Defending Computer Networks

Lecture 15: More HTTP/NIDS

Stuart Staniford
Adjunct Professor of Computer Science
Logistics

• Guest lecture Tuesday
  – Cornell ITSO staff
  – Content part of curriculum, fair game on quizzes

• HW3.
  – Due Weds 10/22/14 11:59pm

• Project interim milestone deadline
  • Friday November 7th
Google discloses Web encryption vulnerability

Tuesday, 14 Oct 2014 | 6:06 PM ET

A Google Inc spokesman said on Tuesday that researchers with the company have uncovered a vulnerability in widely used SSL web encryption technology, finding a bug in the SSL 3.0 protocol.

SSL 3.0 is nearly 15 years old, but it is still widely used, Google said, in a Tuesday evening blog post. Even browsers that use newer protocols will retry failed connections with older protocol versions, including SSL 3.0.

"Because a network attacker can cause connection failures, they can trigger the use of SSL 3.0 and then exploit this issue," Google said, in the statement. The immediate fix to the problem will "break some sites, and those sites will need to be updated quickly."

"In the coming months, we hope to remove support for SSL 3.0 completely from our client products," Google said.
Obama Said to Warn of Crippling Cyber Attack Potential

President Barack Obama believes cyber terrorism is one of the biggest threats to national security and says the White House is bracing for a possible doomsday scenario if hackers can successfully penetrate government and business computer systems, the FOX Business Network has learned.

The president shared his thoughts on cyber terrorism last week, during a fundraising tour in New York City and a stop in Greenwich Conn., according to people who attended the events. At the same time, the Obama administration has ramped up efforts to strengthen the nation's cybersecurity and limit future damage if cyber attacks are launched.
CS Colloquium Today

Thursday, October 16th
4:15pm, G01 Gates – Mentors Lecture Hall
Refreshments at 3:45pm in front of New Visions – 416

Information Technology Implications of the President's NSA Review Group

Professor Peter Swire of the Scheller College of Business served on President Obama's Review Group on Intelligence and Communications Technology, which published its report in December to widespread public attention. The President has adopted many of the group's 46 proposals, and others remain under consideration. This talk will describe the process for drafting the report. It will discuss the major recommendations, with a particular focus on information technology issues including encryption, zero-day attacks, and the role of offense and defense in cybersecurity. It will also discuss issues related to Internet governance in light of the intense public debate about how to use modern communications networks for diverse activities including surveillance, military operations, e-commerce, and the daily communications of individual users. The talk will feature an extensive period for Q&A about these issues of surveillance, democracy, and technology.
Assigned Reading

• Javascript Tutorial
  – [http://www.w3schools.com/js/](http://www.w3schools.com/js/)
  – Recommend you play around with at least the basics to get a feel for it
Main Goals for Today

• HTTP responses
• NIDS in Context of HTTP Server Attacks
• Start on web-client side attacks
HTTP Request Basics

• Text lines separated by \r\n  
  – Servers often accept “\n” only, but protocol is “\r\n”
• Header is terminated by a blank line (\r\n\r\n)
• Initial request line
  
  – GET /dumprequest HTTP/1.1\r\n  
    • Other methods include POST, CONNECT, HEAD, DELETE, etc.
    • Focus on GET for now
• Followed by headers of form
  
  – Header: Value...\r\n
  – No request headers are actually required
HTTP Request

GET /dumprequest HTTP/1.1
Host: djce.org.uk
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;v=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/30.0.1599.101 Safari/537.36
DNT: 1
Referer: https://www.google.com/url?
Accept-Language: en-US, en; q=0.8

Try it at http://www.procato.com/my+headers/
A Few Popular Request Headers

• Host:
  – Used to specify domain (server might have several).

• User-Agent:
  – Gives browser specifics (allows server to customize responses to browser)

• Referer:
  – What page (etc) sent us here

• Accept-Language:
  – We speak English, or...

• Accept:
  – media formats we accept (eg text/html)
HTTP Response

HTTP/1.1 404 Not Found
Content-Type: text/html; charset=UTF-8
X-Content-Type-Options: nosniff
Date: Mon, 21 Oct 2013 19:37:20 GMT
Server: sffe
Content-Length: 946
X-XSS-Protection: 1; mode=block
Alternate-Protocol: 80:quic

<!DOCTYPE html>
...


HTTP Response Basics

• Text lines separated by \r\n
• Header is terminated by a blank line (\r\n\r\n)

• Initial response line
  – HTTP/1.1 404 Not Found\r\n    • Indicates status of request.

• Followed by headers of form
  – Header: Value...\r\n  – No response headers are actually required
    • Though hard to get much done without them...
Important Response Codes

• 200 OK
• 301 Moved Permanently
• 304 Not Modified
• 400 Bad Request
• 404 Not Found
• 500 Internal Server Error
A Few Popular Response Headers

• Content-Type:
  − Media-type of entity attached after header

• Content-Length:
  − Length of same (in bytes)

• Content-encoding:
  − ‘gzip’ means compression applied

• Date:

• Server: software being run on the server
Let’s try it

• telnet on 80 to a few popular websites
Entity Body

• Follows header
  – either request or response, but more consistently in response direction
  – Can be any media type:
    • text/html, text/plain, image/jpeg, audio/mpeg
    • http://www.iana.org/assignments/media-types
  – Three methods to delineate length:
    • Content-length
    • Transfer-encoding: chunked
    • Connection: close
Detecting Attacks on Web Servers

• Has been a major industry for 15+ years
• Exploits on the servers themselves
• Exploits on cgi scripts,
  – other server-side plugins
• SQL Injection
• Cross-site scripting
• Also HTTP command-and-control
  – Similar issues of detecting bad HTTP requests
Top Snort Rule Files

Stuarts-MacBook-Pro:rules stuarts$ du -s -k *.rules |sort -n -r |head -10
6152 deleted.rules
1216 browser-plugins.rules
792 malware-cnc.rules
688 blacklist.rules
568 server-webapp.rules
392 file-identify.rules
348 file-office.rules
344 server-other.rules
328 pua-adware.rules
316 browser-ie.rules
Snort Example 4

alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg:"MALWARE-CNC Win.Trojan.Zbot variant in.php outbound connection"; flow:to_server,established; urilen:7; content:"/in.php"; http_uri; content:".ru|0D 0A|User-Agent|3A 20|Mozilla/4.0|0D 0A|"; fast_pattern:only; http_header; content:"|0A|Content-Length|3A 20|"; http_header; metadata:policy balanced-ips drop, policy security-ips drop, ruleset community, service http; reference:url,zeustracker.abuse.ch/monitor.php?ipaddress=195.22.26.231; classtype:trojan-activity; sid: 26023; rev:3;)

alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS

**Timeline**

- **Disclosure Date**: 2013-02-04
- **Time to Exploit**: 52 days
- **Time to Vendor Response**: 7 days

**Description**

Multiple D-Link routers contain a flaw that is triggered when input passed via the 'cmd' parameter is not properly sanitized before being used in the command.php script. This may allow a remote attacker to execute arbitrary commands.

**Classification**

- **Location**: Remote / Network Access
- **Attack Type**: Input Manipulation
- **Impact**: Loss of Integrity
- **Solution**: Solution Unknown
- **Exploit**: Exploit Public
- **Disclosure**: Vendor Disputed, Third-party Verified
- **OSVDB**: Web Related

**Solution**

OSVDB is not currently aware of a solution for this vulnerability.

**Products**

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>D-Link Corporation/D-Link Systems, Inc.</td>
<td>2.12b02</td>
</tr>
<tr>
<td></td>
<td>2.13b01</td>
</tr>
<tr>
<td></td>
<td>2.14b01</td>
</tr>
<tr>
<td>DIR-300</td>
<td>2.12</td>
</tr>
<tr>
<td>DIR-600</td>
<td>2.13</td>
</tr>
</tbody>
</table>
HTTP Level Evasions

- HTTP is a very complex protocol
  - Many important sub-protocols/formats
    - URIs
    - Character sets
    - Media types of entities

- As a result
  - Hard to inspect
  - Very evasion prone
  - Extensive work required in IDS to deal with issues

- We will start to work on URI issues...
Obscure HTTP Methods

• “HEAD” instead of “GET”.
• RFC 2616:

9.4 HEAD

The HEAD method is identical to GET except that the server MUST NOT return a message-body in the response. The metainformation contained in the HTTP headers in response to a HEAD request SHOULD be identical to the information sent in response to a GET request. This method can be used for obtaining metainformation about the entity implied by the request without transferring the entity-body itself. This method is often used for testing hypertext links for validity, accessibility, and recent modification.
Pipelining of Requests

• If IDS doesn’t properly reassemble TCP and parse protocol:

```
GET foo.html HTTP/1.1
GET bar.html HTTP/1.1
```

• Could miss the “bar.html”
• Have seen commercial products with this issue recently...
Directory Type Evasions

• Suppose IDS looking for “/servlet/command.php” in URL

• So attackers might try:
  – /servlet//command.php
  – /servlet///command.php
  – /servlet/./command.php
  – /servlet/././command.php
  – /servlet/subdir/..command.php

• On Windows based web servers:
  – /servlet\command.php
URL Encoding

• RFC 2396 specifies URL format:

  2.4.1. Escaped Encoding

  An escaped octet is encoded as a character triplet, consisting of the percent character "%" followed by the two hexadecimal digits representing the octet code. For example, "%20" is the escaped encoding for the US-ASCII space character.

    escaped  = "%" hex hex
    hex      = digit | "A" | "B" | "C" | "D" | "E" | "F" |
               | "a" | "b" | "c" | "d" | "e" | "f"

• And RFC 2616 says:

  The Request-URI is transmitted in the format specified in section 3.2.1. If the Request-URI is encoded using the "% HEX HEX" encoding [42], the origin server MUST decode the Request-URI in order to properly interpret the request. Servers SHOULD respond to invalid Request-URIs with an appropriate status code.

• So IDS must do the same...
Double Percent Encoding

• %25 is ‘%’ in ASCII
• %41 is ‘A’
• So if you write %2541 and decode once
  – you get %41
• Decode again
  – you get ‘A’
• Unbelievably, IIS did this...
  – IDS must follow...
Double Nibble Hex Encoding

• %34%31
• On first decoding goes to %41
• On second decoding goes to A
• Again, Microsoft IIS supported this encoding
• Also variations like %341 and %4%31
  • Also get correctly transformed to A
– Not a current issue by default
Loose Implementations

• RFC says:
  – Method <space> URI <space> HTTP/ Version CRLF CRLF

• But some Apache versions allow
  – Method <tab> URI <tab> HTTP/ Version CRLF CRLF

• IDS must follow implementations exactly, or attacker can fool
Case Insensitivity of Windows

- /SerVLeT/ComMaNd.Php
- May well work fine if underlying OS is case insensitive
- IDS must match behavior of target
Web Drive-By Download Attacks

• Have been the main action since then.
• Attacker response to firewall/IPS technology.
  – Largely circumvents those defenses.
  – Took a while to develop useful defenses.
    • Still a very active arms-race.
Two Main Schemas

• Scan/Compromise legit websites
  – Eg SQL Injection attacks
  – Insert <iframe>s into site
  – Iframes include content from an exploit server

• Malverts
  – Malicious ads bought through chains of middle men
  – Redirects to malicious content (often swf (Flash))
Either Way

- Exploit server runs an exploit kit
- Exploit kit tests nature of browser/plugins
  - Java
  - PDF
  - Flash
- Picks one or more exploit objects
- Takes control of browser/plugins
- Installs malware/trojans
- Command and control for instructions
- Exploit kits often have extensive management infrastructure
- Profit!
Also, social engineering

- Trick humans into installing/running malware
- Also works pretty well
- Let’s look at a few examples
Fake AV

Microsoft Security Warning
Antivirus 360 Web Scanner detected dangerous spyware on your system!
Detected malicious programs can damage your computer and compromise your privacy. It is **strongly recommended** to remove them immediately.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Risk level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware.IEMonster.b</td>
<td>Spyware</td>
<td>CRITICAL</td>
</tr>
<tr>
<td>Zlob.PornAdvertiser.Xplicit</td>
<td>Spyware</td>
<td>High</td>
</tr>
<tr>
<td>Trojan.InfoStealer.Banker.s</td>
<td>Trojan</td>
<td>Medium</td>
</tr>
</tbody>
</table>
More Social Engineering

And More