Who am I?

- Senior Application Security Engineer
  @ Aspect Security
- Creator & Leader OWASP AppSensor
- Security Blogger
  - http://michael-coates.blogspot.com
- Life Outside Security?
  - Motorcycle, Triathlons
SSL: Super Shiny Locks
Padlock != Secure
SSL Growth

> 1 Million SSL Certificates
The Good

- Confidentiality
- Integrity
- Replay Protection
- End Point Authentication
The Bad - Usability

The security certificate presented by this website was not issued by a trusted certificate authority.

The security certificate presented by this website was issued for a different website's address.
The Bad – User Expectations

- How did you get to the site?
- Is HTTPS in the URL?
- Are those zeros or o’s?
- Did you get any browser warning messages?
- Did you click “ok” or “accept” to any popup boxes?

“I've told many people about the https and they didn't know!” – dad
The Bad – Websites are Configured Wrong!

■ Scenario 1: Non-SSL Landing Page

```
<form method="POST" action="https://mybank.com/login">
Username: <input type="text" name="user">
<br>
Password: <input type="password" name="pass">
<br>
</form>
```
Non-SSL Landing Page Attack

HTTP REQUEST
GET http://mybank.com

HTTP POST
POST http://mybank.com
user:Steven&pass:JOSHUA

...<form method="POST" action="https://mybank.com/login" >
...

mybank.com
The Bad – Websites are Configured Wrong!

- Scenario 2: HTTP to HTTPS redirects

![Image of a login page](https://mybank.com)
HTTP to HTTPS redirects

1. Get http://mybank.com
2. 302 Redirect
   Location: https://mybank.com
3. Get https://mybank.com
   SSL
   200 Found
HTTP to HTTPS redirects

Get http://mybank.com

302 Redirect
Location: https://mybank.com

http://mybank.com
https://securemybank.com
http://phishingsite.com
http://malware.com
The Bad – Websites are Configured Wrong!

Scenario 3: Mixed Content
The Bad – Not All SSL is equal

- **View Ciphers by Strength**
  
  ```bash
  openssl ciphers <strength> -v
  ```

- **Test Server:**
  
  ```bash
  openssl s_client -connect site.com:443 -cipher <strength>
  ```

- **Test Client:**
  
  ```bash
  openssl s_server -www -cert cacert.pem -key cakey.pem
  ```

**<strength>=NULL|LOW|MEDIUM|HIGH|FIPS**

---

**FIPS Approved Ciphers**
- ADH-AES256-SHA
- DHE-RSA-AES256-SHA
- DHE-DSS-AES256-SHA
- AES256-SHA
- ADH-AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-DSS-AES128-SHA
- AES128-SHA
- ADH-DES-CBC3-SHA
- EDH-RSA-DES-CBC3-SHA
- EDH-DSS-DES-CBC3-SHA
- DES-CBC3-SHA

**LOW Strength Ciphers**
- ADH-DES-CBC-SHA
- EDH-RSA-DES-CBC-SHA
- EDH-DSS-DES-CBC-SHA
- DES-CBC-SHA
- DES-CBC-MD5
The Ugly

- **MD5 Collision Rogue CA Creation**
  - Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, Benne de Weger

- **SSLstrip**

- **Null Prefix Attacks Against SSL/TLS Certificates**
  - Moxie Marlinspike
  - [http://www.thoughtcrime.org/software/sslstrip/](http://www.thoughtcrime.org/software/sslstrip/)
MD5 Collision Rogue CA

1. Root CA
2. MD5 Collision
3. Rogue CA

amazon.com
Null Prefix Attack

Part 1: Certificate Authority

- CA verifies ownership of root domain
  www.\textit{foo.com} = www.anything.\textit{foo.com} = nonexistent.a.b.c.\textit{foo.com}
- What about? amazon.com\textbackslash0.\textit{foo.com}

Part 2: Browser SSL Verification

- Microsoft CryptoAPI - \textbackslash0 is eos
  amazon.com = amazon.com\textbackslash0.\textit{foo.com}
- Vulnerable: “Firefox, Internet Explorer, Chrome, Thunderbird, Outlook, Evolution, Pidgin, AIM, irssi”
SSLstrip

- MitM SSL Connections
  - ARP Spoofing
  - IP Tables
- Auto Strip SSL -> HTTPS to HTTP
- Execute Null Prefix Attack
- Block Certificate Revocation Messages
  - OCSP Attacks
Is There Hope?

- Average User == Not Technical
- Most Deployments Vulnerable
- Specialized Tools Available
Doing It Right...

The Application
- SSL only
- No HTTP -> HTTPS redirects: HTTP shows “User Education” message
- No SSL errors or warnings

The User
- Bookmark the HTTPS page
- Stop if any SSL warnings/errors presented

The Browser
- Set realistic user expectations
- Provide “Secure” mode option
Internal Network SSL

- Protect the data on internal network too!
## Resources - ssllabs.com (Ivan Ristic)

### Recently Seen
- **amazon.com**
- **chase.com**
- **bankofamerica.com**
- **gmail.google.com**

### Recent Best-Rated
- **B (67) sparklit.com**
- **B (72) www.startssl.org**
- **C (60) ais2.uniba.sk**
- **C (64) blog.startcom.org**

### Recent Worst-Rated
- **A (91) webmail.verte.com.br**
- **A (88) webmail.stiefel.com**
- **A (88) www.kaching.com**
- **A (88) imperva.com**

#### SSL Report: **amazon.com** (72.21.207.65)

**Summary**

![SSL Summary Graph]

- **Overall Rating**: B (67)
- **Certificate**: 100
- **Protocol Support**: 55
- **Key Exchange**: 90
- **Cipher Strengths**: 60

*The scores are explained in the SSL Server Rating Guide 2010.*
Resources – sslfail.com (Tyler Reguly, Marcin Wielgoszewski)

Rogers Webmail SSLFail Follow-up

Posted by Tyler on July 21, 2009
SSLFail / No Comments

A while back we posted a screenshot of the Rogers Webmail SSLFail. I decided to follow up with Rogers to see if they were going to resolve the issue anytime soon. I contacted Rogers and asked them what was going on for the issue. A couple of days later I got the following reply:

WindowsUpdate SSL fails

Posted by roman on March 17, 2009
SSL Fail Images / No Comments

Temporary LinkedIn SSLFail!

Posted by Tyler on July 26, 2009
SSLFail / No Comments

We had an interesting screen shot sent in today from Sheldon (his post on the wall). It appears as though the SSL certificate on LinkedIn expired today and they waited until after the expiration to update their cert, leaving people with SSL errors temporarily. This doesn’t seem like a great way to foster user trust. I’d prefer my sites update their certificates early, rather than wait for them to expire. If this was a matter of they forgot the date and weren’t ready for the expiration, then I’m really concerned, that mistake should not happen - especially with a site that I trust with so much of my personal information.
Thanks

Questions:

Lobby –or–

michael.coates@aspectsecurity.com –or–

http://michael-coates.blogspot.com