Breaking the Security Myths of Extended Validation SSL Certificates

Alexander Sotirov

phreedom.org

Mike Zusman

intrepidusgroup.com

Introduction

- SSL certificate authorities have been thoroughly broken in the last year or two
- EV-SSL is often seen as a stronger assurance of site security
- If SSL is broken, can we trust EV-SSL?
- No! A rogue non-EV certificate can be used to do MITM attacks against EV sites

Organization

- State of the SSL PKI
- EV to the rescue
- Breaking EV certificates
  - mixed content attacks
  - same origin attacks
  - SSL rebinding
  - cache poisoning
- Fixing this mess

Part 1

State of the SSL PKI

Race to the bottom

1999

- 51 trusted root certificate authorities
- $895 certificates
- fax company information, wait multiple days

2009

- 136 trusted root certificate authorities
- free 90-day certificates, issued automatically
- all you need is an email address in the domain

```
webmaster@example.com
info@example.com
...
```

Breaking Certificate Authorities

- No validation at all
  - Comodo resellers
- Breaking domain validation
  - CA web application flaws
  - sslcertificates@live.com gets you a cert for login.live.com
  - Null-bytes in domain names
- Crypto attacks
  - MD5 collision attack against RapidSSL
  - SHA-1 attacks rapidly improving

Who watches the watchmen?

- Browser vendors have failed to enforce CA security standards
  - Despite multiple security failures, no CA has ever been removed from a browser
  - CA security outsourced to WebTrust
- WebTrust certification is run by accountants, not security professionals
  - No web application pentesting
  - No enforcement of crypto standards
  - They get paid by the CAs they certify

Part II

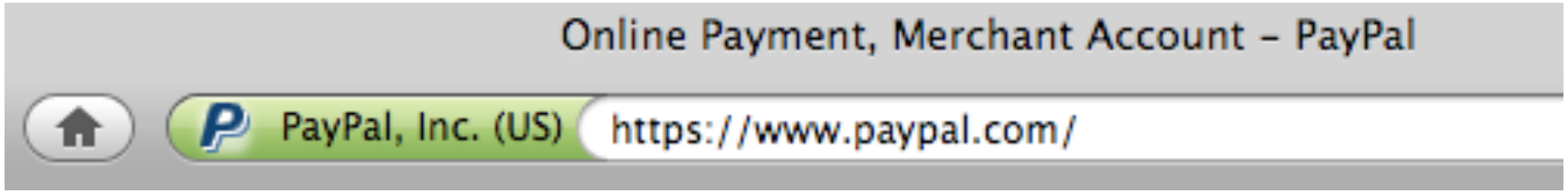
Extended Validation Certificates

EV to the rescue

EV certificates have stronger validation and make it easier for users to trust a site.

CA/Browser Forum sets the requirements:

- extensive legal identity validation
- no MD5 or 1024-bit RSA after 2010
- mandatory support for CRL or OSCP



EV goals

1. Identify the legal entity that controls a website
2. Provide stronger validation than the email domain validation
3. Enable encrypted communication
4. Prevent phishing with SSL certs like www.paypal.com.blahblahblah.evil.com

EV marketing

"The increasing awareness to this problem has presented an opportunity to e-commerce providers to **capitalize on consumer fears** by displaying trust indicators"

Comodo

"The green address bar in Internet Explorer 7 means that this website is an EV website and has gone through extra rigorous steps with an authorized certificate authority to prove they are a **secure site**."

Thawte

Flawed assumptions

- The CA/Browser forum assumed that regular SSL is trustworthy
- We now know that regular SSL is broken
- EV security is undermined as well

EV reality

1. Identify the legal entity that controls a website
2. Provide stronger validation than the email domain validation
3. Enable encrypted communication
4. Prevent phishing with SSL certs like www.paypal.com.blahblahblah.evil.com

Part 3

Breaking EV certificates

Assumptions

- Attacker has a non-EV certificate for the target domain
  - rogue cert created using an MD5 collision
  - own the email server for target domain
  - exploit the CA validation system
- Attacker can intercept and tamper with SSL connections to the website
  - ARP spoofing on a local network
  - open 802.11 access points
  - DNS spoofing of the target domain

Attacks

Multiple attack vectors allow MITM attacks:

- Mixed content on EV sites
- Same origin JavaScript injection
- SSL rebinding
- SSL cache poisoning

Mixed content policy

Browsers allow EV sites to load JavaScript or CSS content from non-EV servers:

- https://www.paypal.com uses EV, but it loads JavaScript from https://www.paypalobjects.com/global.js
- Every EV site that uses Google Analytics loads https://ssl.google-analytics.com/ga.js

MITM with mixed content

1. The user requests https://www.paypal.com/, which is served with an EV certificate and is displayed with a green bar
2. The page includes a script from https://www.paypalobjects.com/global.js
3. We MITM the connection to www.paypalobjects.com with a non-EV certificate and inject our script
4. The script allows us to modify the page, capture keystrokes, intercept form submissions

MITM with mixed content

What if the site used an EV certificate for both paypal.com and paypalobjects.com?

It doesn’t matter, the attack still works!

We can replace an EV cert with a non-EV and the browser won’t care.

Same origin policy

The same origin policy doesn't distinguish between EV and non-EV sites (this attack was described by Collin Jackson and Adam Barth in 2008)

An attacker can MITM one connection with a non-EV certificate and inject JavaScript into pages loaded with an EV certificate.

MITM with same origin

1. The user requests https://www.paypal.com/
2. We MITM the connection and return HTML that opens https://www.paypal.com/popup.html as a popup
3. We MITM the second connection and return HTML that refreshes the popup's parent window
4. The browser requests https://www.paypal.com/ again and we let the connection through to the real EV server. The browser shows a green bar.
5. The popup injects JavaScript into the page and closes itself.

SSL rebinding

Browsers don’t care if the SSL certificate for a website changes from one connection to the next.

Switching from non-EV to EV:

- JavaScript injection on the previous slide

Switching from EV to non-EV:

- steal session cookies and form data
- no JavaScript or popups required

MITM with SSL rebinding

1. The user requests https://www.paypal.com/
2. We MITM the connection, capture the cookies and any submitted form data, and return HTML that immediately refreshes itself
3. The browser requests https://www.paypal.com/ again and we let the connection through to the real EV server. The browser shows a green bar.
4. We repeat steps 1-3 for each new SSL connection the browser opens.

Demo

SSL rebinding against an EV protected site

SSL cache poisoning

If we cache content with a non-EV certificate and the EV site responds with a 304, the browser will show the green bar.

- The attacker can use a non-EV certificate to poison the cache for an EV site
- We can use an iframe on a HTTP site: no need for the user to visit the target site
- The attacker controls the poisoned EV site even when the user returns to a trusted network that cannot be MITMed

MITM with SSL cache poisoning

1. The user requests http://www.google.com/
2. We modify the HTML and inject an iframe that loads https://www.paypalobjects.com/foo.js
3. We MITM the SSL connection and return our JavaScript with Last-Modified header set to 2010, Expires header set to 2011 and Cache-Control: public
4. Every time an SSL website requests this URL with a If-Modified-Since header, the server will return a 304 Not Modified response

Demo

SSL cache poisoning of an EV protected site

Impact of attacks

1. Identify the legal entity that controls a website
2. Provide stronger validation than the email domain validation
3. Enable encrypted communication
4. Prevent phishing with SSL certs like www.paypal.com.blahblahblah.evil.com

Part 4

Fixing EV

Is this really a problem?

- "EV was only designed to stop phishing, so it is not broken"
- If the attacker can do a MITM attack on SSL, they don't need to do phishing!
- Without MITM protection, the green bar is nothing but snake oil.

Fixing EV

Unrealistic solutions:

- Drop support for non-EV certificates
- Make non-EV certificates trustworthy again (how?)

We need a solution that allows EV sites to coexist with broken non-EV certificates

Mixed content policy

Do not allow EV sites to load content from server with non-EV content

- Opera is the only browser that tried to do this, but they backed off
- mixed content should break EV sites

Same origin policy

The origin of a document must include an EV indicator

- Prevents JavaScript injection from non-EV to EV sites
- Collin Jackson and Adam Barth suggest httpev:// vs. https://
- there’s no need to expose this to the user, it can be an internal flag

SSL rebinding

Solution:

- Don’t allow multiple SSL certificates for a domain during a browser session

Many deployment problems:

- how do you upgrade certs on a server?
- load balancing and content delivery networks may use multiple SSL certs

SSL rebinding

Better solution:

- don’t allow switching from an EV to a non-EV certificate for a domain during a browser session

Cache poisoning

Fixing the mixed content policy, same origin policy and SSL rebinding is not enough.

Fixing cache poisoning:

- discard cached content from non-EV sites when going to an EV site

Part 5

Conclusion

Conclusion

- The state of SSL PKI is dismal
- EV certificates prevent basic phishing attacks, but fail against MITM attacks
- We need a focused effort from the CA/ Browser forum and especially the browser vendors to fix this

Questions?

alex@sotirov.net
mike.zusman@intrepidusgroup.com