Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

Ανεπιθύμητη ηλεκτρονική αλληλογραφία και χρήση παγίδων “honeypot” για τη μελέτη της

Επιμέλεια:
Αικατερίνη Σωτηράκη

Επιβλέπων καθηγητής:
Αντώνιος Συμβώνης

1 Ιουλίου 2013

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Οι περισσότεροι χρήστες e-mail δέχονται σχεδόν καθημερινά ανεπιθύμητα μηνύματα. Οι χρήστες δεν έχουν ζητήσει να λαμβάνουν αυτά τα e-mails, ίσως δε γνωρίζουν καν τους αποστολείς τους και τον τρόπο με τον οποίο αυτοί βρήκαν τις e-mail διευθύνσεις τους. Ο τύπος των μηνυμάτων αυτών διαφέρει. Μπορεί να περιέχουν διαφημίσεις ή εκτελέσιμα αρχεία, που τελικά είναι κακόβουλο λογισμικό. Οι αποστολείς αυτών των μαζικών μηνυμάτων, που ονομάζονται "spam", εκμεταλλεύονται την ανωνυμία που προσφέρει η παρούσα υποδομή για την αποστολή μηνυμάτων και καταφέρνουν να έχουν μεγάλα κέρδη από αυτή τη δραστηριότητα.

Η ετυμολογία της λέξης spam συνήθως αποδίδεται σε ένα παλιό sketch των Monty Python [16]. Σε αυτό, η λέξη spam αναφέρεται σε ένα είδος κονσερβοποιημένου κρέατος και είναι το ακρωνύμιο για τη φράση "**S**houlder of **P**ork and H**am**". Γι' αυτό και τα κανονικά e-mails αναφέρονται και ως ham.

Τα τελευταία χρόνια έχουν προταθεί αρκετοί τρόποι αντιμετώπισης του spam. Άλλα ακόμη δεν έχει βρεθεί κάποια μέθοδος που να αντιμετωπίζει οριστικά το πρόβλημα αυτό.

1.1 Ορισμός και βασικά χαρακτηριστικά

Τα τελευταία χρόνια υπάρχει μία ραγδαία αύξηση των χρηστών του Internet και της χρήσης των e-mails. Όμως, παράλληλα έχει παρατηρηθεί μία δραματική αύξηση των μαζικών ανεπιθύμητων ηλεκτρονικών μηνυμάτων (που αναφέρονται συχνά ως spam). Σύμφωνα με την εταιρία anti-spam λογισμικού, Brightmail, ο όγκος των spam που στάλθηκαν τον Ιούλιο του 2003 ήταν περίπου το 50% όλων των e-mails εκείνου του μήνα και το ποσοστό αυτό αναμένεται να αυξηθεί στο μέλλον [12].

Προς το παρόν, δεν υπάρχει κάποιος γενικά αποδεκτός ορισμός του spam, καθώς

ένας περιεκτικός ορισμός θα έπρεπε πιθανόν να ενσωματώνει ένα σύνολο στοιχείων που σχετίζονται με την εμπορική συμπεριφορά, την ψυχολογία του παραλήπτη, το ευρύ νομικό πλαίσιο, οικονομικούς παράγοντες και τεχνικά ζητήματα [16, 12].

Κάποια χαρακτηριστικά που μπορούν να σχετισθούν με τα spam είναι τα ακόλουθα [12]:

- **Ηλεκτρονικά μηνύματα:** Τα spam στέλνονται σε ηλεκτρονική μορφή. Αν και το e-mail είναι ο πιο συνήθης τρόπος αποστολής spam, υπάρχουν και άλλοι τρόποι, όπως μέσω SMS.
- **Μαζικά:** Τα spam συνήθως στέλνονται μαζικά, ωστόσο μπορεί να σταλούν σε μικρά "πακέτα" μέσω δωρεάν λογαριασμών e-mail.
- **Ανεπιθύμητα:** Τα spam στέλνονται χωρίς τη συγκατάθεση του παραλήπτη. Ο προσδιορισμός ενός μηνύματος ως ανεπιθύμητου είναι, όμως, δύσκολος στις περιπτώσεις στις οποίες συναντάται μία προϋπάρχουσα σχέση μεταξύ του αποστολέα και του παραλήπτη.
- **Εμπορικά:** Στις περισσότερες περιπτώσεις, τα spam εξυπηρετούν κάποιον εμπορικό σκοπό, ίσως την προώθηση ή την πώληση κάποιου προϊόντος. Ωστόσο, κάποια μη εμπορικά μηνύματα μπορούν, επίσης, να θεωρηθούν spam, όπως για παράδειγμα αυτά που αφορούν μία πολιτική καμπάνια ή περιέχουν κακόβουλο λογισμικό.
- **Χρησιμοποιούν διευθύνσεις που έχουν συλλεχθεί ή πωληθεί χωρίς την άδεια του κατόχου τους:** Οι spammers συχνά χρησιμοποιούν διευθύνσεις οι οποίες δεν έχουν συλλεχθεί με τη ρητή άδεια του κατόχου τους. Για παράδειγμα, πολλοί spammers χρησιμοποιούν λίστες διευθύνσεων συλλεγμένες από δημόσιες πηγές, όπως είναι οι ιστοσελίδες ή τα newsgroups.
- **Ανωφελή:** Τα spam συχνά θεωρούνται ανωφελή ή και άχρηστα από τους παραλήπτες.
- **Στέλνονται χωρίς διακρίσεις ή στόχο:** Τυπικά, τα spam στέλνονται χωρίς συγκεκριμένο στόχο, χωρίς καμία γνώση για τον παραλήπτη εκτός από την e-mail διεύθυνσή του.
- **Επαναλαμβανόμενα:** Πολλά spam είναι επαναλαμβανόμενα, κάποιες φορές ως ακριβή αντίγραφα προηγούμενων μηνυμάτων και άλλες φορές με μικρές παραλλαγές.

- **Περιέχουν παράνομο ή προσβλητικό περιεχόμενο:** Σε αρκετές περιπτώσεις, τα spam λειτουργούν ως φορέας δόλιου ή παραπλανητικού υλικού. Ορισμένα spam περιέχουν προσβλητικό υλικό ή υλικό του απευθύνεται σε ενήλικες, κάτι που μπορεί να είναι παράνομο σε κάποιες χώρες.
- **Αδιάκοπτα:** Συνήθως, οι παραλήπτες spam δεν έχουν τη δυνατότητα να σταματήσουν την παραλαβή των μηνυμάτων αυτών, καθώς τα unsubscribe links τις περισσότερες φορές δε λειτουργούν σωστά ή και καθόλου.
- **Ανώνυμα ή συγκαλυμμένα:** Τα μηνύματα spam συχνά στέλνονται με τρόπο που ο αποστολέας τους να μην μπορεί να βρεθεί, ίσως χρησιμοποιώντας ψευδείς διευθύνσεις ή πληροφορίες επικεφαλίδας. Οι spammers σε αρκετές περιπτώσεις χρησιμοποιούν μη εξουσιοδοτημένους e-mail servers τρίτων.

Τα χαρακτηριστικά αυτά χωρίζονται σε δύο κατηγορίες, τα πρωτογενή και τα δευτερογενή, όπως φαίνεται στον ακόλουθο πίνακα.

Primary characteristics	Secondary characteristics
Electronic message	Uses addresses collected without prior consent or knowledge
Sent in bulk	Unwanted
Unsolicited	Repetitive
Commercial	Untargeted and indiscriminate
	Unstoppable
	Anonymous and/or disguised
	Illegal or offensive content
	Deceptive or fraudulent content

Source: OECD Secretariat.

1.2 Κατηγορίες περιεχομένου

Τα spam μπορούν να κατηγοριοποιηθούν ανάλογα με τον στόχο του spammer. Αρκετοί spammers στέλνουν μαζικά μηνύματα για εμπορικούς λόγους (π.χ. δια-

φημίσεις ή πολιτικές εκστρατείες), ενώ άλλοι πραγματοποιούν κάποια απάτη ή διανέμουν κακόβουλο λογισμικό (π.χ. ιούς ή Trojan horses)[16].

1. **Εμπορικές διαφημίσεις:**

   Τα spam που έχουν οποιονδήποτε εμπορικό χαρακτήρα αναφέρονται ως UCEs (Unsolicited Commercial E-mails). Κατά κύριο λόγο, τα UCEs θεωρούνται από τις εταιρίες ένα πολύτιμο εργαλείο προσεγγίσεις πελατών, καθώς το e-mail αποτελεί έναν φθηνό και εύκολο τρόπο επικοινωνίας με έναν μεγάλο αριθμό πελατών. Ωστόσο, τα περισσότερα UCEs δεν στέλνονται από τις ίδιες τις διαφημιζόμενες εταιρίες, αλλά από spammers, οι οποίοι λαμβάνουν προμήθεια από τις εταιρίες αυτές.

2. **Μη εμπορικές διαφημίσεις:**

   Τα διαφημιστικά e-mails δεν είναι απαραίτητο να είναι εμπορικά. Μπορεί, επίσης, να αφορούν πολιτικές, πολιτιστικές, θρησκευτικές ιδέες ή οργανώσεις.

3. **Απάτες και phishing:**

   Ορισμένοι spammers στέλνουν σκοπίμως παραπλανητικά e-mails ή e-mails που εξυπηρετούν κάποιο είδος απάτης. Αυτά τα μηνύματα αναφέρονται συχνά ως "scam". Παραδείγματα τέτοιων μηνυμάτων είναι αυτά που υποτίθεται ότι συλλέγουν χρήματα για θύματα κάποιας καταστροφής. Μία άλλη τέτοια περίπτωση είναι η απάτη μεταφοράς χρημάτων, γνωστή ως "Nigerian scam" ή "419 scam" (το όνομα αυτό προήλθε από τμήμα του Ποινικού Κώδικα της Νιγηρίας που παραβιάζεται). Άνθρωποι από όλο τον κόσμο έχουν λάβει μηνύματα από τη Νιγηρία, φαινομενικά από κάποιο "ανώτερο αξιωματούχο της κυβέρνησης" ο οποίος ισχυρίζεται ότι έχει κλέψει εκατομμύρια δολάρια, όμως δεν μπορεί να καταθέσει τα χρήματα αυτά σε δικό του λογαριασμό. Γι' αυτό χρειάζεται κάποιο ξένο λογαριασμό για την κατάθεση αυτή. Ο απατεώνας υπόσχεται ότι αν καταθέσει το ποσό αυτό σε κάποιο λογαριασμό στη συνέχεια ο ιδιοκτήτης του λογαριασμού θα κρατήσει ένα ποσοστό των χρημάτων.

   Ένα ιδιαίτερο είδος απάτης είναι τα phishing e-mails, τα οποία υποτίθεται ότι προέρχονται από κάποια γνωστή εταιρία. Είναι, επίσης, γνωστά ως "brand spoofing" και συχνά στοχεύουν στο να αποκαλύψουν οι παραλήπτες προσωπικά τους δεδομένα, όπως διευθύνσεις e-mail, στοιχεία των τραπεζικών λογαριασμών τους ή κωδικούς.

4. **Hoaxes και e-mail αλυσίδες:**

   Ένα hoax είναι μία προσπάθεια να ξεγελαστεί ο παραλήπτης ότι κάτι ψευδές είναι αληθινό και συνήθως συνοδεύεται από τη σύσταση να προωθηθεί

το e-mail σε όσο το δυνατόν περισσότερους ανθρώπους. Πολλά από αυτά τα e-mails προειδοποιούν τους χρήστες για ιούς ή παραπληροφορούν για πολιτικά ή κοινωνικά γεγονότα. Υπάρχουν, επίσης, και τα charity hoaxes, joke hoaxes και αυτά με εμπορικό προσανατολισμό (π.χ. προσφέροντας δωρεάν κουπόνια). Τα hoaxes μπορούν, επιπλέον, να χρησιμοποιηθούν για τη διάδοση κακόβουλου λογισμικού, εξαπατώντας τον χρήστη ώστε αυτός να επισκεφθεί κάποια ιστοσελίδα που εγκαθιστά το λογισμικό.

Τα e-mails αλυσίδες (chain e-mails)είναι αυτά που ενθαρρύνουν τους χρήστες να τα προωθήσουν σε άλλους.

5. **Joe jobs:**

   Ο όρος "Joe jobs" χρησιμοποιείται για τα πλαστογραφημένα e-mails τα οποία έχουν σταλεί από κάποιον άλλο και όχι από αυτόν που εμφανίζεται ως αποστολέας. Σκοπός τους είναι να προκαλέσουν παράπονα, ή να καταστρέψουν τη φήμη, του φερόμενου ως αποστολέα.

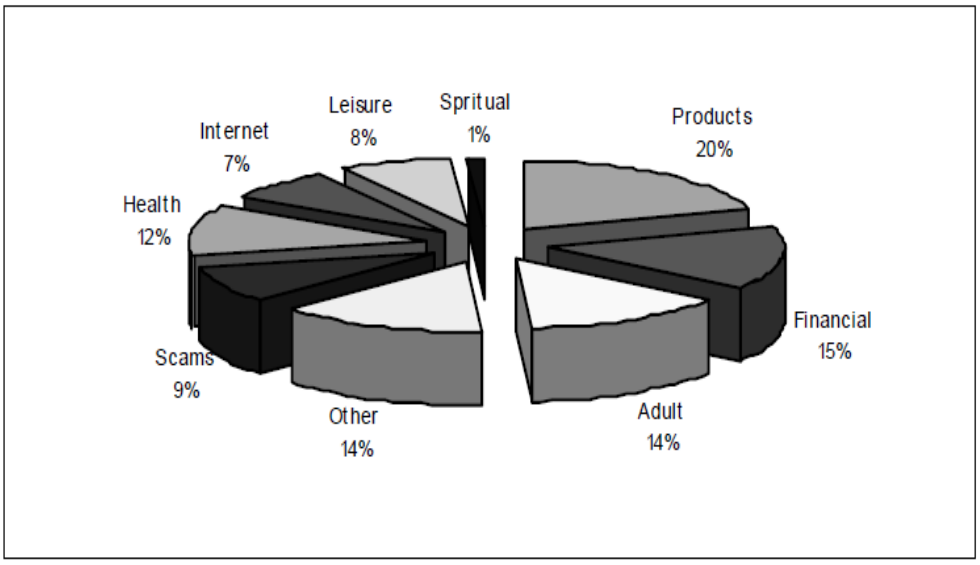
   Το όνομα αυτό χρησιμοποιήθηκε πρώτη φορά για να περιγράψει την περίπτωση του Joe Doll, ο οποίος προσέφερε χώρο για δωρεάν ιστοσελίδες. Ο λογαριασμός ενός χρήστη αφαιρέθηκε, επειδή αυτός έστελνε spam και αυτός ως εκδίκηση έστειλε εκατομμύρια spam με επικεφαλίδα "reply-to" πλαστογραφημένη ώστε να εμφανίζεται σαν να προέρχεται από τον Joe Doll.

6. **Κακόβουλο λογισμικό:**

   Αυτό το λογισμικό είναι σχεδιασμένο ώστε να διεισδύει ή να καταστρέφει τον υπολογιστή. Συνήθως, κατηγορίες τέτοιου λογισμικού είναι οι ιοί (viruses), τα worms, τα Trojan horses, το spyware και το adware. Συχνά, το λογισμικό στέλνεται ως επισύναψη κάποιου μηνύματος, που εγκαθίσταται με το άνοιγμα του μηνύματος. Τα spam και το κακόβουλο λογισμικό είναι αλληλεξαρτώμενα, καθώς τα πρώτα χρησιμοποιούνται για τη διανομή του λογισμικού, αλλά και το λογισμικό αυτό χρησιμοποιείται για τον εξ αποστάσεως έλεγχο του host, ώστε από τον host να σταλούν και άλλα spam. Αυτοί οι μολυσμένοι hosts ονομάζονται "zombie PCs" ή "spambots". Πιστεύεται ότι τα περισσότερα spam στέλνονται από botnets, δηλαδή από δίκτυα αποτελούμενα από zombie PCs, διότι αυτά προσφέρουν πολλά πλεονεκτήματα στους spammers: (1) Η ταυτότητά τους μπορεί να παραμείνει κρυφή, (2) Η πηγή των spam είναι σχεδόν αδύνατο να εντοπισθεί, (3) Η μεγάλη διαθεσιμότητα σε υπολογιστική δύναμη και εύρος ζώνης επιτρέπει μεγάλες ποσότητες spam να μεταδίδονται ακαριαίως, (4) Η διαδικασία αποστολής spam μπορεί να πραγματοποιηθεί από bots που λειτουργούν συνεργατικά και εκτελούν διαφορετικές εργασίες.[6].

7. **Bounce messages:**

   Τα bounce messages είναι e-mails που δεν παραδόθηκαν και επέστρεψαν στον αποστολέα. Όταν ένας e-mail server λάβει ένα μήνυμα με λανθασμένη διεύθυνση, τότε αυτός παράγει ένα "bounce" μήνυμα στον φερόμενο ως αποστολέα για να τον ειδοποιήσει ότι το μήνυμα δεν παραδόθηκε. Αν και τα bounce messages δεν είναι spam, συχνά οφείλονται στο φαινόμενο του spam -όταν αποστέλλονται spam με πλαστογραφημένη return address- και αποτελούν ένα μεγάλο ποσοστό της κυκλοφορίας e-mail (περίπου το 9 %).



Source: Brightmail's Prove Network (2003), "The State of Spam - Impact and Solutions", Brightmail, July, www.brightmail.com/press/state_of_spam.pdf, accessed 9 January 2004.

1.3 Συνέπειες του spam

1.3.1 Κόστος

Το spam επιβάλει ένα αυξανόμενο κόστος σε όλους τους χρήστες του διαδικτύου, καθώς χρησιμοποιεί πόρους χρηστών και παρόχων χωρίς αποζημίωση ή έγκριση. Το spam καταναλώνει υπολογιστικούς πόρους, χρόνο εργασίας από τους e-mail administrators και το προσωπικό των helpdesks και μειώνουν την παραγωγικότητα των εργαζομένων. Αν και είναι δύσκολο να υπολογισθεί το συνολικό κόστος λόγω των spam σε παγκόσμιο επίπεδο, οι εκτιμήσεις δείχνουν ότι το ποσό είναι υψηλό.

Για παράδειγμα, η Ευρωπαϊκή Ένωση με μελέτη της εκτιμάει ότι το κόστος αυτό είναι περίπου 10 δισεκατομμύρια ευρώ τον χρόνο[12].

1. **Κόστος για τους μεμονωμένους χρήστες:**

   Οι καταναλωτές σπαταλούν χρόνο διαγράφοντας επαναλαμβανόμενα και ανεπιθύμητα εμπορικά μηνύματα. Αυτό το κόστος θα μπορούσε, επίσης, να περιλαμβάνει και επιπλεόν χρεώσεις επικοινωνίας από τους ISPs ή χρεώσεις για επιπλέον χώρο αποθήκευσης. Τα κόστη που προκύπτουν στους ISPs για την αντιμετώπιση του spam τείνουν να μεταβιβάζονται στους καταναλωτές.

2. **Κόστος για τις επιχειρήσεις:**

   Χρησιμοποιώντας τεχνικές συλλογής e-mail διευθύνσεων από το Internet, οι spammers δημιουργούν βάσεις δεδομένων με τις διευθύνσεις που συλλέγονται από τα sites των επιχειρήσεων. Επιπλέον, η αύξηση των επιθέσεων με spam στις εταιρίες αποτελεί σοβαρή απειλή. Επίσης, νόμιμοι έμποροι που λειτουργούν μέσω e-mails μπορεί να έχουν κόστος, καθώς τα e-mails τους είναι πιθανό να αναγνωρίζονται ως spam από τα φίλτρα. Τέλος, οι επιχειρήσεις μπορεί να αντιμετωπίσουν προβλήματα αν τα φίλτρα εμποδίσουν λανθασμένα την παράδοση κανονικών e-mails σε υπαλλήλους τους.

   Το κόστος του spam μπορεί να χωρισθεί στην ακόλουθες κατηγορίες: (1) Απώλεια παραγωγικότητας (productivity loss), (2) Κόστος δικτύου και υπολογιστικών πόρων, (3) Επιπλέον ανθρώπινο δυναμικό και οικονομικό κόστος για την ανάπτυξη εργαλείων αντιμετώπισης του spam, (4) Κίνδυνοι ασφαλείας λόγω επιθέσεων λεξικού (dictionary attacks) ή e-mails με επισυναπτόμενους ιούς ή worms, (5) Πιθανή νομική ευθύνη (για παράδειγμα, οι επιχειρήσεις δεν είναι σε θέση να προστατεύσουν τους υπαλλήλους τους από έκθεση σε άσεμνο υλικό στο χώρο εργασίας).

3. **Κόστος για τους ISPs και τους ESPs:**

   Οι ISPs (Internet Service Providers) και οι ESPs (E-mail Service Providers) έχουν περίπου τα ίδια κόστη με αυτά των επιχειρήσεων, που περιλαμβάνουν το εύρος δικτύου, το χώρο αποθήκευσης, το χρόνο εργασίας, την ύπαρξη τηλεφωνικής γραμμής βοήθειας, κόστη επεξεργασίας για την αποθήκευση και τη δρομολόγηση επιπλέον εισερχόμενων μηνυμάτων, επενδύσεις για τεχνολογίες φίλτρων, νομικά τέλη για την καταπολέμηση των spammers. Οι ISPs έχουν και επιπρόσθετα κόστη, καθώς πρέπει να αντιμετωπίσουν πολύ γρήγορα την αύξηση του όγκου των e-mails ώστε να μη γίνει αργή η επικοινωνία μέσω Internet ή να υπερφορτωθούν οι e-mail servers τους. Τελικά, η ποσότητα χρόνου και χρήματος που πρέπει να ξοδέψουν οι ISPs και οι ESPs είναι πολύ μεγαλύτερη συγκριτικά με άλλες επιχειρήσεις.

1.3.2 Προβλήματα σχετικά με τα προσωπικά δεδομένα

Οι πρακτικές που χρησιμοποιούνται από τους spammers, και ιδιαίτερα η συλλογή και πώληση e-mail διευθύνσεων έχει αυξήσει την ανησυχία για την προστασία των προσωπικών δεδομένων [12]. Επίσης, το spam μπορεί να καταπατάει διεθνείς κανονισμούς και νόμους περί προστασίας των προσωπικών δεδομένων.

Ένα από τα κύρια προβλήματα που αντιμετωπίζουν τα άτομα λόγω του spam είναι ότι αυτό εισβάλει στη ζωής τους χωρίς τη συγκατάθεσή τους. Επιπλέον, οι διευθύνσεις τους συλλέγονται χωρίς οι χρήστες να γνωρίζουν τον τρόπο με τον οποίο θα χρησιμοποιηθούν ή χωρίς τη συγκατάθεσή τους. Κάποιοι spammers συλλέγουν διευθύνσεις από ιστοσελίδες, newsgroups και άλλες δημόσιες πηγές στο Internet. Άλλοι χρησιμοποιούν "επιθέσεις λεξικού" για να στείλουν spam και κάποιοι αποκτούν διευθύνσεις αποκτώντας παράνομη πρόσβαση σε ιδιωτικές βάσεις δεδομένων. Επιπρόσθετη εποπτεία της ιδιωτικής ζωής των χρηστών μπορεί να υπάρξει με την εγκατάσταση Web beacons (δηλαδή αντικειμένων που τοποθετούνται σε ιστοσελίδες ή e-mails χωρίς να είναι ορατά στο χρήστη και επιτρέπουν να ελέγχεται αν ο χρήστης έχει δει την ιστοσελίδα ή το e-mail) ή spyware (δηλαδή λογισμικό που παρακολουθεί τις δραστηριότητες του χρήστη στο Internet και μεταδίδει πληροφορίες -όπως e-mail διευθύνσεις, κωδικούς ή αριθμούς πιστωτικών καρτών- σε κάποιον άλλο) στους υπολογιστές των χρηστών εν αγνοία τους [12].

1.3.3 Προβλήματα σχετικά με το περιεχόμενο των spam

Εκτός από το κόστος υπάρχουν και άλλα προβλήματα που σχετίζονται με τα spam [12].

1. **Απάτη και Εξαπάτηση:**

   Τα ψευδή και παραπλανητικά spam μπορούν να έχουν διάφορες μορφές. Οι spammers συχνά κρύβουν την προέλευση του spam, επειδή γνωρίζουν ότι η παράδοση των μηνυμάτων τους θα εμποδιστεί ή επειδή στοχεύουν στο να δελεάσουν τους χρήστες ώστε να ανοίξουν το μήνυμα. Ένα συνηθισμένο τέχνασμα που χρησιμοποιούν οι spammers είναι η πλαστογράφηση των επικεφαλίδων. Η τακτική αυτή οδηγεί σε μηνύματα σε λανθασμένες διευθύνσεις "from" και "reply-to", λανθασμένες πληροφορίες δρομολόγησης, παραπλανητικά πεδία "subject" και αιτήματα αφαίρεσης. Εκτός από την πλαστογράφηση των επικεφαλίδων, οι spammers συχνά χρησιμοποιούν και τη relay function σε mail servers που ανήκουν σε άλλους. Επίσης, χρησιμοποιούνται μηνύματα με σκοπό την εξαπάτηση, όπως στα "Nigerian scam".

2. **Πορνογραφία:**

Τα spam συχνά περιέχουν πορνογραφικές φωτογραφίες ή προϊόντα και υπηρεσίες ακατάλληλες για παιδιά. Όμως, αφού οι spammers δεν στοχεύουν σε συγκεκριμένους παραλήπτες, νεαρά παιδιά είναι πιθανό ακούσια να εκτεθούν σε πορνογραφικό ή προσβλητικό υλικό.

3. **Επιπτώσεις στην ασφάλεια:**

   Οι spammers μπορούν να "γεμίσουν" τα δίκτυα υπολογιστών ή να προκαλέσουν προσωρινή παράλυση ή και μόνιμη ζημιά στους προσωπικούς υπολογιστές όταν μέσω των spam εξαπλώνονται ιοί και worms. Οι μεγάλοι όγκοι από spam επηρεάζουν σημαντικές υποδομές υπολογιστών και θέτουν σε κίνδυνο τη δημόσια ασφάλεια. Επιπλέον, τα spam μπορούν να χρησιμοποιηθούν κακόβουλα σαν επίθεση Denial of Service (DoS). Ορισμένα spam περιέχουν καταστροφικούς ιούς, worms, Web beacons ή spyware. Οι δημιουργοί ιών συνήθως κατασκευάζουν ένα πρόγραμμα που αποκτά πρόσβαση στο βιβλίο διευθύνσεων του χρήστη και διαδίδει τους ιούς στέλνοντάς τους σε όλες τις διευθύνσεις του βιβλίου. Υπάρχουν εκτιμήσεις ότι το 90 % των ιών διαδίδονται μέσω e-mail, καθώς με αυτή τη μέθοδο αποφεύγεται η παρεμπόδιση της παράδοση λόγω της ύπαρξης φίλτρων. Η σύνδεση του spam με την ύπαρξη ιών έχει οδηγήσει σε μεγαλύτερη δυσπιστία ως προς την ασφαλή επικοινωνία μέσω e-mail. Οι spammers, επίσης, εκμεταλλεύονται ενυπάρχουσες αδυναμίες στην τεχνολογία διάδοσης μηνυμάτων, όπως είναι τα open relays ή τα open proxies. Τα open relays θεωρούνται ένας καταλύτης στην ύπαρξη του spam, ενώ οι spammers συχνά προσπαθούν να "ανοίξουν" και τα closed relays.

4. **Κλοπή ταυτότητας:**

   Η κλοπή ταυτότητας εμφανίζει έξαρση και απειλεί το ηλεκτρονικό εμπόριο ελαττώνοντας την εμπιστοσύνη των πελατών. Κάθε e-mail περιέχει πληροφορίες σχετικά με την προέλευσή του, όμως η σημερινή τεχνολογία δεν μπορεί να εγγυηθεί ότι αυτές οι πληροφορίες είναι αληθείς. Αν οι spammers ανακαλύψουν πως όλα τα e-mails από κάποια εταιρία δεν μπλοκάρονται από τα φίλτρα επειδή η εταιρία βρίσκεται σε κάποια whitelist, οι spammers μπορούν να μεταβάλλουν τα μηνύματά τους ώστε να φαίνονται σαν να προήλθαν από αυτή την εταιρία. Η χρησιμοποίηση των στοιχείων μίας επιχείρησης από spammers μπορεί να καταστρέψει τη φήμη της παγκοσμίως και να είναι η αιτία της εισαγωγής του domain name της σε blacklists. Όμως, και μεμονωμένα άτομα μπορεί να πέσουν θύματα κλοπής της ταυτότητάς τους, διότι πολλοί spammers στέλνουν μηνύματα από λογαριασμούς άλλων χωρίς άδεια. Οι ISPs που εφαρμόζουν κάποιο κώδικα συμπεριφοράς σε αυτή την περίπτωση έχουν τη δυνατότητα να καταργήσουν το λογαριασμό που έχει χρησιμοποιηθεί για την αποστολή spam.

5. **Μείωση της εμπιστοσύνης των πελατών:**

   Εκτός από τα κόστη που επιβαρύνουν τους ISPs και τους χρήστες, ένα σημαντικό πρόβλημα του spam είναι ότι προκαλεί δυσπιστία τους χρήστες του Internet απέναντι στην ψηφιακή οικονομία έχοντας αρνητική επίπτωση στην ανάπτυξη του ηλεκτρονικού εμπορίου. Το spam μπορεί να οδηγήσει στην άρνηση συμμετοχής στο Internet ή στην αφαίρεση των e-mail διευθύνσεων από τις επιχειρήσεις ή τις προσωπικές σελίδες από το φόβο μήπως αυτές προστεθούν στις mailing lists των spammers. Επίσης, τα μέτρα που παίρνονται για να αντιμετωπισθεί το πρόβλημα των spam μπορούν να επηρεάσουν και τα κανονικά μηνύματα. Για παράδειγμα, νόμιμα e-mails μπορεί να αποκλεισθούν από φίλτρα, με αποτέλεσμα να μην φτάσουν ποτέ στον παραλήπτη τους [4]. Όλα τα προηγούμενα μπορούν να αποτελέσουν απειλή για τη χρησιμότητα του e-mail, που είναι από τα πιο επιτυχημένα εργαλεία του Internet.

Κεφάλαιο 2

Διαδικασία Παράδοσης και Μοντέλο Υποδομής των e-mails

2.1 Διαδικασία παράδοσης των e-mails

Το σύστημα παράδοσης e-mail αποτελείται από τρία σημαντικά στοιχεία: τους *mail user agents (MUAs)*, τους *mail servers* και το *Simple Mail Transfer Protocol (SMTP)* [11]. Η αποστολή ενός μηνύματος ξεκινάει από τον MUA του αποστολέα, όπου συγγράφεται το μήνυμα και στη συνέχεια μεταβιβάζεται στον τοπικό SMTP client (που αρκετές φορές είναι ενσωματωμένος στον MUA). Ο SMTP client εισάγει, στη συνέχεια, το μήνυμα σε ένα δίκτυο δρομολόγησης από Mail Transfer Agents (MTAs), ώστε αυτό να μεταφερθεί από τον mail server του αποστολέα στον mail server του παραλήπτη και να τοποθετηθεί στο κατάλληλο mailbox. Το SMTP είναι υπεύθυνο για τη μεταφορά του μηνύματος από τον mail server του αποστολέα σε αυτόν του παραλήπτη. Αρχικά, ο SMTP client (του αποστολέα) ζητά από το TCP να δημιουργήσει μία σύνδεση (π.χ. στη θύρα 25) με τον SMTP server (του παραλήπτη). Μετά τη δημιουργία της σύνδεσης, ακολουθεί χειραψία στο στρώμα εφαρμογών, κατά τη διάρκεια της οποίας ο SMTP client δηλώνει τη διεύθυνση του αποστολέα και του παραλήπτη. Στη συνέχεια, αποστέλλεται το μήνυμα από τον SMTP client. Η διαδικασία αυτή επαναλαμβάνεται με την ίδια TCP σύνδεση, αν ο αποστολέας έχει και άλλα μηνύματα για αυτόν τον server, αλλιώς η σύνδεση τερματίζεται.

Όταν ένας MTA της sending organization (SO) λάβει το μήνυμα, μπορεί να το μεταφέρει μέσω SMTP σε άλλους MTAs μέσα στην SO [16]. Επειδή όλοι αυτοί οι MTAs ανήκουν στον ίδιο οργανισμό, αυτό το μέρος της επικοινωνίας είναι αξιόπιστο. Ο τελευταίος MTA της SO μπορεί να συνδεθεί μέσω SMTP με ένα MTA της receiving organization (RO) ή με κάποιον άλλο SMTP server στο Internet. Αυτός ο

server μπορεί να λειτουργήσει ως ενδιάμεσο relay (δηλαδή όπως όλοι οι προηγούμενοι MTAs) ή ως gateway (δηλαδή μπορεί να μεταφέρει το μήνυμα περαιτέρω με τη χρήση διαφορετικών πρωτοκόλλων από το SMTP). Μπορεί να υπάρξουν αρκετά relays ή gateways μέχρι να φτάσει το μήνυμα στον MTA της RO, η οποία μπορεί με τη σειρά της να χρησιμοποιεί, αντίστοιχα με την SO, κάποιους εσωτερικούς MTAs. Ο τελικός MTA παραδίδει το e-mail στον Mail Delivery Agent (MDA), ο οποίος τοποθετεί το μήνυμα στον κατάλληλο αποθηκευτικό χώρο. Ο παραλήπτης συνήθως χρησιμοποιεί ένα MUA που έχει τη δυνατότητα παραλαβής των μηνυμάτων μέσω POP, IMAP ή ακόμα και HTTP.

Όταν ο SMTP client έχει ένα μήνυμα για μετάδοση, δημιουργεί ένα κανάλι διπλής κατεύθυνσης με ένα SMTP server. Η ευθύνη του SMTP client είναι να μεταφέρει το e-mail σε ένα ή περισσότερους SMTP servers ή να αναφέρει την αποτυχία μεταφοράς. Ο server ανταποκρίνεται σε κάθε εντολή με μία απάντηση, η οποία μπορεί να δείχνει ότι η εντολή έγινε δεκτή, ότι αναμένονται επιπλέον εντολές ή ότι υπάρχει κάποιο προσωρινό ή μόνιμο σφάλμα. Η απάντηση του server αποτελείται από έναν κωδικό και ένα μήνυμα.

Η διαδικασία του SMTP αποτελείται από τέσσερα στάδια: την έναρξη της σύνδεσης του SMTP server, την έναρξη της σύνδεσης του SMTP client, τη συναλλαγή του e-mail, τον τερματισμό της σύνδεσης. Μία σύνδεση SMTP ξεκινάει όταν ένας client ζητήσει σύνδεση με τον server και ο server απαντήσει με τις αρχικές πληροφορίες. Ο SMTP server μπορεί να απορρίψει τη συναλλαγή στέλνοντας την απάντηση 554, αλλά σε αυτή την περίπτωση ο server θα πρέπει να περιμένει την αποστολή του "quit" από τον client προτού τερματίσει τη σύνδεση. Αν ο server στείλει το "μήνυμα καλωσορίσματος" και ο client το λάβει, τότε ο client κανονικά στέλνει την εντολή EHLO στον server στην οποία παρουσιάζεται η ταυτότητα του client, γνωστή ως Fully Qualified Domain Name (FQDN). Εκτός από την έναρξη της σύνδεσης, η χρήση της εντολή EHLO δείχνει ότι ο client μπορεί να επεξεργαστεί επεκτάσεις υπηρεσίας (π.χ. SMTP-AUTH). Στη συνέχεια, ο client ζητά από τον server μία λίστα με τις υποστηριζόμενες επεκτάσεις (που παρουσιάζονται με μία λέξη-κλειδί και μία λίστα παραμέτρων). Τα παλαιότερα συστήματα SMTP, που δεν έχουν δυνατότητα υποστήριξης επεκτάσεων, ή clients που δεν απαιτούν τη χρήση επεκτάσεων υπηρεσίας για την έναρξη της σύνδεσης μπορεί να χρησιμοποιήσουν την εντολή HELO αντί της EHLO. Αν ο server δε δεχτεί την εντολή για κάποιο λόγο, ο κωδικός που επιστρέφεται δεν είναι ο 250 και η σύνδεση τερματίζεται.

Κάθε SMTP e-mail συναλλαγή αποτελείται από τρία βήματα:

1. Η συναλλαγή ξεκινάει με την εντολή MAIL FROM, που παρέχει την ταυτοποίηση του αποστολέα, και λέει στον SMTP παραλήπτη ότι μία νέα συναλλαγή e-mail ξεκινάει ώστε αυτός να αδειάσει τους state tables και τους

buffers του. Η εντολή αυτή έχει ως υποχρεωτικό όρισμα το reverse-path, δηλαδή το mailbox του αποστολέα ώστε να μπορούν να αναφέρονται πιθανά λάθη, και ως προαιρετικό όρισμα μία λίστα παραμέτρων, που σχετίζεται με διάφορες SMTP επεκτάσεις. Ο SMTP client πρέπει να επαναλαμβάνει την αποστολή της εντολή MAIL FROM έως ότου λάβει την απάντηση 250 OK από τον SMTP server. Αν για κάποιο λόγο ο προσδιορισμός του mailbox δε γίνεται αποδεκτός, τότε ο SMTP server θα πρέπει να επιστρέψει μία απάντηση, στην οποία θα καθορίζεται αν η αποτυχία αυτή είναι προσωρινή ή μόνιμη.

2. Ακολουθεί μία σειρά από RCPT TO εντολές, που περιέχουν πληροφορίες για τον παραλήπτη. Το πρώτο, ίσως και το μοναδικό, όρισμα αυτής της εντολής είναι το forward-path (που περιέχει ένα mailbox και ένα domain), το οποίο προσδιορίζει έναν παραλήπτη του μηνύματος. Αν το forward-path γίνει δεκτό, τότε ο SMTP server απαντάει με 250 OK και το αποθηκεύει. Αν ο φερόμενος ως παραλήπτης είναι γνωστό ότι είναι μία διεύθυνση στην οποία δεν μπορούν να παραδοθούν μηνύματα, τότε ο SMTP server απαντάει με ένα μήνυμα 550.

3. Τέλος, η εντολή DATA εκκινεί τη μεταφορά των δεδομένων του e-mail. Αν η εντολή αυτή γίνει αποδεκτή, τότε ο server επιστρέφει την ενδιάμεση απάντηση 354 και θεωρεί ότι όλες οι ακόλουθες γραμμές μέχρι το δείκτη τέλους των δεδομένων (συνήθως μία γραμμή που αποτελείται μόνο από το ".") είναι το κείμενο του μηνύματος. Αυτή η διαδικασία περιλαμβάνεται στη μέθοδο send-mail. Όταν ληφθεί και το τέλος του μηνύματος με επιτυχία, τότε ο SMTP server στέλνει ένα μήνυμα 250 OK, προσθέτει τα trace records και αποθηκεύει, προωθεί ή αναμεταδίδει το μήνυμα. Τα δεδομένα του μηνύματος δεν πρέπει να ληφθούν αν πρώτα δεν έχει προηγηθεί το μήνυμα 354.

Τα βήματα αυτά μπορούν να επαναληφθούν μέχρι να μην υπάρχουν άλλα μηνύματα για αποστολή. Τελικά, η σύνδεση τερματίζεται όταν ο SMTP client στείλει την εντολή QUIT. Σε αυτήν την εντολή ο παραλήπτης πρέπει να στείλει μία απάντηση OK και στη συνέχεια να κλείσει το κανάλι μετάδοσης.

Ένας SMTP server μπορεί να τερματίσει τη σύνδεση αν υπάρξει ανάγκη για τερματισμό της υπηρεσίας SMTP. Σε αυτή την περίπτωση, στέλνει τον κωδικό απάντησης 421. Επιπλέον, οι εντολές δεν μπορούν να σταλούν σε τυχαία σειρά. Για παράδειγμα, αν ληφθεί η εντολή RCPT χωρίς να έχει προηγηθεί η εντολή MAIL, τότε ο server πρέπει να στείλει ως απάντηση το 503 "Bad sequence of commands".

Όπως αναφέρθηκε και παραπάνω, όταν ένας SMTP server δέχεται ένα μήνυμα για αναμετάδοση ή τελική παράδοση, αυτός προσθέτει ένα trace record (που ονομάζεται και Received καταχώρηση) στην αρχή των δεδομένων του μηνύματος. Αυτή

η καταχώρηση δείχνει την ταυτότητα του host που έστειλε το μήνυμα, την ταυτότητα του host που παρέλαβε το μήνυμα, την ημερομηνία και την ώρα που λήφθηκε το μήνυμα. Τα μηνύματα που έχουν αναμεταδοθεί πολλές φορές θα έχουν πολλαπλές καταχωρήσεις ημερομηνίας και ώρας. Το trace record πρέπει να περιέχει: (1) το πεδίο FROM με το όνομα του host του αποστολέα (όπως παρουσιάζεται στην HELO/EHLO εντολή) και την IP διεύθυνση της πηγής του μηνύματος (που προσδιορίζεται μέσω της TCP σύνδεσης). (2) Το πεδίο ID. (3) Το πεδίο FOR που μπορεί να περιέχει μία λίστα από μονοπάτια στην περίπτωση που έχουν υπάρξει πολλαπλές εντολές RCPT. Ωστόσο, υπάρχουν υλοποιήσεις του SMTP που δεν προσθέτουν όλα τα απαραίτητα πεδία.

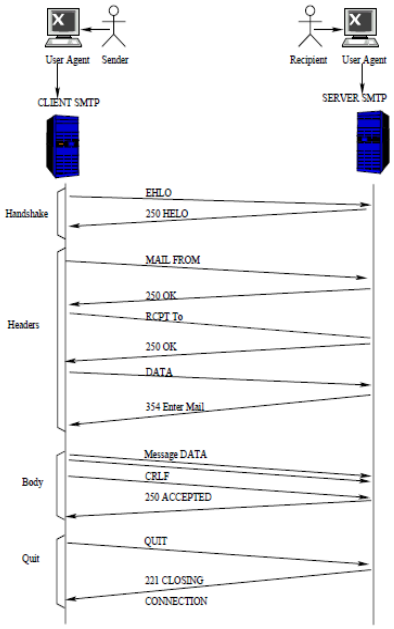
Ένα πρόγραμμα για e-mail θα πρέπει να μην αλλάζει τις Received καταχωρήσεις που έχουν προστεθεί προηγουμένως στην επικεφαλίδα του μηνύματος. Οι SMTP servers θα πρέπει να αναφέρουν τις υπάρχουσες καταχωρήσεις Received χωρίς να αλλάζουν τη σειρά τους ή να προσθέτουν καταχωρήσεις για άλλες τοποθεσίες, καθώς κάθε καταχώρηση αντιστοιχεί σε έναν server, που προσθέτει το trace record του στην αρχή της επικεφαλίδας του μηνύματος που λαμβάνει. Γι' αυτό το λόγο, η διαδρομή παράδοσης ενός e-mail αποτελείται από τα μέρη Received διαβάζοντάς τα από κάτω προς τα πάνω.

Όλα τα δεδομένα που προηγούνται της εντολής DATA αναφέρονται ως φάκελος του μηνύματος (envelope). Τα δεδομένα που στέλνονται μετά την εντολή αυτή είναι τα περιεχόμενα και περιλαμβάνουν την επικεφαλίδα (header) και το σώμα (body). Ακολουθεί ένα e-mail, στο οποίο παρουσιάζονται οι επικεφαλίδες και το σώμα του μηνύματος.

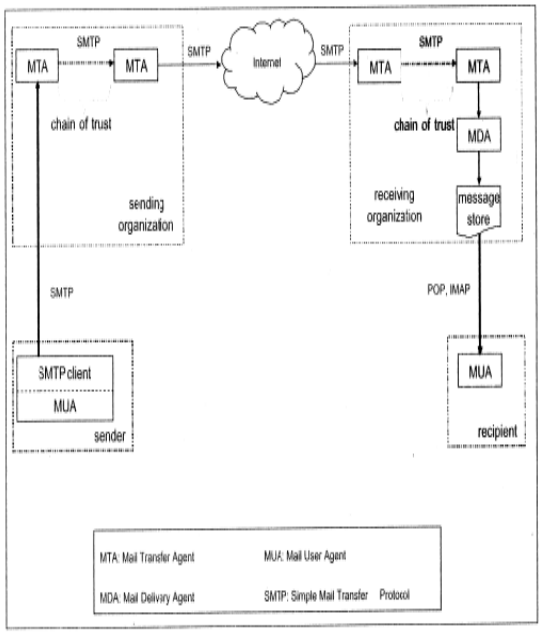
```
Return-Path: <katerina@pythagoras.math.ntua.gr>
X-Original-To: marianna@pythagoras.math.ntua.gr
Delivered-To: marianna@pythagoras.math.ntua.gr
Received: by pythagoras.math.ntua.gr (Postfix, from userid 0)
id 3654B5C07D9; Sun, 16 Jun 2013 13:57:46 +0300 (EEST)
From: katerina@pythagoras.math.ntua.gr
Subject: test
To: marianna@pythagoras.math.ntua.gr
Message-Id: <1371380266.17953@pythagoras.math.ntua.gr>
X-Originating-IP: 193.92.58.68
X-Mailer: Webmin 1.630
Date: Sun, 16 Jun 2013 13:57:46 +0300 (EEST)
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="bound1371380266"
This is a multi-part message in MIME format.
–bound1371380266
```

```
Content-Type: text/plain
Content-Transfer-Encoding: 7bit
This is a test e-mail.
–bound1371380266–
```

Παρακάτω παρουσιάζονται διαγραμματικά τα βήματα του SMTP και η διαδικασία παράδοση των e-mails



Current SMTP Protocol



A sketch of the e-mail delivery process

2.2 Μοντέλο υποδομής των e-mails

2.2.1 Ορισμός και Περιγραφή

Η υποδομή των e-mails μπορεί να περιγραφεί ως ένας κατευθυνόμενος γράφος G [16]. Επειδή το μοντέλο υποδομής των e-mails είναι δυναμικό, δεν είναι χρήσιμο να μοντελοποιείται κάθε συγκεκριμένος κόμβος που παίρνει μέρος στη διαδικασία. Αντιθέτως, οι διαφορετικοί τύποι e-mail κόμβων είναι στατικοί. Ένας e-mail κόμβος (e-mail node) αποτελεί μία μονάδα με κατάλληλο λογισμικό που εμπλέκεται στη διαδικασία παράδοσης e-mail και λειτουργεί στο TCP/IP στρώμα εφαρμογών. Οι βασικές ιδέες για την κατασκευή του G είναι:

- Οι κόμβοι του γραφήματος αντιπροσωπεύουν τους e-mail κόμβους. Οι ακμές αντιπροσωπεύουν τις συνδέσεις μεταξύ e-mail κόμβων, ενώ η κατεύθυνση της κάθε ακμής έχει τον προσανατολισμό "από client σε server". Κάθε ακμή έχει μία συγκεκριμένη τιμή, η οποία δείχνει τα διαθέσιμα πρωτόκολλα για την αντίστοιχη σύνδεση.

- Το σύνολο των e-mail κόμβων που περιγράφονται έχει συλλεχθεί κυρίως από τεχνολογικά έγγραφα (π.χ. RFCs), τεχνολογικές αναφορές του Internet και με βάση εμπειρικούς κανόνες. Επομένως, δεν υπάρχει εγγύηση για την πληρότητα αυτής της προσέγγισης και όπου χρειάζεται το σύνολο αυτό θα πρέπει να διευρύνεται.

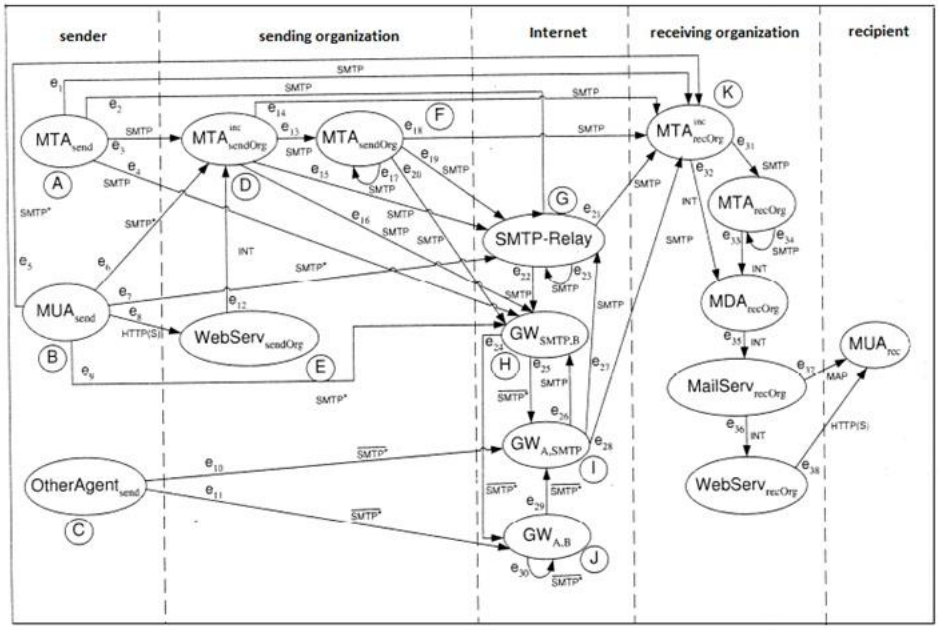
- Κάθε e-mail κόμβος σχετίζεται με κάποια πρωτόκολλα εισερχόμενων συνδέσεων και κάποια πρωτόκολλα εξερχόμενων συνδέσεων. Αυτά συλλέγονται από τις ίδιες πηγές που αναφέρθηκαν προηγουμένως. Η επικοινωνία μεταξύ των κόμβων EN_A και EN_B είναι εφικτή αν και μόνο αν υπάρχει τουλάχιστον ένα πρωτόκολλο που μπορεί να χρησιμοποιηθεί από τον EN_A για εξερχόμενη σύνδεση και από τον EN_B για εισερχόμενη σύνδεση.

Οι κόμβοι μπορούν να χωριστούν σε πέντε κατηγορίες, κάθε μία από τις οποίες συνδέεται με μία οργανωτική μονάδα που παίρνει μέρος στη διαδικασία παράδοσης των e-mails: *αποστολέας*, *SO* ή *ESP*, *Internet*, *RO* και *παραλήπτης*. Στις περιπτώσεις που οι παραλήπτες δε χρησιμοποιούν κάποιον ESP για την παραλαβή των e-mails τους, αλλά χρησιμοποιούν το δικό τους περιβάλλον παραλαβής και επεξεργασίας, οι οργανωτικές μονάδες *RO* και *παραλήπτης* συγχωνεύονται. Αν μία SO παίρνει μέρος στην διαδικασία παράδοσης ενός e-mail αυτή δέχεται το μήνυμα με έναν SMTP-based MTA ($\text{MTA}^{inc}_{sendOrg}$) ή μέσω του διαδικτυακού περιβάλλοντος, οπότε όλα τα e-mails μεταδίδονται σε έναν εσωτερικό MTA μέσω ενός web e-mail server ($\text{WebServ}_{sendOrg}$). Επιπλέον, στην *RO* εμφανίζεται ο κόμβος MDA_{recOrg} (Mail Delivery Agent), ο οποίος αποθηκεύει τα e-mails σε ένα "message store" (mail spool) απ' όπου ένας mail server (MailSer_{recOrg}) τα ανακτά ώστε να τα παραδώσει στον MUA του παραλήπτη είτε άμεσα είτε μέσω ενός web-based e-mail server (WebServ_{recOrg}).

Προτού ένα e-mail βρεθεί στον πρώτο MTA της RO μπορεί να αναμεταδοθεί από ένα ενδιάμεσο SMTP relay. Αυτό περιλαμβάνει και την περίπτωση που ένα mailbox περιέχει κάποιον κανόνα προώθησης (forwarding rule) των e-mails. Το SMTP relay αντιπροσωπεύει έναν ενδιάμεσο Internet e-mail κόμβο που χρησιμοποιεί το SMTP ως εισερχόμενη και ως εξερχόμενη διεπαφή. Όταν χρησιμοποιούνται και άλλες διεπαφές, τρία ακόμη είδη κόμβων είναι πιθανόν να υπάρχουν ($\text{GW}_{SMTP,B}$, $\text{GW}_{A,SMTP}$, $\text{GW}_{A,B}$). Αυτά μπορούν να χρησιμοποιηθούν, για παράδειγμα, για SMTP tunneling και ονομάζονται gateways. Ένας κόμβος gateway

μπορεί να χρησιμοποιηθεί και ως "proxy". Ο όρος "proxy" χρησιμοποιείται για να περιγράψει μία υπηρεσία που επιτρέπει στον client να κάνει έμμεσες συνδέσεις δικτύου με άλλες υπηρεσίες δικτύου. Οι "proxies" συμπεριφέρονται σαν τον αρχικό client και δεν αποκαλύπτουν τον πραγματικό client, μόνο η πρόσβαση στα αρχεία log ενός proxy επιτρέπει την ταυτοποίηση του πραγματικού client. Ο όρος "proxy" δεν παρέχει επιπλέον πληροφορίες για την ανομοιομορφία των χρησιμοποιούμενων πρωτοκόλλων για τις εισερχόμενες και εξερχόμενες συνδέσεις. Ορισμένοι MTAs και κάποια relays είναι ρυθμισμένα σαν proxies με την έννοια ότι δεν εισάγουν μία καταχώρηση *Received* στην επικεφαλίδα του μηνύματος. Επίσης, και ένα "zombie PC" λειτουργεί ως proxy.

Στο γράφημα, κάθε ακμή συνοδεύεται από μία ετικέτα που συμβολίζει το σύνολο των διαθέσιμων πρωτοκόλλων. Το σύνολο SMTP περιέχει το πρωτόκολλο SMTP με όλες τις (IANA-registered) επεκτάσεις υπηρεσίας (αναφέρεται και ως ESMTP), ενώ το SMTP* περιέχει το σύνολο SMTP και επιπλέον όλες τις SMTP επεκτάσεις που αφορούν την παράδοση του μηνύματος από έναν MUA σε έναν e-mail κόμβο που έχει μία εισερχόμενη διεπαφή SMTP. Επίσης, το $\overline{\text{SMTP}^*}$ είναι η ένωση τριών συνόλων: (1) Το πρώτο περιέχει όλα τα πρωτόκολλα του Internet εκτός του SMTP*. (2) Το δεύτερο περιέχει όλα τα ιδιωτικά πρωτόκολλα εφαρμογών του Internet (ώστε να ληφθεί υπόψη το tunneling). (3) Το τρίτο περιέχει όλα τα πρωτόκολλα στον Internet που λειτουργούν στο στρώμα μεταφοράς και δικτύου (π.χ. TCP και IP), καθώς για τη μεταφορά δεδομένων σε ένα δίκτυο δεν είναι απαραίτητη η ύπαρξη πρωτοκόλλου εφαρμογής. Το σύνολο MAP περιέχει όλα τα πρωτόκολλα πρόσβασης e-mail, όπως είναι το IMAP και το POP. Το σύνολο HTTP(S) περιέχει το πρωτόκολλο HTTP και τις ασφαλείς εκδοχές του (π.χ. "HTTP over SSL" και "HTTP over TLS"). Τέλος, το σύνολο INT συμβολίζει τα πρωτόκολλα και τις διαδικασίες που χρησιμοποιούνται εσωτερικά σε έναν οργανισμό για την παράδοση των e-mails. Για παράδειγμα, αναφέρεται στις εσωτερικές διαδικασίες της RO για να μεταφέρει τα e-mails από έναν εσωτερικό MTA της και να τα αποθηκεύσει στο mailbox του χρήστη.



Internet e-mail infrastructure as a directed graph

Σύμφωνα με τον τρόπο κατασκευής του G, οι διαδρομές παράδοσης e-mail αντιπροσωπεύονται από τα μονοπάτια του γραφήματος. Όπως είναι απαραίτητο στη σύγχρονη διαδικασία παράδοσης των e-mails, στην οποία ο τρόπος με τον οποίο ένας κόμβος λαμβάνει το e-mail δεν καθορίζει τον τρόπο με τον οποίο το προωθεί, κάθε μονοπάτι p αντιστοιχεί σε μία εφικτή διαδρομή παράδοσης e-mail. Στη συγκεκριμένη περίπτωση, μας ενδιαφέρει μόνο η διαδικασία παράδοσης ενός e-mail, δηλαδή ο τρόπος με τον οποίο το μήνυμα θα φτάσει στο mailbox του παραλήπτη στον e-mail server του ή στον MTA της RO, που μπορεί στη συνέχεια να εφαρμόζει κάποιο κανόνα προώθησης ή απόρριψης. Ωστόσο, η προώθηση ενός μηνύματος ή η αποστολή ενός bounce μηνύματος πίσω στον αποστολέα αποτελεί μία νέα ακολουθία ενεργειών. Κάθε επιλογή που χρησιμοποιείται για την αποστολή ενός e-mail μπορεί και να χρησιμοποιηθεί από τους spammers για την αποστολή εκατομμυρίων μηνυμάτων. Επιπλέον, λαμβάνονται υπόψη μόνο οι παραδόσεις e-mail οι οποίες ξεκίνησαν από τον client του αποστολέα ή από τον MTA του ESP (π.χ. στην περίπτωση προώθησης ή bounce μηνύματος). Επομένως, το σύνολο των επιλογών για την αποστολή ενός μηνύματος θα πρέπει να ληφθεί υπόψη όταν γίνεται προσπάθεια να βρεθούν οι τρόποι αποστολής των spam.

2.2.2 Κατηγορίες διαδρομών παράδοσης spam

Ένας χρήσιμος τρόπος για να γίνει η κατηγοριοποίηση είναι να χωρισθούν οι διαδρομές με βάση τους τύπους οργανωτικών μονάδων που αφορούν. Επειδή, όμως, η παραλαβή προϋποθέτει την ύπαρξη μίας RO και επειδή ο παραλήπτης δεν επηρεάζει τη διαδικασία, οι δύο αυτές μονάδες μπορούν να αγνοηθούν. Επομένως, υπάρχουν οχτώ διαφορετικοί συνδυασμοί που προκύπτουν από τη συμμετοχή ή τη μη συμμετοχή των οργανωτικών μονάδων *sender*, *SO* και *Internet* και παρουσιάζονται στον ακόλουθο πίνακα.

Spamming categories

No.	Scenario	Sender	Sending organization	Internet
-	-			
-	-			x
I	Provider itself spams or its MTAs were corrupted; direct connection to MTA_{recOrg}		x	
II	Provider itself spams or its MTAs were corrupted; use of intermediate Internet nodes like relays		x	x
III	Spammer uses local client; direct connection to MTA_{recOrg} (via dial-in or LAN connection)	x		
IV	Spammer uses local client; use of intermediate Internet nodes like relays (via dial-in or LAN connection)	x		x
V	Spammer uses local client; use of e-mail provider (via dial-in or LAN connection)	x	x	
VI	Spammer uses local client; use of e-mail provider (via dial-in or LAN connection) which uses intermediate Internet nodes like relays	x	x	x

Στον τρόπο που παρουσιάζεται η επικοινωνία με e-mails παραπάνω, ένας κόμβος του Internet δε θα μπορούσε ποτέ να είναι ο πρώτος συμμετέχων στη διαδικασία παράδοσης ενός e-mail, καθώς ένα e-mail εξέρχεται από ένα κόμβο που ανήκει στο περιβάλλον είτε του αποστολέα είτε της SO, συμπεριλαμβανομένων των περιπτώσεων στις οποίες υπάρχουν μολυσμένοι υπολογιστές που ελέγχονται από απόσταση. Οι πρώτες δύο γραμμές, λοιπόν, του πίνακα είναι καθαρά θεωρητικές περιπτώσεις.

Τα σενάρια I και II συμβαίνουν όταν οι ESPs ή οι MTAs τους έχουν διαφθαρεί και δεδομένου ότι οι ESPs και οι MTAs τους είναι περιορισμένοι σε πλήθος σε σχέση με τους χρήστες, οι περιπτώσεις αυτές λογικά μπορούν να αντιμετωπισθούν αποτελεσματικά. Στα υπόλοιπα σενάρια, τα spam αποστέλλονται από κάποιον τοπικό client, το οποίο είναι και αυτό που συμβαίνει τις περισσότερες φορές.

Στο σενάριο III, ο spammer δε χρησιμοποιεί κάποιον ESP, ενώ φυσικά χρησιμοποιεί κάποιον ISP που λειτουργεί στα στρώματα μέχρι το στρώμα μεταφοράς, δηλαδή απλώς προωθεί πακέτα TCP και πακέτα IP. Ο spammer συνδέεται απευθείας με έναν MTA της RO και επομένως είναι περιορισμένος στις θύρες που εκτελούνται εκεί, δηλαδή συνήθως τη θύρα 25 ή 587. Επομένως, είναι σχετικά εύκολο να αποκλεισθεί ο μεγαλύτερος όγκος των spam που στέλνονται με αυτό τον τρόπο απλώς απορρίπτοντας τα TCP πακέτα που φτάνουν σε αυτή τη θύρα. Το σενάριο III, επίσης, περιλαμβάνει και την περίπτωση των “zombie PCs”.

Το spam που στέλνεται με το σενάριο IV είναι πολύ δύσκολο να αντιμετωπισθεί γιατί ο spammer μπορεί να χρησιμοποιεί όλους τους κόμβους του Internet, συμπεριλαμβανομένων και των gateways.

Στο σενάριο V, τα spam μεταφέρονται μέσω των υπηρεσιών που προσφέρονται από κάποιον ESP. Ακόμη και αν υπάρχει κάποιο όριο στον αριθμό των μηνυμάτων που επιτρέπεται να σταλούν ανά ημέρα και ανά λογαριασμό, πρέπει να επιλυθεί το πρόβλημα της αυτόματης δημιουργίας από τον spammer νέων λογαριασμών κάθε ημέρα. Το σενάριο V περιλαμβάνει, και αυτό, τις περιπτώσεις των “zombie PCs”, τα οποία συνδέονται στην SO και τον ESP του χρήστη.

Το σενάριο VI φαίνεται αρκετά απίθανο, καθώς σε αυτό ο spammer χρησιμοποιεί κάποιον ESP, ο οποίος προωθεί τα μηνύματα, στέλνοντας τα σε ενδιάμεσους κόμβους του Internet. Αυτό μπορεί να συμβεί αν ο ESP υποστηρίζει τις παράνομες δραστηριότητες που σχετίζονται με το spam των πελατών του.

Τα anti-spam μέτρα, τα οποία θα αναλυθούν στη συνέχεια, μπορούν να κατηγοριοποιηθούν ανάλογα με το αν αυτά ελέγχουν συγκεκριμένες διαδρομές παράδοσης ή αυτά λειτουργούν ανεξάρτητα με το ποια είναι η διαδρομή που έχει ακολουθήσει το spam. Τα μέτρα συγκεκριμένης διαδρομής (route-specific measures) είναι τα ακόλουθα:

- Μηχανισμοί αποδοχής ή απόρριψης των e-mails ανάλογα με τη διεύθυνση

IP του αποστέλλων MTA.

- Αποκλεισμός της TCP θύρας 25, που χρησιμοποιείται συνήθως για την αποστολή των e-mails.
- Περιορισμός του αριθμού των εξερχόμενων e-mails ανά λογαριασμό και ανά μονάδα χρόνου.
- Μηχανισμοί πιστοποίησης που βασίζονται σε SMTP επεκτάσεις, κρυπτογραφική πιστοποίηση ή πιστοποίηση μονοπατιού.

Στον επόμενο πίνακα παρουσιάζεται η αποτελεσματικότητα αυτών των μέτρων σε σχέση με τις διαφορετικές διαδρομές που μπορεί να ακολουθήσει το spam. Με "x" συμβολίζεται η αποτελεσματική αντιμετώπιση, με κενό η μη αντιμετώπιση, ενώ με "(x)" συμβολίζεται η αντιμετώπιση η οποία όμως συνοδεύεται από προβλήματα και, επομένως, δεν είναι μακροπρόθεσμα εφικτή. Για παράδειγμα, στην περίπτωση του IP blocking, θα μπορούσε να εμποδιστεί η διαδρομή του σεναρίου V, δηλαδή να αποκλείονται όλες οι IP διευθύνσεις ενός ISP ή ακόμα και μίας ολόκληρης χώρας, όμως αυτό θα οδηγούσε στη δημιουργία ψηφιακού χάσματος. Στο επόμενο κεφάλαιο, εξετάζεται αναλυτικά το κάθε anti-spam μέτρο και η αποτελεσματικότητά του.

Effectiveness of (route-specific) anti-spam

		Anti-spam approaches						
Scenario	Nodes involved	IP blocking	TCP blocking	SMTP extensions	Cryptographic authentication	Path authentication	Limitation of outgoing e-mails	Reputation-based
I	MTAs of provider	x						x
II	MTA of provider, then relay(s)							x
	MTA of provider, then relay(s) and gateway(s)							
	MTA of provider, then at least gateway(s)							
III	Local MTA		x			x		x
IV	Local MTA or MUA, then relay(s)		x		x	x		x
	Local MTA or MUA, then relay(s) and gateway(s)							
	Local agent other than MTA or MUA, then at least gateway(s)							
V	Local MTA or MUA, MTA(s) of provider	(x)		(x)			(x)	(x)
VI	Local MTA or MUA, then MTA(s) of provider, then relay(s)			(x)		x	(x)	(x)
	Local MTA or MUA, then MTA(s) of provider, then at least gateway(s)							
	Local MTA or MUA, then MTA(s) of provider, then relay(s) and gateway(s)							

2.3 Τα τρωτά σημεία του SMTP

Το SMTP είναι ένα πρωτόκολλο ιδιαίτερα τρωτό στο spam, γεγονός που οφείλεται κυρίως σε δύο στοιχεία [16]:

1. Σε αντίθεση με τα συμβατικά μηνύματα (μέσω ταχυδρομείου) η αποστολή e-mail είναι στην ουσία δωρεάν. Οι spammers επιβαρύνονται μόνο από τη χρέωση για τη σύνδεση με τον ISP, η οποία όλο και μειώνεται, γι' αυτό και το κόστος αποστολής e-mail μπορεί να θεωρείται "αμελητέα χαμηλό".

2. Το SMTP είναι σχεδιασμένο για να λειτουργεί σε ένα περιβάλλον στο οποίο δεν υπάρχουν πολλές επιθέσεις, κάτι που δεν ισχύει για το Internet αυτή την στιγμή. Συγκεκριμένα, η έλλειψη απονομής ευθύνης είναι ένας σοβαρός λόγος που το spam αποτελεί πρόβλημα.

Το SMTP επιτρέπει την πλαστογράφηση των στοιχείων της διεύθυνσης και, επομένως, επιτρέπει την ανωνυμία, πράγμα που δυσκολεύει ή και καθιστά αδύνατο τον εντοπισμό του αποστολέα ενός μηνύματος. Αν και στα στοιχεία της διεύθυνσης περιέχεται η IP διεύθυνση της πηγής του μηνύματος, συχνά δεν ελέγχεται κατά πόσο τα δοσμένα στοιχεία συμφωνούν με αυτή τη διεύθυνση. Επιπλέον, υπάρχει περίπτωση, αν και δεν είναι τόσο συχνό, και η IP διεύθυνση να έχει αλλοιωθεί (IP spoofing).

Πολλοί hosts, επίσης, χρησιμοποιούν δυναμικές IP διευθύνσεις, που τους δίνονται από τον αντίστοιχο ISP. Σε αυτή την περίπτωση είναι αδύνατο να βρεθεί ο αποστέλλων host μετά το πέρας της TCP/IP σύνδεσης, εκτός και αν κρατείται ένα log αρχείο που αποθηκεύει την αντιστοιχία μεταξύ των hosts και των IP διευθύνσεων.

Η αυξανόμενη χρήση του Network Address Translation (NAT) μπορεί να οδηγήσει στην ανάγκη για την αποθήκευση περισσότερων αρχείων log. Αν στο NAT υπάρχει μία 1:1 αναλογία των διευθύνσεων που χρησιμοποιούνται εσωτερικά και εξωτερικά του NAT, δεν υπάρχει κανένα πρόβλημα. Στην περίπτωση, όμως, που το NAT συνδέει πολλούς εσωτερικούς hosts με μία IP διεύθυνση, χρησιμοποιώντας διαφορετικές θύρες, είναι απαραίτητη η κράτηση όχι μόνο των IP διευθύνσεων αλλά και των θυρών για να είναι εφικτή η ταυτοποίηση του εσωτερικού host του NAT.

Πρέπει, τέλος, να σημειωθεί ότι ακόμη και αν η επικεφαλίδα δεν περιέχει πλαστές πληροφορίες και ο αποστέλλων host μπορεί να ταυτοποιηθεί, αυτό δεν οδηγεί στην αποκάλυψη του spammer καθώς σε πολλές περιπτώσεις τα spam στέλνονται από παραβιασμένους (hijacked) hosts. Συνεπώς, όλα τα πεδία επικεφαλίδας τα οποία προστέθηκαν πριν από τον τελευταίο αξιόπιστο MTA πρέπει να αντιμετωπίζονται ως πιθανόν πλαστά.

Το SMTP, επίσης, επιτρέπει την πλαστογράφηση της διεύθυνσης e-mail του αποστολέα. Οι spammers εκμεταλλεύονται αυτή την αδυναμία ώστε να δυσχεράνουν την εύρεση του υπεύθυνου για την αποστολή των spam, αλλά και να αποφύγουν πιθανά φίλτρα (π.χ. χρησιμοποιώντας διευθύνσεις που ανήκουν στη whitelist του παραλήπτη).

Ακόμη και όταν χρησιμοποιούνται επεκτάσεις του SMTP, όπως το SMTP-AUTH ή το "SMTP after POP", η χρήση τους περιορίζεται συνήθως στην επικοινωνία του e-mail client του χρήστη με τον SMTP server (το SMTP-AUTH αποτελεί εξαίρεση σε αυτόν τον κανόνα). Τα μειονεκτήματα αυτών των μεθόδων περιλαμβάνουν την περιορισμένη ευελιξία και το χαμηλό επίπεδο ασφαλείας, καθώς η χρήση κωδικών που αποθηκεύονται στον υπολογιστή του χρήστη δε θεωρείται ιδιαίτερα ασφαλής σήμερα.

Η υποδομή για e-mail και το SMTP σχεδιάστηκαν ώστε να είναι ευέλικτα και να αποτρέπουν την κατάρρευση των e-mail κόμβων. Επομένως, η έννοια της αναμετάδοσης (relay) μεταξύ MTAs συμπεριλήφθηκε σε αυτή την κατασκευή. Ένας relay server έχει τη δυνατότητα να αποδεχτεί ή να απορρίψει την ανάληψη της εργασίας αναμετάδοσης μηνυμάτων με τον ίδιο τρόπο που μπορεί να αποδεχτεί ή να απορρίψει ένα μήνυμα για κάποιον τοπικό χρήστη. Ένα open relay είναι ένας server ο οποίος δε θέτει περιορισμούς στο φόρτο των e-mails, δηλαδή επεξεργάζεται e-mails ακόμη και αν ούτε ο παραλήπτης ούτε και ο αποστολέας είναι τοπικοί χρήστες. Τα open relays χρησιμοποιούνται από τους spammers ως ενδιάμεσοι MTAs για τη διάδοση των spam μέσω ενός μη ύποπτου server. Από την στιγμή που θα αποκαλυφθεί πως ένας MTA στέλνει spam, σε σύντομο χρονικό διάστημα περιέχεται σε δημοσίως διαθέσιμες IP blacklists. Στο παρελθόν, η αναμετάδοση των e-mails από τρίτους ήταν χρήσιμη, όμως σήμερα τα open relays αποτελούν μία σοβαρή απειλή στην υποδομή του e-mail και θα πρέπει να αποφεύγονται.

Κεφάλαιο 3

Anti-spam μέτρα

Το εύρος των anti-spam μέτρων περιλαμβάνει νομικά, οργανωτικά, συμπεριφορικά και τεχνολογικά μέτρα [16].

3.1 Νομικά

Λόγω της δριμύτητας και της δυνητικής ζημίας που μπορεί να προκαλέσει το spam πολλές χώρες έχουν αρχίσει να το αντιμετωπίζουν μέσω νομοθεσίας. Ωστόσο, η σημερινή νομοθεσία σε παγκόσμιο επίπεδο σχετικά με την ανεπιθύμητη ηλεκτρονική αλληλογραφία είναι ετερογενής και η αποτελεσματικότητά της είναι αμφιλεγόμενη.

Οι νομοθεσίες κρατών μπορούν να διαφέρουν σε πολλές παραμέτρους, όπως στον τύπο της συνδρομής, στο πεδίο δράσης, στον τύπο του αποστολέα και του παραλήπτη και στο σύνολο των πιθανών κατήγορων. Εξαιτίας όλων αυτών των παραμέτρων, εμφανίζεται μεγάλη ετερογένεια στους anti-spam νόμους παγκοσμίως.

Συνδρομή:

Η έννοια αυτή αναφέρεται στον τρόπο με τον οποίο μπορούν οι παραλήπτες να αρνηθούν την παραλαβή των e-mails. Υπάρχουν δύο προσεγγίσεις: η opt-in, στην οποία ο αποστολέας πρέπει να έχει την άδεια του παραλήπτη για να στείλει το μήνυμα, και η opt-out, στην οποία υπάρχει ένας μηχανισμός ώστε να απορρίπτονται τα μετέπειτα e-mails από τον ίδιο αποστολέα.

Οι προσεγγίσεις αυτές περιλαμβάνουν τις ακόλουθες διατάξεις:

- Διπλό opt-in: Απαιτείται από το συνδρομητή να εκτελέσει δύο ενέργειες. Αρχικά, πρέπει να προστεθεί η διεύθυνση e-mail σε μία λίστα (η προσθήκη στη λίστα μπορεί να γίνει μέσω μιας ιστοσελίδας ή μέσω

e-mail). Στη συνέχεια, ο ιδιοκτήτης της λίστας αποστέλλει ένα μήνυμα επιβεβαίωσης (πρόκληση), που πρέπει να απαντηθεί από τον παραλήπτη. Μόνο όταν η απάντηση αυτή δοθεί, η διεύθυνση προστίθεται στη λίστα. Ο λόγος που ζητείται από τον αποστολέα να επιβεβαιώσει την προσθήκη της διεύθυνσης στη λίστα είναι ότι κάποιος άλλος εκτός από τον κάτοχο της διεύθυνσης μπορεί να την έχει προσθέσει χωρίς την άδεια του κατόχου.

- Επιβεβαιωμένη opt-in: Η περίπτωση αυτή είναι παρόμοια με αύτη του "διπλού opt-in" με τη διαφορά ότι το μήνυμα επιβεβαίωσης πρέπει να απαντηθεί ή κάποιες άλλες ενέργειες πρέπει να γίνουν από τον παραλήπτη για να διαγραφεί από τη λίστα. Για τον αποστολέα, ένα πρόβλημα με αυτή την προσέγγιση υπάρχει όταν, δια νόμου, είναι υποχρέωση του αποστολέα να αποδείξει ότι ο παραλήπτης έχει ρητά αποδεχθεί την παραλαβή των e-mails.
- Απλό opt-in: Σε αυτή την περίπτωση δεν απαιτείται κανενός είδους επιβεβαίωση. Μόλις μία διεύθυνση εισαχθεί, προστίθεται αυτόματα στη λίστα, ακόμη και αν ο κάτοχος της διεύθυνσης δεν έχει δώσει τη συγκατάθεσή του.
- Opt-out: Ένας αποστολέας μπορεί να λάβει ένα e-mail χωρίς να έχει δώσει άδεια εκ των προτέρων, αλλά του παρέχεται ένα link ή μία διεύθυνση e-mail τα οποία μπορούν να χρησιμοποιηθούν για την παύση της επικοινωνίας. Ορισμένες χώρες, όπως οι Η.Π.Α., προτείνουν τη διατήρηση μιας λίστας ("Robinson list") που περιέχει τις διευθύνσεις e-mail των καταναλωτών που δεν επιθυμούν να λαμβάνουν εμπορικά e-mails.

Πεδίο δράσης:

Οι anti-spam νόμοι έμμεσα ή άμεσα αναφέρονται στην αποστολή συγκεκριμένων ειδών μηνυμάτων και στη ζημία που αυτά μπορούν να προκαλέσουν αποφεύγοντας να χρησιμοποιήσουν τη χρήση του όρου spam, καθώς η νομοθετική σημασιολογία του όρου αυτού δεν έχει ακόμη ορισθεί. Το πεδίο δράσης των νόμων μπορεί να καλύπτει την αποστολή (μαζικών) e-mails, τη διανομή κακόβουλου λογισμικού ή τη διανομή πορνογραφικού υλικού. Επιπλέον, όταν οι νόμοι αναφέρονται στην αποστολή (μαζικών) e-mails, πολλές φορές προσδιορίζουν συγκεκριμένους τύπους e-mails, συνήθως επικεντρώνονται σε εμπορικά e-mails (UCEs).

Αποστολέας και Παραλήπτης:

Οι νόμοι μπορεί να προσδιορίζουν συγκεκριμένους τύπους αποστολέα και παραλήπτη, για παράδειγμα ιδιώτες ή οργανισμούς.

Πιθανοί κατήγοροι:

Οι νόμοι μπορεί να θέτουν περιορισμούς στο ποιος μπορεί να μηνύσει τους αποστολείς e-mail. Πολλοί anti-spam νόμοι δεν παρέχουν νομοθετικά μέσα για μεμονωμένα άτομα, αλλά μόνο για κρατικές αρχές και άλλους οργανισμούς.

Άλλες απαιτήσεις:

Μερικές από τις πρόσθετες απαιτήσεις οι οποίες θα μπορούσαν να εμπεριέχονται σε anti-spam νόμους είναι η απαγόρευση χρήσης συλλεγμένων (harvested) e-mail διευθύνσεων, η απαίτηση κάθε e-mail να περιέχει μια έγκυρη διεύθυνση e-mail ή άλλους μηχανισμούς ώστε ο παραλήπτης να μπορεί να διαγραφεί από την εμπορική λίστα διευθύνσεων e-mail.

Σύμφωνα με τα στοιχεία ερευνών αγοράς και anti-spam εταιριών (όπως είναι οι Commtouch, Sophos, Spamhaus), οι χώρες που ευθύνονται για περισσότερο από των 50% όλων των e-mails που κατατάσσονται ως spam, δηλαδή οι Η.Π.Α., η Κίνα, η Δημοκρατία της Κορέας και η Ρωσία, είτε εφαρμόζουν μη περιοριστικούς anti-spam νόμους, όπως opt-out νόμους, είτε δεν έχουν καθόλου anti-spam νόμους.

Σχετικά με την αποτελεσματικότητα των anti-spam νόμων, τα στοιχεία δείχνουν ότι οι opt-in νόμοι έχουν κάποιο θετικό αποτέλεσμα, σε αντίθεση με τους opt-out, οι οποίοι είναι σπανίως απαγορευτικοί. Εντούτοις, πρέπει να αναγνωριστεί ότι και οι opt-out νόμοι είναι αρκετά χρήσιμοι, καθώς παρέχουν σαφείς νομοθετικές οδηγίες για εταιρίες και τους παραλήπτες, ώστε να περιορίζουν την ανεξέλεγκτη διαφήμιση μέσω e-mail των ευυπόληπτων εταιριών.

Αν είναι αληθή τα στοιχεία που δείχνουν ότι η πλειοψηφία των spam που στοχεύει σε χρήστες στην Ευρώπη και στη Βόρεια Αμερική προέρχεται από μία σκληροπυρηνική ομάδα από γνωστούς επαγγελματίες spammers, τότε η δίωξη μικρού αριθμού spammers θα μειώσει σε μεγάλο βαθμό το πρόβλημα του spam. Αυτό αποτελεί κίνητρο για την επιπλέον ενασχόληση με τους anti-spam νόμους και τη διάδοσή τους.

Ορισμένα βασικά προβλήματα που σχετίζονται με τα νομικά μέτρα είναι τα ακόλουθα:

- Ένα γενικό πρόβλημα που σχετίζεται με τη νομοθεσία εναντίον των spam είναι ότι πρόκειται για ένα παγκόσμιο φαινόμενο, το οποίο αντιμετωπίζεται με εθνική νομοθεσία. Πιο συγκεκριμένα, μια σημαντική ποσότητα από spam διασχίζουν τα σύνορα πολλών χωρών και μια από τις ερωτήσεις που σχετίζεται με αυτό το γεγονός είναι κατά πόσο μία χώρα έχει δικαιοδοσία στα spam που προέρχονται από αυτή την χώρα, αλλά κατευθύνονται έξω

από τα σύνορά της ή αν μπορεί να ξεκινήσει νομικές διαδικασίες εναντίον spammers που ζουν σε άλλες χώρες.

- Κάποιοι νόμοι προβλέπουν "αμοιβές" για την αποκάλυψη των spammers. Όμως, μία τέτοια πρακτική δίνει κίνητρο σε hackers να παρεμβαίνουν στα προσωπικά δεδομένα των χρηστών. Μία τέτοια περίπτωση είναι αυτή της Rodona Garst, μίας διαβόητης spammer, που αποκαλύφθηκε όταν ένα από τα "θύματα" της, ο "Man in the Wilderness", απέκτησε πρόσβαση στον υπολογιστή της και αποκάλυψε την ταυτότητά της. [21]

3.2 Οργανωτικά

Τα οργανωτικά μέτρα περιλαμβάνουν "συστήματα κατάχρησης" (abuse systems), που προσφέρουν forum για τους χρήστες που θέλουν να παραπονεθούν για τα spam που λαμβάνουν. Περιέχουν, επίσης, και διάφορες μορφές διεθνής συνεργασίας.

Συστήματα κατάχρησης:

Χρησιμοποιούνται ώστε η κοινότητα του Internet να μπορεί να αναφέρει και να ρυθμίζει την κατάχρηση του δικτύου και τους καταχρηστικούς χρήστες. Τέτοια συστήματα μπορούν να είναι μέρος της υποδομής του ESP ή ενός οργανισμού που δεν εξαρτάται από κάποιον πάροχο. Αν ένας χρήστης δεν ξέρει σε ποιον πρέπει να διαμαρτυρηθεί, τότε μπορεί να στείλει ένα e-mail σε ένα σύστημα κατάχρησης, το οποίο προωθεί το παράπονο στους αντίστοιχους διαχειριστές του συστήματος ή ακόμη και σε διεθνείς οργανισμούς, ομοσπονδίες και υπεύθυνες αρχές.

Με αυτά τα συστήματα σχετίζονται και τα συστήματα τα οποία διατηρούν blacklists, δηλαδή λίστες από IP διευθύνσεις από τις οποίες προέρχονται τα spam. Πιο συγκεκριμένα, e-mails σε συστήματα κατάχρησης που αφορούν τον ίδιο host μπορεί να οδηγήσουν στην εισαγωγή της IP διεύθυνσή του σε κάποια blacklist.

Διεθνής συνεργασία:

Περιλαμβάνει διμερείς κυβερνητικές συνεργασίες, συνεργασίες ανάμεσα σε ιδιωτικές ομάδες ακόμη και πολυμερείς συνεργασίες.

3.3 Συμπεριφορικά

Τα συμπεριφορικά μέτρα αναφέρονται στις διαδικασίες που πρέπει να ακολουθούν οι χρήστες e-mail στη χρήση και στη διανομή των e-mail διευθύνσεών τους και στην αντιμετώπιση των spam που λαμβάνουν.

Η συλλογή (harvesting) διευθύνσεων e-mail είναι ένας τρόπος ώστε να αποκτηθούν έγκυρες e-mail διευθύνσεις. Η προστασία των διευθύνσεων από τη συλλογή τους θεωρείται ότι θα μειώσει τον όγκο των spam, ώστε να μη χρειαζέται αυτά να αντιμετωπισθούν με τεχνολογικά μέτρα, τα οποία καταναλώνουν πολλούς πόρους. Οποιοδήποτε σημείο στο οποίο αποθηκεύονται διευθύνσεις θεωρείται ενδιαφέρον για τους συλλέκτες διευθύνσεων. Παραδείγματα τέτοιων σημείων είναι διάφορες mailing lists, newsletters και ιστοσελίδες.

Έχουν προταθεί αρκετοί τρόποι ώστε να προστατευτούν οι e-mail διευθύνσεις:

- Μία προσέγγιση είναι να δημιουργούνται "αναλώσιμα" e-mail ψευδώνυμα, τα οποία να διανέμονται και μετά από κάποιο καιρό να μη χρησιμοποιούνται ξανά. Υπάρχουν δύο κύρια προβλήματα σε αυτή την προσέγγιση: (1) Με τον καιρό, οδηγεί σε ένα μεγάλο πλήθος αχρησιμοποίητων λογαριασμών και μεγάλο κόστος συντήρησης τόσο για τους χρήστες όσο και για τους παρόχους. (2) Η χρήση "αναλώσιμων" λογαριασμών δεν μπορεί να εμποδίσει τα spam να παραδίδονται σε αυτούς, καθώς οι spammers δεν ξέρουν την κατάσταση ενός λογαριασμού. Από την στιγμή που τα e-mails παραδίδονται επιτυχώς, ο λογαριασμός θεωρείται έγκυρος. Ωστόσο, θα ήταν χρήσιμο να δημιουργούνται e-mail λογαριασμοί για συγκεκριμένους σκοπούς και να καταργούνται όταν γεμίζουν από spam.

- Υπάρχουν πολλές άλλες τεχνικές απόκρυψης των e-mail διευθύνσεων οι οποίες στοχεύουν στο να εμποδιστεί η συλλογή τους από προγράμματα στην περίπτωση που αυτές έχουν κοινοποιηθεί σε ιστοσελίδες. Ένας τρόπος για να γίνει αυτό εφικτό είναι η ενσωμάτωση των διευθύνσεων σε εικόνες ώστε να είναι αναγνωρίσιμες από ανθρώπους, αλλά όχι από μηχανές. Ένας άλλος τρόπος είναι να κωδικοποιούνται ώστε να είναι ασφαλείς από πιθανή συλλογή. Για παράδειγμα, η διεύθυνση anakin.skywalker@starwars.com μπορεί να εμφανίζεται ως anakin.skywalker-AT-starwars.com. Αυτές οι μέθοδοι είναι αποτελεσματικές όσο οι spammers δεν είναι εξοικειωμένοι με τη χρησιμοποίησή τους. Ωστόσο, έχουν περιορισμένη χρησιμότητα σε περιπτώσεις όπου οι διευθύνσεις δεν μπορούν να μετατραπούν με τυχαίο τρόπο (π.χ. εγγραφή σε newsletter).

Αν τα spam φτάσουν, τελικά, στον χρήστη, τότε υπάρχουν αρκετές επιλογές ώστε να τα αντιμετωπίσει:

- Ένα επιχείρημα που υποστηρίζει ότι η απάντηση στα spam μπορεί να έχει κάποιο αποτέλεσμα είναι ότι κάποια στιγμή ο spammer θα βαρεθεί να καταναλώνει τον χρόνο του σε άσκοπες συζητήσεις και θα σταματήσει. Ωστόσο, πολλοί συμβουλεύουν τους χρήστες να μην απαντάνε, ειδικά μέσω της επιλογής "remove me", γιατί με αυτό τον τρόπο ο αποστολέας επιβεβαιώνει ότι το e-mail είναι έγκυρο, ότι ο ISP πιθανόν δεν χρησιμοποιεί αποτελεσματικά spam φίλτρα, ότι ο χρήστης ανοίγει και διαβάζει τα spam και ότι είναι διατεθειμένος να ακολουθήσει τις οδηγίες του spammer (όπως το "πατήστε εδώ για αφαίρεση").

- Ο χρήστης πρέπει να ελέγξει αν λειτουργούν σωστά τα φίλτρα του παρόχου και της εφαρμογής ηλεκτρονικού ταχυδρομείου. Ωστόσο, ο χρήστης πρέπει να γνωρίζει για τις πιθανές λανθασμένες ταξινομήσεις των e-mails του (ειδικά για τις περιπτώσεις των false-positives).

- Μπορεί να γίνει αναφορά των μηνυμάτων σε βάσεις spam, οι οποίες είναι ανοικτές στην anti-spam κοινότητα για ερευνητικούς σκοπούς.

- Έχουν ιδρυθεί αρκετοί οργανισμοί "καταχρήσεων", στους οποίους μπορούν να γίνουν καταγγελίες για spam. Πολλοί ESPs παρέχουν μία e-mail διεύθυνση για να αποστέλλονται εκεί οι καταγγελίες. Στη συνέχεια, αναλύοντας τα spam που στέλνονται σε αυτή τη διεύθυνση μπορούν, για παράδειγμα, να βελτιώσουν τα spam φίλτρα τους ή να λάβουν άλλα τεχνολογικά μέτρα. Επιπλέον, αυτά τα δεδομένα μπορούν να αποσταλούν σε anti-spam οργανισμούς, όπως για παράδειγμα στην Network Abuse Clearinghouse, ή στις αρμόδιες κρατικές αρχές, όπως έχει αναφερθεί προηγουμένως.

Τόσο οι νόμοι και τα ρυθμιστικά μέτρα όσο και τα συμπεριφορικά μέτρα λειτουργούν συμπληρωματικά με τα τεχνολογικά anti-spam μέτρα.

3.4 Τεχνολογικά

Τα anti-spam μέτρα μπορούν να ταξινομηθούν ανάλογα με τα ακόλουθα κριτήρια:

- Μέτρα μπορούν να ληφθούν σε διάφορα στάδια της παράδοσης του e-mail. Μπορούν να ενεργοποιηθούν στην εφαρμογή ηλεκτρονικού ταχυδρομείου, στον MTA του ESP του αποστολέα, σε κόμβους εκτός των ESPs του αποστολέα και του παραλήπτη, στον MTA του ESP του παραλήπτη ή στην εφαρμογή ηλεκτρονικού ταχυδρομείου του παραλήπτη. Οι δύο πρώτες τοποθεσίες επιτρέπουν την εφαρμογή προληπτικών μέτρων, ενώ τα μέτρα που λαμβάνονται στα τελευταία στάδια ονομάζονται δραστικά. Είναι επιθυμητό

να σταματώνται τα spam όσο πιο νωρίς γίνεται ώστε να μην σπαταλώνται διαθέσιμοι πόροι, όπως το εύρος ζώνης, ο αποθηκευτικός χώρος και ο χρόνος του παραλήπτη. Επομένως, πρέπει να δίνεται ιδιαίτερη σημασία στα προληπτικά μέτρα. Ωστόσο, και τα δραστικά μέτρα, όπως είναι οι μηχανισμοί αποκλεισμού και φιλτραρίσματος, είναι πολύ χρήσιμα από τη μεριά του παραλήπτη.

- Τα spam μπορούν να έχουν πολλές διαφορετικές διαδρομές παράδοσης. Για παράδειγμα, ορισμένες φορές οι spammers ιδρύουν τους δικούς τους MTAs και στέλνουν spam στον ESP του παραλήπτη απευθείας. Μία άλλη επιλογή είναι η εκμετάλλευση της υποδομή του ESP για την αποστολή μηνυμάτων μέσω των MTAs του. Αν και κάποια anti-spam μέτρα μπορούν αν ληφθούν ανεξάρτητα από την διαδρομή του spam, υπάρχουν κάποια άλλα, όπως το TCP blocking, που είναι εφαρμόσιμα μόνο αν ο spammer χρησιμοποιεί "κατάλληλες" διαδρομές.

- Τα anti-spam μέτρα μπορούν να ταξινομηθούν λειτουργικά.

- Από πρακτική σκοπιά, τα μέτρα μπορούν να ταξινομηθούν σε βραχυ-, μεσο- και μακρο-πρόθεσμα, ανάλογα με τον χρόνο και την προσπάθεια που χρειάζεται για την εφαρμογή τους. Για παράδειγμα, οι μηχανισμοί φιλτραρίσματος και μπλοκαρίσματος θεωρούνται βραχυπρόθεσμοι, καθώς συνήθως η εφαρμογή τους μπορεί να περιορισθεί στην υποδομή e-mail ενός οργανισμού χωρίς την ανάγκη μεγάλων τροποποιήσεων. Ωστόσο, αυτή η κατηγοριοποίηση είναι κάπως αυθαίρετη και ασαφής επειδή στερείται (αντικειμενικών) κριτηρίων που καθορίζουν σε ποια κατηγορία ανήκει ένα μέτρο.

3.4.1 IP blocking

Όταν ένας χρήστης ξεκινάει μία SMTP σύνδεση, τότε μία TCP/IP σύνδεση εγκαθιδρύεται με τον SMTP server στα στρώματα μεταφοράς και δικτύου. Η διεύθυνση IP του αποστολέα μπορεί να βρεθεί εύκολα και είναι η πρώτη πληροφορία που είναι διαθέσιμη στον server. Ανάλογα με την IP διεύθυνση, ο server έχει τη δυνατότητα να αποφασίσει αν θα δεχτεί ή θα απορρίψει την SMTP σύνδεση.

Αν αυτή η διεύθυνση σχετίζεται με κάποιο spammer, μπορεί η σύνδεση να απορριφθεί. Αυτή η διαδικασία ονομάζεται "blacklisting", καθώς οι ύποπτες IP διευθύνσεις αποθηκεύονται σε *blacklists*. Ορισμένες φορές αποκλείεται ένα εύρος IP διευθύνσεων, για παράδειγμα αν αυτές σχετίζονται με συγκεκριμένο domain ή με συγκεκριμένους ISPs. Παρομοίως, υπάρχουν και *whitelists* οι οποίες σχετίζονται με αξιόπιστους SMTP clients. Αντίθετα με τις blacklists και whitelists, οι *greylists* είναι μία προσέγγιση στην οποία χρησιμοποιούνται οι IP διευθύνσεις ως μέρος

ενός συνόλου πληροφοριών, ώστε να αποφασισθεί η απόρριψη ή η αποδοχή της σύνδεσης.

Το IP blocking μπορεί να εφαρμοσθεί εύκολα και δεν απαιτεί πολλούς πόρους, καθώς η αποδοχή/απόρριψη γίνεται σε πρόωρο στάδιο της SMTP σύνδεσης. Ορισμένα από τα μειονεκτήματα της μεθόδου είναι τα ακόλουθα:

- Το IP blocking δεν είναι αποτελεσματικό αν η διεύθυνση IP έχει πλαστογραφηθεί. Ωστόσο η πλαστογράφηση της IP διεύθυνσης δεν είναι σοβαρό πρόβλημα, καθώς: (1) Επειδή οι SMTP συνδέσεις βασίζονται σε TCP συνδέσεις με αρχική χειραψία τριών σταδίων, η πλαστογράφηση της IP δεν είναι εύκολη και απαιτεί κάποια σχετική γνώση και προσπάθεια. (2) Ένα δίκτυο μπορεί να προστατευθεί από την πλαστογράφηση των IP διευθύνσεων με κάποιες απλές τεχνικές. (3) Το IP blocking συνήθως δεν είναι το μοναδικό anti-spam μέτρο που χρησιμοποιείται από τους σύγχρονους MTAs. Στην πράξη, η πλαστογράφηση της IP, που στοχεύει στην αποστολή spam, παρατηρείται σπάνια.

- Το IP blocking λειτουργεί ευρετικά και, κατ' αρχήν, πάσχει από δύο σφάλματα ταξινόμησης: αν μία non-spam SMTP συναλλαγή απορριφθεί, τότε έχουμε ένα "false-positive", ενώ αν μία spam SMTP συναλλαγή γίνει αποδεκτή, τότε έχουμε ένα "false-negative".

Blacklisting:

Οι blacklists μπορεί να διαφέρουν σε πολλά σημεία. Κάποιες είναι ιδιωτικές (όπως αυτές των ISPs), ενώ κάποιες άλλες παρέχονται από τρίτους είτε δωρεάν είτε επί πληρωμή. Συνήθως, οι blacklists παρέχουν μία τυποποιημένη πρόσβαση σε "realtime" δεδομένα μέσω DNS, σε αυτήν την περίπτωση ονομάζονται DNSBLs. Το "realtime" είναι πολύ σημαντικό, καθώς οι spammers αλλάζουν συχνά "sending hosts". Τα δεδομένα μπορούν να περιέχουν τις IP διευθύνσεις των hosts γνωστών spammers, των open relays ή αυτών που χρησιμοποιούνται παράνομα από τρίτους. Ένα άλλο στοιχείο στο οποίο μπορεί να διαφέρουν οι DNSBLs είναι στην πολιτική τους, η οποία περιέχει πληροφορίες σχετικά με το βαθμό ευθύνης, τον τρόπο με τον οποίο οι IP διευθύνσεις εισάγονται και εξάγονται από την βάση.

Μία διαδεδομένη μέθοδος εισαγωγής IP διευθύνσεων σε blacklists είναι να πραγματοποιηθεί ανάλυση των συχνοτήτων των εισερχομένων e-mails ανά host. Οι spammers συχνά στέλνουν ένα τεράστιο αριθμό από e-mails σε συγκεκριμένο e-mail server σε μικρή χρονική περίοδο, που έχει σαν αποτέλεσμα μια εξαιρετικά υψηλή συχνότητα. Οι host που έχουν με τέτοια συμπεριφορά μπορούν να αποκλείονται. Όμως, οι whitelists είναι απαραίτητες

σε αυτήν την περίπτωση ώστε να λαμβάνονται υπόψη "κανονικά" μαζικά e-mails, όπως είναι τα newsletters.

Τα κύρια μειονεκτήματα των blacklists είναι ότι:

1. δεν μπορούν ποτέ να είναι εξαντλητικές, καθώς οι spammers χρησιμοποιούν συγκεκριμένες IP διευθύνσεις για μικρό χρονικό διάστημα, άρα οι blacklists δεν μπορούν ποτέ να είναι πλήρως ενημερωμένες.
2. περιλαμβάνουν συχνά διευθύνσεις ή εύρος διευθύνσεων που ανήκουν σε κάποιον ESP ή ISP, γιατί κάποιος spammer χρησιμοποιεί την υποδομή του, άρα μέχρι να αντιληφθούν οι διαχειριστές το πρόβλημα και να το επιλύσουν χιλιάδες κανονικά e-mails χάνονται.
3. οι DNSBLs επιφέρουν ένα αυξημένο φόρτο στο διαδίκτυο και κάνουν το DNS έναν καθοριστικής σημασίας πόρο, στοιχείο αρνητικό καθώς το DNS είναι ευάλωτο από άποψη ακεραιότητας και πιστοποίησης (DNS spoofing).

Whitelisting:

Όπως και οι blacklists, οι whitelists μπορούν να διατηρούνται τοπικά ή να παρέχονται δημόσια και όταν δημοσιεύονται μέσω DNS ονομάζονται DNSWLs. Αντιθέτως με τις blacklists, το να είναι συνεχώς ενημερωμένες δεν είναι τόσο σημαντικό. Οι whitelists σπανίως είναι αποτελεσματικές από μόνες τους, καθώς σε αυτή την περίπτωση το ποσοστό των false-positives είναι εξαιρετικά υψηλό (e-mails από άγνωστους αποστολείς απορρίπτονται). Πρέπει να χρησιμοποιούνται συμπληρωματικά με άλλες μεθόδους ως πρώτου επιπέδου μέτρο, που σημαίνει ότι e-mails που προέρχονται από κάποιον host της whitelist δε χρειάζεται να ελεγχθούν από άλλα anti-spam μέτρα.

Greylisting:

Κάθε συναλλαγή e-mail αρχικά απορρίπτεται και ένα σύνολο πληροφοριών (παραμέτρων) που χαρακτηρίζουν αυτήν την ανεπιτυχή συναλλαγή αποθηκεύονται. Αν, σε ένα συγκεκριμένο χρονικό όριο, ο SMTP χρήστης προσπαθήσει να πραγματοποιήσει την αποτυχημένη συναλλαγή ξανά, ο server αποδέχεται την συναλλαγή ταιριάζοντας επιτυχώς τις παραμέτρους της συναλλαγής με τις αποθηκευμένες παραμέτρους. Οι greylists βασίζονται κυρίως στην υπόθεση ότι οι περισσότερες πηγές spam δεν στέλνουν ξανά το e-mail -πιστεύεται ότι οι spammers θεωρούν πως τα "bounced emails" προκύπτουν από μη έγκυρες e-mail διευθύνσεις- σε αντίθεση με τα "κανονικά" συστήματα e-mail.

Ωστόσο, υπάρχουν ορισμένα μειονεκτήματα στη μέθοδο αυτή και η μακροπρόθεσμη αποτελεσματικότητά της φαίνεται περιορισμένη:

1. Για κάθε συναλλαγή e-mail, ο παραλαμβάνων MTA στις περισσότερες περιπτώσεις αποθηκεύει μία τριάδα πληροφοριών που αποτελείται από την IP και άλλα "envelope data". Έτσι, μία SMTP συναλλαγή γίνεται αποδεκτή ή απορρίπτεται όταν όλες οι πληροφορίες είναι διαθέσιμες. Σε αντίθεση με τις blacklists και whitelists, αυτή η διαδικασία χρειάζεται λίγο παραπάνω χρόνο και είναι αναγκαία η ύπαρξη αποθηκευτικού χώρου.
2. Οι greylists έχουν ως αποτέλεσμα την αύξηση του φόρτου των e-mails καθώς τα περισσότερα θα πρέπει να στέλνονται δύο φορές.
3. Το κύριο πρόβλημα των greylists είναι ότι υποθέτουν πως οι spammers δεν επαναλαμβάνουν την αποστολή των e-mails. Έτσι, οι spammers μπορούν εύκολα να παρακάμψουν τις greylists.
4. Αν οι e-mail hosts δεν εφαρμόζουν την επαναποστολή των e-mails ή αν υπάρχουν πολλοί e-mail hosts σε ένα σύστημα, τότε τα μηνύματα δεν περνάνε ποτέ την greylist και χάνονται.
5. Στα σημερινά e-mails επιτρέπεται η χρήση διευθύνσεων στην εντολή MAIL FROM χωρίς την άδεια του κατόχου τους, με αποτέλεσμα να στέλνονται ειδοποιήσεις ή bounce e-mails σε παραλήπτες χωρίς να έχουν επίγνωση.

3.4.2 Filtering

Τα φίλτρα λειτουργούν ευρετικά και προσπαθούν να κατατάξουν τα e-mails σε δύο κατηγορίες, spam και ham. Μπορούν να εφαρμοσθούν από τον ESP του αποστολέα ή του παραλήπτη ή από τον ίδιο τον παραλήπτη. Οι μέθοδοι που χρησιμοποιούνται στα φίλτρα μπορεί να διαφέρουν στο περιεχόμενο που ελέγχεται, στη μέθοδο που χρησιμοποιείται ή στη μορφή συνεργασίας. Κάποια φίλτρα ελέγχουν μόνο την επικεφαλίδα του e-mail, ενώ άλλα ελέγχουν και το περιεχόμενο ή ακόμα και άλλα "envelope data". Υπάρχει, επίσης, ένα ευρύ φάσμα μεθόδων που χρησιμοποιούνται στα φίλτρα, αφού μπορεί να χρησιμοποιηθεί οποιοσδήποτε αλγόριθμος ταξινόμησης κειμένου ή αλγόριθμοι από το πεδίο του machine learning, καθώς το filtering αποτελείται από δύο φάσεις, την *εκμάθηση (training)* και την *ταξινόμηση (classifying)*. Τέλος, κάποια φίλτρα είναι "συνεργατικά", δηλαδή δεν είναι συγκεντρωτικά και περιλαμβάνουν πολλούς servers που μοιράζονται πληροφορίες για τα spam.

Για να είναι αποτελεσματικό ένα φίλτρο πρέπει να ικανοποιούνται ορισμένες προϋποθέσεις:

1. Τα φίλτρα πρέπει να "εκπαιδεύονται" συνέχεια, καθώς οι spammers τείνουν να αλλάζουν συχνά τα e-mails τους ως προς τη δομή και το περιεχόμενο.

2. Τα φίλτρα πρέπει να "εκπαιδεύονται" ατομικά, γιατί διαφορετικοί οργανισμοί και άτομα ίσως χρησιμοποιούν διαφορετική ορολογία. Για παράδειγμα, για ένα νοσοκομείο, τα ονόματα ιατρικών προϊόντων είναι λιγότερο ύποπτα από ότι για ένα μεμονωμένο χρήστη.

3. Τα φίλτρα πρέπει να είναι "ανθεκτικά". Για παράδειγμα, οι spammers προσπαθούν να αποφύγουν τα φίλτρα και μία μέθοδος που χρησιμοποιούν είναι να διαχωρίζουν ή να γράφουν ανορθόγραφα τις λέξεις, ώστε τα φίλτρα να μην τις αναγνωρίζουν. Επίσης, πρέπει να αντιμετωπίζουν το πρόβλημα που προκύπτει όταν τα ham και τα spam γίνονται όλο και πιο όμοια.

Ωστόσο, όλα τα φίλτρα έχουν κάποια μειονεκτήματα, τα οποία είναι ανεξάρτητα της μεθόδου που χρησιμοποιείται:

- Ένα κύριο πρόβλημα είναι ότι δεν είναι δυνατόν ένα φίλτρο να είναι 100% ακριβές, πάντοτε θα υπάρχουν false-positives και false-negatives.
- Τα φίλτρα, ιδιαίτερα αυτά που ελέγχουν το σώμα του e-mail, καταναλώνουν αρκετούς πόρους.
- Όσο περισσότερο μοιάζουν τα spam με ham τόσο λιγότερο αποτελεσματικά είναι τα φίλτρα και οι spammers σήμερα είναι αρκετά ικανοί στο να δημιουργούν αυτήν την ομοιότητα.
- Οι μηχανισμοί των φίλτρων μειώνουν την πιθανότητα ένα spam να παραδοθεί στον παραλήπτη. Όμως, αυτό μπορεί να ενθαρρύνει τους spammers να στέλνουν περισσότερα e-mails σε μια προσπάθεια να παρακάμψουν το φίλτρο. Συμπερασματικά, τα φίλτρα έχουν αρνητική επίδραση στο πρόβλημα της κατανάλωσης πόρων λόγω της ύπαρξης των spam.

Στη συνέχεια ακολουθεί μία περιγραφή συγκεκριμένων μεθόδων και συστημάτων:

Rule-based filtering:

Όταν χρησιμοποιούνται κανόνες ως φίλτρα, τότε αυτοί μπορεί να έχουν δημιουργηθεί χειροκίνητα από τον χρήστη ή αυτόματα. Παράδειγμα ενός κανόνα είναι το ακόλουθο:

spam ← (subject contains "VIAGRA") and (body contains "Dear Sir")

Ένα κύριο μειονέκτημα των ruled-based filters είναι ότι μπορούν εύκολα να παρακαμφθούν αν οι spammers αλλάξουν ελαφρώς τον τρόπο γραφής (για παράδειγμα να γραφεί "V1AGRA" αντί για "VIAGRA") ή χρησιμοποιήσουν φράσεις που βρίσκονται συχνά σε ham.

Signature-based filtering:

Αυτή η μέθοδος δεν ασχολείται με ολόκληρα μηνύματα ή συγκεκριμένα tokens, αλλά μειώνει το μήνυμα σε μία υπογραφή. Αυτό μπορεί να γίνει με διάφορους τρόπους, όπως για παράδειγμα με τη χρήση hash functions. Ωστόσο, αυτές οι μέθοδοι πρέπει να έχουν αντοχή σε μικρές αλλαγές που μπορεί να υπάρξουν στα spam, για παράδειγμα ένα πιο προσωπικό χαιρετισμό, και να ενημερώνονται και πιθανώς να διανέμονται πολύ συχνά καθώς το περιεχόμενο των spam αλλάζει γρήγορα. Η γενική μέθοδος ελέγχου ενός e-mail είναι να κατασκευάζεται η υπογραφή του και στη συνέχεια να συγκρίνεται με υπογραφές γνωστών spam.

Τα σχήματα αυτά μπορεί να διαφέρουν όχι μόνο στη μέθοδο που χρησιμοποιείται για την κατασκευή της υπογραφής, αλλά και σε άλλα στοιχεία. Μπορούν να είναι client- ή server-based, δηλαδή οι χρήστες ή οι διαχειριστές του server αντίστοιχα μπορούν να προσδιορίσουν τα spam. Επίσης, μπορούν να είναι συνεργατικά, σε αυτή την περίπτωση χρησιμοποιούνται συχνά P2P δίκτυα για τη διανομή των υπογραφών, ή μη συνεργατικά. Στην περίπτωση που οι χρήστες είναι αυτοί που αναφέρουν τα spam, πρέπει να ορίζεται ένα threshold, το οποίο πρέπει να υπερβεί ο αριθμός των αναφορών για να θεωρηθεί το μήνυμα spam, γιατί οι εκτιμήσεις ενός χρήστη μπορεί να διαμοιράζονται μεταξύ μικρού αριθμού χρηστών οδηγώντας σε μεγάλο ποσοστό false-positive.

Bayesian filtering:

Τα στατιστικά φίλτρα βασιζόμενα στο θεώρημα Bayes της θεωρίας πιθανοτήτων θεωρούνται χρήσιμα ήδη από το 1998 [15], ενώ είναι ακόμα αρκετά δημοφιλή και εφαρμόζονται ευρέως. Το θεώρημα Bayes είναι το εξής:

$$P(S|M) := \frac{P(M|S) \times P(S)}{P(M)}$$

Κάθε μήνυμα αντιπροσωπεύεται από ένα διάνυσμα $\overrightarrow{x} =< w_1, w_2, ..., w_n >$ όπου τα $w_1, w_2, ..., w_n$ είναι οι τιμές των χαρακτηριστικών $X_1, X_2, ..., X_n$. Συγκεκριμένα, $w_i = 1$ αν το χαρακτηριστικό που συμβολίζεται με X_i εμφανίζεται στο μήνυμα, αλλιώς $w_i = 0$ [2]. Τα χαρακτηριστικά αυτά μπορούν να είναι, για παράδειγμα, μεμονωμένες λέξεις και ονομάζονται *tokens*. Για να διευκρινισθεί η χρήση του θεωρήματος στα Bayesian filters, χρησιμοποιείται το ακόλουθο παράδειγμα: Έστω ότι S είναι το ενδεχόμενο "το μήνυμα είναι spam" και M το ενδεχόμενο "το μήνυμα περιέχει το token 'υποθήκη' ", τότε το $P(S|M)$), που μπορεί να υπολογισθεί από γνωστές πιθανότητες σύμφωνα με το παραπάνω θεώρημα, συμβολίζει την πιθανότητα

ένα μήνυμα, που ανήκει στο ιστορικό των μηνυμάτων και περιέχει το token ‘υποθήκη’, να είναι spam.

Στην πράξη, είναι αναγκαίο να λαμβάνονται υπόψη πολλαπλά tokens στο θεώρημα Bayes:

$$P(S|w_1 \wedge w_2 \wedge ... \wedge w_n) = \frac{P(w_1 \wedge w_2 \wedge ... \wedge w_n|S) \times P(S)}{P(w_1 \wedge w_2 \wedge ... \wedge w_n)}$$

με w_i = το ενδεχόμενο το token i να υπάρχει στο e-mail που εξετάζεται. Μετά από κάποιους μετασχηματισμούς λαμβάνουμε την σχέση:

$$P(S|w_1 \wedge w_2 \wedge ... \wedge w_n) = \frac{\prod_i P(w_i|w_{i+1} \wedge ... \wedge w_n \wedge S) \times P(S)}{P(w_1 \wedge w_2 \wedge ... \wedge w_n)}$$

Ένα Bayesian filter ονομάζεται “naïve” αν θεωρεί την στοχαστική ανεξαρτησία των συμβάντων των tokens $w_i, i = 1, 2, ..., n$. Τότε, η παραπάνω σχέση απλοποιείται:

$$P(S|w_1 \wedge w_2 \wedge ... \wedge w_n) = \frac{\prod_i P(w_i|S) \times P(S)}{P(w_1 \wedge w_2 \wedge ... \wedge w_n)}$$

Για να ληφθούν υπόψη αλλαγές στα κείμενα και στις έννοιες, ένα Bayesian filter μπορεί να “εκπαιδευτεί” προσθέτοντας νέα e-mails στο ιστορικό μηνυμάτων, στοιχείο που προσαρμόζει *αυτόματα* τις πιθανότητες και αποτελεί το κύριο πλεονέκτημα του σε σχέση με τα rule-based φίλτρα [2].

Ένα εργαλείο που χρησιμοποιεί Bayesian filter είναι το SpamBayes [17], το οποίο μπορεί να χρησιμοποιηθεί ως plug-in σε διάφορους mail clients (π.χ. στο Microsoft Outlook). Το SpamBayes βασίστηκε στο άρθρο του Paul Graham *A Plan for Spam* [8], στο οποίο παρουσιάζεται ένα σχήμα για “naïve Bayesian filter”. Ωστόσο, το σχήμα αυτό παρουσιάζει αρκετά μειονεκτήματα. Τα κυριότερα από αυτά είναι ότι το σχήμα απαιτεί τη χρήση κάποιων “magic numbers” και κάποιων “fuzz factors”, που είναι δύσκολο να προσδιορισθούν, ενώ έχει την τάση να παράγει τιμές πιθανοτήτων είτε 1 (σίγουρα spam) είτε 0 (σίγουρα ham), αντί να παράγει και τιμές που δείχνουν αβεβαιότητα (δηλαδή, ότι ένα μήνυμα θεωρείται “unsure”), στοιχείο που οδηγεί σε false-negatives, αλλά και σε false-positives. Στην πρώτη περίπτωση, το φίλτρο χαρακτηρίζει ως ham μηνύματα που στην πραγματικότητα είναι spam και στην δεύτερη, χαρακτηρίζει τα ham ως spam. Το δεύτερο είδος λαθών είναι πολύ σοβαρότερο από το πρώτο, καθώς μπορεί να οδηγήσει στην απόρριψη κανονικών μηνυμάτων.

Για να αντιμετωπισθούν αυτά τα προβλήματα προτάθηκαν διάφορες εναλλακτικές προσεγγίσεις, από τις οποίες αυτή που επικράτησε, αρχικά, ήταν αυτή του Gary

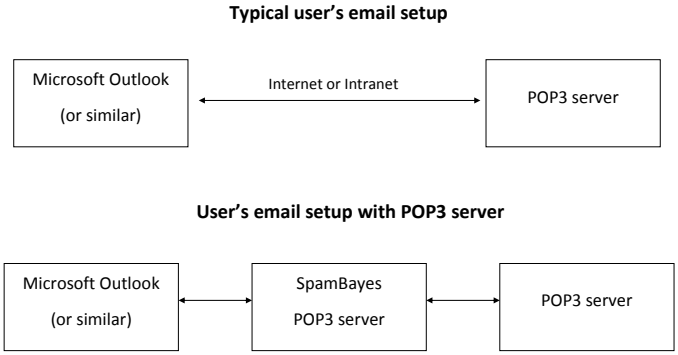
Robinson η οποία κάνει χρήση του Κεντρικού Οριακού Θεωρήματος (Κ.Ο.Θ.). Το σχήμα αυτό παράγει δύο εσωτερικά αποτελέσματα, όπου το ένα δείχνει την πιθανότητα το μήνυμα να είναι ham και το άλλο την πιθανότητα να είναι spam. Επομένως, υπάρχει περίπτωση να επιστραφεί η απάντηση "unsure" αν οι δύο αυτές πιθανότητες είναι εξίσου χαμηλές ή υψηλές. Στη συνέχεια, η προσέγγιση του Κ.Ο.Θ. αντικαταστάθηκε από ένα νέο σχήμα που χρησιμοποιεί πιθανότητες X^2, αλλά λειτουργεί παρόμοια με αυτό του Κ.Ο.Θ.

Το σύστημα του SpamBayes αποτελείται από οχτώ κύριες συνιστώσες:

1. **Μία βάση δεδομένων:** Στην ουσία, πρόκειται για μία συλλογή λέξεων και τις σχετιζόμενες με αυτές πιθανότητες. Για παράδειγμα, μέσω αυτής της βάσης μπορεί να προκύψει ότι ένα μήνυμα που περιέχει τη λέξη "Viagra" έχει πιθανότητα 98% να είναι spam και 2% να είναι ham. Αυτή η βάση δεδομένων προκύπτει από το training του φίλτρου, στο οποίο οι πιθανότητες προσαρμόζονται ανάλογα, και αποθηκεύεται στο αρχείο hammie.db ή στο default_bayes_database (στο plug-in του Outlook).

2. **Ο tokenizer/classifier:** Αυτός είναι ο πυρήνας του συστήματος. Ο tokenizer χωρίζει το μήνυμα σε tokens. Στη σημερινή έκδοση του SpamBayes, τα tokens είναι οι λέξεις από τις οποίες αποτελείται το μήνυμα αφού πρώτα αφαιρεθούν οι HTML tags και άλλα τμήματα, όπως είναι οι εικόνες που μπορεί να περιέχονται στο μήνυμα. Ο classifier ελέγχει αυτά τα tokens ώστε να προσδιορίσει αν το μήνυμα φαίνεται να είναι spam ή όχι. Η χρήση του tokenizer/classifier δεν είναι άμεση, αλλά σχετίζεται με τη λειτουργία άλλων στοιχείων του συστήματος.

3. **Ο POP3 proxy:** Αυτός βρίσκεται μεταξύ του mail client και του incoming e-mail server και προσθέτει την επικεφαλίδα κατάταξης στα e-mails καθώς αυτά κατεβάζονται. Στο ακόλουθο διάγραμμα, παρουσιάζεται ο τυπικός τρόπος λειτουργίας του mail client και ο τρόπος λειτουργίας του με τη χρήση του POP3 server.



Ο POP3 server λειτουργεί είτε στον ISP στην περίπτωση του Internet mail, είτε σε κάποιο εσωτερικό δίκτυο στην περίπτωση του εταιρικού (corporate) mail. Επομένως, αν η αρχική ρύθμιση του mail client είναι να συνομιλεί, για παράδειγμα, με τον "pop3.my-isp.com", η νέα ρύθμιση είναι ο mail client να συνομιλεί με τον proxy και, στη συνέχεια, ο proxy να συνομιλεί με τον "pop3.my-isp.com". Ο POP3 proxy μπορεί να βρίσκεται στον προσωπικό υπολογιστή του χρήστη (σε αυτή την περίπτωση ο mail client ρυθμίζεται ώστε να συνομιλεί με τον localhost), στον ίδιο υπολογιστή που βρίσκεται ο POP3 server ή σε οποιονδήποτε άλλο υπολογιστή. Τέλος, στην περίπτωση πολλαπλών λογαριασμών e-mail, υπάρχει η δυνατότητα ο proxy να συνομιλεί με πολλούς POP3 servers.

4. **Ο SMTP proxy:** Αυτός βρίσκεται μεταξύ του mail client και του outgoing e-mail server. Κάθε μήνυμα που στέλνεται στο spambayes_spam@localhost ή στο spambayes_ham@localhost διακόπτεται και χρησιμοποιείται για να γίνει training του φίλτρου. Η αλλαγή του τρόπου λειτουργίας του mail client χωρίς και με τη χρήση του SMTP proxy είναι παρόμοια με αυτήν της περίπτωσης του POP3 proxy.

5. **Το web interface:** Πρόκειται για έναν server που λειτουργεί παράλληλα με τους POP3 proxy, SMTP proxy και το IMAP filter και δίνει τη δυνατότητα ελέγχου μέσω Internet. Επιτρέπει το ανέβασμα μηνυμάτων ώστε να γίνει training ή classification και σε αυτόν μπορούν να γίνουν ερωτήματα σχετικά με τις πιθανότητες που βρίσκονται στη βάση δεδομένων. Κατά την έναρξη της χρήσης του συστήματος, τα περισσότερα e-mail κατατάσσονται ως "unsure" και τα λάθη είναι συχνά (εκτός και αν γίνει training σε προϋ-

πάρχουσα συλλογή μηνυμάτων). Ωστόσο, κρατούνται αντίγραφα όλων των μηνυμάτων και μέσω του web interface μπορούν αυτά να χρησιμοποιηθούν για να γίνει training του φίλτρου επιλέγοντας σε ποια κατηγορία ανήκει το κάθε μήνυμα. Το web interface κατατάσσει αυτόματα τα μηνύματα στην κατηγορία που πιστεύει ότι ανήκουν και έτσι ο χρήστη απλώς πρέπει να διορθώσει τα λάθη που γίνονται σε αυτή τη διαδικασία, ώστε το φίλτρο να βελτιωθεί.

6. **Το Outlook plug-in:** Για τους χρήστες του Outlook, υπάρχει η δυνατότητα το σύστημα να ελέγχεται μέσω του Outlook. Μπορούν να ρυθμίσουν το plug-in να ελέγχει συγκεκριμένους φακέλους για νέα μηνύματα, να τοποθετεί σε συγκεκριμένο φάκελο τα μηνύματα που κατατάσσονται ως "unsure" ή ως spam. Επιπλέον, περιέχει γραφικό περιβάλλον για το training του φίλτρου.

7. **Το filter script:** Το script αυτό είναι υπεύθυνο για τρείς διαφορετικές εργασίες: το command-line training, το procmail filtering και το XML-RPC. Το command-line training μπορεί να χρησιμοποιηθεί αν υπάρχουν δύο αρχεία σε Unix mailbox format (mbox) από τα οποία το ένα περιέχει μόνο spam και το άλλο μόνο ham. Το procmail filtering μπορεί να χρησιμοποιηθεί σε έναν mail server στην περίπτωση που ο MDA είναι ο procmail ρυθμίζοντας τον procmail να καλεί το SpamBayes προτού παραδώσει τα e-mails στα αντίστοιχα mailboxes. Τέλος, το SpamBayes μπορεί να λειτουργήσει ως XML-RPC server, ώστε να επιτρέπει σε ένα προγραμματιστή να γράψει κώδικα που χρησιμοποιεί κάποιο remote server για να κατατάσσει τα e-mails μέσω προγραμμάτων.

8. **Το IMAP filter:** Αν τα e-mails βρίσκονται σε κάποιον IMAP server, χρησιμοποιείται αυτή η συνιστώσα για να γίνει η κατάταξη των μηνυμάτων. Ο χρήστης μπορεί να προσδιορίσει τους φακέλους που περιέχουν ham και τους φακέλους που περιέχουν spam, ώστε να γίνει το training του φίλτρου. Επίσης, μπορούν να προσδιορισθούν οι φάκελοι στους οποίους ο χρήστης επιθυμεί να γίνει κατάταξη των e-mails και οι φάκελοι στους οποίους επιθυμεί να τοποθετηθούν τα "unsure" και τα "suspected spam". Όταν λαμβάνονται νέα μηνύματα το φίλτρο θα τα τοποθετεί στον κατάλληλο φάκελο (τα ham παραμένουν στον αρχικό φάκελο).

3.4.3 TCP blocking

Σε αντίθεση με το IP blocking, το TCP blocking δεν στοχεύει στην ανίχνευση του spam από την πλευρά του παραλήπτη, αλλά περισσότερο στην πρόληψη του

spam από την πλευρά του αποστολέα, το οποίο είναι προτιμητέο. Επειδή τα SMTP e-mails κατευθύνονται στην θύρα 25, οι ISPs και διάφορες εταιρίες συχνά σταματούν όλη την (εξερχόμενη) TCP κυκλοφορία σε αυτή τη θύρα. Πρόκειται για μία απλή και εύκολα εφαρμόσιμη επιλογή ώστε να εμποδιστούν τα spam που στέλνονται από SMTP clients απευθείας στον MX host. Αυτή η μέθοδος αντιμετωπίζει τα spam στο στρώμα μεταφοράς και αναφέρεται κυρίως σε καταστάσεις στις οποίες οι spammers δημιουργούν SMTP μηχανές στους υπολογιστές τους ή σε εκμεταλλευόμενους υπολογιστές. Ωστόσο, το blocking της θύρας 25 μπορεί να δημιουργήσει προβλήματα στους πελάτες των ISPs που θέλουν να τρέξουν τον δικό τους e-mail server ή να επικοινωνήσουν με κάποιο e-mail server σε κάποιο απομακρυσμένο δίκτυο για να υποβάλλουν τα e-mails τους. Για να επιτραπεί στους πελάτες να εντοπίσουν τον SMTP server τους, συχνά η "e-mail submission" (συνήθως χρησιμοποιώντας την θύρα 587) και το SMTP-AUTH προσφέρονται ως μηχανισμοί πιστοποίησης.

3.4.4 Πιστοποίηση

Τα σχήματα πιστοποίησης χωρίζονται σε τρεις κατηγορίες. Η πρώτη περιέχει τις SMTP επεκτάσεις, η δεύτερη στηρίζεται στην κρυπτογραφική πιστοποίηση και αναφέρεται σε ασφάλεια από άκρη σε άκρη (end-to-end security), ενώ η τρίτη περιλαμβάνει προτάσεις πιστοποίησης μονοπατιού (path authentication), οι οποίες προσδιορίζουν το όνομα του domain του τελευταίου MTA ή του τελευταίου hop. Αυτή η κατηγορία περιλαμβάνει και μία κατηγορία πρωτοκόλλων που ονομάζονται "Lightweight MTA Authentication Protocols"

SMTP επεκτάσεις:

Επεκτάσεις του πρωτοκόλλου, όπως το SMTP-AUTH, "SMTP after POP" και "SMTP after IMAP", παρέχονται ώστε να υποστηρίξουν την πιστοποίηση των χρηστών ή των SMTP clients. Αυτές οι προσεγγίσεις αντιμετωπίζουν το πρόβλημα της πλαστογράφησης των ονομάτων των αποστολέων και/ή των ονομάτων των hosts και έχουν ως στόχο να επιρρίψουν ευθύνες στους ενόχους. Ωστόσο, τα ονόματα των χρηστών και οι κωδικοί τους γενικά δεν αποθηκεύονται με ασφάλεια στους υπολογιστές των χρηστών και έτσι είναι διαθέσιμα στον κακόβουλο κώδικα των zombie PCs. Το SMTP-AUTH μπορεί να χρησιμοποιηθεί για πιστοποίηση ενός χρήστη ή ενός host, αλλά αν τα spam έχουν ήδη φτάσει στον server ή στον λογαριασμό, τότε αυτό είναι άχρηστο.

Κρυπτογραφική πιστοποίηση:

Οι προσεγγίσεις της κρυπτογραφικής πιστοποίησης αντιμετωπίζουν γενικά

το πρόβλημα της πλαστογράφησης e-mail. Μία ψηφιακή υπογραφή προστίθεται στο μήνυμα και γίνεται η επιβεβαίωσή της από τον παραλήπτη. Αυτή η ψηφιακή υπογραφή μπορεί να βασίζεται σε σχήματα δημοσίου κλειδιού ή σε συμμετρική κρυπτογράφηση. Για την επιβεβαίωση της υπογραφής χρησιμοποιείται το σώμα του αρχικού υπογεγραμμένου κειμένου, καθώς η τιμή του μέσω μίας hash function συγκρίνεται με την τιμή που προκύπτει από την αποκρυπτογράφηση της υπογραφής. Οι προσεγγίσεις διαφέρουν, επίσης, στο είδος της ταυτότητας που πιστοποιείται: κάποιες αναφέρονται στους χρήστες ή στις διευθύνσεις, ενώ άλλες προσπαθούν να επαληθεύσουν το domain ή τον ESP.

Μία προσέγγιση κρυπτογραφικής πιστοποίησης παρουσιάζεται από τους Tompkins και Handley [21], οι οποίοι θεωρούν πως το πρόβλημα του spam μπορεί να λυθεί αν αναγνωρισθεί η σημασία της πιστοποίησης των e-mails και της παραχώρησης αδειών. Τα πλεονεκτήματα αυτής της προσέγγισης είναι ότι εξαλείφεται το πρόβλημα των harvested e-mail διευθύνσεων από ιστοσελίδες, της μεταφοράς και της πώλησης διευθύνσεων ή της αποτυχίας του blocking λόγω αλλαγής τοποθεσίας των spammers. Το πλάνο τους συμπληρώνεται από την πρόταση να αποκτήσουν οι e-mail clients τις απαραίτητες δυνατότητες για την διαχείριση των δημοσίων κλειδιών, ώστε η πρότασή τους να μπορεί να υλοποιηθεί απλώς με την ενημέρωση και την εκπαίδευση των χρηστών e-mail.

Σύμφωνα με αυτή την πρόταση, κάθε χρήστης διατηρεί ένα κατάλογο δημοσίων κλειδιών των χρηστών από τους οποίους επιτρέπεται να λάβει e-mails. Αν ληφθεί κάποιο e-mail από χρήστη που δεν βρίσκεται σε αυτό τον κατάλογο, το μήνυμα αυτό μπορεί απλώς να απορριφθεί ή να σταλεί ένα νέο μήνυμα στον αποστολέα ενημερώνοντάς τον ότι πρέπει το δημόσιο κλειδί του να γίνει αποδεκτό από τον παραλήπτη προτού το e-mail παραδοθεί. Ο χρήστης, επιπλέον, θα μπορεί να ρυθμίσει το λογαριασμό του ώστε να λαμβάνει τα e-mails των οποίων το κλειδί έχει την ετικέτα "έγκυρο" (δηλαδή την υπογραφή κάποιου ήδη γνωστού του χρήστη). Προτείνεται, επίσης, η ύπαρξη φορμών κειμένου, όπου μέσω κάποιας ιστοσελίδας οι χρήστες θα μπορούν να λάβουν e-mails από αγνώστους, για παράδειγμα καθηγητές ή εκπροσώπους (για να αποφευχθεί η χρήστη "bots" μπορούν να ενσωματώνονται κάποια CAPTCHA tests σε αυτή τη διαδικασία). Τέλος, κάθε χρήστης μπορεί να έχει πλήθος δημοσίων κλειδιών, καθένα από τα οποία μπορεί να έχει διαφορετική διάρκεια ή να αναφέρεται σε διαφορετική ομάδα αποστολέων.

Τα κυριότερα μειονεκτήματα της κρυπτογραφικής πιστοποίησης σχετίζονται με τα εξής θέματα [16]:

- Κυρίως αντιμετωπίζουν το ζήτημα της πλαστογράφησης e-mail και, επομένως, δεν έχουν αποτέλεσμα αν δεν υπάρχουν πλαστογραφημένα στοιχεία στα e-mails ή αν τα στοιχεία τους δεν μπορούν να κατηγοριοποιηθούν ως πλαστογραφημένα.
- Από την πλευρά του παραλήπτη, είτε ο MTA του παρόχου είτε ο MUA του χρήστη μπορεί να εντοπίσει ένα e-mail με πλαστογραφημένα στοιχεία. Αν πρόκειται για spam, τότε απορρίπτεται, αλλά η απόφαση δεν μπορεί να ληφθεί προτού το e-mail ληφθεί και κατεβαστεί ολόκληρο, ώστε η hash τιμή του να συγκριθεί με αυτή της αποκρυπτογραφημένης ψηφιακής υπογραφής. Ωστόσο, αυτό σημαίνει ότι ήδη πολλοί πόροι έχουν καταναλωθεί.
- Επειδή η ψηφιακή υπογραφή βασίζεται σε όλα ή στα περισσότερα δεδομένα του μηνύματος, οι κρυπτογραφικές υπογραφές μπορεί να αντιμετωπίζουν προβλήματα στην επαλήθευσή τους αν το μήνυμα λαμβάνεται μέσω ενδιάμεσων sites, διότι ορισμένα ενδιάμεσα συστήματα τροποποιούν το μήνυμα (για παράδειγμα από μία κωδικοποίηση σε κάποια άλλη). Στις σημερινές υποδομές διαδικτύου, το μεγαλύτερο ζήτημα με τη διατήρηση των υπογραφών τίθεται από την επεξεργασία μηνυμάτων στις mailing lists, καθώς πολλές από αυτές δεν αναμεταδίδουν απλώς το μήνυμα, αλλά, επίσης, αλλάζουν το θέμα στο πεδίο επικεφαλίδας προσθέτοντας τη λέξη "[list]" ή προσθέτουν στο σώμα του μηνύματος πληροφορίες ώστε οι παραλήπτες να γνωρίζουν ότι πρόκειται για μήνυμα που ήρθε μέσω της λίστας.
- Προτάσεις που αναφέρουν πιστοποίηση σε επίπεδο domain δεν επιτρέπουν την επίρριψη ευθυνών σε επίπεδο χρήστη. Επομένως, είναι πιθανό να κατηγορηθεί μία οργάνωση ως πηγή spam, αλλά όχι ο συγκεκριμένος χρήστης για τον οποίο στέλνει τα spam η οργάνωση. Αυτό σημαίνει ότι οι αποφάσεις αποδοχής/απόρριψης γίνονται σε επίπεδο domain και ως εκ τούτου μπορεί να κατηγορηθούν αθώοι χρήστες. Προτάσεις που αναφέρουν πιστοποίηση σε επίπεδο χρήστη απαιτούν την εφαρμογή κρυπτογραφίας με τη χρήση ασφαλών διαδικασιών και συσκευών από κάθε χρήστη. Αυτό, όμως, όχι μόνο απαιτεί αυξημένη προσπάθεια και πρόσθετο κόστος για τους χρήστες, λόγω των ασφαλών συσκευών, όπως των καρτών και των αναγνωριστών καρτών (card readers), αλλά και την παροχή μίας υποδομής διαχείρισης των κλειδιών.
- Προκειμένου να γίνει εφικτή η επικοινωνία μέσω e-mail σε παγκόσμιο επίπεδο, είναι απαραίτητο να υπάρξουν τυποποιημένες μορφές δεδομένων των κλειδιών και των πιστοποιητικών, αλγόριθμοι κρυπτογράφησης και να επιλυθούν τα θέματα υποδομής ώστε όλοι οι χρήστες

e-mail να μπορούν να επικοινωνήσουν μεταξύ τους ανεξάρτητα από την υλοποίηση του ESP τους. Αυτό, ωστόσο, προϋποθέτει τουλάχιστον τη διαλειτουργικότητα διαφορετικών κρυπτογραφικών περιβαλλόντων. Όλο αυτό, όμως, είναι μία δύσκολη υπόθεση. Χαρακτηρισικό παράδειγμα της δυσκολίας εφαρμογής της πρότασης είναι το γεγονός ότι οι PKIs (public-key infrastructures) δεν αναπτύχθηκαν ποτέ επιτυχώς στα πλαίσια του ιδιαίτερα ετερογενούς Internet.

Πιστοποίηση μονοπατιού:

Προκειμένου να αποφευχθεί η κρυπτογραφική πιστοποίηση, έχει προταθεί μία ασθενέστερη μορφή (κυρίως βασισμένη σε DNS) πιστοποίησης μονοπατιού. Η ιδέα της πιστοποίησης μονοπατιού είναι ότι γενικά αν ο προορισμός επαληθεύσει τον προηγούμενο SMTP client και μπορεί να εμπιστευθεί το αποτέλεσμά του, και αν ο προηγούμενος SMTP client επαληθεύει τον αρχικό αποστολέα, τότε ο αρχικός αποστολέας μπορεί να θεωρηθεί επιβεβαιωμένος και εξουσιοδοτημένος.

Μία οικογένεια μεθόδων πιστοποίησης μονοπατιού εναντίον του spam είναι το "Lightweight Message Authentication Protocol" (LMAP). Το LMAP αντιμετωπίζει το πρόβλημα της πλαστογράφησης των e-mails ελέγχοντας αν ο host από τον οποίο λαμβάνεται το e-mail είναι εξουσιοδοτημένος να στέλνει e-mail χρησιμοποιώντας το domain που εμφανίζεται στην επικεφαλίδα ή στον "φάκελο" του μηνύματος. Το LMAP βασίζεται σε δύο ιδέες: την δημοσίευση των δεδομένων πιστοποίησης από ένα domain (κυρίως μέσω DNS records) και την εφαρμογή αυτών των δεδομένων από τον παραλήπτη (MTA). Επηρεάζει, λοιπόν, τα πρωτόκολλα SMTP και DNS.

Όταν ένα μήνυμα στέλνεται μέσω SMTP, ο λαμβάνων MTA έχει αρκετά στοιχεία που θα μπορούσαν να χρησιμοποιηθούν για την πιστοποίηση του αποστολέα: τη διεύθυνση IP, το HELO/EHLO argument, το μονοπάτι επιστροφής και τις επικεφαλίδες του μηνύματος. Όλα αυτά τα στοιχεία μπορούν να χρησιμοποιηθούν σε πολλά είδη πιστοποίησης. Αυτό έχει οδηγήσει σε πολλές συγκεκριμένες LMAP προτάσεις που διαφέρουν στο είδος της οντότητας που εξουσιοδοτείται, στα δεδομένα με τα οποία η οντότητα συσχετίζεται, στη πηγή δικτύου και στον DNS record type (αν χρησιμοποιείται DNS).

Παρ' όλα αυτά, τα μειονεκτήματα των LMAPs προσεγγίσεων είναι πολυάριθμα [16]:

- Τα LMAPs έχουν ως πρωταρχικό σκοπό να αντιμετωπίσουν κάποιο είδος πλαστογράφησης και όχι τα spam γενικότερα. Άρα, τα LMAPs

δεν είναι αυτόνομες λύσεις εναντίον του spam, αλλά μπορούν να είναι μέρος μίας ολοκληρωμένης προσέγγισης.

- Η αναμετάδοση (relay) και η προώθηση μηνυμάτων επηρεάζεται από το LMAP: οι προωθητές των e-mail συνήθως αφήνουν τον φάκελο του αποστολέα άθικτο. Ας υποθέσουμε μία κατάσταση στην οποία το συμβατό με LMAP domain A στέλνει ένα μήνυμα στη διεύθυνση B, η οποία προωθεί το μήνυμα σε ένα συμβατό με LMAP παραλήπτη C χρησιμοποιώντας την αρχική διεύθυνση από τον A. Αν μία προώθηση $B \rightarrow C$ έχει δημιουργηθεί, τα LMAP records του A θα ελεγχθούν από τον LMAP client του C και ορθώς το μήνυμα θα απορριφθεί. Αν ο παραλήπτης C επιθυμούσε την προώθηση $B \rightarrow C$, μία λύση είναι απαραίτητη. Μία επιλογή είναι ο MTA του B να αντικαταστήσει την διεύθυνση αποστολέα με μία του domain του B, μία δεύτερη είναι να τροποποιηθεί το αρχείο *.forward*, ώστε να εφαρμόζει ένα μονοπάτι επιστροφής στο domain του B. Μία τρίτη επιλογή μπορεί να εφαρμοσθεί στον MTA του C, ο οποίος λαμβάνει μία whitelist που υποδηλώνει ότι είναι αναμενόμενο να λάβει ο C προωθημένα μηνύματα από τον B.
- Πολλά web συστήματα, όπως είναι τα συστήματα αποστολής ευχητήριων καρτών ή αποστολής link, προσφέρουν τη δυνατότητα αποστολής μηνυμάτων μέσω ενός web site σε έναν τρίτο, με τη διεύθυνση του χρήστη της ιστοσελίδας. Λίγα από αυτά τα συστήματα, όμως, πραγματοποιούν επαλήθευση της διεύθυνσης του αποστολέα, αν και ο ρυθμός αποστολής μηνυμάτων σε αυτές τις ιστοσελίδες είναι συνήθως πολύ αργός ώστε να μη χρησιμοποιούνται για την αποστολή spam. Ωστόσο, αφού οι χρήστες μπορούν να εισάγουν οποιαδήποτε διεύθυνση ως δική τους, τα e-mails που στέλνουν είναι τεχνικά μη διακριτά από αυτά που στέλνονται από πλαστές e-mail διευθύνσεις.
- Οι LMAP προτάσεις δεν εμποδίζουν τους χρήστες από το να ισχυρισθούν ψευδώς ότι είναι κάποιος άλλος χρήστης του ίδιου domain.
- Οι spammers μπορούν να δημιουργούν έγκυρα LMAP records για κάποια domains, που σκοπεύουν να χρησιμοποιήσουν για μικρό χρονικό διάστημα. Αφού στείλουν το μαζικό e-mail, τα domain αυτά σύντομα θα εισαχθούν σε blacklists και θα αχρηστευθούν για τους spammers και αυτοί θα δημιουργήσουν καινούρια domains και LMAP records.
- Οι περισσότερες εκδόσεις των LMAPs χρησιμοποιούν DNS για να διανείμουν τα δεδομένα με τα οποία πιστοποιούνται τα e-mails. Αυτό καθιστά το DNS καθοριστικής σημασίας πόρο, αν και είναι γνωστό ότι έχει αρκετά τρωτά σημεία. Για παράδειγμα, μη ασφαλή σημεία του DNS μπορούν να χρησιμοποιηθούν ώστε να επιτρέψουν σε κα-

κόβουλα άτομα να τοποθετήσουν πλαστές πληροφορίες πιστοποίησης στο DNS. Επίσης, διάφορες denial of service επιθέσεις, όπως είναι οι package floods, σε DNS servers μπορεί να καταστήσουν αδύνατο σε ένα LMAP client να αποκτήσει τα απαραίτητα στοιχεια για την πιστοποίηση των LMAP δεδομένων.

3.4.5 Επαλήθευση

Καθώς οι spammers συνήθως στέλνουν εκατομμύρια e-mails, πιστεύεται ότι αγνοούν οποιοδήποτε bounce e-mail λαμβάνουν. Με βάση αυτή τη συμπεριφορά, μηχανισμοί επαλήθευσης έχουν προταθεί για να σταματήσουν τα spam από το να παραδίδονται στον παραλήπτη. Σε ένα σχήμα επαλήθευσης, κανένα e-mail δεν παραδίδεται εκτός και αν ο αποστολέας ή η SO ανήκουν σε κάποια whitelist. Αν ο αποστολέας θελήσει να στείλει ένα μήνυμα σε κάποιο προστατευμένο mailbox, το μήνυμα θα κρατηθεί σε μία "ουρά απομόνωσης" (quarantine queue) και θα επιστραφεί η "πρόκληση". Αυτή μπορεί να είναι τόσο απλή όσο "απαντήστε σε αυτό το μήνυμα". Μπορεί, όμως, να είναι κάποιος απλός μαθηματικός υπολογισμός που θα πρέπει να κάνει ο e-mail client του αποστολέα ή η αποστολή κάποιας εικόνας, στην οποία βρίσκεται κάποια λέξη που ο χρήστης πρέπει να εισάγει (CAPTCHA algorithms). Αν η πρόκληση λυθεί με επιτυχία, τότε η διεύθυνση αποστολέα ή η SO προστίθεται στην whitelist του παραλήπτη και το αρχικό μήνυμα παραδίδεται. Επειδή η πρόκληση του παραλήπτη χρειάζεται μία απάντηση του αποστολέα, αυτή η διαδικασία ονομάζεται και "challenge-response" procedure.

Οι μέθοδοι που βασίζονται σε διαδικασίες "challenge-response" έχουν τα ακόλουθα μειονεκτήματα [16]:

- Η επικοινωνία μέσω e-mail γίνεται πιο πολύπλοκη.
- Ο φόρτος του διαδικτύου αυξάνεται λόγω των e-mails-προκλήσεων και των ενεργειών απάντησης.
- Η αποστολή κανονικών μαζικών e-mails (όπως είναι τα newsletters) στην πράξη αποτυγχάνει όταν απαιτούνται χειροκίνητες ενέργειες, καθώς χρειάζεται πολύ ανθρώπινο δυναμικό ή γίνεται εξαιρετικά ακριβή. Οι διαδικασίες challenge-response έχουν ως σκοπό την αύξηση της υπολογιστικής προσπάθειας της αποστολής e-mail σε βαθμό που να προλαμβάνεται ή τουλάχιστον να μειώνεται η μαζική αποστολή spam, επομένως αυτές οι διαδικασίες επηρεάζουν και τα κανονικά μαζικά e-mails με παρόμοιο τρόπο.
- Όταν η διεύθυνση e-mail ενός αθώου ατόμου χρησιμοποιείται ως διεύθυνση αποστολέα, τότε το μήνυμα-πρόκληση θα παραδοθεί στον αθώο χρήστη, πράγμα που καταλήγει σε ένα ακόμα άχρηστο e-mail.

- Όταν η απάντηση σχετίζεται με ένα CAPTCHA, η ποιότητά του πρέπει να λαμβάνεται υπόψη, καθώς μπορεί να υπάρξουν προβλήματα σε δύο κατευθύνσεις: (1) Ένα άτομο μπορεί να έχει δυσκολία στο να αναγνωρίσει ένα αντικείμενο αν αυτό παρουσιάζεται εν μέσω πολλών άλλων (για παράδειγμα, η χρήση της σημερινής Turing τεχνολογίας μπορεί να έχει ανεπιθύμητα αποτελέσματα σε χρήστες με προβλήματα όρασης), (2) Δεν πρέπει να είναι ευάλωτα σε λογισμικά έξυπνης αναγνώρισης (intelligent recognition software).

- Απαντήσεις οι οποίες σχετίζονται με εργασίες που πραγματοποιεί ο χρήστης μπορεί να είναι ευάλωτες σε επιθέσεις social engineering. Για παράδειγμα, έστω ότι ο spammer πρέπει να αναγνωρίσει μία λέξη σε μία εικόνα και να την γράψει σε μία φόρμα, τότε ο spammer μπορεί να εξαπατήσει ένα χρήστη ώστε αυτός να επισκεφθεί μία ιστοσελίδα, όπου περιέχεται και η εικόνα-πρόκληση, και εκεί ο ανυποψίαστος χρήστης να δώσει την απάντηση, επειδή πιστεύει ότι με αυτό τον τρόπο θα αποκτήσει πρόσβαση σε κάποια δεδομένα. Ο χρήστης, λοιπόν, γράφει τη λέξη και αυτή πλέον βρίσκεται στη διάθεση του spammer σε μορφή αναγνωρίσιμη από τον υπολογιστή. Όλα τα παραπάνω μπορούν να γίνονται αυτόματα.

3.4.6 Προσεγγίσεις πληρωμής

Οι προσεγγίσεις πληρωμής βασίζονται σε συστήματα e-mail που δημιουργούν αντικίνητρα για το spam. Για να επιτευχθεί αυτό, οι e-mail servers απαιτούν μία μικρή πληρωμή ως αντάλλαγμα της παράδοσης ενός e-mail στο inbox του χρήστη ή για την αποδοχή ενός e-mail από τον client του χρήστη. Η πληρωμή είναι αρκετά μικρή ώστε να επιτρέπεται η παράδοση θεμιτών μηνυμάτων, αλλά και τόσο μεγάλη ώστε η αποστολή μεγάλου αριθμού e-mails να γίνεται είτε πολύ ακριβή είτε πολύ χρονοβόρα. Ωστόσο, ταυτόχρονα τίθεται το ζήτημα της παράδοσης των θεμιτών μαζικών e-mails.

Η μορφή πληρωμής μπορεί να είναι CPU χρόνος ή ικανότητα μνήμης -αυτές οι διαδικασίες λέγονται *"proof-of-work" procedures*- ακόμη και νομίσματα, πραγματικά ή εικονικά. Αυτή την στιγμή συστήματα που βασίζονται σε πληρωμή χρησιμοποιούνται σπάνια.

CPU-based:

Οι προσεγγίσεις οι οποίες βασίζονται στον CPU χρόνο είναι χαρακτηριστικό παράδειγμα μίας proof-of-work, που δέχεται μία παραμετροποιήσιμη ποσότητα από CPU εργασία, την οποία πρέπει να υπολογίσει ο αποστολέας. Οι Dwork και Naor ήδη από το 1992 πρότειναν αρκετές διαφορετι-

κές "pricing functions", που βασίζονται στην εύρεση τετραγωνικών υπολοίπων modulo κάποιου πρώτου αριθμού, στο σχήμα υπογραφής Fiat-Shamir ή στο σχήμα υπογραφής Ong-Schnorr-Shamir (Recycling Broken Signature Schemes) [5].

Η κύρια ιδέα πίσω από αυτή τη μέθοδο είναι ότι ο χρήστης πρέπει να υπολογίσει μία σχετικά δύσκολη συνάρτηση (pricing function) για να αποκτήσει πρόσβαση σε κάποιους πόρους. Η συνάρτηση αυτή μπορεί να επιλεγεί έτσι ώστε να έχει κάποιο *shortcut*, δηλαδή δεδομένων κάποιων επιπρόσθετων πληροφοριών ο υπολογισμός να γίνεται σημαντικά απλούστερος, το οποίο μπορεί να χρησιμοποιείται από το διαχειριστή των πόρων (π.χ. για την αποστολή κανονικών μαζικών e-mails). Επιπλέον, η pricing function δεν εφαρμόζεται στο μήνυμα, το οποίο μπορεί να είναι ιδιαίτερα μεγάλο, αλλά στην τιμή που προκύπτει από το e-mail μέσω μίας hash function (π.χ. DES, MD5, Subset Sum ή Snefru).

Επομένως, τα κύρια συστατικά της μεθόδου είναι η pricing function (f_s), το shortcut (c) και η hash function (h), ενώ για να σταλεί ένα μήνυμα m την στιγμή t στον προορισμό d, ο αποστολέας υπολογίζει το $y = f_s(h(\langle m, t, d\rangle))$ και στέλνει το $\langle y, m, t\rangle$ στον d. Ο e-mail client του παραλήπτη επαληθεύει ότι $y = f_s(h(\langle m, t, d\rangle))$, αλλιώς το μήνυμα απορρίπτεται.

Ακολουθεί η σύντομη περιγραφή των τριών υποψηφίων pricing functions σύμφωνα με τους Dwork και Naor:

Εύρεση τετραγωνικών υπολοίπων:

Πρόκειται για μία συνάρτηση χωρίς shortcut. Τα δεδομένα είναι ένας πρώτος αριθμός p σχετικά μεγάλου μήκους, η pricing function είναι η $f_p(x) = \sqrt{x} \mod p$ και η επαλήθευση γίνεται από τον τύπο $y^2 \equiv x \mod p$. Ενώ η επαλήθευση χρειάζεται μόνο ένα υπολογισμό, δεν υπάρχει γνωστή μέθοδος για την εύρεση της τετραγωνικής ρίζας ενός αριθμού mod p που να απαιτεί λιγότερους από $\log p$ πολλαπλασιασμούς.

Fiat-Shamir based scheme:

Είναι η πιο ευέλικτη από τις τρεις προτεινόμενες συναρτήσεις, όμως απαιτεί μία επιπλέον hash function. Τα δεδομένα είναι ένας φυσικός αριθμός $N = pq$, όπου οι p και q είναι επαρκώς μεγάλοι πρώτοι αριθμοί, k τετράγωνα modulo $(y_1 = {x_1}^2, ..., y_k = {x_k}^2)$ και μία hash function h. Το shortcut είναι οι τετραγωνικές ρίζες $x_1, ..., x_k$.

Αν τα x, r και z είναι τέτοια ώστε $h(x, r^2) = b_1...b_k$, όπου κάθε b_i είναι ένα δυαδικό ψηφίο του αποτελέσματος $h(x, r^2)$, και (z, r^2) ώστε $z^2 = r^2 x^2 \prod_{i=1}^{k} {y_i}^{b_i} \mod N$, ο ορισμός της f_s είναι $f_s(x) = (z, r^2)$. Η

επαλήθευση γίνεται από τον τύπο $z^2 = r^2 x^2 \prod_{i=1}^{k} {y_i}^{b_i} \mod N$.

Αν είναι γνωστό το shortcut, δηλαδή τα $x_1, x_2, ..., x_n$, η f_s μπορεί να υπολογισθεί επιλέγοντας τυχαίο r, υπολογίζοντας το $h(x, r^2) = b_1 ... b_k$ και θέτοντας $z = rx \prod_{i=1}^{k} {x_i}^{b_i}$.

Χωρίς το shortcut η αναμενόμενη πολυπλοκότητα είναι της τάξεως του 2^k, ενώ αν το shortcut είναι γνωστό χρειάζονται περίπου k πολλαπλασιασμοί και ένας υπολογισμό της hash function. Παρομοίως και η επαλήθευση χρειάζεται περίπου k πολλαπλασιασμούς και έναν υπολογισμό της hash function, ανεξαρτήτως της γνώσης ή μη του shortcut.

Ong-Schnorr-Shamir based scheme:

Μία πηγή προτάσεων για pricing functions με shortcut είναι τα σχήματα υπογραφής για τα οποία έχει βρεθεί κάποια επιτυχημένη επίθεση. Ο τύπος της επίθεσης αυτής δε θα πρέπει να αποκαλύπτει το ιδιωτικό κλειδί, αλλά παρ' όλα αυτά να επιτρέπει την πλαστογράφηση υπογραφών με ένα σχετικά εύκολο αλγόριθμο. Ένα τέτοιο παράδειγμα είναι το σχήμα Ong-Schnorr-Shamir και ο αλγόριθμος Pollard.

Τα δεδομένα εδώ είναι ένας φυσικός αριθμός $N = pq$, όπου οι p και q είναι επαρκώς μεγάλοι πρώτοι αριθμοί, και ένα $l \in {\mathbb{Z}_n}^*$. Θέτουμε $s = (N, l)$. Το shortcut είναι ένα u ώστε $u^2 = l^{-1} \mod N$

Αν ${x_1}^2 + l{x_2}^2 \equiv x \mod N$, τότε η $f_s = (x_1, x_2)$ υπολογίζεται μέσω του αλγορίθμου του Pollard (πολυπλοκότητας $O(logN)$). Η επαλήθευση προκύπτει από τον τύπο $x = {x_1}^2 + l{x_2}^2$, ενώ, αν είναι γνωστό το shortcut, η f_s μπορεί να υπολογισθεί επιλέγοντας τυχαία $r_1, r_2 \in {\mathbb{Z}_n}^*$ ώστε $r_1 r_2 \equiv m \mod N$ και θέτοντας $x_1 = \frac{1}{2}(r_1 + r_2) \mod N$ και $x_2 = \frac{1}{2}u(r_1 - r_2) \mod N$.

Ανεξάρτητα από τη μέθοδο που χρησιμοποιείται, τα CPU-based anti-spam μέτρα έχουν ορισμένα αρνητικά χαρακτηριστικά [16]:

- Καταναλώνουν τους πόρους του αποστολέα απαιτώντας έναν χωρίς σημασία υπολογισμό. Επομένως, hijacked υπολογιστές μπορεί να υποφέρουν από υψηλή κατανάλωση του CPU χρόνου τους.
- Όταν χρησιμοποιούνται botnets, ο συνολικός CPU χρόνος που απαιτείται για να σταλούν spam κατανέμεται μεταξύ πολλών hosts.
- Οι απαιτήσεις σε χρόνο μπορεί να διαφέρουν ανάλογα με την ταχύτητα της CPU. Επομένως, φαίνεται δύσκολο να βρεθεί η ισορροπία ανάμεσα στο να εμποδισθεί η αποστολή μαζικών ανεπιθύμητων μηνυ-

μάτων και στο να επιτραπεί η αποστολή κανονικών e-mails σε έναν επαρκή χρόνο.

- Είναι απαραίτητο να ενημερώνονται οι e-mail clients και να πεισθούν οι χρήστες να πραγματοποιούν αυτές τις ενημερώσεις. Επιπλέον, τα e-mail πρωτόκολλα θα πρέπει να αλλάξουν ουσιωδώς.
- Οι περισσότεροι υπέρμαχοι των CPU-based προσεγγίσεων προτείνουν ότι αν ο παραλήπτης *R* έχει προηγουμένως δεχθεί να λάβει κάποιο e-mail από τον αποστολέα *S*, τότε κάθε e-mail από τον *S* στον *R* στέλνεται με τον κανονικό τρόπο. Ωστόσο, αυτό απαιτεί μηχανισμούς πιστοποίησης σε επίπεδο χρήστη.
- Δυστυχώς, εξαιτίας ουσιωδών διαφορών μεταξύ των διαφόρων συστημάτων υπολογιστών, αυτή η προσέγγιση μπορεί να είναι αναποτελεσματική εναντίον κακόβουλων χρηστών με ανεπτυγμένα συστήματα, απαγορευτικά αργή για κανονικούς χρήστες με λιγότερο ανεπτυγμένα συστήματα, ή και τα δύο.

Memory-based:

Γενικά, οι memory-based προσεγγίσεις έχουν παρόμοια μειονεκτήματα με τις CPU-based, εκτός από το ότι οι proof-of-work απαιτήσεις σε αυτές δε διαφέρουν τόσο πολύ μεταξύ συστημάτων. Οι Abadi et al. [1] προτείνουν ορισμένες σχετικά δύσκολες, memory-bound συναρτήσεις που μπορούν να χρησιμοποιηθούν σε αυτή τη μέθοδο. Σύμφωνα με αυτή την προσέγγιση ο αποστολέας αναγκάζεται να πραγματοποιήσει πρόσβαση σε μία μη προβλέψιμη ακολουθία στοιχείων ενός μεγάλου διανύσματος.

Η challenge-response διαδικασία είναι η ακόλουθη:

1. Έστω δύο ακέραιοι k και n και μία συνάρτηση $F : \{0, 1, ..., 2^n - 1\} \rightarrow \{0, 1, ..., 2^n - 1\}$, όπου 2^n είναι το μήκος του διανύσματος, και έστω ότι η αντίστροφή της F^{-1} δεν μπορεί να υπολογισθεί σε χρόνο λιγότερο από μία πρόσβαση στη μνήμη. Τα k, n, F θεωρείται ότι είναι γνωστά τόσο στον αποστολέα S όσο και στον παραλήπτη R.
2. Ο R διαλέγει έναν ακέραιο $x_0 \in \{0, ..., 2^n - 1\}$ και υπολογίζει για κάποιο $i \in \{0, ..., k - 1\}$ το $x_{i+1} = F(x_i)$ xor i και το checksum της ακολουθίας $x_0, ...x_k$. Ο R στέλνει στον S το x_k και το checksum.
3. Ο S κατασκευάζει τον πίνακα για την F^{-1} εφαρμόζοντας την F σε όλους τους ακεραίους στο σύνολο $\{0, ..., 2^n - 1\}$, καθώς αν ζητείται από τον αποστολέα πολλές φορές να υπολογίσει κάποιο στοιχείο της F^{-1}, τότε είναι προτιμότερο να κατασκευάσει ένα πίνακα για την F^{-1}.

4. Ο S κατασκευάζει την ακολουθία $y_k, ..., y_0$ ξεκινώντας από το $y_k = x_k$ ώστε $y_i \in F^{-1}(y_{i+1} \text{ xor } i)$.
5. Ο S, δεδομένης της ακολουθίας, επιστρέφει το y_0 στην περίπτωση που ικανοποιείται το checksum.

Ο S μπορεί να κατασκευάσει τις ακολουθίες $y_k, ...y_0$ κατά μήκος ή κατά πλάτος. Σε κάθε περίπτωση, όμως, πρέπει να πραγματοποιήσει πολλές προσβάσεις στον πίνακα της F^{-1}.

Monetary-based:

Αυτές οι προτάσεις τυπικά απαιτούν από τους αποστολείς να πληρώσουν ένα ποσό για κάθε e-mail, συνήθως μόνο αν ο αποδέκτης δεν έχει τοποθετήσει τον αποστολέα σε whitelist. Το νόμισμα που χρησιμοποιείται μπορεί να είναι πραγματικά χρήματα (σχήματα εγγύησης όπου ο αποστολέας δίνει μία εγγύηση σε κάποιον τρίτο, την οποία ο αποστολέας χάνει αν το μήνυμα είναι spam) ή εικονικά/ψηφιακά νομίσματα.

Στην περίπτωση του e-cash [20, 7] χρησιμοποιούνται e-stamps, δηλαδή μοναδικά αλφαριθμητικά που αντιπροσωπεύουν μία μικρή ποσότητα χρημάτων, εκδίδονται από κάποιας μορφής ψηφιακή τράπεζα και έχουν περιορισμένη διάρκεια (περίπου μία εβδομάδα). Σε ένα τέτοιο σύστημα, υπάρχουν τρία βασικά μέρη: μία λίστα αποδοχής, που περιέχει τα άτομα από τα οποία δε θα ζητηθούν χρήματα για την παραλαβή του μηνύματος, ένα σύστημα παραγωγής "νομισμάτων" και ένα συγκεκριμένο ποσό, που θα πρέπει να πληρωθεί στην περίπτωση που ο παραλήπτης θεωρήσει την επικοινωνία ανεπιθύμητη.

Ο αποστολέας τοποθετεί μία e-stamp σε κάθε e-mail που στέλνει και ο παραλήπτης αρνείται να λάβει e-mail χωρίς e-stamp, τουλάχιστον όχι από αγνώστους. Αν ένας άγνωστος στείλει κάποιο e-mail χωρίς e-stamp, τότε λαμβάνει ένα "bounce" που τον ειδοποιεί ότι πρέπει να προστεθεί μία e-stamp στο μήνυμά του ώστε αυτό να παραδοθεί. Όταν ο παραλήπτης λάβει το μήνυμα, τότε μπορεί να προωθήσει την e-stamp στην τράπεζα για εξαργύρωση. Το σύστημα αυτό μπορεί να γίνει απλούστερο αν την ευθύνη για την τοποθέτηση των e-stamps την είχαν τα sites και όχι οι χρήστες. Επιπλέον, η εγγραφή σε mailing lists ή newsletters είναι εφικτή είτε με την αποστολή στον διαχειριστή της λίστας μίας e-stamp που δεν λήγει, η οποία μπορεί να εξαργυρωθεί σε περίπτωση που ο εγγεγραμμένος στη λίστα εξαργυρώσει κάποια e-stamp που περιλαμβάνεται σε e-mail της λίστας, με την ενημέρωση του e-mail client για την εγγραφή στη λίστα είτε με τη δημιουργία προσωπικών e-stamps από τον χρήστη που χρησιμοποιούνται από τον κάτοχο της λίστας κατά την αποστολή των e-mails.

Ορισμένα μειονεκτήματα που σχετίζονται με αυτά τα συστήματα είναι τα ακόλουθα [16]:

- Η πιστοποίηση αποστολέα είναι απαραίτητη ώστε να δοθεί η δυνατότητα στο χρήστη να βρίσκει τα e-mails που στέλνονται από άτομα στη whitelist. Επειδή το πεδίο MAIL FROM του φακέλου όπως και τα δεδομένα της επικεφαλίδας του αποστολέα μπορεί να είναι πλαστογραφημένα, ένας επιπλέον μηχανισμός πιστοποίησης είναι απαραίτητος. Αν και η κρυπτογραφία δημοσίου κλειδιού παρέχει τους απαραίτητους αλγορίθμους, αυτή η προσέγγιση έχει δύο σημαντικά μειονεκτήματα: (1) Είναι απαραίτητη η ύπαρξη μίας PKI που παρέχει ζεύγη κλειδιών όχι μόνο σε οργανισμούς αλλά και σε μεμονωμένα άτομα. (2) Κάθε e-mail είναι απαραίτητο να κατέβει ολόκληρο ώστε να βρεθεί και να επαληθευτεί η ψηφιακή του υπογραφή.
- Όταν ένας χρήστης παραγγέλνει e-stamps, η πιστοποίηση είναι απαραίτητη αφού η χρήση μίας e-stamp σχετίζεται με μία δεσμευτική προσφορά και, επομένως, με τα χρήματα του χρήστη. Η εκμετάλλευση των e-stamps από τρίτους μπορεί να έχει σημαντικές οικονομικές επιπτώσεις για τον κάτοχό τους.
- Δημιουργείται τεράστιο κίνητρο για τη δημιουργία ενός e-mail/ιού που θα προκαλεί την αποστολή e-mail από εκατομμύρια ανθρώπους σε μία ψεύτικη, offshore διεύθυνση e-mail, από όπου ο απατεώνας θα εξαργυρώσει τις εγγυήσεις και θα εξαφανίστεί.
- Πλήρως σχηματισμένο, το σύστημα των e-stamps είναι πολύπλοκο και οι τεχνολογικές και οργανωτικές επιπτώσεις του είναι σημαντικές: μία (παγκόσμια) υποδομή ψηφιακών υπογραφών και ψηφιακά νομίσματα (που θα έχουν χαμηλό κόστος συναλλαγής και μεγάλη διαθεσιμότητα) είναι απαραίτητα. Έχουν προταθεί πολλές τέτοιες υποδομές, αλλά καμία δεν ήταν επιτυχημένη, Επιπλέον, η λύση χρειάζεται νέο λογισμικό τόσο για τον αποστολέα αλλά και τον παραλήπτη.
- Αν η επικοινωνία μέσω e-mail γίνει επί πληρωμή, ενώ μέχρι τώρα ήταν δωρεάν, οι άνθρωποι μπορεί να χρησιμοποιήσουν αυτές τις υπηρεσίες απρόθυμα. Ο κίνδυνος της εγκατάλειψη του e-mail θεωρείται ότι δεν προέρχεται μόνο από το ότι οι άνθρωποι απεχθάνονται την ιδέα του να πληρώνουν για τα e-mails τους, αλλά και επειδή αυτά τα συστήματα είναι κάπως εχθρικά προς το χρήστη. Αν κάποιος άγνωστος στείλει ένα e-mail χωρίς e-stamp, τότε ο χρήστης μπορεί να κρατήσει το μήνυμα σε ξεχωριστό φάκελο για μετέπειτα έλεγχο ή να το επιστρέψει στον αποστολέα με το αίτημα να προστεθεί μία e-stamp. Αυτό το αίτημα είναι μεγάλο, καθώς ένας χρήστης πρέπει να περάσει μία πολύπλοκη

διαδικασία, και, μακροπρόθεσμα για να αποφύγει την επιστροφή μηνυμάτων, πρέπει να αποκτήσει νέο λογισμικό για τα e-mails του ή κάποιο plug-in στο υπάρχον λογισμικό του.

- Τελικά, ο καθένας πρέπει να πληρώσει το κόστος, πράγμα που είναι αντίθετο στην ιδέα του δωρεάν Internet. Γενικά, οι νόμιμοι χρήστες θα προτιμούσαν να μην τιμωρούνται αυτοί για τις λανθασμένες συμπεριφορές άλλων.

3.4.7 Περιορισμός εξερχόμενης αλληλογραφίας

Ορισμένοι ESPs έχουν ορίσει όρια στο ρυθμό της εξερχόμενης αλληλογραφίας. Τα τελευταία χρόνια, οι hackers έχουν αρχίσει να συνωμοτούν με τους spammers με αποτέλεσμα να δημιουργούνται νέοι ιοί και worms που καταλαμβάνουν τους προσωπικούς υπολογιστές εκ μέρους των spammers. Αυτοί οι υπολογιστές, στη συνέχεια, αρχίζουν να δημιουργούν μεγάλες ποσότητες από spam. Αν και αυτή η κατάσταση είναι αρκετά διαδεδομένη σε ESPs που δεν απαιτούν πιστοποίηση, ακόμη και οι ESPs που εφαρμόζουν πιστοποίηση λογαριασμού έχουν αύξηση στο πλήθος των λογαριασμών που καταλαμβάνονται με άλλες τεχνικές, όπως password phishing και Trojans με καταγραφέα πληκτρολόγησης (keystroke loggers). Ο στόχος των ESPs είναι να εμποδίσουν τους spammers να στείλουν μεγάλο πλήθος μηνυμάτων σε μικρό χρονικό διάστημα από παραβιασμένους λογαριασμούς ή από νέους λογαριασμούς που δημιουργούνται από τους spammers.

Προκειμένου να περιορισθεί ο αριθμός των e-mails που ένας χρήστης μπορεί να στείλει, είναι, επίσης, απαραίτητο να εμποδιστεί η αυτοματοποιημένη δημιουργία λογαριασμών. Αυτό απαιτεί ένα είδος ελέγχου που θα επαληθεύει την ύπαρξη κάποιου ατόμου πίσω από την αίτηση και όχι απλώς μία μηχανή που εκτελεί κάποιο script. Για αυτό το λόγο χρησιμοποιούνται CAPTCHA διαδικασίες, με τα μειονεκτήματα που αυτές παρουσιάζουν.

Επιπλέον, είναι στην ευχέρεια των ESPs, και γενικότερα των οργανισμών που παρέχουν πρόσβαση σε e-mail, να εφαρμόσουν κάποιο περιορισμό του πλήθους των εξερχόμενων e-mails ανά μονάδα χρόνου και ανά λογαριασμό. Φαίνεται, όμως, πολύ δύσκολο, έως και αδύνατο να αναπτυχθεί και να ελεγχθεί μία τέτοια εφαρμογή παγκοσμίως.

3.4.8 Τεχνικές απόκρυψης της διεύθυνσης

Οι τεχνικές απόκρυψης διεύθυνσης στοχεύουν στην προστασία των e-mail διευθύνσεων από την κακή χρήση τους από τους spammers. Τα εννοιολογικά ζητήματα και τα μειονεκτήματα διαφέρουν μεταξύ των προσεγγίσεων. Παρακάτω παρου-

σιάζονται και αναλύονται δύο από τις προσιγγίσεις απόκρυψης διεύθυνσης:

1. Ο Hall [9] προτείνει μία μέθοδο απόκρυψης διεύθυνσης, που αναφέρεται ως μέθοδος των "e-mail καναλιών" (e-mail channels). Σύμφωνα με αυτή την πρόταση, ο λογαριασμός e-mail ενός χρήστη θα είναι προσβάσιμος από ένα σύνολο καναλιών, τα οποία θα ελέγχονται από τον χρήστη. Κάθε κανάλι θα έχει μία χαρακτηριστική δομημένη διεύθυνση που θα λαμβάνει τη μορφή *user_name-channel_id@host*, περιέχοντας το όνομα του λογαριασμού και ένα κρυπτογραφικά ασφαλές, ή δύσκολα προβλέψιμο, ψευδοτυχαίο αλφαριθμητικό ασφαλείας, το οποίο λειτουργεί ως αναγνωριστικό στοιχείο του καναλιού. Τα αναγνωριστικά των καναλιών έχουν τη μορφή Cxxxxxxxxxx, όπου το C είναι ένα ψηφίο που δείχνει τον τύπο του καναλιού (π.χ. δημόσιο, ιδιωτικό, μόνο για αποστολή) ακολουθούμενο από το string ασφαλείας.

   Κάθε νόμιμος αποστολέας γνωρίζει μία από αυτές τις διευθύνσεις, ενώ ο κάτοχος του λογαριασμού έχει τη δυνατότητα να δημιουργήσει, να καταργήσει κανάλια, να αλλάξει υπάρχοντα κανάλια με νέα ειδοποιώντας επιλεγμένους χρήστες για αυτή την αλλαγή. Στην πρόταση αυτή, αναφέρεται και το εργαλείο με το οποίο ο χρήστης θα μπορεί να διαχειρίζεται τα διάφορα κανάλια και το οποίο αναφέρεται ως *Personal Channel Agent (PCA)*.

   Κάποια από τα μειονεκτήματα της μεθόδου είναι ότι [16]:

   - η επικοινωνία μέσω e-mail γίνεται πιο πολύπλοκη, καθώς είναι δυσκολότερο να δοθεί σε κάποιον η διεύθυνση joe-2kfhalfgabv@gmail.com παρά η joe@gmail.com.
   - τα αναγνωριστικά των καναλιών είναι πολύ δύσκολο να παραμείνουν μυστικά, ειδικά με την ύπαρξη κακόβουλων λογισμικών που έχουν τη δυνατότητα να διαβάζουν τοπικά βιβλία διευθύνσεων.

2. Μία άλλη πρόταση είναι αυτή των Single-Purpose Addresses (SPAs) [10], στην οποία ένα πρόγραμμα παράγει SPAs που μετέπειτα δίνονται σε οποιαδήποτε εφαρμογή ζητάει μία e-mail διεύθυνση. Επειδή ακριβώς αυτές οι διευθύνσεις προορίζονται για εφαρμογές, όπως είναι το Usenet ή διάφορες mailing lists, δεν χρειάζεται να είναι απλές, εύκολες στην απομνημόνευση ή ακόμα και αναγνώσιμες.

   Η βασική ιδέα είναι ότι σε κάθε περίπτωση που χρειάζεται να δοθεί μία διεύθυνση e-mail, κανόνες για την χρήση της κωδικοποιούνται στην ίδια τη διεύθυνση. Έτσι, μία διεύθυνση αποτελείται από ένα αναγνωριστικό και από την κατάλληλα κωδικοποιημένη περιγραφή της χρήσης της (π.χ. σύμφωνα με τον κανόνα user+extension). Επειδή, όμως, δεν υπάρχει λόγος να αποκαλυφθεί καμία πληροφορία σχετική με την πολιτική χρήσης του χρήστη, η διεύθυνση πρέπει να κρυπτογραφηθεί με ένα κλειδί που είναι γνωστό

μόνο τον χρήστη, στον MTA ή/και στον MUA. Όταν, λοιπόν, λαμβάνεται ένα e-mail, λαμβάνεται η SPA στην οποία στάλθηκε, και αφού αποκωδικοποιηθεί, ελέγχεται αν ικανοποιεί τους απαραίτητους κανόνες και αν δεν τους ικανοποιεί το μήνυμα απορρίπτεται. Τα μειονεκτήματα αυτής της μεθόδου είναι περίπου ίδια με αυτά της μεθόδου των "καναλιών e-mail".

3.4.9 Προσεγγίσεις φήμης

Στις προσεγγίσεις φήμης (reputation-based approaches), ο παραλήπτης δέχεται ή απορρίπτει το μήνυμα βασιζόμενος στη φήμη του αποστολέα ή της SO. Σύμφωνα με την πρόταση των Kaushik et al. [11] πρέπει να υπάρχει μία πολιτική περιορισμού της πρόσβασης στο mailbox του παραλήπτη, που να βασίζεται στα χαρακτηριστικά του αποστολέα. Κυρίαρχο ρόλο σε αυτή την προσέγγιση έχουν οι ESPs, ενώ δεν υπάρχει ανάγκη για την ανάπτυξη PKI, που συνοδεύεται από πολλά μειονεκτήματα. Συγκεκριμένα, προτείνονται τρεις τύποι τακτικών:

1. Η Service Level Agreement Policy (SLAP) αναφέρεται στον τρόπο με τον οποίο ο παραλαμβάνων ESP αποφασίζει να αλληλεπιδράσει με έναν συγκεκριμένο αποστέλλων ESP, ο οποίος έχει ανακοινώσει ότι κατέχει ένα e-mail προς αποστολή. Η είσοδός της περιλαμβάνει την ταυτότητα του ESP του αποστολέα, την κατάστασή του και τη φήμη του (π.χ. μέσω whitelists και blacklists).

2. Η Message Scheduling Policy (MSP), που είναι η έξοδος της SLAP, καθορίζει πώς πρέπει να αντιμετωπίζεται κάθε μήνυμα από τον αποστέλλων ESP. Υπάρχουν δύο τύποι, που σχετίζονται με το πού εκτελείται η εκτίμηση: η "φορητή" και η "τοπική".

3. Η Message Resource Allocation Policy (MRAP) κωδικοποιεί τις συγκεκριμένες απαιτήσεις του παραλήπτη και χρησιμοποιείται για να καθορισθεί ο τρόπος που θα παρουσιασθούν τα μηνύματα στον παραλήπτη.

3.5 Ολιστικές προσεγγίσεις

Αν και πολλά anti-spam μέτρα έχουν προταθεί, όλα έχουν ορισμένους περιορισμούς και δεν προσφέρουν οριστική λύση για το πρόβλημα του spam. Είναι απαραίτητο, λοιπόν, να προταθούν λύσεις που συνδυάζουν πολλά διαφορετικά μέτρα και επιλύουν οριστικά το πρόβλημα του spam. Για να θεωρηθεί μία πρόταση επιτυχημένη θα πρέπει να έχει ορισμένα χαρακτηριστικά [16]:

- Τόσο οι τεχνολογικές όσο και οι οργανωτικές τροποποιήσεις, που θα προτείνει, θα πρέπει να είναι μικρές.
- Η πρόταση θα πρέπει να είναι ανοικτή σε βελτιώσεις, καθώς θα περιλαμβάνει μόνο τις αρχές αντιμετώπισης του spam και δε θα προσφέρει συγκεκριμένους αλγορίθμους ή τύπους δεδομένων.
- Τα spam θα πρέπει να εμποδίζονται όσο πιο κοντά στην πραγματική πηγή τους γίνεται. Η πρόληψη του spam έχει προτεραιότητα σε σχέση με την ανίχνευσή του.
- Η πρόταση θα πρέπει να διασφαλίζει τα μέσα για την αποστολή νόμιμων μαζικών e-mails.
- Η εφαρμογή των καίριων στοιχείων της πρότασης θα πρέπει να μπορεί να γίνει ομαλά και με ευελιξία, δηλαδή η υιοθέτηση της καινούργιας υποδομής να μπορεί να γίνει προοδευτικά.
- Η υποδομή, που προτείνεται, δε θα πρέπει να προκαλεί ένα είδος "πολέμου" με τους spammers, όπως για παράδειγμα συμβαίνει στην προσπάθεια ανάπτυξης φίλτρων.

Μία τέτοια πρόταση παρουσιάζεται από τον G. Schryen [16]. Τα κύρια στοιχεία της πρότασής του είναι: (1) Ο περιορισμός του αριθμού των e-mails που μπορούν να σταλούν ανά μονάδα χρόνου και ανά λογαριασμό. (2) Η απαγόρευση αυτόματης δημιουργίας e-mail λογαριασμών. (3) Η δημιουργία μέσων για τον έλεγχο της τήρησης των προηγούμενων περιορισμών, εισάγοντας ένα στοιχείο συγκεντρωτισμού, την Counter Managing & Abuse Authority (CMAA). Το ρόλο μίας CMAA μπορεί να διαδραματίσει μία ήδη υπάρχουσα (π.χ. κάποιος έμπιστος ESP) ή μία νέα οργάνωση. Σύμφωνα με αυτή την πρόταση, μία SO μπορεί είτε να στείλει ένα e-mail απευθείας σε μία RO, στην περίπτωση που η SO θεωρείται έμπιστη από την RO, είτε να το στείλει μέσω κάποιας οργάνωσης CMAA. Στη δεύτερη περίπτωση, η CMAA ελέγχει αν ο αποστολέας έχει υπερβεί τον αριθμό e-mails που μπορεί να στείλει σε μία ημέρα και ανάλογα με το αποτέλεσμα επιστρέφει το μήνυμα στην SO ή το αναμεταδίδει στην RO.

Επιπλέον, μία CMAA θα πρέπει να κρατάει κάποια στοιχεία σχετικά με τους λογαριασμούς e-mail, τα οποία θα αποθηκεύονται σε αντίστοιχες βάσεις δεδομένων. Για να είναι δυνατή η απόδοση ευθύνης σε περίπτωση κατάχρησης του λογαριασμού, η SO θα πρέπει να δημιουργεί ένα αρχείο για το λογαριασμό κάθε αποστολέα προτού γίνει η αναμετάδοση του πρώτου μηνύματος. Τα στοιχεία αυτά αποθηκεύονται στην Counter Database (CDB). Επειδή η CMAA είναι υπεύθυνη και για την κατάργηση των λογαριασμών λόγω καταγγελιών κατάχρησης, θα πρέπει να

υπάρχει μία βάση δεδομένων αποθήκευσης των καταγγελιών, η οποία ονομάζεται Abuse Database (ADB). Τέλος, στην Organizational Database (ODB) καταγράφονται τα στοιχεία των SOs που είναι εγγεγραμμένες στην CMAA και χρησιμοποιούν τις υπηρεσίες της.

Κεφάλαιο 4

Honeypots

4.1 Ορισμός και κατηγορίες

Τα honeypots είναι ένα ισχυρό και ευέλικτο εργαλείο, το οποίο μπορεί να χρησιμοποιηθεί για την καταπολέμηση του spam. Ωστόσο, η χρήση των honeypots δεν περιορίζεται στην επίλυση κάποιου συγκεκριμένου προβλήματος. Για παράδειγμα, μπορούν να εντοπίσουν από επιθέσεις σε δίκτυα IPv6 μέχρι και τις πιο πρόσφατες απάτες με πιστωτικές κάρτες [18]. Σύμφωνα με τον L. Spitzner, *"ένα honeypot είναι ένας πόρος πληροφοριών συστήματος του οποίου η αξία βρίσκεται στην μη εξουσιοδοτημένη και παράνομη χρήση του"*. Στην ουσία, τα honeypots είναι πόροι χωρίς εξουσιοδοτημένη χρήση, δηλαδή, θεωρητικά, ο φόρτος εργασίας αυτών των πόρων θα έπρεπε να είναι μηδενικός. Επομένως, οποιαδήποτε αλληλεπίδραση με το honeypot πιθανότατα σχετίζεται με κάποια παράνομη και κακόβουλη δραστηριότητα. Ο σκοπός των honeypots μπορεί να είναι η προστασία των συστημάτων μίας εταιρίας ή η συλλογή δεδομένων για ερευνητικούς λόγους.

Υπάρχουν δύο είδη honeypots, που κατασκευάζονται με διαφορετικό τρόπο και χρησιμοποιούνται για διαφορετικούς σκοπούς. Αυτά είναι τα low-interaction και τα high-interaction honeypots. Στην πρώτη κατηγορία ανήκουν τα honeypots τα οποία έχουν χαμηλό βαθμό αλληλεπίδρασης με τον εισβολέα και συνήθως λειτουργούν εξομοιώνοντας υπηρεσίες και λειτουργικά συστήματα. Στη δεύτερη κατηγορία ανήκουν τα πιο πολύπλοκα honeypots που περιλαμβάνουν πραγματικά λειτουργικά συστήματα και εφαρμογές.

Κάποια από τα πλεονεκτήματα της έννοιας του honeypot είναι ότι:

- συλλέγουν μικρό όγκο δεδομένων, ο οποίος, ωστόσο, έχει μεγάλη αξία: Τα honeypots συλλέγουν μόνο κακόβουλη δραστηριότητα και, επομένως, χρειάζεται να αποθηκευτεί και να επεξεργασθεί πολύ μικρότερος όγκος δεδομένων απ' ότι σε κάποιο άλλο σύστημα, αφού δεν υπάρχει καθόλου "θό-

ρυβος" από νόμιμα δεδομένα. Επίσης, η ανάλυση των δεδομένων είναι πολύ πιο εύκολη, καθώς δεν υπάρχει η ανάγκη διαχωρισμού των δεδομένων που προέρχονται από νόμιμη και παράνομη δραστηριότητα. Επομένως, για τη δημιουργία ενός honeypot χρειάζονται σχετικά λίγοι πόροι.

- μπορούν να εντοπίσουν νέα εργαλεία και τακτικές: Στα honeypots, συλλέγεται οτιδήποτε κατευθύνεται προς αυτά, συμπεριλαμβανομένων και νέων κακόβουλων εργαλείων και τακτικών.

- πρόκειται για πολύ απλά συστήματα: Για τη δημιουργία ενός honeypot, δε χρειάζεται η δημιουργία πολύπλοκων αλγορίθμων, η συντήρηση state tables, ούτε η ενημέρωση υπογραφών.

Υπάρχουν, όμως, και κάποια μειονεκτήματα που σχετίζονται με αυτήν την τεχνολογία:

- Περιορισμένη θεώρηση: Τα honeypots μπορούν να εντοπίσουν τη δραστηριότητα που άμεσα αλληλεπιδρά με αυτά. Επομένως, δεν μπορούν να εντοπίσουν επιθέσεις εναντίον άλλων συστημάτων, εκτός και αν ο εισβολέας αλληλεπιδρά ταυτόχρονα και με τα honeypots.

- Κίνδυνος: Όπως όλες οι τεχνολογίες ασφαλείας, έτσι και τα honeypots έχουν κάποιο βαθμό επικινδυνότητας. Πιο συγκεκριμένα, στην περίπτωση των low-interaction honeypots, ο εισβολέας μπορεί αργά ή γρήγορα να καταλάβει ότι πρόκειται για honeypot, όσο καλή και να είναι η εξομοίωση. Αντίθετα, στην περίπτωση των high-interaction honeypots, δεδομένου ότι πρόκειται για πραγματικά συστήματα, είναι αυξημένος ο κίνδυνος ο εισβολέας να τα χρησιμοποιήσει για να βλάψει άλλα συστήματα.

- Δυσκολία επίτευξης συγκεκριμένου στόχου: Αν και τα honeypots μπορούν να εντοπίσουν πολλών ειδών απειλές, ο στόχος δεν είναι πάντα αυτός. Για παράδειγμα, οι επιχειρήσεις μπορεί να μην ενδιαφέρονται για αυτοματοποιημένες ή συνηθισμένες επιθέσεις, αλλά για πιο εξελιγμένες επιθέσεις που στοχεύουν στα κρίσιμα συστήματά τους. Για να καταφέρουν τα honeypots να εντοπίσουν τέτοιες επιθέσεις είναι απαραίτητο να βρίσκονται στον κατάλληλο χώρο και χρόνο και να παρέχουν το κατάλληλο "δόλωμα" στον εισβολέα, πράγμα που απαιτεί μεγάλη οργάνωση και προσπάθεια και είναι αντίθετο με την απλή εφαρμογή και χρήση των honeypots [19].

Τα honeypots μπορούν να χρησιμοποιηθούν για να αντιμετωπίσουν τρεις διαφορετικές καταστάσεις που σχετίζονται με το spam [13]:

1. Την προσπάθεια κλοπής διευθύνσεων από sites στο Internet.

2. Την προσπάθεια σύνδεσης σε proxy για να αποσταλούν μέσω αυτού του server τα spam.

3. Την προσπάθεια προσθήκης SMTP φόρτου σε έναν e-mail server ώστε να σταλούν ανεπιθύμητα μηνύματα.

4.1.1 Harvesting

Το πρώτο βήμα για την αποστολή spam είναι η συλλογή έγκυρων διευθύνσεων e-mail η οποία γίνεται με διάφορους τρόπους [13]. Για παράδειγμα, όταν αποστέλλεται ένα e-mail στο UseNet, τότε η διεύθυνση e-mail είναι διαθέσιμη σε αυτοματοποιημένα προγράμματα που επεξεργάζονται την επικεφαλίδα κάθε μηνύματος που δημοσιεύεται. Με την αποθήκευση συγκεκριμένων πεδίων της επικεφαλίδας (π.χ. From:) οι spammers μπορούν να δημιουργήσουν τεράστιες λίστες με πιθανούς στόχους. Ένα άλλο παράδειγμα συλλογής διευθύνσεων είναι μέσω mailing lists, οι οποίες από λανθασμένη ρύθμιση δίνουν τις διευθύνσεις των συνδρομητών. Μία τρίτη τεχνική βασίζεται σε απλά, αυτοματοποιημένα προγράμματα (crawlers) που ελέγχουν HTML σελίδες στο Internet για links “mailto:”.

Η συχνότερη περίπτωση είναι αυτή των sites, απ’ όπου συγκεντρώνονται e-mail διευθύνσεις. Η ιδέα που μπορεί να χρησιμοποιηθεί για την επίλυση αυτού του προβλήματος είναι ότι αν οι spammers βρουν σε κάποιο site ψεύτικες διευθύνσεις θα εισάγουν στις βάσεις δεδομένων τους μη έγκυρα δεδομένα.

Κατά τη διάρκεια της αυτοματοποιημένης συλλογής διευθύνσεων, οι spammers μπορούν ορισμένες φορές να αναγνωρισθούν από τα εργαλεία που χρησιμοποιούν μέσω του ελέγχου του πεδίου User-Agent που αποστέλλεται από τον browser τους στην επικεφαλίδα της HTTP request. Ένα παράδειγμα πεδίου User-Agent είναι το ακόλουθο:

UserXAgent:(Mozilla/4.0 ((compatible; (MSIE (7.0; (Windows (NT (6.1; (Trident/4.0; (SLCC2; (.NET (CLR (2.0.50727; (.NET (CLR (3.5.30729; (.NET (CLR (3.0.30729; (Media (Center (PC (6.0; (InfoPath.3)

Ορισμένοι προτείνουν τον αποκλεισμό των User-Agents που χρησιμοποιούνται συχνά από spammers ή την ανακατεύθυνσή τους σε sites που περιέχουν πολλές ψεύτικες διευθύνσεις. Ωστόσο, αυτή η πρόταση δεν είναι αποδοτική, καθώς οι spammers μπορούν πολύ εύκολα να αλλάξουν User-Agent. Μία άλλη πρόταση είναι να δημιουργηθούν links, τα οποία δεν είναι ορατά στους επισκέπτες των sites, αλλά θα είναι ορατά στα spambots που ακολουθούν κάθε link και διαβάζουν τον HTML κώδικά του αναζητώντας e-mail διευθύνσεις. Τα sites, λοιπόν, περιμένουν να διαβαστούν από κάποιο spambot και σε αυτή την περίπτωση δημιουργούν δυναμικά ψεύτικες διευθύνσεις.

Υπάρχουν αρκετοί τρόποι να δημιουργηθούν αυτές οι διευθύνσεις. Αυτές οι διευθύνσεις μπορούν να είναι απλώς τυχαία αλφαριθμητικά ή να περιέχουν συγκεκριμένα επιλεγμένες πληροφορίες. Για παράδειγμα, μπορεί να χρησιμοποιηθεί κάποιο script το οποίο θα δημιουργεί δυναμικά ένα link "mailto:" που περιέχει μία ψεύτικη διεύθυνση αποτελούμενη από την IP διεύθυνση του χρησιμοποιούμενου Web client (δηλαδή αυτού που εκκίνησε την HTTP request) και την ημερομηνία. Στη συνέχεια, αν αυτή η διεύθυνση χρησιμοποιηθεί, ο διαχειριστής του mail server θα μπορεί, εφαρμόζοντας έναν έλεγχο ως προς τον παραλήπτη του κάθε μηνύματος, να δει ποιες IP διευθύνσεις χρησιμοποιήθηκαν για τη συλλογή διευθύνσεων και σε ποια ημερομηνία. Ακολουθεί ένα php script που εκτελεί αυτό που περιγράφθηκε παραπάνω.

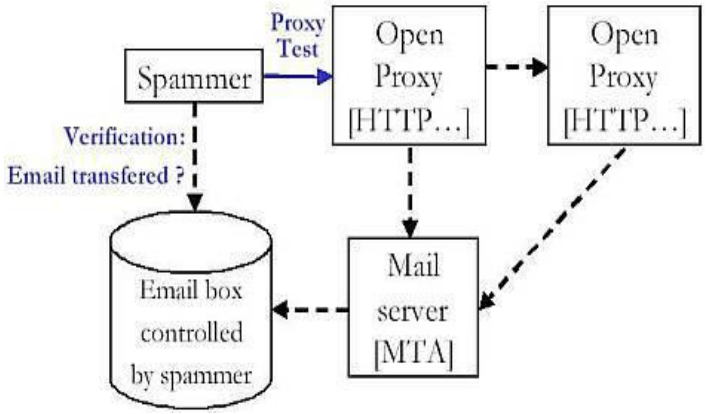
```
<?
echo '<a href="mailto:'.$REMOTE_ADDR.'_'.date('y-m-j')'@host_name" >';
?>
```

Αν και αυτές οι πρακτικές παρουσιάζουν κάποιο ενδιαφέρον, πρέπει να αναφερθεί ότι έχουν αποτέλεσμα μόνο στα απλούστερα είδη spambots, δηλαδή αυτά που χρησιμοποιούνται από όχι και τόσο έμπειρους spammers. Οι πιο έμπειροι spammers συνήθως χρησιμοποιούν open proxies για την αναζήτηση διευθύνσεων σε ιστοσελίδες, οπότε αυτή η μέθοδος θα βοηθούσε στην εύρεση αυτών των open proxies, ενώ οι spammers θα μπορούσαν να διατηρήσουν την ανωνυμία τους.

4.1.2 Open proxies

Μία από τις κύριες διαδρομές που χρησιμοποιούν οι spammers με προορισμό τους mail servers είναι τα open proxies, τα οποία αποδέχονται και αποστέλλουν ελεύθερα requests. Δεν είναι δύσκολο να δημιουργηθεί ένα ψεύτικο open proxy σε κάποιο honeypot, το οποίο μπορεί να εξαπατήσει κάποιους spammers [14]. Πιο συγκεκριμένα, υπάρχουν εργαλεία, όπως το Honeyd, που μπορούν να προσομοιώσουν λειτουργίες των open proxies και των open relays. Ένας spammer μπορεί απλώς να ελέγξει αν ένας server είναι open proxy (δηλαδή υπάρχουν θύρες TCP που απαντάνε) ή και να προσπαθήσει να δει αν το open proxy λειτουργεί σωστά, και στις δύο περιπτώσεις οι πληροφορίες που συλλέγονται από το ψεύτικο open proxy είναι πολύ χρήσιμες.

Τις περισσότερες φορές που ένας spammer συνδέεται σε ένα open proxy προσπαθεί να αποστείλει ένα αρχικό e-mail για να ελέγξει αν λειτουργεί το proxy, όπως φαίνεται στο επόμενο διάγραμμα. Αυτή η στιγμή είναι κρίσιμη στο αν θα εξαπατηθεί ο spammer από το ψεύτικο proxy.



Όταν ο spammer βεβαιωθεί ότι έχει βρει open proxies που λειτουργούν, προσπαθεί μέσω αυτών να φτάσει σε open relays ή σε κάποιο MTA. Αν χρησιμοποιεί αλυσίδα από open proxies, στην οποία ανήκει και το ψεύτικο, τότε είναι δυνατόν από τις πληροφορίες που αυτό συλλέγει από τις TCP συνδέσεις να προσδιορισθούν τα υπόλοιπα open proxies. Με αυτό τον τρόπο μπορούν οι spammers να εντοπισθούν, να επιβραδυνθούν (επιβραδύνοντας τους διαλόγους δικτύου) ή ακόμα και να εμποδιστούν (προσομοιώνοντας και αποφεύγοντας την αποστολή πραγματικών spam).

4.1.3 Open relays

Τα honeypots μπορούν να χρησιμοποιηθούν και για τη δημιουργία ψεύτικων open relays [14]. Υπάρχουν διάφορα εργαλεία που επιτρέπουν τη δημιουργία αυτών των ψεύτικων open relays, όπως είναι το Honeyd που αναφέρθηκε παραπάνω. Η βασική ιδέα είναι τα ψεύτικα open relays να αποδέχονται τα e-mails που στέλνονται σε αυτά και να τα τοποθετούν σε ουρά αποστολής, χωρίς, όμως, να ολοκληρώνουν την αποστολή ποτέ. Φυσικά, θα πρέπει να επιτρέπεται η αναμετάδοση ορισμένων μηνυμάτων, όπως είναι τα αρχικά e-mails που χρησιμοποιούν οι spammers ώστε να ελέγξουν κατά πόσο λειτουργεί σωστά το open relay.

4.2 Δημιουργία honeypot

Στα πλαίσια αυτής της εργασίας δημιουργήθηκε ένα honeypot που σκοπό είχε τη συλλογή πληροφοριών που σχετίζονται με την εύρεση διευθύνσεων σε sites από

τους spammers. Η βασική ιδέα είναι ότι οι spammers, συλλέγοντας με αυτοματοποιημένο τρόπο διευθύνσεις e-mail από διάφορες ιστοσελίδες, θα συλλέξουν και θα χρησιμοποιήσουν και ψεύτικες διευθύνσεις, οι οποίες δεν αντιστοιχούν σε κάποιο χρήστη και ίσως δεν είναι καν ορατές στους επισκέπτες της ιστοσελίδας. Στη συνέχεια, από τα spam που συλλέγονται στο honeypot μπορούν να βρεθούν πληροφορίες για τον spammer και τις τεχνικές που χρησιμοποιεί. Τα βήματα για τη δημιουργία αυτού του honeypot αναλύονται στη συνέχεια.

4.2.1 Mail server

Αρχικά, δημιουργήθηκε ένας mail server σε σύστημα με λειτουργικό σύστημα Ubuntu, του οποίου τα βασικά συστατικά είναι ένας MTA και ένας MDA.

MTA

Ως MTA χρησιμοποιήθηκε ο Postfix, ο οποίος είναι ο προεπιλεγμένος MTA για τα Ubuntu, που σημαίνει ότι λαμβάνει ενημερώσεις ασφαλείας. Κάποιες ιδιαίτερες ρυθμίσεις που έγιναν στον MTA είναι ότι μπλοκαρίστηκε όλος ο φόρτος των εξερχόμενων μηνυμάτων, δηλαδή ρυθμίστηκε ώστε να επιτρέπει μόνο την παραλαβή μηνυμάτων και όχι την αποστολή τους. Αυτό είναι χρήσιμο γιατί ακόμη και αν κάποιος spammer αποκτήσει πρόσβαση σε κάποιο λογαριασμό του συστήματος που αντιστοιχεί σε μία e-mail διεύθυνση, δε θα μπορέσει να στείλει spam μέσω του χρήστη αυτού. Αυτή η ρύθμιση έγινε μέσω της εντολής *transport_maps = hash:/etc/postfix/transport* στο configuration file του Postfix, ενώ το αρχείο που αναφέρεται στην εντολή φαίνεται παρακάτω.

```
server_name :
* discard:
```

Επίσης, κάθε e-mail που αποστέλλεται στον server παραδίδεται οχι μόνο στο αντίστοιχο mailbox, αλλά και σε ένα php script ώστε συγκεκριμένες πληροφορίες των e-mails να εισάγονται σε μία βάση δεδομένων. Το script παρουσιάζεται στο παράρτημα με το όνομα mail.php, ενώ η εντολή στο configuration file του Postfix είναι η *alias_maps = hash:/etc/aliases*. Η γραμμή που ακολουθεί πρέπει να προστεθεί στο αντίστοιχο αρχείο για κάθε mailbox, του οποίου τα εισερχόμενα μηνύματα πρέπει να εισαχθούν στη βάση.

```
mailbox_name: “|php -q mail.php”, mailbox_name
```

MDA

Ως MDA χρησιμοποιήθηκε ο Dovecot, ο οποίος έχει ως πρωταρχικό στόχο την ασφάλεια. Στη συγκεκριμένη περίπτωση ο MDA εγκαταστάθηκε ώστε να υποστηρίζει τόσο το IMAP όσο και το POP3, αλλά και τα πιο ασφαλή IMAPS και POP3S, τα οποία χρησιμοποιούν TLS κρυπτογράφηση για τη σύνδεση.

Ο Dovecot υποστηρίζει δύο μορφές mailbox: το mbox και το Maildir. Αν και το mbox είναι ο πιο συνηθισμένος τρόπος αποθήκευσης των e-mails στα Unix, το Maildir προσφέρει διάφορα πλεονεκτήματα που το καθιστούν καταλληλότερο στις περισσότερες περιπτώσεις.

Η κύρια διαφορά μεταξύ των δύο τύπων είναι ότι στο mbox όλα τα e-mails αποθηκεύονται σε ένα αρχείο, σε αντίθεση με το Maildir στο οποίο κάθε e-mail αποθηκεύεται σε διαφορετικό αρχείο. Λόγω αυτής της διαφοράς, στο Maildir η εύρεση και η διαγραφή κάποιου συγκεκριμένου e-mail γίνεται γρήγορα και δεν υπάρχει η ανάγκη για κλείδωμα αρχείου (file locking), κάτι που είναι απαραίτητο στο mbox αφού παραπάνω από ένα e-mail αποθηκεύονται σε ένα μόνο αρχείο και θα υπήρχε πρόβλημα αλλοίωσης του mailbox αν δύο ή περισσότερες διεργασίες το τροποποιούσαν ταυτόχρονα. Για παράδειγμα, θα μπορούσε ένα πρόγραμμα παράδοσης μηνυμάτων να παραδίδει ένα e-mail, ενώ ταυτόχρονα ένα άλλο πρόγραμμα διαγράφει ένα άλλο e-mail.

Στο συγκεκριμένο mail server χρησιμοποιήθηκε η μορφή Maildir και τα e-mails κάθε χρήστη αποθηκεύονται στο φάκελο *user_name/Maildir/* που περιέχει τους υποφακέλους *cur/*, *new/* και *tmp/*.

Ακολουθεί ένα τμήμα ενός φακέλου τύπου /user_name/Maildir/new. Τα ονόματα των αρχείων χωρίζονται σε τρία μέρη τα οποία διαχωρίζονται με τελεία [3]. Στο πρώτο μέρος, βρίσκεται η ημερομηνία στην οποία παραλήφθηκε το μήνυμα (εδώ η ημερομηνία υπάρχει ως UNIX timestamp, δηλαδή ο αριθμός δευτερολέπτων που έχουν παρέλθει από την 1-1-1970). Στο δεύτερο μέρος, υπάρχει ένα αναγνωριστικό παράδοσης και το τρίτο είναι το όνομα του host. Τέλος, κάθε χαρακτήρας μετά από κόμμα είναι κάποιο “flag” που παίρνει μία τιμή.

```
ls user_name/Maildir/new
1371041453.M472889P16643.host_name,S=3695,W=3755
1371041469.M110295P16674.host_name,S=3715,W=3775
1371041555.M207896P16679.host_name,S=3544,W=3602
1371041737.M718263P16690.host_name,S=3447,W=3504
1371044992.M760696P17035.host_name,S=40974,W=41790
1371048195.M699819P17353.host_name,S=409498,W=414890
```

4.2.2 E-mails

Στη συνέχεια, δημιουργήθηκαν διευθύνσεις e-mail, κάθε μία εκ των οποίων αντιστοιχεί σε έναν χρήστη των Ubuntu. Αν και υπάρχουν και άλλοι τρόποι να δημιουργηθούν διαφορετικές e-mail διευθύνσεις και mailboxes (π.χ. χρησιμοποιώντας virtual mailboxes), ο τρόπος που επιλέχθηκε είναι ο πιο εύκολος και γρήγορος.

Στις διευθύνσεις αυτές λαμβάνονται τα spam, τα οποία αποθηκεύονται στο αντίστοιχο mailbox και χρησιμοποιούνται για την εισαγωγή εγγραφών σε βάση δεδομένων. Για να παραληφθούν spam, οι διευθύνσεις αυτές αναρτήθηκαν σε διάφορα sites χρησιμοποιώντας στο τμήμα boby της HTML ένα tag παρόμοιο με το παρακάτω.

```
<input type="hidden" name="emailContact" value="user_name@host_name">
```

4.2.3 Βάση Δεδομένων

Για να μπορέσουν να εξαχθούν συμπεράσματα για τα spam που λαμβάνονται πρέπει στοιχεία από αυτά να εισάγονται σε μία βάση δεδομένων. Για τη δημιουργία της βάσης χρησιμοποιήθηκε ο MySQL Database Server και τα DDL που κατασκευάζουν τη βάση αυτή εμφανίζονται στο Παράρτημα Α'. Στη βάση εισάγονται στοιχεία από τις επικεφαλίδες των μηνυμάτων, τα path των συνημμένων αρχείων κάθε e-mail, αλλά και το κατά πόσο αυτά τα αρχεία περιέχουν κακόβουλο λογισμικό. Τέλος, λαμβάνονται στοιχεία από διάφορα sites (π.χ. spamcop) τα οποία σχετίζονται με τις IP διευθύνσεις από τις οποίες φαίνεται να προήλθαν τα e-mails, για παράδειγμα το κατά πόσο μία IP διέθυνση ανήκει σε κάποια blacklist. Τα στοιχεία αυτά εισάγονται στη βάση μέσω του php script που περιέχεται στο αρχείο /etc/aliases και διαφόρων php συναρτήσεων, ενώ ένα τμήμα του κώδικα περιλαμβάνεται στο Παράρτημα Β'.

Κεφάλαιο 5

Πιθανές Βελτιώσεις

Η δημιουργία ενός honeypot είναι ένα σημαντικό βήμα προς τη μελέτη του spam. Ωστόσο, υπάρχουν σαφείς περιορισμοί και βελτιώσεις που αφορούν τόσο τεχνικά ζητήματα στον τρόπο λειτουργίας του honeypot, όσο και ιδέες που μπορούν να υλοποιηθούν σε μετέπειτα στάδιο της μελέτης.

Όπως αναφέρθηκε στο κεφάλαιο που περιγράφηκε ο τρόπος δημιουργίας του mail server, το κάθε mailbox αντιστοιχεί σε ένα χρήστη. Αυτή η πρακτική επιλέχθηκε λόγω της απλότητάς της, ωστόσο, δεν μπορεί να γενικευτεί. Για παράδειγμα, αν κριθεί απαραίτητη η δημιουργία κάποιων εκατοντάδων e-mail διευθύνσεων, η μέθοδος αυτή σε καμία περίπτωση δεν είναι η καταλληλότερη. Επομένως, ίσως θα έπρεπε να διερευνηθούν εναλλακτικοί τρόποι δημιουργίας των mailboxes, για παράδειγμα χρησιμοποιώντας virtual domains και virtual mailboxes ή mail aliases.

Επιπλέον, αν και υπάρχει η δυνατότητα εξαγωγής των συνημμένων αρχείων των e-mails, που λαμβάνονται, σε συγκεκριμένο φάκελο, αυτή η εξαγωγή ίσως δεν είναι ο πιο ασφαλής τρόπος επεξεργασίας των συνημμένων αρχείων. Πολλά από τα αρχεία αυτά μπορεί να περιέχουν κακόβουλο λογισμικό, το οποίο μπορεί να βλάψει ή και να καταστρέψει το σύστημα. Ίσως, λοιπόν, θα έπρεπε να βρεθούν άλλοι τρόποι να ελεγχθούν τα αρχεία ώστε να διατηρείται ταυτόχρονα ασφαλές το σύστημα. Μία πιθανή πρόταση είναι η χρήση sandbox.

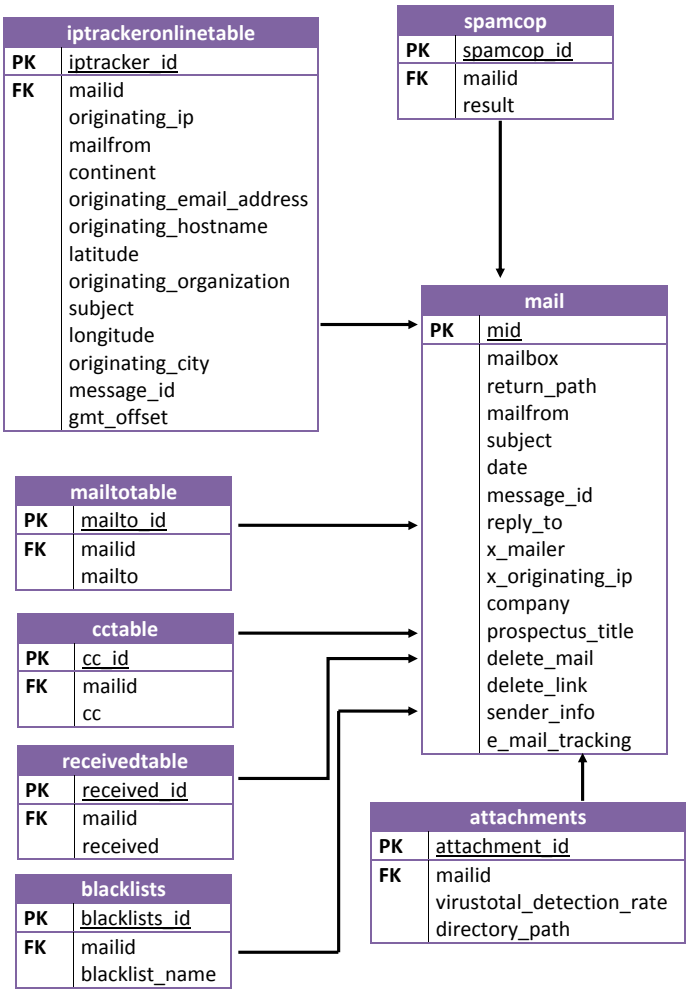
Αν και τα δεδομένα τα οποία συλλέγονται από το honeypot μπορούν να χρησιμοποιηθούν για την εξαγωγή στοιχείων που αφορούν τους spammers και τα μηνύματα που στέλνονται από αυτούς, δεν μπορεί να εξαχθεί κανένα συμπέρασμα για τον τρόπο που έγινε το crawling στις διευθύνσεις. Το script που παρουσιάστηκε στο κεφάλαιο που αφορά τη χρήση των honeypots για την αντιμετώπιση του harvesting (4.4.1) είναι μία πιθανή πρόταση. Ωστόσο, μπορεί να υπάρχουν και καλύτερες εναλλακτικές, καθώς, όπως αναφέρθηκε και εκεί, η πρόταση αυτή μπορεί να παγιδεύσει μόνο τα απλούστερα spambots.

Επίσης, εκτός από το honeypot που δημιουργήθηκε, θα μπορούσαν να διερευνηθούν και τα άλλα δύο είδη honeypots που περιγράφηκαν στο αντίστοιχο κεφάλαιο. Η δημιουργία των τριών ειδών honeypots και η επεξεργασία των δεδομένων που συλλέγονται από αυτά μπορεί να οδηγήσει στην καλύτερη κατανόηση του τρόπου με τον οποίο λειτουργούν οι spammers.

Τέλος, θα πρέπει να μελετηθούν τα δεδομένα που εισέρχονται στο honeypot, ώστε να εξαχθούν χρήσιμα συμπεράσματα. Για παράδειγμα, θα μπορούσαν να αναλυθούν οι IP διευθύνσεις από τις οποίες προέρχονται τα spam και να βρεθεί, αν αυτό είναι δυνατόν, αν χρησιμοποιούνται spambots, open proxies και open relays για αυτή την αποστολή. Θα μπορούσαν να εξάγονται αποτελέσματα όχι μόνο από τις επικεφαλίδες των μηνυμάτων, αλλά και από το σώμα τους. Για παράδειγμα, στην περίπτωση των UCEs να βρεθεί ο διαφημιζόμενος ή στην περίπτωση που το σώμα αποτελείται μόνο από εικόνες να βρεθεί τρόπος εξαγωγής του κειμένου από αυτές. Τα spam που λαμβάνονται θα μπορούσαν, επιπλέον, να χρησιμοποιηθούν στην αξιολόγηση κάποιου φίλτρου (π.χ. του SpamBayes), ιδιαίτερα για μηνύματα που είναι γραμμένα στα ελληνικά.

Παράρτημα Α΄

Βάση Δεδομένων email



Παράρτημα Β΄

PHP scripts

Παρακάτω παρουσιάζονται τα scripts και οι συναρτήσεις που χρησιμοποιήθηκαν για την εισαγωγή των στοιχείων στη βάση δεδομένων. Το mail.php είναι αυτό που συλλέγει τα στοιχεία από τα e-mails όταν αυτά παραδίδονται σε κάποιο mailbox και δέχεται ως όρισμα ($argv[1]) το user_name του χρήστη στον οποίο πρέπει να παραδοθεί το e-mail. Στη συνέχεια, χρησιμοποιώντας και τις βοηθητικές συναρτήσεις που βρίσκονται στο αρχείο functions.php, τα στοιχεία εισάγονται στον κατάλληλο πίνακα της βάσης.

Κάποιες από τις συναρτήσεις του function.php αναζητούν στοιχεία σε ιστοσελίδες, τα οποία εισάγονται σε αντίστοιχους πίνακες της βάσης δεδομένων. Πιο συγκεκριμένα, η iptrackeronline($header) αναζητεί δεδομένα με βάση την επικεφαλίδα του μηνύματος στην ιστοσελίδα *http://www.iptrackeronline.com/email-header-analysis.php*. Επίσης, η spamcop($ip), δεδομένης της IP διεύθυνσης του μηνύματος, όπως αυτή φαίνεται στην επικεφαλίδα του, επιστρέφει αν αυτή είναι στην blacklist του *spamcop.net* ή όχι.

mail.php

```
#!/usr/bin/php
<?php

require_once('functions.php');

// Database info
$hostname = 'localhost';
$dbname   = 'email';
$username = 'user_name';
$password = 'password';

// Email address to send errors to
$email        = “email@which_errors_will_be_sent";

// fetch data from stdin
$data = file_get_contents("php://stdin");

$forwarded = 0;
//check if it is a forwarded mail (this option should be used in abuse systems)
if (is_forwarded($data)) {
  $data = forwarded($data);
  $forwarded = 1;
}

// extract the body
// NOTE: a properly formatted email's first empty line defines the separation between
the headers and the message body
list($data, $body) = explode("\n\n", $data, 2);

//get results from sites
$iptracker = iptrackeronline($data);
$spamcop_ip;
$bl_result;

// explode on new line
$data = explode("\n", $data);

// define a variable map of useful headers
$patterns = array(
  'Return-Path',
  'From',
  'To',
```

```
  'Cc',
  'Subject',
  'Date',
  'Message-ID',
  'Reply-To',
  'X-Mailer',
  'Received',
  'x-originating-ip',
);

// define a variable to hold parsed headers
$headers = array();

// loop through data
foreach ($data as $data_line) {

  // for each line, assume a match does not exist yet
  $pattern_match_exists = false;

  // check for lines that start with white space
  // NOTE: if a line starts with a white space, it signifies a continuation of the previous
header
if (ctype_space(substr($data_line,0,1)) && $last_match) {
  // append to last header
  $headers[$last_match][] = $data_line;
  continue;
}

  // loop through patterns
  foreach ($patterns as $key => $pattern) {

    // create preg regex
    $preg_pattern = '/^' . $pattern .': (.*)$/';

    // execute preg
    preg_match($preg_pattern, $data_line, $matches);

    // check if preg matches exist
    if (count($matches)) {

      $headers[$pattern][] = $matches[1];
      $pattern_match_exists = true;
      $last_match = $pattern;
```

```
    }
  }

  // check if a pattern did not match for this line
  if (!$pattern_match_exists) {
    $headers['UNMATCHED'][] = $data_line;
    $last_match = false;
  }
}

try {
//Connect to the database
  $dbh = new PDO("mysql:host=$hostname;dbname=$dbname", $username,
$password);
  $dbh->setAttribute(PDO::ATTR_ERRMODE, PDO::ERRMODE_EXCEPTION);

  // Insert to table mail
  $stmt1 = $dbh->prepare("INSERT INTO mail(mailbox,return_path,mailfrom,subject
,date,message_id,reply_to,x_mailer,x_originating_ip,forwarded) VALUES
(:mailbox,:return_path,:mailfrom,:subject,:date,:message_id,:reply_to,:x_mailer,:x_origi
nating_ip,:forwarded)");

//Specify values
  $stmt1->bindParam(':mailbox', $argv[1], PDO::PARAM_STR, 255);
  $stmt1->bindParam(':return_path', $headers['Return-Path'][0], PDO::PARAM_STR,
255);
  $stmt1->bindParam(':mailfrom', $headers['From'][0], PDO::PARAM_STR, 255);
  $stmt1->bindParam(':subject', $headers['Subject'][0], PDO::PARAM_STR, 255);
  $stmt1->bindParam(':date', strtotime($headers['Date'][0]), PDO::PARAM_INT);
  $stmt1->bindParam(':message_id', $headers['Message-ID'][0], PDO::PARAM_STR, 255);
  $stmt1->bindParam(':reply_to', $headers['Reply-To'][0], PDO::PARAM_STR, 255);
  $stmt1->bindParam(':x_mailer', $headers['X-Mailer'][0], PDO::PARAM_STR, 255);
  $stmt1->bindParam(':x_originating_ip', $headers['x-originating-ip'][0],
PDO::PARAM_STR, 255);
  $stmt1->bindParam(':forwarded, $forwarded, PDO::PARAM_INT);
  $stmt1->execute();

//Insert to table mailtotable
  $stmt2 = $dbh->prepare("INSERT INTO mailtotable(mailid,mailto) VALUES
(:mailid,:mailto)");
  $sth = $dbh->query("SELECT max(mid) FROM mail");
  $user = $sth->fetch(PDO::FETCH_ASSOC);
  $header = null;
```

```
 $stmt2->bindParam(':mailid', $user['max(mid)'], PDO::PARAM_INT);
 $var = separate_data($headers['To']);
 foreach ($var as $key => $mailto) {
     $stmt2->bindParam(':mailto', $mailto, PDO::PARAM_STR, 255);
     $stmt2->execute();
 }

//Insert to table cctable
 $stmt3 = $dbh->prepare("INSERT INTO cctable(mailid,cc) VALUES (:mailid,:cc)");
 $stmt3->bindParam(':mailid', $user['max(mid)'], PDO::PARAM_INT);
 if (array_key_exists('Cc',$headers)) {
  $var = separate_data($headers['Cc']);
  foreach ($var as $key => $cc) {
     $stmt3->bindParam(':cc', $cc, PDO::PARAM_STR, 255);
     $stmt3->execute();
  }
 }

//Insert to table receivedtable
 $stmt4 = $dbh->prepare("INSERT INTO receivedtable(mailid,received) VALUES
(:mailid,:received)");
 $stmt4->bindParam(':mailid', $user['max(mid)'], PDO::PARAM_INT);
 foreach ($headers['Received'] as $key => $temp) {
     $header .= $temp;
     if ($key==count($headers['Received'])-1 ||
substr($headers['Received'][$key+1],0,5)=='from ') {
       $stmt4->bindParam(':received', $header, PDO::PARAM_STR, 255);
       $stmt4->execute();
       $header = null;
     }
 }

//Insert to table iptrackeronlinetable
 $stmt5 = $dbh->prepare("INSERT INTO iptrackeronlinetable(mailid,originating_ip,
mailfrom, continent, originating_hostname, originating_email_address, latitude,
originating_organization, subject, longitude, originating_country, date, time_zone,
originating_city, message_id, gmt_offset) VALUES (:mailid,:originating_ip, :mailfrom,
:continent, :originating_hostname, :originating_email_address, :latitude,
:originating_organization, :subject, :longitude, :originating_country, :date, :time_zone,
:originating_city, :message_id, :gmt_offset)");
 $stmt5->bindParam(':mailid', $user['max(mid)'], PDO::PARAM_INT);
 $stmt5->bindParam(':originating_ip', $iptracker[0], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':mailfrom', $iptracker[1], PDO::PARAM_STR, 255);
```

```
 $stmt5->bindParam(':continent', $iptracker[2], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':originating_hostname', $iptracker[3], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':originating_email_address', $iptracker[4], PDO::PARAM_STR,
255);
 $stmt5->bindParam(':latitude', $iptracker[5], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':originating_organization', $iptracker[6], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':subject', $iptracker[7],PDO::PARAM_STR, 255);
 $stmt5->bindParam(':longitude', $iptracker[8], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':originating_country', $iptracker[9], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':date', $iptracker[10], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':time_zone', $iptracker[11], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':originating_city', $iptracker[12], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':message_id', $iptracker[13], PDO::PARAM_STR, 255);
 $stmt5->bindParam(':gmt_offset', $iptracker[14], PDO::PARAM_INT, 3);
 $stmt5->execute();

//get result from spamcop
 $spamcop_ip = spamcop($iptracker[0]);

 $stmt6 = $dbh->prepare("INSERT INTO spamcop(mailid,result) VALUES
(:mailid,:result)");
 $stmt6->bindParam(':mailid', $user['max(mid)'], PDO::PARAM_INT);
 $stmt6->bindParam(':result', $spamcop_ip, PDO::PARAM_STR, 255);
 $stmt6->execute();

 $dbh = null;
}
catch(PDOException $e) {
 // If error send email to me
 mail($email, "DB ERROR: " . $headers['Subject'][0], $e->getMessage(), $header);
}
?>
```

functions.php

```
<?php
function nospaces($hname){
 $var = null;
 $i = 0;
 while ($i<strlen($hname)){
  if (!ctype_space(substr($hname,$i,1)) &&  substr($hname,$i,1)<>','){
   $var.=substr($hname,$i,1);
  }
```

```
    $i +=1;
  }
  return $var;
}

function iptrackeronline($header) {
  $post_data['header'] = $header;

  //traverse array and prepare data for posting (key1=value1)
  foreach ( $post_data as $key => $value) {
    $post_items[] = $key . '=' . $value;
  }

  //create the final string to be posted using implode()
  $post_string = implode ('&', $post_items);

  //create cURL connection
  $curl_connection =  curl_init('http://www.iptrackeronline.com/email-header-
analysis.php');

  //set options
  curl_setopt($curl_connection, CURLOPT_CONNECTTIMEOUT, 30);
  curl_setopt($curl_connection, CURLOPT_USERAGENT, "Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1)");
  curl_setopt($curl_connection, CURLOPT_RETURNTRANSFER, true);
  curl_setopt($curl_connection, CURLOPT_SSL_VERIFYPEER, false);
  curl_setopt($curl_connection, CURLOPT_FOLLOWLOCATION, 1);

  //set data to be posted
  curl_setopt($curl_connection, CURLOPT_POSTFIELDS, $post_string);

  //perform our request
  $data = curl_exec($curl_connection);

  //create a dom document to parse the tables
  $dom = new domDocument;

  @$dom->loadHTML($data);
  $dom->preserveWhiteSpace = false;
  $tables = $dom->getElementsByTagName('table');

  $result = array();
```

```
  //parse the Header Analysis table
  $i = 0;$headeranalysis = $tables->item(6)->getElementsByTagName('input');
  foreach ($headeranalysis as $var) {
    $result[$i] = $var->getAttribute('value');
    $i++;
  }

  //parse the IP adresses table
  $ipadresses = $tables->item(5)->getElementsByTagName('tr');
  for($temp=1;$temp < $ipadresses->length; $temp++) {
    $ips = $ipadresses->item($temp)->getElementsByTagName('td')->item(0);
    $result[$i] = $ips->nodeValue;
    $i++;
  }

  //close the connection
  curl_close($curl_connection);
  return $result;
}

function spamcop($ip) {
  $url = 'http://www.spamcop.net/w3m?action=checkblock&ip='. $ip;

  //create cURL connection
  $ch = curl_init();

  //Set curl to return the data instead of printing it to the browser.
  curl_setopt($ch, CURLOPT_URL, $url);

  //set options
  curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 30);
  curl_setopt($ch, CURLOPT_USERAGENT, "Mozilla/4.0 (compatible; MSIE 6.0; Windows
NT 5.1)");
  curl_setopt($ch, CURLOPT_HEADER, 0);
  curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
  curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
  curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);

//perform our request
  $data = curl_exec($ch);

//create a dom document to parse the tables
  $dom = new domDocument;
```

```
  @$dom->loadHTML($data);
  $dom->preserveWhiteSpace = false;
  $tags = $dom->getElementsByTagName('p');

//close the connection
  curl_close($ch);
  $result = $tags->item(0)->nodeValue;
  return $result ;
}

function forwarded($data) {
  list($first_header, $empty_line,$message) = explode("\n\n", $data, 3);
  list($orig_mes,$message) = explode("\n",$message,2);
  return $message;
}

function is_forwarded($data) {
  list($data, $body) = explode("\n\n", $data, 2);
  $data = explode("\n", $data);

  // define a variable map of known headers
  $pattern =  'From';
  // create preg regex
     $preg_pattern = '/^' . $pattern .': (.*)$/';

  foreach ($data as $data_line) {

    // execute preg
    preg_match($preg_pattern, $data_line, $matches);

    // check if preg matches exist
    if (count($matches)) {
      return strpos($matches[1],'Fwd:');
    }
  }
  return false;
}
?>
```

Βιβλιογραφία

[1] Martin Abadi, Mike Burrows, Mark Manasse, and Ted Wobber. Moderately hard, memory-bound functions. *ACM Trans. Internet Technol.*, 5(2):299–327, May 2005.

[2] Ion Androutsopoulos, John Koutsias, Konstantinos Chandrinos, Georgios Paliouras, and Constantine D. Spyropoulos. An evaluation of naive bayesian anti-spam filtering. *CoRR*, cs.CL/0006013, 2000.

[3] Daniel J. Bernstein. Using maildir format.

[4] Gordon V. Cormack. Email spam filtering: A systematic review. *Found. Trends Inf. Retr.*, 1(4):335–455, April 2008.

[5] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '92, pages 139–147, London, UK, UK, 1993. Springer-Verlag.

[6] Christopher Elisan. *Malware, Rootkits and Botnets, A Beginner's Guide*. McGraw-Hill Osborne Media, 2012.

[7] Scott E. Fahlman. Selling interrupt rights: A way to control unwanted e-mail and telephone calls. *IBM Systems Journal*, 41(4):759–, 2002.

[8] Paul Graham. A plan for spam. 2003.

[9] Robert J. Hall. How to avoid unwanted email. *Commun. ACM*, 41(3):88–95, March 1998.

[10] John Ioannidis. Fighting spam by encapsulating policy in email addresses. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2003, San Diego, California, USA*. The Internet Society, 2003.

[11] Saket Kaushik, Paul Ammann, Duminda Wijesekera, William H. Winsborough, and Ronald W. Ritchey. A policy driven approach to email services. In *POLICY*, pages 169–. IEEE Computer Society, 2004.

[12] Oecd. Background paper for the oecd workshop on spam. OECD Digital Economy Papers 78, OECD Publishing, 2004.

[13] Laurent Oudot. Fighting spammers with honeypots: Part 1. 2003.

[14] Laurent Oudot. Fighting spammers with honeypots: Part 2. 2003.

[15] Mehran Sahami, Susan Dumais, David Heckerman, and Eric Horvitz. A bayesian approach to filtering junk e-mail. 1998.

[16] Guido Schryen. *Anti-spam Measures: Analysis and Design*. Springer, Dordrecht, 2007.

[17] SpamBayes-Development-Team. Spambayes: Bayesian anti-spam classifieer written in python.

[18] Lance Spitzner. Honeypots: Definitions and values. 2003.

[19] Lance Spitzner. Problems and challenges with honeypots. 2004.

[20] Brad Templeton. E-stamps.

[21] Trevor Tompkins and Dan Handley. Giving e-mail back to users: Using digital signatures to solve the spam problem. 2003.