Security

1

Data security
Hacker resistance
Fault Tolerance
Intrusion detection and control

Secure Server (one of the best marketing scams I know)

Policies …

2

Is there a problem?

3

See: http://www.cert.org

(Computer emergency response team)

Number of incidents reported
1988-1989

Year	1988	1989
Incidents	6	132

1990-1999

Year	1990	1991	1992	1993	1994	1995	1996	1997	1998	1999
Incidents	252	406	773	1,334	2,340	2,412	2,573	2,134	3,734	9,859

2000-2003

Year	2000	2001	2002	1Q-3Q 2003
Incidents	21,756	52,658	82,094	114,855

4

From Julia H. Allen (CERT; see http://www.cert.org/archive/ppt/NCISSE.ppt)

The Problem - in the Large

- 85% of respondents to Computer Security Institute/FBI 2001 survey reported security breaches (70%, 2000; 62% 1999)*
  - 186 organizations (35%) able to quantify financial loss reported $377.8M (273 organizations [51%], $265.6M in 2000 survey)
    - theft of proprietary information and financial fraud most serious
  - 70% cited their Internet connection as a frequent point of attack (59% in 2000 survey)

*Computer Crime and Security Survey, Computer Security Institute and the FBI, 2001, http://www.gocsi.com/prelea_000321.htm

5

Royal Canadian Mounted Police / Gendarmerie royale du Canada

RCMP Integrated Technology Crime Unit:

- Investigation of Computer Crime
- Assistance of other units regarding computer technology

This unit has a huge mandate including

- Computer forensic analysis
- Education
- Advice
- Investigation into criminal activity
- R&D
- Partnership with Universities, Companies, …

"Major NS companies have been victimized"

"Fraud on the internet will reach 15.5 Billion by 2005; a tenfold jump in 5 years"

6

IFCC
Internet Fraud Complaint Center

http://www1.ifccfbi.gov

The Internet Fraud Complaint Center (IFCC) is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).

Table 1: Amount Lost by Fraud Type for Individuals Reporting Monetary Loss

Complaint Type	*% of Complainants Who Reported Dollar Loss*	*Average (median) $ Loss per Typical Complaint*
Auction Fraud	87	$320
Non-delivery (mdse and payment)	82	$176
Credit/debit Card Fraud	62	$120
Investment Fraud	75	$570
Business Fraud	75	$220
Confidence Fraud	58	$1,000
Identity Theft	15	$2,000
Check Fraud	56	$1,100
*Nigerian letter Fraud**	< 1	$3,864
Communications Fraud	36	$174

* Of 16,164 complaints, 74 individuals lost money totaling $1.6 million

From 2002 report

7

Carnegie Mellon
Software Engineering Institute

CERT
Coordination Center

Will Unpatched Hosts be Discovered? (1)

- San Diego Supercomputer Center conducted an experiment
- Red Hat Linux 5.2 with no security patches installed on machine
- monitoring established to record traffic to and from host
- host not otherwise used by staff

See: http://worm.sdsc.edu

91

From Julia H. Allen (CERT; see http://www.cert.org/archive/ppt/NCISSE.ppt)

8

Carnegie Mellon Software Engineering Institute

CERT Coordination Center

Will Unpatched Hosts be Discovered? (2)

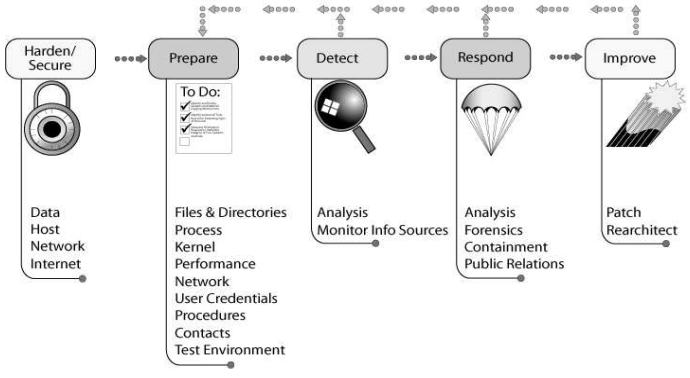
- 8 hours from install
  - probed for Solaris RPC vul, not compromised
- 21 days from install
  - 20 exploits tried for vuls including POP, IMAP, telnet, RPC, and mountd
  - exploit attempts failed because they were exploits for Red Hat 6.x
- about 40 days from install
  - POP server vul compromised
  - wipes some system logs
  - installs rootkit and sniffer

92

9

From Julia H. Allen (CERT; see http://www.cert.org/archive/ppt/NCISSE.ppt)

Security Practices Structure



10

Computer and Network Security includes

- Confidentiality (secrecy)
- Accuracy (integrity)
- Availability

11

Privacy

- Personal Information
- Private Information
- Personally identifiable information
- Anonymized information
- Aggregated information

12

It is easy to record some user information on the web
(often without your knowledge)

- Log files (web server, ISP accounting, …)
- Databases
- Cookies
- Web bugs
- Helper applications (e.g. RealJukeBox)

13

Web server log files

- All accesses to web pages create an entry in the web server's log files
- The access log records the IP address of the visitor, the time of day, the exact URL visited, plus more!
- For high-speed always-on internet users, the IP address maps to your individual machine
- For dial-up accounts, the IP address is assigned temporarily, but combining the server log file with the records of the ISP will uniquely identify your account as having accessed the pages

14

Referrer log files

- If the web server has activated their referrer log file, a record of the page you accessed immediately before the page you are accessing is also recorded on the server
- This information is typically used to determine the start of a session on a server
- By examining where you were immediately before you went to a site, the site administrator knows potentially private information about you
- Some sites use the GET method for forms, which places the field information in the URL – traveling to a new site can cause this potentially confidential information to be placed in the new site's referrer log

15

Cookies

- Used to allow a web server to track a client across multiple http requests (Allows applications such as "shopping cart" to store a session ID in a cookie)
- Once a cookie has been received from a site, the web browser will send the contents of the cookie with every request to that same site
- Cookies are kept in the browser's memory, and persistent cookies are written to a file on the user's hard drive. Cookies which are not persistent are lost when the browser application is quit. Persistent cookies have an expiry date, and can maintain state for the server on the client's hard drive for an arbitrary length of time
- Persistent cookies are good for storing a user's preferences, so that they don't have to be manually set on every visit
- Cookies can be used to track a user's movements within a web site, and also across web sites, thus violating privacy and eliminating anonymity on the web
- Doubleclick, for example, has gif advertisements on over 100,000 web sites, and can track a user's surfing across all of these sites

16

Web bugs

- Invisible graphics is placed in a website or HTML email
- with a link to a server. This can be used to track user information
- Similar to cookies but even across web servers

17

Anonymizers

- An anonymizing web server accepts requests from users and forwards the requests as if they were from the server itself, then replies to the user's request with the returned document
- This type of server is easy to set up, and could be set up for a number of reasons
- The individual running the server is concerned about user privacy, and sets up the system to help users remain anonymous
- The server displays advertisements with the proxied pages, making it a viable business proposition
- The server is run by someone who wants to track the web surfing of people who wish not to be tracked
- Essentially, if you use an anonymizing server, you have to trust that whoever is running that server will not track your surfing

18

Vulnerabilities in Browsers

- Bugs
  - Browser are complex applications, and can have security bugs
  - When bugs are identified, companies are typically quick to release patches, but not everyone downloads the patches or upgrade to the latest version
- Helper Applications
  - To complicate matters, additional functionality is added to browsers through the use of “helper apps”
  - Many applications provide complete access to a machine’s resources through built-in scripting languages, such as Microsoft Word’s Visual Basic scripting language, and should never be configured as helper apps
- PlugIns
  - PlugIns are really glorified helper apps that execute within the browser’s context space

19

Vulnerabilities in Browsers (continued)

- Java
  - Uses the concept of a “sandbox” to restrict a downloaded applet’s access to the computer’s resources
  - Security is effected through the operations of the SecurityManager class, the Class Loader, and the Bytecode Verifier
  - The definition of “valid java code” is “bytecode that passes the Bytecode Verifier” – sort of a circular definition, with no formal theory since the verifier consists of some ad-hoc checks
  - Basically insecure, as has been repeatedly proven over the years (see http://www.cert.org/advisories/CA-2000-15.html for the latest example)
- JavaScript
  - JavaScript is more secure, as there are no primitives allowing access to most system resources
  - JavaScript can, however, easily be used for denial of service attacks

20

Vulnerabilities in Browsers (continued)

- ActiveX
  - MicroSoft's answer to Java, but is really more like plugins than Java
  - Allows "controls" to automatically download and install arbitrary code to temporarily implement functionality on a web page
  - Using "authenticode", provides proof of authorship
  - Since there is no "sandbox" concept, the ActiveX control is capable of anything
  - In the event malicious controls are signed, the signor's certificate is revoked
- Authenticode (or other code signing systems)
  - Problem – how do we know the control is malicious? (no audit trail)
  - What recourse do we have upon encountering a malicious control?

21

Attacks on the end user

- Data Driven Attacks
  - Data driven attacks typically involve exploiting bugs in programs by supplying unexpected parameters
  - Most common approach involves overflowing a buffer, causing the program to crash with part of the overflow data residing on the execution stack, which allows arbitrary code to be executed
- Social Engineering Attacks
  - Attacker tricks the user into providing information or taking some inappropriate action
  - Example - a javascript program displays a window which looks like a dial-up window, and prompts the user for their username and password
  - Example – a javascript program opens a window which fills the screen, has no borders, has a black background, and displays the familiar message for Win95 that "it is now safe to turn off your computer". If the user hits the power button, they may corrupt Win95.

22

Attacks on the end user (cont.)

- Denial of Service attacks
  - Simple javascript program can repeatedly call the “Alert” function in an infinite loop, so that the user can’t shut down the browser
  - An html page containing 1000 nested tables will crash Netscape, as it tries its best to perform layout on all 1000 tables
  - A javascript can repeatedly open its own page in a new window, causing enough windows to open that memory is exhausted an the application fails or the machine crashes
- Spoofing Attacks
  - Decisions to download code or enter private information are typically based on the level of trust the user has in a site
  - Spoofing attacks are a type of social engineering attack, where a javascript window makes it appear to the user that they are on a trusted site or interacting with their local system.

23

Host Security

- Policy
- Password sniffing
- Token-based authentication (SecurID)
- Logging
- Snapshots (tripwire)
- Intrusion detection systems
- Backups
- Minimizing services to minimize risk

24

Web Site Security

- Host-based restrictions
  - (IP address or DNS name)
- Identity-based access control
  - Passwords
  - Cookies
- Using <Limit> blocks
  - htaccess

25

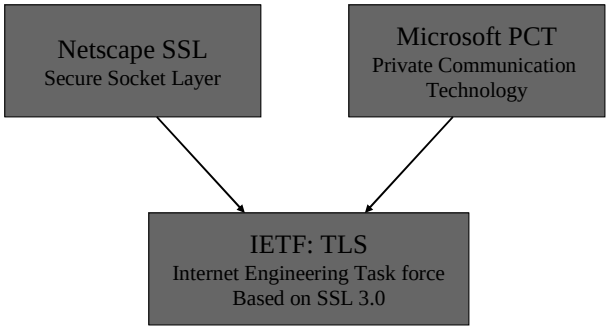
What is SSL/TSL?

- Secure Socket Layer/Transport Layer Security
- Runs commonly on top of TCP/IP
- A protocol that implements
  - privacy against eavesdroppers through encryption of messages
  - message integrity trough hash function
  - authentication through digital signatures
- e.g., connect to https, ssmtp, spop3 (each has a unique port number)

26

New standard for secure communication over the internet

January 1999: Draft version 1.0 (http://www.ietf.org)



Goals:

- `Cryptographic security' (including privacy and authentication
- Interoperability
- Extensibility
- Relative efficiency

27

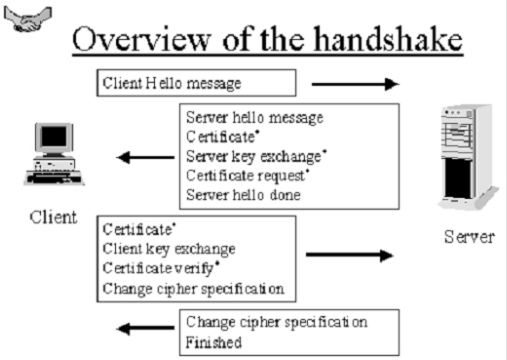
TLS Protocols:

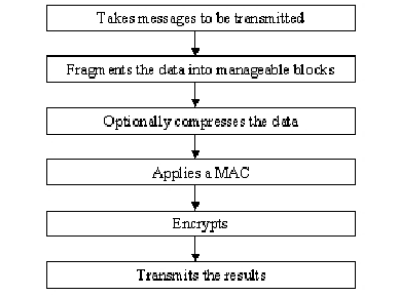
TLS handshake protocol:

Negotiation of
- Session identifier
- Compression method
- Cipher specification
- Master key
- Peer certificate

TLS record protocol:

packaging of data to be transported





28

Cryptosystems supported

- Block cipher (CBC):
  - DES
  - RC2
  - RSA
  - IDEA
- MAC:
  - SHA-1
  - MD5
- Stream cipher:
  - RC4
- Signature:
  - DSS
  - RSA

Authentication: either - both parties
- server authentication
- no authentication

29

Security Analysis

Man-in-the-middle attacks

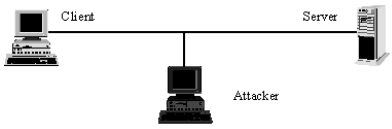
Server is authenticated → Safe

Complete anonymous session → Unsafe

Protecting application data

- Protection with a MAC
- MAC = MD5 + SHA
- The MAC is encrypted

Attacks against the handshake protocol



The attacker changes handshake messages → Client and server computes different values for the handshake message hashes → Without the master key, the attacker cannot repair the finished messages, so the attack will be discovered.

30

However:

- How secure is the cryptographic protocol?
  (e.g. key length, …)
- How is authentication handled
  (e.g. switched on?, signature verification, …)
- Implementation errors

31