ΜΗ ΕΠΙΘΥΜΗΤΗ ΕΠΙΚΟΙΝΩΝΙΑ ΚΑΙ ΕΠΕΞΕΡΓΑΣΙΑ
Τρόποι Αντιμετώπισης

Βασίλης Ζορκάδης
Ηλ. Μηχ., Διδάκτωρ Πληροφορικής Πανεπιστημίου Καρλσρούης
Αρχή Προστασίας Προσωπικών Δεδομένων
zorkadis@dpa.gr

Παρουσίαση στην Ημερίδα του ΤΕΕ
'ΗΛΕΚΤΡΟΝΙΚΕΣ ΕΠΙΚΟΙΝΩΝΙΕΣ, Πόσο ασφαλείς είναι;'
Υπουργείο Μεταφορών & Επικοινωνιών
Αθήνα, 1 Ιουνίου 2006

Περιεχόμενα

- Εισαγωγή στην προβληματική της ανεπιθύμητης επικοινωνίας και επεξεργασίας
- Θεσμικό πλαίσιο (Εθνικό, ΕΕ, USA)
- Τεχνικά Μέτρα
  - Πάροχοι Υπηρεσιών Διαδικτύου και Ηλεκτρονικού Ταχυδρομείου
  - Φίλτρα για τους Τελικούς Χρήστες
- Σχετικές Πρωτοβουλίες (διεθνώς και στη χώρα)
- Ανακεφαλαίωση - Συμπεράσματα

Εισαγωγή

- Το πρόβλημα της ανεπιθύμητης επικοινωνίας και επεξεργασίας
  - 380 εκ. χρήστες Internet (2004, OECD), 137 εκ. με ευρυζωνική σύνδεση (Ιούλιος 2005, OECD), 83 εκ. Domain names, 75 εκ. Web sites (2005, http://news.netcraft.com/)
  - Ανεπιθύμητη επικοινωνία ανέρχεται σε 65-85% της συνολικής, στην Ε.Ε. 53% spam, 80% στην αγγλική, 80% με προέλευση από USA (Wall Street Journal)
  - Παραβίαση Ιδιωτικότητας και πρόβλημα ασφάλειας
  - Επιπτώσεις οικονομικής φύσεως (κόστος, μείωση παραγωγικότητας)
  - Υποβάθμιση ποιότητας παρεχομένων υπηρεσιών
- Εξέλιξη
  - Αρχικά ως διαφημιστικά μηνύματα προϊόντων και υπηρεσιών και ακολούθως και ως μέσα μεταφοράς επιβλαβούς λογισμικού
  - Τεχνολογίες: E-mail (PCs, PDAs, …), κινητή τηλεφωνία (SMS, MMS), Instant Messaging, Weblogs, VoIP
  - Περιεχόμενο: ASCII, HTML, phishing, virus, malicious software
  - Τακτικές:Αποφυγή φίλτρων, απόκρυψη ταυτότητας αποστολέα, εκμετάλλευση υπολογιστικών και επικοινωνιακών πόρων τρίτων

Εισαγωγή

- **Εμπλεκόμενοι, ρόλοι και ανάγκες**
  - Τελικοί χρήστες: θύματα, ανάγκη προστασίας
  - Νομικά πρόσωπα ως παραλήπτες: θύματα, ορισμός δικαιωμάτων, αντιπροσώπου για την περίπτωση συγκατάθεσης
  - Αρχές: αρμόδιες για εφαρμογή της νομοθεσίας (αρχές προστασίας δεδομένων, προστασίας καταναλωτή, αστυνομικές και δικαστικές αρχές), συνεργασία
  - Πάροχοι υπηρεσιών ηλεκτρονικών υπηρεσιών: θύματα (και ίσως και θύτες), επιβολή πολιτικών αποδεκτής χρήσης (Acceptance Use Policy)
  - Ενώσεις διαφημιστών: κώδικες δεοντολογίας
  - Ενώσεις προστασίας καταναλωτών: ενημέρωση – ευαισθητοποίηση
  - Εταιρίες λογισμικού: ευθύνη για εργαλεία συλλογής ηλεκτρονικών διευθύνσεων
- **Μέτρα, Πρωτοβουλίες**
  - Θεσμικό πλαίσιο
  - Διεθνής συνεργασία αρμοδίων αρχών
  - Πρωτοβουλίες και μέτρα εμπλεκόμενων φορέων
  - Τεχνικά μέτρα φορέων και τελικών χρηστών
  - Ευαισθητοποίηση - ενημέρωση

Θεσμικό Πλαίσιο

- **Άρθρο 13 Οδηγίας 2002/58/ΕΚ αναφέρεται στις αυτόκλητες κλήσεις**:
  - Η χρησιμοποίηση αυτόματων συστημάτων κλήσης χωρίς ανθρώπινη παρέμβαση (συσκευές αυτόματων κλήσεων), τηλεομοιοτυπίας ή ηλεκτρονικού ταχυδρομείου για σκοπούς απευθείας προώθησης επιτρέπεται μόνο κατόπιν συγκατάθεσης (opt-in)
  - Εξαίρεση αν στοιχεία επαφής αποκτήθηκαν στο πλαίσιο πώλησης προϊόντων ή υπηρεσιών (opt-out),
  - Σε άλλες περιπτώσεις (με ανθρώπινη παρέμβαση), επαφίεται στον εθνικό νομοθέτη να επιλέξει μεταξύ opt-in και opt-out,
  - Απαγόρευση συγκάλυψης ή απόκρυψης της ταυτότητας του αποστολέα ή του προσώπου προς όφελος του οποίου αποστέλλεται το μήνυμα. Επίσης, απαγόρευση αποστολής μηνυμάτων χωρίς έγκυρη διεύθυνση για ανάκληση συγκατάθεσης ή τερματισμό της επικοινωνίας,
  - Ισχύς προστασίας και για νομικά πρόσωπα.

- **Άρθρο 11 νομοσχεδίου που μεταφέρει την Οδηγία**
  - Opt-in για συστήματα κλήσης χωρίς και με ανθρώπινη παρέμβαση.
  - Ωστόσο, προβλέπει και δυνατότητα δήλωσης συνδρομητών προς τους φορείς παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ότι δεν επιθυμούν γενικώς να δέχονται τέτοιες επικοινωνίες.

Θεσμικό Πλαίσιο

- **Διαφορές στα κράτη-μέλη**:
  - Opt-in ή opt-out,
  - Μητρώα,
  - Προστασία φυσικών και νομικών προσώπων,
  - Επιπτώσεις, European Contact Network of Spam Authorities (CNSA)

- **Νομικό πλαίσιο ΗΠΑ** (Controlling the Assault of Non-Solicited Pornography and Marketing - CAN SPAM Act of 2003)
  - Μελέτη του FTC σχετικά με τη δυνατότητα δημιουργίας Do-Not-Spam-List
  - Απαγόρευση συγκάλυψης ή απόκρυψης της ταυτότητας του αποστολέα,
  - Απαγόρευση αυτόματης συλλογής στοιχείων επικοινωνίας από Web sites ή αυτόματης δημιουργίας δυνατών διευθύνσεων, συνδυάζοντας ονόματα, γράμματα ή αριθμούς,
  - Υποχρέωση συμπερίληψης της πραγματικής φυσική διεύθυνσης του αποστολέα,
  - Επίσης, έγκυρης διεύθυνσης για δυνατότητα opt-out σε κάθε μήνυμα,
  - Απαγόρευση αυτόματων μέσων για την εγγραφή και απόκτηση λογαριασμών ηλεκτρονικού ταχυδρομείου, καθώς και των relay δυνατοτήτων τρίτων
  - Κυρώσεις.

Τεχνικά και Οργανωτικά Μέτρα

- **Πάροχοι Υπηρεσιών Διαδικτύου και Ηλεκτρονικού Ταχυδρομείου**
  - Blacklists (απόρριψη κάθε μηνύματος με διεύθυνση προέλευσης που περιέχεται στη λίστα γνωστών αποστολέων spam),
  - Whitelists (στην περίπτωση μαζικών αποστολών, αποδοχή των μηνυμάτων που προέρχονται από εγκεκριμένους-καταχωρημένους στη λίστα αποστολείς, άλλως εκκίνηση μηχανισμού challenge – response με την αυτόματη δημιουργία και μετάδοση μηνύματος προς το αποστολέα και την απαίτηση να καταχωρήσει σε δεδομένο σύνδεσμο στοιχεία από το μήνυμα, καθώς και μη αυτοματοποιημένη επίλυση αποδοχής ή μη),
  - Greylisting (προσωρινή απόρριψη (4xx failure codes) μηνυμάτων που προέρχονται από άγνωστους αποστολείς, υποθέτοντας εγκατάλειψη της προσπάθειας μετάδοσης στην περίπτωση ανεπιθύμητης επικοινωνίας, σε αντίθεση με την περίπτωση της επιθυμητής επικοινωνίας. Συνδυάζεται με whitelists, όπου περιέχονται όσοι προσπαθούν και πάλι και βασίζεται σε IP, αποστολέα και παραλήπτη, αλλά και σε σύνοψη του μηνύματος. Εναλλακτικά, καθυστέρηση στην προώθηση μηνυμάτων από άγνωστες πηγές θεωρώντας ότι αν είναι από αποστολείς spam, αυτοί θα εμφανιστούν στο μεταξύ σε σχετικές blacklists), προβλήματα (απώλεια επιθυμητών μηνυμάτων, καθυστέρηση στην παράδοση),

Τεχνικά και Οργανωτικά Μέτρα

- **Πάροχοι Υπηρεσιών Διαδικτύου και Ηλεκτρονικού Ταχυδρομείου**
  - Προσφορά 'disposable' διευθύνσεων (ο κάτοχος μπορεί να προσδιορίσει τις διευθύνσεις από τις οποίες αποδέχεται μηνύματα, ενώ από άλλες διευθύνσεις απορρίπτονται ή η ισχύς μιας διεύθυνσης εκπνέει μετά από κάποιο χρόνο),
  - Αυθεντικοποίηση ηλεκτρονικού μηνύματος (emerging)
    - Sender Policy Framework (SPF), Sender-ID (για να ελεγχθεί αν e-mail server authorized to send on behalf of a given domain, διαφέρουν στην ταυτότητα που ελέγχουν, SPF το πεδίο του φακέλου MAIL FROM (rfc 2821) και SENDER-ID την επικεφαλίδα (rfc 2822). SPF και Sender-ID δημοσιεύονται στο DNS. Ακόμα, έλεγχος της IP του server του αποστολέα.
    - Εφαρμογή ψηφιακής υπογραφής (επισυνάπτεται του μηνύματος και ελέγχεται με τη βοήθεια του δημοσίου ή του κλειδιού επαλήθευσης, που έχει δημοσιοποιηθεί στο DNS)
  - Φίλτρα ταξινόμησης μηνυμάτων,
  - Ενημέρωση-ευαισθητοποίηση συνδρομητών σχετικά με open relays, open proxies, συμπεριλαμβανομένου περιοδικού ελέγχου για τον εντοπισμό τους,
  - Κώδικες δεοντολογίας, αποδεκτές πολιτικές χρήσης

Τεχνικά Μέτρα για Τελικούς Χρήστες

- **Φίλτρα ταξινόμησης εισερχομένων μηνυμάτων**
  - Επιλογή χαρακτηριστικών γνωρισμάτων
    - Ρίζες λέξεων,
    - Stop terms (δεν λαμβάνονται υπόψη άρθρα, αντωνυμίες και γενικά λέξεις που εμφανίζονται σε κάθε τύπο κειμένου),
    - Αμοιβαία πληροφορία,
    - Διάσταση και τύπος διανύσματος γνωρισμάτων.
  - Αλγόριθμοι ταξινόμησης μηνυμάτων
    - Naïve-Bayes,
    - AdaBoost,
    - Classification via Regression,
    - MultiBoost,
    - Random Committee,
    - ADTree,
    - ID3-Tree,
    - Νευρωνικά δίκτυα,
    - Γενετικοί .
  - Εσφαλμένα θετικά versus Εσφαλμένα αρνητικά

Τεχνικά Μέτρα για Τελικούς Χρήστες

- **Φίλτρα ταξινόμησης εισερχομένων μηνυμάτων**

	Training Stage				Validation Stage			
	Legitimate Messages		Spam Messages		Legitimate Messages		Spam Messages	
Algorithm	**Best**	**Worst**	**Best**	**Worst**	**Best**	**Worst**	**Best**	**Worst**
Naive Bayes	**8**	**11**	**56**	**70**	**4**	**10**	**26**	**69**
AdaBoostM1	**5**	**37**	**31**	**82**	**5**	**22**	**26**	**69**
Class.v. Regr.	**3**	**5**	**12**	**17**	**7**	**16**	**15**	**27**
MultiBoostAB	**5**	**37**	**31**	**82**	**5**	**27**	**26**	**69**
R. Committee	**0**	**0**	**0**	**0**	**0**	**2**	**52**	**65**
ADTree	**13**	**20**	**34**	**41**	**8**	**19**	**13**	**37**
trees.Id3	**0**	**0**	**0**	**0**	**20**	**37**	**15**	**25**
RandomTree	**0**	**0**	**0**	**0**	**43**	**52**	**42**	**81**

Σχετικές Πρωτοβουλίες

- Διεθνείς πρωτοβουλίες
  - OECD (Anti-Spam ToolKit)
  - ASTA (Anti-Spa Technical Alliance)
  - ENISA
  - LONDON ACTION PLAN
  - CNSA (European Contact Network of Spam Authorities)
- Πρωτοβουλίες Αρχής Προστασίας Δεδομένων
  - Συνεργασία με αρμόδιες αρχές κρατών-μελών ΕΕ
  - Υποστήριξη παρόχων υπηρεσιών Διαδικτύου για την κατάρτιση κώδικα δεοντολογίας
  - Προετοιμασία εκδηλώσεων ενημέρωσης εμπλεκομένων

Ανακεφαλαίωση - Συμπεράσματα

- Εμπόδιο στην ανάπτυξη της ψηφιακής επικοινωνίας, σοβαρή απειλή για την ιδιωτικότητα και την ασφάλεια
- Θεσμικό πλαίσιο, αρμόδιες αρχές
- Άλλοι εμπλεκόμενοι φορείς (ISPs, ενώσεις καταναλωτών, εταιρίες λογισμικού)
- Αναγνώριση αναγκαιότητας συνεργασίας των εμπλεκομένων φορέων
- Εφαρμογή κατάλληλων τεχνικών μέτρων, λαμβάνοντας ιδίως υπόψη και την ανάπτυξη συστημάτων περιρρέουσας νοημοσύνης (ambient intelligence ή ubiquitous copmuting) σε συνδυασμό με τα ιδιαίτερα προβλήματα που δημιουργούνται