BlackHat Briefings, 2009

Breaking the Myths of Extended Validation SSL Certificates

Alexander Sotirov
phmsecurity.com

Mike Zusman
intrepidusgroup.com

Introduction

- Chosen-prefix MD5 collisions allowed us to create a rogue Certificate Authority and issue arbitrary certificates
- Our team, as well as browser vendors and CAs believed that EV certificates were not affected. We were wrong!
- A rogue non-EV certificate can be used to do MITM attacks against an EV site

Previous work

- *Beware of Finer-Grained Origins* by Collin Jackson and Adam Barth, May 2008http://crypto.stanford.edu/websec/origins/

- Nobody brought this paper up when we presented our MD5 attack and few people realized its full impact

- Today we'll present some more advanced attacks on EV and talk about mitigations

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
- Breaking domain validation
  - DNS spoofing of the MX record for a domain
  - CA Web Application Flaws
  - sslcertificates@live.com owns login.live.com
- Crypto attacks
  - RSA signature forgery with exponent 3
  - MD5 collision attack against RapidSSL

MD5 collision attack

Outline of the attack:

- Generate two X.509 certificates with different contents and the same MD5 hash
- Get a CA to sign the “legit” certificate
- Copy the signature into the “rogue” cert

Results:

- Rogue intermediate CA signed by the RapidSSL root CA
- Ability to sign arbitrary certificates

MD5 collision attack

Challenges:

- Predict the serial number of a certificate 3 days in advance of time T
- Generate a collision in less than 3 days
- Get the certificate signed at time T

Paper with crypto details:

http://eprint.iacr.org/2009/111

Part II

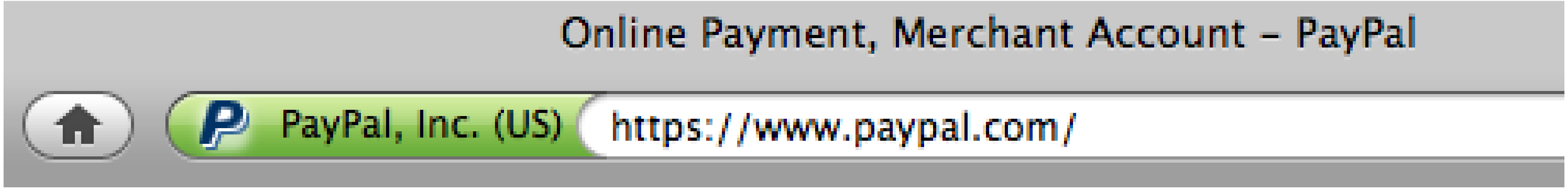
Extended Validation Certificates

EV to the rescue

CA/Browser Forum sets the requirements:

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

Common EV indicators adopted by browsers:



Online Payment, Merchant Account – PayPal

EV goals

1. Identify the legal entity that controls a website
2. Enable encrypted communication
3. Prevent phishing attacks
   - solve the problem of weak domain validation when issuing certificates
   - solve the problem of issuing SSL certs for www.bank.com.blahblahblah.evil.com
   - make it easier to investigate phishing

EV and MD5 collisions

- Browsers require EV certs to chain to a known EV root certificate
- RapidSSL is not an EV root
- None of the EV roots have ever used MD5 to sign certificates
- Unaffected by the MD5 collision attack?

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

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!

Same origin policy

The same origin policy doesn’t distinguish between EV and non-EV certificates (this is the Collin Jackson and Adam Barth attack)

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

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. Enable encrypted communication
3. Prevent phishing attacks
   - solve the problem of weak domain validation when issuing certificates
   - solve the problem of issuing SSL certs for www.paypal.com.blahblahblah.evil.com
   - make it easier to investigate phishing

Part 4

Fixing EV

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 currently does this, but it simply treats the site as non-EV and still displays it
- mixed content should break EV sites

Same origin policy

The origin of a document must include an EV indicator

- 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

Alternative solution:

- don’t allow switching between EV and non-EV certificates for a domain during a browser session

Problems:

- browser sessions could last months
- how do you upgrade from non-EV to EV certificates without breaking all current sessions?

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 solve the identity problem, but fail against MITM attacks
- We need a focused effort from the browser vendors to fix this

Questions?

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