OWASP - The Open Web Application Security Project

Ελληνική Ομάδα Εργασίας - http://www.owasp.gr

Μηνιαίο Ενημερωτικό Δελτίο – Δεκέμβριος 2006

ΕΛΛΗΝΙΚΗ ΕΠΙΚΑΙΡΟΤΗΤΑ

Μηνιαίο Ενημερωτικό Δελτίο Ελληνικής Ομάδας Εργασίας του OWASP

Καλώς ήλθατε στο πρώτο μηνιαίο ενημερωτικό δελτίο της Ελληνικής ομάδας εργασίας του OWASP. Στόχος μας είναι η ενημέρωση γύρω από τα θέματα της ελληνικής επικαιρότητας που αφορούν στην ασφάλεια των εφαρμογών διαδικτύου αλλά και στην ασφάλεια γενικότερα. Αν και στο Internet υπάρχουν ήδη πολλές πηγές ενημέρωσης γύρω από θέματα ασφάλειας (π.χ. securityfocus, cryptogram, blogs, κλπ), αυτές επικεντρώνονται συνήθως στη διεθνή επικαιρότητα. Έτσι, μοιραία η ενημέρωση για τα security θέματα που αφορούν στην Ελλάδα προέρχεται από τα τοπικά ειδησεογραφικά site και μέσα.

Με το μηνιαίο αυτό newsletter στοχεύουμε στην αποτύπωση των κυριότερων θεμάτων ασφάλειας που απασχολούν την Ελληνική επικαιρότητα κάθε μήνα, αλλά και σημαντικών νέων από τη διεθνή infosec επικαιρότητα που κρίνουμε πως πρέπει να σχολιάσουμε. Παράλληλα, θα υπάρχουν ενδιαφέροντα επιστημονικά θέματα αλλά και ενημέρωση γύρω από τη δραστηριότητα του OWASP. Το newsletter θα διαμοιράζεται μέσω της mailing list του OWASP.gr, ενώ ταυτόχρονα θα δημοσιεύεται και στο site σε μορφή pdf.

Ελπίζουμε πως θα βρείτε το newsletter αυτό ενδιαφέρον και χρήσιμο. Φυσικά, βρίσκεται σε… εμβρυικό στάδιο. Για το λόγο αυτό κάθε συνεισφορά σας στη δημιουργία του θα ήταν ιδιαίτερα σημαντική, για να γίνει το newsletter πιο χρήσιμο για όλους. Έτσι, για οποιαδήποτε σχόλια, προσθήκες, προτάσεις, παρατηρήσεις ή συζητήσεις μπορείτε να απευθύνεστε στη mailing list του OWASP.gr (owasp-greece@lists.owasp.org).

Internet Governance Forum: Openness and Security

Από τις 30 Οκτωβρίου ως τις 2 Νοεμβρίου, πραγματοποιήθηκε στη χώρα μας το 1ο Παγκόσμιο Συνέδριο για τη Διακυβέρνηση του Internet (Internet Governance Forum), που διοργάνωσε το Υπουργείο Μεταφορών και Επικοινωνιών υπό την αιγίδα του ΟΗΕ. Το συνέδριο συγκέντρωσε μεγάλο ενδιαφέρον καθώς συμμετείχαν αντιπροσωπείες από όλο τον κόσμο αλλά και σημαντικές προσωπικότητες του Internet. Τα κυριότερα θέματα που συζητήθηκαν ήταν ο ανοιχτός χαρακτήρας του Internet (Openness), η ασφάλεια, η διαφορετικότητα και η ελευθερία πρόσβασης.

Το OWASP παρακολούθησε τη δεύτερη μέρα του συνεδρίου, που επικεντρώθηκε σε θέματα ασφάλειας και openness. Το πρωί, στο πάνελ του Openness, του οποίου

προέδρευε ο υπουργός κ. Θ. Ρουσόπουλος, συμμετείχαν εκπρόσωποι του BBC, της CreativeCommons, της Microsoft, του Ευρωπαϊκού Κοινοβουλίου και άλλοι. Η συζήτηση που έγινε σχετικά με τον ανοιχτό χαρακτήρα του Internet ήταν πολύ ενδιαφέρουσα καθώς θίχτηκαν θέματα ελευθερίας της έκφρασης και της δημιουργίας, πνευματικών δικαιωμάτων αλλά και του δικαιώματος στην ελεύθερη και αντικειμενική ενημέρωση. Η παρουσία εκπροσώπων φορέων που εκφράζουν αντιδιαμετρικές απόψεις στα παραπάνω θέματα συνετέλεσε στη διεξαγωγή ενός γόνιμου διαλόγου που προβλημάτισε τους παρευρισκόμενους. Η συνεδρία κατέληξε με την αναμενόμενη ερώτηση προς τον κ. Ρουσόπουλο, σχετικά με τη σύλληψη του Έλληνα blogger. Ο υπουργός, αν και δήλωσε άγνοια για το περιστατικό, επιτέθηκε στους Έλληνες bloggers αναφέροντας ότι ουσιαστικά διαδίδουν ψευδείς ειδήσεις και πληροφορίες χωρίς να επιτρέπουν αντίλογο και υποστήριξε ότι θα έπρεπε να υπάρχει ενιαίος κώδικας δεοντολογίας για τα blogs, παρόμοιος με αυτός που ισχύει για τους δημοσιογράφους.

Παράλληλα με την κύρια συνεδρία, υπήρχαν πιο εξειδικευμένες ομιλίες σε ενδιαφέροντα workshops. Στο Infrastructure Security συζητήθηκαν κυρίως θέματα ασφάλειας των root servers του Internet ενώ διατυπώθηκε έντονος προβληματισμός για το κόστος της ασφάλειας των διαδικτυακών υποδομών αλλά και τη διακρατική συνεργασία. Σε ένα άλλο πάνελ (Privacy and Identity Matters) συζητήθηκαν θέματα που αφορούν στην ιδιωτικότητα και την προστασία των προσωπικών δεδομένων. Ειδικότερα, η συζήτηση επικεντρώθηκε σε συστήματα διαχείρισης ταυτοτήτων, στους όρους προστασίας προσωπικών δεδομένων αλλά και στο δικαίωμα της ανωνυμίας και του απορρήτου. Στα θέματα ιδιωτικότητας επικεντρώθηκε και το workshop με τίτλο «Privacy, Development and Globalisation», δίνοντας έμφαση σε διεθνή θέματα, όπως η προστασία των προσωπικών δεδομένων σε διακρατικές συναλλαγές και η αντίστοιχη νομοθεσία σε διαφορετικές χώρες. Συζήτηση έγινε και για το θέμα της «διαρροής» προσωπικών πληροφοριών μέσα από την υπηρεσία WHOIS. Επίσης, παρουσιάστηκαν συνοπτικά τα αποτελέσματα της έρευνας που διεξήγαγε η οργάνωση Privacy International σχετικά με την ιδιωτικότητα, στα οποία η Ελλάδα βαθμολογήθηκε πολύ καλά, σε αντίθεση με χώρες όπως η Αγγλία και η Αμερική (http://www.privacyinternational.org/survey/phr2005/phr2005spread.jpg).

Στην απογευματινή συνεδρία που θέμα της ήταν η ασφάλεια στο Internet η συζήτηση επικεντρώθηκε στην προστασία από το spam και την ασφάλεια στις ηλεκτρονικές συναλλαγές. Ενδιαφέρον είχε η παρουσία εκπροσώπου της κυβέρνησης της Κίνας, ο οποίος δέχτηκε πολλές ερωτήσεις για τους ελέγχους και τους περιορισμούς που επιβάλλει η χώρα του στο Internet. Παράλληλα, εκφράστηκε έντονα η άποψη ότι δεν αρκεί να χρεώνονται όλα τα προβλήματα ασφάλειας του Internet στην έλλειψη ενημέρωσης και εκπαίδευσης των χρηστών, αλλά θα πρέπει το ίδιο το μέσο να γίνει εγγενώς ασφαλέστερο. Τέλος, αίσθηση προκάλεσε η δήλωση εκπροσώπου Αφρικανικής χώρας που κατηγόρησε τους παρευρισκόμενους για την έλλειψη ενδιαφέροντος για τη διείσδυση του Internet στην ήπειρό του. Το συγκεκριμένο θέμα συζητήθηκε την επόμενη μέρα του συνεδρίου.

Στο τελευταίο workshop της ημέρας (Freedom of Expression, Internet Filtering & Blocking by States) αναλύθηκαν ζητήματα που αφορούν στον έλεγχο της πρόσβασης στο Internet. Ενδεικτικά αναφέρθηκε ότι περίπου 40 κράτη παγκοσμίως έχουν εγκαταστήσει μηχανισμούς ελεγχόμενης πρόσβασης στο διαδίκτυο ενώ η συζήτηση επικεντρώθηκε στα φίλτρα ελέγχου περιεχομένου και την αποτελεσματικότητά τους.

Η αίσθηση που προκάλεσε το πρώτο Internet Governance Forum ήταν μάλλον αυτή του προβληματισμού και του διαλόγου παρά των συμπερασμάτων. Έντονη ήταν η ανησυχία σχετικά με το τι μέλλει γεννέσθαι μετά το συνέδριο και με το αν οι υπεύθυνοι θα λάβουν σοβαρά υπόψη τους τα συμπεράσματα και τις ανησυχίες των ειδικών αλλά και των χρηστών. Γεγονός είναι πάντως πως αν μη τι άλλο το συνέδριο

συγκέντρωσε έντονο ενδιαφέρον και προσωπικότητες από όλο τον κόσμο. Ας ελπίσουμε ότι ο ρόλος που θα διαδραματίσει θα είναι ο προσδοκώμενος, πράγμα που πιθανώς θα φανεί σε ένα χρόνο στο 2ο Internet Governance Forum.

Ευχαριστούμε θερμά τον tnu, από το post του οποίου στο group dit.internet του news server testnews.di.uoa.gr αντλήθηκαν πολύτιμες πληροφορίες και εμπειρίες για το IGF. Για μια αναλυτικότερη (και πιο γλαφυρή) επισκόπηση των ομιλιών και των συζητήσεων που έλαβαν χώρα στο IGF, μπορεί κανείς να ανατρέξει στο παραπάνω group. Επίσης, στην επίσημη ιστοσελίδα του IGF (http://www.igfgreece2006.gr) είναι διαθέσιμες όλες οι ομιλίες.

Σύλληψη Έλληνα Blogger

Λίγο πριν ξεκινήσει τις εργασίες του το 1ο Παγκόσμιο Συνέδριο για τη Διακυβέρνηση του Internet, ο διαδικτυακός κόσμος προβληματίστηκε έντονα από την αποκάλυψη της δίωξης του ιδιοκτήτη του blogme.gr. Το blogme.gr είναι από τους πιο γνωστούς blog aggregators στην Ελλάδα, που συγκεντρώνει καθημερινά υλικό από την Ελληνική blogοσφαίρα. Ο δημιουργός του blogme.gr, Αντώνης Τσιπρόπουλος, συνελήφθη, διότι το site του περιείχε δυσφημιστικό υλικό, το οποίο σύμφωνα με πληροφορίες που κυκλοφορούν, αφορούσε σε «γνωστό δημόσιο πρόσωπο». Η υπόθεση αυτή, η οποία εκκρεμεί ακόμα, είναι πρωτοφανής όχι μόνο για τα ελληνικά αλλά και τα διεθνή δεδομένα. Χαρακτηριστικό επίσης είναι ότι η αποκάλυψή της συνέπεσε με το IGF, παρόλο που απ' ότι φαίνεται η σύλληψη είχε γίνει 5 μήνες πριν. Αξίζει, τέλος, να σημειωθεί, ότι πέρα από την ελευθερία της έκφρασης που θίγεται άμεσα από τέτοιες διώξεις, το θέμα είναι και τεχνικό, καθώς ουσιαστικά δε μηνύεται αυτός που δυσφημεί αλλά κάποιος που απλά παρέχει ένα σύνδεσμο προς αυτόν.

Παραπλανητικές επιστολές της…Coca Cola: snail mail phishing

Πρόσφατα η Γενική Γραμματεία Καταναλωτή ενημέρωσε το κοινό ότι κύκλωμα επιχειρεί να εξαπατήσει πολίτες αποστέλλοντας τους επιστολές με το λογότυπο της Coca Cola, καθώς και άλλων εταιριών, που αναφέρουν πως έχουν κερδίσει ένα μεγάλο ποσό σε κάποιο διαγωνισμό. Για να λάβουν οι… τυχεροί το ποσό αυτό, απαραίτητο είναι να στείλουν στοιχεία όπως ΑΦΜ, αριθμούς τραπεζικών λογαριασμών, πιστωτικών καρτών κ.α. σε μία διεύθυνση στην Ισπανία. Πρόκειται φυσικά για απάτη, ουσιαστικά phishing, η οποία φαίνεται πως έχει λάβει μεγάλες διαστάσεις.

Νέα κρούσματα phishing σε Ελληνικές τράπεζες

Μέσα στο Νοέμβριο εμφανίστηκαν τουλάχιστον τρία νέα κρούσματα απόπειρας phishing με στόχο γνωστές Ελληνικές τράπεζες. Ειδικότερα, πολλοί χρήστες έλαβαν e-mail που τους καλούσαν, για λόγους ασφαλείας, να υποβάλουν προσωπικά τους στοιχεία σε κάποιο site που έμοιαζε οπτικά με αυτό της τράπεζας. Είναι φανερό πως και η χώρα μας έχει πλέον εισέλθει για τα καλά στο στόχαστρο των phishers, οι οποίοι μάλιστα φαίνονται να έχουν βελτιώσει σημαντικά τα Ελληνικά τους. Οι τράπεζες από τη μεριά τους, με συνεχείς σχετικές ανακοινώσεις και προειδοποιήσεις, προσπαθούν να ενημερώσουν το κοινό. Βέβαια, μία απλή ανακοίνωση στο site συχνά περνά απαρατήρητη. Αντίθετα, μία επισήμανση στην πρώτη σελίδα της υπηρεσίας e-banking ή ακόμα καλύτερα, στη μηνιαία έκθεση λογαριασμού που αποστέλλεται στο σπίτι, μάλλον θα γινόταν περισσότερο αισθητή.

Αυξημένα μέτρα για την τρομοκρατία και στο Ελ. Βενιζέλος

Από τις 6 Νοεμβρίου ισχύουν και στην Ελλάδα τα αυξημένα μέτρα που έχει επιβάλει η Ευρωπαϊκή Ένωση σχετικά με τη μεταφορά υγρών από επιβάτες στα αεροπλάνα.

Έτσι, πλέον, οι επιβάτες έχουν δικαίωμα να μεταφέρουν μικρές μόνο ποσότητες υγρών στις χειραποσκευές τους, σε δοχεία χωρητικότητας μέχρι 100ml, που συνολικά να μην ξεπερνούν το 1 λίτρο. Τα δοχεία θα τοποθετούνται σε ειδική σακούλα και κάθε επιβάτης θα μπορεί να μεταφέρει μόνο μία τέτοια σακούλα. Από τους περιορισμούς εξαιρούνται αντικείμενα που αγοράζονται από τα καταστήματα αφορολογήτων ειδών. Το αεροδρόμιο Ελευθέριος Βενιζέλος αύξησε κατά 30% το προσωπικό ασφαλείας, ενώ φρόντισε για την έγκαιρη και σωστή ενημέρωση του επιβατικού κοινού με αποτέλεσμα να μην υπάρξουν σημαντικές καθυστερήσεις.
Τα νέα μέτρα ασφαλείας στα αεροδρόμια έχουν προκαλέσει πολλές συζητήσεις ήδη από τότε που πρωτο-εφαρμόστηκαν στην Αμερική και δυστυχώς μάλλον πρόκειται για νέους ανούσιους και άχρηστους περιορισμούς. Πέρα από την δεδομένη ταλαιπωρία οι επιβάτες, οι οποίοι μετά από τους νυχοκόπτες τους είδαν τα σαμπουάν τους να κατηγορούνται ως τρομοκρατικά όπλα, θα επωμιστούν και το παραπάνω κόστος των νέων μέτρων, είτε αυτό είναι αποτέλεσμα των καθυστερήσεων είτε της αύξησης του προσωπικού. Στην Αμερική έχουν ήδη αναφερθεί πολλά τραγελαφικά περιστατικά, με υπεύθυνους ασφαλείας να ισχυρίζονται ότι το ίδιο μπουκαλάκι σαμπουάν είναι ακίνδυνο όταν μεταφέρεται μέσα στην ειδική σακούλα, αλλά εξαιρετικά επικίνδυνο όταν βρίσκεται εκτός σακούλας. Και βέβαια, όσα μπουκαλάκια κατάσχονται, είτε γιατί υπερβαίνουν το όριο βάρους είτε γιατί κρίνονται επικίνδυνα, είτε γιατί μεταφέρονται εκτός της ειδικής σακούλας, πετιούνται στα… σκουπίδια κι ας θεωρούνται επικίνδυνα χημικά, εκρηκτικά ή ό,τι άλλο.

OWASP.gr

Η Ελληνική ομάδα εργασίας του OWASP επικεντρώνεται στη διάδοση του OWASP στην Ελλάδα. Στα πλαίσια της προσπάθειας αυτής έρχεται σε επαφή με επαγγελματίες του χώρου και ενημερώνει σχετικά με τις δραστηριότητές της τον ειδικό τύπο. Σταδιακά προετοιμάζεται και η πρώτη συνάντηση των μελών, η οποία προγραμματίζεται να πραγματοποιηθεί στις αρχές του 2007.

Ο Υπάτιος Ασμανίδης μαζί με τον Ιωάννη Τζίμο ανέλαβαν τη μετάφραση του «Web Services Security». Όποιος επιθυμεί να βοηθήσει στην προσπάθεια αυτή μπορεί να επικοινωνήσει μαζί τους μέσω της λίστας ηλεκτρονικού ταχυδρομείου της Ελληνικής ομάδας εργασίας του OWASP (owasp-greece@lists.owasp.org).

Η Ελληνική ομάδα εργασίας του OWASP προετοιμάζει μία λίστα με συμβουλές για την αντιμετώπιση του phishing (OWASP Anti-phishing Top 10). Μπορείτε να υποβάλλετε τις προτάσεις και τις ιδέες σας στην παραπάνω λίστα.

Στις 30 Οκτωβρίου το OWASP παρουσίασε την πρώτη έκδοση του OWASP Pantera, ενός Web Assessment εργαλείου. Πρόκειται για μία σουίτα εργαλείων που συνδυάζει έναν pentest proxy, έναν application scanner και ένα έξυπνο πλαίσιο ανάλυσης. Στόχος του Pantera είναι να αυτοματοποιήσει την ανάλυση και τις εργασίες που επαναλαμβάνονται, αφήνοντας τις σημαντικές αποφάσεις στους ειδικούς. Το OWASP Pantera είναι διαθέσιμο σύμφωνα με το GPL από τη διεύθυνση: http://www.owasp.org/index.php/Category:OWASP_Pantera_Web_Assessment_Studio_Project

ΔΙΕΘΝΗ ΚΑΙ ΑΛΛΑ

Έρευνα για την ιδιωτικότητα και τα ανθρώπινα δικαιώματα
Ο διεθνής οργανισμός Privacy International παρουσίασε τα αποτελέσματα της ετήσιας έρευνας που έκανε σχετικά με το σεβασμό της ιδιωτικότητας του ατόμου σε διεθνές επίπεδο. Η φετινή έκθεση ερευνά την πρόοδο που έχει γίνει σε 70 χώρες σχετικά με την προστασία των δικαιωμάτων και της ιδιωτικότητας των πολιτών αλλά και τις «κοινωνίες επιτήρησης». Περισσότεροι από 200 ειδικοί ανά τον κόσμο προσέφεραν υλικό για το 1200 σελίδων κείμενο που δημιουργήθηκε. Μάλιστα, για πρώτη φορά χώρες βαθμολογήθηκαν σε διάφορους σχετικούς τομείς. Έτσι δημιουργήθηκε μία λίστα που συμπεριλαμβάνει όλες τις χώρες της Ευρωπαϊκής Ένωσης αλλά και 11 ακόμα. Στα αποτελέσματα, η Ελλάδα εμφανίζεται να είναι από τις πρώτες χώρες στην Ευρώπη όσον αφορά στην προστασία των δικαιωμάτων του πολίτη, με μόνο μελανό σημείο τις υποκλοπές των τηλεπικοινωνιών. Η Γερμανία λαμβάνει την πρώτη θέση στην αντίστοιχη λίστα, ενώ η Αγγλία έρχεται τελευταία στους περισσότερους τομείς. Το πλήρες περιεχόμενο της έκθεσης υπάρχει εδώ: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-545269

Windows Vista: Χρειάζονται antivirus ή όχι;
Σε μία τηλεφωνική συνέντευξη, ο Jim Allchin, co-president της Microsoft, δήλωσε σίγουρος ότι στα Windows Vista, τα οποία θα είναι διαθέσιμα στους κατασκευαστές μέχρι το τέλος του μήνα, δε θα υπάρχει ανάγκη για antivirus. Ειδικότερα, δήλωσε πως ο 7χρονος γιος του χρησιμοποιεί ήδη τα Windows Vista χωρίς κανένα πρόβλημα, αφού ειδικό λογισμικό για parental control δεν του επιτρέπει να κατεβάσει οτιδήποτε δεν προέρχεται από site που έχει αυτός εγκρίνει. Εκτός από τα parental controls που συνοδεύουν τα Vista, ο Allchin αναφέρθηκε και στο Address Space Layout Randomization (ASLR), το οποίο πρακτικά καθιστά κάθε εγκατάσταση των Vista διαφορετική. Έτσι, αν βρεθεί κάποιο exploit για μία συγκεκριμένη εγκατάσταση των Vista, αυτό δε θα μπορεί να χρησιμοποιηθεί με επιτυχία σε άλλες εγκαταστάσεις. Πρόκειται για τουλάχιστον δύο νέα χαρακτηριστικά των Vista που θα αποτρέπουν την εγκατάσταση και την εξάπλωση των ιών.
Είναι γεγονός πως οι δηλώσεις του Allchin εμπεριέχουν αρκετά στοιχεία εντυπωσιασμού αλλά και ο ίδιος ήταν αρκετά συγκρατημένος, αφού παραδέχθηκε πως οι hackers εξελίσσουν διαρκώς τις τεχνικές τους. Έτσι μπορεί να αφήνει για την ώρα το γιο του να χρησιμοποιεί τα Vista χωρίς antivirus (ούτως ή άλλως δεν υπάρχει ακόμα antivirus για τα Vista), εφόσον έχει φροντίσει ο ίδιος να ρυθμίσει κατάλληλα το λειτουργικό ώστε να είναι ασφαλές. Η Microsoft όντως φαίνεται να έχει φτιάξει το «ασφαλέστερο λειτουργικό της ως σήμερα» αλλά μήπως δεν ίσχυε το ίδιο και με τα XP; Το ASLR φαίνεται μία πολύ καλή προσθήκη, αλλά ας μην ξεχνάμε πως ακόμα δεν έχει ασχοληθεί κανείς hacker μαζί του. Κατά πάσα πιθανότητα τα Vista θα μπορούν να τρέξουν με ασφάλεια χωρίς antivirus, αλλά όπως και με τα XP σήμερα, κανείς δε θα σύστηνε κάτι τέτοιο σε έναν απλό χρήστη.

ΕΠΙΣΤΗΜΟΝΙΚΑ

Οι μπαταρίες μπορούν να ανιχνεύουν εισβολείς
Σε μία πρόσφατη εργασία που δημοσιεύτηκε στο περιοδικό Security and Privacy της IEEE, μελετάται η δυνατότητα εντοπισμού εισβολέων, ύστερα από παρατήρηση της ενέργειας που καταναλώνεται. Συγκεκριμένα, οι ερευνητές παρατήρησαν ότι συσκευές, όπως κινητά τηλέφωνα, PDAs, κλπ., ανάλογα με την κατάσταση στην οποία βρίσκονται (π.χ. κλειστά, αδρανή, σε ετοιμότητα, σε λειτουργία), καταναλώνουν συγκεκριμένη ενέργεια από τη μπαταρία τους και προσπάθησαν να μοντελοποιήσουν την κατανομή της ενέργειας ανάλογα με τις διάφορες καταστάσεις

των συσκευών. Στη συνέχεια, θεώρησαν ότι μεγάλη παρέκκλιση από το μοντέλο αυτό πιθανώς να οφείλεται στην ύπαρξη κάποιου εισβολέα (π.χ. ιού) ή γενικότερα σε κάποια επίθεση. Έτσι, για παράδειγμα, αν ένα κινητό εμφανίζει μεγάλη κατανάλωση ενώ είναι σε κατάσταση αναμονής, πιθανώς να έχει κολλήσει κάποιον ιό που απασχολεί τον επεξεργαστή της συσκευής ή να δέχεται κάποια επίθεση τύπου Denial of Service. Η συγκεκριμένη ερευνητική ομάδα κατασκεύασε και δοκίμασε κάποιες πρωτότυπες εφαρμογές ανίχνευσης εισβολέων που βασίζονται στη θεωρία αυτή. Τα αποτελέσματα της έρευνας κρίνονται ιδιαίτερα ενδιαφέροντα και ίσως αποτελέσουν τη βάση για τη δημιουργία κάποιου hardware μηχανισμού παρακολούθησης της κατανάλωσης.

Πηγή: Grant A. Jacoby, Randy Marchany, Nathaniel J. Davis IV, "Using Battery Constraints within Mobile Hosts to Improve Network Security," *IEEE Security and Privacy*, vol. 04, no. 5, pp. 40-49, Sept/Oct, 2006.

ΗΣΥΧΙΑ, ΤΑΞΗ ΚΑΙ… ΑΣΦΑΛΕΙΑ

- Μια του blogger, δυο του blogger, τρεις και τον τσακώσανε.
- Πήγε βέβαια μακριά η βαλίτσα αλλά το ποτήρι δεν ξεχείλισε διότι απαγορεύονται τα υγρά.
- Τα ψάρια όμως μπορούν και επιβιώνουν αφού αποφεύγουν τα… επικίνδυνα δολώματα. Μένει να δούμε τι άλλο θα σκαρφιστούν οι… πθαράδες.
- Να δούμε και πόσο θα… ψαρώνουν τα Vista.
- Τα οποία τελικά θα είναι κατάλληλα για όλους ή θα είναι απαραίτητη η γονική συναίνεση;