Λειτουργικά Συστήματα (HY321)

Διάλεξη 19:
Ασφάλεια

Χρήστος Δ. Αντωνόπουλος
25/5/2017

Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών, Πανεπιστήμιο Θεσσαλίας

Κρυπτογράφηση

- Βασική ιδέα: Αποθήκευσε και μετάδωσε την πληροφορία σε κρυπτογραφημένη μορφή που «δε βγάζει νόημα»
- Ο βασικός μηχανισμός:
  - Ξεκίνησε από το μήνυμα που πρέπει να προστατευθεί. Το αρχικό, αναγνώσιμο μήνυμα λέγεται clear text.
  - Κρυπτογράφησε το clear text ώστε να μη βγάζει κανένα απολύτως νόημα. Το ακαταλαβίστικο μήνυμα λέγεται cipher text. Η κρυπτογράφηση ελέγχεται από μυστικό password ή αριθμό
    - Αυτό λέγεται κλειδί κρυπτογράφησης (*encryption key*).
  - Το κρυπτογραφημένο μήνυμα μπορεί να αποθηκευτεί σε αναγνώσιμο αρχείο, ή να μεταδοθεί πάνω από μη ασφαλές κανάλι.
  - Για να γίνει κατανοητό το μήνυμα του cipher text, πρέπει να αποκωδικοποιηθεί. Αυτό γίνεται με αλγόριθμο που χρησιμοποιεί ένα άλλο μυστικό password ή αριθμό, το κλειδί αποκρυπτογράφησης (decryption key).

Απαιτήσεις

- Η συνάρτηση κρυπτογράφησης δε θα πρέπει να είναι εύκολα αντιστρέψιμη
  - Δε μπορείς να βρεις το αρχικό μήνυμα αν δεν ξέρεις το κλειδί αποκρυπτογράφησης.
- Η κρυπτογράφηση και η αποκρυπτογράφηση θα πρέπει να γίνονται σε ασφαλές σύστημα, ώστε το ακρυπτογράφητο μήνυμα να μη μπορεί να κλαπεί
- Τα 2 κλειδιά πρέπει να προστατεύονται.
  - Στα περισσότερα συστήματα μπορείς να υπολογίσεις το ένα κλειδί από το άλλο (ή συχνά είναι και το ίδιο κλειδί),άρα δεν επιτρέπεται να διαρρεύσει κάποιο…

Ασφαλής επικοινωνία

- Πρόβλημα: Πώς εγκαθιστώ ένα ασφαλές κανάλι;
  - Δηλαδή, πώς μοιράζω τα κλειδιά;
- Κρυπτογράφηση δημόσιου κλειδιού:
  - Η γνώση του κλειδιού κρυπτογράφησης δε βοηθάει στην εύρεση του κλειδιού αποκρυπτογράφησης (και το αντίστροφο).
  - Ο χρήστης δίνει ένα password, και το σύστημα το χρησιμοποιεί για να παράγει τα 2 κλειδιά
    - Με μη αντιστρέψιμη συνάρτηση, ώστε να μη βρίσκεται το password από οποιοδήποτε από τα κλειδιά.
  - Το ένα κλειδί παράγει το «αντίστροφο» αποτέλεσμα από το άλλο
    - Μπορείς π.χ. να κρυπτογραφήσεις με το κλειδί αποκρυπτογράφησης και μετά να αποκρυπτογραφήσεις με το κλειδί κρυπτογράφησης.
  - Κάθε χρήστης κρατά το ένα κλειδί μυστικό και δημοσιοποιεί (σε όλο τον κόσμο) το άλλο

Ασφαλές Mail - Ιδιωτικότητα

- Χρησιμοποίησε το δημόσιο κλειδί του παραλήπτη για να κρυπτογραφήσεις το mail.
  - Οποιοσδήποτε μπορεί να το κάνει αυτό, και θα είναι σίγουρος ότι μόνο ο συγκεκριμένος χρήστης μπορεί να το διαβάσει.
  - Ο αποστολέας χρειάζεται μόνο το δημόσιο κλειδί του παραλήπτη.
  - Πώς ξέρει ο παραλήπτης από ποιον στάλθηκε το mail;

Ψηφιακή υπογραφή

- Μπορείς να χρησιμοποιήσεις τα κλειδιά για ταυτοποίηση:
  - Χρησιμοποίησε το κρυφό κλειδί σου για να κρυπτογραφήσεις ένα μήνυμα π.χ. “Συμφωνώ να πληρώνω ισοβίως στους φοιτητές μου 100€ / χρόνο.”
  - Μπορείς να στείλεις το μήνυμα σε όλο τον κόσμο, και αυτοί μπορούν να επιβεβαιώσουν ότι ήρθε από εσένα, αν αποκωδικοποιείται με το δημόσιο κλειδί σου και βγάζει κάτι με νόημα (ψηφιακή υπογραφή).
- Αυτές οι 2 μορφές κρυπτογραφίας μπορούν να συνδυαστούν.
  - Π.χ. για να υπογράψεις ένα ασφαλές mail, κρυπτογράφησε πρώτα με το ιδιωτικό σου κλειδί και μετά με το δημόσιο κλειδί του παραλήπτη.

Περιορισμοί Κρυπτογράφησης

- Η κρυπτογράφηση νικάει τους ωτακουστές και βοηθάει την πιστοποίηση.
  - Αλλά όχι στην περίπτωση των δούρειων ίππων.
- Μεγάλο πρόβλημα: Πώς μπορούμε να ξέρουμε αν ένας μηχανισμός κρυπτογράφησης είναι ασφαλής;
  - Πολύ δύσκολο να αποδειχθεί.
  - Σημαντικό θέμα έρευνας: Οι θεωρητικοί ψάχνουν να βρουν προβλήματα που μπορούν να αποδείξουν ότι είναι δύσκολα.
    - Και μετά τα αξιοποιούν για να αποδείξουν / βελτιώσουν την ασφάλεια της κρυπτογράφησης.
- Πόσο ασφαλής είναι η κρυπτογράφηση;
  - Γιατί έχουμε φτάσει σε κλειδιά 128bits;

Βελτίωση της Ασφάλειας Κρυπτογράφησης

- Αφαίρεσε «συνήθεις ακολουθίες» από το αρχικό μήνυμα
  - Π.χ.: «Αξιότιμοι κύριοι» ή το όνομά σου.
  - Συμπίεσε πριν την κρυπτογράφηση.
- Μη στέλνεις μεγάλα ποσά πληροφορίας με το ίδιο κλειδί.
  - Άλλαζε συχνά κλειδιά.
  - Π.χ.: ενώ στέλνεις ένα αρχείο 100 MB.
- Η κρυπτογράφηση χρειάζεται να βελτιώνεται όσο οι υπολογιστές γίνονται πιο ισχυροί.
  - Distributed.net + EFF = 22 ώρες για να σπάσουν το DES, Ιανουάριος 1999.

Κρυπτογραφικά Ασφαλή Αθροίσματα Ελέγχου (checksums)

- Πρόβλημα: Μου στέλνουν ένα εκτελέσιμο. Πώς ξέρω αν κάποιος το άλλαξε στη διαδρομή;
  - Χρειάζομαι έναν έλεγχο με άθροισμα ελέγχου (checksum).
- Κρυπτογραφικά ασφαλές άθροισμα ελέγχου (checksum).
  - f(αρχείο) = Μεγάλος ακέραιος.
  - Λέγεται και Message Digests ή ψηφιακό αποτύπωμα.
  - Π.χ.: MD5/SHA1
- Αν οι κατασκευαστές έφτιαχναν PC που τρέχουν μόνο προγράμματα με προκαθορισμένα message digests?
  - Χρησιμοποίησε τα message digests για να χτίσεις περιβάλλον εμπιστοσύνης.
  - Κάνει τους δούρειους ίππους πιο απίθανους.
  - “Trusted” computing.

Ζητήματα σχετικά με τους Μηχανισμούς Προστασίας

- Κράτα το μηχανισμό μυστικό
  - Δυσκολότερο να εισβάλεις.
  - Δυσκολότερο να αλλάξεις τον μηχανισμό αν το μυστικό πάψει να είναι μυστικό...
- Δημοσίευσε το μηχανισμό.
  - Ενθάρρυνε τη μάχη καλού – κακού.
  - Η φιλοσοφία του Unix και (ακόμα περισσότερο) του Linux και του λογισμικού ανοιχτού κώδικα (OSS).
- Μηχανές ηλεκτρονικής ψηφοφορίας Diebold
  - Μυστικό σύστημα.
  - Ο κώδικας εμφανίστηκε στο web.
  - Η ασφάλεια ήταν (και είναι) ανέκδοτο.

Κρυπτογραφία Σήμερα

- Τάση: Χρήση τεχνολογίας κρυπτογράφησης για:
  - Επικοινωνία:
    - Εγκατάσταση ασφαλούς επικοινωνίας πάνω στο δίκτυο.
  - Ταυτοποίηση:
    - Βεβαιώσου για την ταυτότητα
    - Βεβαιώσου για την προέλευση πληροφορίας

Βασικό Πρόβλημα: Διαμοίραση Κλειδιού

- Πρόβλημα: Η τεχνική δημόσιου κλειδιού δεν κάνει τη διαμοίραση κλειδιού πολύ ευκολότερη
  - Γιατί; Ακούτε: «Εγώ, ο cda, λέω ότι το δημόσιο κλειδί μου είναι το Κ"
  - Ποιος το είπε;
- Λύση:
  - Trusted server: Εξυπηρετητής ταυτοποίησης (Authentication server)
    - Τον εμπιστεύονται όλοι
    - Δε χρειάζεται να έχουμε N*N κλειδιά.
  - Trusted computing base (TCB)
    - Το λογισμικό και το υλικό πρέπει να «συμπεριφέρονται» με τον ορθό τρόπο
    - Fail-secure.
      - Ασφαλές υπό την παρουσία αστοχιών.

Διαμοίραση κλειδιού με trusted server

1) Ο Α ζητά από τον trusted server (AS) ένα κλειδί για να μιλήσει με τον Β.
    1) Εδώ δε χρειάζεται κρυπτογράφηση
2) Ο AS απαντά με ένα νέο κλειδί διαλόγου (conversation key – CK).
    1) Το μήνυμα είναι κρυπτογραφημένο με το κλειδί του Α ώστε να μπορεί να το διαβάσει μόνο ο Α.
    2) Περιέχει ένα κλειδί, και το κλειδί αποκρυπτογράφησης κρυπτογραφημένο με το κλειδί του Β.
3) Ο Α στέλνει στον Β μήνυμα με το κλειδί.
    1) Ο Α δε μπορεί καν να διαβάσει το περιεχόμενο του μηνύματος, γιατί είναι κρυπτογραφημένο με το κλειδί του Β.

- Παράδειγμα χρήσης: Kerberos.