



Web Security

Computer Security

Royal Holloway

December 14th 1998

Introduction

- History : from harmless prank to sophisticated intrusion
- What and why Web security ?
- Academic classification
 - according to types of
 - ◆ incidents
 - ◆ vulnerabilities
 - ◆ security tools and mechanisms

Our approach

Browsers	Servers	Java	Other
- general	- Microsoft IIS	- security model	- spoofing
- Microsoft's Explorer	- Apache	- mobile code	- DNS attack
- Netscape's Communicator	- CGI scripts	- JDK 1.1 versus 1.2	- cookies
		- flaws	- firewalls

Today's topics

■ *Browser security*

↳ 2 examples of browser flaws

■ *Server security*

↳ 'Out of box nightmare' and CGI scripts

■ *Java*

↳ security model

↳ example of flaw

■ *Other*

↳ spoofing



Browser Security

- Internet, not secure
- The Web
 - ◆ free sharing of resources
 - ◆ seems safe and anonymous
- Mobile Code brings a new window of opportunities and risks
- Race between Netscape and Microsoft produces flawed browsers

Browser Flaws

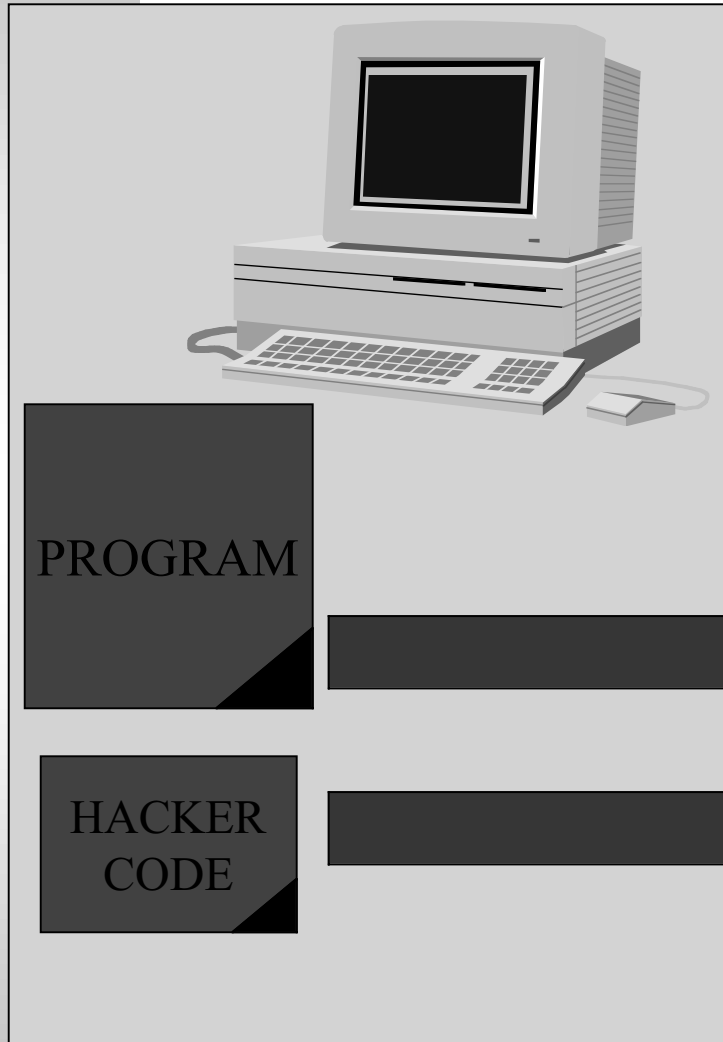
Netscape Navigator

- *JavaScript related*
 - ◆ *Cache memory*
 - ◆ *Meta-tags*
 - ◆ *Preferences file (prefs.js)*
- *Buffer overflow*
 - ◆ *MIME type*
- *Reading HDD information*
- *Frame Spoofing*
- *Random Number Generator*

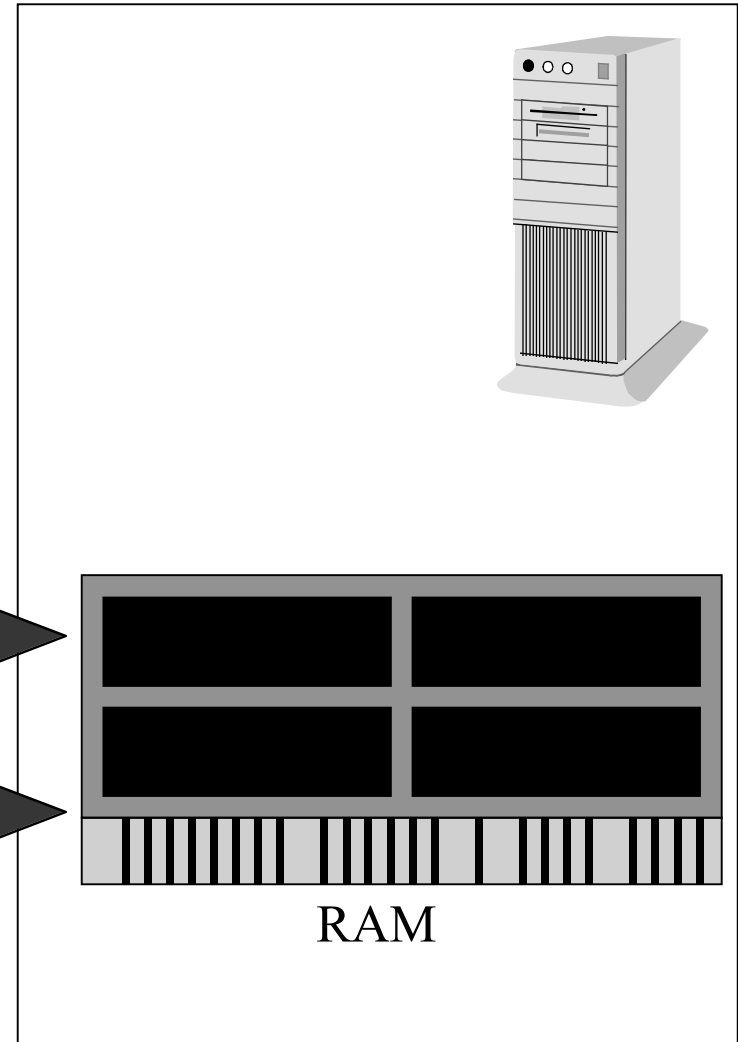
Microsoft Explorer

- *Buffer overflows*
 - ◆ *HTML decoding*
 - ◆ *mk://*
 - ◆ *res://*
- *Recursive Frames*
- *Shortcut Bug*
- *Dotless IP Address (Security Zones)*

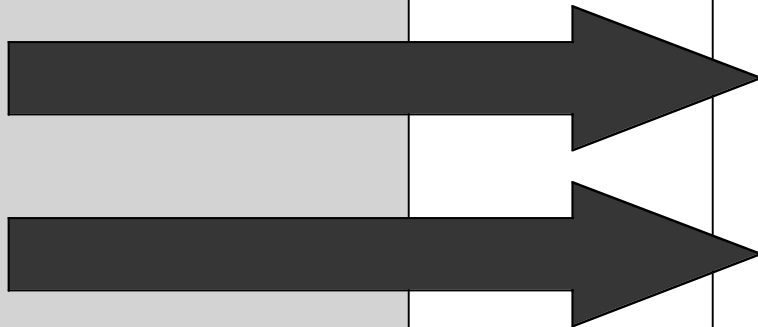
Buffer Overflow



ATTACKER



VICTIM



Browser's Buffer Overflow

- Changing security settings or disabling active documents have no effect.
- Explorer: static region of memory (buffer) to allocate URL or other HTML
- Netscape: fixed size buffer to hold titles of bookmarks.
- For more information on Explorer:
 - ◆ <http://www.10pht.com/advisories>

Server security

'Out of the box' problem

- majority of software packages need patches
 - ↳ continuous upgrades necessary
- default configurations are insecure
 - ↳ e.g. access rights granted to user by default
- performance and functionality vs. security
 - ↳ disable 'whistles and bells' ?

Server security

CGI scripts

- what is a CGI program ?
 - ◆ useful client-side solution
 - ◆ e.g. process data of submitted form
 - ◆ executable : major source of security holes
- two dangers :
 - ◆ leaking of information : can lead to intrusion
 - ◆ remote user tricks script into execution of system commands

Server security

CGI scripts

Programming languages

- no access to source code
- less likely to contain bugs than script and Perl interpreter
- invocation of system commands more difficult

Scripting languages

- scripts shorter and less likely to contain security holes
- built-in features to catch some potential flaws

Server security

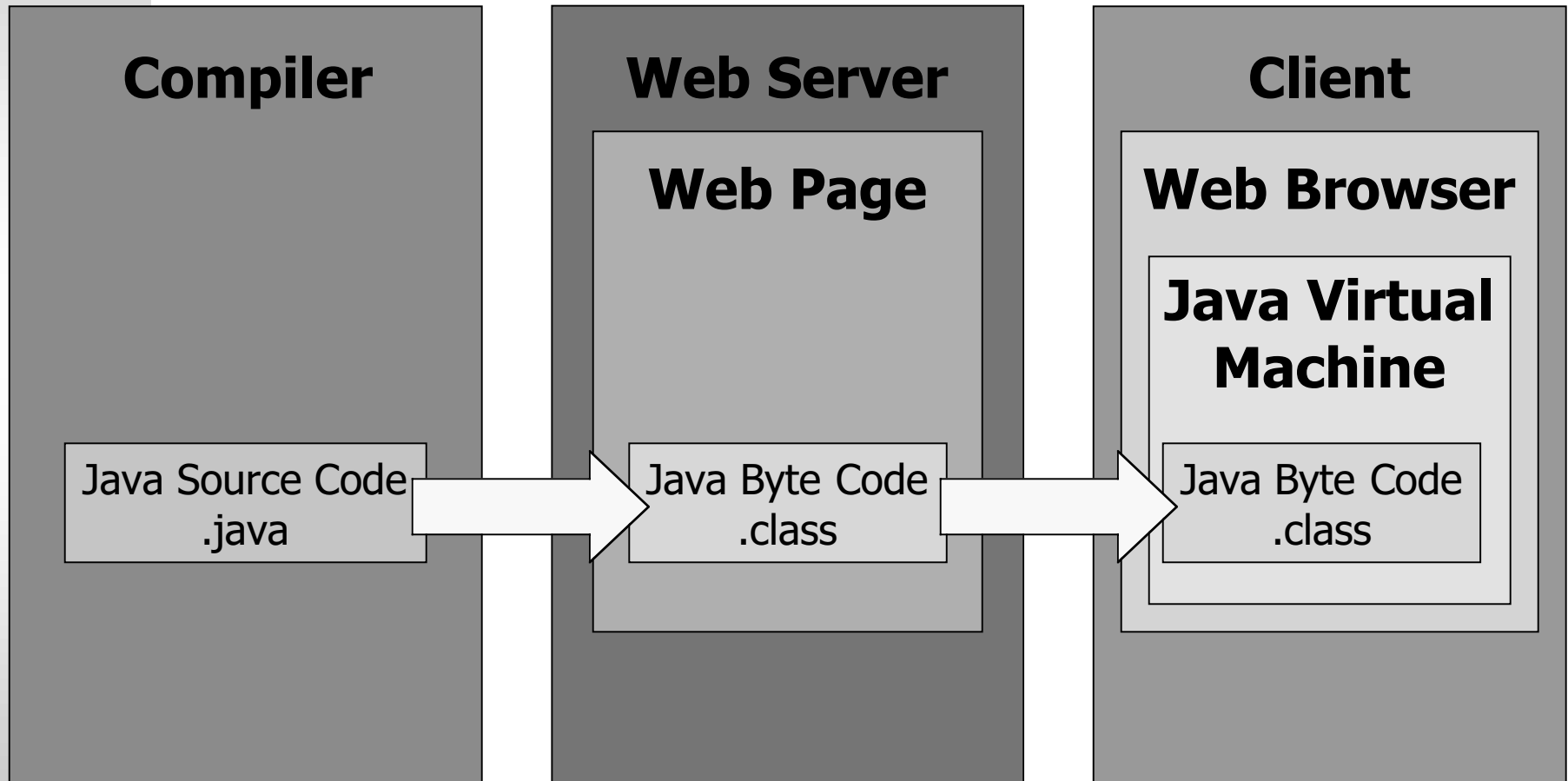
CGI scripts

- possible security incidents can include root compromise
- caution and common sense :
 - ◆ avoid unnecessary complexity
 - ◆ do not give away too much info about your system
 - ◆ do not make assumptions about the size of the user input
 - ◆ check interactions with other programs

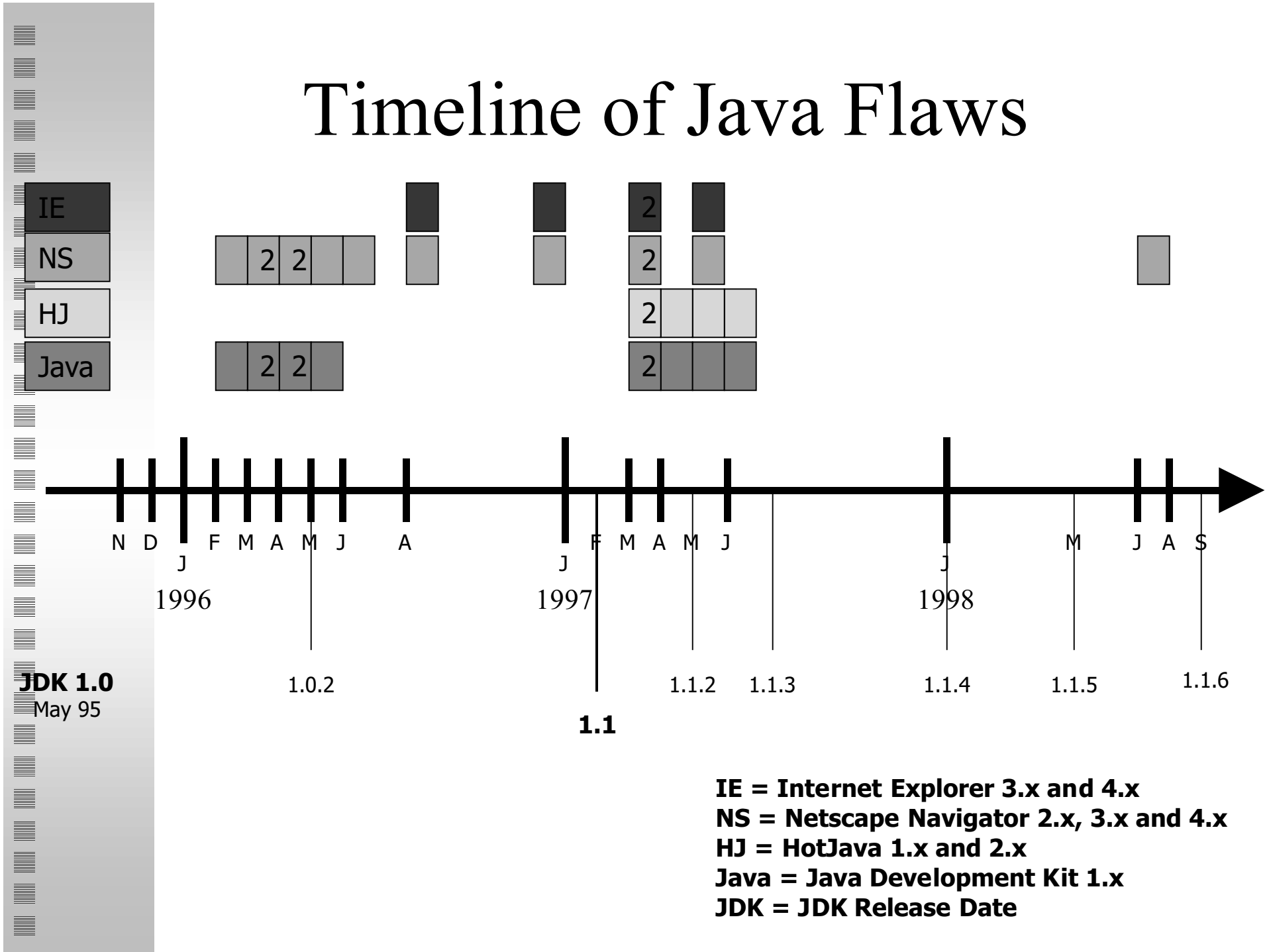
Mobile Code Security

- Possible for server to provide program as content
- Same problem with different twist
- Different approaches by different companies
 - ◆ Java: type safety and dynamic loading
 - ◆ Authenticode: authenticode (digital signatures)
 - ◆ JavaScript: no mechanism

Java Security Model



Timeline of Java Flaws



Security Concepts Affected



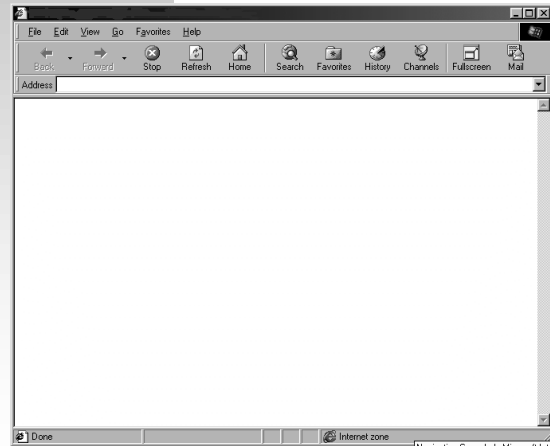
JAVA Flaws

The Mar97 (6) bug was not explained by JavaSoft. They only released the fix.

Web spoofing

- *URL rewriting* to catch victim in false Web
 - ↳ e.g. `http://www.attacker.org/http://netscape.com`
- spoofing of *forms* equally possible
- ‘*secure connections*’ don’t help
 - ↳ the connection is secure
- *actual attack* : lure victim into false Web
- *fine-tuning* of the attack : get rid of all the evidence
 - ↳ e.g. hide status line and location line

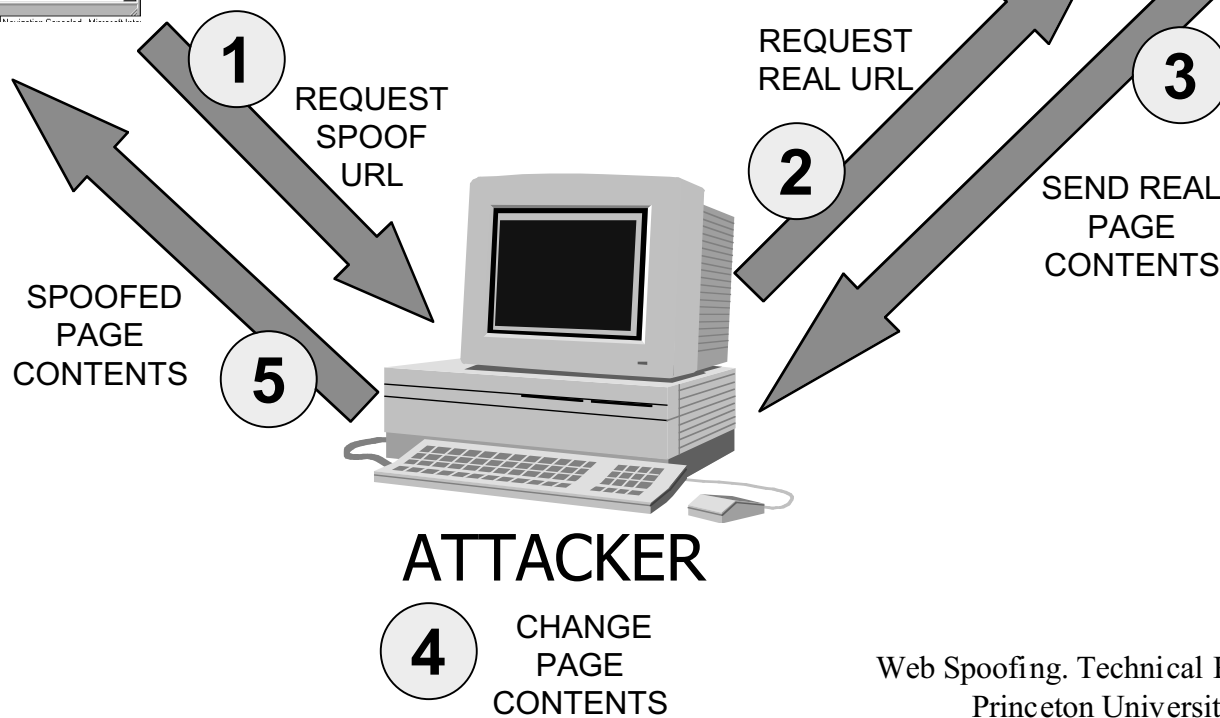
Web Spoofing



CLIENT



WEB SERVER





Future : important issues

- internetworking protocols
- intrusion detection
- software engineering and system survivability
- web-related programming and scripting languages
- intelligent autonomous agents



Thank you !

Merry Christmas !

Happy New year !