

Appendix F. WORLD WIDE WEB SECURITY ISSUES

This Page Intentionally Blank



Wide Open to the World's Web

Security Issues for Web Users and Providers



Scramble to Fix Computer Security Flaws

- By SARA ROBINSON, August 3, 1999

Three giants of the computer industry Microsoft, Hewlett-Packard and Compaq Computer -- found themselves scrambling today to address a rash of serious security vulnerabilities in software designed to interact with Microsoft's Internet Explorer Web ...



Secure or Not, the Internet Has Become a Part of Life's Routine

- By AMY HARMON - February 13, 2000
“When Jon Tara first heard that unknown vandals with unclear motives had managed to sabotage several of the Internet's most prominent businesses last week, the San Diego software engineer posted a probing message to an online investing forum...”



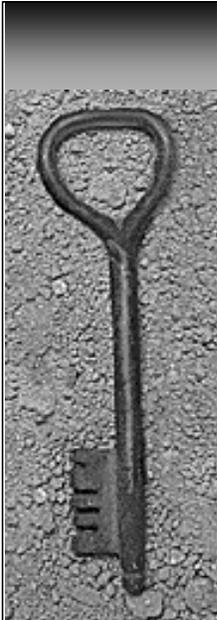
Britain Closes Web Site With Spies' Names

- By WARREN HOGE - May 14, 1999
“An embittered former British spy has used the Internet to make public the names of a large number of secret agents, but officials in London said today that the Web site had been shut down and that no duplicates had surfaced...”



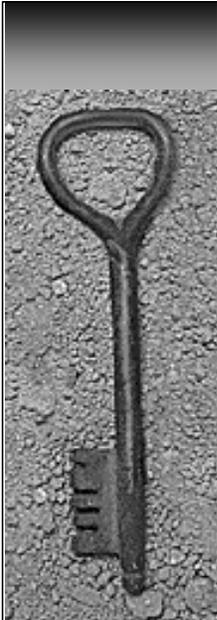
New Security Fears As Hackers Disrupt 2 Federal Web Sites

- By MICHAEL JANOFFSKY - May 29, 1999 “An enduring cat-and-mouse game between Federal agents and computer hackers took a novel twist this week as the hackers turned on their pursuers, disrupting the Web sites of the Federal Bureau of Investigation and the United States Senate...”



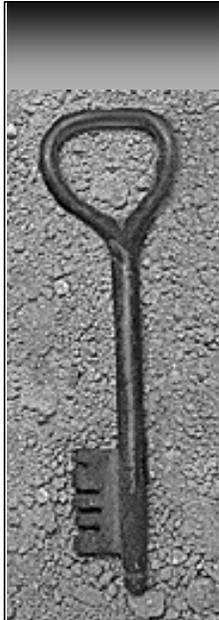
Hack, CouNterHaCk

- By Bruce Gottlieb - October 3, 1999
"Would you like to see how to knock someone off the Web?" Silicosis asks. Sili, as he is known, is a slim young man with serious eyes set deeply into a delicate face. He's the newest member of a hacker collective known as L0pht (pronounced "loft") ..."



Web Attacks Might Have Many Sources

- By MATT RICHTEL and SARA ROBINSON - February 11, 2000
“Computer security experts said today that evidence now suggests that the three days of attacks on leading Web sites may have been the work of more than one person or group. The analysis that more than one group was at work...”

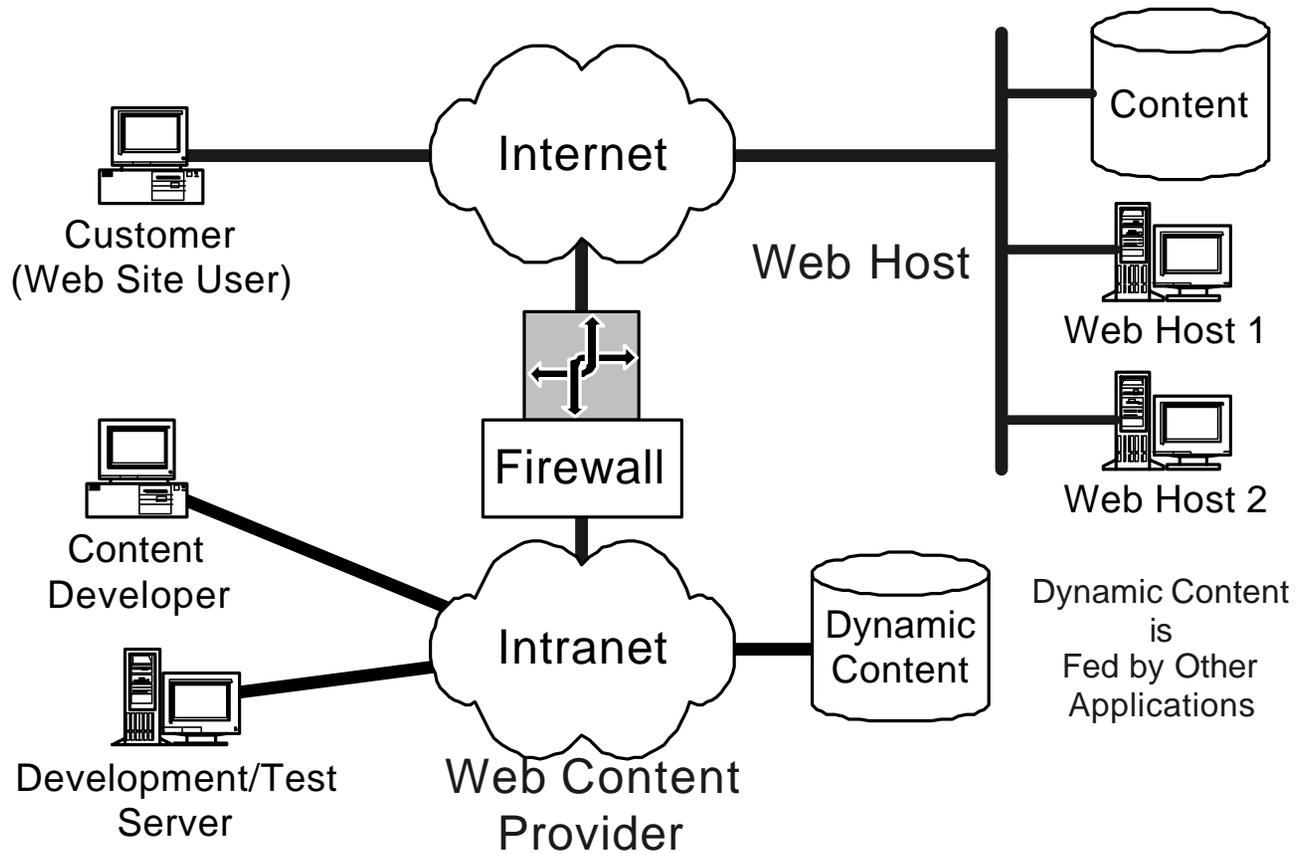


Are there real Web Security Issues?

Obviously



The Model for Web Services



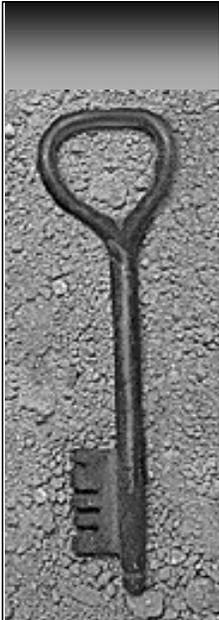


Who needs to be concerned?

- Each and every Web Host
- Each and every Web Content Provider
 - As a provider you may have ethical and legal issues
 - At a minimum you are at risk of embarrassment
- Each and every Web Site User
 - It doesn't matter if you use Netscape or Microsoft's Internet Explorer
 - The problems are real either way, although they may be different



Issues and Responsibilities for the Web User



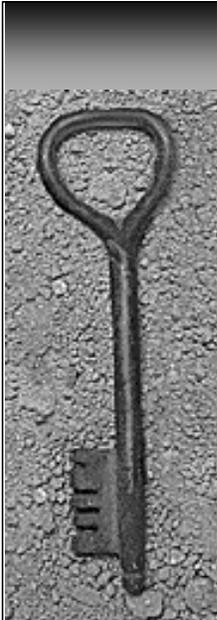
What are the issues for Web users?

- Damage may be done to your computer.
- Information may be stolen from your computer.
- Information that you provide to Web sites may be wrongly used or distributed.
- You may receive misinformation from web sites.
- You may receive stolen property from web sites.
- You may not be able to get the service you need.



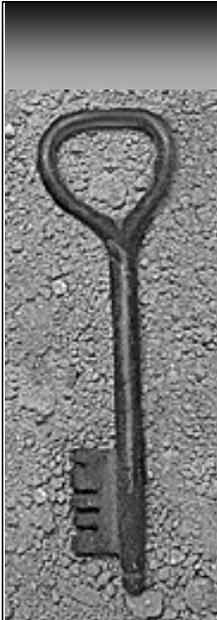
How can a hacker steal or damage my information?

- Hacker's Goal: Install or run a program on your computer
- Approach: Run a script ("active content") through the browser (CGI, Java Applet, ActiveX, JavaScript) or cause you to run a program (a .COM, .BAT, .EXE, or a document with macros)
- Damage: Destroy information with a virus or plant a program that provides a conduit to steal information



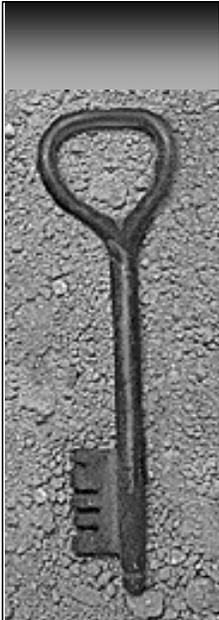
How do I protect my computer?

- Keep an up-to-date backup of key data
 - Keep your documents in one place (e.g., My Documents) and back that up every day
 - Don't worry as much about application software (e.g., Windows, Word, etc.) – you can always reinstall that
- If you have any sensitive or valuable information
 - Either store that information on removable disks (floppy, Zip, etc.) and lock it up, or
 - Encrypt any sensitive information on your hard disk



How do I protect my computer?

- Run virus protection software and keep the virus definitions up to date
- Try not to visit questionable sites
 - Stick to the sites you need, know, and trust
 - Don't surf
- Be very careful when downloading and running programs
 - If possible, don't do it
 - Don't "click" on programs you get through E-mail



Summary: Recommend that Your Web Users...

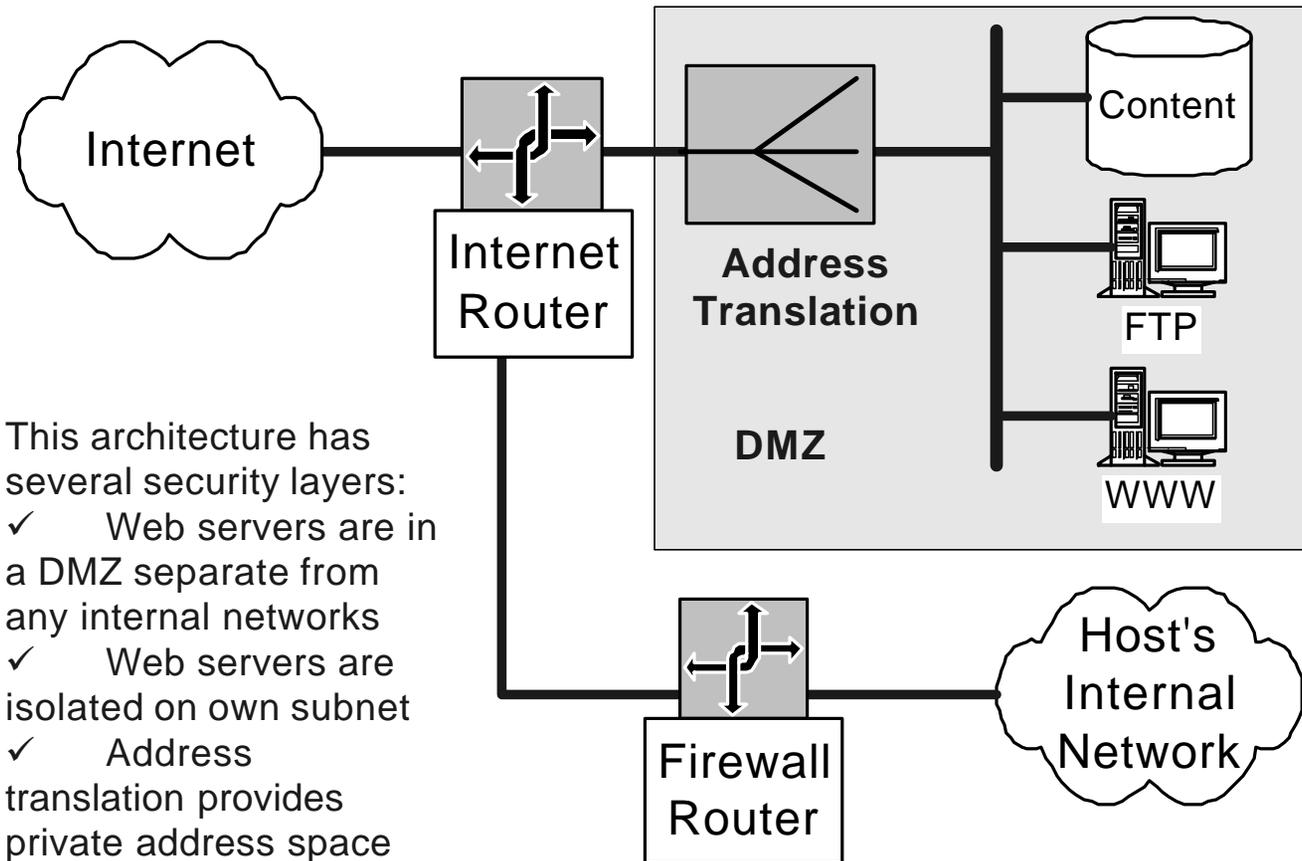
- Treat active content as suspicious and potentially dangerous
- Stick to the web sites they know, trust, and need
- Avoid downloading and running executable programs
- Keep security controls, such as certificates, in place



Issues and Responsibilities for the Web Host and Web Content Provider



Network Architecture Can Enhance the Host's Security



This architecture has several security layers:

- ✓ Web servers are in a DMZ separate from any internal networks
- ✓ Web servers are isolated on own subnet
- ✓ Address translation provides private address space for Web servers



Summary: Your Web Host Should...

- Have a published security and privacy policy
- Use good physical security
- Configure servers properly
- Administer the servers for security with the latest patches

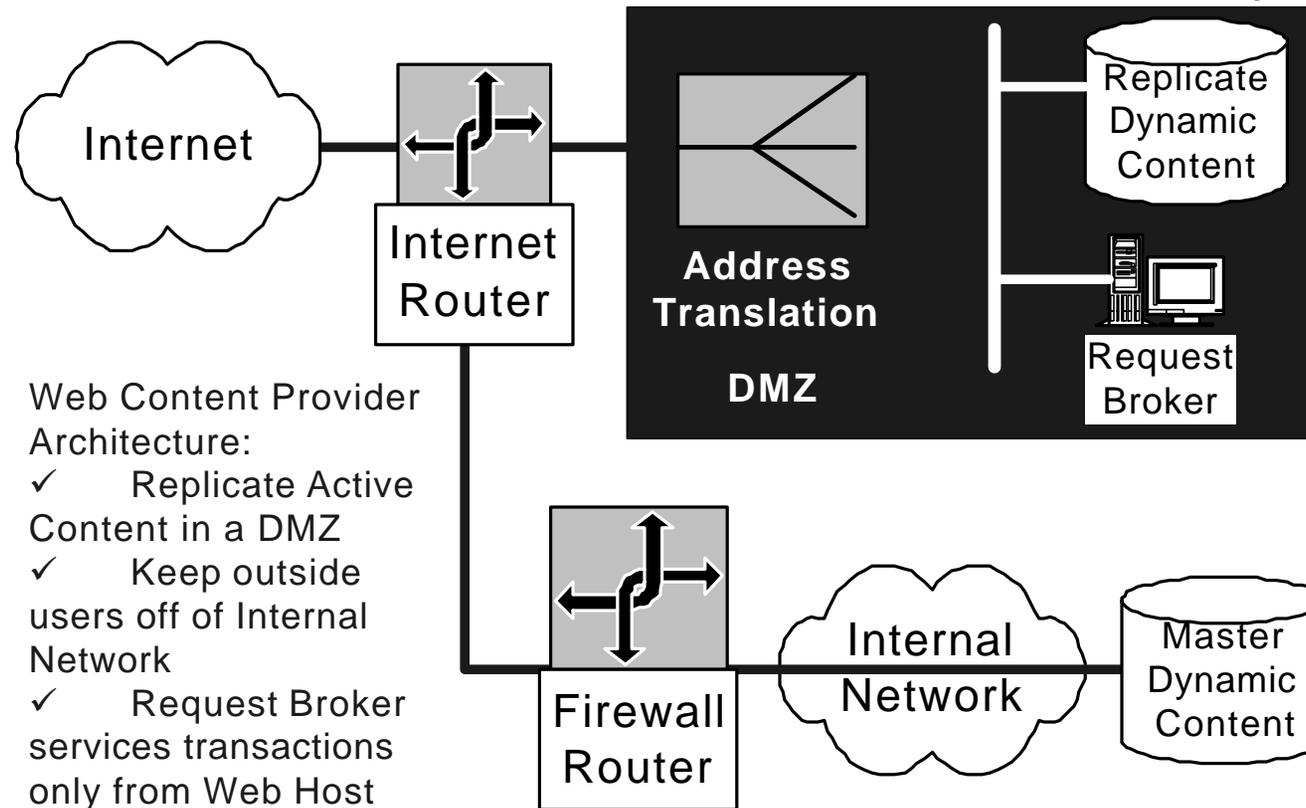


Keeping the Server Secure

- Rule #1: Don't do development on the web server!
 - Web site development should be done in a development environment
 - Port code to the server after extensive testing
- Take footprints and look for unexpected changes
 - Take a snapshot of the working server with a tool like TripWire
 - Periodically compare the server to the snapshot
 - Investigate unexpected changes



Network Architecture Can Enhance the Provider's Security



- Web Content Provider Architecture:
- ✓ Replicate Active Content in a DMZ
 - ✓ Keep outside users off of Internal Network
 - ✓ Request Broker services transactions only from Web Host



Summary: Your Web Content Provider Should...

- Treat web content like software and use good systems for review, documentation, change, publication, and testing
- Test code thoroughly before production
- Have one person who releases production code
- Have one Web Master (a different person) who installs production code



More detail follows on Host
and Content Provider security
issues

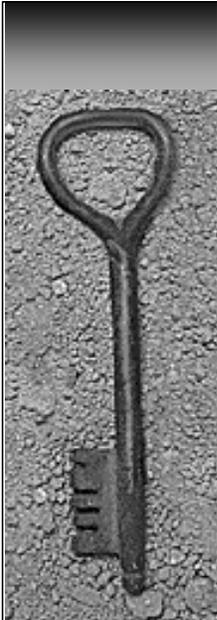


Issues and Responsibilities for the Web Host



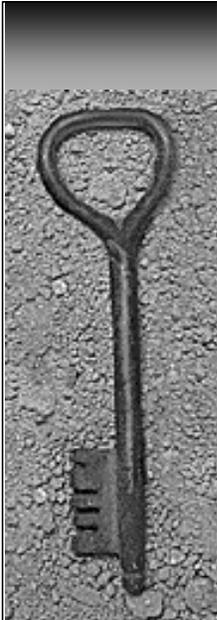
Web Host: Make or Buy Decision

- Should we provide our own web servers?
 - More control, tailored and tuned to our requirements (security and performance)
 - Significant overhead and responsibility
- Should we buy this service?
 - Many organizations in the business: Digital Nations; BBN/GTE; Digital Island; AT&T
 - Those heavily involved as service providers, particularly for E-Commerce, have a strong vested interest in security



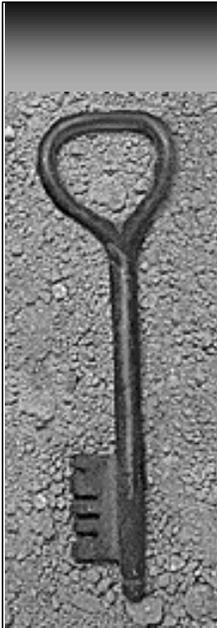
What security can we expect from our host?

- Very difficult to mandate a specific security solution
 - Requirements are difficult to construct without detailed knowledge of vendor's architecture
 - Many reasonably safe solutions; no absolutely safe solution
- Probably should be an evaluation criteria for source selection



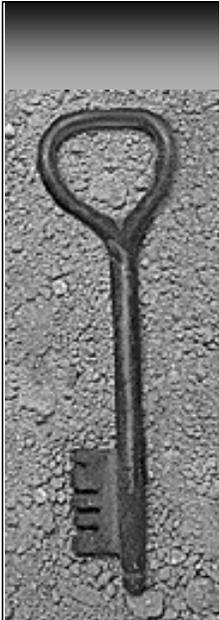
Policies are the Basis for Security

- Web host must have a written Privacy policy
 - Under what circumstances will they distribute information about clients
 - See <http://www.TRUSTe.org>
- Web host should have a written and published security policy
- You should ask for both of these policies as part of any RFP for web services



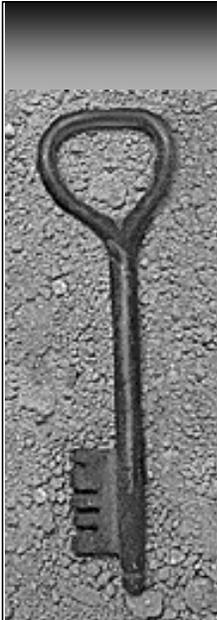
Physical Security for Web Servers

- Protected from unauthorized physical access
 - Located in a locked room with limited access
 - Located on a secure site with 24x7 security
 - Protected with power-on passwords
- Protected from water, fire, and theft
- Protected with clean power and standby power



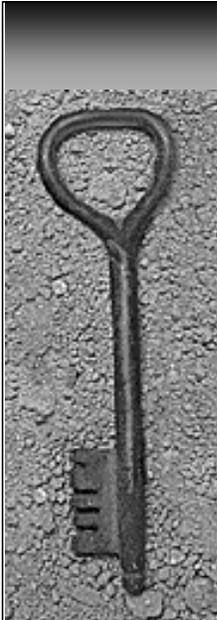
How is your web site spread between host servers?

- There are distinct advantages for you if you have one or more dedicated servers for your site
 - Multiple servers are more robust
 - Less susceptible to denial of service attacks
 - Avoid sharing a server with a prime hacker target
- This is more expensive for the host provider, so it may be more costly for you
- One cost-effective solution may be your own “slice” of a mainframe web server



Proper Server Configuration and Administration is Most Important

- Web servers are designed for outside access, so blocking the path to the server is not an option
- Three considerations for server defense:
 - (1) Which web server
 - (2) Which operating system
 - (3) How is security administered?
- The last of these is by far the most important



Which web server software is more secure?

- The main key is whether or not the web server software has to run as a privileged application
- Of the big three
 - Apache is great for security because it does not run in a privileged mode
 - Netscape Server runs privileged but has a good security reputation
 - Microsoft Information Index Server (IIS) both runs privileged and has a poor reputation
- IBM Web Sphere on OS/390 is potentially very secure



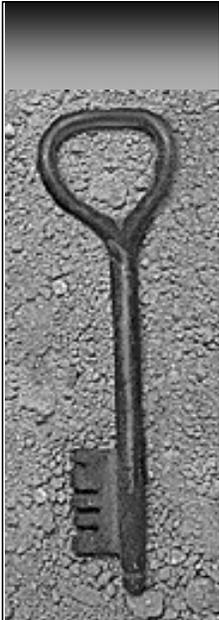
Which operating system is more secure?

- IBM's OS/390 is far more secure than UNIX or NT
 - Only economical at large scale
 - Big role in E-Commerce
- Both UNIX and NT can be made secure with proper administration, configuration, and tools



Key Points for Operating System Security

- Install all security patches promptly
- Carefully control account access
 - No unattributed accounts; e.g., root logons
 - No Guest accounts
 - Limit privileges to only those needed
- Don't share web server with other applications
- Pay attention! Log access and examine the logs for security problems



Run Only Those Services Needed for Web on the Web Server

- On NT run
 - Server, TCP/IP, and WebServer
 - If required, RPCBind and Domain Authentication
- On UNIX some replacements of infamous services can increase security
 - Run the latest version of the Perl 5 scripting language
 - Run the latest version of Xntpd, network time protocol
 - Run the latest version of DNS (domain name services)
 - Run PRO FTP if a File Transfer Protocol server is required
 - Wietse's replacements for rpcbind and the infamous UNIX mail program sendmail



Use Security Tools to Help; Keep Up With the Bug Tracks

- Security monitoring tools should be part of a security architecture
- Some common tools include
 - Tripwire (<ftp://coast.cs.perdue.edu/pub/COAST/Tripwire/>)
 - COPS (<ftp://ftp.cert.org>)
 - Swatch (<ftp://ftp.stanford.edu/general/security-tools/swatch>)
- One has to keep up with the security bugs that are constantly discovered
 - <http://www.ntsecurity.net>
 - <http://www.sans.org/>
 - <http://www.cert.org/nav/training.html#infosecurity>



Issues and Responsibilities for the Web Content Provider



What are the concerns for Web Content Providers?

- Information meant to be private may be stolen from your site.
- Your site may be used to present misinformation.
- Your site may be damaged or destroyed.
- Access may be disrupted (Denial of Service).
- Your site (or intended site) might be used to cause damage to or steal information from your users.



Is the content secure?

- All the host security is of no value if the content is not secure:
- Who is authorized to place content on your web site?
- Under what rules do they operate?
- What types of tools and languages are they allowed to use?



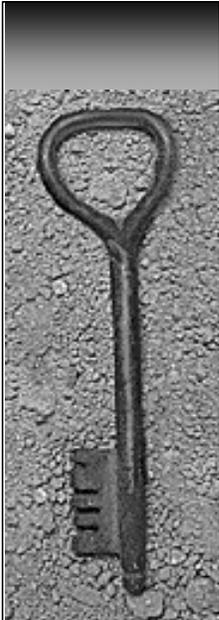
Develop On a Test Environment

- The ability to compose HTML with Notepad does not make one a Web Master
- Do not develop on the Web Host Server
- Test all code thoroughly before it is ported to the web server
- Only one or two Web Masters should have authority to port code to the Web Host



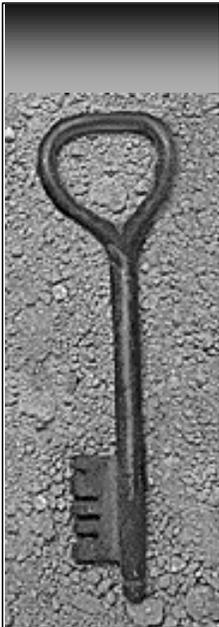
Quality Control for Content

- Get code reviews in place: Peer review and senior review
- Have a single approval authority for production code
- Have a single web master for placing code in production
- Implement change control for content
- Monitor code footprint for changes



Not All Content is Safe

- Active X controls can be spoofed into real controls which can attack client machines
- Java and (especially) JavaScript have active hacker exploitation
- Neither Active X nor Java Script are confined to their own “sandbox”
- Both Java and Active X support third-party certificates to guarantee original code: “Original” is not the same as “safe.”



References

- SANS Security, “Fundamentals of Web Security,” presented at SANS Security Conference by John Stewart and Dave Kensiski, December 13, 1999
- Hacking Exposed: Network Security Secrets and Solutions, by Stuart McClure, Joel Scambray, and George Kurtz, published by Osborne, 1999
- Hacker Proof, by Lars Klander, JAMSA Press, 1997, Chap. 6, 7, and especially 19
- Go to the World Wide Web Consortium at <http://www.w3.org> and search on “security”