη, κατά συνέπεια επιτρέποντας ενδεχομένως σε οποιοδήποτε στο δημόσιο δίκτυο να επιτεθεί ή να αποκτήσει πρόσβαση στο γεφυρωμένο δίκτυο και

3) χρησιμοποιούν κεραίες υψηλής απόδοσης για να βελτιώσουν την εκπομπή τους και να αυξήσουν την περιοχή κάλυψης, επιτρέποντας κατά συνέπεια στους κακόβουλους χρήστες να κρυφακούσουν ευκολότερα το σήμα τους.

Με τη σύνδεση με τα δίκτυά τους μέσω ενός τρίτου δικτύου, οι χρήστες μπορούν να δημιουργήσουν ευπάθειες για τα δίκτυα και τα συστήματα επιχείρησής τους εκτός αν οι οργανώσεις τους λαμβάνουν μέτρα για να προστατεύσουν τους χρήστες τους και τους ίδιους. Οι χρήστες πρέπει να έχουν πρόσβαση στους πόρους που οι οργανώσεις τους κρίνουν είτε δημόσιους είτε ιδιωτικούς. Οι αντιπροσωπείες μπορούν αν θελήσουν να προστατεύσουν τους δημόσιους πόρους τους

χρησιμοποιώντας ένα πρωτόκολλο ασφαλείας όπως το Transport Layer of Security (TLS), μέσω μιας τυποποίησης του που αποκαλείται Secure Socket Layer (SSL). Εντούτοις, στις περισσότερες αντιπροσωπείες αυτό είναι περιττό, δεδομένου ότι οι πληροφορίες έχουν δημόσιο χαρακτήρα. Για τους ιδιωτικούς πόρους τους, οι αντιπροσωπείες πρέπει να θεωρήσουν ως μια λύση το VPN για να εξασφαλιστούν οι συνδέσεις τους και επειδή αυτό θα βοηθήσει να αποτραπεί κάποιος από το να κρυφακούσει όπως επίσης θα αποτραπεί και η αναρμόδια πρόσβαση στους ιδιωτικούς αυτούς πόρους [8], [9], [10].

Βιβλιογραφία-Αναφορές:

[1] IEEE 802.11 WG, IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), International Standard [for] Information Technology - Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 2007

[2] Peikari C. & Fogie S., Maximum Wireless Security, 2002

[3] Stallings William Ασύρματες Επικοινωνίες και Δίκτυα, Εκδ. Τζιόλα

[4] Tanenbaum, A. S. (2000). Δίκτυα Υπολογιστών. Αθήνα: Εκδόσεις Παπασωτηρίου.

[5] Perez-Romero, J., Sallent, O., Agusti, R., & Diaz-Guerra, M. (2005). Radio Resource Management Strategies in UMTS. John Wiley & Sons.

[6] Rummler, R., Chung, Y., & Aghvami, H. (2005). Modeling and Analysis of an Efficient Multicast Mechanism for UMTS. IEEE Transactions on Vehicular Technology, vol. 54, no. 1, pp. 350-365.

[7] Sesia, S., Toufik, I., & Baker, M. (2009). LTE - The UMTS Long Term Evolution: From Theory to Practice. John Wiley & Sons.

[8] Spaniol, O. (2003). Mobility Management in UMTS. Datacommunication & Distributed Systems.

[9] Yang, S., & Lin, Y. (2003). Performance evaluation of location management in UMTS. IEEE Transactions on Vehicular Technology, vol. 52, no. 6, pp. 1603-1615.

[10] Βαρβαρίγος, Ε., & Μπερμπερίδης, Κ. (2004). Κινητά Δίκτυα Επικοινωνιών, Πανεπιστημιακές Παραδόσεις. Πανεπιστήμιο Πατρών.

ΚΕΦΑΛΑΙΟ 3: Το IoT (Internet of Things)

3.1. Ορισμός του IoT

Το Internet of Things (IoT) είναι ένα δίκτυο φυσικών αντικειμένων, συσκευών, οχημάτων, κτιρίων αλλά και άλλων αντικειμένων τα οποία περιέχουν ενσωματωμένα ηλεκτρονικά συστήματα, λογισμικά, αισθητήρες και διαδικτυακή δυνατότητα σύνδεσης - κάτι που επιτρέπει σε αυτά τα αντικείμενα να συλλέγουν και να ανταλλάσσουν δεδομένα. Το IoT δίνει την δυνατότητα στα αντικείμενα αυτά να ελέγχονται απομακρυσμένα μέσω της υπάρχουσας δικτυακής υποδομής δημιουργώντας ευκαιρίες άμεσης ενσωμάτωσης του φυσικού κόσμου με τα υπολογιστικά συστήματα έχοντας ως αποτέλεσμα τη βελτίωση της αποτελεσματικότητας και της ακρίβειας αλλά και τη μείωση του κόστους. Από την στιγμή μάλιστα που το IoT εξοπλίζεται με αισθητήρες και ενεργοποιητές αποτελεί μέρος έξυπνων συστημάτων της καθημερινότητας όπως είναι τα έξυπνα σπίτια, οχήματα και πόλεις. Κάθε αντικείμενο αναγνωρίζεται μοναδικά από το ενσωματωμένο υπολογιστικό σύστημα και μπορεί να λειτουργεί τόσο αυτόνομα όσο και σε συνεργασία με την υπόλοιπη διαδικτυακή υποδομή.

Ο όρος Internet of Things προτάθηκε από τον Kevin Ashton το 1999 αν και ήταν υπό συζήτηση τουλάχιστον από το 1991. Η ιδέα του Internet of Things αρχικά έγινε δημοφιλής μέσω του Auto-ID Center στο MIT αλλά και μέσω σχετικών δημοσιεύσεων ανάλυσης της αγοράς. Εκείνες τις ημέρες η ταυτοποίηση ραδιοσυχνοτήτων (RFID) θεωρήθηκε ως προϋπόθεση για το Internet of Things, αφού αν όλα τα αντικείμενα και οι άνθρωποι ήταν εξοπλισμένοι στην καθημερινότητα με αναγνωριστικά, θα μπορούσαν να διαχειρίζονται και να απογράφονται από υπολογιστές. Εκτός από την χρήση RFID, η σήμανση των πραγμάτων μπορεί να επιτευχθεί μέσα από τεχνολογίες όπως η κοντινού τύπου επικοινωνία, οι κώδικες QR, τα barcodes και η ψηφιακή υδατογράφηση.

Πριν αρχίσουμε να κατανοούμε τη σημασία του IoT είναι πρώτα απαραίτητο να καταλάβουμε τις διαφορές μεταξύ του Διαδικτύου (Internet) και του Παγκόσμιου Ιστού (World Wide Web) όροι που συχνά χρησιμοποιούνται εναλλακτικά.

Το Διαδίκτυο είναι το φυσικό επίπεδο που αποτελείται από μεταγωγείς, δρομολογητές και άλλες συσκευές. Η κύρια λειτουργία του είναι να μεταφέρει πληροφορίες από το ένα σημείο στο άλλο γρήγορα, αξιόπιστα και με ασφάλεια. Ο

Παγκόσμιος Ιστός από την άλλη πλευρά, είναι έλα επίπεδο εφαρμογών που λειτουργεί πάνω από το Διαδίκτυο. Ο κύριος ρόλος του είναι να παρέχει μία διεπαφή που καθιστά τις πληροφορίες που ρέουν σε όλο το Διαδίκτυο χρησιμοποιήσιμες.

3.2. Το IoT στη ζωή μας

Σήμερα ο όρος Internet of Things (το Διαδίκτυο των Πραγμάτων) χρησιμοποιείται για να υποδηλώσει την προηγμένη συνδεσιμότητα συσκευών, συστημάτων και υπηρεσιών πέρα από τη μηχανή με μηχανή επικοινωνία αφού καλύπτει μία ποικιλία από πρωτόκολλα, τομείς και εφαρμογές.

Η Cisco δημιούργησε έναν δυναμικό "μετρητή συνδέσεων" προκειμένου να παρακολουθεί τον εκτιμώμενο αριθμό συνδεδεμένων αντικειμένων από τον Ιούλιο του 2013 μέχρι τον Ιούλιο του 2020. Η ιδέα αυτή, όπου οι συσκευές συνδέονται στο Διαδίκτυο/Παγκόσμιο Ιστό μέσω χαμηλής ισχύος ραδιοσήματα, είναι η πιο ενεργή περιοχή έρευνας στο IoT. Τα ραδιοσήματα χαμηλής ισχύος δεν χρειάζεται να χρησιμοποιούν Wi-Fi ή Bluetooth. Χαμηλότερης ενέργειας και χαμηλότερου κόστους εναλλακτικές διερευνώνται υπό την κατηγορία του Chirp Networks. Βρίσκεται υπό σκέψη μια εκδοχή που θέλει όλες τις συσκευές να χρησιμοποιούν μία διεύθυνση IP ως ένα μοναδικό αναγνωριστικό. Για κόμβους, γέφυρες και άλλες συσκευές τύπου δρομολόγησης αυτό φαίνεται να είναι περιττό [1].

Το Internet of Things (IoT), κάποιες φορές αναφέρεται ως το Διαδίκτυο των αντικειμένων και υπόσχεται να αλλάξει τα πάντα συμπεριλαμβανομένων και εμάς τους ίδιους. Αυτό μπορεί να μοιάζει σαν μία τολμηρή δήλωση αλλά λαμβάνοντας υπόψη τον αντίκτυπο που έχει στην εκπαίδευση, την επικοινωνία, τις επιχειρήσεις, την επιστήμη αλλά και την ανθρωπότητα, αναμφισβήτητα το Διαδίκτυο είναι ένα από τα πιο σημαντικά και ισχυρά δημιουργήματα σε όλη την ανθρώπινη ιστορία. Έτσι, θεωρώντας ότι το IoT αντιπροσωπεύει την επόμενη εξέλιξη του Διαδικτύου, κάνει ένα τεράστιο άλμα στην ικανότητά του να συγκεντρώνει, να αναλύει και να διανέμει δεδομένα που μπορούμε να μετατρέψουμε σε πληροφορίες, γνώσεις και τελικά σοφία. Στο πλαίσιο αυτό το IoT γίνεται ιδιαίτερα σημαντικό και χρήσιμο.

Ήδη, οι εργασίες του IoT βρίσκονται σε εξέλιξη και υπόσχονται να κλείσουν το χάσμα μεταξύ φτώχειας και πλούτου, βελτιώνοντας την κατανομή των πόρων του κόσμου σε αυτούς που τα χρειάζονται περισσότερο, βοηθώντας μας έτσι να

κατανοήσουμε τον πλανήτη μας έτσι ώστε να μπορούμε να είμαστε πιο παραγωγικοί και λιγότερο αντιδραστικοί. Παρόλα αυτά υπάρχουν πολλά εμπόδια που απειλούν να επιβραδύνουν την ανάπτυξη του IoT, συμπεριλαμβανομένης της μετάβασης στο IPv6, έχοντας ένα κοινό σύνολο προτύπων και ανάπτυξης των πηγών ενέργειας για εκατομμύρια, ακόμη και δισεκατομμύρια μικροσκοπικούς αισθητήρες. Ωστόσο καθώς οι επιχειρήσεις, οι κυβερνήσεις, οι οργανισμοί τυποποίησης και η ακαδημαϊκή κοινότητα λύνουν τις προκλήσεις αυτές, το IoT θα συνεχίσει να προοδεύει.

3.3. Κύρια χαρακτηριστικά του IoT

Από τεχνικής άποψης, το Internet of Things δεν είναι το αποτέλεσμα μιας μόνο πρωτότυπης τεχνολογίας. Σε αντίθεση, διάφορες συμπληρωματικές τεχνικές εξέλιξης παρέχουν δυνατότητες που συνεργάζονται για να βοηθήσουν να γεφυρωθεί το χάσμα μεταξύ του εικονικού και του φυσικού κόσμου. Οι δυνατότητες αυτές περιλαμβάνουν:

• Επικοινωνία και συνεργασία: Τα αντικείμενα έχουν την δυνατότητα να δικτυώνονται με τους πόρους του Διαδικτύου ή ακόμη και το ένα με το άλλο, να κάνουν χρήση των δεδομένων και των υπηρεσιών και να ενημερώνουν την κατάστασή τους. Οι ασύρματες τεχνολογίες, όπως το GSM και UMTS, Wi-Fi, Bluetooth, ZigBee και διάφορα άλλα ασύρματα πρότυπα δικτύωσης που είναι αυτή τη στιγμή υπό ανάπτυξη, ιδιαίτερα εκείνων που σχετίζονται με τα προσωπικά ασύρματα δίκτυα (WPANs), έχουν πρωταρχική σημασία εδώ.

• Διευθυνσιοδότηση: Σε ένα Internet of Things, τα αντικείμενα μπορούν να τοποθετούνται και να διευθυνσιοδοτούνται μέσω της ανεύρεσης ή το όνομα των υπηρεσιών κι έτσι έχουν την δυνατότητα να επιβεβαιώνονται ή να ρυθμίζονται εξ αποστάσεως.

• Ταυτοποίηση: Τα αντικείμενα είναι μοναδικά αναγνωρίσιμα. Οι τεχνολογίες RFID, NFC (Near Field Communication) και οι οπτικά αναγνώσιμοι κώδικες (bar codes) είναι παραδείγματα τεχνολογιών με τις οποίες μπορούν να εντοπιστούν ακόμη και παθητικά αντικείμενα που δεν έχουν ενσωματωμένους ενεργειακούς πόρους και να αναγνωριστούν με τη βοήθεια ενός ‘διαμεσολαβητή’ όπως μία συσκευή αναγνώρισης RFID ή ένα κινητό τηλέφωνο. Η ταυτοποίηση επιτρέπει στα αντικείμενα να συνδέονται με πληροφορίες που σχετίζονται με το συγκεκριμένο

αντικείμενο και μπορούν να ανακτηθούν από έναν διακομιστή, υπό τον όρο ο μεσολαβητής να είναι συνδεδεμένος στο δίκτυο.

• Ανίχνευση: Τα αντικείμενα διαθέτουν αισθητήριες με την βοήθεια των οποίων συλλέγουν πληροφορίες σχετικά με το περιβάλλον τους, καταγράφοντας, διαβιβάζοντας ή αντιδρώντας άμεσα σε αυτό.

• Ενεργοποίηση: Τα αντικείμενα περιέχουν ενεργοποιητές προκειμένου να χειριστούν το περιβάλλον τους. Για παράδειγμα μετατρέποντας τα ηλεκτρικά σήματα σε μηχανική κίνηση. Τέτοιοι ενεργοποιητές μπορούν να χρησιμοποιηθούν για να ελέγξουν εξ αποστάσεως διεργασίες στον πραγματικό κόσμο μέσω του Διαδικτύου.

• Ενσωματωμένη επεξεργασία πληροφοριών: Έξυπνα αντικείμενα διαθέτουν έναν επεξεργαστή ή μικροελεγκτή, καθώς και την ικανότητα αποθήκευσης. Αυτοί οι πόροι μπορούν να χρησιμοποιηθούν για παράδειγμα, για να επεξεργάζονται και να ερμηνεύουν πληροφορίες των αισθητήρων ή ακόμη και να παρέχουν στα προϊόντα μία μνήμη για το πως έχουν χρησιμοποιηθεί.

• Εντοπισμός: Τα έξυπνα αντικείμενα έχουν επίγνωση της φυσικής τους θέσης ή μπορούν να εντοπίζονται. Το GPS ή το δίκτυο κινητής τηλεφωνίας είναι κατάλληλες τεχνολογίες για την επίτευξη αυτού του στόχου, καθώς και οι ραδιοφάροι (π.χ. γειτονικοί WLAN σταθμοί βάσεις ή αναγνώστες RFID με γνωστές συντεταγμένες) όπως επίσης και οι οπτικές ίνες.

• Διεπαφές χρήστη: Τα έξυπνα αντικείμενα μπορούν να επικοινωνούν με τους ανθρώπους με κατάλληλο τρόπο (είτε άμεσα είτε έμμεσα, για παράδειγμα μέσω ενός smart phone). Καινοτόμα παραδείγματα αλληλεπίδρασης είναι: χειροπιαστές διεπαφές χρήστη, ευέλικτες πολυμερείς βάσεις εικόνας και φωνής ή μέθοδοι αναγνώρισης χειρονομιών.

Οι περισσότερες ειδικές εφαρμογές χρειάζονται μόνο ένα υποσύνολο αυτών των δυνατοτήτων, ιδιαίτερα μετά την εφαρμογή όλων αυτών είναι συχνά δαπανηρό και απαιτεί σημαντική τεχνική προσπάθεια. Οι εφαρμογές Logistics για παράδειγμα, αυτή τη στιγμή επικεντρώνονται στην προσέγγιση εντοπισμού (δηλ. τη θέση του τελευταίου σημείου ανάγνωσης) και στην σχετικά χαμηλού κόστους αναγνώριση των αντικειμένων που χρησιμοποιούν RFID ή bar codes. Αισθητήρες δεδομένων ή ενσωματωμένοι επεξεργαστές είναι περιορισμένοι σε τέτοιες εφαρμογές εφοδιασμού

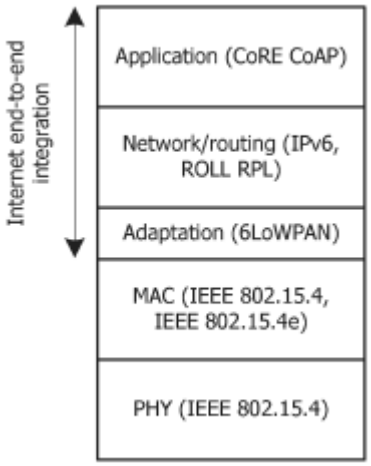
όπου οι πληροφορίες είναι απαραίτητες και ουσιαστικής σημασίας, όπως η θερμοκρασία που πρέπει να ελέγχεται κατά τη μεταφορά εμβολίων. Οι προάγγελοι της επικοινωνίας σε αντικείμενα καθημερινής χρήσης έχουν κάνει ήδη την εμφάνισή τους, ιδιαίτερα σε σχέση με το RFID, για παράδειγμα, η επικοινωνία μικρής εμβέλειας όπως η χρήση έξυπνων κλειδιών- καρτών από τις πόρτες των δωματίων ενός ξενοδοχείου ή αντίστοιχα εισιτήρια για σκι που επικοινωνούν με τα lift. Περισσότερο φουτουριστικά σενάρια περιλαμβάνουν ένα έξυπνο τραπέζι παιγνιόχαρτων, όπου η πορεία του παιχνιδιού βιντεοσκοπείται χρησιμοποιώντας τραπουλόχαρτα εξοπλισμένα με RFID. Παρόλα αυτά όλες αυτές οι εφαρμογές εξακολουθούν να περιλαμβάνουν ειδικά συστήματα σε τοπική ανάπτυξη, επομένως δεν μιλάμε για ένα 'Διαδίκτυο' με την έννοια ενός ανοικτού, επεκτάσιμου και τυποποιημένου συστήματος [2].

3.4 Ασφάλεια

Μια διαφορετική κριτική είναι ότι το IoT αναπτύσσεται ταχύτατα χωρίς την κατάλληλη εξέταση των σημαντικών προκλήσεων ασφαλείας που εμπλέκονται και των ρυθμιστικών αλλαγών που ενδέχεται να χρειαστούν. Πιο συγκεκριμένα όπως το IoT εξαπλώνεται ευρέως οι επιθέσεις στο κυβερνοχώρο τείνουν να γίνουν φυσικές (και όχι απλώς εικονικές) [3].

3.4.1 Τα πρωτόκολλα του IoT

Όπως είναι γνωστό ο χώρος του Διαδικτύου είναι ένας χώρος που δημιουργεί σε όλους μας μία αμφοβολία σε ότι αφορά την ασφάλειά του. Γι' αυτό το λόγο το Ινστιτούτο των Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) η IETF (Internet Engineering Task Force) σχεδιάζουν μία σειρά από πρωτόκολλα επικοινωνίας και ασφαλείας που θα παίξουν σημαντικό ρόλο στο IoT. Ο σχεδιασμός και η εφαρμογή αυτών των πρωτοκόλλων λαμβάνουν υπόψη του τους περιορισμούς και τα χαρακτηριστικά των συσκευών-αισθητήρων που δομούν το IoT. Αυτά τα χαρακτηριστικά είναι η χαμηλή κατανάλωση ενέργειας και ο χαμηλός ρυθμός μετάδοσης των ασύρματων συνδέσεων. Τα ίδια χαρακτηριστικά είχαν εμπνεύσει και τα Ασύρματα Δίκτυα Αισθητήρων (WSN) στο παρελθόν με σκοπό να απομονώσουν και να προστατεύσουν αυτά τα δίκτυα από τις διαδικτυακές επιθέσεις. Στην εικόνα που ακολουθεί συνοψίζονται τα επικοινωνιακή πρωτόκολλα του IoT.



Τα πρωτόκολλα του IoT

Αναλύουμε αυτά τα πρωτόκολλα από κάτω προς τα πάνω:

- Επικοινωνίες χαμηλής κατανάλωσης ενέργειας στο φυσικό στρώμα (PHY) και στο Μέσο Πρόσβασης (MAC: Medium Access Protocol) που υποστηρίζονται από το IEEE 802.15.4. Είναι μία βάση για την ορθή εκκίνηση του IoT και βοηθάει στην ομαλή λειτουργία και συνεργασία του φυσικού στρώματος με τα ανώτερα στρώματα.
- Τα συγκεκριμένα πρωτόκολλα χρειάζονται 102 bytes για τη μετάδοση δεδομένων, τιμή που είναι αισθητά μικρότερη από την MTU (Maximum Transmission Unit) του IPV6 που είναι 1280 bytes. Ακολουθεί το 6LoWPAN που είναι ένα πρωτόκολλο προσαρμογής-προθάλαμος για τα πρωτόκολλα που υλοποιούν τη διαδικτυακή λειτουργία του IoT. Το συγκεκριμένο πρωτόκολλο επιτρέπει τη μετάδοση IPv6 πακέτων ενθυλακωμένα στο IEEE 802.15.4. Ουσιαστικά το 6LoWPAN υλοποιεί λειτουργίες όπως θρυμματισμός πακέτων και επανένωσή τους στον τελικό αποδέκτη.
- Η Δρομολόγηση με χρήση του 6LoWPAN υποστηρίζεται από πρωτόκολλα δρομολόγησης για χαμηλή ισχύ και μετάδοση με απώλειες (Lossy). Πιο συγκεκριμένα, οι εφαρμογές του IoT ενσωματώνουν μία σειρά από προφίλ λειτουργίας τα οποία προκαθορίζουν τις απαιτήσεις δρομολόγησης και τους στόχους για βέλτιστη μετάδοση.
- Τέλος στο επίπεδο εφαρμογής συναντάμε το CoRE CoAP. Αυτό το πρωτόκολλο έχει σχεδιαστεί από τον IETF με σκοπό την παροχή

διαλειτουργικότητας σε συμμόρφωση με την αναπαραστατική αρχιτεκτονική μεταφοράς καταστάσεων του διαδικτύου.

Η χρήση του IPv6 στο IoT μπορεί να δώσει πολλές ευκαιρίες, λόγω της αφθονίας διευθύνσεων. Όμως είναι απαραίτητη η ευελιξία και η βελτίωση σε κάθε επίπεδο του πρωτοκόλλου ειδικά όταν πρόκειται για παράδοση IPv6 πακέτων σε δίκτυα περιορισμένης ενέργειας σε συνδέσμους (links) 802.15.4 (Low Power and Lossy Networks- 6LoWPANs).

Το κίνητρο για τη χρήση IP δικτύων σε τέτοια περιβάλλοντα δεν είναι άλλο από την διεισδυτικότητα που έχουν αποκτήσει μέχρι τώρα, προσφέροντας ήδη υπάρχουσες υποδομές, και τεχνολογίες που λειτουργούν αποδεδειγμένα. Επιπλέον, τα ανοικτά πρότυπα αποτελούν λόγω υιοθέτησής τους, όπως και η μη ανάγκη για ενδιάμεσες συσκευές, όταν πρόκειται για διασύνδεση συσκευών που επικοινωνούν μέσω IP. Υπάρχει η ανάγκη για επίσημη προσαρμογή του IPv6 σε δίκτυα που χρησιμοποιούν το φυσικό επίπεδο του προτύπου IEEE 802.15.4, το οποίο έχει σημαντικές διαφορές από άλλες τεχνολογίες. Η ομάδα εργασίας του 6LoWPAN έχει ορίσει μηχανισμούς συμπίεσης για την ενθυλάκωση (encapsulation) και τις κεφαλίδες (header) των πακέτων που στέλνονται και λαμβάνονται μέσω δικτύων βασισμένα στο πρότυπο IEEE 802.15.4. Το πρωτόκολλο 6LoWPAN προσφέρει ένα επίπεδο προσαρμογής που επιτρέπει τη μεταφορά IPv6 πακέτων σε 802.15.4 συνδέσμους και περιλαμβάνει τον τεμαχισμό και την ανασυναρμολόγηση (Fragmentation / reassembly) IPv6 πακέτων, όπως και συμπίεση των κεφαλίδων IPv6 και UDP/ICMP. Μετά τη συμπίεση επιτυγχάνεται σύμπτυξη των παραπάνω που μπορεί να φτάνουν τα 7 bytes το οποίο εμφανώς αφήνει χώρο για περισσότερο payload. Όσον αφορά στη θεματική περιοχή του Internet of Things επειδή οι συσκευές είναι μικρές σε μέγεθος, με περιορισμένες δυνατότητες επεξεργασίας, το πρωτόκολλο αυτό θεωρήθηκε ιδανικό για εφαρμογή σε συσκευές που συμμετέχουν στο συγκεκριμένο περιβάλλον Το 6LoWPAN είναι το ακρώνυμο της έκφρασης “Ipv6 over Low power Wireless Personal Area Networks”. Επίσης είναι και το όνομα μιας ερευνητικής ομάδας σχετικής με το Διαδίκτυο στον οργανισμό IETF. Η ιδέα του 6LoWPAN, ξεκίνησε από το γεγονός ότι το πρωτόκολλο του Internet (IP) μπορούσε και έπρεπε να βρει εφαρμογή και σε μικρότερες συσκευές. Οι μικρής ισχύος συσκευές με περιορισμένη υπολογιστική ισχύ θα πρέπει να μπορούν να χρησιμοποιούνται στο Internet of Things.

Η ερευνητική ομάδα 6LoWPAN όρισε την διαδικασία ενθυλάκωσης και τον μηχανισμό συμπίεσης προμετωπίδας ώστε να επιτρέπεται στα IPv6 να στέλνονται και να λαμβάνονται πακέτα πάνω από IEEE 802.15.4. Όπως τα πρωτόκολλα IPv4 και IPv6 είναι υπεύθυνα για την δρομολόγηση και παράδοση δεδομένων στα LAN, MAN και WAN δίκτυα, έτσι και οι συσκευές IEEE 802.15.4 παρέχουν δυνατότητα της ασύρματης επικοινωνίας των δεδομένων των αισθητήρων. Ωστόσο η εγγενής φύση των δύο δικτύων είναι διαφορετική. [8].

3.4.2 Απαιτήσεις Ασφαλείας

Σε γενικές γραμμές τα πρωτόκολλα που μόλις αναφέραμε θα πρέπει να δίνουν τις απαιτούμενες εξασφαλίσεις σε όρους όπως εμπιστευτικότητα, ακεραιότητα, αυθεντικότητα και τη μη άρνηση, πράγμα που συμβαίνει για όλες τις προϋποθέσεις ασφαλείας όλων των δικτύων. Για την ορθή ασφάλεια του IoT υπάρχουν δύο τρόποι: Ή μέσω του πρωτοκόλλου αυτού καθαυτού ή από μία σειρά εξωτερικών μηχανισμών.

Ένα άλλο σκέλος ασφαλείας αφορά τις έννοιες: προστασία της ιδιωτικής ζωής, την ανωνυμία, την ευθύνη και την εμπιστοσύνη, οι οποίες θα είναι θεμελιώδεις για την κοινωνική αποδοχή των περισσότερων από τις μελλοντικές εφαρμογές IoT που απασχολούν συσκευές ανίχνευσης. Οι συγκεκριμένες έννοιες ασφαλείας είναι πολύ πιο απαιτητικές και πιο δύσκολα διαχειρίσιμες.

3.4.3 Παρουσίαση του πρωτοκόλλου IoT

Η IEEE 802.15 είναι μία ομάδα που δημιουργήθηκε απο την επιτροπή της IEEE για να καθορίσει τα πρότυπα για τα προσωπικά ασύρματα δίκτυα επικοινωνίας (WPAN). Η ομάδα IEEE 802.15.4 καθορίζει ένα χαμηλού ρυθμού WPAN με 20kbps, 40kbps kai 250kbps για διαφορετικές ζώνες συχνοτήτων όπως θα δούμε στη συνέχεια. Το πρότυπο 802.15.4 της επιτροπής IEEE ειναι ένα πρότυπο το οποίο περιγράφει το φυσικό επίπεδο και το MAC υποεπίπεδο για χαμηλού ρυθμού μετάδοσης ασύρματα προσωπικά δίκτυα. Η πρώτη έκδοση του προτύπου αυτού είχε ανακοινωθεί το 2003. Μέσα απο το πέρας των χρόνων το πρότυπο αναθεωρείται και βελτιωμένες εκδόσεις του προτύπου ανακοινώνονται. Οι πιο σημαντικές εξ αυτών είναι του 2006 και του 2011. Το πρότυπο αυτό εξυπηρετεί, σαν PHY και MAC επίπεδα, για τις περισσότερες απο τις πιο γνωστές ασύρματες τεχνολογίες δικτύων, όπως: ZigBee, ISA100.11a, WirelessHART, MiWi, Thread και μπορεί να

χρησιμοποιηθεί ακόμα και με το 6LoWPAN. Αυτές οι τεχνολογίες επέκτειναν το πρωτόκολλο συμπεριλαμβάνοντας και άλλα επίπεδα τα οποία δεν περιγράφονται στο συγκεκριμένο πρότυπο της ομάδας 802.15. Συσκευές που χρησιμοποιούν τέτοιες τεχνολογίες χρησιμοποιούνται για να μεταδώσουν πληροφορίες σε σχετικά μικρές αποστάσεις και χρειάζονται, σε αντίθεση με τα WLAN's δίκτυα, πολύ μικρότερη ή και καθόλου υποδομή. Αυτό το τόσο σημαντικό χαρακτηριστικό επιτρέπει την δημιουργία μικρών, ενεργειακά αποδοτικών και φτηνών λύσεων για ενα τεράστιο εύρος συσκευών. Το βασικό πρότυπο υποστηρίζει επικοινωνία μέχρι και δέκα μέτρα και διαφορετικούς ρυθμούς μεταφοράς δεδομένων και συχνοτήτων. Αυτά ορίζονται απο τα διαφορετικά φυσικά επίπεδα που ορίζονται και εξηγούνται απο το πρότυπο.

Όπως προαναφέρθηκε, ο στόχος του IEEE 802.15.4 προτύπου είναι να καθορίσει το PHY επίπεδο και το MAC υποεπίπεδο, που πολλές φορές αναφέρεται σαν επίπεδο ζεύξης δεδομένων, Data Link Layer (DLL), για ασύρματα δίκτυα χαμηλού ρυθμού μετάδοσης τα οποία αποτελούνται από σταθερές ή κινητές συσκευές. Οι συσκευές αυτές τροφοδοτούνται από μπαταρίες ή κάποια άλλη πηγή περιορισμένης ενέργειας.

Το πρότυπο IEEE 802.15.4 έχει στόχο τα δίκτυα μικρής εμβέλειας και χαμηλής ενέργειας (low-power personal area networks) και συνιστά χαμηλό κόστος. Υποστηρίζει data rates στα 250 kb/s, 40 kb/s και 20 kb/s, λειτουργία σε αρχιτεκτονικές αστέρα και peer-to-peer και αξιοπιστία μεταφοράς δεδομένων. Επιπλέον η κατανάλωση ενέργειας λειτουργίας προσφέρει γρήγορη επικοινωνία μεταξύ των συσκευών (low latency devices).

Βασικές έννοιες που πρέπει να γνωρίζει κάποιος για το πρότυπο είναι ο συντονιστής (coordinator), PAN coordinator, και συσκευή δικτύου (network device). Ο coordinator είναι η συσκευή με λειτουργικότητα συσκευής δικτύου που προσφέρει συντονισμό και άλλες υπηρεσίες στο δίκτυο. Ο PAN coordinator είναι ο κυρίαρχος συντονιστής (controller) του PAN δικτύου. Κάθε τέτοιο δίκτυο περιλαμβάνει ακριβώς έναν PAN coordinator. Τέλος, μια συσκευή δικτύου είναι κάθε υλοποίηση συσκευής που περιλαμβάνει έλεγχο πρόσβασης στο IEEE 802.15.4 και φυσική διεπαφή στο ασύρματο μέσο [3].

Το πρότυπο IEEE 802.15.4 καθορίζει μικρό μέγεθος πακέτου στο data link layer. Αυτό συμβαίνει αφενός λόγω της ανάγκης χαμηλής κατανάλωσης και αφετέρου λόγω της φύσης του δικτύου που συνιστά απώλειες, ενώ η επανάληψη αποστολής πακέτων

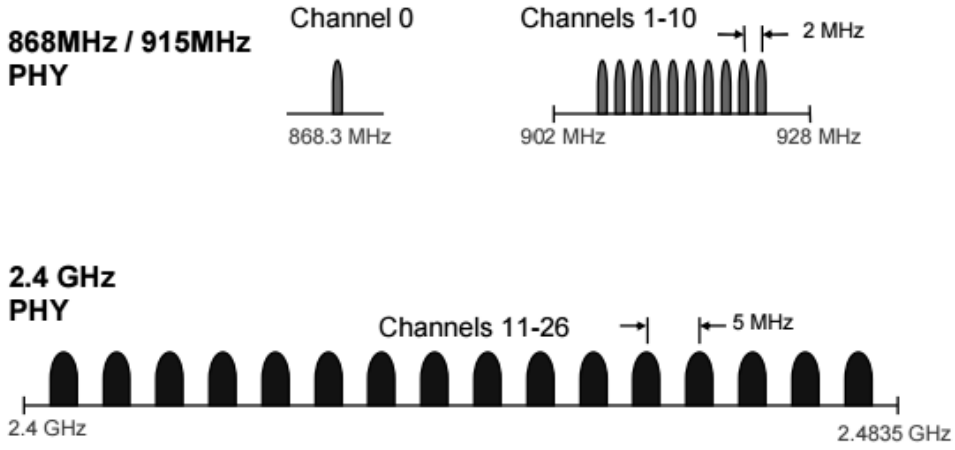
πρέπει να γίνεται με όσο γίνεται μικρότερο μέγεθος πακέτου. Με συνολικό μέγεθος πλαισίου (frame) 127 bytes, οι κεφαλίδες καταλαμβάνουν περίπου 68 bytes (με 40 byte IPv6 κεφαλίδα, 8 byte UDP κεφαλίδα, περίπου 20 byte data link layer κεφαλίδα και πιθανόν πρόσθετες κεφαλίδες του IPv6) μένουν για δεδομένα (payload) περίπου 58 byte για δεδομένα, το οποίο σημαίνει πως περίπου το μισό πακέτο που στέλνεται αποτελείται από κεφαλίδες.

Η αρχιτεκτονική IEEE 802.15.4 παρουσιάζεται με την μορφή ενός αριθμού μπλοκ, προκειμένου να απλοποιηθεί το πρότυπο. Αυτά τα μπλοκ ονομάζονται επίπεδα (layers). Κάθε επίπεδο είναι υπεύθυνο για ένα μέρος του προτύπου και προσφέρει υπηρεσίες σε τα ανώτερα στρώματα. Οι διασυνδέσεις μεταξύ των επιπέδων χρησιμεύουν για να καθορίσουν τις λογικές συνδέσεις που περιγράφονται σε αυτό το πρότυπο. Μια συσκευή LR-WPAN περιλαμβάνει τουλάχιστον ένα επίπεδο PHY, το οποίο περιέχει τον πομποδέκτη ραδιοσυχνοτήτων (RF), μαζί με έναν μηχανισμό παρακολούθησης χαμηλού επιπέδου, και ένα επίπεδο MAC που παρέχει φυσική πρόσβαση στο κανάλι για όλους τους τύπους μεταφοράς δεδομένων.

3.4.3.1 Επίπεδο PHY του IEEE 802.15.4

Το επίπεδο PHY παρέχει δύο υπηρεσίες: την υπηρεσία δεδομένων PHY και την υπηρεσία διαχείρισης PHY. Η υπηρεσία δεδομένων PHY επιτρέπει τη μετάδοση και λήψη μονάδων δεδομένων πρωτοκόλλου PHY (PPDUs-Phy Protocol Data Units) σε όλη την φυσική ακτίνα του καναλιού.. Τα χαρακτηριστικά του PHY είναι η ενεργοποίηση και απενεργοποίηση του ασύρματου πομποδέκτη, η διαδικασία ED (Energy Detection), η διαδικασία LQI (Link Quality Indication), η επιλογή καναλιού, η διαδικασία αξιολόγησης ελεύθερου καναλιού (CCA-Clear Channel Assessement), καθώς και η μετάδοση και λήψη πακέτων μέσω του φυσικού μέσου.

Παρέχει τη διασύνδεση με το φυσικό μέσο μετάδοσης (π.χ. ραδιόφωνο). Το PHY αποτελείται από δύο στρώματα που λειτουργούν σε δύο ξεχωριστές περιοχές συχνοτήτων. Η χαμηλότερη συχνότητα PHY στρώμα καλύπτει τόσο την ευρωπαϊκή ζώνη 868MHz και 915MHz μπάντα που χρησιμοποιούνται σε χώρες όπως οι ΗΠΑ και η Αυστραλία. Η υψηλότερη συχνότητα PHY στρώμα (2.4GHz) χρησιμοποιείται σχεδόν σε όλο τον κόσμο.

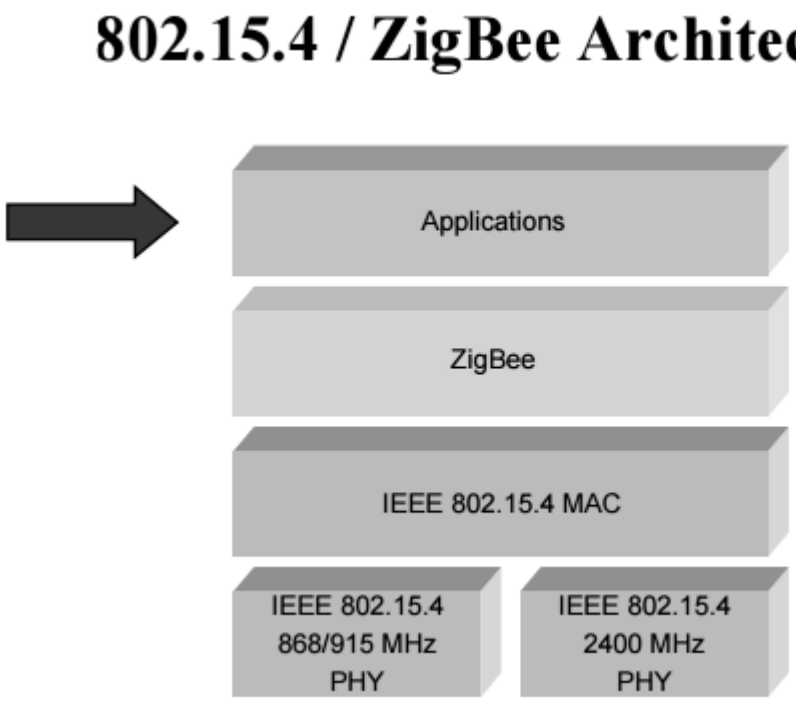


Ενώ και τα δύο αυτά ασύρματα πρότυπα ασχολούνται με εφαρμογές υψηλότερου εύρους ζώνης πρόσβασης στο Διαδίκτυο, το 802.15.4 αναπτύχθηκε με χαμηλότερο ρυθμό μετάδοσης δεδομένων, για απλή συνδεσιμότητα και χαμηλή κατανάλωση ενέργειας. Το πρότυπο 802.15.4 ορίζει ότι η επικοινωνία μπορεί να κυμαίνεται στα 868 - 868,8 MHz, στα 902-928 MHz ή 2,400 - 2,4835 GHz για τις βιομηχανικές, επιστημονικές και ιατρικές (ISM) ζώνες. Αν οποιαδήποτε από αυτές τις μπάντες είναι τεχνικά δυνατόν να χρησιμοποιηθεί από τις συσκευές , η ζώνη των 2,4 GHz είναι πιο δημοφιλής, καθώς είναι ανοιχτή στις περισσότερες χώρες σε όλο τον κόσμο. Τα 868 MHz, καθορίζονται κατά κύριο λόγο για ευρωπαϊκή χρήση , ενώ η ζώνη 902-928 MHz μπορεί να χρησιμοποιηθεί μόνο στις Ηνωμένες Πολιτείες, τον Καναδά και σε μερικές άλλες χώρες και εδάφη που δέχονται την FCC (Federal Communications Commission) Ομοσπονδιακή Επιτροπή Επικοινωνιών. Το πρότυπο 802.15.4 ορίζει ότι η επικοινωνία πρέπει να γίνεται σε κανάλια των 5 MHz που κυμαίνονται μεταξύ 2,405 - 2,480 GHz . Στη ζώνη συχνοτήτων 2,4 GHz, κατ 'ανώτατο όριο over-the –air, ο ρυθμός δεδομένων έχει καθοριστεί στα 250 kbps, αλλά λόγω του γενικού του πρωτοκόλλου το πραγματικό θεωρητικό μέγιστο ποσοστό των δεδομένων είναι περίπου το μισό από αυτό. Ενώ το πρότυπο καθορίζει κανάλια των 5 MHz, μόνο τα 2 MHz περίπου του καναλιού καταναλώνονται από το χρησιμοποιούμενο εύρος ζώνης. Στα 2,4 GHz, το 802.15.4 καθορίζει τη χρήση του Direct Sequence Spread Spectrum και χρησιμοποιεί ένα Offset Quadrature Phase Shift Keying (O - QPSK) με παλμό μισού ημιτόνου διαμόρφωσης ώστε να διαμορφώνει το RF φορέα [14].

3.4.3.2 Επίπεδο MAC του IEEE 802.15.4

Το επίπεδο MAC παρέχει δύο υπηρεσίες: την υπηρεσία δεδομένων MAC και την υπηρεσία διαχείρισης MAC διασυνδεόμενη με την οντότητα διαχείρισης MAC επιπέδου (MLME) ονομαζόμενη σημείο πρόσβασης υπηρεσίας (SAP-Service Access Point) (Γνωστός ως MLMESAP). Η υπηρεσία δεδομένων MAC επιτρέπει τη μετάδοση και λήψη μονάδων δεδομένων πρωτοκόλλου MAC (MPDUs- Mac Protocol Data Units) σε όλη την υπηρεσία δεδομένων PHY. Τα χαρακτηριστικά του επιπέδου MAC είναι η διαχείριση των Beacon , η πρόσβαση στο κανάλι, η διαχείριση των GTS, επικύρωση δεδομένων, αναγνωρισμένη παράδοσης πλαισίου δεδομένων, η σύνδεση και η αποσύνδεση από το δίκτυο. Επιπλέον, το επίπεδο MAC παρέχει μέσα για την δημιουργία μηχανισμών ασφαλείας που σχετίζονται με την εφαρμογή. Είναι υπεύθυνο για την παροχή αξιόπιστης επικοινωνίας μεταξύ ενός κόμβου και των άμεσων γειτόνων του, συμβάλλοντας στην αποφυγή συγκρούσεων και στη βελτίωση της αποτελεσματικότητας. Το στρώμα MAC είναι επίσης υπεύθυνο για τη συναρμολόγηση και την αποσύνθεση των πακέτων δεδομένων και πλαισίων. Τα κύρια χαρακτηριστικά του είναι:

- Εξαιρετικά χαμηλό κόστος
- Ευκολία εφαρμογής
- Αξιόπιστη μεταφορά δεδομένων
- Λειτουργία μικρής εμβέλειας
- Πολύ χαμηλή κατανάλωση ενέργειας



3.4.3.3 Δομή SuperFrame

Το πρότυπο αυτό επιτρέπει την προαιρετική χρήση της δομής υπερ-πλαισίου (superframe). Η μορφή του superframe ορίζεται από τον συντονιστή. Το superframe οριοθετείται με beacons (φάροι) δικτύου που αποστέλλονται από το συντονιστή και διαιρείται σε 16 υποδοχές ίσης διάρκειας. Προαιρετικά, το superframe μπορεί να έχει ένα ενεργό και ένα ανενεργό τμήμα. Κατά την διάρκεια του ανενεργού τμήματος, ο συντονιστής είναι σε θέση να εισέλθει σε μία κατάσταση χαμηλής κατανάλωσης εξοικονομώντας ενέργεια. Η μετάδοση του πλαισίου beacon ξεκινά από την αρχή της πρώτης υποδοχής του κάθε superframe. Αν ένας συντονιστής δεν επιθυμεί να χρησιμοποιήσει μια δομή superframe, απενεργοποιεί τις μεταδόσεις beacon. Τα beacons χρησιμοποιούνται για τον συγχρονισμό των συνδεδεμένων συσκευών, για τον προσδιορισμό του PAN και για την περιγραφή της δομής του superframe.

Κάθε συσκευή που επιθυμεί να επικοινωνήσει κατά τη διάρκεια της περιόδου contention access period (CAP) μεταξύ των δύο beacon, ανταγωνίζεται άλλες συσκευές μέσω μηχανισμού ALOHA ή CSMA-CA, ανάλογα με την περίπτωση. Για εφαρμογές χαμηλής χρονικής καθυστέρησης ή εφαρμογές που απαιτούν

συγκεκριμένο εύρος ζώνης δεδομένων, οι συντονιστής PAN εκχωρεί τμήματα του ενεργού υπερπλαισίου στην εφαρμογή αυτή. Αυτά τα τμήματα ονομάζονται εγγυημένα χρονικά slots (GTS-guaranteed time slots). Τα GTSS αποτελούν την περίοδο contention free period (CFS), η οποία εμφανίζεται πάντα στο τέλος ενός υπερπλαισίου. Ο συντονιστής PAN μπορεί να διαθέσει σε συσκευές μέχρι και επτά από αυτά τα GTS, και ένα GTS επιτρέπεται να καταλαμβάνει περισσότερα από ένα χρονικά slots. Όλες οι συναλλαγές της περιόδου CAP πρέπει να έχουν ολοκληρωθεί πριν την έναρξη της περιόδου CFP. Επίσης κάθε συσκευή που αποστέλλει σε ένα τμήμα GTS πρέπει να ολοκληρώσει την ενέργεια αυτή πριν την έναρξη του επόμενου GTS ή του τέλους της περιόδου CFP.

3.4.3.4 Μοντέλο Μεταφοράς Δεδομένων

Υπάρχουν τρεις τύποι μεταφοράς δεδομένων. Η πρώτη συναλλαγή είναι η μεταφορά δεδομένων σε ένα συντονιστή όπου μια συσκευή μεταδίδει τα δεδομένα. Η δεύτερη συναλλαγή είναι η μεταφορά δεδομένων από ένα συντονιστή όπου μια συσκευή λαμβάνει τα δεδομένα. Η τρίτη συναλλαγή είναι η μεταφορά δεδομένων μεταξύ δύο συσκευών peer-to-peer. Στην τοπολογία αστέρα, μόνο δύο από αυτές τις συναλλαγές δεδομένων χρησιμοποιούνται επειδή τα δεδομένα ανταλλάσσονται μόνο μεταξύ του συντονιστή και μιας συσκευή. Σε μια peer-to-peer τοπολογία, τα δεδομένα που ανταλλάσσονται μεταξύ δύο οποιοδήποτε συσκευών στο δίκτυο PAN κατά συνέπεια και οι τρεις συναλλαγές χρησιμοποιούνται σε αυτήν το τοπολογία. Οι μηχανισμοί για κάθε τύπο μεταφοράς εξαρτάται από το αν το δίκτυο υποστηρίζει τη μετάδοση των περιοδικών beacons όπως αναφέρθηκε προηγουμένως στην δομή υπερπλαισίου. Ένα beacon enabled PAN χρησιμοποιείται σε δίκτυα που είτε απαιτούν συγχρονισμό ή υποστήριξη για low latency συσκευές, όπως τα περιφερειακά του υπολογιστή. Αν το δίκτυο δεν χρειάζεται συγχρονισμό ή υποστήριξη για low latency συσκευές, μπορεί να επιλεγεί να μην χρησιμοποιηθούν τα beacons για τις κανονικές μεταφορές δεδομένων. Ωστόσο, beacons απαιτούνται ακόμη για την ανακάλυψη του δικτύου (network discovery). Όταν μια συσκευή επιθυμεί να μεταφέρει δεδομένα σε έναν συντονιστή σε beacon enabled PAN, ακούει πρώτα για το beacon του δικτύου. Όταν βρεθεί το beacon, η συσκευή συγχρονίζεται με τη δομή υπερπλαισίου. Στο κατάλληλη στιγμή, η συσκευή εκπέμπει το πλαίσιο δεδομένων (data frame) της στον συντονιστή. Ο συντονιστής θα αναγνωρίσει την επιτυχής λήψη των δεδομένων διαβιβάζοντας μια επιβεβαίωση του πλαισίου(

acknowledgement frame), εφόσον ζητηθεί. Όταν μια συσκευή επιθυμεί να μεταφέρει δεδομένα σε ένα nonbeacon enabled PAN, μεταδίδει απλά το πλαίσιο δεδομένων του στον συντονιστή. Ο συντονιστής αναγνωρίζει την επιτυχή λήψη των δεδομένων μεταδίδοντας μία προαιρετική επιβεβαίωση του πλαισίου, ολοκληρώνοντας την συναλλαγής. Όταν ο συντονιστής επιθυμεί να μεταφέρει δεδομένα σε μια συσκευή σε ένα beacon-enabled PAN, δηλώνει στο beacon δικτυού το μήνυμα δεδομένων που εκκρεμεί. Η συσκευή ακούει περιοδικά το beacon του δικτύου και, αν ένα μήνυμα είναι σε εκκρεμότητα, μεταδίδει μια εντολή MAC που ζητεί τα δεδομένα. Ο συντονιστής αναγνωρίζει την επιτυχή λήψη του αιτήματος δεδομένων μεταδίδοντας ένα πλαίσιο επιβεβαίωσης. Το εκκρεμών πλαίσιο δεδομένων στη συνέχεια, αποστέλλεται από τον συντονιστή. Η συσκευή αναγνωρίζει την επιτυχή λήψη των δεδομένων μεταδίδοντας ένα πλαίσιο επιβεβαίωσης, εάν ζητηθεί. Η συναλλαγή έχει πλέον ολοκληρωθεί. Μετά την επιτυχή ολοκλήρωση της συναλλαγής δεδομένων, το μήνυμα διαγράφεται από τον κατάλογο των εκκρεμών μηνυμάτων στο beacon. Όταν ένας συντονιστής επιθυμεί να μεταφέρει δεδομένα σε μια συσκευή σε nonbeacon-enabled PAN, αποθηκεύει τα δεδομένα για την κατάλληλη συσκευή για να έρθει σε επαφή και να ζητήσει τα δεδομένα. Μια συσκευή ζητά δεδομένα με την μετάδοση μιας MAC εντολή που ζητεί τα δεδομένα στον συντονιστή της. Ο συντονιστής αναγνωρίζει την επιτυχή λήψη της αίτησης δεδομένων, μεταδίδοντας ένα πλαίσιο επιβεβαίωσης. Αν ένα πλαίσιο δεδομένων εκκρεμεί, ο συντονιστής μεταδίδει το πλαίσιο δεδομένων. Αν κανένα πλαίσιο δεδομένων δεν εκκρεμεί, ο συντονιστής αναφέρει το γεγονός αυτό, είτε στο πλαίσιο επιβεβαίωσης που ακολουθεί το αίτημα των δεδομένων ή σε ένα πλαίσιο δεδομένων με μηδενικού μήκους ωφέλιμο φορτίο. Εάν ζητηθεί, η συσκευή αναγνωρίζει την επιτυχή λήψη του πλαισίου δεδομένων με μετάδοση ενός πλαισίου επιβεβαίωσης. Σε ένα PAN peer-to-peer, κάθε συσκευή επικοινωνεί απευθείας με κάθε άλλη συσκευή στην εμβέλεια της. Για να γίνει αυτό αποτελεσματικά, οι συσκευές που επιθυμούν να επικοινωνήσουν θα πρέπει να ειναι σε λειτουργία όπου λαμβάνουν συνεχώς ή να συγχρονίζονται μεταξύ τους. Στην πρώτη περίπτωση, η συσκευή μπορεί απλά να μεταδώσει τα δεδομένα της Στην τελευταία περίπτωση, πρέπει να ληφθούν, να επιτευχθεί ο συγχρονισμός, άλλα μέτρα [11].

3.4.3.5 Μηχανισμοί CSMA-CA

Το IEEE 802.15.4 LR-WPAN χρησιμοποιεί δύο τύπους μηχανισμού πρόσβασης σε κανάλι, ανάλογα με την διαμόρφωση του δικτύου. Τα nonbeacon-enabled PAN χρησιμοποιούν έναν unslotted CSMA-CA μηχανισμό πρόσβασης σε κανάλι. Κάθε φορά που μια συσκευή επιθυμεί να μεταδώσει πλαίσια δεδομένων ή εντολών MAC, περιμένει ένα τυχαίο χρονικό διάστημα. Εάν διαπιστωθεί ότι το κανάλι παραμένει αδρανές, μετά την τυχαία αναμονή, η συσκευή μεταδίδει τα δεδομένα της. Εάν διαπιστωθεί ότι το κανάλι είναι απασχολημένο μετά την τυχαία αναμονή, η συσκευή περιμένει για μια τυχαία χρονική περίοδο πριν προσπαθήσει να συνδεθεί ξανά στο κανάλι. Τα πλαίσια επιβεβαίωσης αποστέλλονται χωρίς τη χρήση CSMA-CA μηχανισμού. Τα beacon-enabled PAN χρησιμοποιούν έναν slotted CSMA-CA μηχανισμό πρόσβασης στο κανάλι, όπου οι περίοδοι υποχώρησης/αναμονής είναι ευθυγραμμισμένοι με την έναρξη της μετάδοσης ενός beacon. Οι περίοδοι αναμονής όλων των συσκευών εντός ενός PAN ευθυγραμμίζονται με τον συντονιστή PAN. Κάθε φορά που μια συσκευή επιθυμεί να μεταδώσει πλαίσια δεδομένων κατά τη διάρκεια της περιόδου CAP, εντοπίζει το όριο της επόμενης περιόδου υποχώρησης(backoff period) και στη συνέχεια περιμένει για έναν τυχαίο αριθμό περιόδων υποχώρησης. Εάν το κανάλι είναι απασχολημένο, μετά από αυτή την τυχαία αναμονή, η συσκευή περιμένει για ένα άλλο τυχαίο αριθμό περιόδων υποχώρησης πριν προσπαθήσει να συνδεθεί ξανά στο κανάλι. Εάν το κανάλι είναι σε αδράνεια, η συσκευή ξεκινά να εκπέμπει στο όριο της επόμενης διαθέσιμης περιόδου υποχώρησης. Τα πλαίσια επιβεβαίωσης και τα beacons αποστέλλονται χωρίς τη χρήση ενός CSMA-CA μηχανισμού.

3.4.3.6 Κατανάλωση Ισχύος

Σε πολλές εφαρμογές που χρησιμοποιούν αυτό το πρότυπο, οι συσκευές τροφοδοτούνται με μπαταρία, και η αντικατάσταση της μπαταρίας ή επαναφόρτιση της σε τακτά χρονικά διαστήματα είναι ανέφικτη. Ως εκ τούτου, η κατανάλωση ενέργειας αποτελεί θέμα ύψιστης σημασίας στο πρότυπο. Το πρωτόκολλο έχει αναπτυχθεί για να ευνοήσει τις συσκευές που τροφοδοτούνται από μπαταρία. Ωστόσο, σε ορισμένες εφαρμογές, μερικές συσκευές θα μπορούσαν τροφοδοτούνται ηλεκτρικά. Συσκευές που λειτουργούν με μπαταρίες, απαιτούν duty-cycling για να μειώσουν την κατανάλωση ενέργειας. Αυτές οι συσκευές θα περνούν το μεγαλύτερο

μέρος της λειτουργικής ζωής σε κατάσταση ύπνου, ωστόσο, κάθε συσκευή ακούει περιοδικά το κανάλι RF (radio frequency), για να καθορίσει αν κάποιο μήνυμα εκκρεμεί. Αυτός ο μηχανισμός επιτρέπει στο σχεδιαστή εφαρμογών να αποφασίσει σχετικά με την ισορροπία μεταξύ της κατανάλωσης της μπαταρίας και την καθυστέρηση των μηνυμάτων. Υψηλότερης κατανάλωσης συσκευές έχουν τη δυνατότητα να ακούν το κανάλι RF συνεχώς. Εκτός από τα χαρακτηριστικά εξοικονόμησης ενέργειας του συστήματος LR-WPAN, το UWB PHY παρέχει επίσης μία υβριδική διαμόρφωση που επιτρέπει την πολύ απλές αρχιτεκτονικές δέκτη για την περαιτέρω ελαχιστοποίηση της ισχύος κατανάλωσης και της πολυπλοκότητα υλοποίησης [10].

3.4.4 Τύποι Κόμβων Δικτύου στο 802.15.4

Σε ένα IEEE 802.15.4 δίκτυο μπορούν να λάβουν μέρος δύο ειδών συσκευές οι οποίες καθορίζονται απο το πρότυπο.

• Πλήρους λειτουργίας: Μία συσκευή FFD μπορεί να εξυπηρετεί τον σκοπό του κεντρικού συντονιστή σε ένα δίκτυο PAN, ενός τοπικού συντονιστή ή τον σκοπό μίας απλής συσκευής.

• Μειωμένης λειτουργίας: Μία συσκευή RFD δεν μπορεί να εξυπηρετεί τον σκοπό του συντονιστή PAN ή ενος απλού συντονιστή. Μία συσκευή RFD προορίζεται για εφαρμογές που είναι εξαιρετικά απλές όπως ένας διακόπτης μίας λάμπας, όπου η αποστολή μεγάλων ποσοτήτων δεδομένων δεν είναι απαραίτητη. Συνεπώς μία συσκευή RFD μπορεί να λειτουργήσει σαν απλή συσκευή και να υλοποιηθεί με ελάχιστους πόρους και χωρητικότητα μνήμης.

Ενα LR-WPAN που ικανοποιεί το παρών πρότυπο αποτελείτε απο δύο ή περισσότερες συσκευές εκ των οποίων μία εξ αυτών πρέπει να είναι FFD η οποία λειτουργεί σαν συντονιστής δικτύου PAN. Οι συσκευές FFD έχουν την δυνατότητα να επικοινωνούν με άλλες συσκευές FFDs ή RFDs και αποτελούν τον βασικό κορμό του δικτύου, ενώ οι RFD συσκευές δεν μπορούν να επικοινωνούν παρά με μόνο μία FFD συσκευή κάθε φορά. Το φυσικό επίπεδο (εν συντομία θα αναφέρεται σαν PHY) παρέχει μια διασύνδεση μεταξύ του MAC layer και του φυσικού ασύρματου καναλιού μέσω του λογισμικού των κυκλωμάτων ραδιοσυχνότητας (RF) και των RF του υλικού. Είναι δηλαδή η διεπαφή αυτή που επιτρέπει την μετάδοση ψηφίων (bit

streams) από το φυσικό μέσο επικοινωνίας. Το PHY layer παρέχει δύο οντότητες υπηρεσιών. Την PHY υπηρεσία δεδομένων και την διαχείριση υπηρεσιών διασύνδεσης μέσω του διαχειριστικού φορέα (PLME), του φυσικού επιπέδου. Η PHY υπηρεσία δεδομένων επιτρέπει τη μετάδοση και υποδοχή των μονάδων πρωτοκόλλου δεδομένων (PPDU) σε όλο το φυσικό ασύρματο κανάλι. Οι διεργασίες που πρέπει να υποστηρίζει ένα ολοκληρωμένο φυσικό επίπεδο, και περιγράφονται στο πρότυπο, είναι:

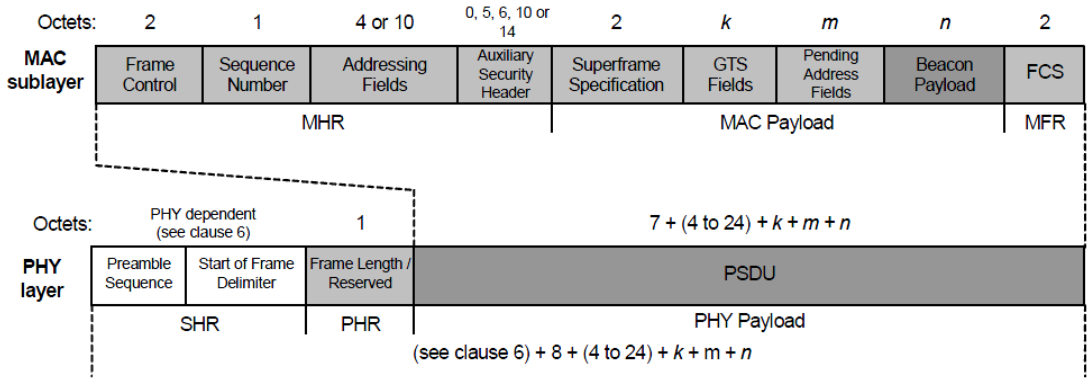
- Ενεργοποίηση και απενεργοποίηση του ραδιο-πομποδέκτη
- Ένδειξη ποιότητας σύνδεσης (LDI)
- Επιλογή καναλιού
- Ανίχνευση ενέργειας (ED)
- Αξιολόγηση του καναλιού - Clear Channel Assesment (CCA)
- Μετάδοση και λήψη πακέτων σε όλο το φυσικό μέσο

3.4.5 Δομή Πλαισίων

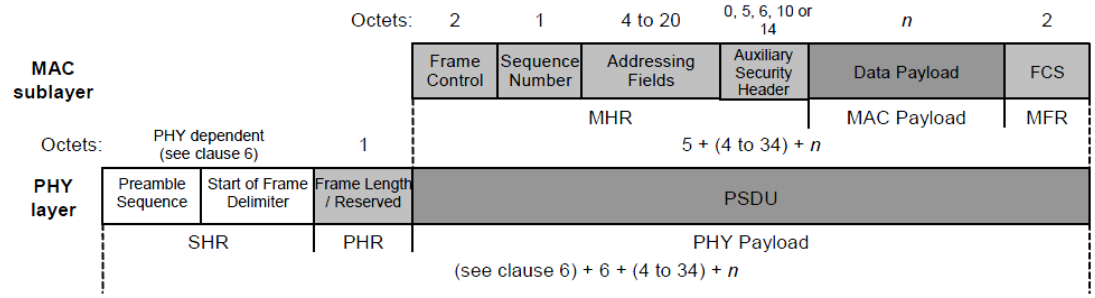
Η δομή του πλαισίου (frame) έχει σχεδιαστεί κατά τέτοιο τρόπο ώστε να κρατά χαμηλά την πολυπλοκότητα ενώ παράλληλα καθιστά αποτελεσματική την αναμετάδοση τους ακόμη και σε κανάλια με θόρυβο. Το φυσικό επίπεδο προσθέτει την επικεφαλίδα συγχρονισμού (synchronization header - SHR), η οποία χρησιμοποιείται για τον συγχρονισμού των συμβόλων από τον δέκτη, καθώς επίσης και την επικεφαλίδα PHY, η οποία δίνει το μήκος του φορτίου του φυσικού επιπέδου σε octets. Υπάρχουν τέσσερις βασικοί τύποι πλαισίων:

- Πλαίσιο beacon: χρησιμοποιείται από έναν coordinator για να αναμεταδώσει beacons.
- Πλαίσιο δεδομένων: χρησιμοποιείται από όλες τις συσκευές για να στείλουν δεδομένα.
- Πλαίσιο επιβεβαίωσης: χρησιμοποιείται για να επιβεβαίωση επιτυχή λήψη πλαισίου.

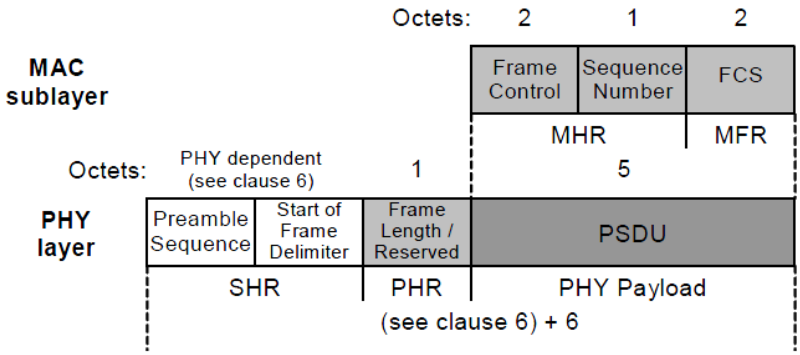
• Πλαίσιο εντολής MAC: χρησιμοποιείται για να ελέγξει τις ομότιμες MAC οντότητες του δικτύου.



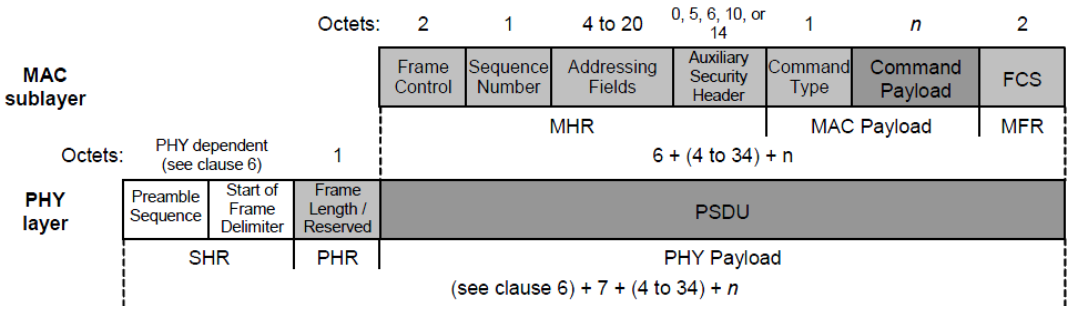
Πλαίσιο beacon και το πακέτο επίπεδου PHY



Πλαίσιο δεδομένων και το πακέτο επίπεδου PHY



Πλαίσιο επιβεβαίωσης και το πακέτο επίπεδου PHY



Πλαίσιο εντολής MAC και το πακέτο επίπεδου PHY

3.4.6 Αξιοπιστία και Κρυπτογράφηση

Για την αποφυγή συγκρούσεων δεδομένων η πρόσβαση στο κανάλι επικοινωνίας γίνεται μέσω του αλγόριθμου CSMA-CA. Εναλλακτικά ο έλεγχος πρόσβασης στο κανάλι επικοινωνίας μπορεί να γίνει από τον συντονιστή του δικτύου με χρήση σημάτων beacon. Τα μηνύματα επιβεβαίωσης είναι προαιρετικά σε συγκεκριμένες περιπτώσεις στις οποίες θεωρείται ότι έχει γίνει σωστά η λήψη. Εάν μια συσκευή δεν μπορεί να επεξεργαστεί ένα πλαίσιο, δεν επιβεβαιώνει την λήψη του και το ξανά λαμβάνει μέσω επανεκπομπής, λόγω λήξης χρόνου. Για την αποφυγή δημιουργίας κενού ασφαλείας, επανεκπομπές ίδιων μηνυμάτων πραγματοποιούνται έως έναν ορισμένο αριθμό.

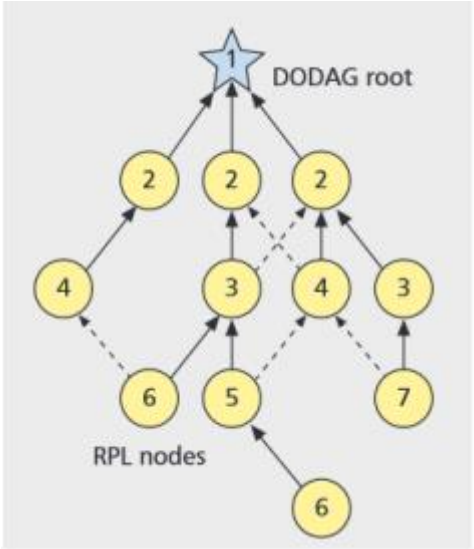
Στο επίπεδο ελέγχου μέσου (MAC) παρέχεται η υποδομή για υπηρεσίες ασφαλείας από τα ανώτερα επίπεδα. Τα ανώτερα επίπεδα έχουν τη δυνατότητα να ορίσουν κλειδιά συμμετρικής κρυπτογραφίας για να εξασφαλίσουν την προστασία των δεδομένων και την λήψη τους μόνο από συγκεκριμένες συσκευές του δικτύου. Ο τύπος της κρυπτογραφίας που χρησιμοποιείται ονομάζεται συμμετρικός επειδή χρησιμοποιείται το ίδιο κλειδί για την κρυπτογράφηση και για την αποκρυπτογράφηση [7].

3.5 Routing Over Low-power and Lossy networks (RoLL)

Για τη δρομολόγηση σε περιβάλλοντα με περιορισμένη ενέργεια-LLNs χρειάζεται ειδική μεταχείριση αφού τα ήδη υπάρχοντα πρωτόκολλα μπορεί να μην καλύπτουν τις απαιτήσεις. Γι’ αυτό το λόγο αναπτύχθηκε το πρωτόκολλο RPL (IPv6 Routing Protocol for LLNs) το οποίο χαρακτηρίζεται ως distance vector (χρήση BellmanFord αλγόριθμου), λειτουργεί με IPv6 και πρέπει να έχει χαμηλή

κατανάλωση, κάτι το οποίο έρχεται σε αντίθεση με την ανάγκη διάδοσης πληροφοριών δρομολόγησης σε ταχύ χρόνο [9].

Βασικό χαρακτηριστικό του πρωτοκόλλου είναι η δυνατότητα ανάκαμψης από συνδέσεις που δεν είναι πλέον διαθέσιμες, το οποίο μπορεί να συμβεί σε περιβάλλοντα με δύσκολες συνθήκες και παρεμβολές. Αυτό γίνεται για επίτευξη αξιοπιστίας και υλοποιείται διατηρώντας πολλές διαδρομές για έναν προορισμό αντί για έναν. Επιπλέον, σε αντίθεση με άλλα πρωτόκολλα, το RPL δεν υπολογίζει τα κόστη των διαδρομών στατικά αλλά περιλαμβάνει δυναμικές μετρικές συνδέσμων για καθορισμό της αξιοπιστίας (όπως μέγιστο αριθμό μεταδόσεων). Το πρωτόκολλο RPL υποστηρίζει τον υπολογισμό και εγκατάσταση μονοπατιών δρομολόγησης ενώ οι κόμβοι που το χρησιμοποιούν μπορούν να ανακαλύπτουν, να υπολογίζουν και να εγκαθιστούν διαδρομές (routes) αυτόνομα. Οι κόμβοι σχηματίζουν Directed Acyclic Graphs (DAGs), δηλαδή γράφους που δεν σχηματίζουν κύκλους, οι οποίοι επιτρέπουν σε κάθε κόμβο να επιλέγει και να διατηρεί άλλους κόμβους ως πιθανούς πατέρες στο δένδρο (μπορεί και περισσότερους του ενός) για την δρομολόγηση μέσα στο RPL δίκτυο προς την ρίζα του δικτύου (root).



Ακυκλικό Διάγραμμα Προσανατολισμού (DODAG) [8]

Το RPL υποστηρίζει τρία πρότυπα κίνησης:

- multipoint-to-point (MP2P): Κίνηση πληροφοριών μεταξύ πολλών κόμβων προς την ρίζα του γράφου.
- point-to-multipoint (P2MP): Κίνηση μεταξύ ενός κόμβους και πολλών.

- point-to-point (P2P): Κίνηση που ανταλλάσσεται μεταξύ δύο κόμβων.

Στα LLNs είναι πολύ συνηθισμένο όταν πρόκειται για MP2P και P2MP η κίνηση προς και από ένα σημείο εξόδου. Κόμβοι που έχουν το ρόλο του Low power and lossy network Border Router (LBR) μπορούν τυπικά να αποτελούν τη ρίζα σε ένα τέτοιο δίκτυο. Το RPL πρωτόκολλο δρομολόγησης, χρησιμοποιεί μετρητές δρομολόγησης για τον υπολογισμό του συντομότερου μονοπατιού. Οι τρείς μετρήσεις που χρησιμοποιούνται είναι:

- Σύνδεση έναντι των μετρήσεων του κόμβου.
- Ποιότητα έναντι της ποσότητας.
- Δυναμικού έναντι του στατικού.

Έτσι, με βάση της μετρήσεις δημιουργείται ο γράφος, επιλέγοντας πάντα την πιο σύντομη διαδρομή. Σε περίπτωση που κάποιος κόμβος, για οποιοδήποτε λόγο, δεν είναι πλέον προσβάσιμος στο δίκτυο, ή κάποια σύνδεση μεταξύ δύο κόμβων δεν είναι πλέον διαθέσιμη, υποστηρίζεται ο υπολογισμός και η εγκατάσταση διαφορετικής διαδρομής για όλους τους επηρεαζόμενους κόμβους.

3.6 Το πρωτόκολλο CoAP

Το CoAP έχει σχεδιαστεί ώστε να μεταφράζεται εύκολα σε HTTP για απλοποιημένη ενοποίηση με το διαδίκτυο, ενώ και για την κάλυψη εξειδικευμένων απαιτήσεων, όπως είναι η υποστήριξη πολλαπλής διανομής (multicast support), πολύ χαμηλή επιβάρυνση (overhead) και απλότητα. Η πολλαπλή εκπομπή (multicast support), το χαμηλό overhead και η απλότητα είναι πολύ σημαντικά χαρακτηριστικά για το Διαδίκτυο των Πραγμάτων (IoT) και για M2M (machine-to-machine) συσκευές, οι οποίες τείνουν να είναι ενσωματωμένες και να έχουν έτσι πολύ λιγότερη μνήμη καθώς και χαμηλή κατανάλωση από αυτές που έχουν οι παραδοσιακές συσκευές διαδικτύου. Ως εκ τούτου, η αποτελεσματικότητα είναι πολύ σημαντική. Το CoAP μπορεί να λειτουργήσει στις πιο πολλές συσκευές που υποστηρίζουν το UDP (User Datagram Protocol) πρωτόκολλο.

Η ομάδα εργασίας CoRE σχεδίασε το CoAP με βάση τα ακόλουθα χαρακτηριστικά, δίνοντας έμφαση στην ανάλυση της πολυπλοκότητας του πρωτοκόλλου:

• URI(Unirform Resource Identifier) και υποστήριξη περιεχομένου.

• Υποστήριξη για την ανακάλυψη πόρων που παρέχονται από γνωστές CoAP υπηρεσίες.

• Απλή αποθήκευση προσωρινής μνήμης (caching) βασισμένη στην μέγιστη ηλικία (maxaged based).

• Απλή εγγραφή (subscription) για έναν πόρο, και ως αποτέλεσμα την προώθηση ειδοποιήσεων (push notifications) [12].

Στόχος του CoAP δεν είναι η τυφλή συμπίεση του HTTP πρωτοκόλλου, αλλά η υλοποίηση ενός υποσυνόλου κοινών REST μεθόδων με το HTTP, αλλά και η βελτιστοποίηση των M2M εφαρμογών. Παρόλο που το CoAP θα μπορούσε να χρησιμοποιηθεί για την αναδιαμόρφωση απλών HTTP διεπαφών σε ένα πιο συμπαγές πρωτόκολλο, το πιο σημαντικό είναι ότι προσφέρει επίσης δυνατότητες για M2M, όπως είναι η ανακάλυψη πόρων και υπηρεσιών, η υποστήριξη πολλαπλής εκπομπής και η ασύγχρονη ανταλλαγή μηνυμάτων.

3.7 Το πρωτόκολλο DTLS (Datagram Transport Layer Security)

Το πρωτόκολλο Datagram Transport Layer Security, που καθορίστηκε στο RFC 4347, αναπτύχθηκε για να καλύψει την ανάγκη για παροχή ισοδύναμης προστασίας με το TLS στα πρωτόκολλα του στρώματος εφαρμογής που χρησιμοποιούν το UDP ως πρωτόκολλο μεταφοράς, όπως κάνει το SIP. Το DTLS είναι παρόμοιο με το TLS σε πολλά σημεία, συμπεριλαμβανομένου του περιορισμού απαίτησης μιας νέας εγκατάστασης συνεδρίας μεταξύ των hops ώστε να προστατευθούν τα SIP μηνύματα από ένα τελικό σημείο σε άλλο.

Μια θεμελιώδης διαφορά μεταξύ του TLS και του DTLS είναι ότι το DTLS παρέχει έναν μηχανισμό για να χειριστεί την αναξιοπιστία που συσχετίζεται με το UDP, όπως η πιθανότητα απώλειας πακέτων ή της επαναδιάταξης. Εάν η απώλεια πακέτων συμβεί κατά τη διάρκεια μιας TLS handshake, η σύνδεση αποτυγχάνει. Το TLS Record Layer, όπου πραγματοποιείται η κρυπτογράφηση δεδομένων, απαιτεί τα αρχεία να παραλαμβάνονται και να υποβάλλονται σε επεξεργασία με διαδοχική σειρά. Εάν το αρχείο n δεν παραλαμβάνεται, το αρχείο n + 1 δεν μπορεί να αποκρυπτογραφηθεί επειδή το TLS στρώμα κρυπτογράφησης κυκλοφορίας

χρησιμοποιεί το CBC (Cipher Block Chaining), το οποίο απαιτεί τη γνώση του προηγούμενου αρχείου για να αποκρυπτογραφήσει το επόμενο αρχείο στην ακολουθία. Η πιο πρόσφατη έκδοση του TLS, η 1.1, έχει προσθέσει σαφείς CBC οδηγίες στα αρχεία για να αντιμετωπίσει αυτό το ζήτημα.

Ένας άλλος περιορισμός του TLS είναι ότι χρησιμοποιεί μία MAC (Message Authentication Code) για κάθε αρχείο για την προστασία ενάντια στην επανάληψη και στην επαναδιάταξη. Η MAC παράγεται χρησιμοποιώντας τους αριθμούς ακολουθίας των αρχείων που είναι μοναδικοί για κάθε αρχείο. Επομένως, εάν συμβεί απώλεια πακέτων, η ανίχνευση της επανάληψης καθίσταται άχρηστη. Το DTLS έχει σχεδιαστεί για να υπερνικήσει τους περιορισμούς του TLS με την παροχή των εξής:

- Αξιοπιστία κατά τη διάρκεια της DTLS handshake (απώλεια πακέτων και επαναδιάταξη).
- Ανίχνευση επανάληψης πακέτων.

Για να αντισταθμίσει τις συνθήκες απώλειας πακέτων, το DTLS παρέχει ένα χρονόμετρο αναμετάδοσης. Όταν ένας client διαβιβάζει το ClientHello μήνυμα, αρχίζει το χρονόμετρο και περιμένει ένα HelloVerifyResponse μήνυμα από τον server. Ο server διατηρεί επίσης ένα χρονόμετρο μετάδοσης μηνυμάτων. Εάν το χρονόμετρο του client λήξει, υποθέτει ότι είτε το ClientHello είτε το HelloVerifyResponse χάθηκε και αναμεταδίδει το ClientHello μήνυμα.

Από την άλλη μεριά, ο server δεν θα αναμεταδώσει το HelloVerifyResponse μήνυμα πριν από τη λήψη της αναμετάδοσης του ClientHello από τον client. Για την ανίχνευση της επανάληψης, το πρωτόκολλο DTLS προτείνει την χρησιμοποίηση ενός bitmap παραθύρου από αρχεία τα οποία ο client ή ο server έχει διαβιβάσει, αντίστοιχα.

Ο μετρητής πακέτων του δέκτη αρχικοποιείται στο μηδέν όταν εγκαθίσταται η συνεδρία, και για κάθε λαμβανόμενο αρχείο, ο δέκτης πρέπει να ελέγξει εάν το αρχείο που εξετάζεται αυτήν την στιγμή είναι μέσα στα όρια του παραθύρου. Το δεξί όριο του παραθύρου δείχνει τον υψηλότερο αριθμό ακολουθίας αρχείων που έχει ελεγχθεί μέσα σε μια συνεδρία. Τα αρχεία με αριθμούς ακολουθίας λιγότερους από n + 32 (αριστερό όριο) απορρίπτονται.

Αν και η επιλογή για το μέγεθος του παραθύρου του δέκτη είναι εξαρτώμενη εφαρμογή, το RFC εξουσιοδοτεί την υποστήριξη μιας ελάχιστης τιμής μεγέθους παραθύρου ίσο με 32. Η Sliding Window ιδιότητα είναι προαιρετική για τις εφαρμογές σύμφωνα με το RFC 4347 επειδή ο διπλασιασμός πακέτων δεν είναι πάντα κακόβουλος και μπορεί να εμφανιστεί λόγω λαθών δρομολόγησης. Μια άλλη ιδιότητα του DTLS είναι η χρήση μιας cookies τεχνικής για την προστασία ενάντια στις DOS επιθέσεις. Κατά τη διάρκεια της αρχικής ανταλλαγής μηνυμάτων (παραδείγματος χάριν, ClientHello και HelloVerifyRequest), ο server περιλαμβάνει ένα cookie στην απάντησή του για να ελέγξει ότι το αίτημα προήλθε από τον μακρινό client και όχι από έναν μιμητή. Ο νόμιμος client θα πρέπει να υπολογίσει ένα άλλο cookie βασισμένο στις πληροφορίες που παραλαμβάνονται από τον server και να παράγει ένα νέο ClientHello μήνυμα που περιλαμβάνει το cookie του client. Το cookie υπολογίζεται χρησιμοποιώντας την MD5 πάνω σε μία μυστική τιμή, την IP διεύθυνση του πελάτη, και τις παραμέτρους του client που παραλήφθηκαν στο ClientHello μήνυμα. Αυτός ο μηχανισμός βοηθάει στον μετριασμό των επιπτώσεων ενάντια στις DOS επιθέσεις αντανάκλασης όπου ο επιτιθέμενος χρησιμοποιεί τις εξαπατημένες IP διευθύνσεις για να πλημμυρίσει ένα θύμα με απαντήσεις του server [13].

Βιβλιογραφία-Αναφορές:

[1] https://newsroom.cisco.com/feature-content?articleId=1208342 [Πρόσβαση 28/3/2017]

[2] Frankel, S., Bemard, E., Les, O., & Scarfone, K. (2007). Establishing Wireless Robust Security Networks: A Guide to 802.11i. Special Publication 800-97.

[3] Smith, N. Green & S. A Spy in your Pocket? s.l. : The Regulation of Mobile Data in the UK, Surveillance and Society, 2004.

[4] Gutierrez, José A. IEEE Std. 802.15.4 Enabling Pervasive Wireless Sensor Networks ppt. s.l. : Eaton Corporation, 2005.

[5] Schonwalder, Jurgen. Internet of Things:802.15.4, 6LoWPAN, RPL, COAP presentation. s.l. : Jacobs University, 2010.

[6] Montenegro, G., Transmission of IPv6 Packets over IEEE 802.15.4 Networks. s.l. : Network Working Group , 2007. RFC 4944.

[7] Hui, J. και Thubert, P. Compression format for IPv6 Datagrams over IEEE 802.15.4-Based. 2011

[8] Ko, JeongGil, και συν. Connecting Low-Power and Lossy Networks to the Internet. IEEE Communications Magazine. 2011.

[9] Hui, J. και Vasseur, JP. The Routing Protocol for Low-Power and Lossy Networks (RPL) Option. Internet Engineering Task Force (IETF). [Ηλεκτρονικό] IETF, 03 2012. [Παραπομπή: 22/09/2014.] http://tools.ietf.org/html/rfc6553. 2070- 1721

[10] Chiara Buratti, Student Member, IEEE, and Roberto Verdone, Member, IEEE, "Performance Analysis of IEEE 802.15.4 Non Beacon-Enabled Mode"

[11] IEEE Computer Society "IEEE Std 802.15.4™-2011(Revision of IEEE Std 802.15.4-2006)"

[12] Comments (RFC) 7252, The Constrained Application Protocol (CoAP)", June 2014

[13] T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.1, IETF RFC 4346.

[14] Security and Privacy in Sensor Networks, Howen Chan & Andrian Perrig, October 2003.

ΚΕΦΑΛΑΙΟ 4: Επικινδυνότητα σε Κρίσιμες Επικοινωνιακές Υποδομές (Critical Infrastructure-Critical Information Infrastructure).

4.1 Εισαγωγή-Γενικά

Ο ρόλος των Κρίσιμων Πληροφοριακών-Επικοινωνιακών Υποδομών είναι καθοριστικός, τόσο για την ίδια την Υποδομή, όσο και για την κοινωνία στο σύνολό της. Οι τομείς μου μπορεί να επηρεάσει μια πιθανή αποτυχία αναμενόμενης λειτουργίας, είτε λόγο σφάλματος στο σύστημα, είτε λόγο φυσικής καταστροφής, ή ακόμη και από ηθελημένη παρέμβαση (επίθεση), ποικίλλουν και συνεπώς οι επιπτώσεις μπορούν να επηρεάσουν πολλές πτυχές μιας κοινωνίας. Το τελευταίο συμβαίνει κατά κύριο λόγο εξαιτίας της ύπαρξης αλληλεξαρτήσεων μεταξύ των διαφόρων Υποδομών και Τομέων, το οποίο είναι συχνό φαινόμενο σε όλες τις αναπτυγμένες χώρες. Η εισαγωγή ειδικά της Πληροφοριακής και Επικοινωνιακής Τεχνολογίας (ΤΠΕ), έχει δημιουργήσει μεγαλύτερου βαθμού εξαρτήσεις μεταξύ των Τομέων. Ακολουθούν μία σειρά από ορισμούς που αφορούν το συγκεκριμένο θέμα[1]:

- Ευπάθεια (Vulnerability)

Ένα ελάττωμα ή μια αδυναμία στις διαδικασίες ασφάλειας ενός συστήματος, όπως στο σχεδιασμό, την υλοποίηση, ή σε εσωτερικούς ελέγχους, που μπορεί κατά λάθος ή σκόπιμα να χρησιμοποιηθεί και να οδηγήσει σε ένα ρήγμα ασφάλειας (security breach), ή παραβίαση της πολιτικής ασφάλειας του συστήματος.

- Απειλή (Threat)

Το ενδεχόμενο μια πηγή απειλής (threat source), όπως αυτή ονομάζεται, να εκμεταλλευτεί κατά λάθος, ή σκόπιμα μια ευπάθεια.

- Συνέπεια (Consequence)

Το αποτέλεσμα μιας κατάστασης ή ενός γεγονότος, το οποίο εκφράζεται ποιοτικά, ή ποσοτικά και μπορεί να είναι μια απώλεια, ένας τραυματισμός, ένα οποιοδήποτε μειονέκτημα, ή ένα κέρδος. Οι επιδράσεις των συνεπειών μπορεί να αφορά τους ανθρώπους, την οικονομία, ή το περιβάλλον.

- Αντίκτυπο (Impact)

Αρνητική μεταβολή του επιπέδου των επιχειρησιακών στόχων που έχουν επιτευχθεί.

- Κίνδυνος Ασφάλειας Πληροφοριών (Information Security Risk)

Το ενδεχόμενο ότι μια δεδομένη απειλή θα εκμεταλλευτεί ευπάθειες ενός αγαθού ή συνόλου αγαθών, με αποτέλεσμα να προκαλέσει ζημιά στον οργανισμό. Συνήθως εκφράζεται ως συνδυασμός της πιθανότητας ενός συμβάντος και των συνεπειών αυτού.

- Ετοιμότητα (Preparedness)

Μέτρα για να ασφαλίσουμε ότι κοινότητες και οργανισμοί είναι ικανοί να αντιμετωπίσουν τις επιδράσεις των έκτακτων περιστατικών.

- Υποδομή (Infrastructure)

Το πλαίσιο αλληλεξαρτώμενων δικτύων και συστημάτων, τα οποία αποτελούνται από αναγνωρίσιμες βιομηχανίες, ιδρύματα (συμπεριλαμβανομένων των ανθρώπων και των διαδικασιών), και ικανότητες διανομής που παρέχουν μια αξιόπιστη ροή προϊόντων και υπηρεσιών, σημαντικών στην άμυνα και την οικονομική ασφάλεια των Ηνωμένων Πολιτειών, στην ομαλή λειτουργία των κυβερνήσεων σε όλα τα επίπεδα, αλλά και της κοινωνίας στο σύνολό της.

- Κρίσιμη Υποδομή (CI ή CI/KR)

Οι Κρίσιμες Υποδομές ή Υποδομές Ζωτικής Σημασίας όπως αλλιώς ονομάζονται, αποτελούν μεγάλης κλίμακας υποδομές, των οποίων η υποβάθμιση ή καταστροφή θα είχε σοβαρό αντίκτυπο στην υγεία, την ασφάλεια ή την ευημερία των πολιτών, ή στην αποτελεσματική λειτουργία των κυβερνήσεων και/ή της οικονομίας. Χαρακτηριστικά παραδείγματα τέτοιων Υποδομών αποτελούν οι Τομείς των Τηλεπικοινωνιών, της Ηλεκτρικής Ενέργειας, του Φυσικού Αερίου και Πετρελαίου, του Τραπεζικού και Οικονομικού συστήματος, της Μεταφοράς, των συστημάτων Παροχής Νερού, των Κυβερνητικών Υπηρεσιών, των υπηρεσιών Άμεσης Ανάγκης, της Τροφής/Γεωργίας (παραγωγή, αποθήκευση, και διανομή), της Υγείας, της Εκπαίδευσης, αλλά και πολυάριθμων αγαθών (σίδερο, ατσάλι, αλουμίνιο).

Αξίζει να σημειωθεί ότι οι Κρίσιμες Υποδομές διακρίνονται σε τέσσερα επίπεδα, το επιχειρηματικό/στρατηργικό (business/strategic), το οποίο περιλαμβάνει την κεντρική επιχειρησιακή διαδικασία, το οργανωτικό (organizational), το οποίο αφορά τη δομή, τις διαδικασίες και την ανθρώπινη συμπεριφορά, το κυβερνοχωρικό (cyber) το οποίο σχετίζεται με τα δεδομένα, τα επικοινωνιακά και πληροφοριακά συστήματα, συμπεριλαμβανομένου τα συστήματα διαχείρισης για το φυσικό επίπεδο και τέλος το φυσικό (physical) στο οποίο συναντάμε τις φυσικές συσκευές της εκάστοτε Υποδομής

- Κρίσιμη Πληροφοριακή Υποδομή (CII)

Αφορούν τις προαναφερθείσες Κρίσιμες υποδομές, οι οποίες κάνουν χρήση των πληροφοριακών και επικοινωνιακών τεχνολογιών και εξαρτώνται σημαντικά από αυτές. Να διευκρινίσουμε ότι οι Υποδομές αυτές είναι Κρίσιμες τόσο για τις ίδιες, όσο και για τη λειτουργία άλλων Κρίσιμων υποδομών. Λόγω του ότι στις μέρες μας η λειτουργία των Υποδομών βασίζεται στην αποθήκευση, επεξεργασία και διακίνηση πληροφοριών, είναι πρόκληση η προστασία τους σε περιπτώσεις αποτυχιών, επιθέσεων, ή ατυχημάτων, αλλά και η ελαχιστοποίηση του χρόνου ανάκαμψης.

- Κρισιμότητα (Criticality)

Αποτελεί το επίπεδο της συμβολής μιας Υποδομής στην κοινωνία, ώστε να διατηρηθεί το ελάχιστο επίπεδο του εθνικού και διεθνούς νόμου και της τάξης, της δημόσιας ασφάλειας, της οικονομίας, της δημόσιας υγείας και του περιβάλλοντος, ή το επίπεδο του αντικτύπου που θα έχει στους πολίτες ή στην κυβέρνηση η έλλειψη ή η καταστροφή της Υποδομής. Με άλλα λόγια πρόκειται για τη σοβαρότητα μιας συνέπειας τόσο για την ίδια την Υποδομή όσο και για την κοινωνία.

- Κρισιμότητα εναντίον Επικινδυνότητας

Ο βασικός συνδετικός τους κρίκος αποτελεί η έννοια του αντικτύπου (impact). Η έννοια της κρισιμότητας αποτελεί τόσο υποσύνολο όσο και υπερσύνολο της επικινδυνότητας. Ως υποσύνολο αντιμετωπίζεται, καθώς πολλά από τα κριτήρια ή παράγοντες αντικτύπου που χρησιμοποιούνται στην προστασία Κρίσιμων Υποδομών, χρησιμοποιούνται και στις παραδοσιακές μεθόδους ανάλυσης επικινδυνότητας, οπότε στις τελευταίες υπολογίζεται εν μέρει και η κρισιμότητα. Από την άλλη πλευρά, υπερσύνολο αποτελεί διότι όταν σε μια Υποδομή εξετάζεται το μέγεθος κρισιμότητάς

της, λαμβάνονται υπόψην κάποιοι επιπρόσθετοι παράγοντες ή κριτήρια αντικτύπου, σε σχέση με τις παραδοσιακές μεθόδους ανάλυσης επικινδυνότητας.

- Ανάλυση Επικινδυνότητας (Risk Analysis)

Η συστηματική χρήση πληροφοριών για την πραγματοποίηση των επιμέρους διαδικασιών του Προσδιορισμού επικινδυνότητας και της Εκτίμησης επικινδυνότητας. Ο προσδιορισμός επικινδυνότητας είναι μια διαδικασία όπου βρίσκει και καταγράφει τους κινδύνους και τα ιδιαίτερα χαρακτηριστικά αυτών, ενώ η Εκτίμηση επικινδυνότητας αναθέτει τιμές στην πιθανότητα και τις συνέπειες του κάθε κινδύνου.

- Αποτίμηση Επικινδυνότητας (Risk Assessment)

Η συνολική διαδικασία της Ανάλυσης Επικινδυνότητας (Risk Analysis) και της Αξιολόγησης Επικινδυνότητας (Risk Evaluation). Να σημειώσουμε ότι με τον όρο Risk Evaluation εννοούμε τη σύγκριση του εκτιμώμενου κινδύνου με βάση κάποια συγκεκριμένα κριτήρια επικινδυνότητας, προκειμένου να προσδιορίσουμε τη σημαντικότητα αυτού.

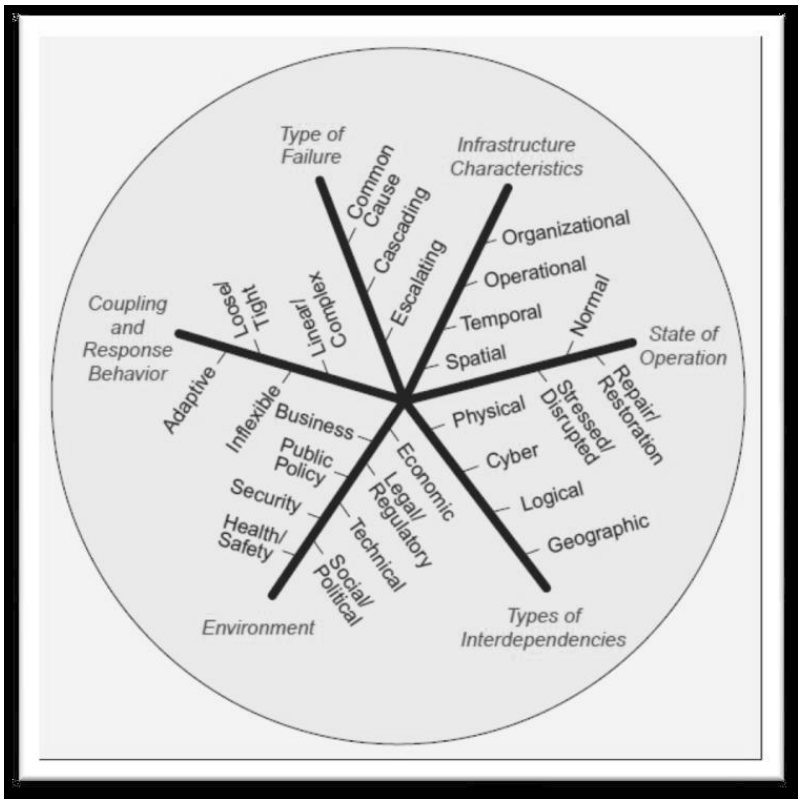
- Εξαρτήσεις (Dependencies) - Αλληλεξαρτήσεις (Interdependencies)

Με τον όρο εξάρτηση (dependency) μεταξύ δύο Υποδομών εννοούμε μια μονόδρομη σύνδεση μεταξύ αυτών, έτσι ώστε η κατάσταση της i Υποδομής να εξαρτάται από την αντίστοιχη της j [2].

4.2 Κρίσιμες Υποδομές και Εξαρτήσεις

Παρατηρούνται δύο ειδών εξαρτήσεις, αυτές μεταξύ διαφορετικών επιπέδων της ίδιας Υποδομής (intra-dependency) και αυτές μεταξύ διαφορετικών Υποδομών(inter-dependency). Ωστόσο, συχνά συναντώμενο φαινόμενο αποτελούν και οι αλληλεξαρτήσεις μεταξύ διαφορετικών τομέων (sectors), όπου Τομέας είναι ένα σύνολο Υποδομών με κοινά χαρακτηριστικά, όπως είναι ο τομέας της ενέργειας. Σε αυτήν την περίπτωση, αναφερόμαστε με τον όρο δια-τομεακές αλληλεξαρτήσεις (cross-sector interdependencies). Η ύπαρξη αλληλεξαρτήσεων αυξάνει την πολυπλοκότητα σε ένα δίκτυο Υποδομών και απαιτείται μια συλλογική αντιμετώπιση του προβλήματος [3].

Η εικόνα που ακολουθεί δείχνει παραστατικά την πολυδιάστατη αντιμετώπιση του αντικτύπου σε ένα ενδεχόμενο περιστατικό ασφάλειας και αφορά τις υποδομές με κρίσιμη υπόσταση.



Διαστάσεις Κρίσιμων Υποδομών

Πηγή: Rinaldi S., Peerenboom J., Kelly T., "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies", IEEE Control Systems Magazine, Vol. 21, No. 6, pp.11-25, 2001.

Η κατηγοριοποίηση των αλληλοεξαρτήσεων διακρίνεται σε φυσική (physical), κυβερνοχωρική (cyber), γεωγραφική (geographical) και λογική (logical). Συγκεκριμένα, η φυσική αλληλεξάρτηση υποδηλώνει ότι η κατάσταση της κάθε μιας Υποδομής (είσοδος) εξαρτάται από την υλική έξοδο της άλλης. Για παράδειγμα, ένα σιδηροδρομικό δίκτυο και ένα εργοστάσιο παραγωγής ηλεκτρικής ενέργειας με καύση άνθρακα ανήκουν σε αυτή την κατηγορία καθώς η κάθε μια παρέχει αγαθά που η άλλη έχει ανάγκη για να λειτουργήσει σωστά. Η κυβερνοχωρική ενώνει δύο Υποδομές μέσω ηλεκτρονικών, πληροφοριακών συνδέσμων, ενώ το αγαθό που παράγεται ή υπόκειται σε επεξεργασία από την j και εν συνεχεία μεταφέρεται στην i είναι η πληροφορία. Η συγκεκριμένη αλληλεξάρτηση έχει προκύψει με τη ραγδαία εξάπλωση της τεχνολογίας και αποτελεί μια από τις πιο συχνά συναντώμενες. Η

γεωγραφική με τη σειρά της προκύπτει σε περιπτώσεις κατά τις οποίες τα στοιχεία διαφόρων Υποδομών βρίσκονται σε στενή χωρική εγγύτητα, όπως όταν γραμμές ηλεκτρικής ενέργειας και οπτικές ίνες βρίσκονται κάτω από μια γέφυρα. Μια φυσική καταστροφή της τελευταίας, θα οδηγήσει σε άμεσο αντίκτυπο τόσο στον τομές ηλεκτρικής ενέργειας, όσο και σε αυτόν της επικοινωνίας. Ωστόσο, σε αυτήν την κατηγορία, η αιτία μπορεί να είναι εκτός από φυσική καταστροφή, και ανθρώπινη παρέμβαση. Η λογική από την άλλη, δε σχετίζεται με καμία από τις παραπάνω κατηγορίες, καθώς αφορά περιπτώσεις όπου παράγοντες όπως πολιτικά, νομικά ή ρυθμιστικά καθεστώτα, ή γενικά ανθρώπινες αποφάσεις, οι οποίες αφορούν μια Υποδομή, επιφέρουν συνέπειες και σε άλλες. Για παράδειγμα, όταν λόγω της χαμηλής τιμής στα καύσιμα, αυξάνεται η κινητικότητα στους δρόμους, με κίνδυνο δημιουργίας κυκλοφοριακής συμφόρησης ή το γεγονός ότι οι Υποδομές συνδέονται μέσω των οικονομικών αγορών. Να αναφέρουμε ότι η άνθηση της τεχνολογίας σε συνδυασμό με την αυξημένη χρήση του αυτοματοποιημένου ελέγχου και την εξάρτηση για παράδειγμα από την ηλεκτρική ενέργεια για την αγορά και πώληση αγαθών και προϊόντων, έχει οδηγήσει στην ιδιαίτερα ενισχυμένη εμφάνιση των κυβερνοχωρικών και των λογικών αλληλεξαρτήσεων.

Ταυτόχρονα, υιοθετείται μια παρόμοια κατηγοριοποίηση (φυσική (physical), πληροφοριακή (informational), γεωχωρική (geospatial), πολιτική /διαδικαστική (political / procedural)), με τη διαφοροποίηση της πέμπτης αλληλεξάρτησης, αυτή της κοινωνικής (societal). Η τελευταία αφορά τη δημόσια γνώμη, εμπιστοσύνη, φόβο, αλλά και θέματα κουλτούρας [6].

4.3 Πότε αποτυγχάνουν οι κρίσιμες υποδομές;

Με την πάροδο του χρόνου όλο και περισσότερες Κρίσιμες Υποδομές εξαρτώνται από την Τεχνολογία της Πληροφορίας και της Επικοινωνίας (ΤΠΕ), με αποτέλεσμα μια αποτυχία (failure, disruption, interruption, outage) στην τελευταία (initiating failure event), είτε λόγο ατυχήματος, είτε σκόπιμα, να διαδοθεί και σε άλλες υποδομές, υποβαθμίζοντας ή διαταράσσοντας τη λειτουργικότητα αυτών. Με την ίδια λογική, μια αποτυχία σε Κρίσιμη Υποδομή μπορεί επίσης να διαδοθεί στην ICT (cascading failure event) Υποδομή και έτσι να επηρεάσει τη λειτουργία των διαφόρων διασυνδεδεμένων συστημάτων. Πολλές από αυτές τις αποτυχίες ίσως οδηγήσουν σε σοβαρές διαταραχές (disturbances), με αποτέλεσμα να καθίσταται όλο

και πιο επιτακτική η ανάγκη για μια ασφαλή και αξιόπιστη λειτουργία των διαφορετικών Κρίσιμων υποδομών.

Βασική προϋπόθεση για την ομαλή αυτή λειτουργία είναι η κατανόηση των αλληλεξαρτήσεων. Αξίζει να αναφερθεί ότι η τεχνικής φύσεως πολυπλοκότητα που συναντάται στις σημερινές Υποδομές δυσχεραίνει ακόμη περισσότερο την αναγνώριση αλληλεξαρτήσεων και ευπαθειών με αποτέλεσμα την εξάπλωση μιας αρχικά ασήμαντης αποτυχίας. Μελετώντας την προέλευση των αποτυχιών λόγο αλληλεξαρτήσεων (interdependence - related failures) και τον τρόπο με τον οποίο αυτές διαδίδονται, μπορούμε να κατανοήσουμε καλύτερα τις εξαρτήσεις και συνεπώς, λαμβάνοντας τις κατάλληλες αποφάσεις, να σχεδιάσουμε πιο αποδοτικά το σύστημά μας, από πλευράς κόστους, ασφάλειας και αξιοπιστίας [7].

4.4 Προστασία Κρίσιμων Υποδομών για να αποφευχθεί η αποτυχία τους

Κάθε χώρα που επιθυμεί να προστατεύσει τις Κρίσιμες (Πληροφοριακές) Υποδομές της θα πρέπει να έχει αναπτύξει κατάλληλους μηχανισμούς άμυνας και προστασίας. Ειδικότερα, δύο σημαντικά Ευρωπαϊκά έγγραφα τα οποία στοχεύουν στην προστασία των Κρίσιμων υποδομών, το «Green Paper on A European Programme for Critical Infrastructure Protection/2005 (EPCIP)» και το «Council Directive 114/2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve their Protection». Ο στόχος του EPCIP είναι η βελτίωση της προστασίας των Κρίσιμων Υποδομών στην Ευρώπη. Αυτό επιτυγχάνεται με την υλοποίηση της Ευρωπαϊκής νομοθεσίας ως οδηγίες και συστάσεις από την Ευρωπαϊκή Επιτροπή [7]. Το νομοθετικό πλαίσιο του EPCIP αποτελείται από τα ακόλουθα στοιχεία.

- Μια διαδικασία για τον προσδιορισμό των Κρίσιμων Ευρωπαϊκών Υποδομών (ECI) και μιας κοινής προσέγγισης για την εκτίμηση της αναγκαιότητας βελτίωσης της ασφάλειάς τους, με την τελευταία να καθιερώνεται μέσω μιας Οδηγίας (Directive).
- Μέτρα για τη διευκόλυνση βελτιώσεων στο EPCIP, συμπεριλαμβανομένου ενός σχεδίου δράσης (action plan), ενός προειδοποιητικού συστήματος (CIWIN) στις Κρίσιμες Υποδομές από την επιτροπή της Προστασίας Κρίσιμων Υποδομών σε επίπεδο Ευρωπαϊκής Ένωσης, διαδικασίες για

ανταλλαγή πληροφοριών σχετικά με την Προστασία Κρίσιμων Υποδομών, προσδιορισμός και ανάλυση των αλληλεξαρτήσεων.

- Παροχή βοήθειας στα Κράτη Μέλη (MS) για βελτίωση της ασφάλειας σε μια Κρίσιμη εθνική Υποδομή (CNI) και σχέδια παρέμβασης (intervention plans).

Πιο πρόσφατα, το Ευρωπαϊκό έγγραφο «Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security» του 2011, επισημαίνει τις κινήσεις που πρέπει να γίνουν για την ενίσχυση της συνεργασίας σε εθνικό και διεθνές επίπεδο, προκειμένου να αντιμετωπιστούν αποτελεσματικά οι αλληλεξαρτήσεις [8]. Πιο συγκεκριμένα, για να επιτευχθεί ενημέρωση (awareness) και ετοιμότητα (preparedness) προτείνεται:

- Ετοιμότητα και Πρόληψη (Prevention)

Ανταλλαγή πληροφοριών μέσω του «European Forum for Member States (EFMS)» αλλά και συνεργασία μεταξύ των εθνικών ομάδων «CERTs». Επίσης, η εγκαθίδρυση του «European Public-Private Partnership for Resilience (EP3R)» για την ύπαρξη ενός ευρωπαϊκού πλαισίου διακυβέρνησης σε θέματα ανθεκτικότητας (resilience) των ΤΠΕ Υποδομών.

- Ανίχνευση (Detection) και Αντιμετώπιση (Response)

Η δημιουργία μέσω του «European Network and Information Security Agency (ENISA)» ενός «European Information Sharing and Alert System (EISAS) μέχρι το 2013, το έργο του οποίου θα ενισχύεται από τις ομάδες «CERTs», αλλά και τα «alert sharing systems» του ιδιωτικού τομέα, με την προστασία των προσωπικών δεδομένων να αποτελεί έναν από τους βασικούς στόχους αυτού.

- Μετριασμός των Επιπτώσεων (Mitigation) και Ανάκαμψη (Recovery)

Ο σχεδιασμός αντιμετώπισης απρόβλεπτων περιστατικών (Contingency Plan) αλλά, ο συχνός έλεγχος των Σχεδίων Ανάκαμψης από Καταστροφή (Disaster Recovery Plans), της Αντιμετώπισης Περιστατικών Ασφάλειας (Security Incident Response), καθώς επίσης η διοργάνωση Παν-Ευρωπαϊκών ασκήσεων (Pan-European exercises) σε περιστατικά ασφάλειας.

- Διεθνής Συνεργασία

Να δοθεί έμφαση στην ανθεκτικότητα του Διαδικτύου μέσω ευρωπαϊκών αρχών και κατευθυντήριων γραμμών, προκειμένου να δημιουργηθεί ένα κοινώς αποδεκτό πλαίσιο, αλλά και να ελέγχεται μέσω παγκόσμιων ασκήσεων σε Διαδικτυακά περιστατικά.

- Κριτήρια για τις Ευρωπαϊκές Κρίσιμες Υποδομές στον τομέα της ΤΠΕ

Ο προσδιορισμός συγκεκριμένων κριτηρίων με βάση τα οποία θα γίνεται η κατηγοριοποίηση των Κρίσιμων Υποδομών στον τομέα της ΤΠΕ (CII).

4.5 Προστασία Κρίσιμων Υποδομών και Διαδίκτυο

Οι Κρίσιμες Πληροφοριακές Υποδομές (ή Κρίσιμες Πληροφοριακές Υποδομές ή CIIs) είναι υποσύνολο των Κρίσιμων Υποδομών και απειλούνται τόσο από φυσικές όσο και από κυβερνοχωρικές κακόβουλες πηγές. Με τη σειρά τους οι Κρίσιμες Υποδομές, εξαιτίας της εξάρτησής τους από τις CIIs είναι ευπαθείς σε απειλές του κυβερνοχώρου. Για το λόγο αυτό, τόσο οι Κρίσιμες Υποδομές όσο και οι Κρίσιμες Πληροφοριακές Υποδομές συνδέονται με την ασφάλεια στον κυβερνοχώρο (cybersecurity).

Συνεπώς, για να επιτευχθεί ασφάλεια στον κυβερνοχώρο θα πρέπει να ληφθούν υπόψη τόσο οι Κρίσιμες Πληροφοριακές Υποδομές όσο και οι μη Κρίσιμες / Εθνικές Πληροφοριακές Υποδομές. Επίσης, βασικό ρόλο προς αυτήν την κατεύθυνση αποτελεί η υλοποίηση Αποτιμήσεων Επικινδυνότητας (risk assessments), έτσι ώστε να προσδιοριστούν οι περιοχές με την υψηλότερη επικινδυνότητα και οι λύσεις να επικεντρωθούν σε επιλεγμένα αγαθά (assets) μιας Υποδομής [9].

4.6 Ανθεκτικότητα Κρίσιμων Υποδομών

Η εξάρτηση των Κρίσιμων Υποδομών από τα επιτεύγματα της τεχνολογίας έχει καταστήσει τον παράγοντα της διαθεσιμότητας (availability) καθοριστικό για την ομαλή λειτουργία τους. Η μεταβλητή φύση όμως της τεχνολογίας, έχει επηρεάσει την αξιοπιστία (reliability) των Κρίσιμων Υποδομών. Έτσι, η δημιουργία ανθεκτικών (resilient) Κρίσιμων Υποδομών (CIR) αποτελεί μια πρόκληση. Η ανθεκτικότητα (resilience/fault tolerance) εστιάζει στην αποτροπή εμφάνισης Κρίσιμων αποτυχιών ή στην ελαχιστοποίηση του αντικτύπου τους αν εν τέλει εκδηλωθούν. Πρόκειται ουσιαστικά για την ικανότητα της Υποδομής να αντισταθεί στις επιπτώσεις μιας

απειλής (εξωτερικής ή εσωτερικής) και να διατηρήσει τη βασική λειτουργικότητά της. Η ανθεκτικότητα ορίζεται ως η ικανότητα να απορροφήσεις (absorb), να ανακάμψεις (recover), ή να προσαρμοστείς (adapt) επιτυχώς σε αντιξοότητες ή σε αλλαγή συνθηκών [10].

Ως ανθεκτικότητα μιας Υποδομής πολλές φορές ορίζεται η ύπαρξη ρωμαλεότητας (robustness) στα επιμέρους στοιχεία αυτής, δηλαδή περίσσεια (redundancy), έτσι ώστε να αποτραπεί η διάδοση μιας αποτυχίας και οι σοβαρές επιπτώσεις αυτής. Με άλλα λόγια, αποτρέπεται η δημιουργία μοναδικού σημείου αποτυχίας (single point of failure) [11].

Σε αυτήν την περίπτωση, η ανθεκτικότητα ορίζεται με βάση τρείς παραμέτρους, την ρωμαλεότητα (robustness), δηλαδή την ικανότητα μιας Υποδομής να αντισταθεί σε μια απειλή, την ανάκαμψη (recovery), δηλαδή την ικανότητα μιας Υποδομής να ανακάμψει μετά από μια Κρίσιμη κατάσταση (crisis situation) και την ύπαρξη πόρων (resourcefulness), τόσο για την αποφυγή μιας αποτυχίας, όσο και για τη γρήγορη ανάκαμψη από αυτή.

Ακολουθούν διάφορες προσεγγίσεις για τη διαχείριση ανεπιθύμητων περιστατικών:

- Θεωρίες Αξιοπιστίας (Reliability Theories)

Υπάρχουν δύο βασικές θεωρίες που σχετίζονται με την αξιοπιστία, αυτή των «Φυσιολογικών» Ατυχημάτων (NAT) και αυτή της Υψηλής Αξιοπιστίας (HRT). Όσον αφορά στην πρώτη, αντιμετωπίζει τις πιθανές αποτυχίες – ατυχήματα ως αναπόφευκτα, καθώς είναι απόρροια της αλληλεπιδραστικής (interactive) πολυπλοκότητας και των στενών συνδέσεων (couplings) που υπάρχουν μεταξύ των σύγχρονων συστημάτων, ενώ η δεύτερη διατυπώνει πως με την ύπαρξη κατάλληλων προληπτικών μέτρων είναι εφικτή η αποφυγή τους [12].

- Ετοιμότητα απέναντι στην Κρίση (Crisis Preparedness)

❖ Σχέδιο Ανάκαμψης από Καταστροφή (Disaster Recovery Plan-DRP)

Εστιάζει στις αποτυχίες που προκύπτουν από φυσικές καταστροφές και την εξάρτηση από Πληροφοριακά Συστήματα, αγνοώντας τις μη τεχνικής φύσεως ευπάθειες και σε άλλες εξωτερικές απειλές. Επίσης, αποτελεί ένα πλάνο το οποίο εφαρμόζεται εφόσον

έχει πραγματοποιηθεί κάποια αποτυχία και συνεπώς δεν λαμβάνει υπόψην διάφορες διορθωτικές ενέργειες (corrective actions) που μπορούν να λάβουν χώρα προκειμένου να αποτραπεί μια ανεπιθύμητη αποτυχία – περιστατικό [13].

- Διαχείριση Κρίσιμων Καταστάσεων (Crisis Management)

Δίνει έμφαση στον προσδιορισμό τρόπων αποφυγής εμφάνισης κρίσιμων καταστάσεων και κατ' επέκταση στην αποτελεσματικότερη διαχείριση όσων τελικά προκύψουν. Στόχος αυτής της προσέγγισης είναι η καλύτερη οργάνωση ενός οργανισμού – Υποδομής έτσι ώστε τυχόν αποτυχίες να μην κλιμακωθούν σε κρίσιμες καταστάσεις.

Πιο συγκεκριμένα, πριν την εμφάνιση της αποτυχίας και την κλιμάκωσή της σε Κρίσιμη υπάρχει η φάση «Pre-Crisis», η οποία φροντίζει για την αποτροπή οποιασδήποτε μορφής αποτυχίας μέσω για παράδειγμα Αποτιμήσεων Επικινδυνότητας. Ωστόσο, λόγο της αδυναμίας πρόβλεψης όλων των αποτυχιών μεριμνά και για την προετοιμασία διαχείρισης τυχόν Κρίσιμων καταστάσεων, μια διαδικασία που ονομάζεται «Σχεδιασμός Κρίσιμης Κατάστασης (Crisis Planning / Contingency Planning)». Με την εμφάνιση της Κρίσιμης κατάστασης, φάση «Crisis», ξεκινά η υλοποίηση των προσχεδιασμένων πλάνων για τον περιορισμό των συνεπειών και την ομαλή μετάβαση στην μετέπειτα φάση «Post-Crisis». Με την ολοκλήρωση και της τελευταίας φάσης, θα πρέπει να εντοπιστούν τα σημεία που χρήζουν βελτίωσης και να γίνουν οι κατάλληλες ενέργειες.

Παρόλα αυτά, η εν λόγω διαδικασία εξετάζει κυρίως συγκεκριμένες αποτυχίες, πραγματοποιώντας «Αποτίμηση Επικινδυνότητας βάση Προτεραιότητας (Priority-based Risk Assessment)», ενώ αδυνατεί να συμπεριλάβει και απρόβλεπτα περιστατικά. Εξαιτίας της παραπάνω αδυναμίας, η εισαγωγή της ανθεκτικότητας στις Υποδομές κρίθηκε αναγκαία.

- Διαχείριση Επιχειρησιακής Συνέχειας (Business Continuity Management-BCM)

Επιχειρεί τη εξισορρόπηση μεταξύ πρόβλεψης μη αναμενόμενων αποτυχιών και της ανθεκτικότητας. Στόχος της Διαχείρισης Επιχειρησιακής Συνέχειας είναι η εξασφάλιση της διαθεσιμότητας όλων των σημαντικών επιχειρησιακών πόρων που απαιτούνται για την υποστήριξη Κρίσιμων διαδικασιών της επιχείρησης. Η

διαδικασία που ακολουθείται είναι αρχικά η Αποτίμηση Επικινδυνότητας (Risk Assessment), στη συνέχεια η Ανάλυση Επιχειρησιακού Αντικτύπου (Business Impact Analysis-BIA) και τέλος το Πλάνο Επιχειρησιακής Συνέχειας (Business Continuity Planning-BCP), το οποίο διαφέρει από το Σχέδιο Ανάκαμψης από Καταστροφή, καθώς το τελευταίο εστιάζει σε τεχνολογικά θέματα και στην ουσία αποτελεί κομμάτι του Πλάνου Επιχειρησιακής Συνέχειας. Επίσης, το Πλάνο Επιχειρησιακής Συνέχειας εστιάζει στη διαθεσιμότητα, ενώ το Σχέδιο Ανάκαμψης από Καταστροφή στη γρήγορη ανάκαμψη [14].

4.7 Λόγοι Αναγκαιότητας στις κρίσιμες υποδομές

Η ανάγκη δημιουργίας ανθεκτικών Κρίσιμων Υποδομών και ειδικά ICT Κρίσιμων Υποδομών έχει επισημανθεί πολλές φορές στη βιβλιογραφία. Οι περισσότερες Υποδομές που θεωρούνται Κρίσιμες χρησιμοποιούν τη σύγχρονη τεχνολογία, όπως για παράδειγμα το σύστημα SCADA και συνεπώς εκτός των φυσικών ευπαθειών γίνονται επιρρεπείς και σε κυβερνοχωρικές επιθέσεις [15].

Οι κυριότερες ευπάθειες και απειλές που συναντώνται στις Κρίσιμες Υποδομές αναλύονται ακολούθως:

- Ευπάθειες Κρίσιμων Υποδομών:

  ο Αλληλεξαρτήσεις

Στην περίπτωση των αλληλεξαρτώμενων Κρίσιμων Υποδομών η δυνατότητα πρόβλεψης όλων των αποτυχιών καθίσταται ακόμη πιο δύσκολη και έτσι υπάρχει επιτακτική ανάγκη για εύρεση μιας εναλλακτικής μεθόδου διαχείρισης ανεπιθύμητων περιστατικών σε τέτοιου είδους Υποδομές. Να σημειώσουμε ότι όταν ο βαθμός σύνδεσης είναι «σφιχτός», τότε οι αποτυχίες αυξάνονται. Με την κατασκευή πιο ανθεκτικών υποδομών, οι οποίες θα λαμβάνουν υπόψην την τυχόν ύπαρξη άμεσων αλληλεξαρτήσεων, θα επιτευχθεί μια πιο αποτελεσματική αντιμετώπιση των ποικίλλων πιθανών αποτυχιών.

  ο Περιπλοκότητα (Complexity)

Εκτός από τις εξαρτήσεις, επίσης η ύπαρξη πολυπλοκότητας σε μια Υποδομή αυξάνει τις ευπάθειες αυτής, αλλά και τις πιθανότητες εκδήλωσης ενός κρίσιμου περιστατικού (critical incident). Η σύγχρονη τεχνολογία και η εξάρτηση των

Υποδομών από αυτή καθιστά τις τελευταίες ακόμη πιο ευάλωτες σε ηθελημένες ή μη επιθέσεις.

ο Έλλειψη Κεντρικού Σημείου Ελέγχου

Η πλειοψηφία των Κρίσιμων Υποδομών ανήκουν στον Ιδιωτικό τομέα, το οποίο δυσχεραίνει την ύπαρξη ενός κεντρικού σημείου επίβλεψης του συνόλου των Κρίσιμων Υποδομών σε εθνικό επίπεδο.

- Απειλές Κρίσιμων Υποδομών:

ο Φυσικές Καταστροφές (Natural disasters)

Είναι σοβαρές επιπτώσεις διαφόρων φυσικών φαινομένων και επηρεάζουν αρνητικά τη λειτουργία, δομή και ακεραιότητα της εκάστοτε Υποδομής.

ο Ατυχήματα Τεχνολογικής Φύσεως (Technological accidents)

Πρόκειται για περιστατικά τα οποία έχουν αρνητικό αντίκτυπο σε ένα σύστημα (λειτουργία, δομή και ακεραιότητα) εξαιτίας εσωτερικών παραγόντων, όπως είναι λάθη και αποτυχίες. Οι παράγοντες αυτοί μειώνουν την αξιοπιστία της κάθε Υποδομής και προκαλούν μη ελεγχόμενη υποβάθμιση της παρεχόμενης υπηρεσίας. Ο ανθρώπινος παράγοντας διαδραματίζει σημαντικό ρόλο σε αυτού του είδους την απειλή.

ο Κυβερνοχωρικές Απειλές (Cyber attacks)

Αφορά σε μια στοχευμένη ενέργεια ενάντια πληροφοριακών αγαθών μιας Κρίσιμης Υποδομής, με σκοπό την απόκτηση, τροποποίηση ή ολοκληρωτική καταστροφή δεδομένων ή / και πληροφοριακού συστήματος. Η ασφάλεια των συστημάτων, μέσω κρυπτογραφικών μηχανισμών και ασφαλών πρωτοκόλλων επικοινωνίας, προσθέτει ένα επίπεδο προστασίας σε τέτοιου είδους επιθέσεις.

ο Εγκληματικές Ενέργειες (Criminal Activities)

Αποτελεί μια παράνομη ενέργεια με στόχο την απόκτηση ή καταστροφή στοιχείων μιας Κρίσιμης Υποδομής. Η ενδυνάμωση της Φυσικής Ασφάλειας είναι ένα μέτρο για τον περιορισμό της.

ο Τρομοκρατικές Ενέργειες (Terrorist Attacks)

Αναπαριστά επίσης μια μη νόμιμη δραστηριότητα η οποία οδηγεί στην υποβάθμιση ή καταστροφή στοιχείων μιας Κρίσιμης Υποδομής. Η ενδυνάμωση της Φυσικής Ασφάλειας είναι ένα μέτρο για τον περιορισμό της [10].

4.8 Πλαίσια και πολιτικές ανθεκτικότητας

Ο σπουδαίος ρόλος της εισαγωγής της ανθεκτικότητας στις Κρίσιμες Υποδομές έχει επισημανθεί σε ένα πλήθος πλαισίων, αναφορών και πολιτικών. Ενδεικτικά αξίζει να αναφέρουμε τα παρακάτω που αφορούν τις Ηνωμένες Πολιτείες της Αμερικής [29]:

- National Security Strategy

Περιλαμβάνει τη λογική της ανθεκτικότητας αναφέροντας παραμέτρους όπως πλεονασμός και αποφυγή μοναδικού σημείου αποτυχίας

- National Strategy for the Physical Protection of Critical Infrastructure and Key Resources

Αναφέρει την ρωμαλεότητα των Υποδομών και την ανθεκτικότητα, η οποία μπορεί να επιτευχθεί μέσω αποτελεσματικής προστασίας και σχεδιασμού αντιμετώπισης περιστατικών (response planning).

- Critical Infrastructure Task Force of the Homeland Security Council

Τονίζει την ανεπάρκεια της προστασίας των Κρίσιμων Υποδομών, καθώς δεν μπορούν να αντιμετωπιστούν όλες οι πιθανές ευπάθειες μιας Υποδομής. Έτσι, προτείνει την εισαγωγή της ανθεκτικότητας η οποία θα περιέχει την παράμετρο της προστασίας, ετοιμότητας και προσπάθειας για αποφυγή εκδήλωσης επιθέσεων, επισημαίνοντας ότι είναι πιο κερδοφόρο για μια επιχείρηση να επενδύει σε τρόπους μείωσης του χρόνου ανάκαμψης.

- National Infrastructure Advisory Council

Θεωρεί πως η τρέχουσα πολιτική είναι ασφαλής για τον σκοπό που εξυπηρετεί, αλλά θα μπορούσε να βελτιωθεί εισάγοντας τις αρχές της ανθεκτικότητας. Επιπρόσθετα, προτείνει το «Department of Homeland Security» να επιχορηγεί προσπάθειες για την ανθεκτικότητα, να ενθαρρύνει τον κάθε τομέα στην θέσπιση

στόχων ανθεκτικότητας και να βοηθήσει στην κατασκευή ανθεκτικών Υποδομών νέας γενιάς.

- National Infrastructure Protection Plan : Partnering to enhance protection and resilience

Κάνει αναφορά στην ανθεκτικότητα μιας Υποδομής και τη σημασία της σχεδόν τις διπλάσιες φορές σε σχέση με το αντίστοιχο έγγραφο του 2006.

- Homeland Security Studies and Analysis Institute

Έχει εκδώσει ένα πλήθος αναφορών με κύριο στόχο την ανάπτυξη ενός πλαισίου για την ενσωμάτωση της ανθεκτικότητας στις Κρίσιμες Υποδομές.

- Quadrennial Homeland Security Review

Προτείνει τη χρήση τόσο της προστασίας όσο και της ανθεκτικότητας συνδυαστικά.

- Presidential Decision Directive 8, National Preparedness

Προωθεί την ενδυνάμωση τόσο της προστασίας όσο και της ανθεκτικότητας, μέσω της συστηματικής προετοιμασίας για τις απειλές που θέτουν την πιο υψηλή επικινδυνότητα. Πιο συγκεκριμένα προτείνει την ανάπτυξη ενός «National Preparedness Goal» με πέντε κύριες αποστολές, την αποτροπή, την προστασία, τον μετριασμό των συνεπειών, την απόκριση, και την ανάκαμψη.

Το πεδίο των Κρίσιμων Υποδομών έχει πολλούς κινδύνους. Ένας βασικός παράγοντας αποτελεί η ύπαρξη εξαρτήσεων μεταξύ αυτών, οι οποίες γίνονται ακόμη πιο στενές με την εξέλιξη των ΤΠΕ. Το τελευταίο έχει οδηγήσει σε μια υποκατηγορία των Κρίσιμων Υποδομών, αυτή των Κρίσιμων Πληροφοριακών Υποδομών. Η υποκατηγορία αυτή εισάγει νέες απειλές και ευπάθειες τόσο για τις Κρίσιμες Πληροφοριακές Υποδομές, όσο και για τις Κρίσιμες Υποδομές που εξαρτώνται από τη σωστή λειτουργία αυτών. Οι απειλές που προκύπτουν είναι κυρίως κυβερνοχωρικές, γεγονός που καθιστά το ρόλο του «Cybersecurity» καθοριστικό για την προστασία των Κρίσιμων Υποδομών στο σύνολό τους.

Ο αριθμός των αποτυχιών που έχει παρατηρηθεί λόγο των αλληλεξαρτήσεων είναι μεγάλος, γεγονός που μαρτυρά τη μη επαρκή αντιμετώπιση αυτών. Η βασική

προσέγγιση που ακολουθείται είναι αυτή της Προστασίας των Κρίσιμων (Πληροφοριακών) Υποδομών, δηλαδή της πρόληψης εμφάνισης περιστατικών ασφάλειας. Ωστόσο, η πρόληψη δεν είναι πάντοτε εφικτή για όλο το δυνατό πλήθος των απειλών. Έτσι, κρίνεται επιτακτική η ανάγκη υιοθέτησης μηχανισμών ενίσχυσης της ανθεκτικότητας των Κρίσιμων (Πληροφοριακών) Υποδομών, καθώς έτσι δίνεται έμφαση στις συνέπειες μιας αποτυχίας και πως μπορούν αυτές να μετριαστούν, ένα σενάριο που μοιάζει πιο ρεαλιστικό και πιο αποδοτικό οικονομικά για μια Υποδομή. Αξίζει ωστόσο να αναφερθεί ότι ο συνδυασμός της προστασίας και της ανθεκτικότητας αποτελεί τον ιδανικό τρόπο αντιμετώπισης του δυναμικού περιβάλλοντος των σημερινών Κρίσιμων (Πληροφοριακών) Υποδομών.

4.9 Αποτίμηση Επικινδυνότητας σε Κρίσιμες Υποδομές

Λαμβάνοντας υπόψη τους πολλαπλούς κινδύνους που ελλοχεύουν, υπάρχει έντονο ενδιαφέρον για τον προσδιορισμό των Κρίσιμων Υποδομών και την εύρεση νέων ή τη βελτίωση υπαρχόντων τεχνικών για την προστασία αυτών. Στην ενότητα αυτή, θα παραθέσουμε τις πιο πρόσφατες τεχνικές αποτίμησης της επικινδυνότητας μιας κρίσιμης υποδομής, οι οποίες στοχεύουν αρχικά στην εύρεση μιας Κρίσιμης Υποδομής και εν συνεχεία στην αποτίμηση του δυνητικού κινδύνου που αυτή καλείται να αντιμετωπίσει. Με άλλα λόγια, οι τεχνικές αυτές επιχειρούν την πρόληψη περιστατικών ασφάλειας (security incidents), τα οποία προκύπτουν ως απόρροια ευπαθειών της Υποδομής και εκμετάλλευσης αυτών από ακούσιους ή μη παράγοντες.

4.9.1 Σύγχρονες Προσεγγίσεις

Η Ευρωπαϊκή Επιτροπή ορίζει ότι ένα εθνικό πρόγραμμα ασφάλειας περί προστασίας μιας Κρίσιμης Υποδομής θα πρέπει να περιλαμβάνει ορισμένα κριτήρια στις αποτιμήσεις επικινδυνότητας της υπό εξέταση Υποδομής. Όσον αφορά την ένταση – σπουδαιότητα (intensity) ενός περιστατικού, θα πρέπει να λαμβάνεται υπόψη η δημόσια επίδραση (πληττόμενος πληθυσμός, απώλεια ζωής, τραυματισμό, ασθένεια), η οικονομική επίδραση (GDP), η περιβαλλοντική επίδραση, οι αλληλεξαρτήσεις, η πολιτική επίδραση (εμπιστοσύνη στην κυβέρνηση) και η ψυχολογική επίδραση. Τα κριτήρια αυτά αξιολογούνται με βάση την έκταση (scope), δηλαδή τοπική, περιφερειακή, εθνική, διεθνής, αλλά και τη διάρκεια, τόσο κατά τη στιγμή εκδήλωσης του περιστατικού όσο και μετά τη λήξη αυτού [16].

Η ολλανδική προσέγγιση στη συνέχεια, τονίζει την αναγκαιότητα ύπαρξης μιας «process-oriented» ανάλυσης για τη σωστή αποτίμηση των υποδομών ζωτικής σημασίας στην Ολλανδία, λόγω των ποικίλων αλληλεξαρτήσεων που δημιουργεί κυρίως ο ΤΠΕ τομέας. Αναφέρει τους όρους «έμμεση ζωτικότητα (indirect vitality)», ως το βαθμό στον οποίο άλλα προϊόντα ή υπηρεσίες επηρεάζουν ένα προϊόν ή μια υπηρεσία, σχετικά με τη σημαντικότητά του στην κοινωνία, αλλά και «άμεση ζωτικότητα (direct vitality)», ως το βαθμό στον οποίο το ίδιο το προϊόν ή η υπηρεσία θεωρείται σημαντικό για τη συνέχιση της κανονικής ροής της κοινωνίας. Ουσιαστικά, η άμεση ζωτικότητα είναι μια πρώτης τάξης εξάρτηση (first-order dependency), ενώ η έμμεση ζωτικότητα είναι ν-τάξης εξάρτηση (n-order dependency), η οποία προκαλεί τα λεγόμενα «cascading effects», λόγω της αλυσίδας εξάρτησης (dependency chain) που δημιουργείται. Σύμφωνα με τη συγκεκριμένη προσέγγιση, χρησιμοποιώντας τον πίνακα εξάρτησης (dependency matrix), όλες οι επιδράσεις (effects) δεύτερης και υψηλότερης τάξης πολλαπλασιαζόμενες με τον αριθμό των εξαρτήσεων και προστιθέμενες στις πρώτης τάξης επιδράσεις, μπορεί να καθορίσουν τη συνολική επίδραση της απώλειας, ή διακοπής μιας υπηρεσίας στην κοινωνία. Επίσης, προκειμένου να αποτιμηθεί η άμεση ζωτικότητα πρώτης τάξης, όλα τα προϊόντα και υπηρεσίες τοποθετήθηκαν σε ένα σχήμα με άξονες την άμεση και την έμμεση ζωτικότητα, από το οποίο και προέκυψε ότι οι τομείς με την μεγαλύτερη ζωτικότητα στην κοινωνία είναι αυτοί των τηλεπικοινωνιών, της ενέργειας και των μεταφορών. Επίσης, εισάγει τους όρους «backward dependency» για τα προϊόντα ή τις υπηρεσίες που εξαρτώνται από άλλα προϊόντα ή υπηρεσίες και «forward dependency» για τα προϊόντα ή υπηρεσίες που επηρεάζουν άλλα προϊόντα ή υπηρεσίες. Για τα προϊόντα και τις υπηρεσίες με ζωτική σημασία εξετάζει επιπλέον, το χρόνο που μεσολαβεί από τη στιγμή που αυτά τεθούν εκτός λειτουργίας μέχρι να φτάσουν στο ελάχιστο επίπεδο ποιότητας (minimum quality level), δηλαδή τη στιγμή που το αντίκτυπο επηρεάζει περισσότερο την κοινωνία, καθώς και το χρόνο που απαιτείται για την ελάχιστη ή πλήρη ανάκαμψη αυτών. Με γνώμονα τα παραπάνω, χωρίζει τα προϊόντα και τις υπηρεσίες σε πέντε κατηγορίες, γρήγορη εμφάνιση αντικτύπου με αργή ανάκαμψη, όπως η ποιότητα του νερού, αργή εμφάνιση αντικτύπου με αργή ανάκαμψη, όπως η ναυτιλία, γρήγορη εμφάνιση αντικτύπου με γρήγορη ανάκαμψη, όπως οι τηλεπικοινωνίες, αργή εμφάνιση αντικτύπου με γρήγορη ανάκαμψη και πολύ γρήγορη εμφάνιση αντικτύπου με πολύ γρήγορη ανάκαμψη, όπως οι επικοινωνίες έκτακτης ανάγκης [17].

Μια μεταγενέστερη ολλανδική προσέγγιση, προτείνει μια στρατηγική εθνικής ασφάλειας (NSS), η οποία διακρίνεται σε δύο φάσεις, τη φάση ανάλυσης (analysisphase) και τη φάση στρατηγικού σχεδιασμού (strategic planning phase). Η «εθνική αποτίμηση επικινδυνότητας (NRA)», η οποία έχει αναπτυχθεί με στόχο την αποτίμηση των κινδύνων σε εθνική κλίμακα, αποτελεί τμήμα της φάσης ανάλυσης και έπεται αυτής. Στη φάση ανάλυσης οι κίνδυνοι συγκεντρώνονται και αναλύονται, με τη μορφή ενός ή περισσοτέρων σεναρίων, για παράδειγμα την επίδραση (effect) ενός περιστατικού στη συνέχιση μιας κρίσιμης υποδομής, ή οι συνέπειες ενός περιστατικού, όσον αφορά στη φύση και την κλίμακα. Η σοβαρότητα των σεναρίων υπολογίζεται με βάση τη βαθμολογία που συγκεντρώνουν σε δέκα κριτήρια αντικτύπου (impact factors). Η επικινδυνότητα και σε αυτή την προσέγγιση ορίζεται ως ένας συνδυασμός αντικτύπου (impact), δηλαδή το σύνολο των συνεπειών (consequence) του περιστατικού – σεναρίου, και της πιθανότητας (likelihood), δηλαδή της εμφάνισης ενός περιστατικού – σεναρίου με τις συνέπειές του. Τα βήματα της μεθοδολογίας είναι [18]:

- Έλεγχος της Πληρότητας της Περιγραφής του Σεναρίου

Το σενάριο θα πρέπει να περιέχει επαρκείς πληροφορίες για την αποτίμηση του αντικτύπου και της πιθανότητας.

- Αποτίμηση του Αντικτύπου του Σεναρίου (Impact Assessment)

Κάθε σενάριο αναλύεται και αποτιμάται σύμφωνα με τα κριτήρια αντικτύπου (impact criteria).

- Αποτίμηση της Πιθανότητας Εμφάνισης του Σεναρίου (Likelihood Assessment)

Κάθε σενάριο αναλύεται και αποτιμάται ανάλογα με την πιθανότητα εμφάνισής του.

- Εκτίμηση της Επικινδυνότητας (Risk Assessment) του σεναρίου και αναφορά των ευρημάτων

Πιο συγκεκριμένα, σε ό,τι αφορά την αποτίμηση αντικτύπου (impact assessment), τα κριτήρια αντικτύπου τα οποία έχουν επιλεγεί για την «εθνική αποτίμηση επικινδυνότητας» αντικατοπτρίζουν το σκοπό της στρατηγικής, δηλαδή

την προστασία των ζωτικών συμφερόντων της Ολλανδίας. Κάθε ένα από τα παρακάτω πέντε ζωτικά συμφέροντα μετατρέπονται σε ένα έως το πολύ τρία κριτήρια αντικτύπου, σχηματίζοντας συνολικά δέκα κριτήρια. Τα κριτήρια αυτά θεωρούνται από τη δεδομένη προσέγγιση αντιπροσωπευτικά για την αποτίμηση και κατάταξη όλων των πιθανών συμβάντων με βάση το αντίκτυπο αυτών.

Για κάθε ένα από τα παραπάνω κριτήρια, το αντίκτυπο καθίσταται μετρήσιμο, χωρίζοντας τα κριτήρια σε πέντε κατηγορίες. Συγκεκριμένα, στην κατηγορία A (Περιορισμένες συνέπειες), την κατηγορία B (Σημαντικές συνέπειες), την κατηγορία C (Σοβαρές συνέπειες), την κατηγορία D (Πολύ Σοβαρές συνέπειες) και την κατηγορία E (Καταστροφικές συνέπειες). Με την κατηγοριοποίηση επιτυγχάνεται η διαχείριση της αβεβαιότητας σχετικά με τα δεδομένα, για παράδειγμα ο αριθμός των θανάτων μεταξύ 100 – 1000 εμπίπτουν στην ίδια κατηγορία. Να διευκρινίσουμε ότι όλα τα κριτήρια αξιολογούνται με βάση την έκταση (range) και τη διάρκεια (duration) του περιστατικού. Συνεπώς για κάθε σενάριο προκύπτει μια βαθμολογία σε κάθε κριτήριο. Καθώς πρόκειται για μια ανάλυση πολλαπλών κριτηρίων (MCA), οι βαθμολογίες του εκάστοτε σεναρίου αθροίζονται, προκειμένου να επιτευχθεί μια ισορροπημένη μέσου όρου τελική αποτίμηση του βαθμού αντικτύπου του κάθε σεναρίου. Το τελευταίο γίνεται μέσω διαφόρων μεθόδων, όπως «Weighted Sum», «Medal Method» και «EvaMix». Είσοδος σε κάθε μέθοδο είναι οι βαθμοί του κάθε σεναρίου στα δέκα διαφορετικά κριτήρια, καθώς και η σημαντικότητα (weight) του εκάστοτε κριτηρίου. Ωστόσο, η σημαντικότητα των κριτηρίων γίνεται μέσω πέντε διαφορετικών προφίλ προτίμησης (preference profiles), καθώς η αξιολόγηση των κριτηρίων είναι υποκειμενική [19].

Αναφορικά με την αποτίμηση της πιθανότητας εμφάνισης ενός περιστατικού, να αναφέρουμε αρχικά ότι οι πηγές πληροφόρησης είναι συνήθως βασισμένες σε ιστορικό, πιθανοτικά μοντέλα, σε δένδρα απόφασης (decision trees) και αναλύσεις δικτύου, αλλά και σε απόψεις ειδικών. Εν συνεχεία, η πιθανότητα χωρίζεται επίσης σε πέντε κατηγορίες, όπου κατηγορία A (Εξαιρετικά Απίθανο), την κατηγορία B (Απίθανο), την κατηγορία C (Δυνατό - Possible), την κατηγορία D (Πιθανό – Likely) και την κατηγορία E (Πολύ Πιθανό). Επίσης, στις κατηγορίες από A έως D, η πιθανότητα χωρίζεται σε επιπλέον τρείς υποκατηγορίες, Χαμηλή (Low), Μεσαία (Medium) και Υψηλή (High). Η δημιουργία υποκατηγοριών είναι σημαντική για να καθορίζονται η προβλεπόμενη τιμή για την πιθανότητα του συμβάντος (V), το

κατώτερο όριο για την πιθανότητα του συμβάντος (Ο) και το ανώτατο όριο για την πιθανότητα του συμβάντος (Β). Η πιθανότητα ενός περιστατικού καθορίζεται πρώτον από το ερέθισμα (trigger), δηλαδή την αιτία του συμβάντος. Γι' αυτό γίνεται διαχωρισμός μεταξύ των σεναρίων κινδύνου (hazard scenarios), δηλαδή των περιστατικών λόγω μη κακόβουλων ή εσκεμμένων ενεργειών και των σεναρίων απειλής (threat scenarios), τα οποία προέρχονται από κακόβουλη πρόθεση.

Η Καναδική προσέγγιση έχει αναπτυχθεί από τον κλάδο διαχείρισης έκτακτων αναγκών και εθνικής ασφάλειας της Δημόσιας Ασφάλειας και Ετοιμότητας Έκτακτων Αναγκών του Καναδά (PSEPC) και συγκεκριμένα μέσω του προγράμματος Διασφάλισης της Εθνικής Κρίσιμης Υποδομής (NCIAP). Στόχος του τελευταίου, ήταν να προσδιορίσει τα αγαθά και να καθορίσει την κρισιμότητα αυτών, σαν τμήμα μιας ενσωματωμένης διαδικασίας διαχείρισης επικινδυνότητας, έτσι ώστε να προστατευθούν τα κρίσιμα αγαθά και να διασφαλιστούν οι κρίσιμες υπηρεσίες. Το «Critical Infrastructure Priority Assessment Screening Model» που προτείνεται αντικατοπτρίζει την προσέγγιση διαχείρισης επικινδυνότητας πάνω στην οποία βασίζεται το NCIAP. Προκειμένου να προσδιορίσουν και να βαθμολογήσουν τα κρίσιμα αγαθά (critical assets) προτείνονται τα ακόλουθα βήματα [20]:

- Καταγραφή των Αγαθών

Αρχικά προσδιορίστηκαν οι κρίσιμοι τομείς, δηλαδή αυτός της Ενέργειας, των Τηλεπικοινωνιών και της Πληροφορικής, της Οικονομίας, της Υγείας, των Βασικών αναγκών (φαγητού και νερού), των Μεταφορών, της Ασφάλειας, της Κυβέρνησης και της Βιομηχανίας. Στη συνέχεια, καταγράφηκαν οι υπο-Τομείς προκειμένου να εστιάσουν στα ιδιαίτερα χαρακτηριστικά της εκάστοτε υποδομής.

- Καθορισμός Κρισιμότητας

Προτείνεται η χρήση ποιοτικών μέτρων, όπως «Χαμηλή», «Μεσαία» και «Υψηλή». Επίσης, η αξιολόγηση μιας Υποδομής ως προς την κρισιμότητά της γίνεται μέσω παραγόντων αντικτύπου (impact factors) ή παραγόντων κρίσιμων αγαθών (critical asset factors) και κριτηρίων συνεπειών (consequence criteria).

- Αποτίμηση του Αντικτύπου της Απώλειας ενός Αγαθού

Γίνεται χρήση των λεγόμενων παραγόντων αντικτύπου, τα οποία αποτελούν κριτήρια που χρησιμοποιούνται έτσι ώστε να δοθεί προτεραιότητα σε κρίσιμα αγαθά και Υποδομές. Για την αποτίμηση του αντικτύπου προτείνονται οι ακόλουθοι παράγοντες. Οι τελευταίοι αναλύονται με βάση την έκταση (scope), το μέγεθος (magnitude) και χρονική διάρκεια.

Πιο αναλυτικά, ο πρώτος παράγοντας, «Concentration of people and assets» αναφέρεται στον αριθμό των θανάτων, των τραυματιών και των επιπτώσεων στο περιβάλλον, ενώ εστιάζει σε εταιρικό επίπεδο. Εν συνεχεία, είναι οι οικονομικές απώλειες, «Economic factor», λόγο φυσικών, πληροφοριακών και ανθρώπινων βλαβών, το οποίο εστιάζει επίσης σε εταιρικό επίπεδο. Ο τρίτος παράγοντας. «Critical infrastructure Sector (CIS)», εστιάζει σε επίπεδο τομέα και αναφέρεται στην επιρροή των απωλειών των αγαθών ή των υπηρεσιών σε έναν τομέα κρίσιμων υποδομών. Το αντίκτυπο της αλληλεξάρτησης εστιάζει σε διατομεακό επίπεδο και εξετάζει την επίδραση που έχει σε άλλες κρίσιμες υπηρεσίες ή τομείς η απώλεια ή υποβάθμιση μιας υπηρεσίας. Το εν λόγω κριτήριο παρέχει επίσης και αποτίμηση των πιθανών εξαρτήσεων που έχουν άλλες κρίσιμες υπηρεσίες με το συγκεκριμένο αγαθό. Στόχος είναι να ελεγχθεί κατά πόσο η απώλεια ενός αγαθού ή μιας υπηρεσίας μπορεί να επηρεάσει άλλες κρίσιμες υπηρεσίες εντός του ίδιου τομέα ή διαφορετικού και να οδηγήσει σε ένα cascading effect. Να αναφέρουμε ότι οι αλληλεξαρτήσεις σε αυτήν την περίπτωση είναι φυσικές, χωρικές και λογικές. Σχετικά με την παροχή υπηρεσιών, «Service delivery» σε διατομεακό επίπεδο, είναι ένας συνδυασμός διαθεσιμότητας, χρόνου και κόστους που προκύπτει πριν την ανάκτηση μιας υπηρεσίας ή ενός αγαθού μετά από απώλεια. Ως τελευταίος παράγοντας ορίζεται η δημόσια εμπιστοσύνη, «Public confidence», στην ικανότητα για παράδειγμα της κυβέρνησης να προστατεύσει τη δημόσια υγεία, την ασφάλεια της οικονομίας ή να διαβεβαιώσει την παροχή βασικών υπηρεσιών, ως αποτέλεσμα της απώλειας ενός αγαθού ή μιας υπηρεσίας.

- Αποτίμηση των Συνεπειών της Απώλειας ενός Αγαθού

Θέτονται ερωτήματα στην ομάδα αποτίμησης προκειμένου να αποκτηθούν επιπρόσθετες πληροφορίες για τις συνέπειες που σχετίζονται με τον εκάστοτε παράγοντα αντικτύπου. Ενδεικτικές ερωτήσεις μπορούν να βασιστούν στα υπάρχοντα σχέδια ασφάλειας και αποτιμήσεις, όπως για παράδειγμα η αποτίμηση ευπαθειών

(VA), τα σχέδια επιχειρησιακής συνέχειας (BCPs), τα σχέδια ανάκαμψης από καταστροφή (DRPs) και τα σχέδια διαχείρισης έκτακτων αναγκών (EMPs).

Επίσης, το 2009 οι Ηνωμένες Πολιτείες της Αμερικής υιοθέτησαν το «Εθνικό Πλάνο Προστασίας Υποδομών» (National Infrastructure Protection Plan - NIPP). Το Νομοσχέδιο Εσωτερικής Ασφάλειας (HSA) του 2002 αναθέτει στο DHS την αρμοδιότητα για την προστασία των Κρίσιμων Υποδομών μέσω ενός εθνικού σχεδίου, αλλά και την πρόταση μέτρων για να επιτευχθεί αυτό, σε συντονισμό με άλλες υπηρεσίες της Ομοσπονδιακής Κυβέρνησης και κατόπιν συνεργασίας με το Κράτος και τις τοπικές κυβερνητικές υπηρεσίες και αρχές, τον ιδιωτικό τομέα, και άλλους φορείς. Μέσω της Προεδρικής Οδηγίας Εσωτερικής Ασφάλειας 7 (HSPD-7), δημιουργήθηκε το επιθυμητό εθνικό σχέδιο. Κατόπιν, ο Πρόεδρος ανέθεσε στον Υπουργό Εσωτερικής Ασφάλειας να κατευθύνει τις προσπάθειες για την προστασία των Κρίσιμων Υποδομών από τους εμπλεκόμενους που προαναφέραμε, ενώ στους SSAs την εφαρμογή του πλαισίου NIPP σε κάθε Τομέα, ανάλογα με τα ιδιαίτερα χαρακτηριστικά και τους κινδύνους του εκάστοτε, με αποτέλεσμα να υπάρχουν 18 SSPs.

Στο πλαίσιο του «Εθνικού Πλάνου Προστασίας Υποδομών» ο όρος προστασία περιλαμβάνει ενέργειες για την αποτροπή των απειλών, τον μετριασμό των ευπαθειών, ή την ελαχιστοποίηση των συνεπειών, αναφορικά με μια τρομοκρατική επίθεση ή άλλη ανθρωπογενή ή φυσική καταστροφή. Ενδεικτικά παραδείγματα τέτοιων ενεργειών είναι η βελτίωση των πρωτοκόλλων ασφάλειας, η εισαγωγή ανθεκτικότητας και πλεονασμού, η εγκατάσταση συστημάτων ασφάλειας και η υλοποίηση μέτρων για προστασία στον κυβερνοχώρο, εκπαίδευση και σχέδιο επιχειρησιακής συνέχειας.

Το «Εθνικό Πλάνο Προστασίας Υποδομών» παρέχει ένα περιεκτικό και ενοποιημένο πλαίσιο για την προστασία κρίσιμης υποδομής και βασικών πόρων (CI/KR). Πιο συγκεκριμένα, ασχολείται με τις αλληλεξαρτήσεις μεταξύ των τομέων, την ασφάλεια στον κυβερνοχώρο (cybersecurity) και τη διεθνή φύση των απειλών σε μια κρίσιμη υποδομή. Όπως φαίνεται και στην ακόλουθη εικόνα το πλαίσιο διαχείρισης επικινδυνότητας NIPP χωρίζεται σε έξι βήματα:

- Βήμα 1: Καθορισμός των Στόχων Ασφάλειας

Σε αυτό το σημείο λαμβάνονται υπ' όψιν κρίσιμα ζητήματα, όπως η απώλεια ανθρώπινης ζωής, το οικονομικό αντίκτυπο και το αντίκτυπο στην εθνική ασφάλεια.

- Βήμα 2: Προσδιορισμός Αγαθών, Συστημάτων, Δικτύων και Λειτουργιών

Είναι το πρώτο βήμα έτσι ώστε μια υποδομή να εξασφαλίσει την ανθεκτικότητά (resilience) της.

- Βήμα 3: Αποτίμηση Επικινδυνότητας (Risk Assessment)

Μέσω ποσοτικών, συστηματικών και αυστηρών διαδικασιών παράγονται ολοκληρωμένα αποτελέσματα.

- Βήμα 4: Ιεράρχηση (Prioritization) Ενεργειών

Το Τμήμα Εσωτερικής Ασφάλειας της Αμερικής (DHS) μέσω της ιεράρχησης, προσδιορίζει πότε η μείωση της επικινδυνότητας είναι πιο σημαντική και στη συνέχεια καθορίζει ποια μέτρα προστασίας θα πρέπει να παρθούν, καταλήγοντας σε μια πιο αποδοτική από πλευράς κόστους απόφαση.

- Βήμα 5: Υλοποίηση Προγραμμάτων Προστασίας (protective – proactive)

Υλοποίηση των μέτρων προστασίας που έχουν καθοριστεί στο προηγούμενο βήμα.

- Βήμα 6: Μέτρηση Αποτελεσματικότητας

Η αποτελεσματικότητα των προηγούμενων βημάτων αξιολογείται σε αυτό το στάδιο, μέσω κατάλληλων δεικτών.

Το «Εθνικό Πλάνο Προστασίας Υποδομών» χρησιμοποιεί ένα σύνολο βασικών κριτηρίων (core criteria), για τις αποτιμήσεις επικινδυνότητας, έτσι ώστε να προσδιορίσει τα χαρακτηριστικά και τις πληροφορίες που χρειάζονται για την παραγωγή αποτελεσμάτων, τα οποία μπορούν να χρησιμοποιηθούν για τη σύγκριση επικινδυνότητας μεταξύ των Τομέων. Συγκεκριμένα, τα κριτήρια αυτά περιλαμβάνουν ορισμένες βασικές αρχές οι οποίες εφαρμόζονται σε όλα τα τμήματα μιας μεθοδολογίας επικινδυνότητας, αλλά και σε συγκεκριμένες οδηγίες σχετικά με τις πληροφορίες που θα πρέπει να λάβουν υπόψη για κάθε συστατικό της επικινδυνότητας (C, V, T). Όσον αφορά στις αρχές, το «Εθνικό Πλάνο Προστασίας

Υποδομών» ορίζει ότι μια αποτίμηση επικινδυνότητας θα πρέπει να αναφέρει επαρκώς τις χρησιμοποιούμενες πληροφορίες και πως αυτές συνδυάζονται, να παράγει συγκρίσιμα και επαναλαμβανόμενα αποτελέσματα ακόμη και στην περίπτωση αποτιμήσεων διαφορετικών Κρίσιμων Υποδομών και από διαφορετικούς αναλυτές. Με άλλα λόγια, μια αποτίμηση θα πρέπει όσο το δυνατόν να μην επηρεάζεται από υποκειμενικές κρίσεις. Επίσης, θα πρέπει σύμφωνα με το «Εθνικό Πλάνο Προστασίας Υποδομών» να χρησιμοποιούνται ειδικοί στον τομέα της αποτίμησης επικινδυνότητας και τυχόν αβεβαιότητα σχετικά με τις εκτιμήσεις συνεπειών, ευπαθειών και απειλών θα πρέπει να αναφέρονται. Σημαντική θεωρείται και η αποτίμηση των τριών συστατικών του κινδύνου για το εκάστοτε σενάριο επικινδυνότητας. Στο τελευταίο, στηρίζονται και οι οδηγίες των βασικών κριτηρίων, τις οποίες για λόγους πληρότητας αναφέρουμε ακολούθως.

- Οδηγίες για Αποτίμηση Συνεπειών (Consequence Assessment) Αρχικά θα πρέπει να καταγράφονται τα σενάρια που έχουν αποτιμηθεί, τα εργαλεία που έχουν χρησιμοποιηθεί και οποιαδήποτε σημαντική υπόθεση έχει γίνει. Στη συνέχεια, γίνεται αποτίμηση του αριθμού των τραυματιών, των θανάτων, των ασθενειών, όπου αυτό είναι εφικτό, επίσης της οικονομικής απώλειας, προσδιορίζοντας το είδος και τη διάρκεια αυτής, καθώς και οι υπόλοιποι δύο παράγοντες που έχουμε προαναφέρει. Μπορούν επιπρόσθετα να καταγραφούν τυχόν μέτρα προστασίας, αφότου το περιστατικό έχει λάβει χώρα.
- Οδηγίες για την Αποτίμηση Ευπαθειών (Vulnerability Assessment) Να γίνει καταγραφή των ευπαθειών που σχετίζονται με φυσικούς, κυβερνοχωρικούς και ανθρώπινους παράγοντες (εσωτερικών και εξωτερικών απειλών), με κρίσιμες εξαρτήσεις και φυσική εγγύτητα με τους κινδύνους (hazards). Να περιγραφούν όλα τα υπάρχοντα μέτρα και πως αυτά μπορούν να μειώσουν την ευπάθεια του κάθε σεναρίου, αλλά και να εκτιμηθεί η πιθανότητα επιτυχίας του κάθε σεναρίου. Όσον αφορά στους φυσικούς κινδύνους (hazards), να γίνεται αποτίμηση της πιθανότητας πρόκλησης ζημιάς σε ένα αγαθό, σύστημα, ή δίκτυο, δεδομένου ότι ο κίνδυνος συμβαίνει στην περιοχή ενδιαφέροντος για το σενάριο κινδύνου.
- Οδηγίες για την Αποτίμηση Απειλών (Threat Assessment) – HITRAC

- ❖ Εχθρική Απειλή Προτείνεται ο καθορισμός της ικανότητας ενός κακόβουλου να αναγνωρίσει το στόχο, αλλά και του βαθμού αποτροπής που εμπεριέχουν τα υπάρχοντα μέτρα ασφάλειας. Επίσης, να προσδιοριστούν οι μέθοδοι επίθεσης που ενδέχεται να πραγματοποιηθούν σε συνδυασμό με την ικανότητα ενός κακόβουλου να τις επιτύχει και το βαθμό σπουδαιότητας που έχει για τον τελευταίο να επιτεθεί στο στόχο. Σημαντικό θεωρείται να εκτιμηθεί η απειλή ως η πιθανότητα ο επιτιθέμενος να επιχειρήσει μια δεδομένη μέθοδο επίθεσης εναντίον του στόχου. Ωστόσο, αν η πιθανότητα απειλής δεν μπορεί να εκτιμηθεί, αναφέρεται η χρήση υποθετικών τιμών επικινδυνότητας (συνέπεια, ευπάθεια).
- ❖ Φυσικές Καταστροφές και Κίνδυνοι Χωρίς Πρόθεση Προτείνεται η χρήση εργαλείων ανάλυσης (analytic tools) και ιστορικών δεδομένων για την εκτίμηση της πιθανότητας κάποιο περιστατικό να επηρεάσει τις Κρίσιμες Υποδομές.

4.9.2 Βασική Προσέγγιση Αποτίμησης Επικινδυνότητας

Η πιο γνωστή προσέγγιση αποτίμησης Επικινδυνότητας, σε αντίθεση με την παραδοσιακή, δίνει έμφαση στο πιθανό αντίκτυπο σε μια κοινωνία ή έναν Τομέα (Sector), εξετάζει τις αλληλεξαρτήσεις, ενώ το αντίκτυπο είναι πολύ πιο υψηλό. Συγκεκριμένα, για να χαρακτηρίσει μια Υποδομή ως Κρίσιμη για την κοινωνία, ή τον Τομέα στον οποίο ανήκει, αποτιμά το επίπεδο αντικτύπου (impact level) που θα προκύψει από την παρουσία απειλών ασφάλειας. Οι παράγοντες αντικτύπου (impact factors) ή οι παράγοντες κρίσιμων αγαθών (critical asset factors), αποτελούν κριτήρια που χρησιμοποιούνται έτσι ώστε να δοθεί προτεραιότητα σε κρίσιμα αγαθά και υποδομές. Η μεθοδολογία για ανάλυση κρισιμότητας (criticality analysis) που προτείνεται αποτελείται από τα παρακάτω έξι βήματα [21]:

- Προσδιορισμός των Κρίσιμων Αγαθών

Όμοια με την ανάλυση επικινδυνότητας (risk analysis) καταγράφονται τα αγαθά της υπό εξέταση Κρίσιμης Υποδομής.

- Καθορισμός των Διασυνδέσεων (Interconnections) και Εξαρτήσεων

Οι διασυνδέσεις χωρίζονται σε δύο κατηγορίες, των εξαρτώμενων (dependent) Κρίσιμων Υποδομών, δηλαδή Υποδομών που εξαρτώνται από την υπό εξέταση

Υποδομή και των απαιτούμενων (requisite), δηλαδή Υποδομών που απαιτούνται από την υπό εξέταση Υποδομή για τη λειτουργία της. Στην ανάλυση κρισιμότητας οι διασυνδεδεμένες Κρίσιμες Υποδομές, οι οποίες συνεπάγονται ένα γενικό κοινωνικό κίνδυνο, θα πρέπει να λαμβάνονται υπόψη ακόμη και στην περίπτωση που δεν επιφέρουν κάποιο κίνδυνο για την Υποδομή. Το τελευταίο επιβάλλεται καθώς οι διασυνδέσεις βοηθούν στην εκτίμηση των σφαιρικών απειλών και ευπαθειών εντός των διασυνδεδεμένων Κρίσιμων Υποδομών.

- Εκτίμηση του Αντικτύπου Κρισιμότητας (Criticality Impact)

Οι Παράγοντες Αντικτύπου (Impact Factors), τους οποίους θα αναφέρουμε στη συνέχεια, δίνουν έμφαση στο κοινωνικό παρά στο εσωτερικό αντίκτυπο και η εκτίμησή του γίνεται με βάση την έκταση, τη σοβαρότητα και το χρόνο.

- Καθορισμός Απειλών

Καθώς η ανάλυση κρισιμότητας βασίζεται στις διασυνδεδεμένες Κρίσιμες Υποδομές, θα πρέπει να δημιουργηθεί μια λίστα των εν δυνάμει απειλών. Ενδεικτικά να αναφέρουμε, την προσποίηση ενός αυθεντικοποιημένου χρήστη (masquerading attack), τη μη αυθεντικοποιημένη χρήση πόρων τη Υποδομής, την εισαγωγή ιομορφικού λογισμικού, την παρεμπόδιση (interception) ή παραποίηση (manipulation) επικοινωνιών, τις αποτυχίες επικοινωνίας, τις αποτυχίες τεχνικής φύσεως, τις διακοπές ρεύματος, τις αποτυχίες λογισμικού, τα λειτουργικά σφάλματα, τα σφάλματα συντήρησης, τα σφάλματα χρηστών, τη φωτιά, τις φυσικές καταστροφές, τις ελλείψεις προσωπικού, την εκ προθέσεως καταστροφή, την τρομοκρατία και την κατασκοπεία.

- Εκτίμηση του Επιπέδου Απειλών και Ευπαθειών

Οι πιθανές απειλές αφορούν τόσο το εσωτερικό της υπό εξέταση Κρίσιμης Υποδομής, αλλά και όλη την έκταση των διασυνδέσεων και εξαρτήσεων αυτής. Η πιθανότητα της απειλής μπορεί να βασιστεί στο ιστορικό προηγούμενων περιστατικών, στην υπάρχουσα βιβλιογραφία και σε συνεντεύξεις με ειδικούς. Οι απειλές που συναντώνται σε μια Κρίσιμη Υποδομή είναι ένα υπερσύνολο όσων συναντάμε σε μια παραδοσιακή ανάλυση επικινδυνότητας. Ομοίως, πρέπει να γίνει ο καθορισμός και των ευπαθειών της Υποδομής, ο οποίος δεν είναι εύκολος, καθώς οι ευπάθειες μπορεί να κληρονομηθούν και από άλλες Κρίσιμες Υποδομές.

- Εκτίμηση των «Criticality Risk Factors»

Όπως συμβαίνει και στην τυπική ανάλυση επικινδυνότητας, η επικινδυνότητα είναι συνάρτηση των απειλών, των ευπαθειών και του αντικτύπου κρισιμότητας.

Τα κριτήρια χωρίζονται σε τρεις διακριτές κατηγορίες, την έκταση, τη σοβαρότητα και το χρόνο. Η πρώτη αποτελείται από τον Πληγέντα Πληθυσμό (Population Affected) λόγω ενός συμβάντος, την Πυκνότητα του Πληθυσμού (Population Concentration), άνθρωποι/km2, και την Εμβέλεια (Range), έτσι ώστε να προσδιορίσει κατά πόσο ένα περιστατικό είναι τοπικό ή διεθνές παραδείγματος χάριν. Στη συνέχεια, η Σοβαρότητα/Σπουδαιότητα ενός περιστατικού εξαρτάται από διάφορους παράγοντες. Καταρχήν, εξαρτάται από την Οικονομική Επίπτωση (Economic Impact) ενός συμβάντος, όπως για παράδειγμα τις απώλειες στην ίδια την Υποδομή από την υποβάθμιση της υπηρεσίας, ή τις απώλειες σε αγαθά και πληροφορία, το κόστος ανάκαμψης (recovery cost), αλλά και την εκτιμώμενη απώλεια λόγω των διαδοχικών επιδράσεων (cascading effects). Για την εκτίμηση της οικονομικής απώλειας μπορεί να χρησιμοποιηθεί το ακαθάριστο εγχώριο προϊόν (GDP). Ο επόμενος παράγοντας, αυτός της Αλληλεξάρτησης (Interdependency) ο οποίος είναι βασικός όρος στην παρούσα εργασία, εκτιμά την πιθανότητα μιας διαδοχικής επίδρασης εντός ενός Τομέα και μεταξύ διαφόρων Τομέων. Η Δημόσια Εμπιστοσύνη (Public Confidence) στη συνέχεια εκτιμά την επίπτωση στη δημόσια εμπιστοσύνη ή στην ικανότητα της κυβέρνησης για παράδειγμα να προσφέρει δημόσιες υπηρεσίες και να διατηρεί την υγεία και την ασφάλεια. Οι επόμενοι πέντε παράγοντες που ακολουθούν χρησιμοποιούνται στην ανάλυση επικινδυνότητας και στην προστασία Κρίσιμων Υποδομών, είναι κατά βάση κοινωνικής φύσεως, έχουν σχετικά υψηλή εκτίμηση (7 έως 10 στην κλίμακα από 1 έως 10), ενώ γενικά δεν εφαρμόζονται στους εμπορικούς οργανισμούς. Ο πρώτος παράγοντας είναι οι Διεθνείς Σχέσεις (International Relations) και αντιπροσωπεύει την επίπτωση ενός περιστατικού στις διπλωματικές σχέσεις μιας χώρας, όπως για παράδειγμα η ακύρωση συμφωνιών εμπορίου. Ο δεύτερος παράγοντας αξιολογεί την επίπτωση στη Δημόσια Τάξη (Public Order), εξαιτίας για παράδειγμα της αποκάλυψης εμπιστευτικών πληροφοριών, ή της μη διαθεσιμότητας κρίσιμων δημόσιων υπηρεσιών (όπως ρεύματος, ή παροχής νερού). Ο τρίτος παράγοντας είναι αυτός της Δημόσιας Πολιτικής και Λειτουργίας (Policy and Operations of Public Service), η οποία εκτιμά την ικανότητα της κυβέρνησης να τις φέρει εις πέρας. Ο παράγοντας

αυτός διαφοροποιείται από αυτόν της Δημόσιας Εμπιστοσύνης, καθώς ο πρώτος δε λαμβάνει υπόψη ψυχολογικές επιπτώσεις. Ο τέταρτος παράγοντας ακολούθως είναι η Δημόσια Ασφάλεια (Safety) και συμπεριλαμβάνει τραυματισμούς, χρόνιες ασθένειες, ακόμη και θανάτους. Ωστόσο, σε αντίθεση με τα κριτήρια έκτασης δε λαμβάνει υπόψη τον αριθμό των ατόμων που επηρεάζει. Ως πέμπτος και τελευταίος παράγοντας είναι αυτός της Άμυνας (Defense), δηλαδή της ικανότητας της κυβέρνησης να προστατεύσει τον πληθυσμό από εχθρικές επιθέσεις, είτε λόγω αποκάλυψης ή τροποποίησης κρίσιμων πληροφοριών, είτε λόγω μη διαθεσιμότητας Κρίσιμων Υποδομών. Ο εν λόγω παράγοντας, λόγο της φύσης του έχει μεσαία έως υψηλή τιμή. Όσον αφορά στο κριτήριο του Χρόνου, όπως φαίνεται και από τον πίνακα, αποτελείται από τον Χρόνο Ανάκαμψης (Recovery Time), και τη Διάρκεια (Duration) του αντικτύπου. Το πρώτο, επηρεάζεται από τη διαθεσιμότητα κάποιου υποκατάστατου και το κόστος μέχρι την αποκατάσταση του αγαθού, ενώ το δεύτερο είναι διαφορετικό από το πρώτο, καθώς κάποιες υπηρεσίες μπορεί να αποκτούν και πάλι τη λειτουργικότητά τους, αλλά οι μακροχρόνιες επιπτώσεις από την προσωρινή μη διαθεσιμότητά τους να επηρεάζουν ακόμη την Κρίσιμη Υποδομή και το περιβάλλον της, για παράδειγμα οι οικονομικές απώλειες που προκλήθηκαν. Συνήθως η διάρκεια του αντικτύπου κυμαίνεται από κάποιες ώρες μέχρι και χρόνια. Καταληκτικά, προτείνονται και δύο παράγοντες που ανήκουν στην κατηγορία του χρόνου, αλλά εστιάζουν στη στιγμή που το κρίσιμο συμβάν λαμβάνει χώρα. Αυτοί είναι η στιγμή που το περιστατικό παράγει την πιο σοβαρή επίδρασή του (Impact Peak) και η περίοδος που αποδεικνύει μεταβολές στην κρισιμότητα (Critical Time Frames), κατά τη διάρκεια της κανονικής λειτουργίας και μιας κρίσιμης κατάστασης. Οι δύο τελευταίοι παράγοντες πρέπει να εξετάζονται όταν ένα συμβάν ενδέχεται να έχει μεγαλύτερο αντίκτυπο, έτσι ώστε να εκτιμηθεί η συνολική κρισιμότητα μιας απειλής ή ενός περιστατικού. Αξίζει να σημειώσουμε ότι η συγκεκριμένη τεχνική προτείνει την προσέγγιση της χειρότερης περίπτωσης (worst-case), αντί της χρήσης της μέσης τιμής για τον υπολογισμό του αντικτύπου. Συγκεκριμένα, το αντίκτυπο υπολογίζεται για κάθε παράγοντα και αυτό με τη μεγαλύτερη τιμή λογίζεται ως το συνολικό.

Η σημαντικότητα ύπαρξης μιας μεθόδου αποτίμησης επικινδυνότητας στις Κρίσιμες Υποδομές, φαίνεται από το μεγάλο εύρος των προσπαθειών που έχουν καταβληθεί σε παγκόσμιο επίπεδο. Με τη βοήθεια μια τέτοιας μεθόδου είναι δυνατόν

να αποτιμηθούν οι πιθανοί κίνδυνοι και να παρθούν πιο σωστές αποφάσεις από τη Διοίκηση της εκάστοτε Υποδομής, με αποτέλεσμα την επίτευξη μιας σχετικής ισορροπίας μεταξύ κόστους για την επίτευξη προστασίας στις Κρίσιμες Υποδομές και αντίστοιχου κέρδους.

4.10 Μοντέλα αλληλοεξαρτήσεων

Εκτός από τις μεθόδους οι οποίες είναι προσανατολισμένες στη μοντελοποίηση και στον προσδιορισμό των αλληλεξαρτήσεων ενός συγκεκριμένου Τομέα, όπως είναι αυτός της ηλεκτρικής ενέργειας και των Τεχνολογιών Πληροφορίας και Επικοινωνίας υπάρχουν και πιο γενικές, με εφαρμογή σε μια ποικιλία Υποδομών. Τα γενικά μοντέλα αλληλεξαρτήσεων ανήκουν σε μια από τις ακόλουθες κατηγορίες. Πρώτη κατηγορία είναι τα εργαλεία συνολικής προσφοράς και ζήτησης (aggregate supply and demand tools), τα οποία εκτιμούν τη συνολική ζήτηση για υπηρεσίες της Υποδομής σε μια περιοχή και την ικανότητα προσφοράς αυτών των υπηρεσιών. Συγκεκριμένα, το μοντέλο ακολουθεί αναλύσεις τύπου «what-if», έτσι ώστε να καθορίσει τις συνέπειες και τις διαδοχικές επιδράσεις μιας απώλειας από την πλευρά της προσφοράς και της ζήτησης. Με άλλα λόγια, πόσο θα επηρεαστεί μια υποδομή και πόσο θα επηρεάσει με τη σειρά της άλλες υποδομές, αν δεν μπορεί να ικανοποιήσει τις ανάγκες της. Δεύτερη είναι οι δυναμικές προσομοιώσεις (dynamic simulations), οι οποίες εξετάζουν τις λειτουργίες των υποδομών, τις επιδράσεις των αποδιοργανώσεων (disruptions) και τις σχετικές συνέπειες, ενώ οι αλληλεξαρτήσεις αντιμετωπίζονται ως ροές αγαθών και υπηρεσιών μεταξύ διαφορετικών υποδομών. Στην τρίτη κατηγορία είναι τα μοντέλα βασισμένα σε αντιπροσώπους (agent-based), οι οποίοι λόγω του ότι μπορούν να μοντελοποιήσουν τα φυσικά συστατικά των υποδομών, επιτρέπουν την ανάλυση των λειτουργικών χαρακτηριστικών και των φυσικών καταστάσεων των υποδομών. Μέσω μικροοικονομικής ανάλυσης, δίνει τη δυνατότητα εξέτασης του βαθμού επιρροής των αποδιοργανώσεων μιας υποδομής στις επιχειρήσεις και την ικανότητα αυτών να ανταπεξέρχονται κατά τη διάρκεια και μετά το πέρας των εν λόγω αποδιοργανώσεων. Όσον αφορά στη φυσική διάσταση των υποδομών χρησιμοποιούνται μοντέλα (physics-based), τα οποία μέσω τεχνικών μηχανικής μελετούν μια κρίσιμη υποδομή σε επίπεδο Συνιστώσας (Component) και συνεπώς αποκτούν αναλυτικές πληροφορίες για αυτή. Για παράδειγμα, οι αναλύσεις σταθερότητας και ροής του ρεύματος μπορούν να γίνουν στα δίκτυα ηλεκτρικής ενέργειας. Τα μοντέλα κινητικότητας του

πληθυσμού (population mobility) αναπαριστούν τους ανθρώπους ως οντότητες, οι οποίες κινούνται σε μια αστική περιοχή, και τις αλληλεπιδράσεις μεταξύ αυτών ως αποτέλεσμα της παραγωγής και της κατανάλωσης αγαθών και υπηρεσιών από διάφορες υποδομές. Τα μοντέλα αυτά προσφέρουν υψηλή ανάλυση και πιστότητα των αστικών αλληλεξαρτήσεων, οι οποίες μελετώνται για παράδειγμα στα πλαίσια της επιδημιολογίας, των μεταφορών και των ασύρματων επικοινωνιών. Η τελευταία κατηγορία που αναφέρεται στη βιβλιογραφία αφορά το μοντέλο Leontief Input-Output, το οποίο εξετάζει από οικονομικής πλευράς την εξάπλωση της επικινδυνότητας μεταξύ αλληλεξαρτημένων υποδομών [22].

Γενικά μια Υποδομή μπορεί να εξετασθεί, όσον αφορά στις αλληλεξαρτήσεις που αυτή περιέχει, σε επίπεδο Συνιστώσας (Component level), Υποδομής (Infrastructure level) και Τομέα (Sector level). Σε επίπεδο Συνιστώσας οι πληροφορίες που εξάγονται είναι πιο λεπτομερείς, καθώς απεικονίζει αναλυτικά μια Υποδομή, ενώ σε επίπεδο Τομέα η Υποδομή εξετάζεται από μια πιο σφαιρική οπτική γωνία. Ωστόσο, σε επίπεδο Συνιστώσας είναι πιο δύσκολη η ακριβή αποτίμηση της επικινδυνότητας [23].

- Επίπεδο Συνιστώσας

Οι αλληλεπιδράσεις μεταξύ τόσο των συστατικών, όσο και των χρηστών της Υποδομής, μοντελοποιούνται με τη μορφή ενός κατευθυνόμενου πολυγράφου και κατ' επέκταση με τη χρήση μιας συνάρτησης απόκρισης (response function). Παράλληλα, μέσω ιστογραμμάτων δείχνει την επίδραση τόσο των μονόδρομων (one-way) ή γραμμικών (linear) όσο και των αμφίδρομων (two-way) ή κυκλικών (cyclical) αλληλεξαρτήσεων μεταξύ διαφορετικών υποδομών, μετά από μια ηθελημένη ή ακούσια μη λειτουργικότητα ενός αριθμού κόμβων. Όπως είναι αναμενόμενο, οι αμφίδρομες αλληλεπιδράσεις, επηρεάζουν και τις δύο υποδομές, σε μεγαλύτερο ποσοστό από τις μονόδρομες. Επίσης, αποδεικνύει ότι η ύπαρξη «buffered resources», καθυστερούν την επιρροή των αλληλεξαρτήσεων, καθώς μια υποδομή δεν εξαρτάται αποκλειστικά από την εισερχόμενη κίνηση, με αποτέλεσμα την καθυστέρηση εμφάνισης των διαδοχικών επιδράσεων (cascading effects). Όσον αφορά στη διαρθρωτική ευπάθεια, απαιτείται η γνώση της τοπολογίας της υποδομής, ενώ για να εκτιμηθεί η διαρθρωτική αποδοτικότητα χρησιμοποιείται η έννοια του μικρότερου μονοπατιού (shortest path length), το οποίο όσο πιο μικρό είναι, τόσο πιο

μεγάλη είναι η αποδοτικότητα, λόγο της καλής δόμησης του δικτύου. Η λειτουργική ευπάθεια στο ηλεκτρικό δίκτυο αποτιμάται με τη μείωση της παροχής ηλεκτρικής ενέργειας μετά την εκδήλωση μιας επίθεσης, ενώ στους αγωγούς φυσικού αερίου με το ποσοστό των εναπομεινάντων κόμβων, οι οποίοι λαμβάνουν τόση ποσότητα φυσικού αερίου, όση χρειάζονται για την κάλυψη των αναγκών τους. Η διαφορά των δύο ευπαθειών έγκειται στο γεγονός ότι η διαρθρωτική βοηθάει στο σχεδιασμό και τη βελτίωση των αλληλεξαρτώμενων Υποδομών μακροπρόθεσμα, ενώ η λειτουργική βραχυπρόθεσμα. Το πιο σημαντικό κομμάτι στη συγκεκριμένη ανάλυση ευπάθειας, είναι η μοντελοποίηση των αλληλεξαρτήσεων. Για να υπολογιστεί η αλληλεξαρτώμενη αποδοτικότητα κάθε Υποδομής, ένα ποσοστό των κόμβων αφαιρείται και από τις δύο υπό εξέταση αλληλεξαρτώμενες Υποδομές [24].

- Επίπεδο Υποδομής

Μοντελοποιούνται οι εξαρτήσεις με βάση τη συστημική προσέγγιση, δηλαδή ως είσοδοι σε μια διαδικασία (process), ή αλλιώς ως συναρτήσεις απόκρισης (response functions), όπου διαδικασία είναι μια Κρίσιμη Υποδομή. Για να επιτύχει την παραπάνω μοντελοποίηση λαμβάνει υπόψη διάφορους παράγοντες. Αρχικά, είναι οι παράγοντες ποιότητας, οι οποίοι ποικίλλουν ανάλογα με τον τύπο της υποδομής. Για παράδειγμα, σε μια Υποδομή ΤΠΕ λαμβάνεται υπόψη η αξιοπιστία και η ταχύτητα μεταφοράς των πληροφοριών, ενώ σε μια Υποδομή ηλεκτρικής ενέργειας, η συχνότητα και η τάση. Έτσι, μελετάει την κάθε Υποδομή με ξεχωριστά κριτήρια, αντί απόλυτων, όπως η ολοκληρωτική ή μη διαθεσιμότητα. Όπως προαναφέραμε, μια εξάρτηση είναι ένα είδος συναρτήσεως απόκρισης, συνεπώς το αποτέλεσμα της συνάρτησης αυτής εξαρτάται από την είσοδο. Με άλλα λόγια η έξοδος, δηλαδή αυτό που παράγει μια εξαρτώμενη υποδομή, επηρεάζεται από την υποδομή από την οποία εξαρτάται. Επίσης, η έξοδος επηρεάζεται και από τον παράγοντα του χρόνου. Σε αυτήν την κατηγορία, ανήκει η επίδραση που θα έχει η ταχύτητα μιας μερικής διακοπής μιας εξάρτησης στην έξοδο μιας Κρίσιμης Υποδομής, όπως για παράδειγμα η επίδραση που θα έχει η απότομη αύξηση της βενζίνης στο απόθεμα αυτής. Παράλληλα, μια εξάρτηση επηρεάζεται και από την κατάσταση λειτουργίας μιας Κρίσιμης Υποδομής, η οποία μπορεί να είναι κανονική, υπό πίεση, κρίσιμη και ανακτώμενη. Περιβαλλοντικοί παράγοντες, όπως η εποχή, όπου το χειμώνα απαιτείται μεγαλύτερη ποσότητα αερίου για θέρμανση, συμβάλλουν και αυτοί στη

διαμόρφωση των υπαρχουσών αλληλεξαρτήσεων, ή ακόμη και στη δημιουργία νέων [25].

- Επίπεδο Τομέα

Η αναγκαιότητα ανάλυσης των αλληλεξαρτήσεων προέκυψε από τα αποτελέσματα μιας μελέτης που πραγματοποίησε η Τεχνική Επιτροπή Κρίσιμης Υποδομής του NISC στην Ιαπωνία το 2007 στις δέκα Κρίσιμες Υποδομές της χώρας. Η μελέτη αυτή επιβεβαίωσε τη διάδοση των δυσμενών επιδράσεων μιας δυσλειτουργίας σε IT υπηρεσίες ενός Κρίσιμου Τομέα σε έναν ή περισσότερους, η οποία επηρέαζε και υπηρεσίες που δεν είχαν άμεση συγγένεια με IT. Το πλαίσιο που προτάθηκε για τη μοντελοποίηση των αλληλεξαρτήσεων, συνδυάζει το μοντέλο μη λειτουργικότητας εισροών-εκροών (IIM) του Leontief, όσον αφορά στις οικονομικές αλληλεξαρτήσεις, και τα Μπαϋεσιανά Δίκτυα (Bayesian Networks) για τις λειτουργικές. Το IIM υπολογίζει την οικονομική απώλεια λόγω μη διαθεσιμότητας σε διαφορετικούς Κρίσιμους Τομείς, η οποία βασίζεται στις αλληλεξαρτήσεις αυτών. Ένα Μπαϋεσιανό Δίκτυο από την άλλη μεριά, είναι ένα πιθανοτικό μοντέλο, αρκετά αποτελεσματικό και εύκολα διατηρήσιμο για λίγους κόμβους. Με τον τρόπο αυτό, αφού αποκτηθούν οι πληροφορίες για τις λειτουργικές εξαρτήσεις και κατασκευαστούν τα δίκτυα για κάθε υπό εξέταση Τομέα, το αποτέλεσμα εισάγεται στο IIM. Επιπρόσθετα, επισημαίνεται ότι οι τιμές της μη λειτουργικότητας αποδεικνύουν τις ευπάθειες ενός Τομέα και συνεπώς μπορεί να υπολογιστεί εκτός από την οικονομική απώλεια, η επιρροή στον πληθυσμό και σε κρίσιμους πόρους εθνικής εμβέλειας [26].

Βιβλιογραφία-Αναφορές

[1] Adar E. and Wuchner A., “Risk management for critical infrastructure protection challenges: Best practices and tools”, in Proc. of the First IEEE International Workshop on Critical Infrastructure Protection, 2005.

[2] Theoharidou M., Kotzanikolaou P., Gritzalis D, “Risk assessment methodology for interdependent critical infrastructures”, International Journal of Risk Assessment and Management (Special Issue on Risk Analysis of Critical Infrastructures), Vol. 15, No. 2/3, pp. 128-148, 2011.

[3] Elky S., “An Introduction to Information System Risk Management”, SANS Institute InfoSec Reading Room, May 31, 2006.

[4] Official website of the Department of Homeland Security, Critical Infrastructure, available at: http://www.dhs.gov/critical-infrastructure [Πρόσβαση 4/4/2017]

[5] International Standard ISO/IEC 27005, “Information technology - Security techniques - Information security risk management”, First edition 2008-06-15.

[6] Dudenhoeffer D. D., Permann M. R., Manic M., “CIMS: a framework for infrastructure interdependency modeling and analysis”, in the Proc. of the 38th conference on winter simulation, Winter simulation conference, Monterey, California, 2006, p. 478–85.

[7] Jose M. Yusta, Gabriel J. Correa, Roberto Lacal-Arántegui, “Methodologies and applications for critical infrastructure protection: State-of-the-art”, Energy Policy, Volume 39, Issue 10, October 2011, Pages 6100-6119.

[8] European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection ‘Achievements and next steps: towards global cyber-security’”, COM(2011)163 final, Brussels, 2011.

[9] Rhodes K. A., Willemssen J., “Technology Assessment - Cybersecurity for Critical Infrastructure Protection”, United States Government Accountability Office, Washington, May 28, 2004.

[10] Lukas L., Hromada M., “Resilience as main part of protection of critical infrastructure”, International Journal of Mathematical Models and Methods in Applied Sciences, Vol. 5, No. 6, pp. 1135-1142, 2011.

[11] T.D. O’Rourke, “Critical Infrastructure, Interdependencies, and Resilience”, pp. 22-29, The BRIDGE National Academy of Engineering, Vol. 37, No. 1, Spring 2007.

[12] Cookea D. L. and Rohledera T. R., “Learning from incidents: from normal accidents to high reliability”, Journal of the System Dynamics Society, System Dynamics Review, Vol. 22, No. 3, pp. 213–239, 2006.

[13] Sinclair N., “Resilience in Critical Infrastructures: The case of the Queensland Electricity Industry”, Master Thesis, School of Management – Faculty Business, Queensland University of Technology, Australia, 2009.

[14] Australian National Audit Office, “Business Continuity Management: Keeping the wheels in motion”, A guide to effective control, Better practice, January 2000.

[15] European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”, COM(2009)149 final, Brussels, 2009.

[16] European Commission, “Communication from the Commission of 12 December 2006 on a European Programme for Critical Infrastructure Protection”, COM (2006)786 Final, Brussels, Belgium, 2006.

[17] Luiijf E., Burger H., Klaver M., “Critical infrastructure protection in the Netherlands: A quick-scan”, in the Proc. of the EICAR Conference, 2003.

[18] Ministry of the Interior and Kingdom Relations, “National Risk Assessment Method Guide 2008”, The Hague, The Netherlands, 2008.

[19] Popescu C.-A., Simion C.P., “A method for defining critical infrastructures”, 8th World Energy System Conference, (WESC-2010), Vol. 42, No. 1, pp. 32-34, June 2012.

[20] Haimes Y. Y, Risk Modeling Assessment and Management, Wiley & Sons, Inc, New Jersey, 2009 (3rd edition).

[21] Santos J. R., “Inoperability input-output modeling of disruptions to interdependent economic systems”, Systems Engineering, Vol. 9, No. 1, pp. 20-34, January 2006.

[22] Rinaldi, S., “Modeling and simulating critical infrastructures and their interdependencies”, in Proc. of the 37th Hawaii International Conference on System Sciences, Vol. 2., USA, IEEE, 2004.

[23] Svedsen, N., Wolthunsen, S., “Connectivity models of interdependency in mixed-type critical infrastructure networks”, Information Security Technical Report, Vol. 1, pp.44-55, 2007.

[24] Min O., Liu H., Zi-Jun M., Ming-Hui Y., Fei Q., “A methodological approach to analyze vulnerability of interdependent infrastructures”, Simulation Modeling Practice and Theory, Vol. 17, pp.817-828, 2009.

[25] Nieuwenhuijs A., Luiijf E., Klaver M., “Modeling dependencies in critical infrastructures”, in Critical Infrastructure Protection, IFIP series, Vol. 253, pp. 205-214, Goetz E., Shenoi S. (Eds), Springer, 2008.

[26] Aung Z. and Watanabe. K., “A framework for modeling Interdependencies in Japan's Critical Infrastructures”, in 3rd IFIP International Conference on Critical Infrastructure Protection (CIP-2009), pp.243-257, Palmer C., Shenoi S. (Eds.) Springer, USA 2009.

ΚΕΦΑΛΑΙΟ 5: ΠΟΛΙΤΙΚΕΣ ΑΣΦΑΛΕΙΑΣ ΣΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Η πολιτική ασφάλειας αναπτύσσεται και καθορίζεται βασιζόμενη σε προκαθορισμένους κανόνες και μεθοδολογίες σε συνάρτηση με την εκάστοτε περίπτωση που έχουμε να αντιμετωπίσουμε. Εφαρμόζοντας το πρότυπο ISO-27002 στον σχεδιασμό της πολιτικής επιτυγχάνουμε την εξασφάλιση της απαιτούμενης ασφάλειας. Το πρότυπο αυτό μπορεί να εφαρμοστεί σε όλες τις επιχειρήσεις ανεξαρτήτως μεγέθους και εντάσσονται στο πλαίσιο ανάπτυξης και διοίκησης ενός αποτελεσματικού συστήματος ασφάλειας πληροφοριών.

Οι βασικές αρχές που χαρακτηρίζουν το πρότυπο ISO-27002 είναι ότι θεωρεί τις πληροφορίες ως σημαντικό περιουσιακό στοιχείο, καλύπτοντας όλες τις δυνατές μορφές τους. Με τη πλήρη συμμόρφωση της πολιτικής στις απαιτήσεις του προτύπου, στοχεύουμε στην εξασφάλιση της εμπιστευτικότητας, της ακεραιότητας, και της διαθεσιμότητας. Προκειμένου να αναπτύξουμε μία πολιτική η οποία θα είναι πλήρης και ολοκληρωμένη, θα πρέπει να ακολουθήσουμε κάποια προκαθορισμένα στάδια τα οποία εμπεριέχονται στο πρότυπο που εφαρμόζουμε. Το αρχικό στάδιο απαιτεί το διάλογο και τη συζήτηση με την επιχείρηση, και πιο συγκεκριμένα, με την διοίκηση της προκειμένου να καθοριστεί ο γενικός στόχος της πολιτικής ασφάλειας. Κρίσιμο ζήτημα είναι να υπάρξει η δέσμευση της διοίκησης για διάθεση των απαιτούμενων πόρων, υποστήριξη, αλλά και αλλαγή ή προσαρμογή της νοοτροπίας και φιλοσοφίας εργασίας ώστε να συμβάλλει δυναμικά στην τήρηση των νέων προδιαγραφών. Επίσης είναι αναγκαίο να προσδιοριστεί η έκταση εφαρμογής της πολιτικής, καθώς είναι απαραίτητο να καθοριστούν τα τμήματα ή οι δραστηριότητες στις οποίες θα γίνει η εφαρμογή, καθώς και να εξεταστούν οι διασυνδέσεις/ αλληλεπιδράσεις με άλλα συστήματα. Μέσω αυτών των διεργασιών η εταιρεία ουσιαστικά στοχεύει στην προστασία των κεφαλαίων της, την προστασία της παραγωγικής διαδικασίας, τη διαφύλαξη των εταιρικών και μη πληροφοριών και τέλος τη προστασία των πελατών και των συνεργατών με τον καλύτερο δυνατό τρόπο.

Το επόμενο βήμα μας περιλαμβάνει τον καθορισμό των πολιτικών που θα ακολουθηθούν, δηλαδή αν θα υπάρχει μία γενικευμένη πολιτική ή θα σχεδιαστούν υποπολιτικές οι οποίες θα είναι εξειδικευμένες σε ένα τομέα, και όλες μαζί με την ιεραρχία που θα οριστεί θα περιλαμβάνονται στην βασική πολιτική. Είναι αυτονόητο λοιπόν ότι για να προχωρήσουμε στον σχεδιασμό της πολιτικής θα πρέπει αρχικά να

προσδιορίσουμε τα περιουσιακά στοιχεία της εταιρείας (assets), την αξία ή τη χρησιμότητα τους, την οικονομική τους αξία και τα οφέλη τους. Τα στοιχεία που εντάσσονται στα πλαίσια του σχεδιασμού της πολιτικής μπορεί να είναι πληροφορίες, hardware, software, δίκτυα, τηλεπικοινωνίες, συστήματα επεξεργασίας και αποθήκευσης, επιχειρησιακές διαδικασίες, brand names, πνευματική περιουσία, εικόνα, φήμη και προσωπικό.

Για κάθε ένα από τα παραπάνω στοιχεία στα οποία η εταιρεία θα αποφασίσει να εφαρμόσει την πολιτική ασφάλειας, θα πρέπει να υλοποιηθεί διεξοδικός έλεγχος για να καθοριστούν τα σημεία στα οποία εντοπίζονται οι αδυναμίες και χρήζουν βελτίωσης ή απαιτούν προσαρμογή στα νέα δεδομένα. Θα πρέπει να γίνει προσδιορισμός των κινδύνων που ενέχουν, και έπειτα να αξιολογηθούν, να υπολογισθεί η πιθανότητα εμφάνισης τους και οι επιπτώσεις τους. Η πολιτική ασφάλειας που θα σχεδιαστεί θα περιλαμβάνει όλα αυτά τα στοιχεία, σε αυτοτελής "υπο-πολιτικές" έτσι ώστε να είναι εφικτή η εξειδίκευση σε κάθε θέμα αλλά και παράλληλα να είναι πιο ευέλικτες ως προς μελλοντικές αλλαγές και προσθήκες [1], [2].

5.1 Η οργανωτική ασφάλεια

Η οργανωτική ασφάλεια έχει ως σκοπό να διαχειριστεί την ασφάλεια πληροφοριών μέσα στον οργανισμό. Προαπαιτείται να εδραιωθεί ένα διοικητικό δίκτυο ώστε πρώτα να αρχικοποιήσει και στη συνέχεια να ελέγχει την εφαρμογή των πολιτικών ασφαλείας μέσα στον οργανισμό. Η διοίκηση θα πρέπει να εγκρίνει την πολιτική ασφαλείας και να αναθέσει τους ρόλους ασφαλείας στο προσωπικό. Η ασφάλεια των πληροφοριών ενός οργανισμού είναι ένα θέμα που αφορά όλους τους υπαλλήλους του, οπότε είναι σαφές ότι όλοι οι υπάλληλοι θα πρέπει να είναι ενήμεροι για την πολιτική ασφάλειας που ακολουθείται και θα πρέπει να την εφαρμόζουν με προσοχή.

Όπως προαναφέραμε, η διοίκηση θα πρέπει να υποστηρίζει ενεργά την ασφάλεια μέσα στον οργανισμό μέσω της παροχής σωστής καθοδήγησης, της δέσμευσης, της εξειδικευμένης ανάθεσης αρμοδιοτήτων, και της αναγνώριση των ευθυνών που απαιτεί η ασφάλεια πληροφοριών.

Η διοίκηση θα πρέπει:

- να διασφαλίσει ότι αναγνωρίζονται οι στόχοι της ασφαλείας πληροφοριών, να καλύπτει τις απαιτήσεις του οργανισμού, και να τις εντάσσει σε διάφορες διαδικασίες

- να αναμορφώσει, να ανασκοπήσει, και να αποδεχτεί την πολιτική ασφάλειας πληροφοριών

- να ανασκοπήσει την αποτελεσματικότητα της εφαρμογής της πολιτικής ασφαλείας

- να παρέχει καθαρή καθοδήγηση και ορατή διοικητική υποστήριξη για πρωτοβουλίες ασφαλείας

- να αποδεχτεί την ανάθεση ειδικευμένων ρόλων και υπευθυνοτήτων για την ασφάλεια πληροφοριών μέσα στον οργανισμό

- να αρχικοποιήσει τα σχέδια και τα προγράμματα που συντηρούν την επίγνωση της ασφάλειας πληροφοριών

- να διασφαλίσει ότι η εφαρμογή των ελέγχων ασφαλείας πληροφοριών είναι συντονισμένη μέσα στον οργανισμό [3].

5.2 Περιεχόμενα Πολιτικής Ασφαλείας

Το κείμενο της πολιτικής ασφαλείας θα πρέπει να περιλαμβάνει τουλάχιστον τα ακόλουθα:

•Τον ορισμό της ασφάλειας των πληροφοριών, το σκοπό της και τη σπουδαιότητά της ως μηχανισμό που επιτρέπει την ανταλλαγή πληροφοριών.

•Τους σκοπούς της διοίκησης και την υποστήριξή της αναφορικά με την ασφάλεια.

•Την επεξήγηση της πολιτικής ασφαλείας, των αρχών, των προτύπων και των απαιτήσεων που πρέπει να ικανοποιήσει η εταιρεία ή οργανισμός, όπως σχετική νομοθεσία, προστασία από ιούς, επιπτώσεις μη συμμόρφωσης με την πολιτική ασφάλειας, διαχείριση επιχειρηματικής συνέχειας κλπ.

•Τον ορισμό γενικών και ειδικών καθηκόντων για τη διαχείριση της ασφάλειας και την αναφορά συμβάντων.

•Αναφορές σε άλλα κείμενα που μπορούν να υποστηρίξουν την πολιτική ασφαλείας, όπως περιγραφές συγκεκριμένων διαδικασιών και κανονισμών.

Παρ'ότι οι πολιτικές ασφαλείας είναι γενικά υποκειμενικές και προσαρμόσιμες στις συγκεκριμένες ανάγκες και τους στόχους κάθε εταιρίας ή οργανισμού, υπάρχουν ορισμένα ζητήματα τα οποία είναι τόσο σημαντικά που θα πρέπει να αντιμετωπίζονται σε όλες τις πολιτικές ασφαλείας. Αυτά είναι [4]:

- Φυσική ασφάλεια

Το μέγεθος της δικτυακής οντότητας μιας εταιρίας μπορεί να εκτείνεται από ένα κτίριο ή κτιριακό συγκρότημα μέχρι μια χώρα ή ολόκληρο τον κόσμο. Αυτό σημαίνει ότι η ασφάλεια του δικτύου έχει άμεση συνάρτηση με τη φυσική ασφάλεια. Χωρίς την εξασφάλιση της φυσικής ασφάλειας, οι βασικές απαιτήσεις για την ασφάλεια των πληροφοριών, δηλαδή η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα θα διατρέχουν σοβαρότατο κίνδυνο. Η ενότητα της πολιτικής ασφαλείας που αφορά τη φυσική ασφάλεια δηλώνει ρητά πώς θα προστατευθούν οι εγκαταστάσεις και ο υλικός εξοπλισμός της εταιρίας. Καθορίζει, επίσης, ποιοι εργαζόμενοι έχουν δικαίωμα πρόσβασης σε απαγορευμένες περιοχές, όπως είναι τα δωμάτια των servers ή οι αποθήκες των καλωδίων.

- Ασφάλεια δικτύου

Η ενότητα της ασφάλειας δικτύου δηλώνει τον τρόπο προστασίας των στοιχείων που αποθηκεύονται στο δίκτυο. Μπορεί επίσης να περιλαμβάνει μέτρα ασφάλειας σχετικά με τις τεχνολογίες προστασίας του δικτύου, όπως είναι τα firewalls και τα intrusion detection systems (συστήματα ανίχνευσης επιθέσεων).

- Έλεγχος πρόσβασης

Η ενότητα του ελέγχου πρόσβασης καθορίζει ποιος έχει πρόσβαση σε τι. Πρέπει να υπάρχει μια κατάλληλη διαδικασία που να εξασφαλίζει ότι μόνο οι αρμόδιοι για κάθε υπηρεσία ή πηγή πληροφοριών θα έχουν πρόσβαση σε αυτή. Ο έλεγχος πρόσβασης θα πρέπει να διευκολύνει τους διαχειριστές στη δουλειά τους και να είναι σχετικά εύκολος και κατανοητός ώστε να αποφεύγονται τα λάθη.

- Πιστοποίηση

Εκφράζει τον τρόπο που οι χρήστες πιστοποιούν την ταυτότητά τους στο δίκτυο. Ο τύπος της πιστοποίησης που χρησιμοποιείται ποικίλλει ανάλογα με τον τρόπο πρόσβασης των χρηστών στο δίκτυο. Για πρόσβαση από το γραφείο τους, ένα απλό όνομα χρήστη και ένας κωδικός είναι αρκετοί αφού ο έλεγχος πιστοποίησης ενισχύεται από τη φυσική ασφάλεια. Για πρόσβαση όμως στο δίκτυο της εταιρίας μέσω του Internet μπορεί να χρειαστεί μια πιο περίπλοκη και ασφαλής πιστοποίηση.

- Συμμόρφωση

Η ενότητα της συμμόρφωσης επεξηγεί τον τρόπο εφαρμογής της πολιτικής ασφαλείας. Μπορεί επίσης να καθορίζει τις μεθόδους διερεύνησης τυχόν παραβιάσεων της πολιτικής καθώς επίσης και την επιβολή τιμών.

- Σχέδιο για την αντιμετώπιση περιστατικών και εκτάκτων αναγκών

Το σχέδιο αυτό εξηγεί τον τρόπο αντιμετώπισης κάθε είδους περιστατικού, από την επίθεση κακόβουλων χρηστών μέχρι μια φυσική καταστροφή. Μπορεί επίσης να απαριθμεί τα μέλη μιας ομάδας αντιμετώπισης έκτακτων περιστατικών που θα διαχειριστούν τέτοια περιστατικά.

- Ασφάλεια λογισμικού

Η ενότητα της ασφάλειας λογισμικού επεξηγεί τον τρόπο χρήσης του λογισμικού. Καθορίζει ποιοι έχουν το δικαίωμα να αγοράζουν και να εγκαθιστούν πακέτα λογισμικού στον υλικό εξοπλισμό της εταιρίας, καθώς επίσης και τα μέτρα ασφάλειας όσον αφορά τη λήψη λογισμικού από το Internet.

Εκτός από τα ζητήματα που αντιμετωπίζει, η πολιτική ασφαλείας έχει και κάποιες βασικές προϋποθέσεις που θα πρέπει να εκπληρώνονται ώστε να έχει το επιθυμητό αποτέλεσμα:

•Απαιτεί συμμόρφωση από το προσωπικό του οργανισμού. Το έγγραφο της πολιτικής ασφαλείας θα πρέπει να είναι στη διάθεση όλου του προσωπικού.

•Εκφράζει γενικότερες απόψεις ή αρχές του οργανισμού.

•Είναι σαφής ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της και εφαρμόσιμη από άποψη κόστους.

•Είναι γενικεύσιμη ώστε η εφαρμογή της να είναι επεκτάσιμη σε μελλοντικά συστήματα που ενδεχομένως ενταχθούν στο πληροφοριακό σύστημα του οργανισμού.

•Είναι απαλλαγμένη από μη απαραίτητους τεχνικούς όρους και εξειδικευμένες αναφορές ώστε να μην καθίσταται δύσκολη στην εφαρμογή της και εξαρτημένη από τεχνολογικές επιλογές, καθώς και να μην τροποποιείται συχνά, παρά μόνο όταν συμβαίνουν σημαντικές αλλαγές στα εξής:

-Στην οργανωτική δομή και στην κουλτούρα του οργανισμού

-Στις απαιτήσεις ασφαλείας

-Στις τεχνολογικές εξελίξεις [5]

Οι ακόλουθοι παράγοντες έχουν ιδιαίτερη σημασία στην εξασφάλιση της ασφάλειας δικτύων και πληροφοριών μέσα σε έναν οργανισμό:

•Πολιτική ασφάλειας, στόχοι και δραστηριότητες που αντικατοπτρίζουν τους στόχους του οργανισμού.

•Εφαρμογή διαδικασιών ασφάλειας με τρόπο συμβατό με την κουλτούρα του οργανισμού.

•Ενεργή υποστήριξη από τη διοίκηση του οργανισμού.

•Κατανόηση των απαιτήσεων ασφάλειας, της αποτίμησης κινδύνων και της διαχείρισής τους.

•Κατανόηση από όλο το προσωπικό του οργανισμού της αναγκαιότητας ύπαρξης και λειτουργίας μηχανισμών ασφάλειας.

•Γνώση της πολιτικής ασφάλειας από όλο το προσωπικό και από τους εξωτερικούς συνεργάτες.

•Εκπαίδευση και επιμόρφωση του προσωπικού.

•Ένα κατανοητό και ισορροπημένο σύστημα μέτρησης που να μπορεί να αξιολογήσει την απόδοση του συστήματος ασφάλειας των πληροφοριών και να προτείνει πιθανές βελτιώσεις [6].

5.3 Οδηγίες για τη σωστή εφαρμογή της πολιτικής ασφαλείας

Με στόχο την ελαχιστοποίηση των κινδύνων προσβολής του κατανεμημένου συστήματος, μέσω της δικτυακής υποδομής θα πρέπει να εφαρμοστεί μία συνεπής πολιτική ασφάλειας. Το πλαίσιο της πολιτικής αυτής διαφοροποιείται ανάλογα με την έκταση και τη λειτουργία του συστήματος. Σε περιπτώσεις εκτεταμένων συστημάτων (π.χ. δημόσια δίκτυα), όπου οι χρήστες καλύπτουν ιδιωτικές - προσωπικές ανάγκες είναι υπό αμφισβήτηση η έκταση και η φύση του διαχειριστικού ελέγχου. Προκύπτει δηλαδή το ερώτημα, αν είναι θεμιτή η παρακολούθηση των εργασιών ενός χρήστη από το διαχειριστή του δικτύου ή αν το γεγονός αυτό θεωρείται παραβίαση της ιδιωτικής του δραστηριότητας. Για να αποφύγουμε πιθανά παρόμοια προβλήματα περιορίζουμε την έκταση των συστημάτων, που εξετάζουμε, σε αυτά που καλύπτουν τις πληροφοριακές ανάγκες μίας μεγάλης επιχείρησης-οργανισμού. Οι χρήστες των συστημάτων αυτών δεσμεύονται με κάποια σύμβαση, στην οποία θα πρέπει να καταγράφονται οι πληροφοριακές απαιτήσεις και το επιτρεπτό επίπεδο πρόσβασης για την εκτέλεση της καθημερινής εργασίας τους. Τα συστήματα αυτά υποστηρίζονται επικοινωνιακά από τοπικά, μητροπολιτικά και δημόσια δίκτυα περιορισμένης όμως πρόσβασης. Η πολιτική ασφάλειας, που θα πρέπει να εφαρμόζεται στις περιπτώσεις αυτές θα πρέπει να περιέχει τις ακόλουθες βασικές οδηγίες:

•Η πρόσβαση στις επικοινωνιακές υπηρεσίες περιορίζεται σε συγκεκριμένες οντότητες (χρήστες, διαδικασίες, διεργασίες) και για καθορισμένο χρονικό διάστημα. Κάθε λειτουργία, που έχει τη δυνατότητα να εκτελεστεί τοπικά, δε θα επιτρέπεται να χρησιμοποιεί απομακρυσμένους πόρους.

•Οι διαθέσιμες διαδικασίες ταυτοποίησης και εξακρίβωσης γνησιότητας θα πρέπει να ελέγχουν όλες τις οντότητες, που χρησιμοποιούν την επικοινωνιακή υποδομή. Για την εξακρίβωση της ορθότητας των μηνυμάτων είναι χρήσιμη η μέθοδος των ψηφιακών υπογραφών. Ειδικά κατά τη διάρκεια πρόσβασης σε κρίσιμους πόρους του συστήματος (π.χ. εξυπηρετητές), θα πρέπει οι διαδικασίες ταυτοποίησης και εξακρίβωσης γνησιότητας να είναι διπλές.

•Κάθε πρόσβαση στο δίκτυο θα πρέπει να καταγράφεται (ημερομηνία, ώρα, κόμβος, χρήστης, εφαρμογή, διάρκεια, αρχεία και συσκευές πρόσβασης). Η λειτουργία κατάλληλων εφαρμογών παρακολούθησης και καταγραφής των επικοινωνιακών δραστηριοτήτων και του προκαλούμενου φόρτου είναι αναγκαία, καθώς και η επισήμανση καταστάσεων συναγερμού σε πραγματικό χρόνο.

•Τα συνθηματικά των χρηστών των επικοινωνιακών υπηρεσιών θα πρέπει να αλλάζουν σε τακτικά χρονικά διαστήματα.

•Βελτιστοποιημένες μέθοδοι κρυπτογράφησης θα πρέπει να χρησιμοποιούνται για την αποφυγή διαρροής πληροφοριών. Θα πρέπει να τονιστεί ότι στην περίπτωση που δεν εφαρμόζονται κρυπτογραφικές μέθοδοι σε όλα τα μηνύματα, θα πρέπει να εφαρμόζονται τουλάχιστο στα μηνύματα, που μεταφέρουν ταυτότητες και συνθηματικά. Είναι γνωστό ότι η πλειοψηφία των εφαρμογών υπηρεσιών δικτύου (rlogin, ftp, κλπ) μεταφέρουν αυτούσια τις ταυτότητες - συνθηματικά μέσω δικτύου σε μορφή κειμένου. Το ίδιο ισχύει και στις εφαρμογές πρόσβασης βάσεων δεδομένων, που λειτουργούν σύμφωνα με το μοντέλο πελάτη-εξυπηρετητή, καθώς και στις κατανεμημένες βάσεις δεδομένων. Κάθε χρήστης, συνεπώς, που έχει δυνατότητα πρόσβασης στις εφαρμογές παρακολούθησης του δικτύου ή έχει γνώσεις προγραμματισμού κατανεμημένων εφαρμογών (RPC), είναι δυνατό να υποκλέψει σταδιακά τα μεταφερόμενα συνθηματικά.

•Στις περιπτώσεις συνεχών αποτυχημένων προσπαθειών πρόσβασης θα πρέπει να απενεργοποιείται η μέθοδος πρόσβασης (πχ getty-login στο Unix) και να ειδοποιείται ο διαχειριστής του συστήματος, κρατώντας παράλληλα την ταυτότητα με την οποία επιχειρήθηκε η πρόσβαση. Σαν εναλλακτική τακτική προτείνεται η εισαγωγή του εισβολέα σε φαινομενικό περιβάλλον-κέλυφος (μετά από συνεχή εισαγωγή λανθασμένων συνθηματικών) με παράλληλη ενεργοποίηση διαδικασιών συναγερμού του διαχειριστή. Με τη μέθοδο αυτή είναι δυνατός ο φυσικός εντοπισμός του εισβολέα.

• Παράλληλα με τα μέτρα ασφάλειας του συστήματος από τους χρήστες, θα πρέπει να διασφαλίζονται και οι χρήστες έναντι του συστήματος. Συγκεκριμένα, όπως ο χρήστες ταυτοποιούνται στο σύστημα με τον ίδιο τρόπο το σύστημα θα πρέπει να ταυτοποιείται στον χρήστη. Συνηθισμένη πρακτική των εισβολέων είναι η δημιουργία προγραμμάτων ταυτοποίησης παρόμοια με αυτά των λειτουργικών-δικτυακών

συστημάτων με στόχο την υφαρπαγή των συνθηματικών, κατά τη διαδικασία καταχώρησης τους από τους τελικούς χρήστες.

•Θα πρέπει να μελετηθεί στατιστικά οι κυκλοφορία, που εισάγει στο δίκτυο κάθε χρήστης. Με τον τρόπο αυτό θα είναι δυνατός ο εντοπισμός του υπερβολικού κυκλοφοριακού φόρτου, τον οποίο προκαλούν οι εισβολείς, με τελικό σκοπό τη δημιουργία καθυστερήσεων και την πιθανή πλήρη κατάρρευση του δικτύου.

•Θα πρέπει να υπάρχουν διπλές διαδικασίες επιβεβαίωσης (από δύο τουλάχιστον διαχειριστές), για κάθε ζωτική αλλαγή της σύνθεσης (νέος κόμβος, νέοι χρήστες, διαδικασίες συντήρησης), καθώς και για τις διαδικασίες παρακολούθησης (monitoring) του συστήματος. Σε κάθε εγκατάσταση νέου κόμβου, νέου λογισμικού θα πρέπει να αλλάζουν τα συνθηματικά που δίδονται από τις κατασκευάστριες εταιρίες, τα οποία συνήθως καλύπτουν βασικές λειτουργίες των συστατικών αυτών του κατανεμημένου συστήματος (εγκατάσταση, συντήρηση).

•Σταθμοί εργασίας χωρίς δισκέτες ή σκληρούς δίσκους θα πρέπει να χρησιμοποιούνται όπου είναι δυνατόν. Με τη μέθοδο αυτή θα αποφεύγεται η εισαγωγή προγραμμάτων ιών και η ανεπιθύμητη αντιγραφή μηνυμάτων-πληροφοριών. Οι διαδικασίες εκκίνησης των συστημάτων (boot) αυτών θα ενεργοποιούνται από μνήμες EPROM ή από απομακρυσμένους κόμβους (remote boot).

•Όλα τα ενεργά συστατικά του δικτύου (κόμβοι, εξυπηρετητές, συσκευές διαδικτύωσης, συγκεντρωτές, επαναλήπτες), θα πρέπει να είναι φυσικά προστατευμένα. Σε εκτεταμένες εγκαταστάσεις είναι αναγκαία η προστασία των συσκευών, οι οποίες δεν ελέγχονται από απομακρυσμένους κόμβους. Τέτοιες συσκευές είναι οι παθητικοί επαναλήπτες χωρίς υποστήριξη SNMP πρωτοκόλλου, καθώς και οι εξυπηρετητές 'κουτών' τερματικών (terminal servers).

•Οι καλωδιώσεις πρέπει να διασχίζουν χώρους μη προσβάσιμους από το κοινό και να ευρίσκονται σε μεταλλικές σωληνώσεις. Τα κιβώτια διακλαδώσεων θα πρέπει να προστατεύονται από κλειδαριές. Η χρήση οπτικών ινών συστήνεται λόγω δυσκολίας στη διακλάδωσή τους, καθώς επίσης και η ύπαρξη εναλλακτικών καλωδιώσεων - διαδρομών με αυτόματη ενεργοποίηση των εφεδρικών φυσικών διαδρομών.

•Συνίσταται να αποφεύγεται η χρήση δημοσίων δικτύων. Αν αυτό δεν είναι δυνατόν θα πρέπει να χρησιμοποιούνται αποκλειστικές γραμμές και να δεσμεύεται ο τηλεπικοινωνιακός οργανισμός, με κατάλληλη σύμβαση, σχετικά με πιθανή εισβολή με δική του υπαιτιότητα.

Οι οδηγίες, που αναφέραμε, αφορούν την προστασία της δικτυακής υποδομής από πιθανές εισβολές. Για την πλήρη διαθεσιμότητα και σωστή λειτουργία του συστήματος θα πρέπει να ληφθούν επιπρόσθετα μέτρα [7].

5.4 Οι πολιτικές ασφαλείας στο στρατιωτικό περιβάλλον

Η ανάπτυξη της επιστήμης της Πληροφορικής σε συνδυασμό με την ελευθερία που χαρακτηρίζει την πρόσβαση οποιουδήποτε ατόμου στη συγκεκριμένη γνώση, εκτός των αδιαμφισβήτητων ευεργετικών επιτευγμάτων για την ανθρωπότητα, κατέστησε δυνατή και την εκτέλεση ενός ευρέως φάσματος εγκληματικών ενεργειών από κακόβουλους χρήστες, οι οποίοι διαθέτουν την απαιτούμενη εξειδίκευση και τεχνική κατάρτιση. Συνεπακόλουθα, ορισμένα από τα πλέον διαδεδομένα εγκλήματα διαπράττονται πια υπό τη μορφή «κυβερνο-εγκλημάτων», με τους δράστες να εκμεταλλεύονται τα χαρακτηριστικά του νέου χώρου δράσης για να αποφύγουν τον εντοπισμό και τη σύλληψή τους. Η έξαρση του νέου τύπου εγκληματικότητας και οι καταστροφικές συνέπειες που μπορεί να έχει σε κάθε επίπεδο, από κυβερνητικό-εταιρικό έως προσωπικό, καθιστά την αντιμετώπισή της εξαιρετικής σημασίας. Αυτός είναι και ο λόγος που ο τομέας της Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας γνωρίζει αντίστοιχη ανάπτυξη με το Κυβερνοέγκλημα.

Το προσωπικό το οποίο επιφορτίζεται με τα καθήκοντα της αντιμετώπισης και διερεύνησης των περιστατικών ασφαλείας, προβαίνει σε ενέργειες αναγνώρισης, συλλογής, εξέτασης και ανάλυσης των κατάλληλων αποδεικτικών στοιχείων, τα οποία εν τέλει θα χρησιμοποιηθούν σε δικαστικές ή εσωτερικές πειθαρχικές διαδικασίες. Οι ενέργειες αυτές είναι ιδιαίτερα πολύπλοκες και επίπονες, ενώ κατά τη διάρκεια υλοποίησής τους οι ερευνητές θα βρεθούν αντιμέτωποι και με προβληματισμούς νομικής φύσεως. Αυτοί συνήθως αφορούν στην εγκυρότητα των ψηφιακών πειστηρίων που συλλέχθηκαν και στην ιδιωτικότητα των χρηστών των Πληροφοριακών Συστημάτων που ελέγχθηκαν. Για να εξασφαλισθεί η αξιοπιστία των μεθόδων συλλογής και ανάλυσης των δεδομένων, η αποδοχή των πειστηρίων από τις δικαστικές λειτουργίες καθώς και για να αποφευχθεί τυχόν παραβίαση του

δικαιώματος οποιοδήποτε χρήστη στην ιδιωτικότητα, το προσωπικό που διεξάγει τις έρευνες θα πρέπει να λειτουργεί εντός των καθορισμένων εθνικών νομικών πλαισίων και σύμφωνα με τις πολιτικές ασφαλείας που ισχύουν σε κάθε περιβάλλον, οι οποίες διευκρινίζουν περαιτέρω τα συγκεκριμένα θέματα.

Πέραν των όσων προβλέπονται από την ισχύουσα νομοθεσία μιας χώρας και αφορούν στην προστασία και διακίνηση όλων των τύπων πληροφοριών, ένας Οργανισμός οφείλει να προχωρήσει στη σύνταξη των ιδιαίτερων, για το περιβάλλον του, Πολιτικών Ασφαλείας Πληροφοριών ώστε να καθορίσει περισσότερες λεπτομέρειες σχετικά με το πώς θα προσπαθήσει να επιτύχει το μεγαλύτερο δυνατό επίπεδο ασφάλειας. Όταν η πολιτική ασφαλείας εξειδικεύεται σε θέματα που αφορούν στην ασφάλεια των πληροφοριών που διακινούνται στα Πληροφοριακά Συστήματα του Οργανισμού, τότε αντίστοιχα προκύπτει μια Πολιτική Ασφαλείας Πληροφοριακών Συστημάτων, η οποία συμπληρώνει την Πολιτική Ασφαλείας Πληροφοριών [8].

Στο ελληνικό στρατιωτικό περιβάλλον, η ασφάλεια των πληροφοριών που διακινούνται στα Πληροφοριακά Συστήματα των Ενόπλων Δυνάμεων περιγράφεται τόσο στον Εθνικό Κανονισμό Ασφαλείας (Ε.Κ.Α.), ο οποίος αποτελεί την Εθνική Πολιτική Ασφαλείας, όσο και στον Στρατιωτικό Κανονισμό (Σ.Κ.) 80-20 «Κανονισμός Ασφαλείας Πληροφοριακών Συστημάτων», ο οποίος ουσιαστικά αποτελεί την Πολιτική Ασφαλείας Πληροφοριακών Συστημάτων του Στρατού Ξηράς. Επίσης, τα τελευταία χρόνια, οι κεντρικές υποδομές Πληροφορικής Υποστήριξης του Ελληνικού Στρατού έχουν πιστοποιηθεί κατά ISO 27001:2013 για τη λειτουργία Σύστηματος Διαχείρισης Ασφάλειας Πληροφοριών (Σ.Δ.Α.Π.) σύμφωνα με τα όσα ορίζει τα συγκεκριμένο πρότυπο. Τόσο στα αναγραφόμενα στο Σ.Δ.Α.Π. όσο και στα άρθρα των δύο συγγραμμάτων περιέχονται διατάξεις που άπτονται των θεμάτων της Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, καθορίζοντας μεταξύ άλλων τον αποδεκτό τρόπο χρήσης των υπηρεσιακών Πληροφοριακών Συστημάτων και τα δικαιώματα των χρηστών καθώς και την υποχρέωση του αρμόδιου προσωπικού για έλεγχο των παρεχόμενων πόρων στις περιπτώσεις εμφάνισης οποιουδήποτε περιστατικού ασφαλείας. Για την πλήρη περιγραφή της λειτουργίας των δυνατοτήτων Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, εφόσον προχωρήσει η υλοποίησή τους στο στρατιωτικό περιβάλλον, θα απαιτηθεί η σύνταξη ιδιαίτερης αντίστοιχης

πολιτικής η οποία θα καθορίζει όλες τις απαραίτητες λεπτομέρειες. Στη συνέχεια της ενότητας παρατίθενται τα άρθρα των υφιστάμενων πολιτικών που αναφέρονται στα παραπάνω θέματα [9], [10].

5.4.1 Εθνικός Κανονισμός Ασφαλείας

Ο Εθνικός Κανονισμός Ασφαλείας αποτελεί την Εθνική Πολιτική Ασφαλείας. Στο δεύτερο μέρος του, περιλαμβάνει διατάξεις που αφορούν στα τεχνικά και διαδικαστικά μέτρα ασφαλείας, τα οποία θα πρέπει να εφαρμόζονται και να ισχύουν για όλα τα εθνικά συστήματα και δίκτυα τα οποία διαχειρίζονται διαβαθμισμένες πληροφορίες. Αρκετές από τις διατάξεις του σχετίζονται τις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας. Οι κυριότερες είναι:

- Άρθρο 51: Στην παράγραφο 1 αναφέρεται ότι «Η αυτόματη ή χειρόγραφη καταγραφή ενεργειών διατηρείται ως ημερολόγιο πρόσβασης στις διαβαθμισμένες πληροφορίες». Τα αρχεία αυτόματης καταγραφής ενεργειών των χρηστών (log files) αποτελούν από τις σημαντικότερες πηγές πληροφοριών κατά τις διαδικασίες Ψηφιακής Εγκληματολογίας.

- Άρθρο 52: Στην παράγραφο 1 δηλώνεται η υποχρέωση ελέγχου όλων των μετακινούμενων μέσων αποθήκευσης διαβαθμισμένων πληροφοριών. Συγκεκριμένα αναφέρεται ότι «Όλα τα μέσα αποθήκευσης που είναι δυνατόν να αφαιρεθούν (π.χ. σκληρός δίσκος, οπτικός δίσκος, μαγνητική ταινία, δισκέτα, κλπ.), όπου πρόκειται να αποθηκευτούν διαβαθμισμένες πληροφορίες, αναγνωρίζονται, σημαίνονται και ελέγχονται κατάλληλα. Η αναγνώριση και οι έλεγχοι περιλαμβάνουν τουλάχιστον τα εξής:» και συνεχίζοντας στην υποπαράγραφο 1γ «Περιοδικούς δειγματοληπτικούς ελέγχους και συγκέντρωση των μετακινούμενων μέσων αποθήκευσης για να εξασφαλίζεται η συμμόρφωση με τις υπάρχουσες διαδικασίες αναγνώρισης και ελέγχου. Όλα τα μετακινούμενα μέσα αποθήκευσης συγκεντρώνονται και ελέγχονται τουλάχιστον σε ετήσια βάση από τις αρμόδιες αρχές ασφαλείας». Πέραν των προγραμματισμένων περιοδικών ελέγχων, γίνεται αντιληπτό ότι κατά τη διάρκεια εμφάνισης ενός περιστατικού ασφαλείας τα υπηρεσιακά μετακινούμενα μέσα αποθήκευσης που συνδέθηκαν με το προσβληθέν σύστημα αποτελούν αντικείμενα έκτακτου ελέγχου.

• Άρθρο 59: Το συγκεκριμένο άρθρο περί «Ελέγχου για την παρουσία επιβλαβούς λογισμικού – ιών υπολογιστών» στην παράγραφο 1 αναφέρει ότι «Ο έλεγχος για την παρουσία επιβλαβούς λογισμικού και ιών υπολογιστών διεξάγεται σύμφωνα με τα αιτήματα της Εθνικής Αρχής Διαπίστευσης Ασφαλείας (Ε.Α.Δ.Α.)», ορίζοντας την αρμόδια αρχή η οποία θα αιτηθεί τον ανάλογο έλεγχο ενός συστήματος από το εξειδικευμένο προσωπικό, σε περίπτωση υποψίας ή ανίχνευσης ενός περιστατικού ασφαλείας. Επίσης, στην παράγραφο 2 περιγράφεται η υποχρέωση κατά την οποία «...περιοδικοί έλεγχοι πρέπει να γίνονται στο εγκατεστημένο λογισμικό. Οι έλεγχοι αυτοί πρέπει να γίνονται συχνότερα, εάν το Σύστημα Επικοινωνιών Πληροφορικής (ΣΕΠ) συνδέεται με άλλο ΣΕΠ ή εάν συνδέεται με δίκτυο διαβίβασης δεδομένων».

• Άρθρο 65: Το συγκεκριμένο άρθρο εντάσσει σε παρόμοιουςελέγχους με αυτούς που αναφέρθηκαν στο άρθρο 52 για τα μετακινούμεναμέσα αποθήκευσης και τους μικροϋπολογιστές, αναφέροντας ότι «Οι μικροϋπολογιστές με ενσωματωμένους σκληρούς δίσκους (ή άλλα μέσα αποθήκευσης σταθερής μνήμης), που λειτουργούν είτε ανεξάρτητα είτε σε δίκτυο και τα φορητά μηχανήματα (για παράδειγμα φορητοί υπολογιστές και ηλεκτρονικά βοηθήματα) με ενσωματωμένους δίσκους, θεωρούνται ως μέσα αποθήκευσης πληροφοριών με την ίδια έννοια όπως οι δισκέτες ή άλλα μετακινούμενα μέσα αποθήκευσης υπολογιστών».

• Άρθρο 66: «Απαγορεύεται η χρήση ιδιωτικών μέσων αποθήκευσης υπολογιστών, λογισμικού και υλικού ΣΕΠ (για παράδειγμα μικροϋπολογιστές και φορητά μηχανήματα) για αποθήκευση, επεξεργασία και διαβίβαση διαβαθμισμένων πληροφοριών». Με το παραπάνω άρθρο απαγορεύεται η χρήση οποιουδήποτε προσωπικού εξοπλισμού Πληροφορικής από τους χρήστες για την εκτέλεση των καθηκόντων που σχετίζονται με την μεταχείριση διαβαθμισμένων πληροφοριών. Με αυτόν τον τρόπο θωρακίζεται και διευκολύνεται το έργο του προσωπικού Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας, αφού οι υπηρεσιακοί πόροι αποτελούν περιουσία της εκάστοτε υπηρεσίας, παρέχονται για την εκτέλεση συγκεκριμένης υπηρεσιακής εργασίας και υπόκεινται στους άμεσους ελέγχους αυτής από το εξειδικευμένο προσωπικό.

5.4.2 Στρατιωτικός Κανονισμός 80-20

Ο Στρατιωτικός Κανονισμός (Σ.Κ.) 80-20 με τίτλο «Κανονισμός Ασφαλείας Πληροφοριακών Συστημάτων», καθορίζει τις αρχές και τη Πολιτική Ασφαλείας Πληροφοριακών Συστημάτων του Στρατού Ξηράς και περιγράφει τις βασικές υποχρεώσεις ασφαλείας που έχει το προσωπικό το οποίο χρησιμοποιεί μέσα πληροφορικής αλλά και γενικότερα όσοι επεξεργάζονται στρατιωτικά δεδομένα και πληροφορίες με αξιοποίηση της τεχνολογίας των πληροφοριών. Ο κανονισμός αυτός συμπληρώνει τον Ε.Κ.Α. στα εξειδικευμένα θέματα της ασφάλειας Πληροφοριακών Συστημάτων και οι χρήστες θα πρέπει υποχρεωτικά να λαμβάνουν γνώση των διατάξεών του. Παρά το γεγονός ότι πραγματεύεται σε γενικότερο πλαίσιο τα θέματα ασφαλείας, αρκετές από τις παραγράφους του σχετίζονται άμεσα με τις δυνατότητες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας και θα αποτελέσουν τα συνδετικά σημεία στην περίπτωση δημιουργίας ξεχωριστής πολιτικής για τον εν λόγω τομέα. Παρακάτω γίνεται αναφορά σε μερικές από τις παραγράφους που προσεγγίζουν τα θέματα ενδιαφέροντος:

- Παράγραφος 14: Στη συγκεκριμένη παράγραφο περιγράφονται οι ειδικές απαιτήσεις τις οποίες πρέπει να πληρούν τα στρατιωτικά επιχειρησιακά Πληροφοριακά Συστήματα. Ειδικότερα, στην πρώτη υποπαράγραφο αναλύεται η απαίτηση για επιβιωσιμότητα, δηλαδή «η δυνατότητα ενός συστήματος να λειτουργεί ικανοποιητικά και με προκαθορισμένα επίπεδα απόδοσης σε περιπτώσεις εχθρικών πράξεων, καταστροφών ή οποιασδήποτε άλλης μορφής αστοχιών και ανθρωπίνων σφαλμάτων». Το χαρακτηριστικό αυτό βρίσκεται σε άμεση σχέση με τους στόχους Επιχειρησιακής Συνέχειας των διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας. Επιπρόσθετα, στα ενδεικνυόμενα μέτρα για την εξασφάλιση της επιβιωσιμότητας αναφέρεται και η «δυνατότητα απόκρουσης επιθέσεων άρνησης παροχής υπηρεσιών στα πλαίσια εχθρικών επιχειρήσεων Κυβερνοπολέμου», η οποία επίσης εντάσσεται στα καθήκοντα της Ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας.

- Παράγραφος 15: Στις αρμοδιότητες και υποχρεώσεις των χρηστών για την ασφάλεια των Πληροφοριακών Συστημάτων περιλαμβάνονται «…η υποχρέωση και ευθύνη να συμβάλλουν στην επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων Πληροφορικής και να αναφέρουν οποιοδήποτε γεγονός υποπέσει στην αντίληψή τους

που μπορεί να οδηγήσει σε παραβίαση της ασφάλειας του συστήματος» καθώς και «…η επαγρύπνηση για τον εντοπισμό πιθανής προσπάθειας μη εξουσιοδοτημένης πρόσβασης, στο τμήμα του συστήματος που εργάζονται (αρχεία, προγράμματα κ.α.) και η αναφορά σχετικά». Πρόκειται για ορισμένους από τους τρόπους με τους οποίους πραγματοποιείται το στάδιο της Ανίχνευσης Περιστατικών σε ένα μοντέλο διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας. Για να εκμεταλλευθούν στο έπακρο οι υποχρεώσεις των χρηστών, στην ιδιαίτερη πολιτική που θα συνταχθεί θα πρέπει να καθοριστεί ο ακριβής τρόπος και οι αναγκαίες πληροφορίες οι οποίες θα πρέπει να αναφέρονται άμεσα στο αρμόδιο προσωπικό, ώστε να προσδιορισθεί όσον το δυνατόν καλύτερα το περιστατικό και να ξεκινήσουν οι προβλεπόμενες ενέργειες αντιμετώπισής του.

- Παράγραφος 16: Όσον αφορά στην υπευθυνότητα σχετικά με την πρόσβαση στις πληροφορίες, ο Σ.Κ. 80-20 ορίζει ότι «Όλα τα δεδομένα του συστήματος ανήκουν στη δικαιοδοσία της Υπηρεσίας η οποία και ευθύνεται, δια των οργάνων ασφαλείας, για την προστασία των διαβαθμισμένων πληροφοριών» και ότι «Υπεύθυνος για το σύνολο των δεδομένων του συστήματος είναι ο Διευθυντής ή Διοικητής, ο οποίος έχει και την ευθύνη ασφαλείας των πληροφοριών που απορρέουν από την επεξεργασία τους». Από τα παραπάνω συμπεραίνεται ότι ο επικεφαλής ενός Οργανισμού ή Υπηρεσίας έχει τη συνολική ευθύνη για τις πληροφορίες που διακινούνται στα Πληροφοριακά Συστήματα και πρέπει να ενεργεί ανάλογα όταν υποπτεύεται ή διαπιστώνει περιστατικά ασφαλείας. Οι διακινούμενες πληροφορίες χαρακτηρίζονται ως ιδιοκτησία της Υπηρεσίας και όχι προσωπικά δεδομένα ενός συγκεκριμένου χρήστη, οπότε μπορούν να συλλεχθούν και να αναλυθούν από το εξειδικευμένο προσωπικό στα πλαίσια των ερευνών ενός περιστατικού ασφαλείας, κατόπιν αιτήσεως του έχοντος την ευθύνη ασφαλείας τους.

- Παράγραφος 18: Η πολιτική ασφαλείας, με τη συγκεκριμένη παράγραφο, επιβάλλει την υποχρέωση ύπαρξης Σχεδίου Επαναλειτουργίας για κάθε σύστημα ξεχωριστά. Το παραπάνω σχέδιο δύναται να αποτελεί επιμέρους τμήμα του γενικότερου Σχεδίου Επιχειρησιακής Συνέχειας ενός Οργανισμού, το οποίο με τη σειρά του αποτελεί εργαλείο για την υλοποίηση ενός εκ των πρωταρχικών στόχων της Αντιμετώπισης Περιστατικών Ασφαλείας που αφορά στην άμεση αποκατάσταση της λειτουργίας των συστημάτων. Συγκεκριμένα, στην πολιτική αναφέρεται ότι «Επιβάλλεται η ύπαρξη Σχεδίου Επαναλειτουργίας του Συστήματος σε περιπτώσεις

που αυτό ή κάποιο μέρος του σταματήσει να λειτουργεί…» και ότι πρέπει απαραίτητα να προηγηθεί «Αναγνώριση των πιθανότερων αιτιών μερικής ή ολικής κατάρρευσης του συστήματος. Απαιτείται συγκεκριμένη ανάλυση και προσδιορισμός των αποτελεσμάτων της κάθε αιτίας ξεχωριστά», ενέργειες που προβλέπονται στο στάδιο Αρχικής Αντιμετώπισης ενός μοντέλου διαδικασιών Αντιμετώπισης Περιστατικών Ασφαλείας.

- Παράγραφος 19: Ανάμεσα στα μέτρα για την ασφάλεια των προσωπικών υπολογιστών, και σε συνέχεια των όσων αναφέρθηκαν στην παράγραφο 16, αναφέρεται η «Απαγόρευση σύνδεσης σε προσωπικούς υπολογιστές μη εγκεκριμένου υλικού. Ιδιαιτέρως σημαντική είναι η αποτροπή σύνδεσης σε προσωπικούς υπολογιστές κινητών τηλεφώνων, έξυπνων τηλεφώνων, συσκευών αναπαραγωγής μουσικής κλπ. καθώς διαθέτουν αποθηκευτικούς χώρους μεγάλης χωρητικότητας και μπορούν να μεταφέρουν εκούσια ή ακούσια το μεγαλύτερο μέρος των διαθέσιμων δεδομένων ενός προσωπικού υπολογιστή». Το συγκεκριμένο μέτρο είναι ιδιαιτέρως σημαντικό καθώς, όπως αναφέρθηκε, τα δεδομένα που διακινούνται στα στρατιωτικά Πληροφοριακά Συστήματα αποτελούν ιδιοκτησία της Υπηρεσίας και υπεύθυνος για τις πληροφορίες ο Διοικητής ή Διευθυντής της. Στην περίπτωση κατά την οποία μεταφερθούν υπηρεσιακά δεδομένα σε μια συσκευή προσωπικής ιδιοκτησίας ενός χρήστη, οι διαδικασίες Ψηφιακής Εγκληματολογίας που θα πραγματοποιηθούν στα πλαίσια της έρευνας ενός περιστατικού διαρροής πληροφοριών είναι πιθανό να συναντήσουν εμπόδια νομικής φύσεως σχετικά με την προστασία των προσωπικών δεδομένων του χρήστη.

- Παράγραφος 80: Παρά το γεγονός ότι η υποχρέωση τήρησης αναλυτικών αρχείων καταγραφής (log files) τονίζεται σε πολλά σημεία τόσο της παρούσας πολιτικής ασφαλείας όσο και του Ε.Κ.Α., στη συγκεκριμένη παράγραφο, η οποία περιλαμβάνεται στις Βασικές Οδηγίες Ασφαλείας, περιγράφεται αναλυτικά η υποχρέωση στο σύνολό της, αναφέροντας ότι «Στο σύστημα θα πρέπει να τηρούνται αρχεία που να καταγράφουν κάθε συμβάν σχετικό με την ασφάλεια του συστήματος. Τα αρχεία αυτά θα πρέπει να φυλάσσονται για συγκεκριμένο χρονικό διάστημα, ώστε να είναι δυνατή η αξιοποίησή τους σε ενδεχόμενες έρευνες. Θα πρέπει να περιλαμβάνουν την ταυτότητα των χρηστών, τον ακριβή χρόνο σύνδεσης και αποσύνδεσης των χρηστών, το τερματικό το οποίο χρησιμοποίησε ο χρήστης και τις επιτυχείς και ανεπιτυχείς προσπάθειες του χρήστη να προσπελάσει το σύστημα ή

δεδομένα του συστήματος. Κάποια από τα αρχεία που τηρούνται στο σύστημα είναι δυνατό να διατηρούνται για μεγαλύτερα χρονικά διαστήματα, σύμφωνα με τις ανάγκες τις Υπηρεσίας ή τη σχετική νομοθεσία». Η εφαρμογή της οδηγίας έχει σαν αποτέλεσμα την ύπαρξη μιας σημαντικής πηγής πληροφοριών για τις έρευνες σχετικά με ένα περιστατικό ασφαλείας, ενώ παράλληλα αποτελεί νομική υποχρέωση του Οργανισμού αλλά και σημείο επιθεώρησης κατά της διαδικασίες πιστοποίησης και διαπίστευσής του [11], [12].

5.4.3 Διαχείριση Ασφαλείας Ελληνικού Στρατού

Στην τεκμηρίωση του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Σ.Δ.Α.Π.) του Ε.Σ., περιλαμβάνονται αρκετές διατάξεις οι οποίες αναφέρονται σε θέματα που βρίσκονται σε άμεση σχέση με τις διαδικασίες Αντιμετώπισης Περιστατικών Ασφαλείας και Ψηφιακής Εγκληματολογίας. Ειδικότερα, σε ότι αφορά στην ενημέρωση των τελικών χρηστών, οι οποίοι αποτελούν και τη σημαντικότερη παράμετρο για την ασφάλεια ενός Πληροφοριακού Συστήματος, σχετικά με τον τρόπο χρήσης των υπηρεσιακών πόρων αλλά και των υποχρεώσεων και δικαιωμάτων τους, το Σ.Δ.Α.Π. προβλέπει τη συμπλήρωση ειδικού εντύπου αίτησης για τη χορήγηση δικαιωμάτων πρόσβασης στα Πληροφοριακά Συστήματα αλλά και την εμφάνιση ειδικού προειδοποιητικού μηνύματος (warning banner) κατά την έναρξη λειτουργίας ενός συστήματος.

Με το έντυπο αίτησης εισόδου στα υπηρεσιακά Πληροφοριακά Συστήματα επιτυγχάνεται η ταχεία και περιληπτική ενημέρωση κάθε νέου χρήστη σχετικά με τις διατάξεις του Ε.Κ.Α. και του Σ.Κ. 80-20, οι οποίες αφορούν στις υποχρεώσεις των τελικών χρηστών και αναγράφονται υπό την μορφή όρων παροχής πρόσβασης στη συγκεκριμένη αίτηση. Για να χορηγηθεί άδεια πρόσβασης σε ένα χρήστη, μεταξύ άλλων ενημερώνεται ότι:

- Αποτελεί υποχρέωσή του να συμβάλλει στην επίτευξη υψηλού επιπέδου ασφάλειας των υπηρεσιακών Πληροφοριακών Συστημάτων.

- Οφείλει να αναφέρει άμεσα οποιοδήποτε γεγονός υποπέσει στην αντίληψή του και το οποίο μπορεί να οδηγήσει σε παραβίαση της ασφάλειας των συστημάτων.

- Είναι υπεύθυνος για την αποκλειστική χρησιμοποίηση των Η/Υ για υπηρεσιακή χρήση και ότι τα αρχεία που δημιουργεί στα συστήματα Πληροφορικής στης Υπηρεσίας παραμένουν στην ιδιοκτησία της.

- Η αποθήκευση εγγράφων προσωπικού ενδιαφέροντος δεν επιτρέπεται στους υπηρεσιακούς Η/Υ.

- Κάθε προσπάθεια παραβίασης της ασφάλειας των Πληροφοριακών Συστημάτων ή πρόσβασης σε μη επιτρεπόμενη περιοχή αρχείων καταγράφεται από τα συστήματα ασφαλείας του δικτύου και της εκάστοτε εφαρμογής.

- Δεν επιτρέπεται η χρησιμοποίηση προσωπικών μέσων αποθήκευσης ή προσωπικών Η/Υ.

- Οφείλει να εξασφαλίζει ότι οι ενέργειές του δεν διακυβεύουν την ασφάλεια των συστημάτων Πληροφορικής και να δέχεται τους προγραμματισμένους ή αιφνιδιαστικούς ελέγχους από το εξουσιοδοτημένο προσωπικό ασφαλείας στους Η/Υ που χρησιμοποιεί.

Τα ειδικά προειδοποιητικά μηνύματα (warning banners) κατά την έναρξη λειτουργίας ενός συστήματος, αποτελούν ακόμα ένα μέτρο ώστε να υπενθυμίζονται οι υποχρεώσεις που αναλαμβάνουν οι χρήστες κάθε φορά που πρόκειται να χρησιμοποιήσουν τα υπηρεσιακά συστήματα καθώς και το δικαίωμα της Υπηρεσίας να εκτελεί, μέσω του κατάλληλου προσωπικού, τους αναγκαίους ελέγχους ασφαλείας [9], [10].

Βιβλιογραφία-Αναφορές:

[1] Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology Gary Stoneburner, Alice Goguen, and Alexis Feringa

[2] European Network and Information Security Agency http://www.enisa.europa.eu

[3] Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών http://www.adae.gr

[4] v. Security of the Internet, Carnegie Mellon Software Engineering Institute, CERT Coordination Center

[5] Σωκράτης Κάτσικας & Δημήτρης Γκρίτζαλης & Στέφανος Γκρίτζαλης, Ασφάλεια πληροφοριακών συστημάτων, 2004

[6] Computer Networking: A top Down Approach 4th edition, K.W.Ross & J.F.Kurose, 2008

[7] Κοκολάκης Σ., "Ανάπτυξη και Διαχείριση Ασφάλειας Πληροφοριακών Συστημάτων"

[8] Joseph Migga Kizza, A Guide to Computer Network Security, Spinger-Verlag, London 2009.

[9] Γενικό Επιτελείο Εθνικής Άμυνας (2009) "Εθνικός Κανονισμός Ασφαλείας".

[10] Γενικό Επιτελείο Στρατού, Διεύθυνση Έρευνας και Πληροφορικής (2009) "Κανονισμός Ασφάλειας Πληροφοριακών Συστημάτων ΣΚ 80-20", Τυπογραφείο Ελληνικού Στρατού 2009.

[11] Stallings W., Βασικές Αρχές Ασφάλειας Δικτύων: Εφαρμογές και πρότυπα, 3η Αμερικάνικη Έκδοση, Κλειδάριθμος, Αθήνα 2008.

[12] Scambray J.- McClure S. – Kurtz G., Hacking Exposed: Network Security Secrets & Solutions, Sixth Edition, McGraw-Hill, 2009.

ΣΥΜΠΕΡΑΣΜΑΤΑ-ΕΠΙΛΟΓΟΣ

Η εξέλιξη των ασυρμάτων δικτύων και της ασύρματης επικοινωνίας γενικότερα είναι ραγδαία με την πάροδο των ετών. Η εξυπηρέτηση και η καινοτομία των δικτύων κινητής επικοινωνίας είναι αδιαμφισβήτητη. Ο αριθμός των ασυρμάτων συσκευών τείνει να ταυτιστεί με τον πληθυσμό πάνω στον πλανήτη. Όλη αυτή η εξέλιξη, ενώ σε πρώτη άποψη φαντάζει άκρως θετική, ελοχεύει μία σειρά από επικίνδυνες καταστάσεις όπως είναι η παραβίαση του απορρήτου στις επικοινωνίες. Και όσο οι χρήστες αυξάνονται τόσο γίνεται και πιο ορατός αυτός ο κίνδυνος.

Γι' αυτό το λόγο αναγκαίο καθίσταται μαζί με την εξέλιξη της τεχνολογίας των επικοινωνιών και της πληροφορίας, να υπάρξει και ανάλογη εξέλιξη και θωράκιση στα συστήματα ασφαλείας των κινητών επικοινωνιών, έτσι ώστε ο πολίτης να διακατέχεται από ένα αίσθημα ασφαλείας.

Παράλληλα, ραγδαία είναι και η διείσδυση στον τεχνολογικό κόσμο του Internet of Things. Ωστόσο, η ανεξέλεκτη προώθησή του μπορεί να οδηγήσει τον κόσμο των επικοινωνιών σε μία άναρχη πορεία αν δεν προκαθοριστούν οι κανόνες και οι ασφαλιστικές δικλείδες λειτουργίας του μέσω της εξονυχιστικής ανάλυσης των πρωτοκόλλων του.

Στη διεθνή βιβλιογραφία το ευρύ φάσμα των Κρίσιμων Υποδομών μελετάται είτε συνολικά, είτε εστιάζοντας σε κάποιον συγκεκριμένο τομέα Κρίσιμων Υποδομών. Ωστόσο, παρατηρείται ελλιπής αναφορά των Κρίσιμων Πληροφοριακών Υποδομών και κατ' επέκταση του τρόπου μελέτης και αποτίμησης αυτών. Σε μια εποχή μάλιστα που ο τεχνολογικός παράγοντας κατέχει κυρίαρχη θέση, με τις απειλές και τις επιθέσεις ασφάλειας να αυξάνονται με γεωμετρικό ρυθμό, η αναγκαιότητα ύπαρξης μιας μεθοδολογίας αποτίμησης της επικινδυνότητας πιθανών περιστατικών ασφαλείας – αποτυχιών κρίνεται ακόμη πιο επιτακτική.

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

BCP Business Continuity Plan

BEA Bureau of Economic Analysis

CBA Cost-Benefit Analysis

CERT/CSIRT Computer Emergency Response Team/Computer Security Incident Response Team

CI Critical Infrastructure

CIAO Critical Infrastructure Assurance Office

CII Critical Information Infrastructure

CIIP Critical Information Infrastructure Protection

CI/KR Critical Infrastructure and Key Resource

CIO Critical Infrastructure Operator

CIP Critical Infrastructure Protection

CIR Critical Infrastructure Resilience

CIWIN Critical Infrastructure Warning Information Network

CNI Critical National Infrastructure

COSSI Centre Opérationnel de la Sécurité des Systèmes d'Information

DBN Dynamic Bayesian Network

DHS Department of Homeland Security

DRP Disaster Recovery Plan

ECI European Critical Infrastructure

EIF Environmental Impact Factor

EMP Emergency Management Plan

FCC Federal Communication Commission

FMEA Failure Mode and Effects Analysis

FTA Fault Tree Analysis

GDP Gross Domestic Product

HITRAC Homeland Infrastructure Threat and Risk Analysis Center

HSA Homeland Security Act

HSPD-7 Homeland Security Presidential Directive 7

ICT Information and Communication Technology

IIM Inoperability Input-Output Model

I-O Input-Output

IRGC International Risk Governance Council

IRF Inherent Risk Factor

MCA Multi-Criteria Analysis

NCIAP National Critical Infrastructure Assurance Program

MS Member States

NISC National Information Security Center

NRA National Risk Assessment

NSS National Security Strategy

NERC North American Electric Reliability Corporation

PBX Private Branch eXchange

PSEPC Public Safety and Emergency Preparedness Canada

ROI Return on Investment

RVA Risk and Vulnerability Analysis

SCADA Supervisory Control and Data Acquisition

SCFs Societal Critical Functions

SGDN Secrétariat Général de la Défense Nationale

SLA Service Level Agreement

SSAs Sector-Specific Agencies

SSPs Sector-Specific Plans

UPS Uninterruptible Power Supply

VA Vulnerability Assessment

ΤΠΕ Τεχνολογία της Πληροφορίας και της Επικοινωνίας

WI-FI WIRELESS FIDELITY

Α.Π.Δ.Π.Χ.

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

G.S.M. GLOBAL SYSTEM FOR MOBILE

Ε.Ε.Τ.Τ.

ΕΘΝΙΚΗ ΕΠΙΤΡΟΠΗ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΑΧΥΔΡΟΜΕΙΩΝ

S.I.M. SUBSCRIBER IDENTIFICATION MODULE

Ε.Σ.Ρ.

ΕΘΝΙΚΟ ΣΥΜΒΟΥΛΙΟ ΡΑΔΙΟΤΗΛΕΟΡΑΣΗΣ

G.P.S. GLOBAL POSITIONING SYSTEM

Ε.Υ.Π.

ΕΘΝΙΚΗ ΥΠΗΡΕΣΙΑ ΠΛΗΡΟΦΟΡΙΩΝ

G.P.R.S. GENERAL PACKET RADIO SERVICES

Τ.Π.Ε. ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΕΠΙΚΟΙΝΩΝΙΩΝ

I.M.E.I. INTERNATIONAL MOBILE EQUIPMENT IDENTITY

M.M.S. MULTIMEDIA MESSAGING SERVICE

S.M.S. SHORT MESSAGE SERVICE

T.M.S.I. TEMPORARY MOBILE SUBSCRIBER IDENTITY

I.M.S.I. INTERNATIONAL MOBILE SUBSCRIBER IDENTITY

V.O.I.P. VOICE OVER INTERNET PROTOCOL

I.S.P. INTERNET SERVICE PROVIDER

IP INTERNET PROTOCOL

S.S.I.D. SERVICE SET IDENTIFIER

V.P.N. VIRTULA PRIVATE NETWORK

D.N.S. DOMAIN NAME SYSTEM

C.D.R. CALL DETAIL RECORD

C.E.R.T. COMPUTER EMERGENCY RESPONSE TEAM

M.A.C. MEDIA ACCESS CONTROL

K.M.L. KEYHOLE MARKUP LANGUAGE

I.S.D.N. INTEGRATED SERVICES DIGITAL NETWORK I

P.D.A. PERSONAL DIGITAL ASSISTANT

V.S.A.T. VERY SMALL APERTURE TERMINAL