



Božo Krstajić, Ph.D
University of Montenegro
Electrical Engineering Faculty
bozok@cg.ac.yu

Web Application Security

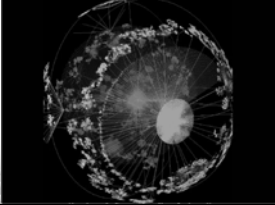
Content

- 1 Introduction
- 2 Security Threats for Networks
- 3 A Typical Hacker Strategy
- 4 Web Application Security
- 5 Instead of Conclusion

Introduction – the Internet

- ◆ **The Internet is a massive global network of networks connecting millions of computers together.**
- ◆ **Information that travels over the Internet does so by the way of “protocols” or languages and instructions that determine how the information is transmitted.**

An attempt to display the Internet infrastructure (2002)



Introduction – Internet Service Providers

- ◆ **An ISP is a company that provides an Internet connection to a person or business. ISPs are beginning to offer different types of connections to their subscribers. Here are the top 4:**
 1. Analog modem (dial-up phone line)
 2. Digital modem (ISDN/DSL phone line)
 3. Cable modem (using your cable TV line)
 4. Leased line (pair or fiber optic)

Introduction – WWW (WEB)

- ◆ **World Wide Web (WEB) is most popular Internet service which is based on HTTP protocol.**
- ◆ **HTTP protocol was designed to be fast and easy to use, although insecure, as it transmits data in plain-text.**
- ◆ **In addition to HTTP, web servers can use "HTTPS" or HTTP over a secure connection.**

Introduction – Web Sites, Servers and Pages

- ◆ **A "web site" is a general term.**
A web site usually refers to some collection of information that may be easily accessed by anyone with a web browser and Internet connection.
- ◆ **A "web page" is a document.**
Typically, web pages reside on a "web site." The documents themselves are really not much different than any other kind of electronic document. They may contain more than just text and links to other web pages. In fact, most web pages contain images, interactive forms, or even more dynamic content such as your bank account transaction history.
- ◆ **A "web server" is a software.**
A special software which running on a computer with a fast Internet connection to "serve" or provide web pages.

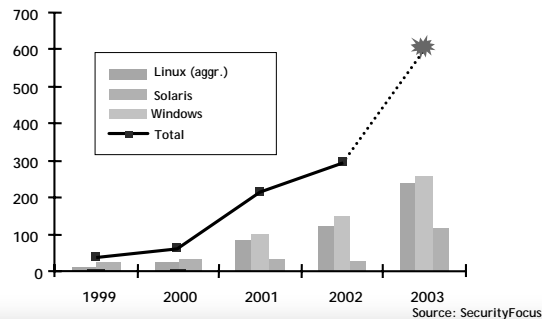
Introduction – Web Browsers and Protocols

- ◆ **One common misconception regarding web browsers is that they are in constant communication with the web server. This is usually not true.**
- ◆ **Browser/server communication is event-driven. It only takes place from the moment you click something until the next web page has loaded into your browser.**
- ◆ **It's important to know that once a web page has loaded into your browser, you are effectively "offline" as far as the web server is concerned.**
- ◆ **When completing a web form there is no information sent to the web server until the form is submitted.**

Security Threats for Networks

- ◆ **A *threat* is:**
 - a person, thing, event or idea which poses some danger to an asset (in terms of confidentiality, integrity, availability or legitimate use).
 - a possible means by which a security policy may be breached.
- ◆ **An *attack* is a realization of a threat.**
- ◆ ***Safeguards* are measures (e.g. controls, procedures) to protect against threats.**
- ◆ ***Vulnerabilities* are weaknesses in safeguards.**

Vulnerability Development



Threats

Threats can be classified as:

- ◆ *deliberate* (e.g. hacker penetration);
- ◆ *accidental* (e.g. a sensitive file being sent to the wrong address).

Deliberate threats can be sub-divided:

- ◆ *passive* (e.g. monitoring, wire-tapping);
- ◆ *active* (e.g. changing the value of a financial transaction).

In general passive threats are easier to realize than active ones.

Fundamental Threats

◆ **Four fundamental threats (matching four 'standard' security goals: Confidentiality; Integrity; Availability (CIA) and legitimate use):**

- Information leakage,
- Integrity violation,
- Denial of service,
- Illegitimate use.

(There are other ways to classify threats)

Fundamental Threat Examples

◆ **Information Leakage**

- Prince Charles mobile phone calls, 1993.

◆ **Integrity violation**

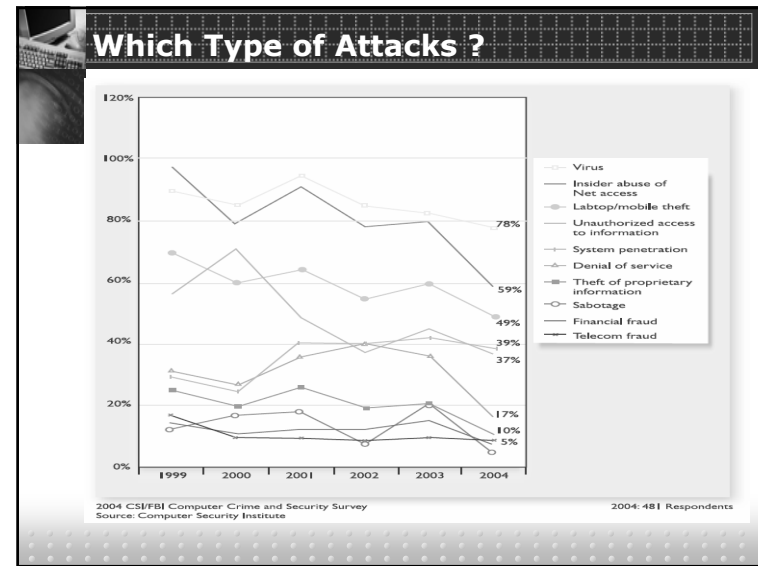
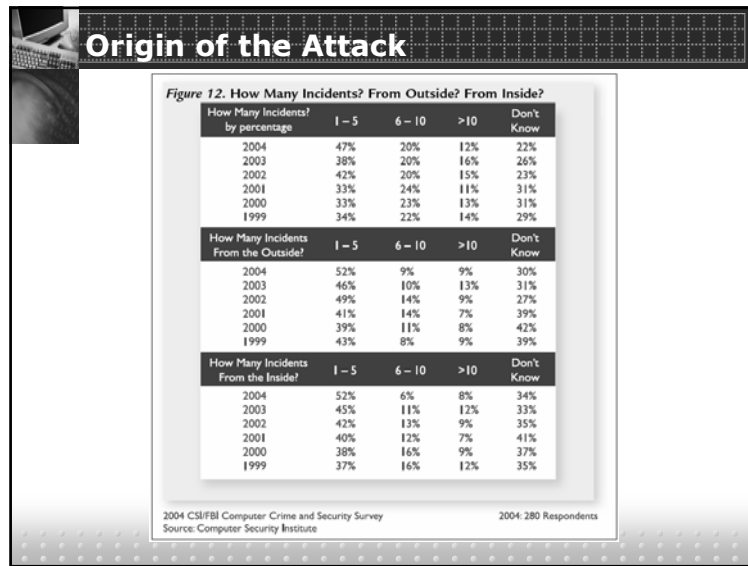
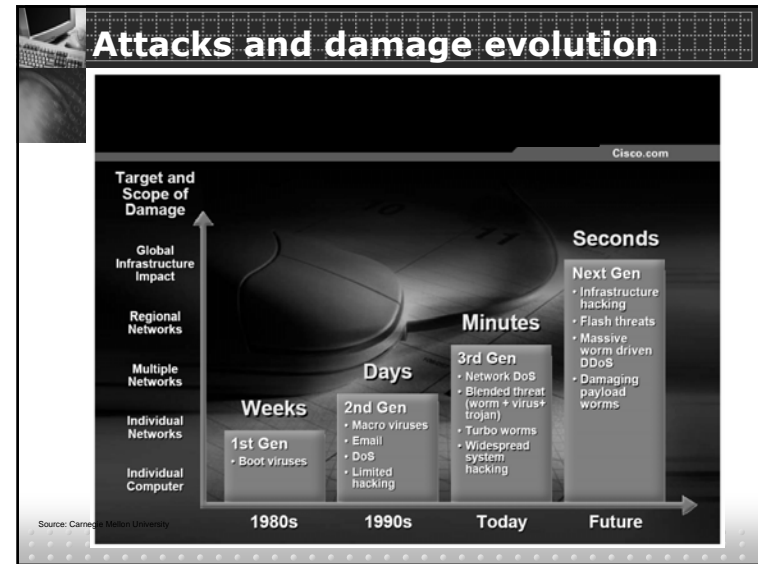
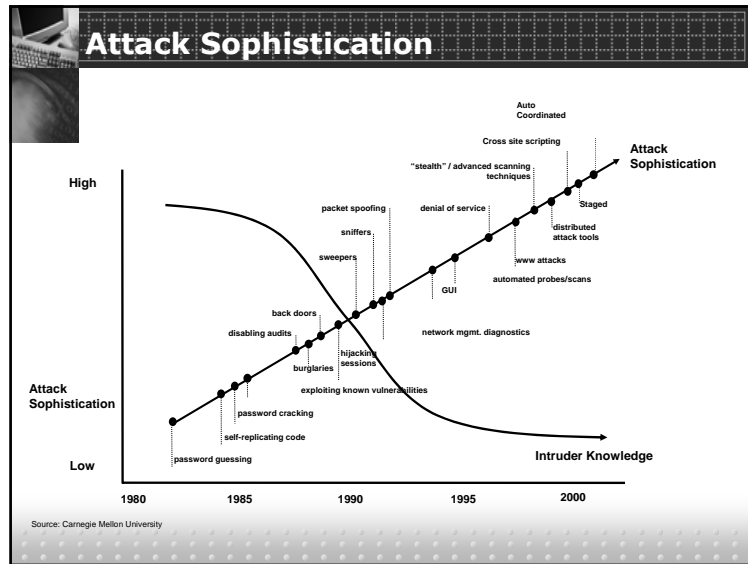
- USA Today, falsified reports of missile attacks on Israel, 7/2002.

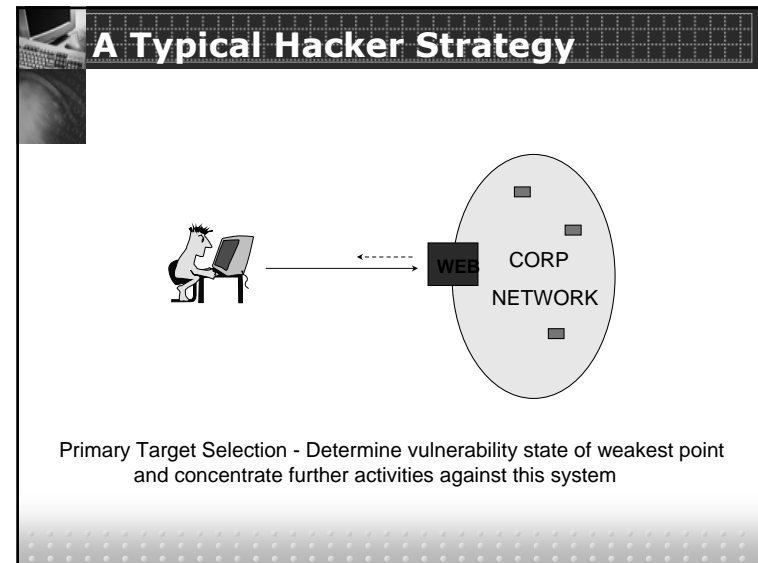
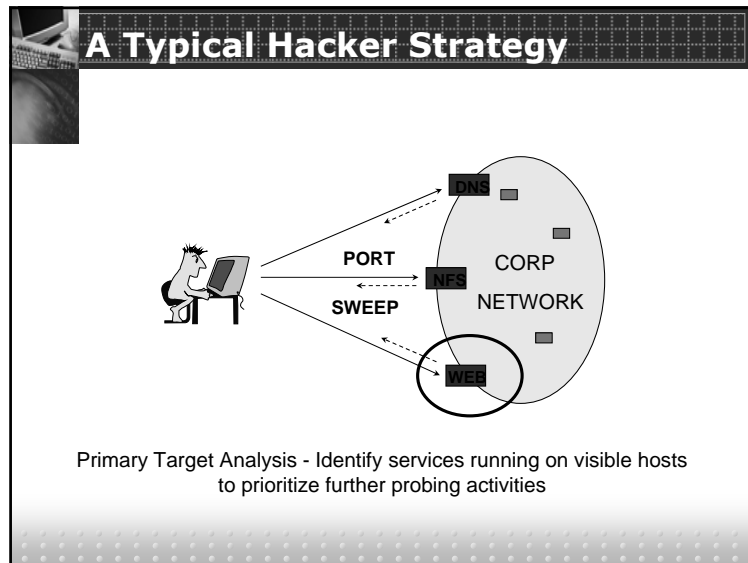
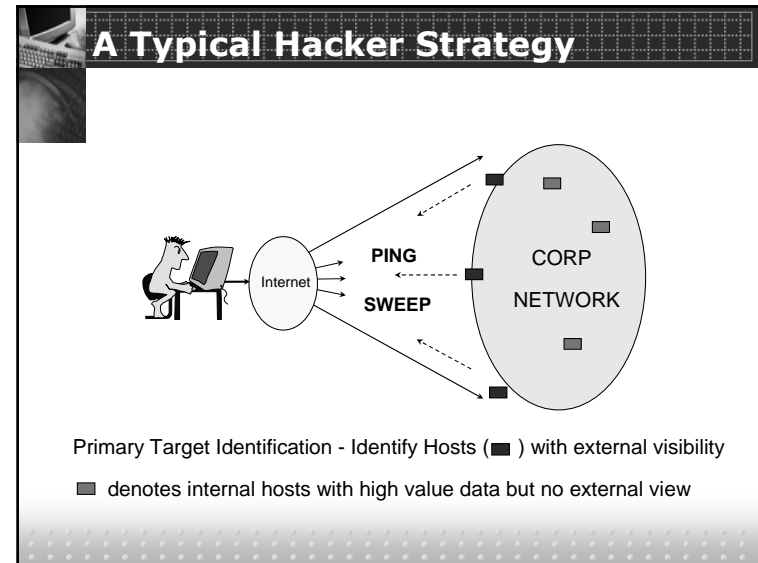
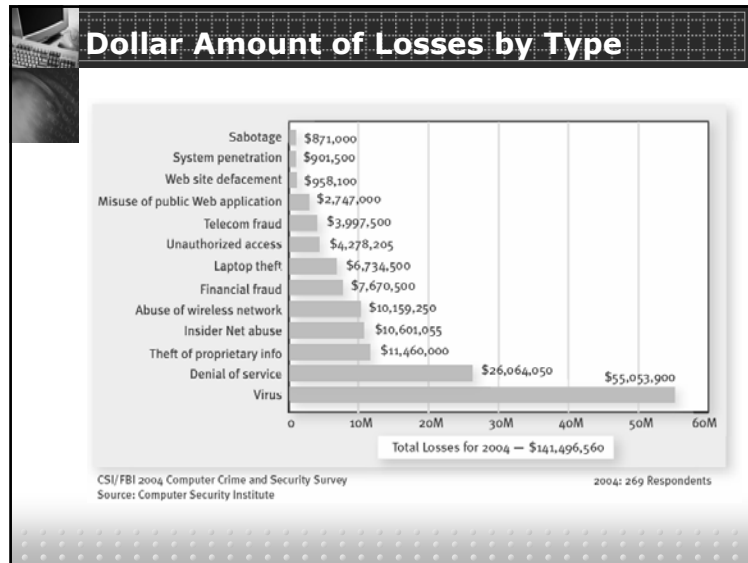
◆ **Denial of service**

- Yahoo, 2/2000, 1Gbps.
- <http://grc.com/dos/grcdos.htm>

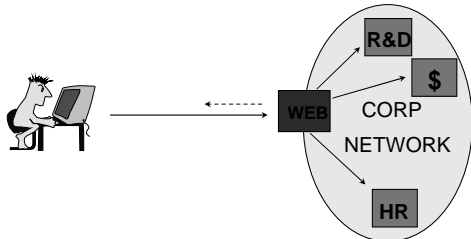
◆ **Illegitimate use**

- Cloning of first generation mobile phone identities.





A Typical Hacker Strategy



Secondary Target Identification - Probing for high value information or systems which are then compromised and data stolen or trojan horses planted, etc.

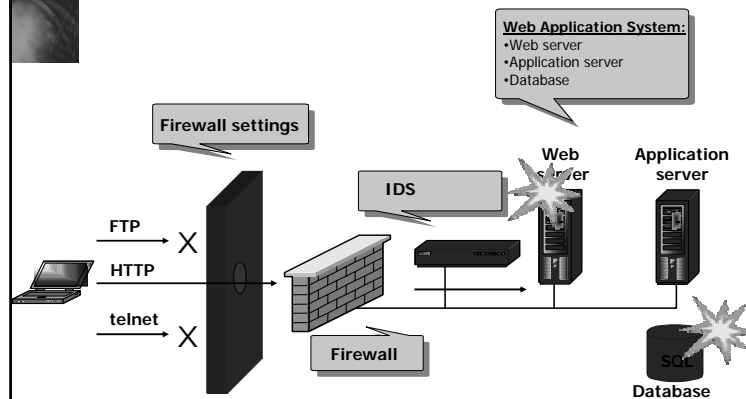
Why WEB ?

- WEB is the most popular Internet service
- 80 % Web applications are vulnerable
- HTTP is simple protocol
- Almost all network devices admit HTTP traffic (firewalls, routers, ...)

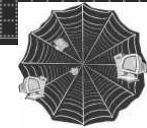
What is a result?

*** 75% of cyber attacks are done at the web application level !!**

Example: A Standard WEB Application



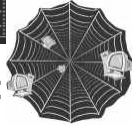
Three Areas of Risk



1. Client 2. Network 3. Server



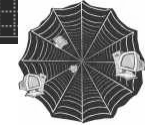
Web server problems



Web server problems that allow remote users to:

- Access confidential documents
- Execute commands on host machine
- Gain information about web server's host machine
- Launch denial-of-service attacks

Web client problems



Browser-side risks:

- Content that crashes browser, damages system or breaches privacy
- Misuse of personal information

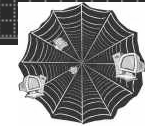
Network problems



Interception of network data eavesdropping at:

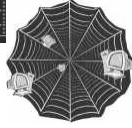
- Browser-side network connection
- Server-side network connection
- End-user user's ISP
- Servers ISP
- Either ISPs' regional access provider

Security Layers



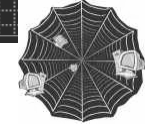
- ◆ Firewalls
- ◆ Server/Client Configuration
- ◆ Web Server Configuration
- ◆ Application Server Configuration
- ◆ Web Applications
- ◆ Data Encryption

Instead of Conclusion



- **Security is a problem**
- **But the risk can be mitigated**
- **The only answer is you!**
- **Take responsibility.**
- **Be smart.**

Useful links



- <http://www.sans.org/>
- <http://www.securityfocus.com/>
- <http://www.w3.org>
- <http://www.cert.org>
- www.incidents.org
- www.cerias.purdue.edu
- <http://www.linuxsecurity.com>
- www.microsoft.com/security

Thank you !