Criminal charges are not pursued: Hacking PKI

Mike Zusman
Principal Consultant
mike.zusman@intrepidusgroup.com
About the Title

☐ From StartCom Critical Event Report
  ■ https://blog.startcom.org/?p=161

☐ Thanks to StartCom for quickly fixing the bug I found
  ■ These guys care about PKI!
Outline

- Intro – The Basics
- CA Domain Validation Mechanisms
- Certificate Provisioning Process
- Web Application Attacks
- Client Side Countermeasures
- CA Countermeasures
- Closing
Intro – SSL vs SSL PKI

- SSL is a sound encryption protocol
  - ...implementation specific bugs, aside
    - Debian PRNG
    - Microsoft SSL PCT Overflow (2004)

- SSL PKI gives us third party trust
  - Site validation
  - Code signing
  - Personal certificates
Intro – Threat Modeling SSL PKI

SSL PKI Threat Model

- Identity Spoofing Threats
- Threats Against Encrypted Traffic
- Certificate Authority Threats
- SSL Client Threats
- SSL Server Threats
- Protected Private Key Threats
Intro - Threat Modeling SSL PKI

SSL PKI Threat Model

Identity Spoofing Threats

- Fraudulent Certificate
- Stolen Certificate
- Invalid Certificate
- Use of revoked certificate
- Forced Root CA Installation
- International Domain Name attacks

Compromise Encrypted Traffic

- MITM
- Use Fraudulent Certificate
- Steal Key from Web Server
- Use Invalid Certificate
- Social Engineering
- Passively Sniff
- Exploit Browser Behavior
- Block OCSP/CRL
- Prevent Encryption
- Exploit Browser Behavior
- Social Engineering of the client

Certificate Authority Threats

- Insider Attacks
- Issue legitimate certificates without validation
- Weaponized CSR
- Binary exploitation of the CA validation mechanism
- Web Application Hacks
- Outsider exploits web application vulnerabilities to by-pass validation
- Social Engineering
- Lax Validation Requirements
- MD5 Attacks
- MD5 Collisions

SSL Client Threats

- Weaponized CRL
- Binary exploitation of the client
- Weaponized Public Keys
- Binary exploitation of the client
- Social Engineering
- Vague SSL Error Messages
- Rogue Certificate Authorities
- Trust malicious CA for “enhanced security”
- Domain Validation
- Domain name mismatch
- Exploit poor SSL Validation
- Binary exploitation on installation
- Weaponized Root Certificate
- Binary Exploitation on validation of signed public key

SSL Server Threats

- Attack CSR Generation Mechanism
- Binary Exploitation of SSL library (OpenSSL/Microsoft CA)
- Attack SSL Handshake
- Binary Exploitation of SSL library
- Attack Application
- Attack is hidden inside SSL encrypted packets
- Attack Proxy Capabilities
- Server becomes an SSL client

Protected Private Key Threats

- Offline Brute force Attack (Weak Debian Keys)
- Web Application Vulnerabilities
Intro – Why hack PKI?

- To exploit third-party trust
  - Maybe you own the DNS
  - Steal data with minimal residue
    - Targeted Attacks
    - SSL VPN
  - If software vendors do their job, endpoints will be harder to attack
  - It’s fun! 😊
Intro – PKI’s Low Hanging Fruit

- Certification Authority Web Sites
  - You pay money for private key access
  - Private key access is controlled by web application logic
  - Web Applications are hard to secure

- Oh, the irony!
  - The companies that sell security are not secure themselves
  - How can you secure the Internet, over the Internet?
Intro – Soft Targets

- Where there is smoke, there is usually fire

- Introducing, a slide-show of insecurity...
* Note the green bar. It is definitely COMODO who is vulnerable to cross site scripting!
Website Identity Assured at 09-Apr 2009 18:48:25

http://www.completessl.com/ has been validated and is authentic. Please ensure the following credentials match the site you are currently visiting:

<table>
<thead>
<tr>
<th>Company:</th>
<th>CompleteSSL Security Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL:</td>
<td><a href="http://www.completessl.com/">http://www.completessl.com/</a></td>
</tr>
<tr>
<td>Address:</td>
<td>12 Tammie Ann Drive. East Hampton, CT, 06424, United States</td>
</tr>
<tr>
<td>Telephone:</td>
<td>860-256-4502</td>
</tr>
<tr>
<td>Fax:</td>
<td>203-286-2408</td>
</tr>
<tr>
<td>Email Contact:</td>
<td><a href="mailto:sales@completessl.com">sales@completessl.com</a></td>
</tr>
</tbody>
</table>
Intro - Soft Targets

Exception occurred: ORA-06502: PL/SQL: numeric or value error: NULL index table key value
Intro - Soft Targets

GasQuery

こんにちは、こちらはAXISサービスです！ / [en]-(Hi there, this is an AXIS service!)
おそらくここにサービスを呼出すためのフォームが存在します... / [en]-(Perhaps there will be a form for invoking the service here...)
Intro - Soft Targets

<xssed>
xss attacks information
</xssed>

VeriSign SSL Certificates
Get the strongest SSL from VeriSign
Protect Important Data - Learn More
www.Verisign.com

Vulnerability Audits
Network Vulnerability Audits. Free Trial -
Audit your Network Today.
vulnerability.audits.qualys.com

Results for "verisign" (limited to 20 entries per section)
XSS:
blogs.verisign.com XSS vulnerability notified by Zeitjak
knowledge.verisign.com XSS vulnerability notified by Zeitjak
foreseeresults.verisign.com XSS vulnerability notified by Zeitjak
servicecenter.verisign.com XSS vulnerability notified by Zeitjak
ispcenter.verisign.com XSS vulnerability notified by Zeitjak
search.verisign.com.au XSS vulnerability notified by Harry Sintonen
verisign-versign.com XSS vulnerability notified by 314 IT -
Intro - Soft Targets
* Note the green bar. It is definitely THAWTE who is vulnerable to cross site scripting!
Intro - Soft Targets

Edit the node description in the space provided below. Press "update" to commit your changes.

Title: B [redacted] Inm, Inc.

Description: [redacted] Inm, Inc.

Invoice Tax Number: Please fill in the company tax number. These details are required for inclusion on all tax invoices. If you do not have a company tax number, please make sure you click the button next to 'I do not have a company tax number'.

- [ ] 32-[redacted]-2
- [ ] I do not have a company tax number
Action Required - thawte certificate application approval

From: customers@thawte.com
Sent: Tue 7/29/08 9:40 AM
To: sslcertificates@live.com

Hi,

You have been identified as the authorizing contact person for a thawte digital certificate that will be issued to LOGIN.LIVE.COM

As the authorizing contact for this order, you are required to approve this application by clicking on the link provided below: This order will only be completed once you have approved the application. Following your approval, the technical contact will receive an e-mail containing further instructions on how to activate the certificate.

To approve this application please click here and follow the two-step process:
https://www.thawte.com/process/retail/processSSL123Pickup?lang=en&secretCode=2660bc2cc006c094613d6b473df00c74

Should you require more information concerning the migration please contact our Technical Support Help Desk at support@thawte.com

Thank you for choosing thawte as your trusted partner. Kind regards,

Customer Support
Domain Validation
Domain Validation

- CAs need to make sure you are authorized to request certification
- A few different techniques
  - Phone Authentication
  - Email Authentication
- Both rely on secret codes
  - Attacker requests a certificate
  - CA sends secret to authorized contact
  - Only those who know the secret can authorize the request
Domain Validation

- How does a CA determine who is an authorized contact?
  - Out of band (but still on the Internet)
    - Email address and/or phone number from Domain Registration Records
  - Certificate Requestor can pick from a list of approved aliases
    - Webmaster, ssladmin, sslwebmaster, etc.
Domain Validation

☐ Choosing the Authorized Contact

■ Attack #1
☐ Take advantage of insecure protocols to alter domain registration data on the wire
☐ Controls relying on insecure protocols should not be considered out of band

■ Attack #2
☐ Take advantage of poor application logic
☐ Controls cannot rely on user-supplied data
Domain Validation

- Delivery of the shared secret
  - Over the phone
    - ?
  - Over email
    - More reliance on insecure protocols
    - Who determines what aliases are authorized to approve SSL certification?

- Multiple Opportunities for Attack
  - Sniff email on the wire
  - Break into an email account
  - Free email providers
Certificate Provisioning Process
Certificate Provisioning Process

- CAs want to make money
  - Automation lowers overhead and makes purchasing certificates easier for customers
  - “Race to the Bottom”
    - The easier it is to get a cert, the less we can trust them (Hello EV!)
  - Automation makes life easier on attackers
Certificate Provisioning Process

- Case Study: Chosen Pre-Fix Collisions
  - Attack against a CA yields a rogue Certificate Authority
  - Two weaknesses
    - Use of MD5
    - Researchers could control serial number and time stamp
  - Web Site automation provided a reliable mechanism for generating predictable SSL certificates
Certificate Provisioning Process

- Case Study: Chosen Pre-Fix Collisions

  - These would have helped

    - A strong CAPTCHA
      - Introduce a human element to the process

    - A random time delay
      - Prevent the requestor from controlling the time the certificate is issued.
Certificate Provisioning Process

- Case Study: No Validation
  - Comodo COMPLETELY disabled validation
    - This happened for one reseller (that we know of)
    - People who ordered certificates had them immediately issued
    - Result: a rogue certificate was issued for mozilla.org
  - Automation makes it easier to make $$$
    - It also makes it easy screw things up
Certificate Provisioning Process

The Black List

- CAs will use a black list to protect sensitive domains
- I know, for a fact, that Verisign.com is on some black lists 😊

Issues

- Who is on the black list?
- How do you get on the black list?
- Good for PayPal.com
- Bad for vpn.governmentcontractor.com
Real CA Attacks

-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDddPnxTxVV3dk0x+...
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQDddPnxTxVV3dk0x+9c82h6FPWtrk/
URb0CtTFEA4NA4GbZvVTO...
www.freebird.in/wp/wp-content/plugins/commentpower/pki/private.key - 2k -
Cached - Similar pages -

-----BEGIN RSA PRIVATE KEY-----
MIICWwIBAAKBgQDT7LTGGnMVU6OvnQ5TdXmGUL3jDLcqfB/gAq+iH0+ScEMyYb7Z...
ismm.dpi.inpe.br/col/dpi.inpe.br/banon-pc2@1905/2006/05.18.15.44/doc/conf/ssl.key/ca.key -
2k - Cached - Similar pages -
Certificate Authority Attacks

- Insecure Direct Object Reference
  - Used to by-pass StartCom Domain Validation
  - Most CAs that offer domain validation do so via email

Certificate Authority Attacks

Enter Domain Name

- Enter the domain name you want to have validated.
- You must be the owner of the top-level domain, sub domains are not supported.

http://intrepidusgroup.com

Continue »»
Certificate Authority Attacks

Select Verification Email

- Select the email address for verification of domain ownership from below.

Verification Email: 
- postmaster@intrepidusgroup.com
- hostmaster@intrepidusgroup.com
- webmaster@intrepidusgroup.com

Continue »
Certificate Authority Attacks

StartSSL™ Certificates

Raw View

Content-Type: application/x-www-form-urlencoded
Referer: https://www.startssl.com/
Content-Length: 126
Cookie: ig=en; ap=12; mn=Hide; STARTS=2522
rs=third_step_validation&rst=&rsrnd=122522&rsargs[]=mikezusman@gmail.com
Certificate Authority Attacks

StartSSL™ Certificates & Public Keys

Complete Validation

Enter the code into the text field below.

623sqrvd1r5glipi

Continue »»

Gmail - Your Authentication Code, 19 Dec 2008 11:57 - mikezusman@gmail.com - Mike Z. Usman

http://mail.google.com/mail/?shva=1#inbox

Facebook | Home

Chats
Sent Mail
Drafts (35)
All Mail
Spam (75)
Trash
Contacts
Tasks
Chat

Your Authentication Code, 19 Dec 2008 11:57

Start show details 4:57 PM (0 minutes ago)  Reply

This mail is intended for the person who requested verification of domain ownership at StartSSL™ (http://www.startssl.com).

Your verification code is 623sqrvd1r5glipi

Copy and paste this code now into the form at your open browser window.
Certificate Authority Attacks

- You have successfully authenticated domain "intrepidusgroup.com".
- You will be able to use this verification for the next 30 days, after which it expires and must be renewed.
Certificate Authority Attacks

StartSSL™ Certificates & Public Key

Tool Box  Certificates Wizard  Validations Wizard

Add Domains

- Select the top target domain name for your certificate.
- Note: Only domain names which were validated within the last 30 days are eligible for selection.

Domain: dishuplink.com  dishuplink.com  phishme.com  intrepidusgroup.com  paypal.com  verisign.com
Certificate Authority Attacks

- StartCom Post-Mortem
  - By-passed validation and received signed certificates for low-profile sites
  - By-passed validation for high-profile sites PayPal and Verisign
  - Certificates were not issued for PayPal & Verisign due to a BLACKLIST
Certificate Authority Attacks (2)

- Information Leakage
  - Used to by-pass domain validation with THAWTE Certificate Authority
  - Appeared to be a common theme on the THAWTE web site

Certificate Authority Attacks (2)

email address:

[ please enter the email address associated with one of the contacts specified in the Domain Registration (please ensure these details are visible online i.e. you have not chosen to keep the information hidden). Alternatively, please enter a standard email alias (like 'administrator' or 'webmaster') or enter another email address that is associated with the domain for which you are requesting the certificate. Please ensure that the email alias has been set up and is available for use before you submit this request. An email will be sent to this address to ask for authorization of the issuance of this certificate. ]

OR
choose a predetermined e-mail alias from this list:

[ alternatively match a pre-determined email alias with the domain for which you are requesting the certificate. Please select from the drop down list on the left. Please ensure that the email alias has been set up and is available for use before you submit this request. ]

chnical contact:

E: This person will receive technical issues with regard to the program (e.g. technical problems with the site).

person should preferably:

◆ be able to handle Technical Support
◆ have access to the server

Please select one:

admin
administrator
hostmaster
info
it
mis
ssladmin
ssladministrator
sslwebmaster
sysadmin
webmaster
Certificate Authority Attacks (2)

We have received a request for a SSL123 certificate to be issued to login.yahoo.com.

The authorizing email address must be listed on the Domain Registration or one of the alia

In order to issue the above request, we must update your email address to one of the follo

domainadmin@yahoo-inc.com

admin@yahoo.com
SSLadmin@yahoo.com
sysadmin@yahoo.com
webmaster@yahoo.com
administrator@yahoo.com
SSLeadministrates@yahoo.com
SSLCerts@yahoo.com
SSLCertificates@yahoo.com
info@yahoo.com
SSLwebmaster@yahoo.com
hostmaster@yahoo.com
support@yahoo.com
sales@yahoo.com
tech@yahoo.com
mail@yahoo.com
manager@yahoo.com
MIS@yahoo.com
IS@yahoo.com
IT@yahoo.com

You must make sure the email account has been set up and is available, or the authorizing
Hi,

You have been identified as the authorizing contact person for a thawte digital certificate that will be issued to LOGIN.LIVE.COM

As the authorizing contact for this order, you are required to approve this application by clicking on the link provided in this email.

This order will only be completed once you have approved the application. Following your approval, the technical department will send an e-mail containing further instructions on how to activate the certificate.

To approve this application please click here and follow the two-step process: https://www.thawte.com/process/retail/processSSL123Pickup?lang=en&secretCode=2660bc2cc006c094613d6b473df00c74

Should you require more information concerning the migration please contact our Technical Support Help Desk at support@thawte.com

Thank you for choosing thawte as your trusted partner. Kind regards,

Customer Support
Certificate Authority Attacks (2)

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issued To</strong></td>
<td>Login.live.com</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>login.live.com</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>login.live.com</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Go to <a href="http://www.thawte.com/repository/index.html">http://www.thawte.com/repository/index.html</a></td>
</tr>
<tr>
<td><strong>Issued By</strong></td>
<td>Thawte Consulting Inc</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>Thawte Consulting Inc</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>MSN-Passport</td>
</tr>
<tr>
<td><strong>Validity</strong></td>
<td></td>
</tr>
<tr>
<td>Issued On</td>
<td>7/28/2008</td>
</tr>
<tr>
<td>Expires On</td>
<td>7/29/2009</td>
</tr>
<tr>
<td><strong>Fingerprints</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issued To</strong></td>
<td>Login.live.com</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>login.live.com</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Microsoft Corporation</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>MSN-Passport</td>
</tr>
<tr>
<td><strong>Issued By</strong></td>
<td>VeriSign Class 3 Extended Validation SSL CA</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>VeriSign Class 3 Extended Validation SSL CA</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>VeriSign, Inc.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>VeriSign Trust Network</td>
</tr>
<tr>
<td><strong>Validity</strong></td>
<td></td>
</tr>
<tr>
<td>Issued On</td>
<td>6/18/2008</td>
</tr>
<tr>
<td>Expires On</td>
<td>7/20/2009</td>
</tr>
<tr>
<td><strong>Fingerprints</strong></td>
<td></td>
</tr>
</tbody>
</table>
Certificate Authority Attacks (2)

☐ Thawte Post-Mortem
  - Information Leakage
    - Staff
    - Web Site
    - Email
  - Live.com was added to their blacklist
  - Certificate was revoked
    - But I still promise not to use it for malicious activities
SSL PKI Relies on Insecure Protocols

Action Required - thawte certificate application approval

From: customers@thawte.com
Sent: Tue 7/29/08 9:40 AM
To: sslcertificates@live.com

Hi,

You have been identified as the authorizing contact person for a thawte digital certificate that will be issued to LOGIN.LIVE.COM.

As the authorizing contact for this order, you are required to approve this application by clicking on the link provided below.

This order will only be completed once you have approved the application. Following your approval, the technical contact will e-mail containing further instructions on how to activate the certificate.

To approve this application please click here and follow the two-step process:
https://www.thawte.com/process/retail/processSSL123Pickup?lang=en&secretCode=2660bc2cc006c094613d6b473df00c74

Should you require more information concerning the migration please contact our Technical Support Help Desk at support@thawte.com.

Thank you for choosing thawte as your trusted partner. Kind regards,

Customer Support
Certificate Authority Attacks (3)

- Demonstration
Post CA Exploitation

Linux Laptop

EVDO ext Antenna

2 Port Ethernet Hub
Using a DV certificate to spoof EV

- EV SSL & SSL Rebinding
  - Mixed Content policies do not distinguish DV SSL from EV SSL
  - SSL Rebinding attacks allow for EV MITM with only a valid DV certificate
  - Browsers cannot handle CA’s “tiers of trust”
  - How do we fix this going forward?
Client Side Countermeasures

- White Listing Public Keys
  - Perspectives Plug-in
    - Not perfect
  - Client side proxies to handle white listing is a better option
Recommendations for CAs

- Check out OWASP
  - Their materials are free
  - Make a donation

- Web App Sec 101
  - Inventory your web apps
  - Get them assessed (not SCANNED)
    - Penetration Test
    - Source Code Review
Thank you

- Questions?

- Mike.zusman@intrepidusgroup.com

- More SSL Proxy code and documentation on my blog.

- http://schmoil.blogspot.com