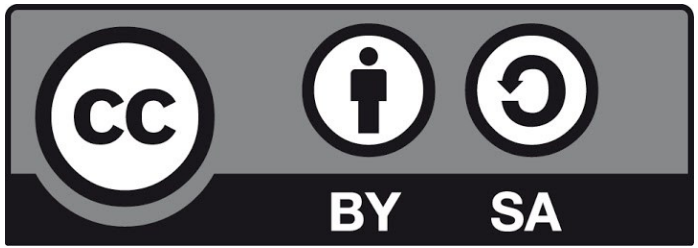
# Εισαγωγή στην Ασφάλεια Δικτύων

Εισηγητής: Χρήστος Δαλαμάγκας
cdalamagkas@gmail.com

# Άδεια χρήσης





# Ύλη μαθήματος

- Κρυπτογράφηση
  - Ασσύμμετρη κρυπτογράφηση με τον RSA και παραδείγματα
  - Πιστοποιητικά και ψηφιακές υπογραφές
  - Υποδομή Δημοσίου Κλειδιού (PKI)
- Τείχη ασφαλείας (αρχιτεκτονικές και παραδείγματα με ACLs
- Εισαγωγή στο TLS και εφαρμογές
  - Χειραψία TLS, εκδόσεις 1.2 και 1.3
  - Εφαρμογές του TLS και παραμετροποίηση (Nginx, DNS over TLS)
- Ανάλυση Απειλών και Ευπαθειών (nmap)
- Είδη κακόβουλου λογισμικού και κατηγοριοποίηση
- Μέθοδοι και πρωτόκολλα αυθεντικοποίησης
- Εισαγωγή στα VPN (IPSec/L2TP, OpenVPN)
- Συστήματα Εντοπισμού Παρείσδυσης (Snort) + Honeypots

# Στόχοι της ασφάλειας

- Να προστατέψουμε τους υπολογιστικούς πόρους έναντι μη εξουσιοδοτημένης/κακόβουλης χρήσης
- Να προστατεύσουμε τα δεδομένα που μεταδίδονται:
  - Ακεραιότητα
  - Εμπιστευτικότητα

# Γιατί ασφάλεια;

- Όλο και μεγαλύτερη η ανάγκη για ασφάλεια
- Ανάπτυξη Διαδικτύου και νέων εφαρμογών
- IoT
- Αυτοματοποίηση λειτουργιών
- Είσοδος του ICT στη βιομηχανία
- Συνεχώς αυξάνεται η διαθέσιμη επεξεργαστική ισχύς
- «Άναρχο» Διαδίκτυο

# Παράδειγμα της Ουκρανίας

- Επίθεση στο smart grid της Ουκρανίας
- Προετοιμασία: spear-phishing emails with BlackEnergy malware;
- Με τη χρήση του malware, εισήλθαν στο δίκτυο του παρόχου ηλ. Ενέργειας
- Μήνες επιθέσεων ανίχνευσης οδήγησαν στην υποκλοπή κωδικών πρόσβασης VPN για πρόσβαση στο δίκτυο ελέγχου
- Μήνες ανίχνευσης του εσωτερικού δικτύου και προετοιμασίας
- Συντονισμένη επίθεση που πήρε τον έλεγχο του συστήματος ελέγχου και κατέστρεψε UPS, αντάπτορες, μηχανήματα αυτοματισμού, υπολογιστές, αρχεία και firmware.
- Ταυτόχρονα, DoS στο call-center για να μην ενημερώσουν οι πελάτες για τη διακοπή ρεύματος.
- Αποτέλεσμα: ~60 υποσταθμοί offline, 230.000+ κάτοικοι χωρίς ρεύμα για 6 ώρες

Πηγή: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

# Τύποι επιθέσεων

- Μη εξουσιοδοτημένη πρόσβαση (masquerade)
- Παθητική παρακολούθηση (passive tapping)
- Ενεργός παρακολούθηση (active tapping)
- Άρνηση εξυπηρέτησης (Denial of Service – DoS)
- Επανεκπομπή μηνυμάτων (replay)
- Αποποίηση (repudation)

# Προβλήματα ασφάλειας

- Μυστικότητα (secrecy) ή Εμπιστευτικότητα
  - Τα δεδομένα που μεταδίδονται υποκλέπτονται από κάποιον τρίτο; Οι επικοινωνίες μας είναι ιδιωτικές;
- Ακεραιότητα (integrity)
  - Τα δεδομένα που στέλνουμε φτάνουν ακέραια στον παραλήπτη; (χωρίς τροποποίηση από κάποιον τρίτο)
- Πιστοποίηση αυθεντικότητας (authentication)
  - Αυτός με τον οποίον επικοινωνούμε, είναι όντως αυτός που υποστηρίζει ότι είναι;

# Η ασφάλεια στα εννοιολογικά στρώματα

- **Φυσικό επίπεδο**: Κρυπτογράφηση, σωστή τοπολογία, ειδικές τεχνικές (scrambling, FHSS – εξάπλωση φάσματος)
- **Επίπεδο ζεύξης δεδομένων**: Κρυπτογράφηση, υλοποίηση VLAN
- **Επίπεδο δικτύου**: Κρυπτογράφηση, HMAC, τείχη ασφαλείας
- **Επίπεδο μεταφοράς**: Κρυπτογράφηση (TLS), τείχη ασφαλείας
- **Επίπεδο εφαρμογών**: Κρυπτογράφηση, AAA, πληρεξούσιοι

**AAA**: Authentication, Authorization, Accounting

# Κρυπτογραφία

- Ορισμός: Μετατροπή πληροφοριών σε μη αναγνώσιμη μορφή με σκοπό την προστασία τους.
- **Απλό κείμενο** (plaintext): Η αρχική πληροφορία
- **Κρυπτογράφημα** (cipher): Το αποτέλεσμα της μετατροπής του απλού κειμένου στην μη αναγνώσιμη μορφή
- **Αλγόριθμος κρυπτογράφησης**: Συνάρτηση υπολογισμού του κρυπτογραφήματος
- Αλγόριθμος αποκρυπτογράφησης: Συνάρτηση ανάκτησης του απλού κειμένου
- **Κλειδί**: Αριθμός/είσοδος στις συναρτήσεις κρυπτογράφησης και αποκρυπτογράφησης
- **Κρυπτανάλυση**: Παραβίαση του κρυπτογραφήματος χωρίς το κλειδί αποκρυπτογράφησης

# Παράδειγμα: Το κρυπτογράφημα του Καίσαρα

- ABC -> DEF
  - Αρχικό μήνυμα;
  - Κρυπτογράφημα;
  - Κλειδί;
  - Αλγόριθμος κρυπτογράφησης;
  - Παράδειγμα κρυπτανάλυσης;

# Στοιχεία διαδικασίας κρυπτογράφησης

- Αλγόριθμος κρυπτογράφησης
- Αλγόριθμος αποκρυπτογράφησης
- Κλειδι (ένα ή περισσότερα)
- Μήκος κλειδιού
- Απλό κείμενο
- Κρυπτογραφημένο κείμενο

# Είδη κρυπτογράφησης

- Συμμετρική
  - Χρησιμοποιείται το ίδιο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση
  - Αποστολέας και παραλήπτης πρέπει να προσυμφωνήσουν για το κλειδί
  - Χρήση: Κρυπτογράφηση
  - **Παραδείγματα**: AES, 3DES
- Ασύμμετρη
  - Υπάρχει ένα δημόσιο κλειδί και ένα ιδιωτικό
  - Το ένα χρησιμοποιείται για κρυπτογράφηση και το άλλο για αποκρυπτογράφηση
  - Χρήσεις: Κρυπτογράφηση, Ψηφιακή υπογραφή, Ψηφιακό πιστοποιητικό, ταυτοποίηση
  - **Παραδείγματα**: RSA, ElGamal

# Εφαρμογές κρυπτογράφησης

- Παροχή μυστικότητας, ακεραιότητας και αυθεντικότητας σε μια επικοινωνία
- Ασφαλής πλοήγηση στο Διαδίκτυο
- Ηλεκτρονική Οικονομία
- Προστασία προσωπικών αρχείων/κωδικών
- Ασφαλής πρόσβαση σε υπηρεσίες/δίκτυα
- ...