# Attacks and Malicious code

# Attacks and Malicious Code

- Denial of Service (DoS)
  - SYN flood
  - Smurf
  - Distributed DoS
- Spoofing
  - IP spoofing
  - ARP poisoning
  - Web spoofing
  - DNS spoofing

# Attacks and Malicious Code

- Man-in-the-middle
- Replays
- TCP Session hijacking
- Social Engineering
  - Dumpster diving
  - Online attacks
- Web defacement

# Attacks and Malicious Code

- Attacks on encrypted data
  - Weak keys
  - Birthday attack
  - Dictionary attack
- Software exploitation
  - Malicious software (virus and worm)
  - Back door
  - Logic bombs
- Countermeasures

# Why we need security?

Good news: Your employees and partners can now access your critical business information

Bad news: Your employees and partners can now access your critical business information

# Why we need security?

**FBI:**

- 40% of security loss due to insider information leak
- Loss due to insider information leak has increased on average 49% per year for the last 5 years

## Pricewaterhouse-Coopers:

- Average loss of $50 M per incident due to information theft
- In 2000, $300 B loss due to IP-theft alone in Fortune 300 companies

# Some Statistics

Financial loss reported due to attacks ~ $500 million
Not every one reports loss due to attacks

| Type of attack | Percentage |
|---|---|
| Virus | 85% |
| Denial of Service | 40% |
| Intrusion | 40% |

Internet as source of attack: 74%

# Main issues

- Security never stops
- New threats constantly emerge
- Security is concerned with risk management
- Existing security products are weakly integrated
- Lack of well understood security policy
- Too much reliance on technology alone for security

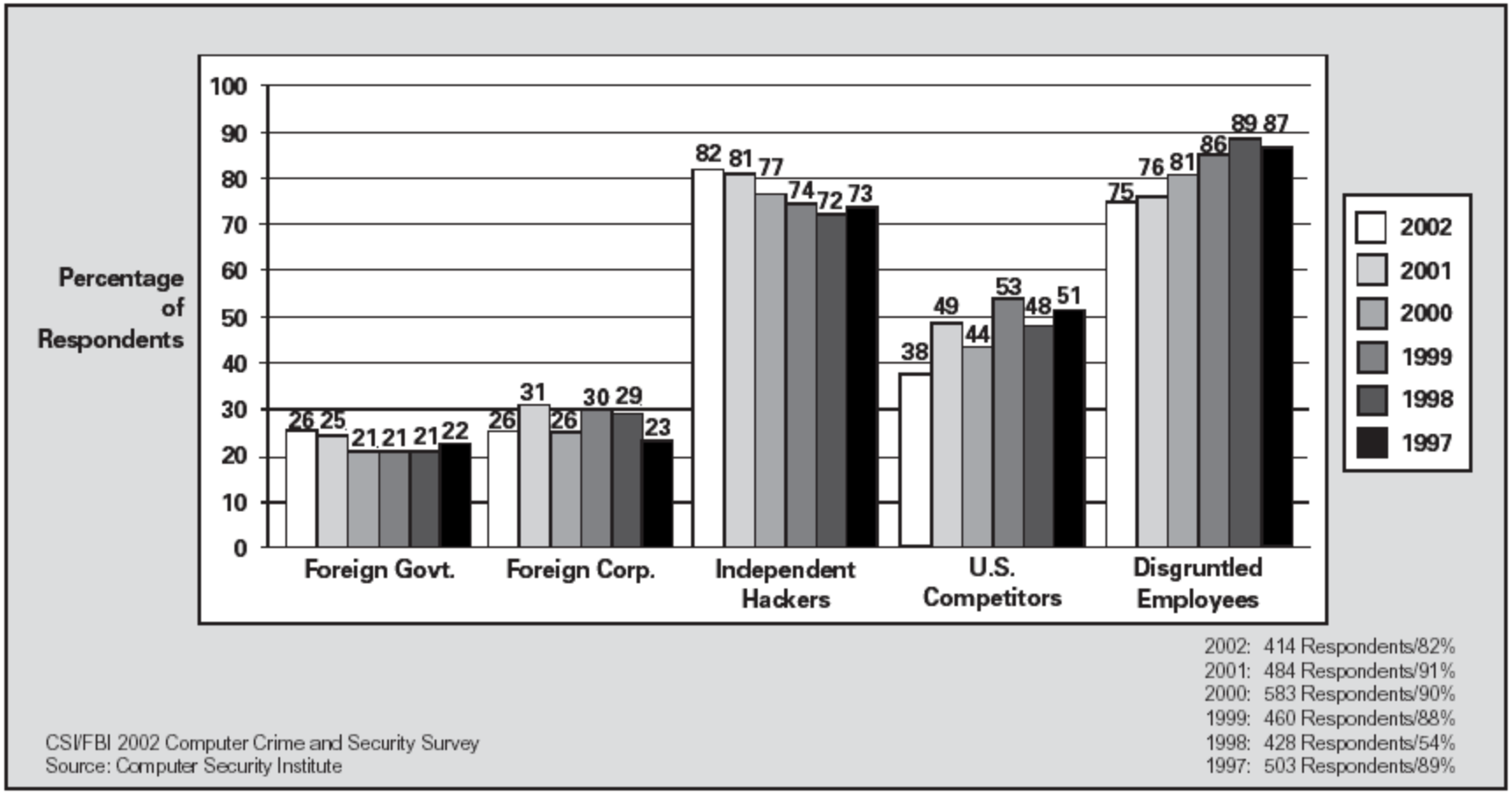
# Does everyone know your security policy?

- Most of the time the answer is NO
- Customer thinks:

  What is explicitly not prohibited is permitted
- Organization thinks:

  What is explicitly not permitted is prohibited

# Likely Sources of Attack



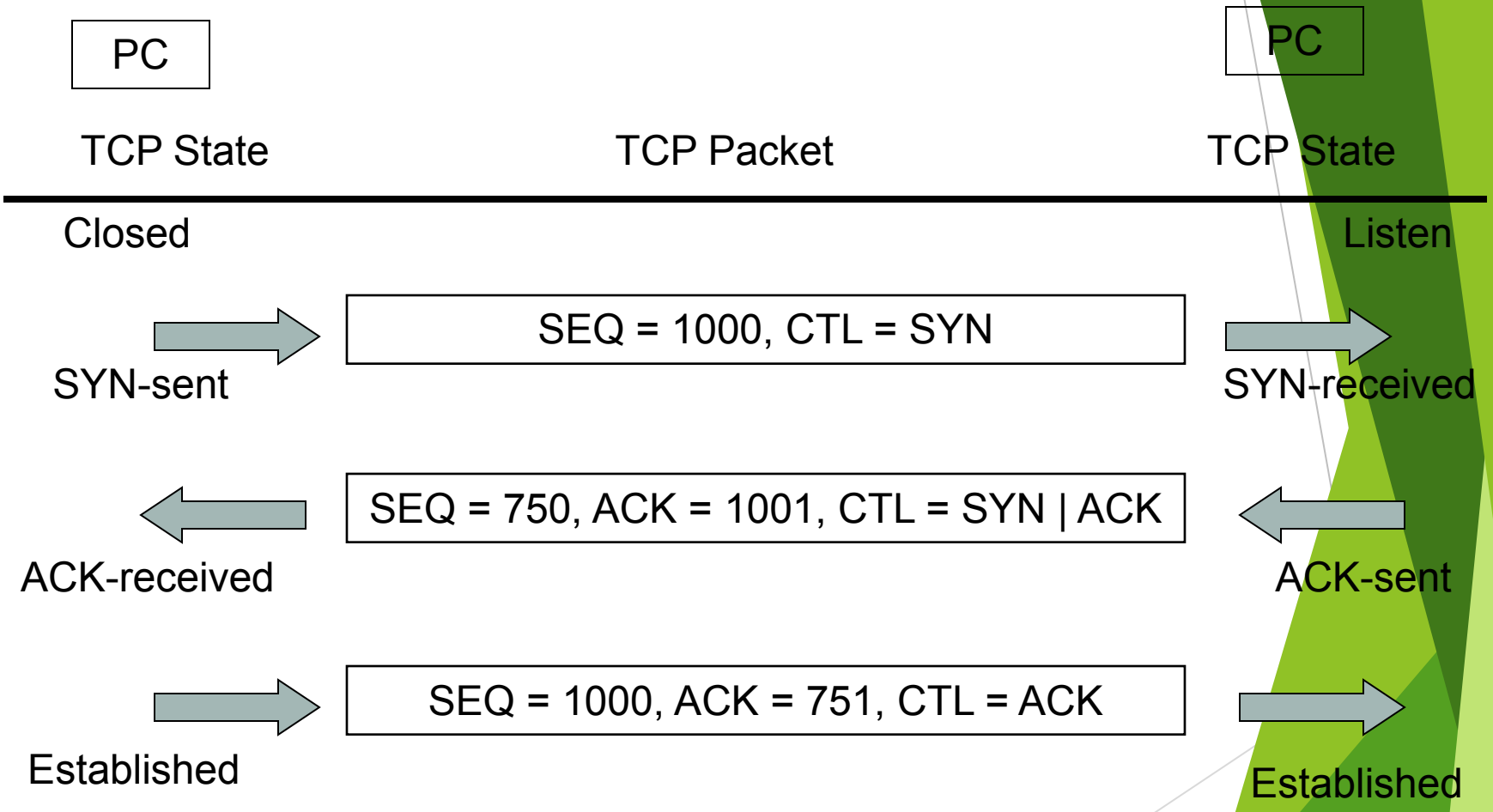

2002: 414 Respondents/82%
2001: 484 Respondents/91%
2000: 583 Respondents/90%
1999: 460 Respondents/88%
1998: 428 Respondents/54%
1997: 503 Respondents/89%

CSI/FBI 2002 Computer Crime and Security Survey
Source: Computer Security Institute

# Common Attacks

- SYN flooding attack
  - This exploits how the 3-way handshake of TCP services for opening a session works.
  - SYN packets are sent to the target node with incomplete source IP addresses
  - The node under attack sends an ACK packet and waits for response
  - Since the request has not been processed, it takes up memory
  - Many such SYN packets clog the system and take up memory
  - Eventually the attacked node is unable to process any requests as it runs out of memory storage space

# TCP 3-way Handshake



# Land attack

- Similar to SYN attack
- Uses the target address as the source address as well
- Causes an infinite loop under the SYN/ACK process

# Smurf attack

- A brute force DOS attack and thus a non-OS specific attack
- A large number of PING requests with spoofed IP addresses are generated from within the target network
- Each ping request is broadcast, resulting in a large number of responses from all nodes on the network
- Clogs the network and prevents legitimate requests from being processed

# Port scanning

- Scanning the source and destination ports for both TCP and UDP for data capture
- TCP ports are commonly monitored but UDP ports are not

# Ping of death

- The hacker sends an illegal echo packet with more bytes than allowed, causing the data to be fragmented.  This causes the data to be stored causing buffer overflows, kernel dumps, and crashes
- This was made possible by some Windows OSs allowing non-standard ICMP (Internet Control Message Protocol) messages to be generated
- Maximum ICMP packet size is 65507 bytes. Any echo packet exceeding this size will be fragmented by the sender and the receiver will try to reconstitute the packet, when overflow would occur

# UDP-flood attack

- Denial of service variant
- Connects the target machine's chargen and echo services to create an infinite loop between two or more UDP services
- Connectivity to the network is sufficient, no network account required for this attack

# Distributed Denial of Service

- Hackers post malicious software on the web
- Script kiddies (people who do not fully understand the code) launch the attacks
- In DDoS, the hacker (also known as Black hat) identifies computers with weak security as handlers. The software in the handlers scan for hosts to be used as agents or zombies. Hundreds of thousands of zombies simultaneously launch the DoS attack in a distributed manner.

# IP Spoofing

- Exploits trust relationships between routers
- This is a difficult attack to launch since the communication set up is based on an initial sequence number for packets. Systems no longer use numbers sequentially. Identifying the algorithm used for numbering packets during set up is important.

# ARP Poisoning

- ARP = Address Resolution Protocol
- ARP is used by routers extensively to find the destination node. Routers have IP addresses (32-bits). In order to deliver the packet to the destination node, the router broadcasts the IP address of the destination and obtains the MAC address (48-bits).

# ARP Poisoning

- Hosts store the IP-to-MAC address mapping in the ARP table. ARP Poisoning means that the ARP communication is intercepted by redirection from a router.
- Example:
  - Assume router's IP is 10.1.1.0
  - Host's IP is 10.1.1.1
  - Malicious host with IP 10.1.1.2 spoofs 10.1.1.1 and replies to requests from 10.1.1.0 with its MAC address
  - From this point on all packets meant for 10.1.1.1 is routed to 10.1.1.2 because the router has the MAC address of 10.1.1.2 in its routing table

# ARP Poisoning

- ARP Poisoning tools are:
  - ARPoison
  - Ettercap
  - Parasite

# Web Spoofing

- In this attack the malicious site pretends to be authentic
- It is a form of man-in-the-middle attack
- This is accomplished by accessing the victim website and putting a link to the malicious site on a legitimate name. For example, www.nytimes.com could be linked to www.hackersite.com but the user would not be aware of this unless they pay attention to the actual site linked.

# DNS Spoofing

- This is similar to web spoofing
- DNS server could be a simple machine placed behind a firewall
- Usually it is isolated from the rest of the nodes in functionality
- Hacker gets access to the DNS server and changes in the lookup table the mapping. For example, **www.nytimes.com** is supposed to point to 199.239.136.200. The hacker could redirect it to his web server instead.

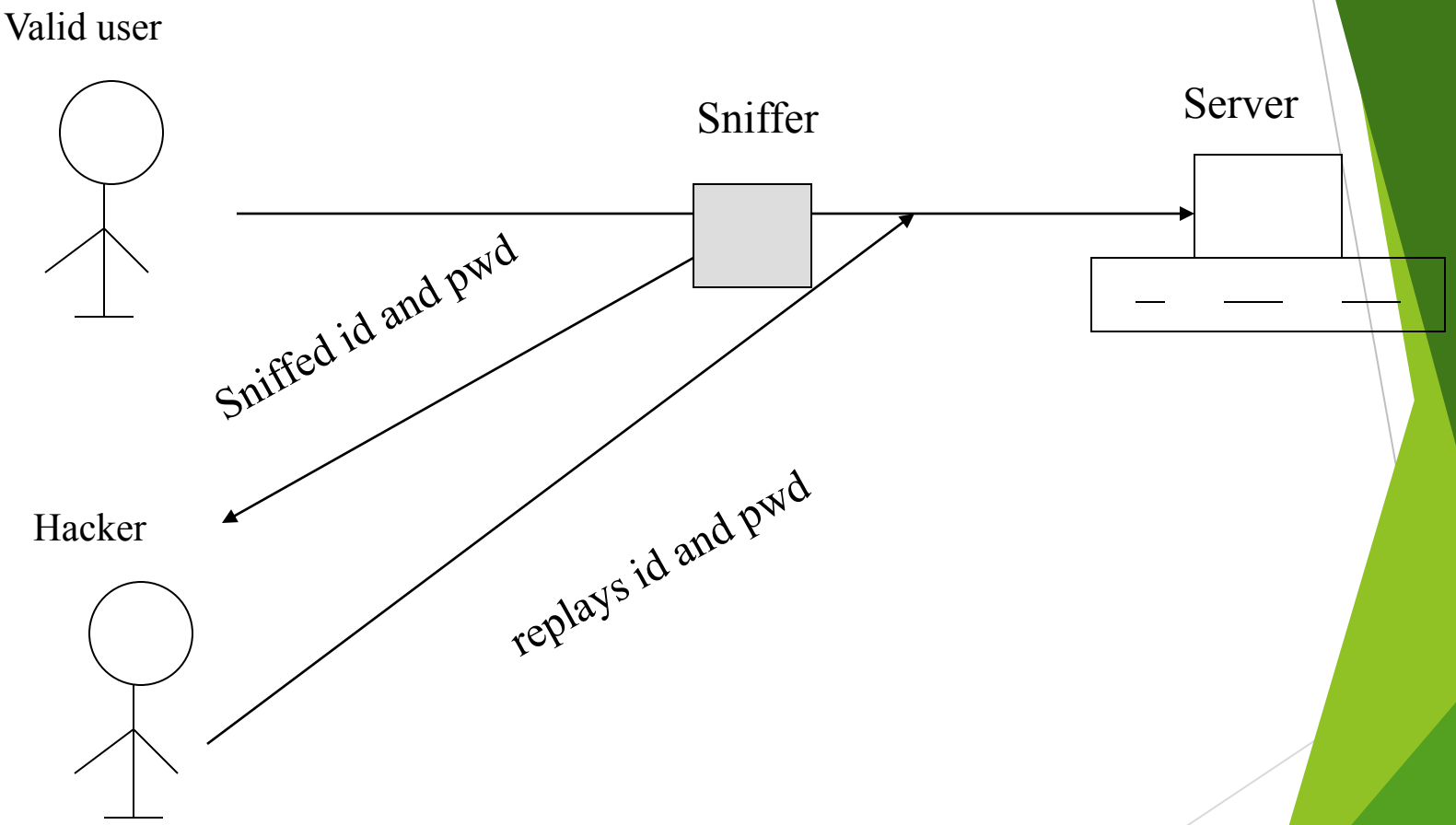
# Replays

- Replay involves capturing traffic while in transit and use that to gain access to systems.
- Example:
  - Hacker sniffs login information of a valid user
  - Even if the information is encrypted, the hacker replays the login information to fool the system and gains access

# Replays

- A sniffer is a program that intercepts and reads traffic on the network
- Sniffers work when the NIC is set to communicate in promiscuous mode

# Replay Attack Diagram



# TCP Session Hijacking

- This means that the hacker has directed traffic to his server instead of a trusted server that the victim is assuming
- To hijack a session, the hacker ARP poisons the router to route all traffic to his computer before it is delivered to the victim
- See Figure 3-14 (p. 68) in the book for details of IP and MAC addresses

# Social Engineering

- It is hacker-speak to convince others to share confidential information with them
- "'Hi, I'm your AT&T rep, I'm stuck on a pole. I need you to punch a bunch of buttons for me.'"
- Pop-up windows can be installed by hackers to look like part of the network and request that the user reenter the username and password to fix some sort of problem

# Social engineering

- “Hello, can I speak with Tom Smith from R&D please?”
- “I'm sorry, he'll be on vacation until next Monday”
- “OK, may I know who's in charge until he gets back?”
- “Bob Jones”
- Hacker calls another employee Michael in R&D and says,

  “By the way Michael, just before Tom Smith went on vacation, he asked me to review the new design. I talked with Bob Jones and he advised me to get a copy of the new design. Could you fax that to me at 111-222-3333? Thanks”

# Social Engineering

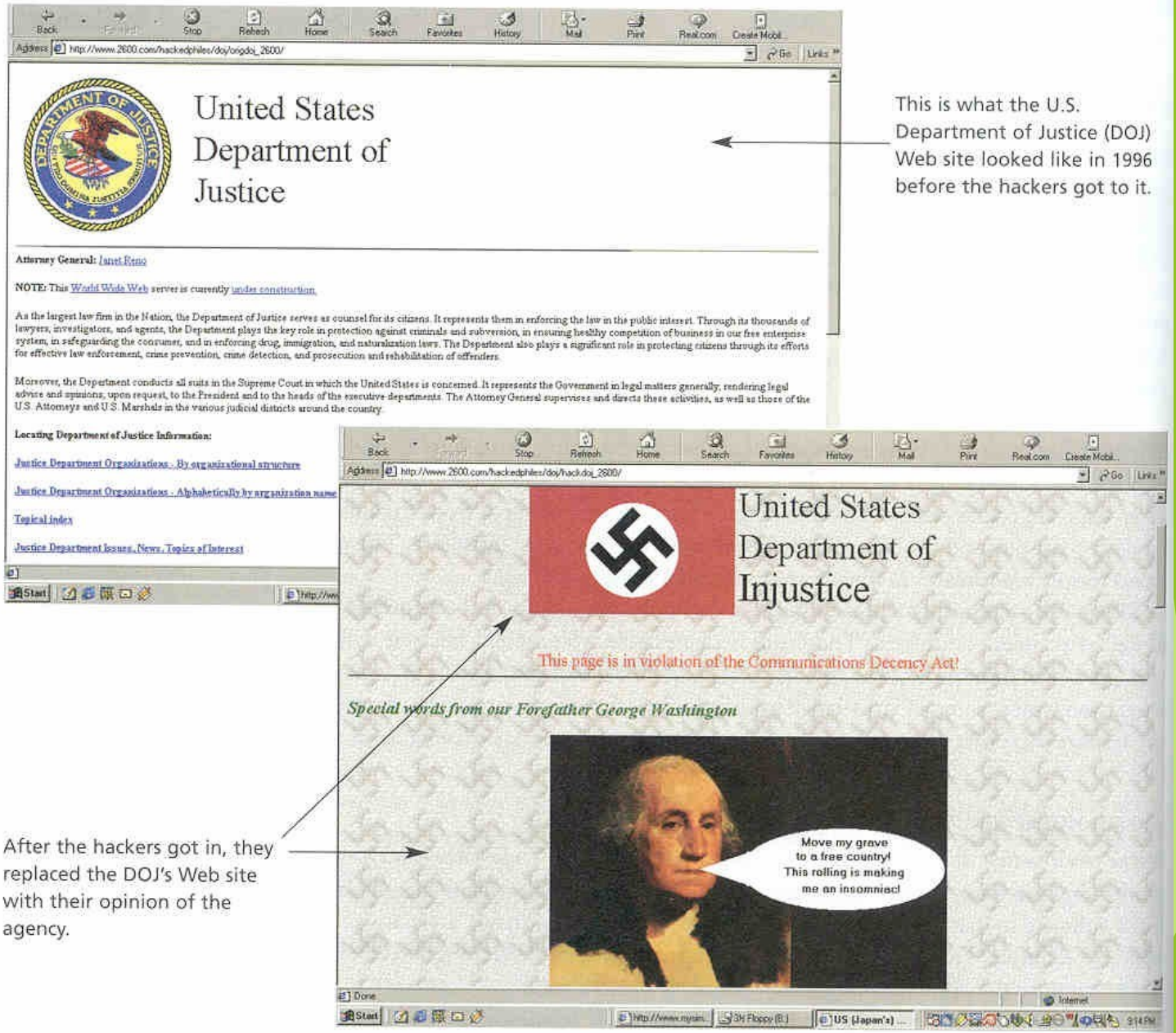
- Dumpster diving is also part of social engineering
- This means that any organization that does not dispose of sensitive documents such as organizational structure and manuals in a proper way could be exposing their system to people who recover documents from dumpsters
- Dumpster could yield office

# Website Defacement

| | |
|---|---|
| China & Taiwan combined | 2,653 |
| US dot com sites | 8,736 |
| Worldwide total | 30,388 |

| Country | Percent increase in 2001 |
|---|---|
| United Kingdom | 378% |
| Pakistan | 300% |
| Israel | 220% |
| India | 205% |
| US .mil sites | 128% |
| US .gov sites | 37% |

Source: MIS for The InfoAge: Haag



# Dictionary attack

- Has an idea of the message
- Has the hashed value from the message
- Exhaustive search to find the original corresponding to the hash
- Credit cards use 16 digits
  - $2^{55} = 10^{16}$
  - This is within the realm of possibility for today's computers to do an exhaustive search
- Does not involve any encryption

# Birthday attack

- A variation of brute-force attack
- Studies have shown that if 23 people are in a room, the probability is over 50% that two people have the same birthday
- The similarity here is, knowing one value can you find the matching value

# Software Exploitation

- Malicious software, also known as malware, includes worms, viruses, and Trojan horses
- How do these propagate?
  - Virus is meant to replicate itself into executables (e.g., Melissa)
  - Worm is meant to propagate itself across the network (e.g., Nimda, Code Red)
  - Trojan horse is meant to entice the unsuspecting user to execute a worm

# Virus

- Virus self-replicates
- Early viruses (1980s to mid-90s) were placed on boot sector of hard and floppy drives as they would not show up in the directory listing
- Second type of virus is known as 'parasitic virus.' This was prevalent in mid-90s.
- Parasitic virus attaches to files and infect files of type exe, sys, com,

# Virus

- Third virus type is ‘multipartite virus’. This infected both boot sector and files. This was also common in the mid-90s.
- Current virus type is known as ‘macro virus.’ These are application specific as opposed to operating system specific. They propagate rapidly through email. Most macro viruses are written in VB Script and they exploit

# Virus

- Current information on viruses can be obtained from CERT, McAfee, Symantec, and Computer Associates
- Major viruses:
  - Melissa March 1999
  - Nimda September 2001

# Worms

- Worm is a self-contained program that tries to exploit buffer overflows and remotely attack a victim's computer
- Code Red and Code Red II are two of the well-known worms
- There is not much of a distinction made between viruses and worms

# Countermeasures

- For SYN-flood attack:
  - Firewall can withhold or insert packets into the data stream, thus providing one means from letting the SYN packets get through
  - Firewall responds immediately to the SYN with its ACK sent to the spoofed address. This way the inquiry is not in the open queue taking up space. Legitimate addresses would respond immediately and they could be forwarded by the firewall to the internal systems. SYN-flood attack

# Countermeasures

- For Smurf attack:
  - Routers should be configured to drop ICMP messages from outside the network with a destination of an internal broadcast or multicast
  - Newer Oss for routers and workstations have protection for known smurf attacks

# Countermeasures

- For IP Spoofing attack:
  - This is a difficult attack to start with for the hacker
  - Hacker should be able to guess correctly the Initial Sequence Number that the spoofed IP would generate
  - To prevent IP spoofing, disable source routing on all internal routers
  - Filter entering packets with a source address of the local network

# Countermeasures

- For Man in the middle attack:
  - Routers should be configured to ignore ICMP redirect packets
- Intrusion Detection System (IDS) is a software that can scan traffic in real time and detect anomalies
- Cisco, Computer Associates, Secure Works are some of the companies that provide IDS software
- Availability of IDS is a requirement in the medical and financial industry for the business to get its license
- The industry is now moving towards an Intrusion Prevention System (IPS) as opposed to an IDS

# Countermeasures

- For Ping of death attack:
  - Prohibit creation of ICMP packets of invalid size
- For Denial of Service attack:
  - Firewalls and routers at network boundaries can use filters to prevent spoofed packets from leaving the network
  - Filter incoming packets with a broadcast address
  - Turning off direct broadcasts on all internal routers

# References


- Network Security: A hacker's perspective by A. Fadia, Course Technology, OH, 2003
- Network Security Fundamentals by P. Campbell, B. Calvert, S. Boswell, Course Technology, OH, 2003
- Cryptography and Network Security, 2nd edition by W. Stallings, Prentice Hall, NJ, 1999
- Web Security Basics by S. Bhasin, Course Technology, OH, 2003
- Principles of Information Security by M. Whitman, H. Mattord, Course Technology, OH, 2003

# References

- You can find a collection of archived defacements of websites at: http://www.attrition.org/security/commentary/
- Trends in Denial of Service Attack Technology

  http://www.cert.org/archive/pdf/DoS_trends.pdf
- Managing the Threat of Denial-of-Service Attacks

  http://www.cert.org/archive/pdf/Managing_DoS.pdf
- A good source for understanding how DDoS

# References


- http://vil.nai.com/VIL/ This link from Network Associates has the library of all viruses known
- http://securityresponse.symantec.com/avcenter/vinfodb.html This link from Symantec has a database that contains information about the latest viruses
- http://www3.ca.com/virusinfo/browse.aspx This link from Computer

# References


- http://www.trendmicro.com/vinfo/virusencyclo/ This link from Trend Micro has several pull down item types for different types of viruses. This is a searchable list of viruses by name or by virus type.

# Security Scenario to Solve

1. Intrusion Detection Systems enable the organization to see in real time the types of data traffic on the network and try to take corrective action. As a network associate you are given the responsibility to examine the types of IDS and IPS systems that are available for implementation. Give a summary of the various types of these systems, including cost, functionality, ease of use, etc. In this context find out what industries (e.g., medical) require the presence of an IDS for their accreditation