Administrivia

Course information sheet
Sign up online (re-register)

Content

- Computing or communicating in the presence of adversaries
- Protecting some resource, communication, activity
- Typically involves information system
  PC, network of computers, cell phones, pay TV, E-mail, cars, ATM machines, RFIDs, iPODs

Internet means attack can come from anywhere!

Security Policy

- Gives desired security objectives or properties
  - "Each registered voter may vote at most once"
  - "Only an admin can modify this file"
  - "The recipient of an email message shall be able to authenticate its sender"

principals with roles perform actions on objects

Categories of Policies

Confidentiality: Information should not be disclosed to unauthorized parties (passwords)

Integrity: information should not be modified in an unauthorized manner (available $ on e-ticket)

Availability: system or resource shall be available for use as intended (Internet: Denial-of-Service attack)

Adversary / Threat model

- May be insider/outsider, vendor
  Ex: Voter may wish to sell her vote
  Election official may be corrupt
  Vendor may sell systems with back doors
  User of iphone wishes to subvert DRM scheme
- What does adversary know?
  Ex: system design & implementation details
  passwords
- What resources does adversary have?
  - Large computers
  - ability to interrupt & modify all communications
  - ability to corrupt some participants (e.g., pay TV subscriber or voter)

Typically make generous assumptions about adversary's abilities.

Security Mechanism

is component, technique or method for (attempting to) achieve or enforce security policy

Ex: smart card for voter
password for sysadmin
digital signature for message sender

Mechanisms (a.k.a. countermeasures) are typically of one of two forms:

- prevention: keep security policy from being violated
  Ex: fence, encryption, memory bounds check
- Detection: identify when policy is violated
  Ex: motion sensor, tamper-evident seal, stored fingerprint ("hash") of all executables

Usually come with recovery mechanism, e.g., remove virus, load files from backup

Mechanisms

- Identification of principals ("user name")
- Authentication of principals (password, biometric)
- Authorization: checking permission list to see if principal is authorized for requested action
- Physical protection: locks, key storage should be secure
- Cryptography: math in service of security

You will see a lot of applied cryptography in this class for authentication, authorization and other mechanisms.

Google attack (Our Theory)

Was not a standard attack of hackers attacking a website.

Gmail stores all of its data in Google File System (GFS)

MAILBOX — file encrypted using a master key → stored on a few very well secured servers

Gmail machines load them up in RAM
(run special kernels that provide strong isolation)

For performance reasons, some cache files stored in GFS are unencrypted and protected by ACLs

needed for inbox view (headers & first words for first few messages)

Attackers had access to Gmail source code
- found out where cache files were
- likely exploited bug in ACLs

Some Principles

- Be skeptical & paranoid
- No security through obscurity
  - crypto is very useful, assume keys are secret, all protocols public
- Physical protection is foundation
- Defense in depth / layered defense
- Trade off cost / security
  - cannot hope for perfect security
- Separation of privilege
  - require 2 people to perform task
- Principle of least privilege