Ιόνιο Πανεπιστήμιο – Τμήμα Πληροφορικής
Εισαγωγή στην Επιστήμη των Υπολογιστών
2017-18

Ασφάλεια Δεδομένων

http://mixstef.github.io/courses/csintro/

Μ.Στεφανιδάκης

Οι απειλές

Εισαγωγή

Ένας κακόβουλος χρήστης
- Καταγράφει μηνύματα που ανταλλάσσονται σε ένα "κανάλι" επικοινωνίας και εισάγει νέα μηνύματα
- Τροποποιεί ξένα δεδομένα

Και μπορεί
- Να υποκλέψει κωδικούς πρόσβασης και δεδομένα
- Να προσποιηθεί ότι είναι κάποιος άλλος
- Να θέσει υπό έλεγχο επικοινωνία μεταξύ τρίτων
- Να αποκλείσει τρίτους από τις υπηρεσίες Διαδικτύου
- κλπ...

Αρχές ασφάλειας δεδομένων

Εισαγωγή

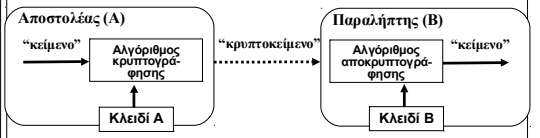
Απόρρητο (privacy)
- Μέσω κρυπτογράφησης

Πιστοποίηση αυθεντικότητας
- Ταυτότητα χρήστη
  - authentication
- Δικαιώματα χρήσης δεδομένων
  - authorization

Ακεραιότητα δεδομένων (integrity)
- Και μη απάρνηση από αποστολέα
  - non-repudiation

Απόρρητο επικοινωνίας

Εισαγωγή
Μυστικό κλειδί



Εξασφάλιση απορρήτου μέσω κρυπτογράφησης

Αποστολέας-παραλήπτης
- Άτομα αλλά και υπολογιστές (π.χ. servers)

Αλγόριθμος κρυπτογράφησης
- Παλαιότερα: κρυφός
- Σήμερα: ευρέως γνωστός (πρότυπο!) – συνεπώς, απαιτείται η χρήση κλειδιών

Κρυπτογράφηση με μυστικό (συμμετρικό) κλειδί

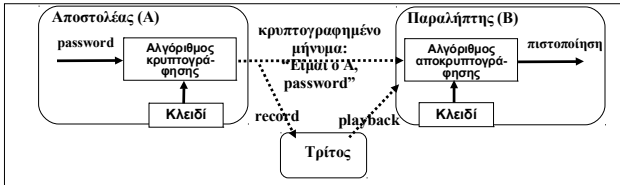
Εισαγωγή
Μυστικό κλειδί

Ίδιο κλειδί αποστολέα (Α) – παραλήπτη (Β)
- Κλειδί Α = Κλειδί Β
- Το κλειδί πρέπει να είναι μυστικό!
- Και μόνο μεταξύ των Α και Β
- Συμμετρικοί αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης

Data Encryption Standard (DES)
- 56-bit κλειδί
- Επαναληπτικά βήματα αντιμετάθεσης bits και πράξεων XOR
- Σήμερα: 3DES, AES (128, 192 ή 256-bit κλειδιά)

Το πρόβλημα
- Η επιλογή και ανταλλαγή του μυστικού κλειδιού μεταξύ Α, Β
- Με ποιον τρόπο θα υπάρξει ασφαλής επικοινωνία;

Πιστοποίηση ταυτότητας με μυστικό κλειδί

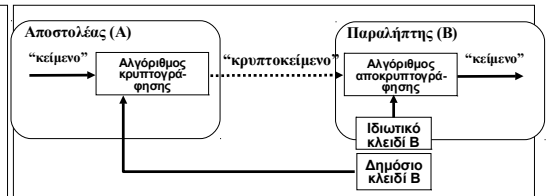


Απόδειξη της ταυτότητας του "συνομιλητή"
- Μέσω κάποιου πρωτοκόλλου πιστοποίησης
- Π.χ. με αποστολή μέσω δικτύου ενός password

Η χρήση του μυστικού κλειδιού
- Κωδικοποίηση password
- Ο κάτοχος του κλειδιού είναι αυτός που ισχυρίζεται
- Με μεγάλη βεβαιότητα
  - Όχι απόλυτη όμως!

Κρυπτογράφηση με δημόσιο κλειδί

Εισαγωγή
Μυστικό κλειδί
Δημόσιο κλειδί



Ζεύγη κλειδιών παραλήπτη (Β)
- Δημόσιο κλειδί: για κρυπτογράφηση (αποστολέας Α)
  - Διαθέσιμο σε όλους
- Ιδιωτικό κλειδί: για αποκρυπτογράφηση (παραλήπτης Β)
  - Γνωστό μόνο στον κάτοχό του (Β)

Ό,τι κρυπτογραφείται με το ένα κλειδί, αποκρυπτογραφείται με το άλλο
- Και αντίστροφα

Κρυπτογράφηση με δημόσιο κλειδί

Εισαγωγή
Μυστικό κλειδί
Δημόσιο κλειδί

Αλγόριθμος Rivest-Shamir-Adleman (RSA)
- Δημιουργία κλειδιών
  - Επιλογή μεγάλων πρώτων αριθμών p,q (n = pq ≥768 bits)
  - Υπολογισμός αριθμών e,d από pq, (p-1)(q-1)
  - Δημόσιο κλειδί: (n,e)
  - Ιδιωτικό κλειδί: (n,d)

Δεν υπάρχει γνωστός γρήγορος αλγόριθμος για εύρεση p,q από n
- Εδώ στηρίζεται η ασφάλεια του RSA

Κρυπτογράφηση
- Έστω "κείμενο" m
- "κρυπτοκείμενο" $c = m^e \bmod n$ (κρυπτογράφηση)
- "κείμενο" $m = c^d \bmod n$ (αποκρυπτογράφηση)
  - Η διαδικασία επιτυγχάνεται και με αντιστροφή κλειδιών!

Κρυπτογράφηση με δημόσιο κλειδί

Χρονοβόρα διαδικασία κρυπτογράφησης – αποκρυπτογράφησης με δημόσιο κλειδί

- Με μυστικό (συμμετρικό) κλειδί: τουλάχιστον 100 φορές γρηγορότερα!

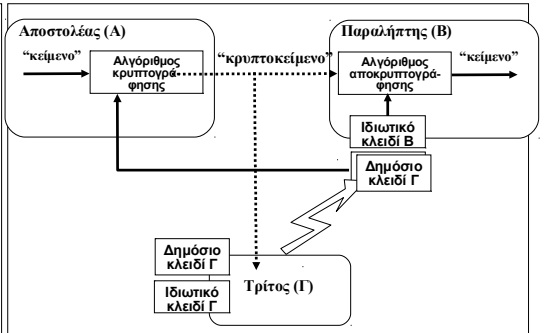
Συνήθως

- Πρώτα ανταλλαγή μυστικού κλειδιού με RSA
- Στη συνέχεια επικοινωνία με (από)κρυπτογράφηση με το μυστικό κλειδί

Ποιος εγγυάται τη διανομή του δημόσιου κλειδιού;

- Σε αντίθεση με το μυστικό κλειδί: εδώ ο καθένας μπορεί να ισχυριστεί ότι είναι ο οποιοσδήποτε!
- Και να στείλει το δημόσιο κλειδί του αντί του σωστού... !

Πιστοποίηση δημόσιου κλειδιού;



Ψηφιακή υπογραφή

Κρυπτογραφική τεχνική για εξασφάλιση:

Ακεραιότητας

- Αποφυγή αλλοίωσης δεδομένων

Αυθεντικότητας

- Ποιος είναι ο δημιουργός-αποστολέας;

Μη απάρνησης

- Από την πλευρά του αποστολέα

Προσοχή: η ψηφιακή υπογραφή δεν εξασφαλίζει το απόρρητο!

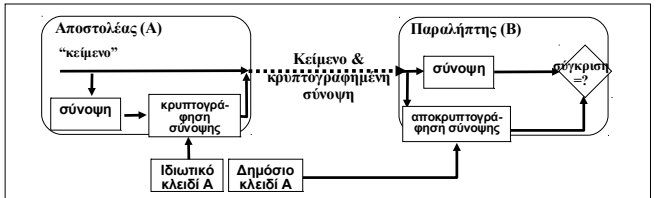
Τεχνική ψηφιακής υπογραφής

Χρήση μεθόδου κρυπτογράφησης δημόσιου κλειδιού

Αντίστροφα με διαδικασία τήρησης απορρήτου:

- Ο αποστολέας κρυπτογραφεί το κείμενο με το ιδιωτικό του κλειδί
- Παραγωγή ψηφιακής υπογραφής, αποστολή μαζί με το αρχικό κείμενο
- Ο παραλήπτης αποκρυπτογραφεί την ψηφιακή υπογραφή με το δημόσιο κλειδί του αποστολέα
- Μόνο με το κλειδί αυτό λαμβάνεται το αρχικό κείμενο
  - Και πιστοποιείται ο αποστολέας

Συνόψεις (digests)



Για την αποφυγή κρυπτογράφησης όλων των δεδομένων

- Δημιουργία σύνοψης
- Αλγόριθμοι κατακερματισμού
  - (Σχεδόν) αδύνατο διαφορετικό μήνυμα να δώσει την ίδια σύνοψη
  - MD5 (128-bit), SHA (160-bit και πλέον)
- Κρυπτογράφηση της σύνοψης μόνο με ιδιωτικό κλειδί αποστολέα

Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI)

Εισαγωγή
Μυστικό κλειδί
Δημόσιο κλειδί
Ψηφιακή υπογραφή
Πιστοποίηση δημόσιων κλειδιών

Έμπιστοι ενδιάμεσοι: αρχές πιστοποίησης

- Certification Authorities (CAs)

Πιστοποίηση ταυτότητας ενός "συνομιλητή"

- Πιστοποίηση εταιριών ηλεκτρονικού εμπορίου
- Σύνδεση ενός δημόσιου κλειδιού με μια "οντότητα"
  - π.χ. διεύθυνση IP, εταιρία...
- Η αξιοπιστία της πιστοποίησης εξαρτάται από την αξιοπιστία της CA!

Υποδομή Δημόσιου Κλειδιού

- Αλυσίδα CAs
  - Root CA

Πιστοποιητικά (Certificates)

Εισαγωγή
Μυστικό κλειδί
Δημόσιο κλειδί
Ψηφιακή υπογραφή
Πιστοποίηση δημόσιων κλειδιών

Πιστοποιητικά (certificates)

- Περιέχουν πληροφορία για έναν χρήστη
- Και το δημόσιο κλειδί του
  - για τα οποία εγγυάται κάποια CA
  - υπογράφοντας ψηφιακά το πιστοποιητικό με το ιδιωτικό κλειδί της

Η CA: XYZ
βεβαιώνει ότι ο: Α
έχει δημόσιο κλειδί: ΔΚ(Α)
<*ψηφιακή υπογραφή από ΙΚ(CA)*>

Αλυσίδα CA

Εισαγωγή
Μυστικό κλειδί
Δημόσιο κλειδί
Ψηφιακή υπογραφή
Πιστοποίηση δημόσιων κλειδιών

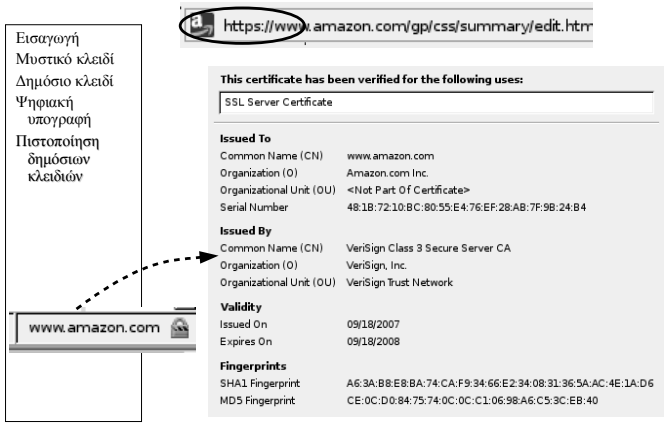
Η CA1: XYZ
βεβαιώνει ότι ο: XYZ
έχει δημόσιο κλειδί: ΔΚ(CA1)
<*ψηφιακή υπογραφή από ΙΚ(CA1)*>

root CA

Η CA1: XYZ
βεβαιώνει ότι ο: MNO
έχει δημόσιο κλειδί: ΔΚ(CA2)
<*ψηφιακή υπογραφή από ΙΚ(CA1)*>

Η CA2: MNO
βεβαιώνει ότι ο: Α
έχει δημόσιο κλειδί: ΔΚ(Α)
<*ψηφιακή υπογραφή από ΙΚ(CA2)*>

Παράδειγμα χρήσης Certificates



- Εισαγωγή
- Μυστικό κλειδί
- Δημόσιο κλειδί
- Ψηφιακή υπογραφή
- Πιστοποίηση δημόσιων κλειδιών