Web Security in the Real World

Steven M. Bellovin

Chief Technologist, FTC

Security is Built on Trust

- **We trust the OS**
- **We trust the browser**
- **We trust the cryptography**
- **We trust the destination website**

“We trust the cryptography”?

- **“These practices and controls include… encrypting the transfer of personal information … via … (SSL)”**
- **Similar statements appear in many websites’ security and privacy policies**
- **People equate security with privacy and trustworthiness, and conflate both with encryption**

Usability

- **Verifying encryption, per one web site:**
  - **A key or a lock at the bottom**
    - **“Unbroken” or “locked”**
    - **Not true on my browers…**
  - **Or the “color of the address bar”**
    - **Green—or blue—or yellow**
    - **Also not true for me…**
- **What’s a user to do?**

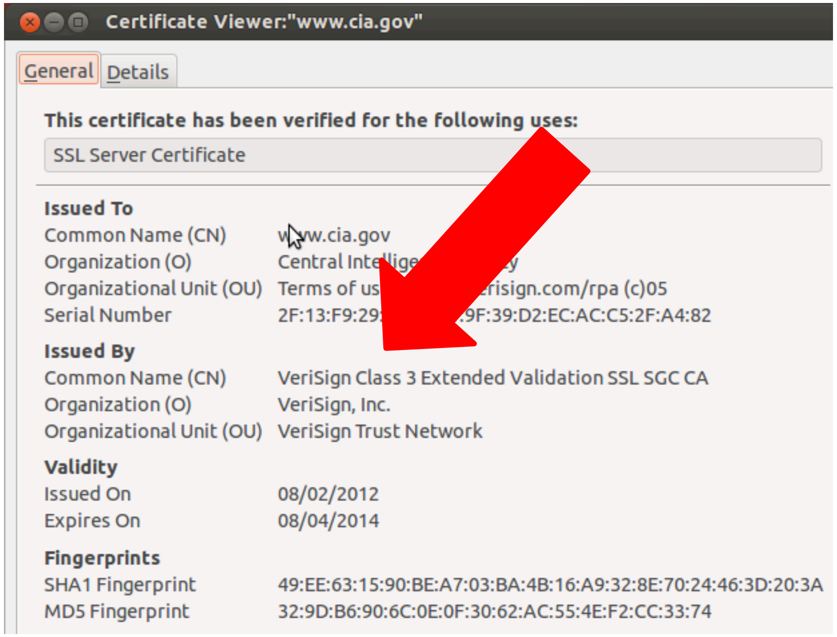
What's a Certificate?

- Very few users know what a certificate is
- Fewer care
- Virtually none know or care about trust anchors
- Can orddinary users employ advanced techniques?

We Understand the Issue

- From a security perspective, too many root CAs in every browser
- Any one of these can issue certificates to any web site
- A compromise of (or misbehavior by) any one of these allows for spoofing of any site
- This has already happened

The CIA



This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	www.cia.gov
Organization (O)	Central Intellige y
Organizational Unit (OU)	Terms of us erisign.com/rpa (c)05
Serial Number	2F:13:F9:29 9F:39:D2:EC:AC:C5:2F:A4:82

Issued By

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

Validity

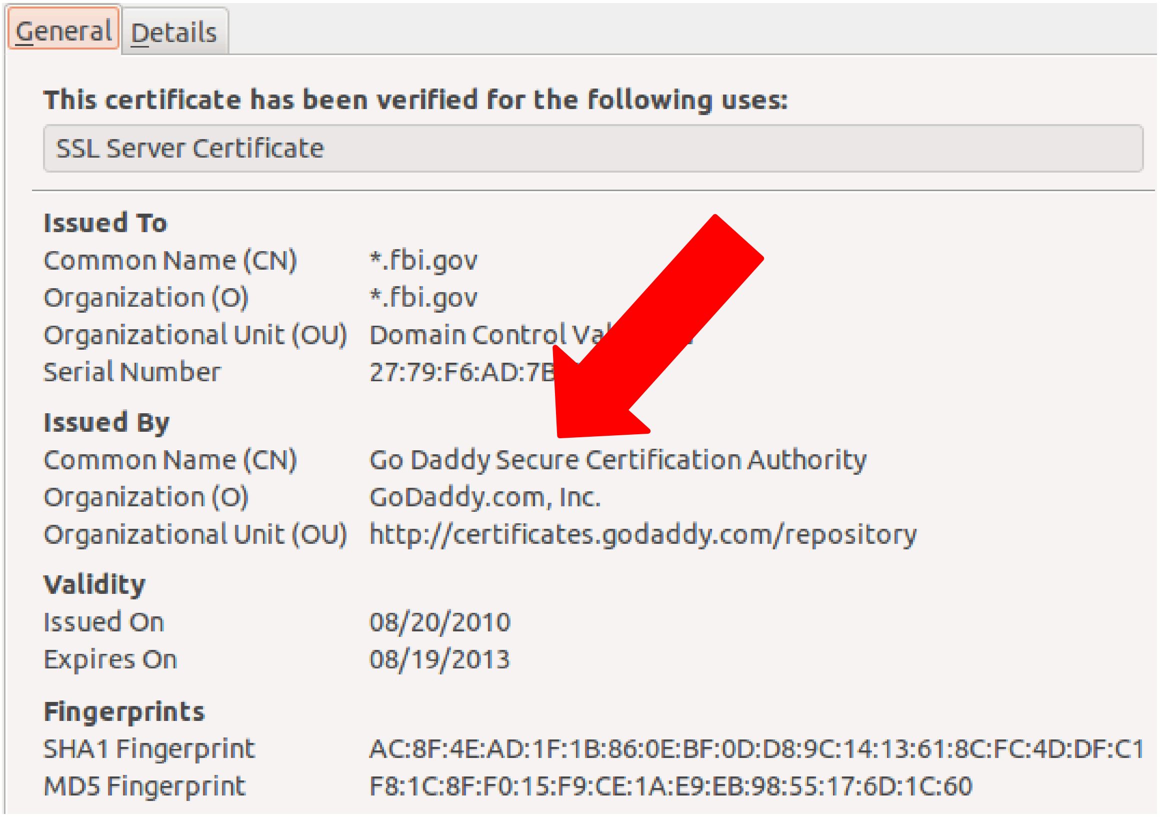
Issued On	08/02/2012
Expires On	08/04/2014

Fingerprints

SHA1 Fingerprint	49:EE:63:15:90:BE:A7:03:BA:4B:16:A9:32:8E:70:24:46:3D:20:3A
MD5 Fingerprint	32:9D:B6:90:6C:0E:0F:30:62:AC:55:4E:F2:CC:33:74

But why does Verisign have to attest to its identity?

Is the FBI Feuding with the CIA?



This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN)	*.fbi.gov
Organization (O)	*.fbi.gov
Organizational Unit (OU)	Domain Control Val
Serial Number	27:79:F6:AD:7B

Issued By

Common Name (CN)	Go Daddy Secure Certification Authority
Organization (O)	GoDaddy.com, Inc.
Organizational Unit (OU)	http://certificates.godaddy.com/repository

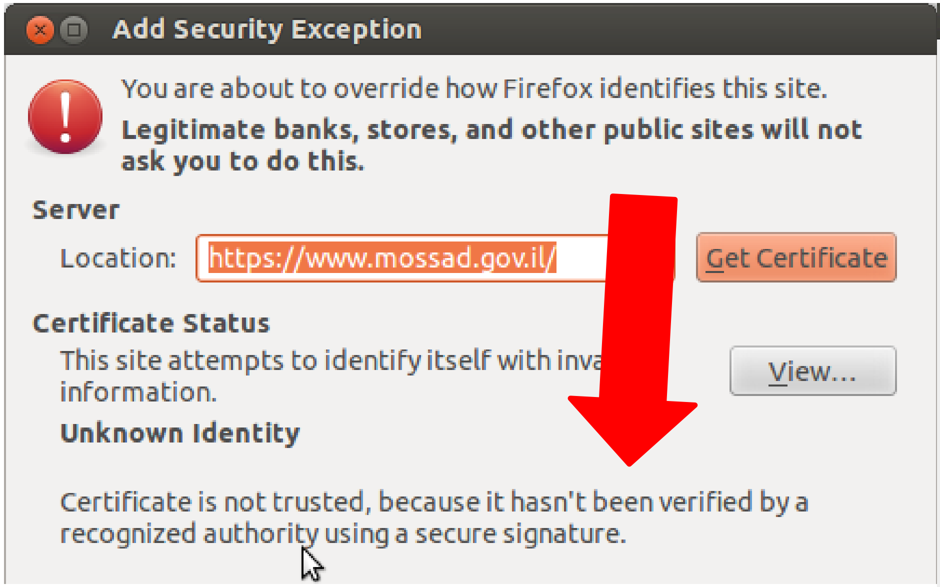
Validity

Issued On	08/20/2010
Expires On	08/19/2013

Fingerprints

SHA1 Fingerprint	AC:8F:4E:AD:1F:1B:86:0E:BF:0D:D8:9C:14:13:61:8C:FC:4D:DF:C1
MD5 Fingerprint	F8:1C:8F:F0:15:F9:CE:1A:E9:EB:98:55:17:6D:1C:60

An Intelligence Agency Playing Games?



You are about to override how Firefox identifies this site.

Legitimate banks, stores, and other public sites will not ask you to do this.

Server

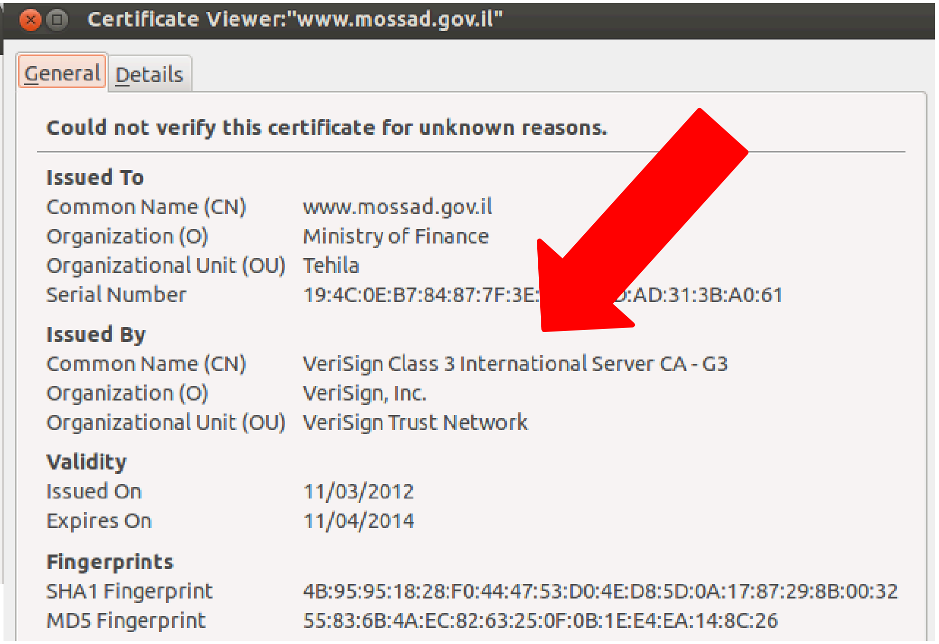
Location: https://www.mossad.gov.il/

Certificate Status

This site attempts to identify itself with inva information.

Unknown Identity

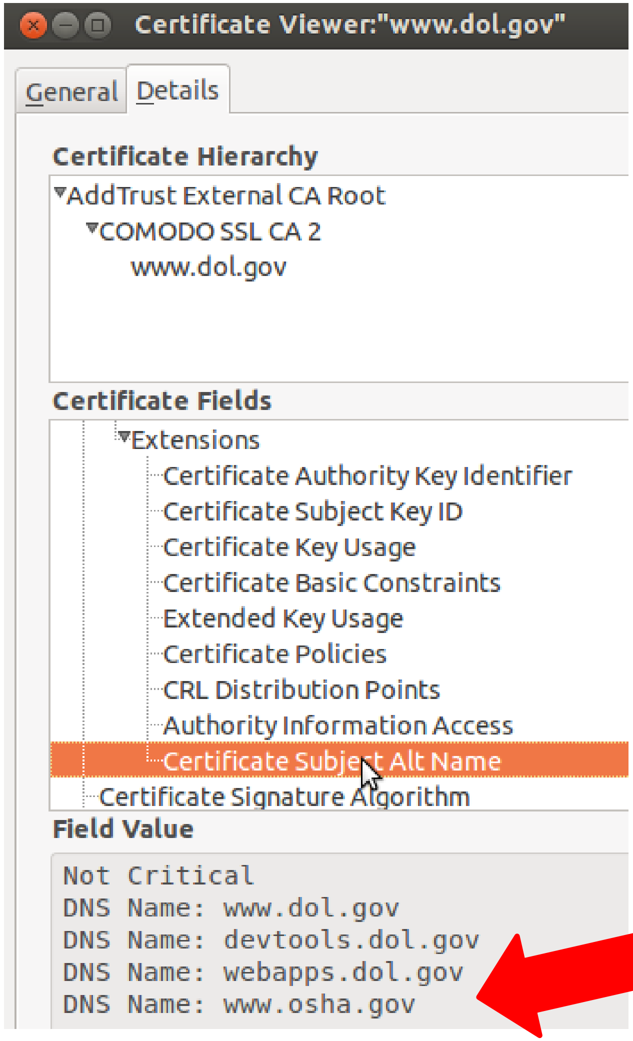
Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.



Could not verify this certificate for unknown reasons.

Issued To	
Common Name (CN)	www.mossad.gov.il
Organization (O)	Ministry of Finance
Organizational Unit (OU)	Tehila
Serial Number	19:4C:0E:B7:84:87:7F:3E: :AD:31:3B:A0:61
Issued By	
Common Name (CN)	VeriSign Class 3 International Server CA - G3
Organization (O)	VeriSign, Inc.
Organizational Unit (OU)	VeriSign Trust Network
Validity	
Issued On	11/03/2012
Expires On	11/04/2014
Fingerprints	
SHA1 Fingerprint	4B:95:95:18:28:F0:44:47:53:D0:4E:D8:5D:0A:17:87:29:8B:00:32
MD5 Fingerprint	55:83:6B:4A:EC:82:63:25:0F:0B:1E:E4:EA:14:8C:26

The Labor Department Gets It



Certificate Hierarchy

- AddTrust External CA Root
  - COMODO SSL CA 2
    - www.dol.gov

Certificate Fields

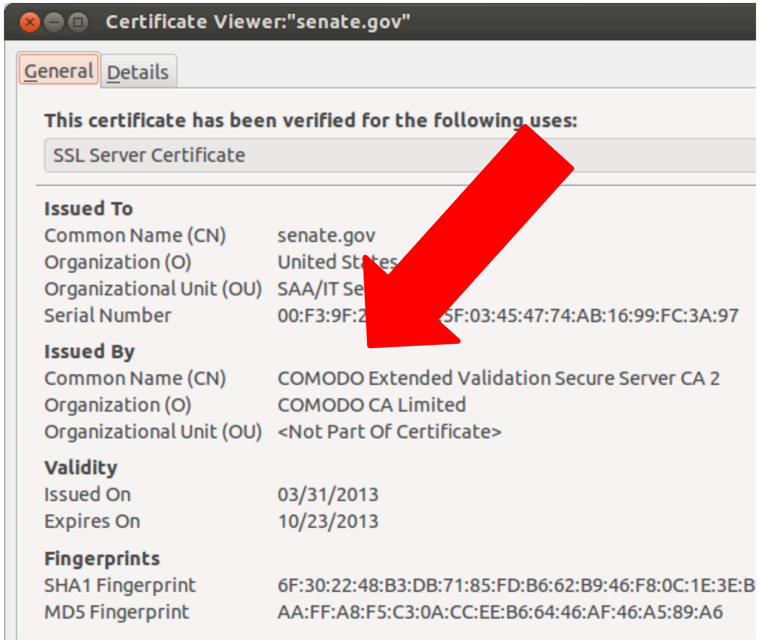
- Extensions
  - Certificate Authority Key Identifier
  - Certificate Subject Key ID
  - Certificate Key Usage
  - Certificate Basic Constraints
  - Extended Key Usage
  - Certificate Policies
  - CRL Distribution Points
  - Authority Information Access
  - Certificate Subject Alt Name
- Certificate Signature Algorithm

Field Value

```
Not Critical
DNS Name: www.dol.gov
DNS Name: devtools.dol.gov
DNS Name: webapps.dol.gov
DNS Name: www.osha.gov
```

OSHA is part of the Labor Department; its address rightly appears in the dol.gov certificate (but how did the CA verify the relationship?)

Congress Divided



Certificate Viewer:"senate.gov"

This certificate has been verified for the following uses:

SSL Server Certificate

Issued To

Common Name (CN) senate.gov
Organization (O) United States
Organizational Unit (OU) SAA/IT Se
Serial Number 00:F3:9F:2 5F:03:45:47:74:AB:16:99:FC:3A:97

Issued By

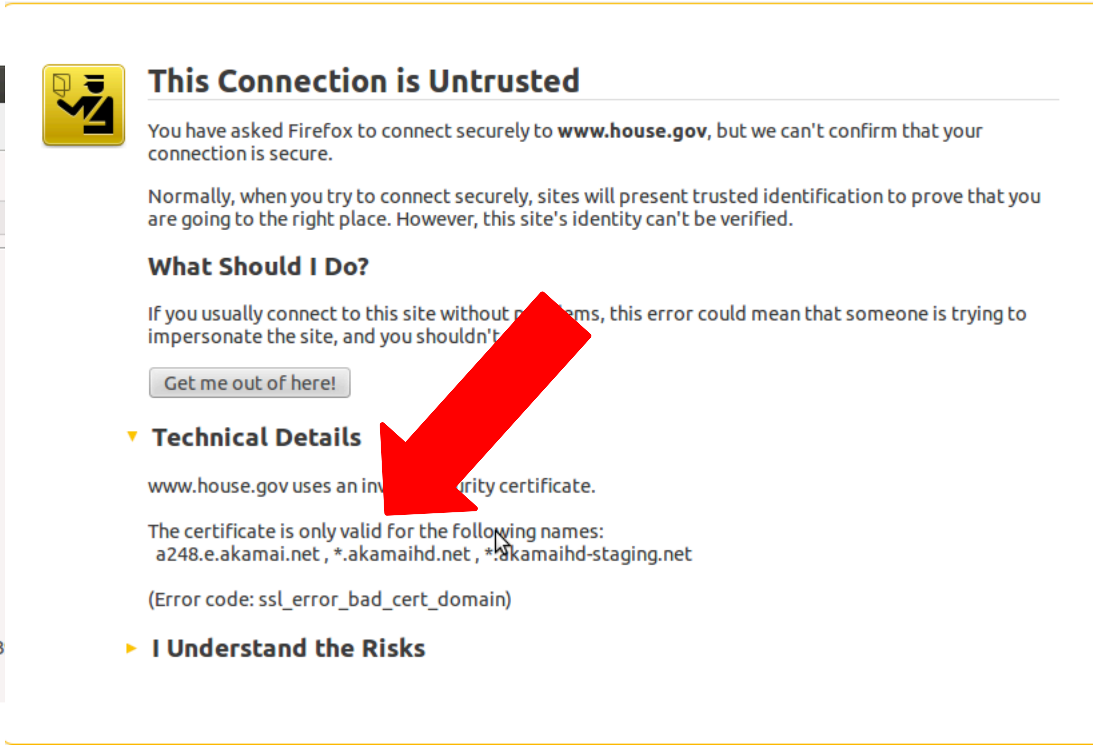
Common Name (CN) COMODO Extended Validation Secure Server CA 2
Organization (O) COMODO CA Limited
Organizational Unit (OU) <Not Part Of Certificate>

Validity

Issued On 03/31/2013
Expires On 10/23/2013

Fingerprints

SHA1 Fingerprint 6F:30:22:48:B3:DB:71:85:FD:B6:62:B9:46:F8:0C:1E:3E:B
MD5 Fingerprint AA:FF:A8:F5:C3:0A:CC:EE:B6:64:46:AF:46:A5:89:A6



This Connection is Untrusted

You have asked Firefox to connect securely to **www.house.gov**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't

Technical Details

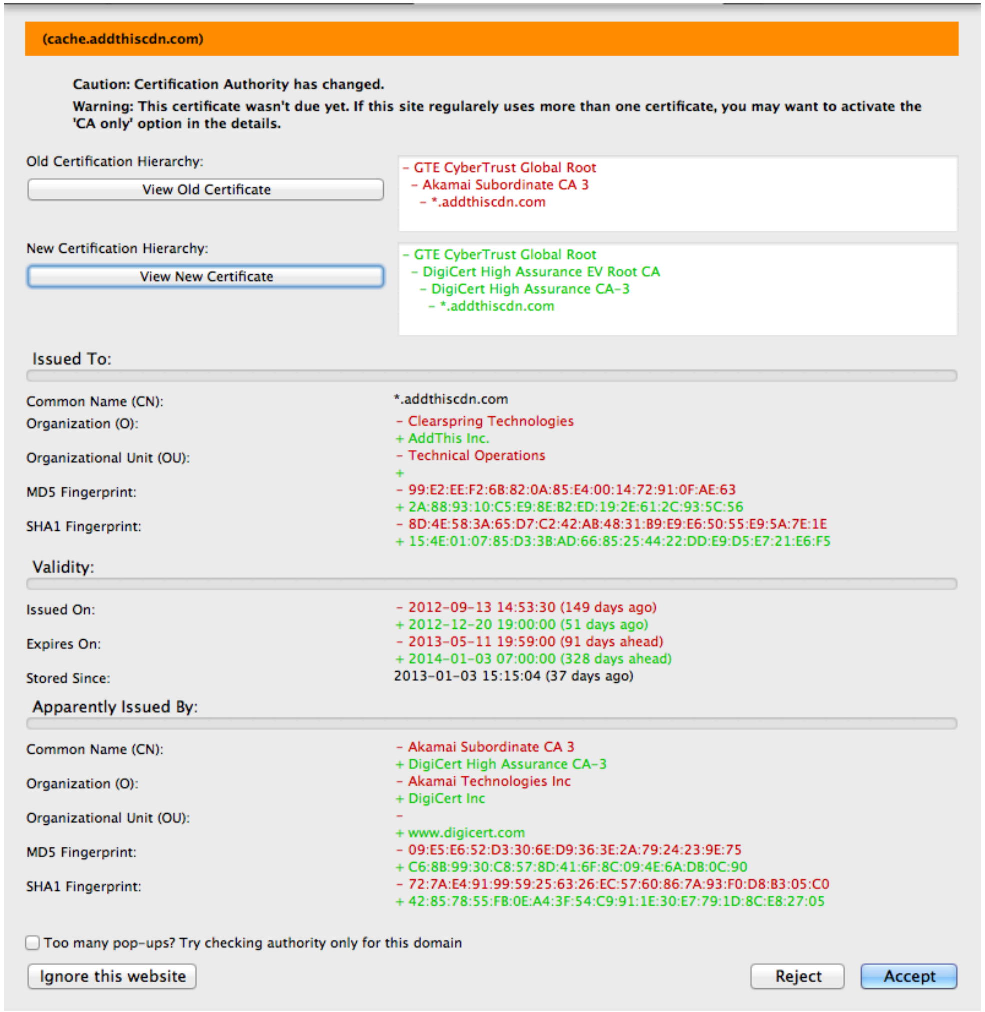
www.house.gov uses an invalid security certificate.

The certificate is only valid for the following names:
a248.e.akamai.net , *.akamaihd.net , *.akamaihd-staging.net

(Error code: ssl_error_bad_cert_domain)

I Understand the Risks

Using CertPatrol



(cache.addthiscdn.com)

Caution: Certification Authority has changed.

Warning: This certificate wasn't due yet. If this site regulerly uses more than one certificate, you may want to activate the 'CA only' option in the details.

Old Certification Hierarchy:

```
- GTE CyberTrust Global Root
  - Akamai Subordinate CA 3
    - *.addthiscdn.com
```

New Certification Hierarchy:

```
- GTE CyberTrust Global Root
  - DigiCert High Assurance EV Root CA
    - DigiCert High Assurance CA-3
      - *.addthiscdn.com
```

Issued To:

Common Name (CN):	*.addthiscdn.com
Organization (O):	- Clearspring Technologies + AddThis Inc.
Organizational Unit (OU):	- Technical Operations +
MD5 Fingerprint:	- 99:E2:EE:F2:6B:82:0A:85:E4:00:14:72:91:0F:AE:63 + 2A:88:93:10:C5:E9:8E:B2:ED:19:2E:61:2C:93:5C:56
SHA1 Fingerprint:	- 8D:4E:58:3A:65:D7:C2:42:AB:48:31:B9:E9:E6:50:55:E9:5A:7E:1E + 15:4E:01:07:85:D3:3B:AD:66:85:25:44:22:DD:E9:D5:E7:21:E6:F5

Validity:

Issued On:	- 2012-09-13 14:53:30 (149 days ago) + 2012-12-20 19:00:00 (51 days ago)
Expires On:	- 2013-05-11 19:59:00 (91 days ahead) + 2014-01-03 07:00:00 (328 days ahead)
Stored Since:	2013-01-03 15:15:04 (37 days ago)

Apparently Issued By:

Common Name (CN):	- Akamai Subordinate CA 3 + DigiCert High Assurance CA-3
Organization (O):	- Akamai Technologies Inc + DigiCert Inc
Organizational Unit (OU):	- + www.digicert.com
MD5 Fingerprint:	- 09:E5:E6:52:D3:30:6E:D9:36:3E:2A:79:24:23:9E:75 + C6:8B:99:30:C8:57:8D:41:6F:8C:09:4E:6A:DB:0C:90
SHA1 Fingerprint:	- 72:7A:E4:91:99:59:25:63:26:EC:57:60:86:7A:93:F0:D8:B3:05:C0 + 42:85:78:55:FB:0E:A4:3F:54:C9:91:1E:30:E7:79:1D:8C:E8:27:05

☐ Too many pop-ups? Try checking authority only for this domain

Remember that famous comment line from early Unix source code? "You are not expected to understand this."

(Nostalgia Time)

```
/*
 * If the new process paused because it was
 * swapped out, set the stack level to the last call
 * to savu(u_ssav). This means that the return
 * which is executed immediately after the call to aretu
 * actually returns from the last routine which did
 * the savu.
 *
 * You are not expected to understand this.
 */
```

(from http://www.cs.bell-labs.com/who/dmr/odd.html)

Fundamental Requirements

- **We need a solution that is (considerably more) secure than what we have today**
- **It must not involve new user interactions**
- **It must not generate (yet more) incomprehensible error messages**
- **It MUST NOT present new dialog boxes with text that will be ignored but still have a button to click labeled “OK”**

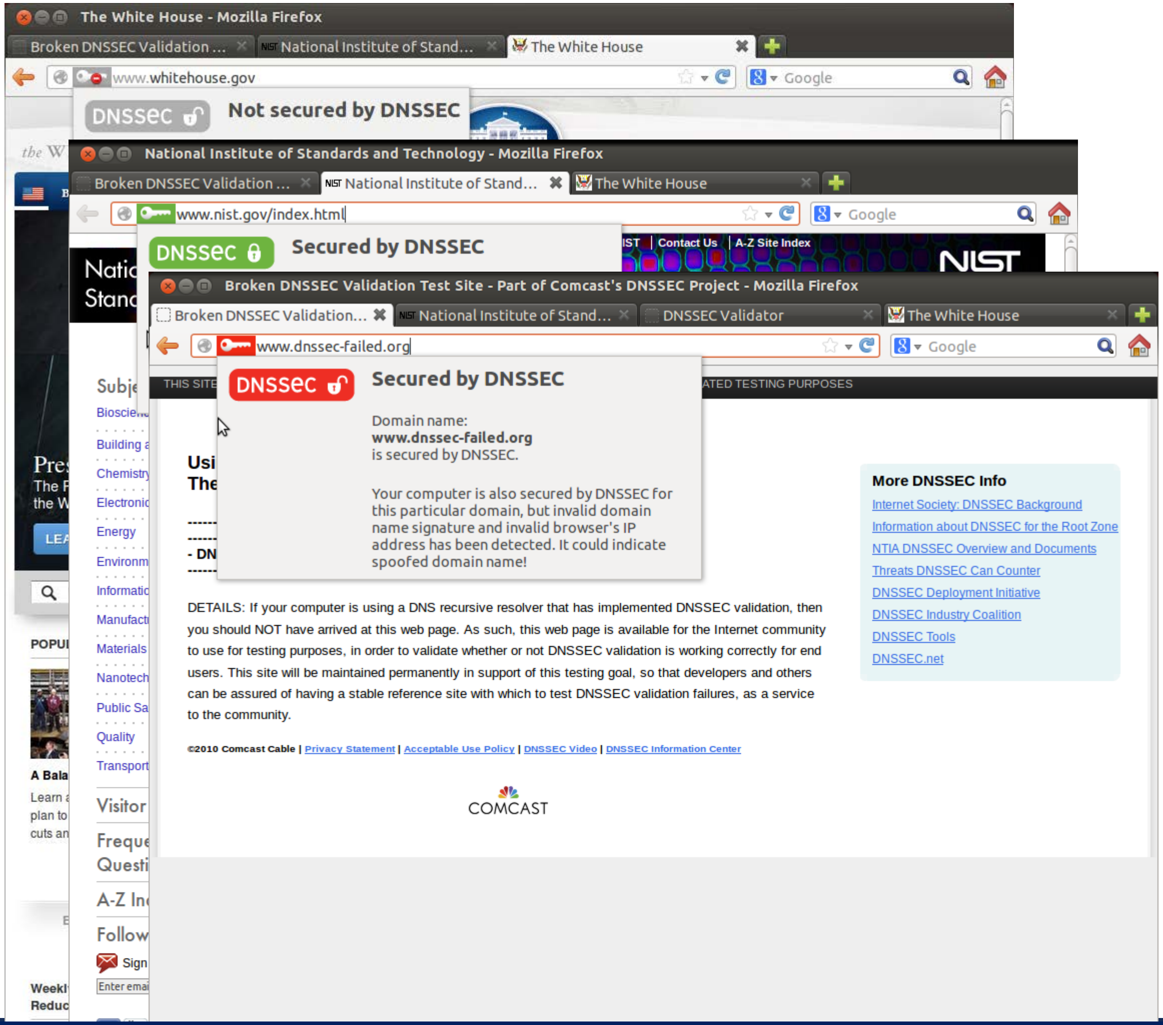
Other Issues

- Existing businesses and business models
- Existing operational practices
- Self-signed certificates
- Enterprise firewalls and IDSs that do certificate-spoofing, to monitor employee conversations
- Non-web (e.g., app) uses of certificates by systems

The User Experience

- **Let’s look at DNSSEC, an element of one proposed solution (DANE)**
- **Comcast and Google do DNSSEC evaluation**
- **What does the user see?**

The DNSSEC Validator Extension



The White House - Mozilla Firefox

Broken DNSSEC Validation ... | National Institute of Stand... | The White House

www.whitehouse.gov

DNSSEC Not secured by DNSSEC

National Institute of Standards and Technology - Mozilla Firefox

Broken DNSSEC Validation ... | National Institute of Stand... | The White House

www.nist.gov/index.html

DNSSEC Secured by DNSSEC

Broken DNSSEC Validation Test Site - Part of Comcast's DNSSEC Project - Mozilla Firefox

Broken DNSSEC Validation... | National Institute of Stand... | DNSSEC Validator | The White House

www.dnssec-failed.org

DNSSEC Secured by DNSSEC

Domain name:
www.dnssec-failed.org
is secured by DNSSEC.

Your computer is also secured by DNSSEC for this particular domain, but invalid domain name signature and invalid browser's IP address has been detected. It could indicate spoofed domain name!

DETAILS: If your computer is using a DNS recursive resolver that has implemented DNSSEC validation, then you should NOT have arrived at this web page. As such, this web page is available for the Internet community to use for testing purposes, in order to validate whether or not DNSSEC validation is working correctly for end users. This site will be maintained permanently in support of this testing goal, so that developers and others can be assured of having a stable reference site with which to test DNSSEC validation failures, as a service to the community.

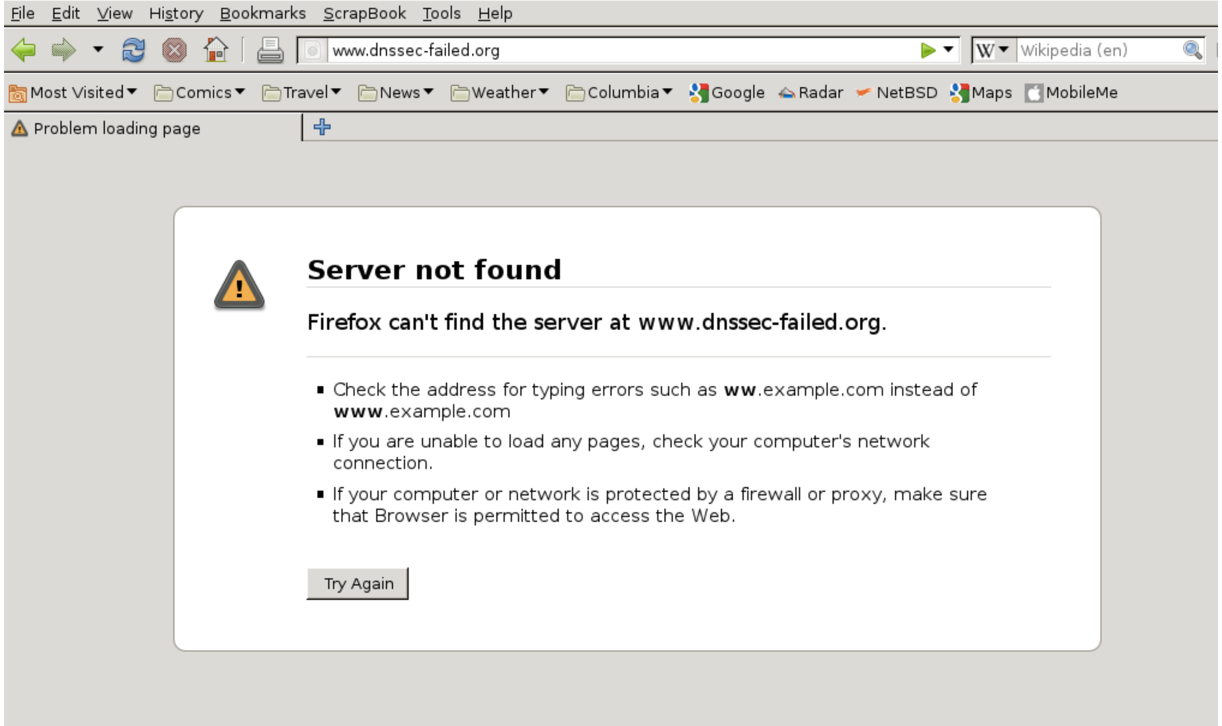
More DNSSEC Info

- Internet Society: DNSSEC Background
- Information about DNSSEC for the Root Zone
- NTIA DNSSEC Overview and Documents
- Threats DNSSEC Can Counter
- DNSSEC Deployment Initiative
- DNSSEC Industry Coalition
- DNSSEC Tools
- DNSSEC.net

©2010 Comcast Cable | Privacy Statement | Acceptable Use Policy | DNSSEC Video | DNSSEC Information Center

- **The primary indicator is a key icon**
- **You only get the box if you click on the key**
- **Who will notice or understand?**

Transparent Checking



Server not found

Firefox can't find the server at www.dnssec-failed.org.

- Check the address for typing errors such as **ww**.example.com instead of **www**.example.com
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Browser is permitted to access the Web.

Try Again

- **It protects the user from bad stuff**
- **It gives no hint what the real issue is**
- **Who will help the helpdesk?**

It’s Not Just the User Interface

- **Most ISPs don’t check DNSSEC**
- **Neither do most hosts**
- **Note that DNSSEC depends on upstream DNS registrars**
- **We’re missing APIs and secure, deployable over-the-wire signaling protocols**
- **RFC 6698 (TLSA): “DNSSEC validation is best performed on-host, even when a secure path to an external validator is available.”**

Whose Behavior Must Change?

- **Users?**
  - **Billions of users; no opportunity for training**
- **Web sites?**
  - **Tens (hundreds?) of millions; retraining sysadmins and webmasters is slow**
- **ISPs?**
  - **What’s in it for them? N.B.: see the comment on helpdesks**
- **Browsers and operating systems?**
  - **What is the upgrade rate?**

DNSSEC Trust Models

- **Sites have to trust a chain of registrars and registries up to the DNS root**
- **Many of these organizations are not accustomed to handling keys**
- **Effectively, though, they’re CAs; however, there’s only one root rather than many**
  - **Better for security, but no opportunity for vendors to compete on basis of security**

What About Business Models?

- **Some proposals (e.g., certificate transparency) require new parties**
- **Who pays them?**
- **Who pays them to *scale*?**
  - **What if there's a DDoS attack on such parties?**
- **Who pays them to respect privacy?**

What About Governments?

- **Many governments, hence many policies about trust, liability, content, privacy, etc.**
- **What ability should governments have to intervene in the trust model?**
- **Which governments should have that right, and under what conditions?**

Trust Model

- **Who *should* vouch for whom?**
  - **In theory, a an organization should vouch for its own subunits**
  - **This is rarely done—is it that hard for an organization to run its own sub-CA?**
  - **On the other hand, how do outside CAs verify not just the real organizational structure of the parent enterprise, but the authorization?**

What Changes Rapidly?

- **(Desktop) operating systems rarely change; machines are replaced instead**
  - **Requirements for better hardware cap the upgrade rate**
- **OS-linked browsers (IE, Safari) are upgraded somewhat slowly (stats source: clicky.com)**
  - **Probably faster than the underlying OS**
- **Independent browsers (Firefox, Chrome) are upgraded more rapidly**

Are the Browsers the Leverage Point?

- They’re effectively the trust anchor anyway; users trust what their browser tells them to trust
- They change more rapidly than operating systems
- There are many more ISPs than browser vendors, and the vendors are probably more agile

Partial Answers?

- **What schemes give us benefits before we have large-scale deployment?**
- **Conversely, what schemes cause user confusion during the transition, especially when it's mostly complete?**
- **Can we increase confidence in a result, even for scenarios where we (should) have less than full trust?**

Who is the Enemy?

- **To do certificate-spoofing, you must:**
  - **Subvert a CA**
  - **Be on-path with the victim**
- **Who can do this?**
  - **Governments**
  - **Sophisticated criminal hackers**
- ***Certificate-spoofing is a two-part attack, aimed at particular victims***

Major Issues

- Usability
- Deployability
- Business model
- Trust model
- Threat model
- Delegation to CDNs
- Organizational structure
- Enterprise needs
- Government needs
- Existing hotspot practices
- More?

Where Are We?

- **The current setup can’t last; it’s too fragile against serious**
- **The enemy is generally very sophisticated**
- **The problem is overconstrained**
- **We have to find a good path nevertheless**