Ο ρόλος των ανοικτών προτύπων και τεχνολογιών στην επίτευξη της ασφάλειας

Διομήδης Σπινέλλης

Αναπληρωτής Καθηγητής
Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας
Οικονομικό Πανεπιστήμιο Αθηνών
http://www.dmst.aueb.gr/dds

Ανοικτά πρότυπα

- De jure
  - Unicode ISO-10646
  - POSIX IEEE 1003.3
  - Ethernet IEEE 802.*
  - EcmaScript ECMA-262
  - Αρχεία σε CD-ROM ISO/IEC-9660
  - SQL ISO-9075

(Λιγότερο;) ανοικτά πρότυπα

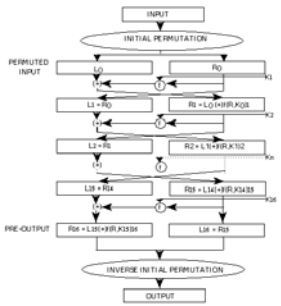
- De facto
  - CIFS (Microsoft)
  - Java (Sun)
  - USB (USB-IF)
  - Eclipse (Eclipse Foundation)

Microsoft

Sun microsystems

Κλειστές τεχνολογίες

- Δεν είναι (εύκολα) διαθέσιμα στοιχεία της
  - διαδικασίας σχεδιασμού
  - υλοποίησης
- Παραδείγματα
  - GSM
  - DVD
  - DES
  - SMB
  - Microsoft Windows
  - Κάρτες γραφικών και Wi-Fi



Πλεονεκτήματα ανοικτών συστημάτων

- Στιβαρός σχεδιασμός
- Αποφυγή λαθών υλοποίησης
- Έλεγχος περιπτώσεων Κερκόπορτας
- Διαλειτουργικότητα

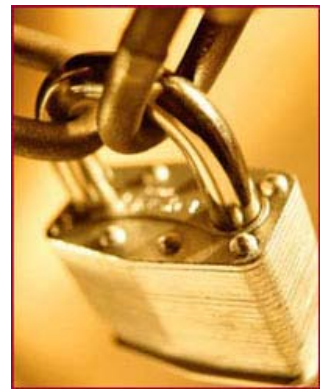
Στιβαρός σχεδιασμός

- Το δόγμα του Kerckhoffs
- Αντιπαραδείγματα
  - DVD CSS
    - DeCSS
  - GSM
    - Σύνοψη Comp128
    - Κωδικοποίηση A5

GSM™ ASSOCIATION

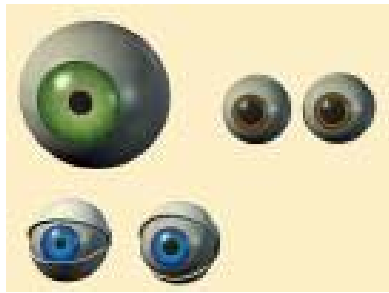
Λογισμικό ανοικτού κώδικα

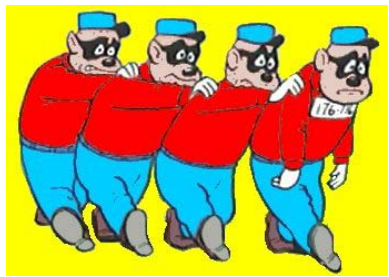
- Η υλοποίηση αποδίδει όταν:
  - βασίζεται σε ανοικτά πρότυπα και γνωστές τεχνολογίες
  - οι αστοχίες δημιουργούν προβλήματα
  - απαιτείται επιθεώρηση από τρίτους
  - υπάρχουν επιχειρηματικά κίνητρα συνεργασίας για διορθώσεις
  - εμφανίζονται οικονομικά φαινόμενα δικτύου
- Όλα τα τα παραπάνω στοιχεία σχετίζονται άμεσα με την ασφάλεια



Αστοχίες σε λογισμικού ανοικτού κώδικα μπορούν:

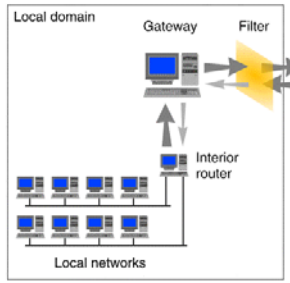
- να εντοπιστούν από τρίτους σε επιθεωρήσεις
- άμεσα να διορθωθούν από έμπειρους χρήστες
- να εντοπιστούν και από κακόβουλους χρήστες
- Να αποτελέσουν κίνητρο για την εύρεση αντίστοιχων λαθών σε άλλα προγράμματα





Έλεγχος περιπτώσεων Κερκόπορτας

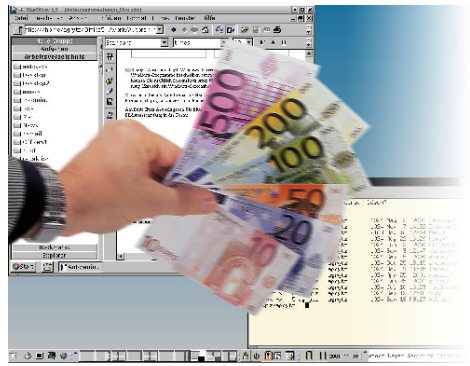
- Παραδείγματα
  - TCP wrappers (NC421)
  - Πυρήνας του Linux (sys_wait4)
  - Crypto AG;
    - Επικοινωνίες της Λιβύης και του Ιράν (NSA)
    - Αποδέκτες: ΗΠΑ και Γαλλία, Ιράκ
  - Microsoft Windows _NSAKEY;



HAGELIN-CRYPTOS
CRYPTO AG

Διαλειτουργικότητα

- Ανταγωνισμός
  - Υψηλότερη ποιότητα
  - Χαμηλότερο κόστος
- Βιοποικιλία



Ιστότοποι

- Open Source Initiative
  - http://www.opensource.org/
- NSA & Crypto AG
  - http://www.aci.net/kalliste/speccoll.htm
- Eric Raymond: The Magic Cauldron
  - http://www.catb.org/~esr/writings/magic-cauldron/
- Windows NSAKEY (Wikipedia)
  - http://en.wikipedia.org/wiki/NSAKEY
- GSM Security Algorithms
  - http://www.gsmworld.com/using/algorithms/index.shtml
- DeCSS Central
  - http://www.lemuria.org/DeCSS/
- Ελεύθερο Λογισμικό / Λογισμικό ανοιχτού κώδικα
  - http://www.ellak.gr/
- Διομήδης Σπινέλλης
  - http://www.spinellis.gr/