

# Criminal charges are not pursued: Hacking PKI

---

Mike Zusman

Principal Consultant

[mike.zusman@intrepidusgroup.com](mailto: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

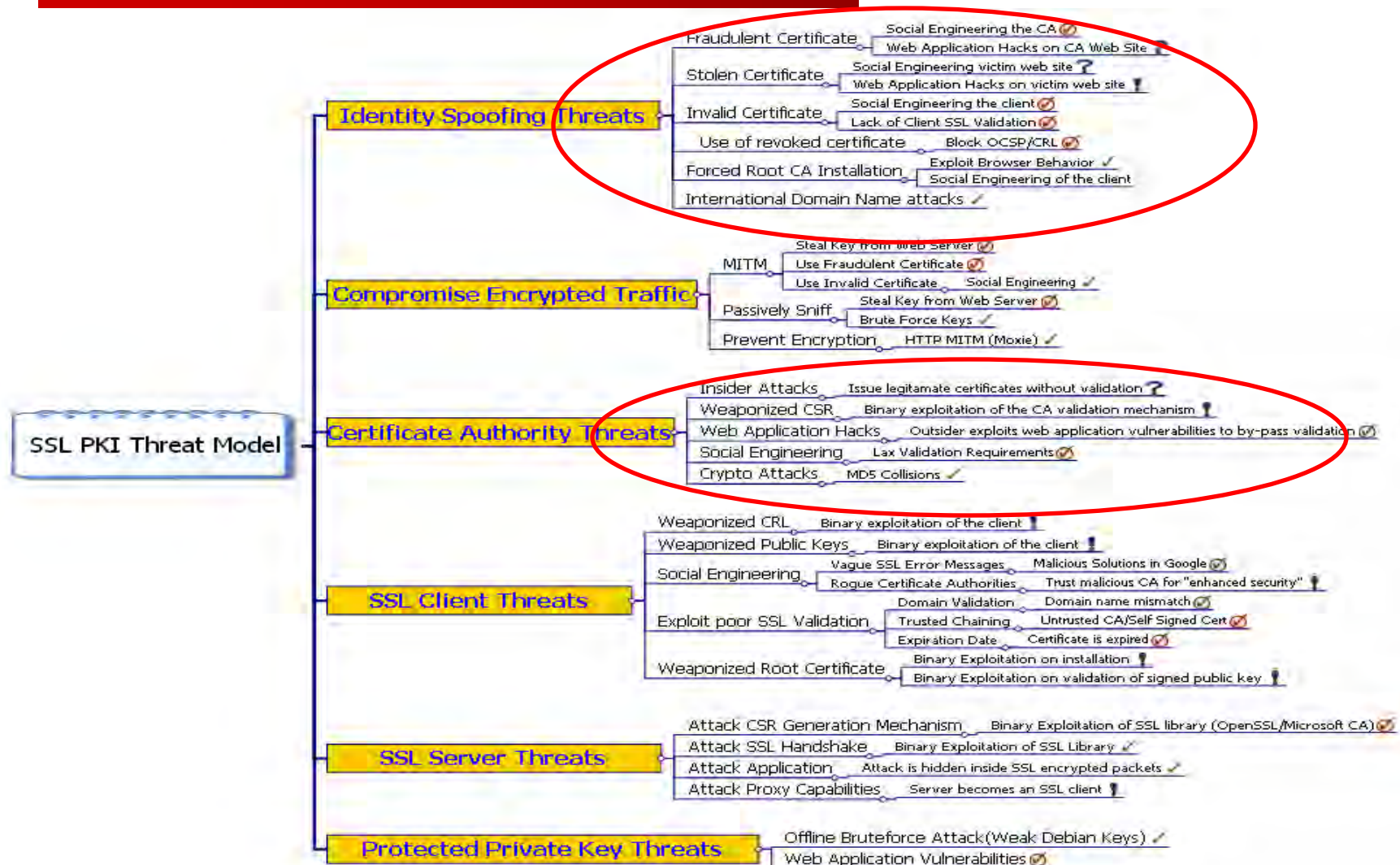
---

- 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



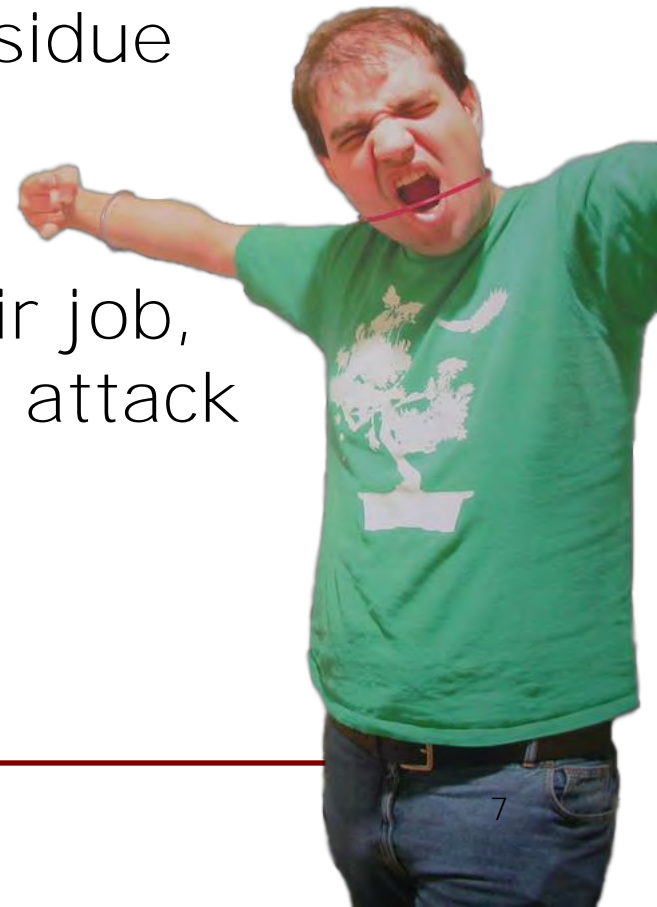
# Intro – Threat Modeling SSL PKI



# 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?



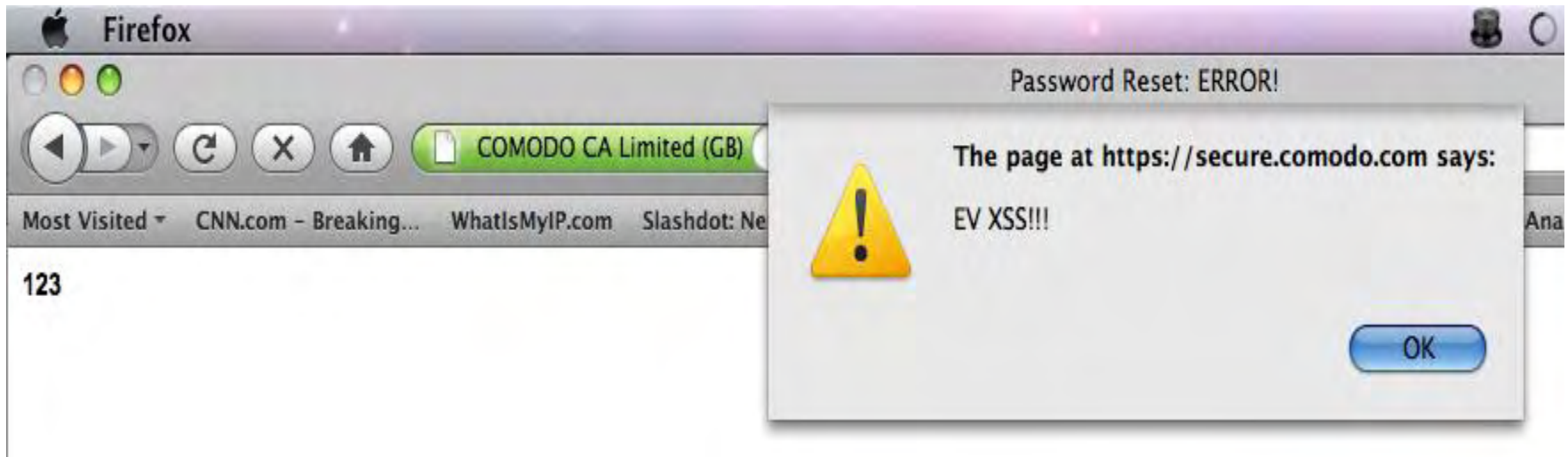
# Intro – Soft Targets

---

- Where there is smoke, there is usually fire
  
- Introducing, a slide-show of insecurity . . .

# Intro - Soft Targets

---




\* Note the green bar. It is definitely COMODO who is vulnerable to cross site scripting!

Safari File Edit View History Bookmarks Window Help

Site Credentials for <http://www.completessl.com/>

[https://www.trustlogo.com/ttb\\_searcher/trustlogo?v\\_querytype=](https://www.trustlogo.com/ttb_searcher/trustlogo?v_querytype=)

PhishMe Ma

 **Safari can't verify the identity of the website "www.trustlogo.com".**

The certificate for this website is invalid. You might be connecting to a website that is pretending to be "www.trustlogo.com" which could put your confidential information at risk. Would you like to connect to the website anyway?

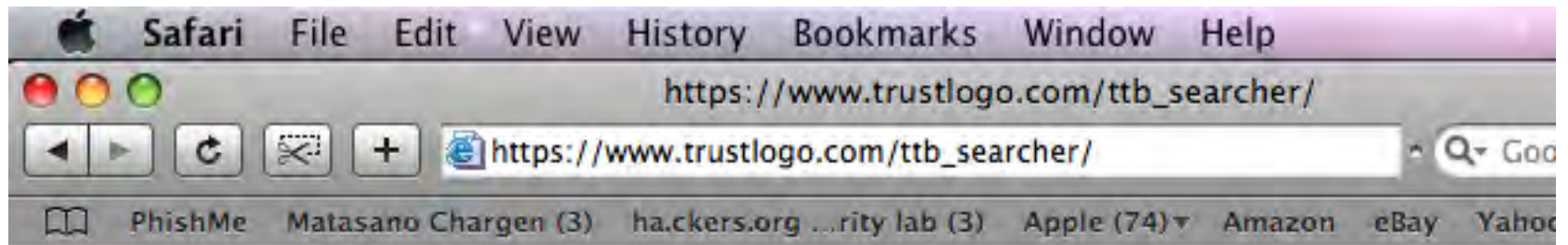
**Website Identity Assured at 09-Apr 2009 18:48:25**

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

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

# Intro - Soft Targets

---



Exception occured:ORA-06502: PL/SQL: numeric or value error: NULL index table key value

# Intro - Soft Targets

---





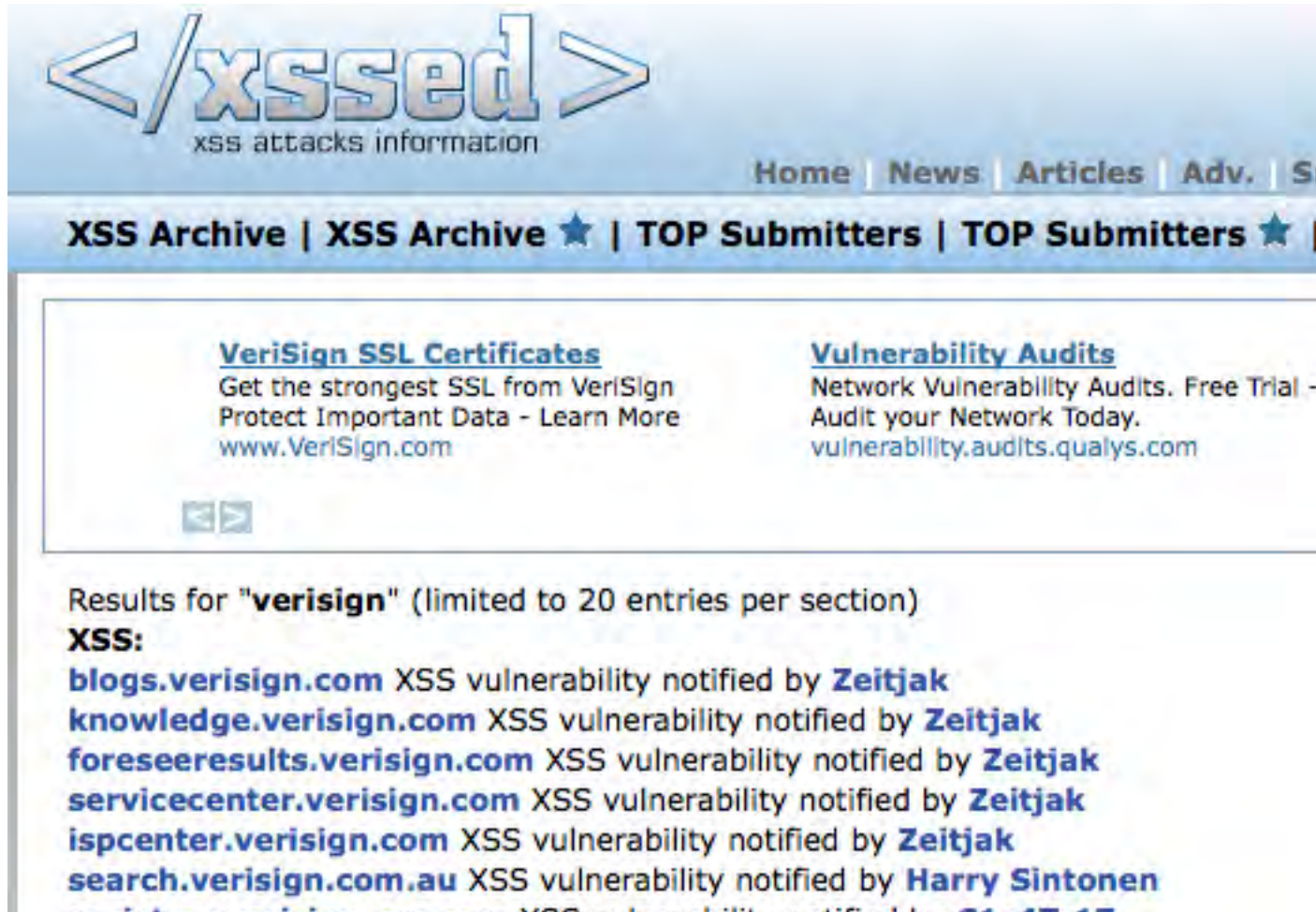
# Intro - Soft Targets

---

```

- <wsdl:definitions targetNamespace="http://stub.order.gasapiserver.esp.globalsign.com">
  - <!--
    WSDLはApache Axis version: 1.4
    Built on Apr 22, 2006 (06:55:48 PDT)によって生成されました / [en]-(WSDL created by Apache Axis version: .
    Built on Apr 22, 2006 (06:55:48 PDT))
  -->
  - <wsdl:types>
    - <schema elementFormDefault="qualified" targetNamespace="http://stub.order.gasapiserver.esp.globalsign.com">
      - <element name="DVOrder">
        - <complexType>
          - <sequence>
            <element name="Request" type="impl:DVOrderRequest"/>
          </sequence>
        </complexType>
      </element>
    - <complexType name="ContactInfo">
      - <sequence>
        <element name="Email" nillable="true" type="xsd:string"/>
        <element name="FirstName" nillable="true" type="xsd:string"/>
        <element name="LastName" nillable="true" type="xsd:string"/>
        <element name="Phone" nillable="true" type="xsd:string"/>
      </sequence>
    
```

# Intro - Soft Targets



The screenshot shows the XSSed website interface. At the top, there is a navigation menu with links for Home, News, Articles, Adv., and Search. Below the navigation, there are links for XSS Archive and TOP Submitters. The main content area displays two advertisements: one for VeriSign SSL Certificates and another for Vulnerability Audits. Below the ads, there is a search results section for the term "verisign", listing several verisign.com domains with XSS vulnerabilities notified by various researchers.

**</xssed>**  
xss attacks information

Home | News | Articles | Adv. | Search

**XSS Archive | XSS Archive ★ | TOP Submitters | TOP Submitters ★ |**

**VeriSign SSL Certificates**  
Get the strongest SSL from VeriSign  
Protect Important Data - Learn More  
[www.Verisign.com](http://www.Verisign.com)

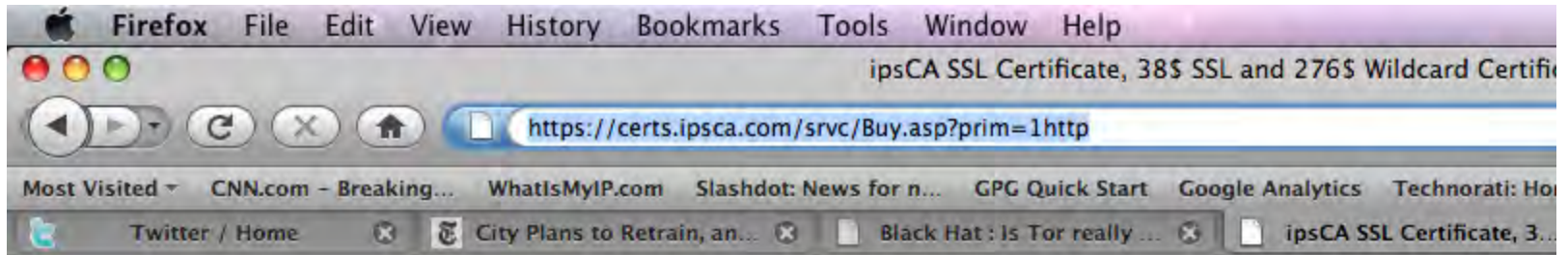
**Vulnerability Audits**  
Network Vulnerability Audits. Free Trial -  
Audit your Network Today.  
[vulnerability.audits.qualys.com](http://vulnerability.audits.qualys.com)

Results for "**verisign**" (limited to 20 entries per section)

**XSS:**

- [blogs.verisign.com](http://blogs.verisign.com)** XSS vulnerability notified by **Zeitjak**
- [knowledge.verisign.com](http://knowledge.verisign.com)** XSS vulnerability notified by **Zeitjak**
- [foreseeresults.verisign.com](http://foreseeresults.verisign.com)** XSS vulnerability notified by **Zeitjak**
- [servicecenter.verisign.com](http://servicecenter.verisign.com)** XSS vulnerability notified by **Zeitjak**
- [ispcenter.verisign.com](http://ispcenter.verisign.com)** XSS vulnerability notified by **Zeitjak**
- [search.verisign.com.au](http://search.verisign.com.au)** XSS vulnerability notified by **Harry Sintonen**

# Intro - Soft Targets

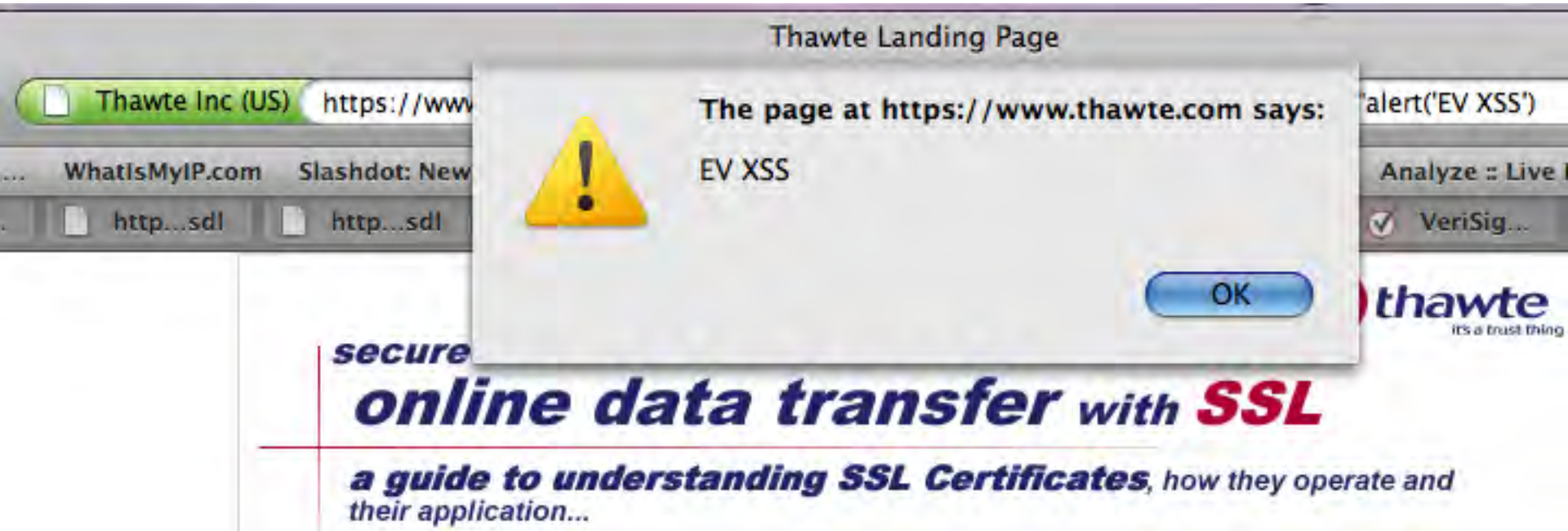


	PRODUCTS	DOWNLOADS	STORE	PARTNERS	SUPPORT	Contact
	FEBRUARY 19, 2009					Log in
	SSL Server	S/MIME Personal	Sign & Encrypt	PLUG-INS		
	<b>PRODUCTS</b>					
<b>OTHER AREAS OF INTEREST</b>	Error de Microsoft VBScript en tiempo de ejecución error '800a000d' No coinciden los tipos: '[string: "1http"]' /srv/ Buy.asp, línea 137					
<a href="#">Product Overview</a> <a href="#">Why ipsCA?</a> <a href="#">Demonstrations</a> <a href="#">Pricing</a>						



# 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] m, Inc.

Description: B [REDACTED] m, 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

# Intro - Soft Targets

---

## 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 p:

This order will only be completed once you have approved the application. Following your approval the technical c:  
 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 sup:

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

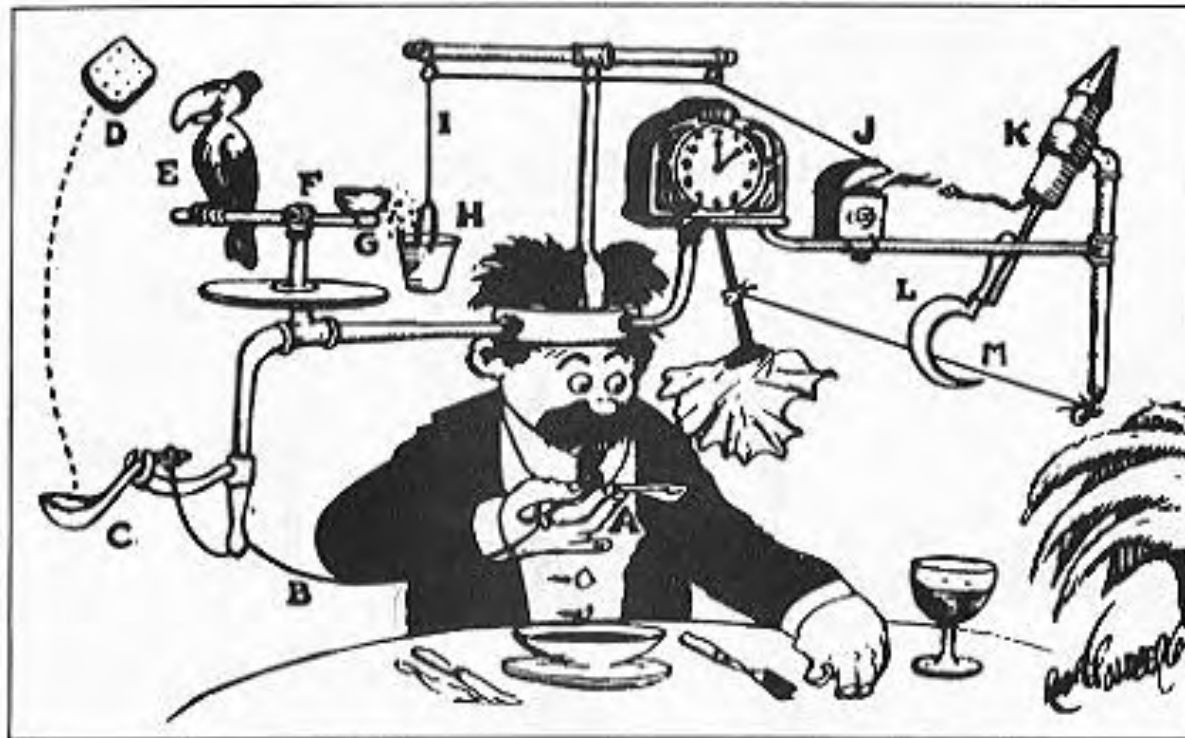
---

- 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

Self-Operating Napkin



# 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

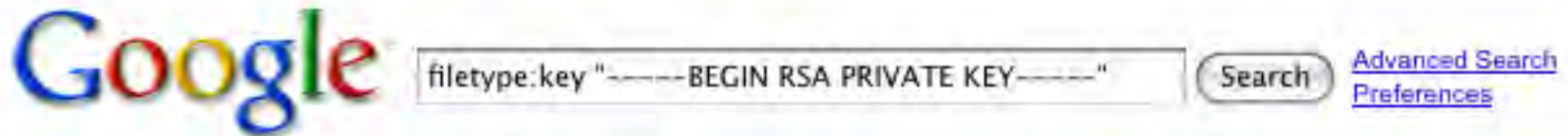
---

## 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

Web [Images](#) [Maps](#) [News](#) [Video](#) [Gmail](#) [more](#) ▼ mikezusman@gmail.com | [Web History](#) | [My Account](#)



Web [Show options...](#) Results 31 - 40 of about 412 for filetype:key "-----BEGIN RSA PRIVATE KEY-----".

[-----BEGIN RSA PRIVATE KEY----- MIICXgIBAAKBgQDddPnxTxVV3dk0x+ ...](#)  

-----BEGIN RSA PRIVATE KEY----- MIICXgIBAAKBgQDddPnxTxVV3dk0x+9c82h6FPWtrk/  
URbOCtTfEA4NA4GbZVvTO ...

[www.freebird.in/wp/wp-content/plugins/commentpower/pki/private.key - 2k -](#)

[Cached](#) - [Similar pages](#) - 

[-----BEGIN RSA PRIVATE KEY ...](#)  

-----BEGIN RSA PRIVATE KEY-----

MIICWwIBAAKBgQDT7LTGGnMVU6OvnQ5TdXmGUL3jDLcqbB/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
  - [http://www.owasp.org/index.php/Top\\_10\\_2007-A4](http://www.owasp.org/index.php/Top_10_2007-A4)



# Certificate Authority Attacks

## StartSSL™ Certificates

Tool Box

Certificates  
Wizard

Validations  
Wizard

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://  .

Continue >>>

# Certificate Authority Attacks

## StartSSL™ Certificates

Tool Box

Certificates  
Wizard

Validations  
Wizard

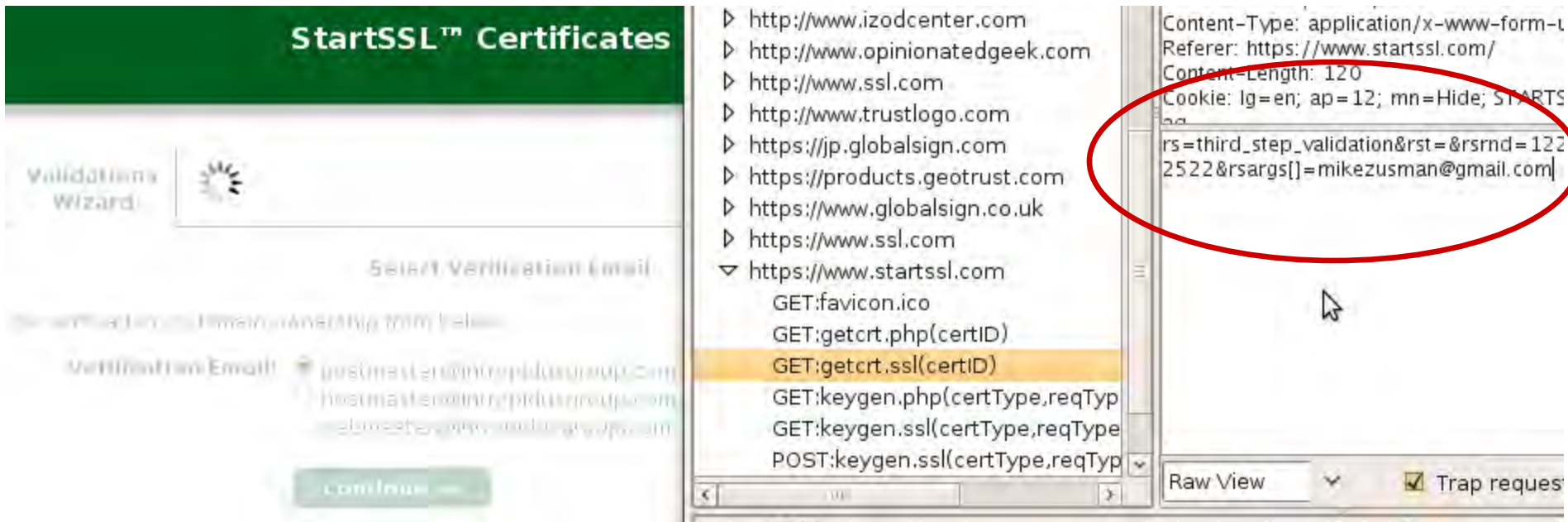
### Select Verification Email

- 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



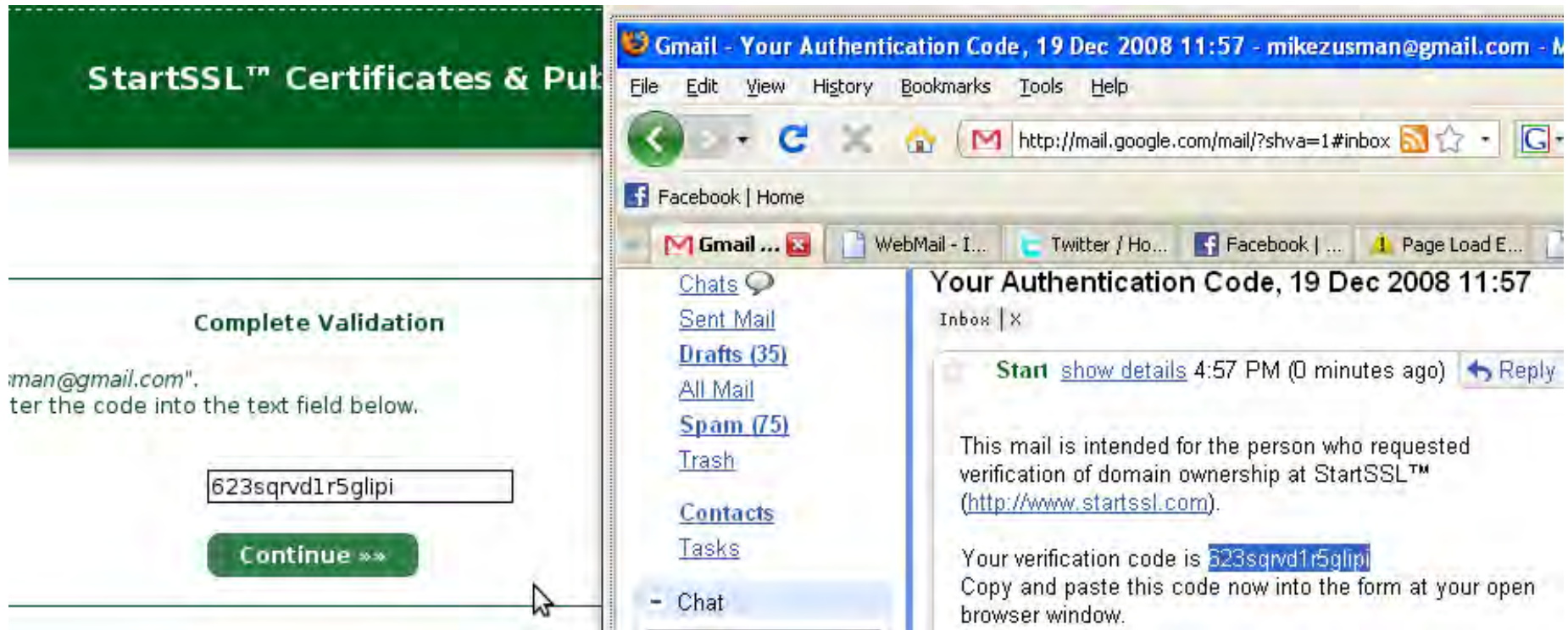
The image shows a screenshot of the StartSSL website's 'Validations Wizard' and a network traffic capture tool. The website interface includes a 'Validations Wizard' section with a 'Select Verification Email' dropdown menu. The network traffic capture tool displays a list of requests, with the following request highlighted:

- GET: getcert.php(certID)

The request body for this request is highlighted with a red circle and contains the following data:

```
Content-Type: application/x-www-form-urlencoded
Referer: https://www.startssl.com/
Content-Length: 120
Cookie: lg=en; ap=12; mn=Hide; STARTS...
rs=third_step_validation&rst=&rsrnd=1222522&rsargs[]=mikezusman@gmail.com
```

# Certificate Authority Attacks



**StartSSL™ Certificates & Public Keys**

**Complete Validation**

man@gmail.com".  
Enter the code into the text field below.

623sqrvd1r5glipi

**Continue** ⇨

**Gmail - Your Authentication Code, 19 Dec 2008 11:57 - mikezusman@gmail.com - M**

File Edit View History Bookmarks Tools Help

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**

Inbox | X

**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

---



Tool Box Certificates Wizard Validations Wizard

### Validation Success

- 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.

Finish >>>

# 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
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
- [http://www.owasp.org/index.php/Top\\_10\\_2007-A6](http://www.owasp.org/index.php/Top_10_2007-A6)



# 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:

your

- admin
- administrator
- hostmaster
- info
- is
- it
- mis
- ssladmin
- ssladministrator
- sslwebmaster
- sysadmin
- webmaster

[ 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. ]

technical contact :

E: This person will receive technical information and renewal notices and communication on outstanding issues with regard to the program. (e.g. technical support)

person should preferably:

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

# 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](mailto:domainadmin@yahoo-inc.com)

[admin@yahoo.com](mailto:admin@yahoo.com)

[SSLadmin@yahoo.com](mailto:SSLadmin@yahoo.com)

[sysadmin@yahoo.com](mailto:sysadmin@yahoo.com)

[webmaster@yahoo.com](mailto:webmaster@yahoo.com)

[administrator@yahoo.com](mailto:administrator@yahoo.com)

[SSLadministrator@yahoo.com](mailto:SSLadministrator@yahoo.com)

[SSLCerts@yahoo.com](mailto:SSLCerts@yahoo.com)

[SSLCertificates@yahoo.com](mailto:SSLCertificates@yahoo.com)

[info@yahoo.com](mailto:info@yahoo.com)

[SSLwebmaster@yahoo.com](mailto:SSLwebmaster@yahoo.com)

[hostmaster@yahoo.com](mailto:hostmaster@yahoo.com)

[support@yahoo.com](mailto:support@yahoo.com)

[sales@yahoo.com](mailto:sales@yahoo.com)

[tech@yahoo.com](mailto:tech@yahoo.com)

[mail@yahoo.com](mailto:mail@yahoo.com)

[manager@yahoo.com](mailto:manager@yahoo.com)

[MIS@yahoo.com](mailto:MIS@yahoo.com)

[IS@yahoo.com](mailto:IS@yahoo.com)

[IT@yahoo.com](mailto:IT@yahoo.com)

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

---

# Certificate Authority Attacks (2)

---

## 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 p:

This order will only be completed once you have approved the application. Following your approval the technical c:  
 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 sup:

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

Customer Support

# Certificate Authority Attacks (2)

Certificate Viewer: 'login.live.com'

General Details

**This certificate has been verified for the following uses:**

SSL Server Certificate

**Issued To**

Common Name (CN) login.live.com  
 Organization (O) login.live.com  
 Organizational Unit (OU) Go to <https://www.thawte.com/repository/index.html>  
 Serial Number 39:47:25:56:5D:82:FB:D0:01:BE:2D:BA:16:03:64:43

**Issued By**

Common Name (CN) Thawte Server CA  
 Organization (O) Thawte Consulting cc  
 Organizational Unit (OU) Certification Services Division

**Validity**

Issued On 7/28/2008  
 Expires On 7/29/2009

**Fingerprints**

SHA1 Fingerprint B3:7C:C5:1C:F0:27:72:17:F1:1F:CB:62:AE:EE:C1:81:0D:A7  
 MD5 Fingerprint 10:23:FC:40:0C:C1:96:5D:45:6D:6D:23:74:5A:B5:A7

Certificate Viewer: 'login.live.com'

General Details

**This certificate has been verified for the following uses:**

SSL Server Certificate

**Issued To**

Common Name (CN) login.live.com  
 Organization (O) Microsoft Corporation  
 Organizational Unit (OU) MSN-Passport  
 Serial Number 69:05:C4:A4:7C:FD:BF:9D:BC:98:DA:CE:38:83:5F:B8

**Issued By**

Common Name (CN) VeriSign Class 3 Extended Validation SSL CA  
 Organization (O) VeriSign, Inc.  
 Organizational Unit (OU) VeriSign Trust Network

**Validity**

Issued On 6/18/2008  
 Expires On 7/20/2009

**Fingerprints**

SHA1 Fingerprint 18:16:D2:5E:AF:DB:85:23:BA:71:66:2F:2D:03:BE:8F:91:BC:44:4E  
 MD5 Fingerprint C2:37:09:CA:60:75:53:71:7C:7E:F0:26:CC:ED:9C:03



# 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 p:

This order will only be completed once you have approved the application. Following your approval the technical c:  
 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 sup:

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

Customer Support



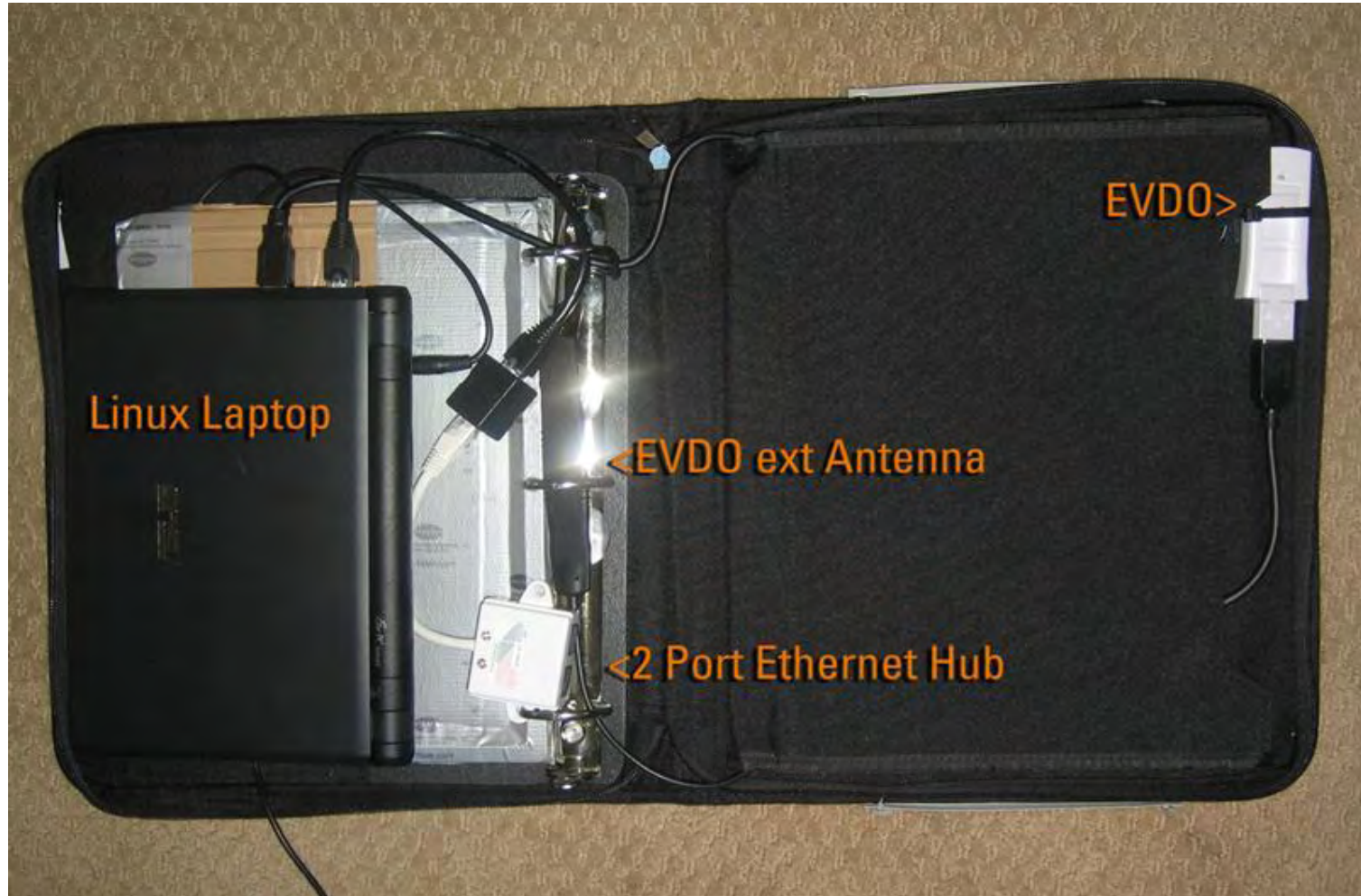
# Certificate Authority Attacks (3)

---

## Demonstration

# Post CA Exploitation

---



# 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 Pubic 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>