Terminology

What is Security?

Security is keeping unauthorized entities from doing things you don't want them to do.

This definition is too informal...

What is Security?

- Confidentiality
- Integrity
- Avaibility

Confidentiality

- "The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity]." [definitions from RFC 2828]
- Not the same as *privacy*.
- **Privacy**: "The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others."
- Privacy is a reason for confidentiality

Integrity

- **data integrity**: "The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner."
- **system integrity**: "The quality that a system has when it can perform its intended function in a unimpaired manner, free from deliberate or inadvertent unauthorized manipulation."
- Often of more commercial interest than confidentiality

Availability

- "The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system; i.e., a system is available if it provides services according to the system design whenever users request them."
- Turning off a computer provides confidentiality and integrity, but hurts availability...
- Denial of service attacks are direct assaults on availability

More Definitions

vulnerability An error or weakness in the design, implementation, or operation of a system

attack A means of exploiting some vulnerability in a system

threat An adversary that is motivated and capable of exploiting a vulnerability

(Definitions from *Trust in Cyberspace*)

Vulnerabilities

- The technical failing in a system
- The primary focus of most computer security classes
- If you can close the vulnerabilities, the threats don't matter
- Or do they?

Threats

- Different enemies have different abilities
- Teenage joy-hackers can't crack a modern cryptosystem
- Serious enemies can exploit the "three Bs": burglary, bribery, and blackmail
- You can't design a security system unless you know who the enemy is

Threats

Joy Hackers

- Many are "script kiddies"; some are very competent.

⇒ The scripts are very sophisticated.

- The hackers share tools more than the good guys do.

Are Joy Hackers a Problem?

- What would it cost you to rebuild a machine?
- What would your CEO say if you ended up on the front page of the NY Times?
- What if they're working for someone else?
- N.B. Their target selection has improved.

Hacking for Profit

- The hackers have allied themselves with the spammers and the phishers
- The primary motivation for most current attacks is *money*
- The market has worked — the existence of a profit motive has drawn new talent into the field
- We are seeing, in the wild, sophisticated attacks
- We're seeing less pure vandalism
- Most of today's worms and viruses are designed to turn victim computers into "bots"
- Turning off the Internet isn't profitable...

Organized and Disorganized Crime

- In many cases, hacking is just another venue for ordinary criminal activity
- The same people who hack steal also credit card numbers, launder money, etc.
- Some are even former drug dealers

Industrial Espionage

- Less than 5% of attacks are detected. Professionals who are after you won't use your machine to attack other companies, and that's how successful penetrations are usually found.
- Professionals are more likely to use non-technical means, too: social engineering, bribery, wiretaps, etc.
- Professionals tend to know what they want.

Inside Jobs

- Insiders know what you have.
- Insiders often know the weak points.
- Insiders are on the inside of your firewall.
- Etc., etc., etc.

$\Rightarrow$ What if your system administrator turns to the Dark Side?

Spies

- Governments may want your technology.
- Some governments lend tangible support to companies in their own countries.
- Spies tend to be sophisticated, well-funded, etc.
- Is cyberwarfare a threat?

Why Does This Matter?

- You have to build your defenses accordingly
- Security is fundamentally a matter of economics.
- How much security can you afford?
- How much do you need?

Assets

What Are You Protecting?

- Host-resident data?
- Bandwidth?
- CPU time?
- Knowledge of what hosts exist?

Scanning a Network


```
Host 192.168.2.1 appears to be up.
MAC Address: 00:04:E2:34:B6:CE (SMC Networks)
Host 192.168.2.79 appears to be up.
MAC Address: 00:11:11:5B:7A:CD (Intel)
Host 192.168.2.82 appears to be up.
MAC Address: 00:10:5A:0D:F6:D7 (3com)
Host 192.168.2.198 appears to be up.
MAC Address: 00:10:DC:55:89:27 (Micro-star Internati
Host 192.168.2.199 appears to be up.
MAC Address: 00:C0:4F:36:33:91 (Dell Computer)
Host 192.168.2.200 appears to be up.
MAC Address: 00:0C:41:22:CC:01 (The Linksys Group)
Host 192.168.2.251 appears to be up.
MAC Address: 00:0F:66:75:3D:75 (Cisco-Linksys)
```

Does That Matter?

- The number of computers an organization has roughly corresponds to the number of people in it
- How large is your competitor?
- (How many computers does Google have in its data centers? They won't say.)

Attacker Powers

- Note the MAC addresses in that output
- (MAC addresses often disclose the device manufacturer)
- Those can only be determined from on-LAN
- Does the attacker have that ability?

Bandwidth Attacks

- Clog your bandwidth — denial of service attack
- Use your bandwidth to attack someone else
- May not require penetrating your hosts: reflector attacks

Reflector Attack

- Find a UDP-based service, such as DNS, where the response is much larger than the query
- Send some server a small query, but forge the source address to point to your victim
- The innocent server sends a large reply to the victim, generating more bandwidth than you could, and absorbing the blame

Network Identity Attack

- Suppose you want to offer illegal content
- Hack someone else's machine, and run a server there
- They'll get blamed, not you
- (Note: the same trick works for clients doing illegal things)

Eavesdropping

- So-called "sniffer" programs can pick up traffic, especially passwords
- Done to major backbones in 1993-4.
- Today: see `http://monkey.org/~dugsong/dsniff/` for off-the-shelf eavesdropping software and more

Sniffing Credit Cards

- It's hard to pick up passwords — they're sometimes sent one character per packet
- Credit card numbers are easy: they're 15 or 16 digits, and self-checking
- It's also easy to pick up images, etc.

Vulnerabilities

The Dichotomy

- We are dealing with the host world and the network world
- We need to protect against both classes of vulnerability
- Techniques differ

Host Vulnerabilities

- Our goal: keeping the bad guy from penetrating the networked host (generally via a buggy application)
- If a penetrated application is used to break host security, it's probably an OS and application security issue
- If the application itself can be tricked into doing nasty things, it's probably a network security problem
- No, the categories aren't neat and clean

Network Vulnerabilities

- What can the attacker do?
- Where is the attacker located?
- What are you trying to protect?

Different Layers

- Each layer has its own vulnerabilities
- Link layer example: ARP-spoofing
- Network layer example: IP address forgery
- TCP example: Sequence-number guessing attack
- Application example: email-borne worms

ARP Spoofing

- ARP is used to map IP addresses into Ethernet addresss:

```
arp who-has chadash.cs.columbia.edu tell
    gg1.cs.columbia.edu
arp reply chadash.cs.columbia.edu is-at
    00:20:78:1e:1f:ef
```

- Another machine can reply; first reply generally wins:

```
00:11:50:28:b3:a8 on ath0 tried to overwrite
    arp info for 192.168.2.1 on wm0
```

Normal TCP 3-Way Handshake

A client C tries to contact a server S:

$$
\begin{aligned}
C \to S: &\quad \mathit{SYN}(\mathsf{ISN}_C) \\
S \to C: &\quad \mathit{SYN}(\mathsf{ISN}_S), \mathit{ACK}(\mathsf{ISN}_C) \\
C \to S: &\quad \mathit{ACK}(\mathsf{ISN}_S) \\
C \to S: &\quad \text{data}
\end{aligned}
$$

In older TCPs, the ISN (Initial Sequence Number) is incremented by a constant amount k after each connection and every half-second.

Sequence-Number Guessing Attack

X opens a legitimate connection to S to learn ISN_S

$$X \to S: \ \mathit{SYN}(\mathsf{ISN}_X)$$
$$S \to X: \ \mathit{SYN}(\mathsf{ISN}_S), \mathit{ACK}(\mathsf{ISN}_X)$$

X impersonates T:

$$X \to S: \ \mathit{SYN}(\mathsf{ISN}_X), \mathit{SRC} = T$$
$$S \to T: \ \mathit{SYN}(\mathsf{ISN}_S + k), \mathit{ACK}(\mathsf{ISN}_X)$$
$$X \to S: \ \mathit{ACK}(\mathsf{ISN}_S + k), \mathit{SRC} = T$$
$$X \to S: \ \mathit{ACK}(\mathsf{ISN}_S + k), \mathit{SRC} = T, \mathsf{nasty\text{-}data}$$

Complexities

- When T sees the *SYN/ACK* packet from S, it will try to respond with a *RST*
- X has to prevent this
- Original attack exploited TCP bug
- Could impersonate a dead host or use a denial of service attack to block T
- New research result: built-in firewall software prevents hosts from seeing packets for connections they didn't initiate; T will never see that packet, and hence will never send the RST...

Protecting a Network

Analysis

- What are you trying to protect?
- Against whom?
- Enumerate vulnerabilities
- Deploy protective measures

Protections

- Replace vulnerable mechanisms by strong ones
- Example: don't use address-based authentication; use cryptography
- Use filters or firewalls to limit access to important but insecure services
- Example: the CS department does not permit outside access to Windows file-sharing ports
- Use procedural mechanims as a last resort
- Example: there's no way to block ARP-spoofing, so you have to keep would-be spoofers off your LAN — the attack can't be launched remotely

Don't Forget the Human Element

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed, but they are sufficiently pervasive that we must design our protocols around their limitations."
Kaufman et al.