

SE-4920: Lecture 3 Engineering Introduction

- Reading: Chapter 1
- Today's Outcomes: Briefly describe the following concepts as they relate to computer security...
 - How data crosses a network
 - Active vs. passive attacks
 - Benefits of cryptography at various layers
 - Authorization systems
 - Tempest and zone of control
 - Key escrow
 - Discretionary and mandatory access controls
 - Covert channels
 - Orange book
 - Overview of legal climate

1

Communication example with the "CI" properties from last time

- Dr. Durant and Scott want to shout messages to each other across the room that only they understand ("Confidentiality")
 - "The room" = insecure medium = many computer networks
- Additional goal on a network
 - Dr. Durant must know the message really came from Scott and that it was not modified in transit ("Integrity")
 - Digital signature – can only be made by Scott; is message specific
- Basis of security and cryptography
 - Only known way to solve certain problems is through "brute force"
 - How long does it take to run an algorithm 2^{64} times or 2^{128} times?
 - Complexity goal (can come close enough to this in practice)
 - $\Theta(N)$ for users
 - $\Theta(2^N)$ for attackers

2

Networking Overview

- (Some of this is review if you took CS-495)
- OSI (Open Systems Interconnection) Reference Model
 - A 7-layer model of how network communications are built up starting with the physical medium
 - An ambitious, general model, but a useful one
 - Many networks use simplified 3-5-layer models
 - Each layer connects directly only to the layer above and the layer below
 - But, logically, it connects to the equivalent layer on the other end of the communication
 - Lower layers add headers to each packet

3



OSI Model

- 7. Application – programs, HTTP, FTP
- 6. Presentation – system dep., *e.g.*, SSL
- 5. Session – (seldom used in IP)
- 4. Transport – reliability, seq., retransmit.
- 3. Network – multiple links, src. to dest.
- 2. Data link – packets, link sharing
- 1. Physical – wires, optical fibers, ...

4



TCP/IP suite (Internet, etc.)

- Layer 4 (Transport)
 - 2-octet source and destination ports
 - TCP: sequencing, unlimited size, retries
 - UDP: size limits, no retrying, best effort
- Layer 3 (Network): IP
 - Header with source and destination addresses
 - 1-octet protocol number (select TCP or UDP)


5



Routing

- Ultimate and next-hop destinations
- Layer 4 (Transport): inner envelope: information about errors, retries
- Layer 3 (Network): middle envelope: contains the ultimate destination
- Layer 2 (Data link): outer envelope: contains the next destination


6



Active vs. Passive Attacks

- Passive attack – attacker observes, but does not modify, network traffic
 - Hard or impossible to detect
 - Goal: gather/analyze information over the long term
 - Countermeasure: good encryption makes observed information useless
- Active attack – attacker modifies, replays, and/or deletes messages from the network
 - Easier, but not always simple to detect
 - Goal: impersonate a party, get a party to divulge secrets
 - Countermeasures: good protocol design, protocols that can prove you know a secret without divulging it, proper use of public key cryptography


7



Layers and Cryptography

- End-to-end
 - Benefits: lower layers need no cryptographic knowledge, no trust in lower layers needed, protect stored messages
- Hop-by-hop
 - Benefits: eavesdroppers can't see source and destination
 - Disadvantage: must trust packet switches
- May combine

8



Authorization – “What you’re allowed to do”

- vs. authentication – “Who are you?”
- ACL (access control list) model
 - Each resource has a list of who can do what associated with it (scaling problems for many users)
- Capability model
 - Each user has a list of capabilities (scales poorly if we need to list capabilities for each resource)
- Solution:
 - Groups: each user is a member of one or more groups, and ACLs can name one or more groups

9



Tempest

- US military program that measures how close one needs to be to a device to be able to detect data from its electronic emanations
- Control zone: the region that must be physically guarded to prevent wireless eavesdropping

10



Key Escrow

- Guard against losing important, secret quantities
 - By backing them up, carefully
- For law enforcement
 - Clipper proposal in mid-1990s
 - User encryption hardware, each with a unique key
 - Keys escrowed in 2 parts ($K = P1 \text{ XOR } P2$)
 - Never caught on; it seems the genie is out of the bottle now
- For careless users
 - May be easy for administrator to re-issue a login key
 - But, what about encryption key for sensitive data?

11



The multi-level model of security

- Discretionary access controls
 - If I have access to information, I can grant others access (*e.g.*, a printout)
- Mandatory access controls
 - The authorized person cannot share
 - No "read-up"
 - Cannot read more secure information than clearance allows
 - No "write-down"
 - Cannot write information that those with lower clearance can read

12



Covert channels

- We generally must live with the risk that a user will memorize sensitive information, walk outside of the secure building, and share it
 - But, the bandwidth is low
- Covert channels
 - Ways to bypass confinement of information
 - Do something that is observable outside the security perimeter
 - Use CPU heavily vs. lightly (performance monitoring)
 - Create a file that a less privileged can test for existence
 - Tend to be of very low bandwidth

13



The Orange Book

- NCSC (National Computer Security Center) criteria for rating the security of a system
- Focuses on
 - keeping data secret
 - and not trusting users (*e.g.*, mandatory access controls),
 - but not data integrity, which may be more important in the commercial world.

14



The Orange Book Classifications

- D – minimal protection (no higher standard met)
- C1 – discretionary security protection
 - Classic timesharing systems: protect memory from overwrites, at least basic access controls on resources (*e.g.*, UNIX ugo:rw), protected password system
- C2 – controlled access protection
 - Adds more granular access control (*e.g.*, ACLs); clearing of allocated memory; configurable, tamper-proof auditing
- B1, B2, B3
 - Add features focusing on attached devices, secure designs, covert channels, and secure crashing
- A1 – Verified design
 - Adds formal procedures for analysis and design

15



Legal issues (another great presentation topic)

- Legal climate has greatly improved in the past 5-10 years
- Many patents on encryption technologies have expired
- US export restrictions have generally been lifted...
 - 7 countries are still on a no-export list
 - 31 countries with no restrictions
 - Remaining countries have a few restrictions

16
