Side Channel Vulnerabilities on the Web - Detection and Prevention

Sebastian Schinzel
Virtual Forge GmbH
University of Mannheim
sebastian.schinzel@virtualforge.de

Copyright 2007 © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.

The OWASP Foundation
http://www.owasp.org
Agenda

- Background side channel vulnerabilities
- Side channel vulnerabilities on the Web
- Timing Side Channels
  - Detection
  - Attack
  - Prevention
- Storage Side Channels
  - Detection
  - Attack
  - Prevention
- Conclusion
Background side channel vulnerabilities

- Intrusive attacks against software systems well researched
- Vulnerabilities in real systems appear if developers don’t apply countermeasures
- Besides: what can attackers still do..?
- Side channel vulnerabilities allow attackers to infer potentially sensitive information just by observing normal behavior of software system
Agenda

- Background side channel vulnerabilities
- Side channel vulnerabilities on the Web
- Timing Side Channels
  - Detection
  - Attack
  - Prevention
- Storage Side Channels
  - Detection
  - Attack
  - Prevention
- Conclusion
Side channel vulnerabilities on the Web

Learn what a user types by observing
  ▶ reflections of monitor picture [1]
  ▶ inter-packet timing in encrypted SSH session [2]

Learn about the action a user performs on a Web application by observing packet sizes in encrypted Web traffic [3]
Side channel vulnerabilities on the Web

- Learn existence of user name from
  - response time of Web application [4]
  - error messages in Web page

- Timing related
  - Learn private key of SSL server [5]
  - Learn amount of hidden images in Gallery [4]
Agenda

- Background side channel vulnerabilities
- Side channel vulnerabilities on the Web
- Timing Side Channels
  - Detection
  - Attack
  - Prevention
- Storage Side Channels
  - Detection
  - Attack
  - Prevention
- Conclusion
Timing Side Channels

Example control flow of login form

- Different control flow depending on whether user name exists
- Control flow have different length and therefore different execution time
- Can we measure this time difference?
Timing Side Channels

Detection and Attack

- Density
- Response Time (ms)

Min: 34
Max: 150
Avg: 39
Med: 37
Timing Side Channels

Preventing timing side channels (white box)

- Change control flow so that paths have same length, e.g.
  - Pad short control paths
Timing Side Channels

Preventing timing side channels (white box)

- Join control paths, e.g.
  - Pack all db queries in one SQL statement

User exists AND Password correct AND User not locked AND User not expired?
Agenda

- Background side channel vulnerabilities
- Side channel vulnerabilities on the Web
- Timing Side Channels
  - Detection
  - Attack
  - Prevention
- Storage Side Channels
  - Detection
  - Attack
  - Prevention
- Conclusion
Storage Side Channels

Example for obvious storage side channel: Error messages of login form

- “Invalid user name” → user name does not exist
- “Invalid password” → user name exists
Storage Side Channels

- **Hidden** storage side channel: Secret-dependent differences that are invisible to "normal user"
  - HTTP headers and values
  - HTML meta data
  - ...

Side Channel Vulnerabilities on the Web - Detection and Prevention, Sebastian Schinzel
Storage Side Channels

- Noise is a problem for measurements
  - lots of dynamic content in HTTP/HTML

```bash
$ diff responses/1.content responses/3.content
2c2
< Date: Tue, 22 Jun 2010 17:20:31 GMT
---
> Date: Tue, 22 Jun 2010 17:20:37 GMT
8c8
< Last-Modified: Tue, 22 Jun 2010 17:20:34 GMT
---
> Last-Modified: Tue, 22 Jun 2010 17:20:38 GMT
122c122
<   <input type="hidden" name="challenge" value="35018d1af7184bad10944cb617677c99" />
---
>   <input type="hidden" name="challenge" value="b50cbc351f525fcad0cb0fc97e080b29" />
```

Time dependent difference

Randomly generated difference
Storage Side Channels

- Widely used Content Management System leaks information by HTTP header ordering

<table>
<thead>
<tr>
<th>Non-existent user name (s=0)</th>
<th>Existing user name (s=1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP/1.1 200 OK</td>
<td>HTTP/1.1 200 OK</td>
</tr>
<tr>
<td>Date: Mon, 25 Jan 2010 11:47:55 GMT</td>
<td>Date: Mon, 25 Jan 2010 11:47:55 GMT</td>
</tr>
<tr>
<td>Server: Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny4 with Suhosin-Patch</td>
<td>Server: Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny4 with Suhosin-Patch</td>
</tr>
<tr>
<td>X-Powered-By: PHP/5.2.6-1+lenny4</td>
<td>X-Powered-By: PHP/5.2.6-1+lenny4</td>
</tr>
<tr>
<td>Expires: Thu, 19 Nov 1981 08:52:00 GMT</td>
<td>Expires: 0</td>
</tr>
<tr>
<td>Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0</td>
<td>Cache-Control: no-cache, must-revalidate, post-check=0, pre-check=0</td>
</tr>
<tr>
<td>Pragma: no-cache</td>
<td>Pragma: no-cache</td>
</tr>
<tr>
<td>Vary: Accept-Encoding</td>
<td>Vary: Accept-Encoding</td>
</tr>
<tr>
<td>Content-Type: text/html;charset=iso-8859-1</td>
<td>Content-Type: text/html;charset=iso-8859-1</td>
</tr>
<tr>
<td>Content-Length: 5472</td>
<td>Content-Length: 5472</td>
</tr>
</tbody>
</table>
Storage Side Channels

Online gallery leaks the amount of private pictures:

7 public images, 0 private image \((s=0)\)

```html
<div style='float:left'>Pictures -
  <a href='display.php?t=bycat&amp;q=4&amp;nr=7&amp;st=0&amp;upto=12&amp;p=1'>
    <span style='color:#fff'>Other</span>
  </a>
</div>
```

7 public images, 1 private image \((s=1)\)

```html
<div style='float:left'>Pictures -
  <a href='display.php?t=bycat&amp;q=4&amp;nr=8&amp;st=0&amp;upto=12&amp;p=1'>
    <span style='color:#fff'>Other</span>
  </a>
</div>
```
Agenda

- Background side channel vulnerabilities
- Side channel vulnerabilities on the Web
- Timing Side Channels
  - Detection
  - Attack
  - Prevention
- Storage Side Channels
  - Detection
  - Attack
  - Prevention
- Conclusion
Bibliography


[4]: Andrew Bortz and Dan Boneh, Exposing private information by timing web applications, WWW, pp. 621-628, ACM, 2007

Conclusion

- Side channel vulnerabilities pose a serious threat for Web applications with high security requirements
- Side channels can appear in various ways
  - Detection is difficult
- Side channel attacks are passive
  - Attacks are feasible for a skilled attacker
- Prevention strategies may have a negative impact on system performance
  - Prevention is difficult
Thank you for your attention!

Critique, feedback, discussion?

Contact:
Sebastian Schinzel
ssc@seecurity.org