Title Goes Here

Introduction to Computer Security

1

The Internet in 1980

ARPANET GEOGRAPHIC MAP, OCTOBER 1980
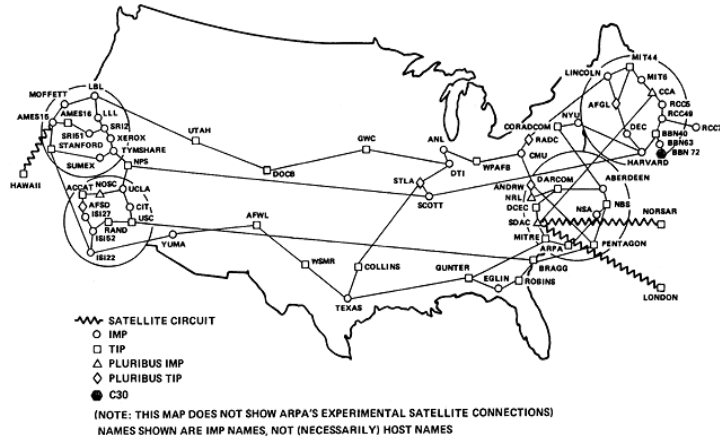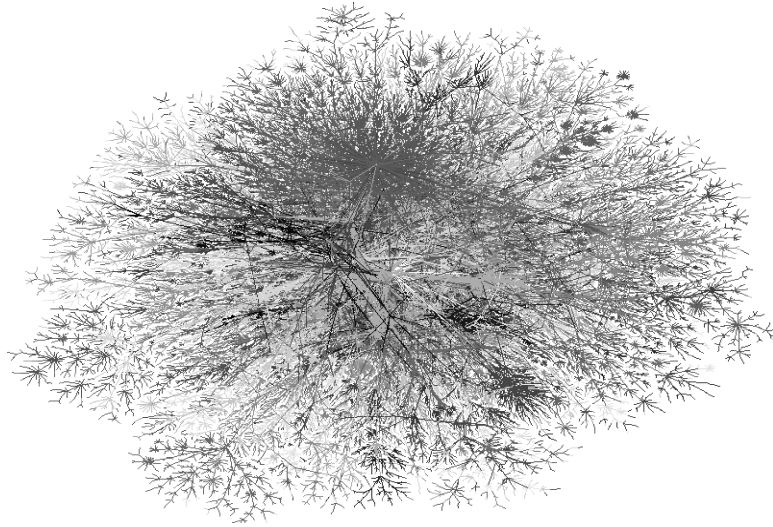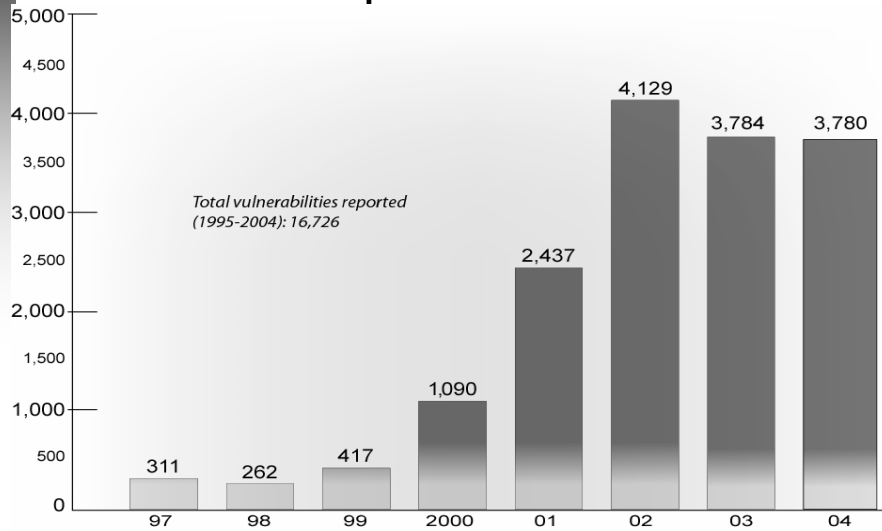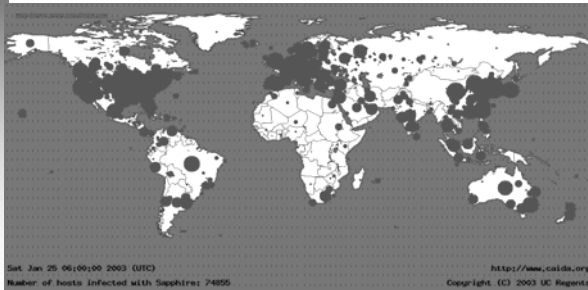
~~~ SATELLITE CIRCUIT
○ IMP
□ TIP
△ PLURIBUS IMP
◇ PLURIBUS TIP
● C30
(NOTE: THIS MAP DOES NOT SHOW ARPA'S EXPERIMENTAL SATELLITE CONNECTIONS)
NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

2

The Internet Today
[http://cm.bell-labs.com/who/ches/map/gallery/index.html]

3

Vulnerabilities Reported to CERT/CC

*Total vulnerabilities reported
(1995-2004): 16,726*

4

2

Bad Code + Big Networks = Big Problems

Geographic spread
of Sapphire worm 30
minutes after release

Source: http://www.caida.org

- CodeRed worm (Summer 2001)
  - Infected 360,000 hosts in 10 hours (CRv2), and still going …
- Sapphire/Slammer worm (Spring 2003)
  - 90% of Internet scanned in <10mins

5

IT Giveth, and IT Taketh Away

- In the US, for example, two-thirds of productivity increases from 1990-2000 are attributed to the use of IT
- At the same time, businesses are bleeding due to disruption in IT services

Melissa virus: **$1 billion** in damages (Computer Economics)	Lloyds of London put the estimate for Love Bug at **$15 billion** 3.9 million systems infected 30 days to clean up	Code Red cost **$1.2 billion** in damages and **$740 million** to clean up from the 360,000 infected servers (Reuters)	Slammer **$1 billion** in damages
1999	**2000**	**2001**	**2003**

Next: $ trillion shutdowns?

6

Hacking

■ **For profit**
  ❯ Hacker accessed Citibank computers and transferred $10M to his account
  ❯ Once caught, he admitted using passwords and codes stolen from Citibank customers to make other transfers to his accounts
  [PBS web site report on Vladimir Levin, 1994]

■ **As a business in information**
  ❯ Internet sites traffic in tens of thousands of credit-card numbers weekly
  ❯ Financial loses of over $1B/year
  ❯ Cards prices at $.40 to $5.00/card – bulk rates for hundreds or thousands
  [New York Times News Service, May 13, 2002]

7

Hacking

■ **As a business for renting infrastructure**
  ❯ Rent a pirated computer for $100/hour
  ❯ Average rate in underground markets
  ❯ Used for sending SPAM, launching DDOS attacks, …
  [Technology Review, September 24, 2004]

■ **For extortion**
  ❯ Hacker convicted of breaking into a business' computer system, stealing confidential information and threatening disclosure if $200,000 not paid
  [U.S. Dept. of Justice Press Release, July 1 2003]

■ **For identity theft**
  ❯ Hackers accessed ChoicePoint's consumer records, potentially viewing the data of about 35,000 Californians; at least one case of identity fraud
  [news.com, Feb 15, 2005]

8

Invasions of Personal Privacy

- At Harvard, transmission of electronic mail and files from the Internet were regularly recorded in a public log
  [Harvard Crimson, February 1995]
- A study of top 100 websites in June 1997 found that none met basic standards for privacy protection
  - Only 17 had explicit privacy policies
  ["Surfer beware: Personal privacy and the Internet", EPIC, June 1997]
- Reporter digs up a wealth of private information about Google CEO simply through Google searches
  ["Google balances privacy, reach", CNet News, July 14 2005]
  - Google retaliates by denying future interviews

9

And New Types of Attacks

- "Spyware" proliferating at alarming rate
  - PCs scanned by Earthlink show 30% have keystroke loggers [The Register, April 16, 2004]
  - America Online survey finds spyware on 80% of systems [IDG News, October 25, 2004]
- "Phishing" a rapidly growing problem
  - Dec. 03 – reports increase 400% over holidays
  - Feb. 04 – reports increase 50% in January
  - March 04 – reports increase 60% in February
  - April 04 – reports increase 43% in March
  - May 04 – reports increase 180% in April
  - Jan 05 – 300% increase over May 04
  [Anti phishing working group (www.antiphishing.org)]

10

5

What is Computer Security?

■ Protecting computers against misuse and interference

■ Broadly comprised of three types of properties
  ❑ <u>Confidentiality:</u> information is protected from unintended disclosure
  ❑ <u>Integrity:</u> system and data are maintained in a correct and consistent condition
  ❑ <u>Availability</u>: systems and data are usable when needed
    ❑ Also includes timeliness

■ These concepts overlap
■ These concepts are (perhaps) not all-inclusive
  ❑ Spam?
  ❑ "Non-business related" surfing?

11

Example Topics of Computer Security Research

■ Access control and authentication in distributed systems
■ Cryptography & cryptographic protocols
■ User authentication
■ Software vulnerabilities
■ Software engineering to reduce vulnerabilities
■ Firewalls
■ Network intrusion detection
■ Network DOS and defenses
■ Online privacy
■ Digital rights management

12

Access Control

- Principal makes a request for an object
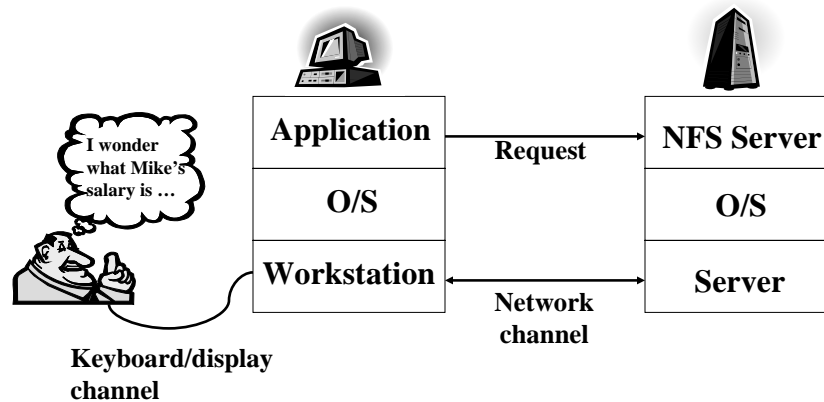- Reference monitor grants or denies the request

Principal	→ Request →	Reference Monitor	→ Yes/No
Ex: Editor	Send file	File server	
Ex: Host	Route packet	Firewall	

- Authentication: Determining who made request
- Authorization: Determining is trusted to access an object
  - The "decision" the reference monitor must make

13

Access Control: The Challenge

I wonder what Mike's salary is …

Application	Request →	NFS Server
O/S		O/S
Workstation	← Network channel →	Server

Keyboard/display channel

- Who is the request "from"?
  - The user? The workstation? The application?
  - All of the above?

14

Cryptography

- Study of techniques to communicate securely in the presence of an *adversary*
- Traditional scenario

Goal: A dedicated, private connection

Alice

Bob

Reality: Communication via an *adversary*

15

Adversary's Goals

1. **Observe what Alice and Bob are communicating**
   - Attacks on "confidentiality" or "secrecy"
2. **Observe that Alice and Bob are communicating, or how much they are communicating**
   - Called "traffic analysis"
3. **Modify communication between Alice and Bob**
   - Attacks on "integrity"
4. **Impersonate Alice to Bob, or vice versa**
5. **Deny Alice and Bob from communicating**
   - Called "denial of service"

- **Cryptography traditionally focuses on preventing (1) and detecting (3) and (4)**

16

8

Getting Around Access Controls

- Authentication and access control could be used to prevent access to resources
- Suppose we want to circumvent access controls … but how?
  - ◤ Compromise keys
  - ◤ Physically break into systems
  - ◤ Fool users
  - ◤ …
  - ◤ Commandeer a trusted client (or the reference monitor itself)
- The most common way this is done is via *buffer overflows*

17

The 10,000-foot View

- `C/C++` allows program to allocate runtime storage from two regions of memory: the *stack* and the *heap*
  - ◤ Stack-allocated data include nonstatic local variables and parameters passed by value
  - ◤ Heap-allocated data result from `malloc()`, `calloc()`, etc.
- Contiguous storage of the same data type is called *a buffer*
- A *buffer overflow* occurs when more data is written to a buffer than it can hold

18

What's the Problem?

- Reading or writing past the end of a buffer can cause a variety of behaviors
  - Program might continue with no noticeable problem
  - Program might fail completely
  - Program might do something unanticipated

- What happens depends on several things
  - What data (if any) are overwritten
  - Whether the program tries to read any overwritten data
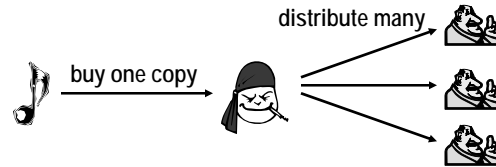 - What data replaces the overwritten data

19

Is This a Big Deal?

- Cause of numerous CERT advisories since 1997

- Example
  - A boolean flag placed after a buffer
  - Flag indicates whether user can access sensitive file
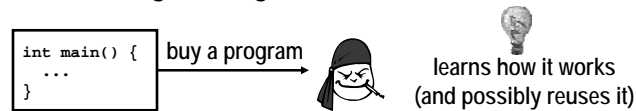 - Overwriting buffer can then reset the flag

- Commonly, buffer overflows used to get an interactive shell on the machine, often running as `root`
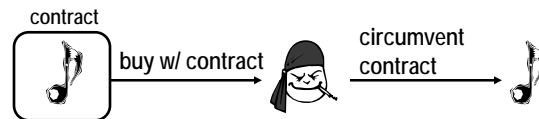
20

Digital Rights Management: Threats

■ Piracy

distribute many

buy one copy

■ Reverse engineering

```
int main() {
   ...
}
```
buy a program

learns how it works
(and possibly reuses it)

■ Tampering

contract

buy w/ contract

circumvent
contract

21

Digital Rights Management: Defenses

■ Watermarking
   ❯ content is distributed with a secret embedded within it
   ❯ knowledge of secret permits ownership to be demonstrated or purchaser to be traced
   ❯ defends against piracy attacks

■ Tamper-proofing
   ❯ any change to code makes the program non-functional
   ❯ defends against tampering attacks

■ Obfuscation
   ❯ transforms program into an equivalent one that is unintelligible
   ❯ defends against reverse engineering

22

11

Security Courses in ECE

- 18-487: Introduction to Computer & Network Security and Applied Cryptography
  - New offering in Spring 2006

- Regular fall offerings
  - 18-630: Introduction to Security and Policy
  - 18-730: Introduction to Computer Security
  - 18-732: Secure Software Systems
- Regular spring offerings
  - 18-731: Network Security
  - 18-733: Applied Cryptography

23

The Internet Worm (Nov 2, 1988)

- Probably the most famous exploit ever unleashed
- Program was released that iteratively spread itself across Berkeley Unix systems, and crippled those it infected
- Exploited three different vulnerabilities
  - `debug` option of `sendmail`
  - `gets`, used in the implementation of `finger`
  - Remote logins exploiting `.rhost` files

- Perpetrator was convicted under the Computer Fraud and Abuse Act of 1986
- Largely the cause for the creation of the Computer Emergency Response Team (CERT)

24

A Cautionary Tale

- Perpetrator was Robert Morris, a Cornell CS graduate student at the time
- Morris intended the worm as a "benign" experiment
  - The worm's propagating behavior was intended
  - The worm's destructive behavior was not

- Lesson: DO NOT try hacking experiments—even "benign" ones—on public networks
  - Most such activities are illegal

25

Computer Fraud and Abuse Act (1986)

- Major provisions
  - Illegal to gain unauthorized access of a federal interest computer with the intention to commit fraudulent theft.
  - Illegal to cause "malicious damage" to a federal interest computer, which involves altering information in, or preventing the use of, that computer.
  - Illegal to traffic in computer passwords with the intent to commit fraud that affects interstate commerce.
- A "federal interest computer" is one "used by or for a financial institution or the United States Government"
  - Includes computers of federally insured banks, thrifts and credit unions; registered securities brokers; members of the Federal Home Loan Bank System, the Farm Credit Administration, and the Federal Reserve System

26

Carnegie Mellon

PATRIOT Act (2001)

- Does lots of things, but in particular it expands government's authority to prosecute hacking and denial of service attacks under Computer Fraud and Abuse Act (CFAA)
- Adds an "attempt to commit an offense" to the list of illegal activities with the same penalties as an offense.
- The law now applies if the damage is done to computers outside the US that affect US Interstate commerce.
- Increases penalties for violations of the statute.
- "Loss" under the statute now expressly includes time spent responding and assessing damage, restoring data, program, system or information, any revenue lost, cost incurred or other consequential damages.

27

Carnegie Mellon

Electronic Communications Privacy Act (1986)

- Extends "Title III" privacy protections to pertain to electronic communication technologies
  - radio paging devices, electronic mail, cellular telephones, private communication carriers, and computer transmissions
- Relates to both government surveillance and "recreational eavesdropping" by private parties.
  - Protections from government surveillance largely eroded by the PATRIOT act
- Also identified specific situations and types of transmissions that would not be protected
  - Most notably an employer's monitoring of employee electronic mail on the employer's system.

28

Digital Millenium Copyright Act

- Major provisions
  - Illegal to bypass technical measures used by copyright owners to protect access to their works.
  - Illegal to manufacture or distribute technologies primarily designed or produced to circumvent technical measures used by copyright owners to protect their works.
  - Illegal to remove or alter copyright management information from digital copies of copyrighted works.

- Ex: Universal City Studios, Inc. v. Reimerdes in August 2000
  - Universal sued 2600 Magazine and its publisher because 2600 posted a copy of a computer program "DeCSS" that bypasses the Content Scrambling System (CSS) used to protect commercially distributed DVD movies.

29

U.S. Export Controls on Encryption

- Encryption software or hardware cannot be sent to "terrorist supporting states"

- Export of most encryption software/hardware requires prior government review and/or reporting

- Export of source code can incur further requirements

30