Computer and Network Security

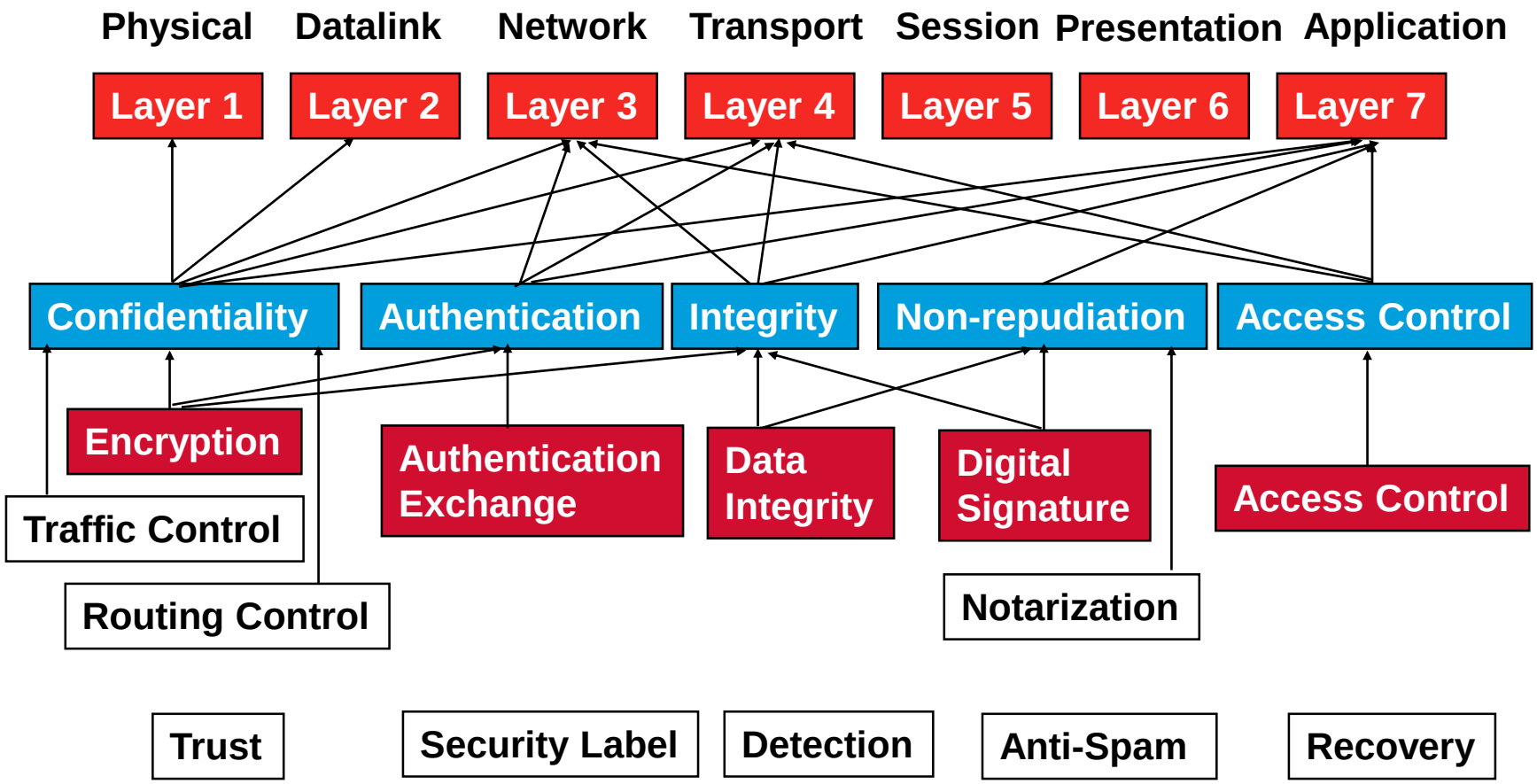
Dr. Chan Yeob Yeun

Week 2

Weekly Lecture Plan

Wk	Contents	Cmt	Wk	Contents	Cmt
1	**Introduction**		9	Foundations of Network Security II	
2	Foundations of Computer Security	Tutorial Assig Plan	10	Network-Based Threats and Attacks	
3	Identification and Authentication I		11	Network Security Protocols I	
4	Identification and Authentication II	Quiz 1	12	Network Security Protocols II	Quiz 3
5	Access Control		13	Firewalls	
6	Modern Computer Attacks		14	IDS / IPS	Assig Submit
7	Malicious Code	Assig Confirm	15	Revision and Presentation	
8	Foundations of Network Security I	Quiz 2	16	Exam	

What is Computer and Network Security ?



General Approaches

Computer security techniques can apply to the design and construction of a secure system and to its correct operation. When we look into design, we will discuss general approaches, as well as considering all the relevant low-level technical aspects. For the correct operation of a system we mainly look at:

AAA: Authentication, Authorization and Auditing.

All defenses come under one of the three categories, in decreasing order of effectiveness:

- Prevention
- Detection
- Response

Prevention

An attack is prevented if the intended action that would cause the negative impact is stopped.

The idea of preventing attacks before they succeed is the most desired scenario in computer security.

But prevention is costly, both in financial terms and trade-off costs in functionality/availability.

And even when it is possible, it is typically only in a limited case.

Either there are theoretical constraints (e.g. brute-force always possible against cryptographic protections) or time constraints (e.g. a certain vulnerability may be patched, but it's typically only a matter of time before the next one is found).

Examples of preventative measures are cryptography, firewalls, IPS systems.

Detection

An attack is detected if an alert is raised during or after it occurs.

If it is possible for an attack can be detected, then it seems like it should have been prevented.

But detection is an easier goal for the simple reason that it can happen at any time after the fact, while prevention needs to be real time.

It is very easy for attack signatures to get “lost in the noise”.

Examples of detective measures are anti-virus scanners and IDS systems.

Response

Response is any action taken as a reaction to a successful attack. The action is likely to be one of recovery. This can include cleaning the system of infection, restoring les from backups, returning configuration to a previously known good state.

To be absolutely sure of removing any lingering trace, a compromised machine can be wiped and have the OS reinstalled, or even physically destroyed.

Other examples of responses are legal actions and updating of security procedures.

Hardware Security: USB

One example of a piece of hardware that is of interest from a computer security point of view is the USB drive.

In terms of productivity, it is very useful. Large les can be transferred quickly between devices, usually regardless of hardware or OS. Because of this convenience, they are popular.

They are difficult to control, being a collection of independent devices.

Almost all computers today have a USB port. How do you protect the information when it is transported on a USB drive?

How do you prevent malicious code from using USB to propagate?

Disabling of Autorun is typically a recommended fix.

Hardware Security: Tamper-Resistant

A device is said to be tamper-resistant if it makes difficult any deliberate altering or modification of the device.

A simple method to achieve this is to use special screws that cannot be opened using standard equipment.

More sophisticated chips will only release sensitive information encrypted, and will zero all keys upon discovery of any attempt at probing or physical tampering (an internal battery will ensure this is possible even when the device is powered off).

Given the number attacks possible if an attacker has the device at his disposal (drilling, solvents, freezing, time and power measurements), tamper-resistance is extremely hard to achieve in practice.

Operating System Security

Operating systems control just about all aspects of what we do on computers. Historically, OSes were single-user and enjoyed hardware enforced protection:

Modern OSes are multiprogramming: capable of managing more than one application, job or user.

The OS needs to manage many resources of different types (memory, I/O devices, storage, applications, libraries, etc.).

In some cases the resources need to be shared (processor, I/O, libraries), and in some cases they need to be separated (memory, storage).

Hardware-enforced protection is generally more reliable than software, but making assumptions about what hardware is present can hurt the commercial appeal.

Operating System Security: Separation

So what can be done by the OS to protect the system?
The basis of the OS protection is separation, keeping one user's objects separate from other users (and from those who are unauthorized). There are a number of ways this can be done:

Physical separation
Temporal separation
Logical separation
Cryptographic separation

But to gain any benefit from using a multiuser OS, there has to be some sharing of different functionality available.

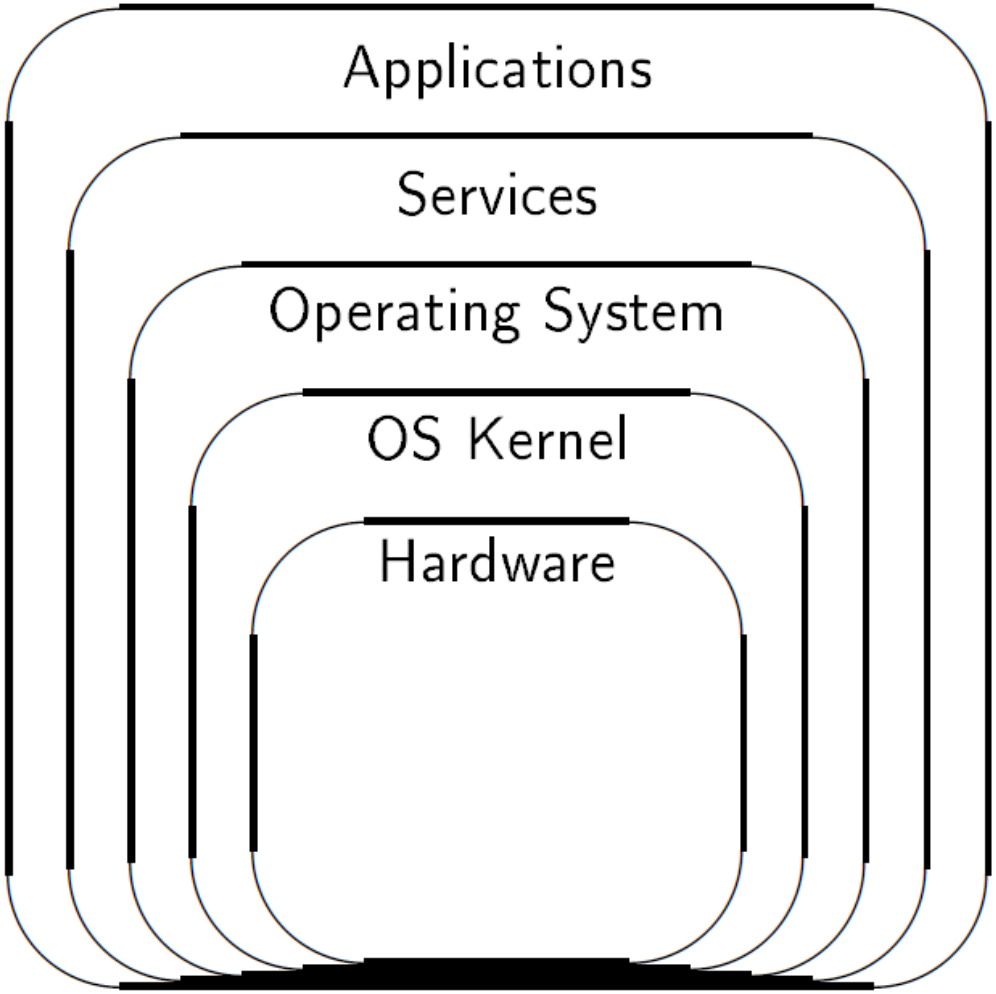
Maintaining separation where necessary and still allowing useful sharing is the main security problem in operating systems.

OS Protection

An operating system controls the access to all the resources on a given device. Because of the power they wield, they are a frequent target for attack. Operating systems provide four primitive security services:

Memory protection
File protection
General object access control
User authentication

Operating System Security: Layered Design



Introduction to Network Security

Network architecture is layered

Lower layer vulnerabilities are inherited at higher levels

Describing exploitable features and vulnerabilities in the scope of each layer makes sense

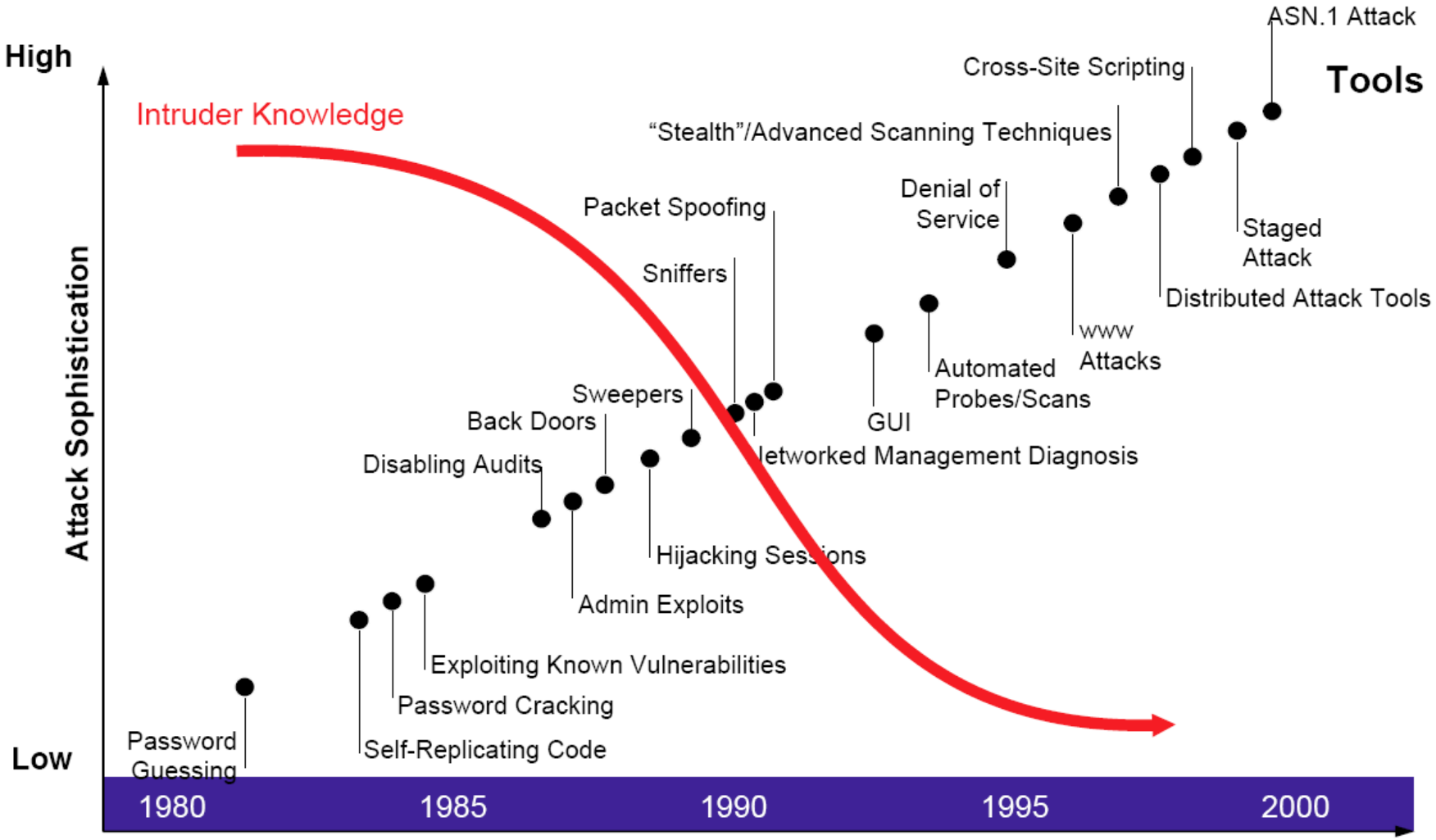
Example: TCP/IP v.4 is dominant design in use

Many vulnerabilities can't be prevented without a major transition to a completely new design, or are hard problems

Most core vulnerabilities can't really be fixed

- This is an important design consideration for any application that needs to use network

Evolution of Attacks



Hacker's Motivation

From a hobby to a **profitable industry**

From annoying to **destructive**

From playing to **stealing**

From simplicity to **complexity**

Source: http://www.discovery.com/area/technology/hackers/hackers.html

Seven Sins in Cyber Space

Cyber Seven Sins

Collapse Of Trust

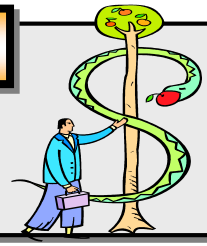
Hacking of Internet Banking

Sphere and Shield

Illegal Spam Mails
Advertisement Mobile Mess

Temptation

Spyware
Adware



ID Theft

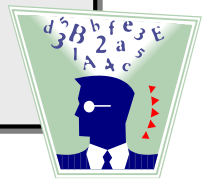
Forgery and alteration of
Civil Affairs Documents

Cyber Terror

Homepage Defacement

Privacy Infringement

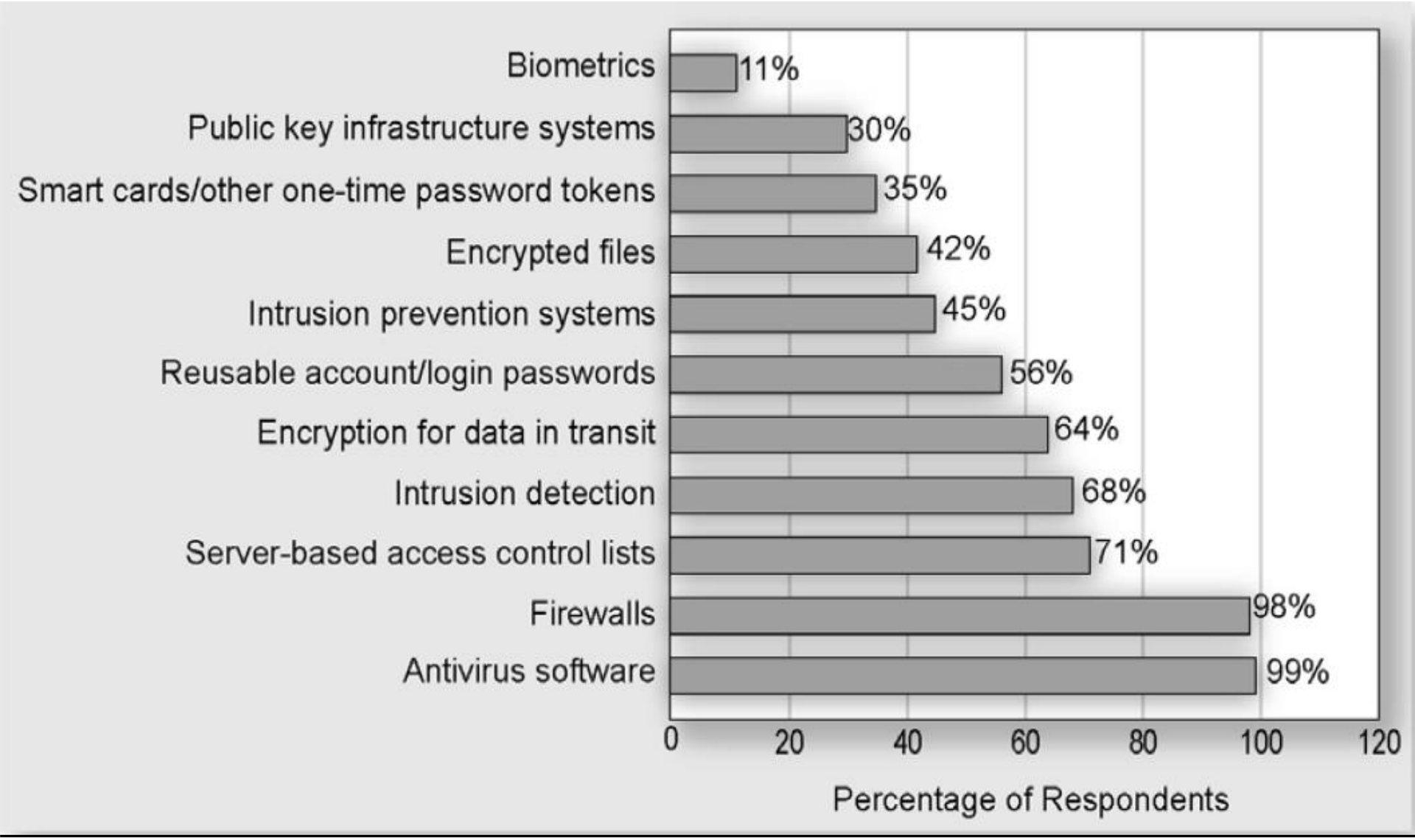
Stealing Social Security Number,
Information Leakage of
Personal and Customer's
information



Digital Fraud

Phishing
Pharming

Tools & Technology



Network Model

OSI Model

- 7 layers
- Old
- Applications often have properties of several layers at once
  - Makes classification difficult, confusing

TCP/IP Model

- "DoD" model (Department of Defense)
- 5 layers

OSI 7-Layer Model

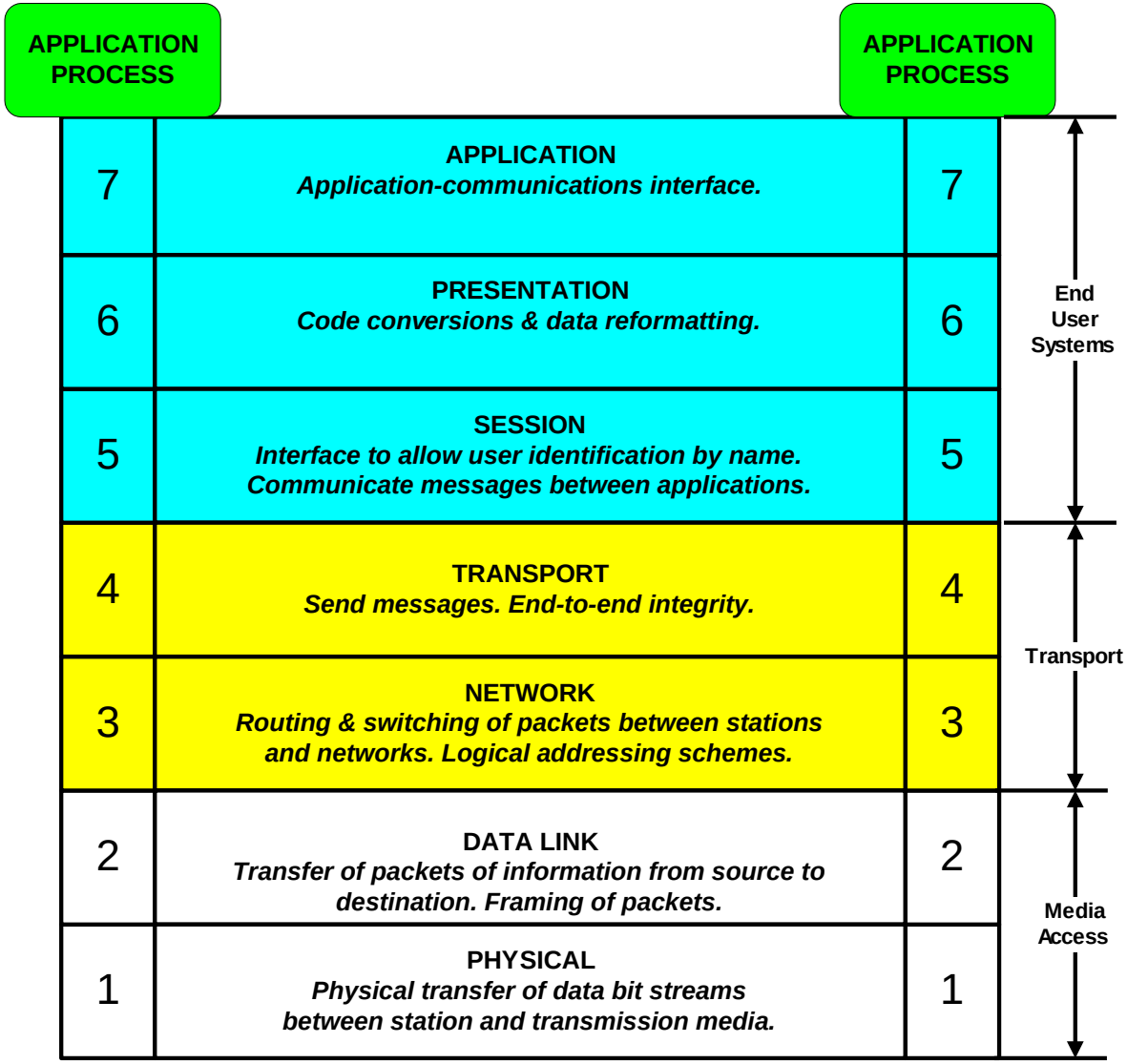
OSI: Open Systems Interconnection

ISO standard

Layered approach provides:

- Simplification
- Abstraction
  - Each layer talks only to the equivalent layer somewhere else
- Division of responsibilities
- Standardization and interchangeability of equipment from different makers

OSI 7-Layer


APPLICATION PROCESS
APPLICATION PROCESS
7
APPLICATION
Application-communications interface.
7
6
PRESENTATION
Code conversions & data reformatting.
6
5
SESSION
Interface to allow user identification by name.
Communicate messages between applications.
5
4
TRANSPORT
Send messages. End-to-end integrity.
4
3
NETWORK
Routing & switching of packets between stations
and networks. Logical addressing schemes.
3
2
DATA LINK
Transfer of packets of information from source to
destination. Framing of packets.
2
1
PHYSICAL
Physical transfer of data bit streams
between station and transmission media.
1
End User Systems
Transport
Media Access

OSI vs. TCP/IP

<table>
<tr><th>OSI
MODEL</th><th>TCP/IP</th></tr>
<tr><td>APPLICATION
7</td><td rowspan="3">APPLICATION

Worldwide Web: http
Remote Login: telnet, rlogin
Remote Commands: rexec, rsh
File Transfers: ftp, rcp, tftp, UUCP
E-mail: SMTP, POP3, IMAP
Remote File Systems: NIS/NFS, RPC</td></tr>
<tr><td>PRESENTATION
6</td></tr>
<tr><td>SESSION
5</td></tr>
<tr><td>TRANSPORT
4</td><td>TRANSPORT

Tranmission Control Protocol (TCP)
User Datagram Protocol (UDP)</td></tr>
<tr><td>NETWORK
3</td><td>INTERNETWORKING

Internet Protocol (IP)
Internet Control Message Protocol (ICMP)</td></tr>
<tr><td>DATA LINK
2</td><td rowspan="2">NETWORK INTERFACE
&
HARDWARE
CONNECTIONS

LAN: Ethernet, Token Ring, FDDI, ATM...
WAN: SLIP/PPP, X.25, Frame Relay...</td></tr>
<tr><td>PHYSICAL
1</td></tr>
</table>

Physical Layer

Specifies the physical signals (electrical, optical, etc...)

- Type
- Levels
- Speed
- Cables if any

Range

Examples:

- Ethernet coaxial cable specification

Physical Layer Risks

- Disconnection
  - Cut cable
  - Barrier to radio waves
  - Availability
- Eavesdropping
  - Tap in cable
  - Confidentiality
- Interference and Jamming
  - Selective jamming
  - Availability
- Interception
  - Splice in cable, with attacker in-between
    - "man-in-the-middle"
    - Can also work on wireless networks (see later)
  - Can selectively remove or modify messages
  - Integrity
- Physical integrity difficult to guarantee
  - Pressurized pipes, etc...
  - Integrity of radio waves

Data Link Layer

How to transmit data between two stations in the same segment

Two components

MAC (Media Access Control)

- Control which station receives which data
- Which station has permission to transmit
- MAC addresses uniquely identify stations (in theory)

LLC (Logical Link Control)

- frame synchronization

  Data unit is called a frame
- flow control
- error checking

Network Layer

- Routing between segments
- Forwarding
- Addressing
- Internetworking
- Error handling
- Congestion control
- Packet sequencing
    - Data units are called "packets"

Network Layer Vulnerability

- We'll discuss IPv4, although other protocols can be used at this level
- IP features
  - Network addresses
  - IP spoofing: Any station can send packets pretending to be from any IP address.
  - Fragmentation: Firewalls and intrusion detection systems (IDS) may reassemble packets differently from how the attacked operating systems do it.
- IP Components:
  - ICMP: Internet Control Message Protocol (Not Authenticated!)
    - **Denial of service by sending forged ICMP unreachable packets**

Transport Layer

- Transport layer components dependent on IP:
  - UDP: User Datagram Protocol
  - TCP: Transmission Control Protocol
- Reliability
  - retransmissions, etc...
- Error recovery
- Flow control

Transport Layer Vulnerability

Transport layer protocols

UDP

- **Best effort delivery**
  - **Letter in the mail, hope it gets there (and does most of the time) – Connectionless**
- **UDP does not in itself introduce new vulnerabilities, but makes the exploitation of IP layer vulnerabilities easy.**
- **Makes applications more difficult to design to prevent amplification and ping-pong effects**
- **When is UDP needed?**
  - **Domain Name System: Normal hosts query DNS servers using UDP in practice**
  - **UDP also used for other DNS functions (more on this later) Streaming video, Voice-over-IP**

TCP

- **Reliable**
  - **Receiver uses sequence numbers to correctly reorder segments and remove duplicates**
- **Establishes connections and monitors deliveries**
  - **Similar to packages requiring signatures at delivery**

Other Layers

Session

- Handles connections between applications

Presentation

- Handles encoding, encryption, etc...

Application

DNS Vulnerability

You can't authenticate based on host names

You can't rely on DNS as per the original RFCs

DNS is more vulnerable if hosted outside your network

Some attacks (IP spoofing) prevented by ingress filtering

- **Don't accept packets from outside, pretending to originate from inside the network**
- **Except if DNS server is hosted outside the network!**
  - **No defense then**

NIS Vulnerability

"Network Information Services (NIS) clients download the necessary username and password data from the NIS server to verify each user login"

How much can you trust the client?

- Doesn't encrypt the username/password information sent to the clients with each login
- All users have access to the encrypted passwords stored on the NIS server

Crack at leisure

Active Directory can specify mechanism

Authentication mechanisms

Kerberos (requires infrastructure support)

NULL sessions (no passwords)

Secure Routing Requirements

Routing information must have:

- Integrity
- Authenticity
- Authorization
- Timeliness
  - **Resist replay attacks**

An attacker can send a packet specifying the return route

- The attacker may control one of the "routers" on the return route
- Attacker needs to send a single valid packet for that new route to be used for the entire TCP connection
  - **Initial sequence number just has to be guessed correctly once**
  - **TCP session sniffing**
  - **Man-in-the-middle attack**
    - **On-the-fly packet modification**
    - **Dropping packets selectively, or all packets**

MIM Routing Attack

Send a message to all gateways, saying the gateway to network A has made network A unreachable

Send another message advertising that you can reach network A cheaply

You will start receiving all traffic for network A

Forward the traffic to the original gateway, after doing whatever you want to do with it

Authentication in OSPF

Open Shortest Path First (OSPF) is an authenticated link state protocol (RFC 2328) running directly on top of IP (proto 89) and using multicasts instead of broadcasts

Alternative to Routing Information Protocol (RIP)

Methods:

1. Password (plain text), vulnerable to sniffers
2. Keyed MD5 (a.k.a. HMAC-MD5)
   - **K is a shared secret key (padded with zeros)**
   - **M is the message**
   - **H() is a hash function like MD5**
   - **F(K, M) is a function that pre-mixes M and K**
   - **Idea: Along with message, send also H(F(K,M)). Routers that know K can verify the integrity of M, as well as authenticate the message.**
   - **See RFC 1828**
   - **Similar to TCP MD5 signature option (RFC 2385)**

TCP/IP Model

5 layers:

- Application (combines presentation and session)
- Transport
- Network
- Data Link
- Physical

We will use this one as it is less ambiguous

SSL / TLS

History

- Standard libraries and protocols for encryption and authentication
- Secure Sockets Layer (SSL) originally developed by Netscape
  - **SSL v3 draft released in 1996**
- Transport Layer Security (TLS) formalized in RFC2246 (1999)

Uses

- HTTPS, IMAP, SMTP, etc

Issues

- Proxies?

Secure Shell (SSH)

- Negotiates use of many different algorithms
- Encryption
- Server-to-client authentication
  - Protects against man-in-the-middle
  - Uses public key cryptosystems
  - Keys distributed informally
  - Signatures not used for trust relations
- Client-to-server authentication
  - Can use many different methods
  - Password hash
  - Public key
  - Kerberos tickets

IPSec

Protection at the network layer

- **Applications do not have to be modified to get security**

Actually a suite of protocols

IP Authentication Header (AH)

- **Uses secure hash and symmetric key to authenticate datagram payload**

IP Encapsulating Security Payload (ESP)

- **Encrypts datagram payload with symmetric key**

Internet Key Exchange (IKE)

- **Does authentication and negotiates private keys**