Computer Security

Εισαγωγή

Dimitris Mitropoulos
dimitro@grnet.gr

Security

- **Εμπιστευτικότητα** (Confidentiality): αφορά την πρόσβαση σε αγαθά (λ.χ. προβολή, αντιγραφή) και το γεγονός του ότι θα πρέπει να είναι περιορισμένη σε όσους έχουν το αντίστοιχο δικαίωμα.

- **Ακεραιότητα** (Integrity): σχετίζεται με το ότι τα αγαθά αλλάζουν (τροποποιούνται, σβήνονται) μόνο με προκαθορισμένους τρόπους από όσους έχουν τα αντίστοιχα δικαιώματα.

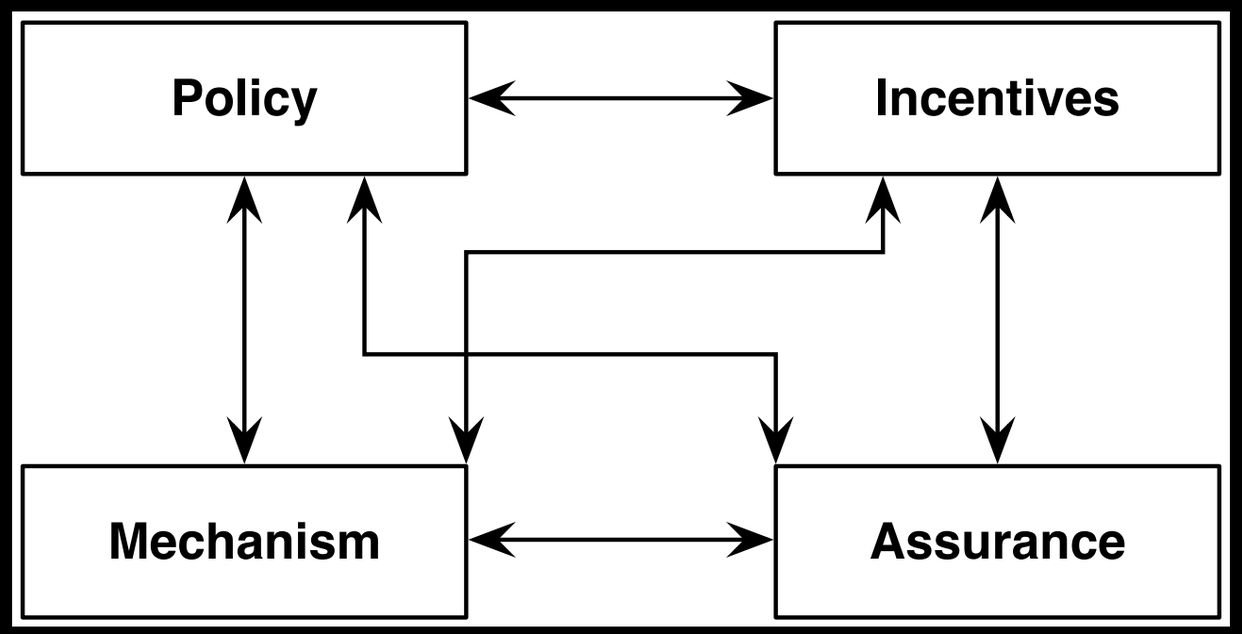
- **Διαθεσιμότητα** (Availability): έχει να κάνει με το ότι τα αγαθά είναι διαθέσιμα σε όσους έχουν το δικαίωμα να τα προσπελάσουν.

Privacy

Ιδιωτικότητα: η ικανότητα ή / και το δικαίωμα να μπορεί κανείς να προστατεύει τα προσωπικά του δεδομένα.

Security Engineering

Analysis Framework



Computer Security Engineering

- Κατανόηση του αντιπάλου.
- Κατανόηση του τρόπου επίθεσης.
- Αντίμετρα.
- Συμβιβασμοί (trade-offs).

Vulnerabilities

- Δημοσιοποίησή τους αφού πρώτα ενημερωθεί ο υπεύθυνος ώστε να δημιουργήσει πλάνο αντιμετώπισης (αρχή απόλυτης διαφάνειας).
- Η δημοσιοποίηση οδηγεί σε θετικές εξελίξεις.
- Η μη δημοσιοποίηση είναι “ωρολογιακή βόμβα”.

Σκεφθείτε:

- Η ασφάλεια δεν μπορεί και δεν πρέπει να είναι επιπρόσθετο χαρακτηριστικό.
- Ένα σύστημα είναι τόσο ασφαλές όσο το πιο ασθενές του συστατικό.

Προσέξτε:

Τα snake-oil security products (unbreakable ciphers, technobabble, secret systems).

Σε αυτό το μάθημα:

- Θα μελετήσουμε πως μπορούμε να αναπτύσσουμε ασφαλή συστήματα και εφαρμογές.
- Θα παρουσιάσουμε συνηθισμένες αδυναμίες και επιθέσεις.
- Θα αναλύσουμε διάφορες μεθόδους ανίχνευσης ευπαθειών και μηχανισμούς προστασίας.
- Θα συζητήσουμε για μερικά βασικά κρυπτογραφικά πρωτόκολλα που χρησιμοποιούν οι εφαρμογές στο διαδίκτυο για να πραγματοποιούν ασφαλείς συναλλαγές.

Βαθμολογία

- Ασκήσεις (3 ή 4): 40% - 50%
- Εξέταση: 50% - 60%
- [Πάνω από τη βάση και στα δυο]

Συμπεριφορά

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

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

Βιβλιογραφία

R. J. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. *John Wiley & Sons, Inc.*, New York, NY, USA, 2001. ISBN 0471389226.

Kevin D. Mitnick, William L. Simon. The Art of Deception: Controlling the Human Element of Security. *John Wiley & Sons, Inc.*, New York, NY, USA, 2011. ISBN 076453839X.

Jerry Kang. Cyberspace privacy: A primer and proposal. *Human Rights Magazine*, 26(1), Winter 1999.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016. http://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016L0680&from=EN.