Web Security...

...in an insecure world
Outline

- Aspects of Web Security
- Attacks
- Security Holes
- SSL and HTTPS
- Java Security
- Conclusion
Aspects of Web Security

- Browser security – Client side
- Server security
- Connection Security
HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent “break-ins” that paralyzed the Amazon.com, Buy.com and eBay websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National Cybercrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we’ve only seen the tip of the iceberg.

“The criminals who knocked out those three major online businesses are the least of our worries,” Yabenson told Weekly World News.

“There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can’t even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

“It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to: blast apart like a large hand grenade.

Sickos can wreak death and destruction from thousands of miles away!

Arnold Yabenson.

...& blow your family to smithereens!

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

“As shocking as this is, it shouldn’t surprise anyone. It’s just the next step in an ever-escalating progression of horrors conceived and instituted by hackers.”

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U.S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America’s major cities.

“As dangerous as this technology is right now, it’s going to get much scarier,” Yabenson said.

“Soon it will be sold to terrorists, cults and fanatical religious-fringe groups.

“Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

“And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

“That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn’t like your looks, can kill you and never be found out.”
Why are Sites Vulnerable?

- Bugs in system software
- Lack of physical security of server hardware
- Networks are not secure
- Insider threats
- Lack of a security policy
- Server-side includes
- Java, CGI, the list goes on
- Frustrated computer science majors
Server-Side Includes

- SSI are parts of server directives that can be embedded in HTML documents.
- They can instruct the server to execute system commands or CGI scripts.
- Can be unintentional.
- Some web servers can let the admin disable which types of includes can execute arbitrary commands (Apache).
Outline

- Aspects of Web Security
- Attacks
- Security Holes
- SSL and HTTPS
- Java Security
- Conclusion
Attacks

- Denial of Service
- Buffer Overflow
- Trojan Horse
- Man in the Middle
- DNS Subversion
Buffer Overflow Attack

- `strcpy(buffer, argv[1]);`
- Integer overflow
- Not checking bounds
Web Spoofing Attack

- Faulty link
- JavaScript can change function of proper looking buttons
- Convince someone they are at the proper site
- Gather password info, other data
- Produce error or go to right page after submission
Outline

- Aspects of Web Security
- Attacks
- Security Holes
- SSL and HTTPS
- Java Security
- Conclusion
Security Holes

- Web Bugs
- Parameter Passing
- Cookies
Web Bugs

- Purpose: watch and learn about your activities and habits
- Accumulate knowledge, demographics
- Make cookies available to others
- Correlate cookies assigned by various sites to collect more information
- Valuable for advertising and promotional companies
Web Bugs in Email

- See if an email message was read
- Provide IP address of someone trying to remain anonymous
- See how many people viewed the same email message
- Remove a person from a junk mail list if they never open their mail.
- Synchronize Web browser cookie to an email list to let their site know who the person is if they view it. Then it can personalize it.
Web Bugs in Action

- Valuable for advertising and promotional companies

- Privacy violation?
Web Bugs

- Quicken
- FedEx
- Metamucil
- Oil of Olay
- StatMarket
Web Bugs: quicken.com

<img src=http://ad.doublecklick.net/ad/pixel.quicken/NEW width=1 height=1 border=->

<IMG WIDTH=1 HEIGHT=1 border=0 SRC=http://media.preferences.com/ping?ML_SD=Intuit TE_Intuit_1x1_RunOfSite_AnyE&db_afcr=4B31-C2FB-10E2C&event=reghome&group=register&time=1999.10.27.20.5 6.37>
Parameter Passing

- Websites that do not check for entries into forms are highly subject to this form of attack.

- View example at http://cgi.cs.duke.edu/~pcd3/test.cgi

- You MUST check boundaries, entry types, etc
#!/usr/local/bin/perl
use CGI qw/:standard/;

# print header(),start_html,h1(""$yr" Calendar"),pre;

print header;
print start_html('Security Example'),
h1('Calendar Example'),
start_form,
"Which year would you like to view? ",textfield('yr'),
p,
submit,
end_form,
h1(""$yr" Calendar"),pre;
print end_html;

if (param()) {
    my $yr=param('yr');
    $|=1;
    print h1(""$yr" Calendar"),pre;
    system("/usr/bin/cal $yr");
}
print end_html;
Cookies

- “Opacity” – a person does not know what kind of things you are recording about them
- Spy would assign a cookie to each user
- The cookie can “encrypt” information by replacing terms that would give away the security breech with terms that either sound ok or are meaningless.
Outline

- Aspects of Web Security
- Attacks
- Security Holes
- SSL and HTTPS
- Java Security
- Conclusion
SSL and HTTPS

- Encrypted Channel
Outline

- Aspects of Web Security
- Attacks
- Security Holes
- SSL and HTTPS
- Java Security
- Conclusion
Java Security

- Web browsers should only allow execution of part of the Java API to prevent applets from...
  - reading and writing local files
  - accessing memory directly
  - making socket connections to anywhere but their machine of origin
Java: The Sandbox and Beyond

- Isolate Applet for instance from trusted local code
- Only gives certain permissions
- Java 1.2 provided further security by creating fine-grained permissions instead of just dividing things into two divisions.
Java Permissions: XML based

- Your reading for today
- Use web.xml to create security permissions
- `<security-constraint>` tag
- This system forces role names to be used so that only someone with the proper name authentication can use this code
- Instead of shooting off error messages if an improper user clicks on something, use the rolecheck method so that the role can be checked and then you can do an if-statement to see if the URL should be included in the page.
SQL Vulnerabilities

- Again, not checking what users input
- SELECT admin_level FROM access, users WHERE users.username='$user_username' AND users.id=access.user_id
- SELECT admin_level FROM access, users WHERE users.username=' ' OR admin_level=2 OR username='x' AND users.id=access.user_id;
- This gains administrator privileges and they can then view the user list, create privileges, approve items, etc.
Is Security Impossible?

- Yes and No
- Secure the OS and web server (install updates)
- Monitor server
- Access control
- Beware of CGI scripting
- Encryption
- Firewall
Outline

- Aspects of Web Security
- Attacks
- Security Holes
- SSL and HTTPS
- Java Security
- Conclusion
Conclusion

- Check ranges
- Be safe to the point of obnoxiousness
- Always think the dumbest person will use your system
- Always think that the smartest hacker will use your system.
- Update with security patches the second they are released
- Be aware of marketing strategies
- Some things appear helpful, but are they?
- Your projects for this semester......