

### Security Paper Rresentation

Στα πλαίσια αυτής της άσκησης θα πρέπει να βρείτε, να διαβάσετε και να παρουσιάσετε μια **ερευνητική εργασία** (paper) που θα αφορά ένα θέμα ασφάλειας υπολογιστών της αρεσκείας σας. Θα πρέπει να ανατρέξετε σε κορυφαία συνέδρια και περιοδικά του χώρου. Δώστε περισσότερη προσοχή στα πρακτικά των τελευταίων χρόνων (2010 μέχρι σήμερα). Ενδεικτικά συνέδρια είναι τα εξής:

- USENIX Security Symposium,
- IEEE Symposium on Security and Privacy (Oakland),
- ACM Conference on Computer and Communications Security (CCS),
- The Network and Distributed System Security Symposium (NDSS).

Ενδεικτικά περιοδικά αποτελούν τα παρακάτω:

- IEEE Transactions on Dependable and Secure Computing,
- ACM Transactions on Privacy and Security,
- Computers & Security.

Δυο βασικές κατηγορίες εργασιών στον τομέα της ασφάλειας υπολογιστών είναι: (1) αυτές που παρουσιάζουν νέες επιθέσεις (**attack papers**), και (2) εργασίες που παρουσιάζουν καινοτόμους αμυντικούς μηχανισμούς (**defense papers**). Στόχος σας είναι να διαλέξετε ένα paper από μια από αυτές τις κατηγορίες. Στην παρουσίασή σας θα πρέπει να είναι ξεκάθαρο το πρόβλημα, το threat model, και η προσέγγιση που ακολουθούν οι ερευνητές για να πετύχουν αυτό που θέλουν. Επιπλέον, στην 1η περίπτωση θα πρέπει να αναφέρετε σε ποιά συστήματα ή εφαρμογές έκαναν τις προτεινόμενες επιθέσεις τους οι ερευνητές, ενώ στην 2η, πως αξιολόγησαν τον αμυντικό μηχανισμό που πρότειναν (overhead, false positives, false negatives). Τέλος θα πρέπει να αναφέρετε εάν ο κώδικας που ανέπτυξαν είναι δημόσια διαθέσιμος.

Η άσκηση είναι **προαιρετική** και ομαδική (2 έως 3 άτομα). Οι ομάδες που θα επιλέξουν να την κάνουν, θα πρέπει να στείλουν ένα email στο **csec.di@gmail.com** με θέμα **"Project 3: Study Group"** μέχρι την Πέμπτη 25/05/2017 και ώρα 23:59. Οι παρουσιάσεις δεν θα πρέπει να ξεπερνούν τα 20 λεπτά. Μετά από κάθε παρουσίαση θα υπάρχουν και 5 έως 10 λεπτά για ερωτήσεις και συζήτηση. Θα πρέπει να έχετε στείλει το pdf της παρουσίασής σας στο email του μαθήματος μέχρι την Πέμπτη 1η Ιουνίου και ώρα 16:00. Την Παρασκευή 2 Ιουνίου θα γίνουν οι παρουσιάσεις. Η Αίθουσα και η ώρα θα ανακοινωθεί.