Θέματα διπλωματικών εργασιών 2012-2013 – Β. Κάτος

1. **Ανάλυση τεχνικών συσκευασίας (packing) σε εκτελεσιμο αρχειο**

Η χρήση συσκευαστών (packers) για την μεταφόρτωση ενός PE (Windows) και ELF (Linux) εκτελέσιμου αρχείου τείνει να γίνει κοινή πρακτική των προγραμματιστών. Ο σκοπός των συσκευαστών είναι η αποφυγή ανάλυσης (reverse engineering) του αρχείου καθώς και η μη ενεργοποίηση του antivirus software σε περίπτωση απομακρυσμένης (καθώς και τοπικής) επίθεσης σε υπολογιστικό σύστημα. Στη εργασία αυτή θα μελετηθούν και θα αναλυθούν τεχνικές συσκευασίας (packing) σε εκτελέσιμα αρχεία..

Επιτροπή: Κάτος, Β., Αθανασιάδης, Ν., Μητιανούδης, Ν.

2. **Εκγληματολογική ανάλυση μέσων κοινωνικής δικτύωσης σε smartphones**

Βάσει μιας πρόσφατης έρευνας, η πλειοψηφία των χρηστών των εφαρμογών κοινωνικής δικτύωσης χρησιμοποιεί κινητές συσκευές. Σκοπός της εργασίας αυτής είναι να δημιουργηθεί εφαρμογή η οποία θα επεξεργάζεται δεδομένα που είναι αποθηκευμένα σε smartphone και θα παράγει πληροφορίες σχετικά με τη δραστηριότητα του χρήστη, το καθεστώς κοινωνικής δικτύωσής του κλπ.

Επιτροπή: Κάτος, Β., Αραμπατζής, Α., Συρακούλης, Γ.

3. **Αυτοματοποιημένη εγκληματολογική διερεύνηση πτητικής μνήμης**

Στην εργασία αυτή θα αξιοποιηθούν και θα επεκταθούν οι δυνατότητες του volatility framework, το οποίο είναι το πιο δημοφιλές εργαλείο για την εγκληματολογική ανάλυση πτητικής μνήμης (RAM forensics). Τα σενάρια θα αφορούν κυρίως κακόβουλο λογισμικό.

Επιτροπή: Κάτος, Β., Τσαουσίδης Β., Σαρρής Θ.

4. **Σύστημα διαχείρισης περιστατικών ασφάλειας υπολογιστικού συστήματος**

Στην εργασία αυτή θα σχεδιασθεί και θα αναπτυχθεί πράκτορας (agent) για υπολογιστικό σύστημα ο οποίος θα μπορεί να δέχεται αιτήματα εξ' αποστάσεως και στη συνέχεια θα εκτελεί συλλογή δεδομένων που σχετίζονται με την κατάσταση του συστήματος αυτού. Ενδεικτικά εργαλεία τα οποία μπορούν να ενσωματωθούν είναι το triage-ir και το 3secure data collection script.

http://code.google.com/p/triage-ir/

Επιτροπή: Κάτος, Β., Καράκος Α., Πρατικάκης Γ.

5. Πηγή και γεννήτρια τυχαίων αριθμών για smartphones

Πολλές εφαρμογές ασφάλειας απαιτούν πρόσβαση σε τυχαία γεννήτρια προκειμένου να παράξουν τα σχετικά κρυπτογραφικά κλειδιά. Η αδυναμία παραγωγής τυχαίων αριθμών οδηγεί σε προβλήματα ασφάλειας καθώς πολλές επιθέσεις επικεντρώνονται στην πρόβλεψη των κλειδιών αυτών. Σκοπός της εργασίας είναι να μελετηθούν οι δυνατότητες παραγαγής τυχαίων αριθμών οι οποίοι θα πετυχαίνουν στους γνωστούς ελέγχους τυχαιότητας. Η σχετική εφαρμογή θα αναπτυχθεί σε smartphone επιλογής του φοιτητή.

Επιτροπή: Κάτος, Β., Εφραιμίδης., Χαμζάς Χ.

6. Ισχυρή πιστοποίηση ταυτότητας χρήστη μέσω smartphone-token

Τα smartphones τείνουν να γίνουν προσωπικό αξεσουάρ και σε γενικές γραμμές χαρακτηρίζουν μονοσήματα ένα φυσικό πρόσωπο. Στην εργασία αυτή θα σχεδιασθεί και θα υλοποιηθεί σύστημα πιστοποίησης ταυτότητας μέσω πρωτοκόλλου πρόκλησης-απάντησης (challenge-response) για εφαρμογές που απαιτούν ισχυρή πιστοποίηση στην εξουσιοδότηση συναλλαγών.

Επιτροπή: Κάτος, Β., Εφραιμίδης, Μάλλιαρης Γ.

7. Επέκταση του εργαλείου ανοικτού κώδικα Digital Forensics Framework

Το Digital Forensics Framework είναι ένα πλαίσιο επάνω στο οποίο ο φοιτητής μπορεί να αναπτύξει modules, επεκτείνοντας έτσι τις λειτουργίες του. Το πλαίσιο παρέχει API σε Python.

- http://www.digital-forensic.org/
- http://wiki.digital-forensic.org/index.php/Ideas_list

Επιτροπή: Κάτος, Β., Αθανασιάδης, Γ., Μητιανούδης, Ν.