Θέματα διπλωματικών εργασιών 2009-2010 – Β. Κάτος

1. **Εργαλεία κρυπτογραφίας για διδασκαλία σε πλατφόρμα e-learning**

   Το κομμάτι της σύγχρονης επικοινωνίας (chat) μιας e-learning εφαρμογής αποτελεί ιδανικό περιβάλλον για την ανάπτυξη και προσθήκη εργαλείων τα οποία μπορούν να υλοποιήσουν κρυπτογραφικά πρωτόκολλα και σενάρια προκειμένου οι συμμετέχοντες να αποκτήσουν γνώση και εξοικείωση στο μάθημα της κρυπτογραφίας.

   Πηγή:
   - Katos, V., King, T., Adams, C. ''Towards a Computer Based Training Tool for Education in Cryptography'', The Keys of Cryptography, UPGRADE Journal, vol V., issue 6, CEPIS, 2004, pp. 30-35

2. **Αναπαράσταση ιστορικής κατάστασης και λειτουργίας υπολογιστικού συστήματος**

   Κατά τη διερεύνηση (ηλεκτρονικού) εγκλήματος είναι πολλές φορές επιθυμητό να γίνεται αναπαράσταση του (ψηφιακού) τόπου του εγκλήματος, ώστε να μπορεί να αναδειχθεί τόσο ο υπαίτιος όσο και ο τρόπος με τον οποίο διαπράχθηκε το έγκλημα. Στην εργασία αυτή θα πρέπει να περιληφθεί μια μελέτη που θα αφορά στα χαρακτηριστικά εκείνα ενός συστήματος τα οποία θα μπορούν να συσχετισθούν και να προσδώσουν πληροφορίες ώστε να γίνει εφικτή μια αναπαράσταση της κατάστασης του υπολογιστή την περίοδο που διαπράττονταν το έγκλημα.

   Πηγές:
   - Kevin Cardwell, Jack Wiles, Anthony Reyes, The best damn cybercrime and digital forensics book period, Syngress, 2007
   - Farmer & Venema, Forensic Discovery, http://www.freetechbooks.com/forensic-discovery-t654.html
   - Digital Investigation, Elsevier, http://www.elsevier.com/locate/diin
   - http://sillydog.org/mshidden.php

3. **Εξατομικευμένο κακόβουλο λογισμικό**

   Στόχος της εργασίας αυτής είναι να αναπτυχθεί ένα πρωτότυπο (proof-of-concept) που να βοηθήσει στη μελέτη κακόβουλου λογισμικού που στοχεύει συγκεκριμένη επιχειρησιακή λογική (business logic). Το κακόβουλο λογισμικό θα είναι συνδυασμός τεχνικών σε πολλά επίπεδα επικοινωνίας και θα εξαπατά το χρήστη καταρρίπτοντας κυρίως την ακεραιότητα των δεδομένων.

   Πηγές:
   - M. Pemble, Evolutionary trends in bank customer-targeted malware, Network Security, No. 10, 2005, pp.4-7
   - M. Sunner, The rise of targeted trojans, Network Security, No. 12, 2007

4. **Εκγληματολογική ανάλυση συσκευών GPS (GPS forensics)**

   Οι φορητές συσκευές GPS εκτός από την αναμενόμενη εφαρμογή και λειτουργία της πληροφόρησης του οδηγού, μπορούν να θεωρηθούν και συσκευές-”μάρτυρες” καθώς συλλέγουν αυτόματα και σιωπηλά στοιχεία κίνησης του οδηγού. Στόχος της εργασίας αυτής είναι η ανάπτυξη μεθόδου και λογισμικού συλλογής και ανάλυσης πειστηρίων που σχετίζονται με την τοποθεσία και διαδρομή της συσκευής.

   Πηγές:
   – http://www.gpsforensics.org/

5. **Πιστοποίηση ταυτότητας με γραφικά συνθηματικά πρόσβασης**

   Οι φορητές υπολογιστικές συσκευές έχουν φυσικούς περιορισμούς και μειονεκτήματα όσο αφορά τη συσκευή εισόδου (π.χ. πληκτρολόγια). Αυτό καθιστά προβληματική μια λύση πρόσβασης που βασίζεται σε συνθηματικά πρόσβασης που αποτελούνται από αλφαριθμητικούς χαρακτήρες. Επίσης, η ενδεχόμενη υιοθέτηση μιας λύσης PIN αυξάνει το ρίσκο διότι ο χώρος των πιθανών PIN είναι σχετικά μικρός και συνεπώς ευάλωτος σε επιθέσεις εξαντλητικής αναζήτησης. Σκοπός της εργασίας είναι να μελετηθεί και να αναπτυχθεί μια λύση όπου ο κωδικός πρόσβασης θα βασίζεται σε περιοχές pixels μιας ή περισσοτέρων εικόνων. Μια τέτοια προσέγγιση αποσκοπεί στην ευκολία χρήσης χωρίς να θυσιάζεται η ασφάλεια.

   Πηγή:
   – http://research.microsoft.com/en-us/um/people/darkok/projectssyscli.htm

6. **Ασφαλής εκκινήσιμη συσκευή για εκτέλεση εργασιών ηλεκτρονικού εμπορίου**

   Στόχος της εργασίας αυτής είναι η μελέτη ασφάλειας λειτουργικών συστημάτων και η δημιουργία “ζωντανού” USB ώστε να μπορεί ο χρήστης να προηγηθεί στο Διαδίκτυο και να εκτελεί με ασφάλεια ηλεκτρονικές συναλλαγές ακόμη και από υπολογιστές τρίτων οι οποίοι δεν είναι έμπιστοι και έχουν ενδεχομένως προσβληθεί από κακόβουλο λογισμικό ή λογισμικό υποκλοπών (spyware).

   Πηγή:
   – http://en.wikipedia.org/wiki/Ubuntu_Live_USB_creator

7. **Εγκληματολογική ανάλυση πτητικής μνήμης**

Η εγκληματολογική ανάλυση πτητικής μνήμης είναι ένα αντικείμενο το οποίο εξελίσσεται ραγδαία τα τελευταία χρόνια. Σκοπός της εργασίας αυτής είναι η μελέτη εργαλείων και ανάπτυξη μεθόδου συλλογής δεδομένων που σχετίζονται με την κατάσταση και το περιεχόμενο της μνήμης ενός υπολογιστή, καθώς και την αποκωδικοποίηση και παρουσίαση των δεδομένων σε φιλική προς τον άνθρωπο μορφή. Επίσης θα πρέπει να εξετασθεί η περίπτωση συλλογής των δεδομένων μέσω της διεπαφής firewire, ώστε να παρακάμπτεται η ασφάλεια του λειτουργικού συστήματος του υπό εξέταση υπολογιστή.

Πηγή:

– Amari,Techniques and Tools for Recovering and Analyzing Data from Volatile Memory, SANS Reading Room, 2009, http://www.sans.org/reading_room/whitepapers/forensics/techniques_and_tools_for_recovering_and_analyzing_data_from_volatile_memory_33049