



Computer Security

Εισαγωγή

Aggelos Kiayias



Security

- Αγαθά
- Χρήστες
- Αντίπαλος





Στόχοι

- **Μυστικότητα/Confidentiality:** Πρόσβαση στα αγαθά (viewing/printing/copying/listing) είναι περιορισμένη σε όσους έχουν το αντίστοιχο δικαίωμα.
- **Ακεραιότητα/Integrity:** Τα αγαθά αλλάζουν (modified/altereD/created/deleted etc.) μόνο με προκαθορισμένους τρόπους από όσους έχουν τα αντίστοιχα δικαιώματα.
- **Διαθεσιμότητα/Availability:** Τα αγαθά είναι διαθέσιμα σε όσους έχουν το δικαίωμα να τα προσπελάσουν.



Πως μπορούν να επιτευχθούν οι στόχοι;

- Κατανόηση του αντιπάλου
 - (what are the resources available?)
 - (what is the goal of the attack?)
- Κατανόηση του τρόπου της επίθεσης.
 - (in what ways can the attack be launched?)
 - (what are the vulnerabilities?)
- Κατανόηση “trade-offs” μεταξύ χρηστικότητας/διαθεσιμότητας και ασφάλειας
 - (A turned-off system is a secure system.)



Σκεφτείτε:

- Η ασφάλεια δεν μπορεί να είναι επιπρόσθετο χαρακτηριστικό



ΣΚΕΦΤΕΙΤΕ:

- Ένα σύστημα είναι τόσο ασφαλές όσο το πιο ασθενές του συστατικό.
 - Δεν υπάρχει τίποτε που μπορείτε να προσθέσετε στο σύστημα σας (firewalls, antivirus, encryption, biometrics, etc.) το οποίο μπορεί να το κάνει ασφαλές από μόνο του.
- Προσέξτε για “snake-oil” security products.
 - “Unbreakable ciphers”
 - “No key cryptosystems”
 - “Secret cipher”
 - “1-million bit length”



Σκεφτείτε:

- Το να σκέφτεστε σαν τον αντίπαλο είναι πρωταρχικής σημασία ικανότητα για να ασφαλίσετε ένα σύστημα.
- Πάντα αναρωτηθείτε
 - Ποιος είναι ο αντίπαλος;
 - Ποιές είναι οι πιθανές δρομολογήσεις των επιθέσεων;
 - Τι πρέπει να προστατευτεί και πόσο αξίζει;



ΣΚΕΦΤΕΙΤΕ:

- “Security holes” και “vulnerabilities” βρίσκονται συνέχεια.
- Η αρχή της απόλυτης διαφάνειας:
 - Δημοσιοποίηση των επιθέσεων αφού ενημερωθεί ο υπεύθυνος του αδύναμου συστήματος ώστε να δημιουργήσει πλάνο αντιμετώπισης
 - Η δημοσιοποίηση οδηγεί σε θετικές εξελίξεις.
 - Η μη δημοσιοποίηση είναι “ωρολογιακή βόμβα.”
- Η ασφάλεια δεν μπορεί να επιτευχθεί με κρυφά επιμέρους συστατικά.



Αυτό το Μάθημα:

- Μελετά πως μπορούμε να ασφαλίσουμε
 - Λογισμικό
 - Δίκτυα
 - Λειτουργικά
 - Βάσεις
- Δίνει μια εισαγωγή σε διάφορα εργαλεία για το χτίσιμο ασφαλών συστημάτων: ciphers, hash functions, signatures...
- Κρίνει την ασφάλεια σε συνδυασμό με πλευρές που έχουν να κάνουν με νομικές, ηθικές και επιχειρηματικές οπτικές.



Software

- Programming & Security.
 - Vulnerabilities in Software
 - and how they can be exploited.
- Software with malicious/questionable intent
 - Viruses, Worms, Trojan Horses, etc.
 - Spyware
 - Web bugs.
 - Cryptoviruses
 - How to protect against the above, write better code, test whether they are present etc.



Βαθμολογία

- 4 projects : 50%
- Τελική Εξέταση 50%
- [Πάνω από τη βάση και στα δύο μέρη]



Συμπεριφορά φοιτητών

- Στην τάξη θα συζητηθούν ευαίσθητα θέματα ασφάλειας και προχωρημένες τεχνικές επιθέσεων.
- Αν ένας φοιτητής βρεθεί να εφαρμοζει υλικό της τάξης με το σκοπό να κάνει κάποια επίθεση (πέρα από αυτές που θα ζητηθούν ως ασκήσεις :-) **θα πάρει τον αυτόματο βαθμό “τρία” στην τελική κατάσταση.**



Σελίδα του μαθήματος

<https://crypto.di.uoa.gr/csec>

- Τι θα βρείτε εκεί
 - σημειώσεις.
 - ανακοινώσεις.



Bulletin Board της τάξης

<http://comspec.di.uoa.gr>