Security Goals

Slides adapted from "Foundations of Security: What Every Programmer Needs To Know" by Neil Daswani, Christoph Kern, and Anita Kesavan (ISBN 1590597842; http://www.foundationsofsecurity.com). Except as otherwise noted, the content of this presentation is licensed under the Creative Commons 3.0 License.

Welcome!
Course Goals:

- Security Goals
- Security Design Principles
- Malware
- Buffer Overflows & Other Control Hijacking
- Client-State Manipulation
- Password Security
- SQL Injection
- Cross-Site Attacks
- Cryptography

Preliminaries

- Slide numbers correspond to book chapters / sections
- Will not cover all chapters / sections (may also not go in order)
- Resources available at: www.foundationsofsecurity.com

Security Goals

Agenda

- Seven Key Security Concepts:
  - Authentication
  - Authorization
  - Confidentiality
  - Data / Message Integrity
  - Accountability
  - Availability
  - Non-Repudiation
- System Example: Web Client-Server Interaction

1.1. Security Is Holistic

- Physical Security
- Technological Security
  - Application Security
  - Operating System Security
  - Network Security
- Policies & Procedures
- All Three Required

1.1.1. Physical Security

- Protecting against information leakage and document theft
- Limit access to physical space to prevent asset theft and unauthorized entry
- Ex: *Dumpster Diving* - gathering sensitive information by sifting through the company's garbage

1.1.2. Technological Security (1) (Application Security)

- No flaws in identity verification process
- Configure server correctly
  - local files
  - database content
- Interpret data robustly

1.1.2. Technological Security (2) (OS & Network Security)

- Apps (e.g. servers) use OS for many functions
- OS code likely contains vulnerabilities
  - Regularly download patches to eliminate (e.g. Windows Update for critical patches)
- Network Security: mitigate malicious traffic
- Tools: Firewalls & Intrusion Detection Systems

1.1.3. Policies & Procedures

- Ex: *Social engineering attack* - taking advantage of unsuspecting employees (e.g. attacker gets employee to divulge his username & password)
- Guard sensitive corporate information
- Employees need to be aware, be educated to be somewhat paranoid and vigilant

Security Concepts

- Authentication
- Authorization
- Confidentiality
- Data / Message Integrity
- Accountability
- Availability
- Non-Repudiation

Archetypal Characters

- Alice & Bob – “good guys”
- Eve – a “passive” eavesdropper
- Mallory – an “active” eavesdropper
- Trent – trusted by Alice & Bob

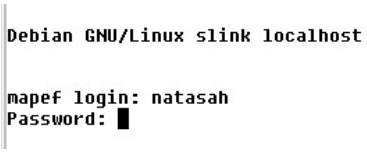
Alice

Bob

1.2. Authentication

- Identity Verification
- How can Bob be sure that he is communicating with Alice?
- Three General Ways:
  - Something you ***know (i.e., Passwords)***
  - Something you ***have (i.e., Tokens)***
  - Something you ***are (i.e., Biometrics)***

1.2.1. Something you *KNOW*



- Example: Passwords
  - Pros:
    - Simple to implement
    - Simple for users to understand
  - Cons:
    - Easy to crack (unless users choose strong ones)
    - Passwords are reused many times
- One-time Passwords (OTP): different password used each time, but it is difficult for user to remember all of them

1.2.2. Something you *HAVE*

- OTP Cards (e.g. SecurID): generates new password each time user logs in
- Smart Card: tamper-resistant, stores secret information, entered into a card-reader
- Token / Key (i.e., iButton)
- ATM Card
- Strength of authentication depends on difficulty of forging

1.2.3. Something you *ARE*

- Biometrics

Technique	Effectiveness	Acceptance
Palm Scan	1	6
Iris Scan	2	1
Retinal Scan	3	7
Fingerprint	4	5
Voice Id	5	3
Facial Recognition	6	4
Signature Dynamics	7	2

- Pros: “raises the bar”
- Cons: false negatives/positives, social acceptance, key management
  - false positive: authentic user rejected
  - false negative: impostor accepted

1.2.4. Final Notes

- Two-factor Authentication: Methods can be combined (i.e. ATM card & PIN)
- Who is authenticating who?
  - Person-to-computer?
  - Computer-to-computer?
- Three types (e.g. SSL):
  - Client Authentication: server verifies client's id
  - Server Authentication: client verifies server's id
  - Mutual Authentication (Client & Server)
- Authenticated user is a "Principal"

1.3. Authorization

- Checking whether a user has permission to conduct some action
- Who you are vs what you are allowed to do
- Is a "subject" (Alice) allowed to access an "object" (open a file)?
- *Access Control List*: mechanism used by many operating systems to determine whether users are authorized to conduct different actions

1.3.1. Access Control Lists (ACLs)

- Set of three-tuples
  - <User, Resource, Privilege>
  - Specifies which users are allowed to access which resources with which privileges
- Privileges can be assigned based on roles (e.g. admin)

Table 1-1. *A Simple ACL*

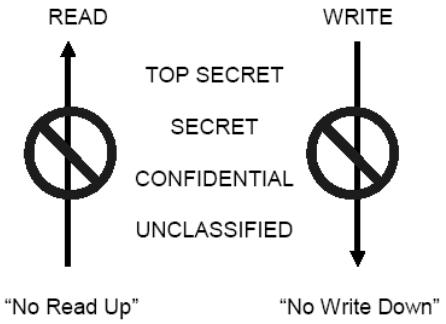
User	Resource	Privilege
Alice	/home/Alice /*	Read, write, execute
Bob	/home/Bob /*	Read, write, execute

1.3.2. Access Control Models

- ACLs used to implement these models
- *Mandatory*: computer system decides exactly who has access to which resources
- *Discretionary* (e.g. UNIX): users are authorized to determine which other users can access files or other resources that they create, use, or own
- *Role-Based* (Non-Discretionary): user's access & privileges determined by role

1.3.3. Bell-LaPadula Model

- Classifications:
  - Top Secret
  - Secret
  - Confidential
  - Unclassified
- 3 Rules/Properties
  - Simple property
  - *-property (confinement)
  - Tranquility property



1.4. Confidentiality

- Goal: Keep the contents of communication or data on storage secret
- Example: Alice and Bob want their communications to be secret from Eve
- *Key* – a secret shared between Alice & Bob
- Sometimes accomplished with
  - Cryptography, Steganography, Access Controls, Database Views

1.5. Message/Data Integrity

- Data Integrity = No Corruption
- *Man in the middle attack*: Has Mallory tampered with the message that Alice sends to Bob?
- *Integrity Check*: Add redundancy to data/messages

- Techniques:
  - Hashing (MD5, SHA-1, …), Checksums (CRC…)
  - Message Authentication Codes (MACs)
- Different From Confidentiality:
  - A -> B: "The value of x is 1" (not secret)
  - A -> M -> B: "The value of x is 10000" (BAD)
  - A -> M -> B: "The value of y is 1" (BAD)

1.6. Accountability

- Able to determine the attacker or principal

- Logging & Audit Trails

- Requirements:
  - Secure Timestamping (OS vs. Network)
  - Data integrity in logs & audit trails, must not be able to change trails, or be able to detect changes to logs
  - Otherwise attacker can cover their tracks

1.7. Availability

- Uptime, Free Storage
  - Ex. Dial tone availability, System downtime limit, Web server response time
- Solutions:
  - Add redundancy to remove single point of failure
  - Impose "limits" that legitimate users can use
- Goal of DoS (Denial of Service) attacks are to reduce availability
  - Malware used to send excessive traffic to victim site
  - Overwhelmed servers can't process legitimate traffic

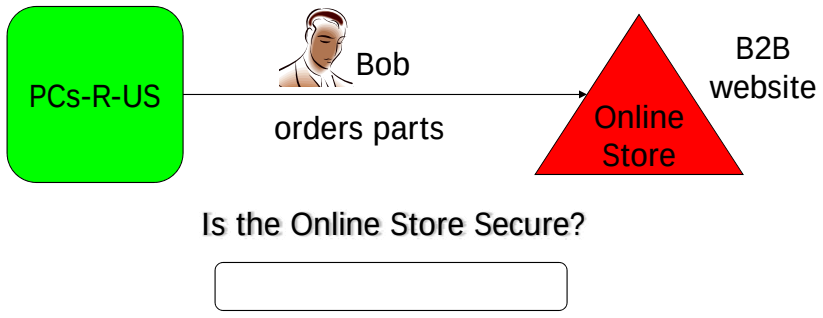
1.8. Non-Repudiation

- Undeniability of a transaction
- Alice wants to prove to Trent that she did communicate with Bob
- Generate evidence / receipts (digitally signed statements)
- Often not implemented in practice, credit-card companies become de facto third-party verifiers

Lots of concepts!

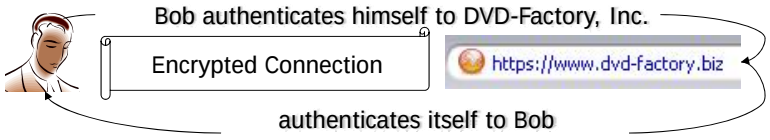
- Popular mnemonic acronyms
- AAA:
  Authentication, Authorization, Accounting
- CIA:
  Confidentiality, Integrity, Availability

1.9. Concepts at Work (1)



1.9. Concepts at Work (2)

- Availability:
  - Online Store ensures its web site is running 24-7
- Authentication:



- Confidentiality:
  - Bob's browser and Online Store web server set up an encrypted connection (lock on bottom left of browser)

1.9. Concepts at Work (3)

- Authorization:
  - Online store web site consults DB to check if Bob is authorized to order widgets on behalf of PCs-R-Us
- Message / Data Integrity:
  - Checksums are sent as part of each TCP/IP packets exchanged (+ SSL uses MACs)
- Accountability:
  - Online store logs that Bob placed an order for Sony DVD-R 1100
- Non-Repudiation:
  - Typically not provided w/ web sites since TTP req'd.

Summary

- Technological Security In Context
- Seven Key Security Concepts
- Online Store Example:
  Security Concepts at Work