Network Security

Alexandre Barbosa Augusto

CRACS/INESCTEC, DCC-FCUP

Agenda

- Basic Tenets of Security
  - Good Security is Hard
  - Massively Deploy-able Security is Even Harder.
  - Problems with Passwords
  - Level of Authentication
- Public Key Infrastructure (PKI)
  - X.509
  - PGP
  - Smartcard

Basic Tenets of Security

- Identity
  - RW (RealWorld): My Name
  - DW(DigitalWorld): Login
- Authentication
  - RW: My Voice
  - DW: Password
- Authorization
  - RW: Money
  - DW: Cookie Session
- Privacy
  - RW: My thoughts
  - DW: Encrypted data

Good Security is Hard

- Always a compromise between:
  - Easy of Use (convenience for the user)
  - Effectiveness (Confidentiality, Integrity, Privacy and Non-repudiation)
  - Cost

- It must be preceded by a comprehensive Analysis of Risk.
  - Otherwise security could end up being more costly then what needs to be protected.

Massively Deployable Security is Even Harder.

- What can you do when you have an installed base of thousands/millions ?
  - Security mechanisms must be extremely:
    - Cheap to deploy
    - Easy to use
    - Configurable by the user
- There is one such popular mechanism.
  - The LOGIN/PASSWORD

Problems with Passwords

- Selection
  - Good secure passwords are hard to find
- Memorization
  - It is easy to forget infrequently used passwords
  - It is hard to remember secure passwords
- Reuse
  - To many different passwords to memorize
  - People reuse the same password all over

Problems with Passwords

- Online Banking is one prime example of management of highly valuable assets on the Internet.
  - Online Banks are very convenient for the costumer and save of lot money to the Banks.
  - “Phishing” attacks became widespread and are quite effective at stealing user credentials.
  - Banking dedicated Malware provides high returns to the attacker

Risk Analysis tell us that Login/Password is not appropriate to protect these assets.

Level of Authentication

- Are based on:
  - Something you know (password/PIN)
  - Something you have (Token, Smartcard)
  - Something you are (Biometric)
- The typically single-factor authentication is the "username/password".
- The two-factor authentication adds something else, usually something you have.

Public Key Infrastructure (PKI)

- Is responsible to:
  - bind an identity to a public key by the usage of digital signature(s) in order to create the certificate.
  - Manage the digital certificates (create, store, distribute and revoke)
- Grants a two-factor authentication
- There are different concepts in order to manage a PKI.

X.509 certificate

- Is issued by a certificate authority (CA).
- Hierarchical approach
- Supports only one signature.
- Massively deployed over computer systems:
  - On browsers to prove web site authenticity and to establish a secure channel for data exchange.
  - On single sign-on (SSO) systems to give temporary access to a resource.

PGP (pretty good privacy) cert.

- Is issued by its creator (self-signed) .
- Supports multiple signatures in order to grant a greater trust on network
- Based on a web of trust
- Widely used on emails systems in order to prove an identity or cypher information
- It is free

Smartcard

- Grants a non tampering security feature
- Provide the necessary crypto components allowing:
  - Secure personal and cryptographic data
  - Identification
  - Strong authentication
  - Digital signature
  - Encrypt data

Smartcard

- Grants:
  - a two-factor authentication
  - Data integrity
  - Privacy
  - Non-repudiation
- It is widely deployed on the world:
  - Citizen card
  - Bank cards
  - Universities

Question ?