Defending Computer Networks
Lecture 19: Proxies and XSS

Stuart Staniford

Adjunct Professor of Computer Science

Quiz 2

- 40 mins,
- Closed book:
  - no notes/phones/tablets/laptops/etc

Logistics

- Project milestone 1 due Friday

Latest News

U.S. Chamber Warns Cyberattack Disclosures Could Hurt Corporate Profits

Chamber Tells SEC Mandatory Disclosures Could 'Paint A Target' on Companies' Backs

By ANDREW ACKERMAN

0 COMMENTS

Oct. 29, 2014 3:00 p.m. ET

WASHINGTON—The U.S. Chamber of Commerce is trying to head off efforts to force publicly traded firms to share more information about cyberattacks, warning policy makers that such disclosures could unduly harm corporate profits.

In a letter to the Securities and Exchange Commission—which has been debating whether to ratchet up disclosure requirements—the Chamber said the agency could "paint a target" on the backs of companies if they are forced to reveal information about specific breaches.

Rootpipe: Major Security Vulnerability in Apple OS X Yosemite Won't be Patched until 2015

By David Gilbert

November 4, 2014 10:23 GMT

Apple has been made aware of a big security vulnerability in its OS X 10.10 (Yosemite) desktop operating system (OS) called Rootpipe which won't be patched until 2015.

The security flaw will allow hackers to gain root access to a computer running the latest version of Apple's desktop software.

The vulnerability was discovered by Swedish security researcher Emil Kvarnhammar who reported the issue to Apple, and after initially being ignored, was asked by the technology giant to withhold publishing details about Rootpipe until the company was able to publish a patch for the software.

Kvarnhammar did however tweet some information about the flaw.

Assigned Reading

- http://www.cert.org/tech_tips/malicious_code_mitigation.html

Where We Are in Syllabus

Rough Lecture Syllabus:

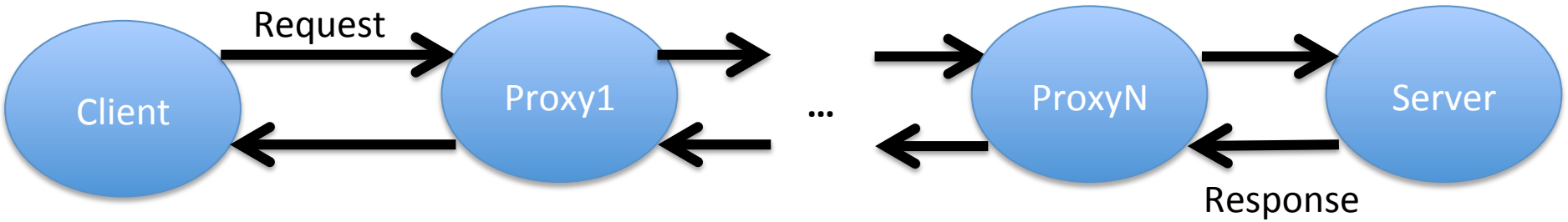
✔ 1. The technical nature of software vulnerabilities and techniques used for exploiting them.
✔ 2. The pressures of commercial software development, and why firms very rarely produce secure software, even though they should.
✔ 3. Basics of monitoring a network, intro/refresher on TCP/IP. Switches, wireless access devices, routers.
✔ 4. Network reconnaissance techniques – ping sweeps, port scans, etc.
✔ 5. Algorithms for detecting port scans on the network.
✔ 6. Firewalls and network segmentation as a defense against inbound attacks.
✔ 7. Detecting exploits with string matching approaches (Snort and similar).
✔ 8. Network layer approaches to evading detection.
✔ 9. Large scale attacks – worms and distributed denial of service.
☞ 10. HTTP attacks as a way around the firewall. Drive-by downloads and social engineering.
☞ 11. Defending against HTTP attacks. Web-proxies, in-browser defenses, anti-virus systems.
12. SMTP attacks – spear-phishing, and defenses against it.
13. HTTPS: Encryption and virtual private networks as a means to maintain confidentiality.
☞ 14. The modern enterprise network: what a large-scale network looks like, and emerging trends affecting it (BYOD, cloud).
15. Legal and ethical issues in defending networks.

Main Goals for Today

- Web proxies
- Cross-site Scripting (maybe)

Web Proxies

- HTTP designed to support chains of proxies:



- Browser/OS has support to designate a proxy
- Try it..

Some HTTP Features for Proxies

- If-Modified-Since: <date>
  - Request side header
  - Allows a 304 Not Modified response
- If-Match: <entity-tag>
- Cache-Control: no-cache (etc)
- Via: <proxy>
- X-forwarded-for: <client-ip-list>

URL Blacklists

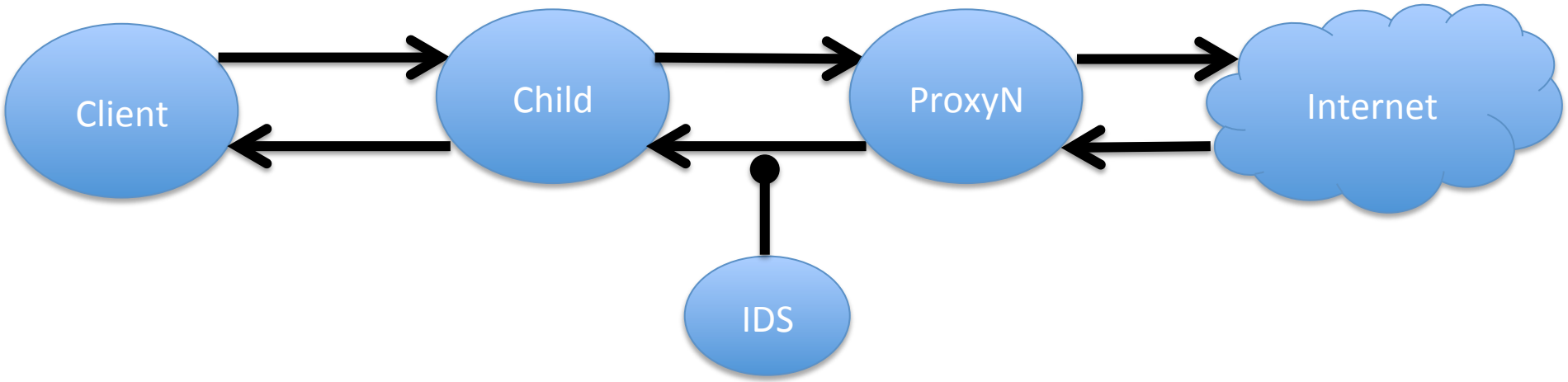
- List of “bad” urls
  - Known malicious
    - Malware, etc
    - Google safe browsing is most famous
  - Productivity problem categories
    - Adult
    - Gambling
    - Social Media
    - Hobby
    - Sports
    - News
  - Uncategorized
    - Blocking this avoids many problems, but also FPs

Building a URL Blacklist

- Build a big farm of clients (eg in VMs)
- Crawl the web
- Try to get infected
- Note the bad URLs
- If you were the bad guys, what would you do?

Reasons for Client-side proxy chains

- Acquisitions
  - When BigCo acquires SmallCo
  - Easiest thing is make SmallCo proxy point to BigCo proxy
  - Don't have to change settings on all SmallCo computers
- Proxy Sandwich
  - Allow for monitoring between child and parent



X-Forwarded-For

- When there is a client-side proxy
  - Anything on Internet side will not see original IP address of client
  - If this is desirable,
    - X-forwarded-for: <ip1>, <ip2>, …
    - Records the chain of IP addresses (original client and proxies along the way).
- In proxy sandwich architecture, often see
  - Child proxy adds X-forwarded-for
  - Parent proxy removes it again

Cross-Site Scripting

Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3]	79.0	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75.0	CWE-798	Use of Hard-coded Credentials
[8]	75.0	CWE-311	Missing Encryption of Sensitive Data
[9]	74.0	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)
[13]	69.3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[14]	68.5	CWE-494	Download of Code Without Integrity Check
[15]	67.8	CWE-863	Incorrect Authorization
[16]	66.0	CWE-829	Inclusion of Functionality from Untrusted Control Sphere
[17]	65.5	CWE-732	Incorrect Permission Assignment for Critical Resource
[18]	64.6	CWE-676	Use of Potentially Dangerous Function
[19]	64.1	CWE-327	Use of a Broken or Risky Cryptographic Algorithm
[20]	62.4	CWE-131	Incorrect Calculation of Buffer Size
[21]	61.5	CWE-307	Improper Restriction of Excessive Authentication Attempts
[22]	61.1	CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
[23]	61.0	CWE-134	Uncontrolled Format String
[24]	60.3	CWE-190	Integer Overflow or Wraparound
[25]	59.9	CWE-759	Use of a One-Way Hash without a Salt

Still a Live Issue

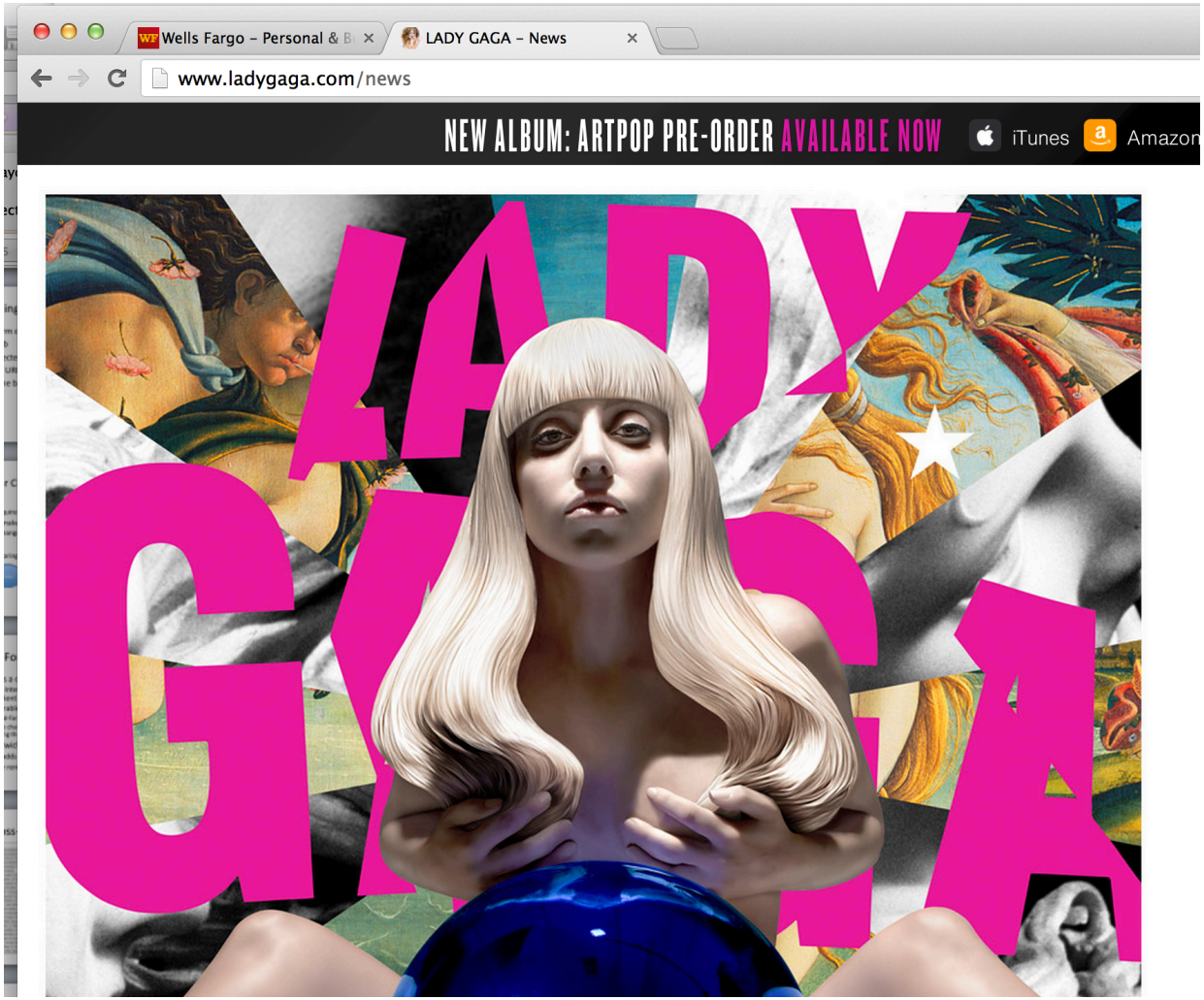
Facebook Login Page hacked through XSS by Mauritania Attacker

Posted by: HNBulletin in Facebook, Mauritania Attacker, News, XSS June 2, 2013 2 Comments

*Founder of Anonghost team "Mauritania Attacker" found XSS Vulnerability in Facebook.com which adds their own message (**HACKED BY MAURITANIA ATTACKER**) in the Facebook Login Page and we also checked that it is still working.*

Same Origin Policy

- When can a piece of js access a DOM?



Same Origin Policy

- Principle enforced by browser is:
  - Protocol, host, and port must all match

Compared URL	Outcome	Reason
http://www.example.com/dir/page2.html	Success	Same protocol and host
http://www.example.com/dir2/other.html	Success	Same protocol and host
http://username:password@**www.example.com**/dir2/other.html	Success	Same protocol and host
http://www.example.com:**81**/dir/other.html	Failure	Same protocol and host but different port
https://www.example.com/dir/other.html	Failure	Different protocol
http://**en.example.com**/dir/other.html	Failure	Different host
http://**example.com**/dir/other.html	Failure	Different host (exact match required)
http://**v2.www.example.com**/dir/other.html	Failure	Different host (exact match required)
http://www.example.com:**80**/dir/other.html	Don't use	Port explicit. Depends on implementation in browser.

So ladygaga.com <script>s shouldn't be able to talk to wellsfargo.com

Form Generation

- http://www.w3schools.com/html/html_forms.asp
  - Especially examine the submit button form
  - Use the submit button
  - Examine the url with parameters
  - Examine the generated output html source
  - What is the server code doing here?
  - Try inputting blah