

# IE: Internet Exposure

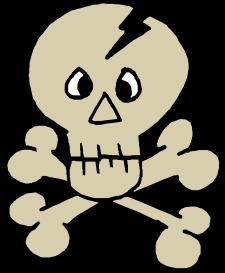
---

Internet Explorer Vulnerabilities  
and What You Can do About Them

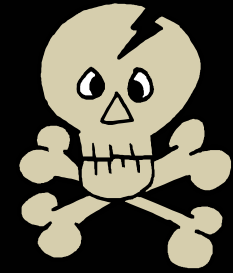


Paul Asadoorian, Lead IT Security Specialist  
Brown University

---



# WARNING



*The following presentation features hacking performed either by professionals or under the supervision of professionals. Accordingly, we must insist that no one attempt to recreate or re-enact any hacking or hacking activity contained in this presentation. If you do so, it is at your own risk.*

# Outline

---

- Why pick on IE?
- Vulnerabilities
- Improving IE Security
- Alternatives

# Why pick on IE?

---

- Long history of vulnerabilities
- Exploited frequently to gain unauthorized access to computers
- Many undocumented vulnerabilities...

# Why pick on IE?

---

- Vulnerabilities still remain:
  - [http://www.safecenter.net/UMBRELLAWEBV4/ie\\_unpatched/](http://www.safecenter.net/UMBRELLAWEBV4/ie_unpatched/)
  - 24 unpatched according to the above we site
  - Most deal with active scripting, ActiveX, etc..

# Why pick on IE?

---

- Installed on every windows computer
- It is the default browser by default
- Most people use IE, simply because its there
- Microsoft is traditionally slow to produce patches

# Why pick on IE?

---

- Turning on IE security settings break applications and web sites
- Some sites only work correctly in IE
- Industry analysts have begun to advise looking at alternatives...

# Why pick on IE?

---

“Time to Dump Internet Explorer”

<http://www.securityfocus.com/columnists/249>

*"IE is a buggy, insecure, dangerous piece of software, and the source of many of the headaches that security pros have to endure..."*

- Scott Granneman, SecurityFocus Columnist

# Why pick on IE?

---

“Why You Should Dump Internet Explorer”

[http://channels.lockergnome.com/news/archives/20040615\\_why\\_you\\_should\\_dump\\_internet\\_explorer.phtml](http://channels.lockergnome.com/news/archives/20040615_why_you_should_dump_internet_explorer.phtml)

*“...the benefits of using IE are too few - and the faults too great — to put off the adoption of an alternative any longer.”*

- Daniel Miessler for Lockergnome

# Why pick on IE?

---

“Internet Explorer Is Just Too Risky ”

[http://www.businessweek.com/technology/content/jun2004/tc20040629\\_7734\\_tc120.htm](http://www.businessweek.com/technology/content/jun2004/tc20040629_7734_tc120.htm)

*“I've been growing increasingly concerned about IE's endless security problems, and this episode has convinced me that the program is simply too dangerous for routine use. ”*

- Stephen H. Wildstrom, Business Week Online

# Why pick on IE?

---

“US-CERT Vulnerability Note”

<http://www.kb.cert.org/vuls/id/713878>

*“There are a number of significant vulnerabilities in technologies relating to the IE domain/zone security model, the DHTML object model, MIME type determination, and ActiveX.”*

***“It is possible to reduce exposure to these vulnerabilities by using a different web browser, especially when browsing untrusted sites.”***

# Why pick on IE?

---

- IE Security problems lead to:
  - Credit Card theft
  - Loss of personal information
    - Spyware, Spyware, and more Spyware
    - Banking Information
  - Installation of malicious software:
    - Keystroke loggers
    - SPAM related software
    - Backdoor Trojans

# Vulnerabilities

---

- Phishing (Patched)
- Frame Redirecting (Patched)
- Embedded Image URI Obfuscation **(UNPATCHED!)**

# Phishing

---

- URL redirection
- Used quite often to harvest credit card numbers
- <http://www.microsoft.com%00@ebay.com/>



# Phishing

---



- Patch Available
- Took some time to become available
- Only fix used to be use another browser
  - Others browsers warn, just watch!

# Phishing

---

- Links:

- <http://www.kb.cert.org/vuls/id/652278>
- <http://security.nnov.ru/search/news.asp?binid=3110>
- <http://www.theregister.co.uk/content/55/34447.html>
- <http://netsquirrel.com/spoof/> - Nice write-up



# Frame Redirecting

---

- Latest exploit for IE
- Allows code to be executed with Local Machine privileges
- Web sites can now install software

# Frame Redirecting

---

- Attackers used an IIS flaw to compromise web servers
- Installed code on web server to infect vulnerable browsers
- Installed malware on all computers that visited web site
  - SPAM Relays
  - Keystroke loggers

# Frame Redirecting

---

- Links:
  - <http://www.incidents.org> – Handlers Diary
    - <http://www.incidents.org/diary.php?date=2004-06-24>
  - <http://www.kb.cert.org/vuls/id/713878>
  - <http://secunia.com/advisories/11793/>

# Embedded Image URI Obfuscation

---

- Hides the real destination of the URL
- Mouse-Over an image to see URL location
- Click on image takes you somewhere else

# Embedded Image URI Obfuscation

---

- No patch available
- Often comes in the form of Email
- Example...

# Embedded Image URI Obfuscation

---

- Links:

- <http://www.securityfocus.com/bid/10308>
- <http://xforce.iss.net/xforce/xfdb/16102>
- <http://www.incidents.org/diary.php?date=2004-06-26> – New phishing attack

# Improving IE Security

---

 Caution – Changing security settings in IE may  cause web sites to no longer function

- Guides to securing IE:

- <http://www.computerstuff.net/security/ieconfig.htm>
- <http://www.sans.org/rr/paper.php?id=287>
- <http://www.microsoft.com/windows/ie/using/howto/security/settings.mspix>
- <http://www.microsoft.com/security/incident/settings.mspix>

- You should still try!

# Alternatives

---

- Mozilla Project <http://www.mozilla.org>
  - Mozilla (Latest Version 1.7)
  - Firefox (Latest Version 0.9.1)
- Opera <http://www.opera.com/>
  - Opera Web Browser (Latest Version 7.51)

# Paul's Favorite = Firefox

---

- Trimmed down version of Mozilla
- Tabbed Browsing
- Pop-up blocker
- Themes and Extensions...

# Paul's Favorite = Firefox

---

- IEView Extension

- Right click and open link in IE

- <http://update.mozilla.org/extensions/moreinfo.php?application=firefox&id=35&vid=145>

- Single Window Extension

- Open all new windows as tabs

- <http://update.mozilla.org/extensions/moreinfo.php?application=firefox&id=50&vid=53>

# Paul's Favorite = Firefox

---

- Bookmark toolbar, supports folders
- Nice download manager
- Works with most web sites, applications, and appliances
  - Cisco VPN, Cisco ACS, Netscreen, etc...

# Being more secure

---

- Use extreme caution when using IE
  - Read the HTML or other code before clicking
- Follow IE security guides
- Use a different browser for general web browsing
- Follow Paul's Top Ten Security Tips...

# Paul's Top Ten Security Tips

---

1. Patch Your Machine
2. Use a Firewall
3. Use Anti-Virus Software
4. Use good passwords
5. Don't Use Internet Explorer for everything
6. Use a separate credit card for online purchasing
7. Secure your wireless
8. Use Anti-Spyware tools
9. Don't open email attachments
10. Monitor Children's Usage

**/\* The End \*/**

---

## **Essential Security Links**

<http://packetstormsecurity.nl/>

<http://www.security.nnov.ru/>

<http://www.cert.org>

<http://www.whitehats.com>

<http://rr.sans.org>

<http://www.incidents.org>

<http://www.astalavista.com/>

<http://www.incidents.org>

<http://www.l0t3k.org/>

<http://www.securiteam.com/>

**My Web Site: <http://pauldotcom.com>**

**This Presentation:**

**<http://pauldotcom.com/InternetExposure.pdf>**