SSL and Browsers: The Pillars of Broken Security

Ivan Ristic

Wolfgang Kandek

Qualys, Inc.

Session ID: TECH-403

Session Classification: Intermediate

RSA CONFERENCE 2012

SSL, TLS, And PKI

- SSL (or TLS, if you prefer) is the technology that secures the Internet
  - Designed with aim to secure credit card transactions
  - Ended up as a generic encryption protocol for the transport layer
  - Design based on the old threat model shows cracks in use today

Overview Of Major Attacks

- Identity/account compromise:
  - Financial loss (theft)
  - Data leakage
  - Spam
  - Embarrassment
- Eavesdropping
- Mass surveillance

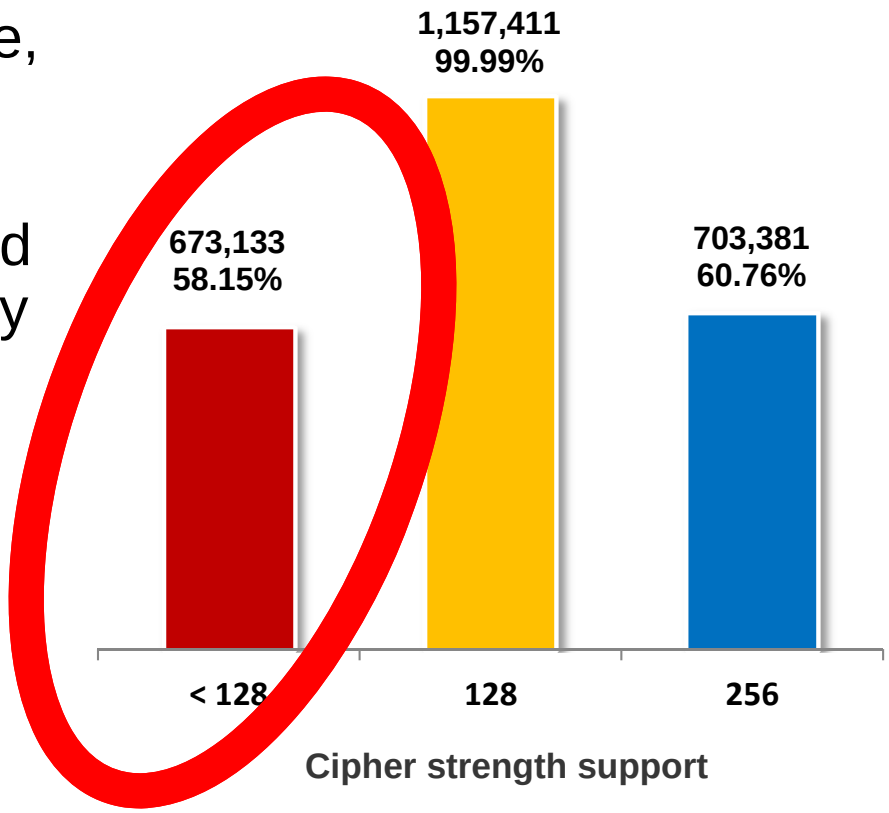
SSL Ecosystem

- Protocol designers (IETF TLS Working Group)
- Library developers (Microsoft, OpenSSL, NSS, …)
- Vendors
  - Server vendors
  - Browser vendors
- Certificate authorities and resellers
- System administrators
- Consumers

SSL/TLS Server Configuration Issues

Weak Encryption Still Common

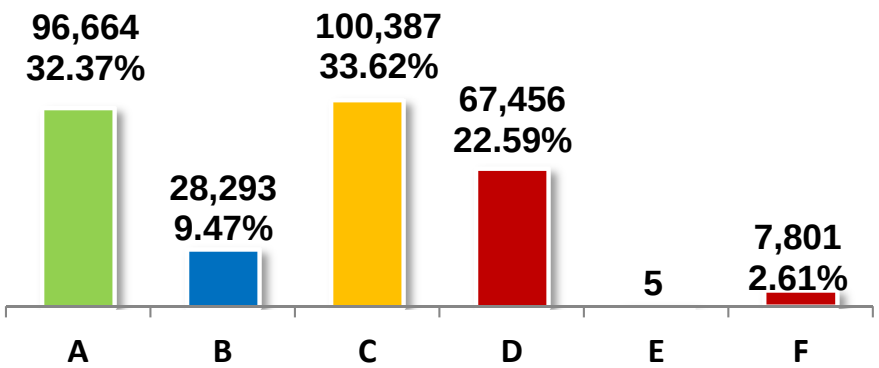
- Private keys under 1024 bits are easy to break
  - Few public servers vulnerable, but issues likely in internal legacy internal systems
  - Digicert Sdn. Bhd. (not related to DigiCert, Inc.), was recently caught issuing 512-bit certs
- Ciphers weaker than 128 bits equally weak



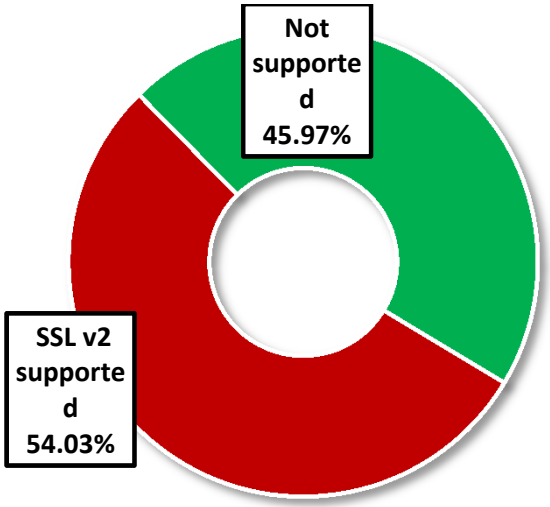
SSLv2 Insecure, Yet Widely Supported

More than half of all servers tested support the insecure SSL v2 protocol

- **SSL v2 can be easily broken**
- An active MITM can force browsers to fall back to SSL v2, if supported in both client and server
- Modern browsers do not support SSLv2, but old do



Grades of 300,000 most popular SSL sites



Protocol	Support	Best protocol
SSL v2.0	625,484	-
SSL v3.0	1,156,033	13,471
TLS v1.0	1,143,673	1,141,458
TLS v1.1	2,191	2,007
TLS v1.2	211	211

Reasons

- Hard to configure ?

In the Wild…

- Amazon EC2 console here – search for a wordpress AMI

In the Wild…

BitNami WordPress Stack - Mozilla Firefox

BitNami WordPress Stack

amazonaws.com https://ec2-107-22-13-224.

Google

BITNAMI

Welcome!

Access BitNami WordPress Stack

WordPress

The BitNami Project was created to help spread the adoption of freely available, high quality Open Source web applications. BitNami aims to make it easier than ever to discover, download and install Open Source software such as document and content management systems, wikis and blogging software.

You can learn more about BitNami at http://bitnami.org

WordPress is an open source, standards-compliant, fast, light and free personal publishing platform. The project was started in 2003 as a personal publishing platform, with a set of features designed to make the internet publishing experience easy. WordPress blogs now reach a combined 70 million global visitors and 300 million pageviews each month.

You can learn more about WordPress at http://www.wordpress.org

The BitNami WordPress Stack greatly simplifies the installation of WordPress and runtime dependencies on Amazon EC2. It includes ready-to-run versions of Apache, MySQL and PHP. BitNami WordPress Stack is distributed for free under the Apache 2.0 license.

In the Wild…

BitNami WordPress Stack - Mozilla Firefox

BitNami WordPress Stack

amazonaws.com https://ec2-107-22-13-224.

Google

BITNAMI

Welcome!

The BitNami WordPress Stack greatly simplifies the installation of WordPress and runtime dependencies on Amazon EC2. It includes ready-to-run versions of Apache, MySQL and PHP. BitNami WordPress Stack is distributed for free under the Apache 2.0 license.

WordPress

You can learn more about BitNami at http://bitnami.org

WordPress is an open source, standards-compliant, fast, light and free personal publishing platform. The project was started in 2003 as a personal publishing platform, with a set of features designed to make the internet publishing experience easy. WordPress blogs now reach a combined 70 million global visitors and 300 million pageviews each month.

You can learn more about WordPress at http://www.wordpress.org

The BitNami WordPress Stack greatly simplifies the installation of WordPress and runtime dependencies on Amazon EC2. It includes ready-to-run versions of Apache, MySQL and PHP. BitNami WordPress Stack is distributed for free under the Apache 2.0 license.

In the Wild…

Qualys SSL Labs - Projects / SSL Server Test / cert.kandek.com - Mozilla Firefox

Qualys SSL Labs - Projects / SS…

ssllabs.com https://www.ssllabs.com Google

QUALYS SSL LABS

Home Qualys.com Projects Cont

You are here: Home > Projects > SSL Server Test > cert.kandek.com > 107.22.13.224

SSL Report: cert.kandek.com (107.22.13.224)

Assessed on: Wed Feb 01 23:32:55 UTC 2012 | Clear cache

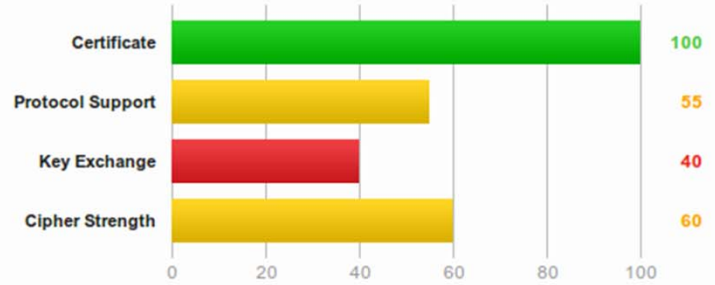
Scan Another

Summary

Overall Rating

C

52



The scores are explained in the SSL Server Rating Guide 2009

This server is vulnerable to the BEAST attack (more info)

In the Wild…

Qualys SSL Labs - Projects / SSL Server Test / cert.kandek.com - Mozilla Firefox

Qualys SSL Labs - Projects / SS…

ssllabs.com https://www.ssllabs.com Google

Protocols

TLS 1.2	No
TLS 1.1	No
TLS 1.0	Yes
SSL 3.0	Yes
SSL 2.0+ upgrade support	Yes
SSL 2.0 *INSECURE*	Yes

Cipher Suites (sorted by strength; we could not determine if server has a preference)

SSL_RC4_128_EXPORT40_WITH_MD5 (0x20080) *WEAK*	40
SSL_RC2_128_CBC_EXPORT40_WITH_MD5 (0x40080) *WEAK*	40
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) *WEAK*	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) *WEAK*	40
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (0x8) *WEAK*	40
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (0x14) DH 512 bits (p: 64, g: 1, Ys: 64) *WEAK*	40
SSL_DES_64_CBC_WITH_MD5 (0x60040) *WEAK*	56
TLS_RSA_WITH_DES_CBC_SHA (0x9) *WEAK*	56
TLS_DHE_RSA_WITH_DES_CBC_SHA (0x15) DH 1024 bits (p: 128, g: 1, Ys: 128) *WEAK*	56

In the Wild… - the Fix

ssllabs.com's own Apache

https://community.qualys.com/message/12495#12495

QUALYS® COMMUNITY

HOME NEW YOUR STUFF HISTORY BROWSE

You are here: Qualys Community > SSL Labs > Discussions

539 Views 1 Reply Latest reply: Dec 22, 2011 3:26 AM by Ivan Ristic

Ivan Ristic
59 posts since
Jul 23, 2010

Dec 22, 2011 3:26 AM (in response to wootic9)

ssllabs.com's own Apache SSL Config Directives

Here are the relevant directives:

```
# Disable SSLv2
SSLProtocol all -SSLv2
# Choose cipher suites
SSLHonorCipherOrder On
# Use only strong authentication and ciphers; prioritise RC4 to mitigate BEAST
SSLCipherSuite RC4-SHA:HIGH:!ADH
```

By the way, we are currently working on a Best Practices for SSL Deployment document, which should tell you all you need to know to properly deploy SSL. It will be published during the RSA Conference in February next year.

Report Abuse Like (0) Reply

In the Wild… - the Fix

ssllabs.com's own Apache

https://community.qualys.com/message/12495#12495

QUALYS® COMMUNITY

HOME NEW YOUR STUFF HISTORY BROWSE

```
# Disable SSLv2
SSLProtocol all -SSLv2
# Choose cipher suites
SSLHonorCipherOrder On
# Use only strong authentication and ciphers; prioritise RC4 to mitigate BEAST
SSLCipherSuite RC4-SHA:HIGH:!ADH
```


```
# Choose cipher suites
SSLHonorCipherOrder On
# Use only strong authentication and ciphers; prioritise RC4 to mitigate BEAST
SSLCipherSuite RC4-SHA:HIGH:!ADH
```


By the way, we are currently working on a Best Practices for SSL Deployment document, which should tell you all you need to know to properly deploy SSL. It will be published during the RSA Conference in February next year.

Report Abuse Like (0) Reply

In the Wild… - the Fix

root@ip-10-98-5-207: /opt/bitnami/apache2/conf/extra

```
SSLEngine on

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL

#   Server Certificate:
#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that a kill -HUP will prompt again.  Keep
#   in mind that if you have both an RSA and a DSA certificate you
#   can configure both in parallel (to also allow the use of DSA
#   ciphers, etc.)
SSLCertificateFile "/opt/bitnami/apache2/conf/server.crt"
#SSLCertificateFile "/opt/bitnami/apache2/conf/server-dsa.crt"

#   Server Private Key:
#   If the key is not combined with the certificate, use this
#   directive to point at the key file.  Keep in mind that if
#   you've both a RSA and a DSA private key you can configure
#   both in parallel (to also allow the use of DSA ciphers, etc.)
SSLCertificateKeyFile "/opt/bitnami/apache2/conf/server.key"
                                                        90,1          40%
```

In the Wild… - the Fix

```
root@ip-10-98-5-207: /opt/bitnami/apache2/conf/extra
SSLEngine on

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
# Disable SSLv2
SSLProtocol all -SSLv2
# Choose cipher suites
SSLHonorCipherOrder On
# Use only strong authentication and ciphers; prioritise RC4 to mitigate BEAST
SSLCipherSuite RC4-SHA:HIGH:!ADH

#   Server Certificate:
#   Point SSLCertificateFile at a PEM encoded certificate.  If
#   the certificate is encrypted, then you will be prompted for a
#   pass phrase.  Note that a kill -HUP will prompt again.  Keep
#   in mind that if you have both an RSA and a DSA certificate you
#   can configure both in parallel (to also allow the use of DSA
#   ciphers, etc.)
SSLCertificateFile "/opt/bitnami/apache2/conf/server.crt"
#SSLCertificateFile "/opt/bitnami/apache2/conf/server-dsa.crt"

                                                        97,0-1        39%
```

In the Wild… - the Fix

Qualys SSL Labs - Projects

https://www.ssllabs.com/ssldb/analyze.html?d=cert%2ekandek%2ecom&s=107%2e22%2e13%2e224

QUALYS SSL LABS

Home Qualys.com Projects Contac

You are here: Home > Projects > SSL Server Test > cert.kandek.com > 107.22.13.224

SSL Report: cert.kandek.com (107.22.13.224)

Assessed on: Sat Feb 04 00:47:31 UTC 2012 | Clear cache

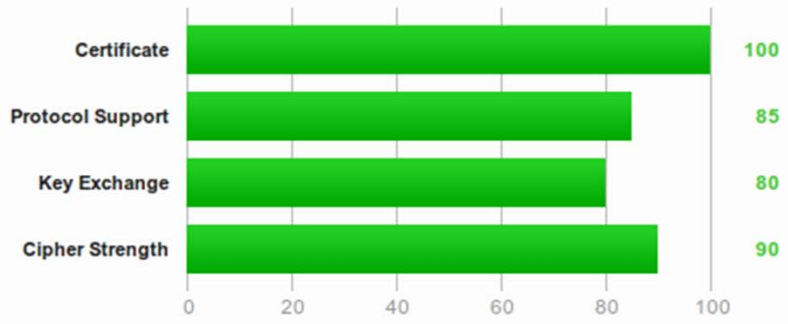
Scan Another >

Summary

Overall Rating

A

85



The scores are explained in the SSL Server Rating Guide 2009

In the Wild… - the Fix

ssllabs.com's own Apache

https://community.qualys.com/message/12495#12495

QUALYS® COMMUNITY

HOME NEW YOUR STUFF HISTORY BROWSE

You are here: Qualys Community > SSL Labs > Discussions

By the way, we are currently working on a Best Practices for SSL Deployment document, which should tell you all you need to know to properly deploy SSL. It will be published during the RSA Conference in February next year.

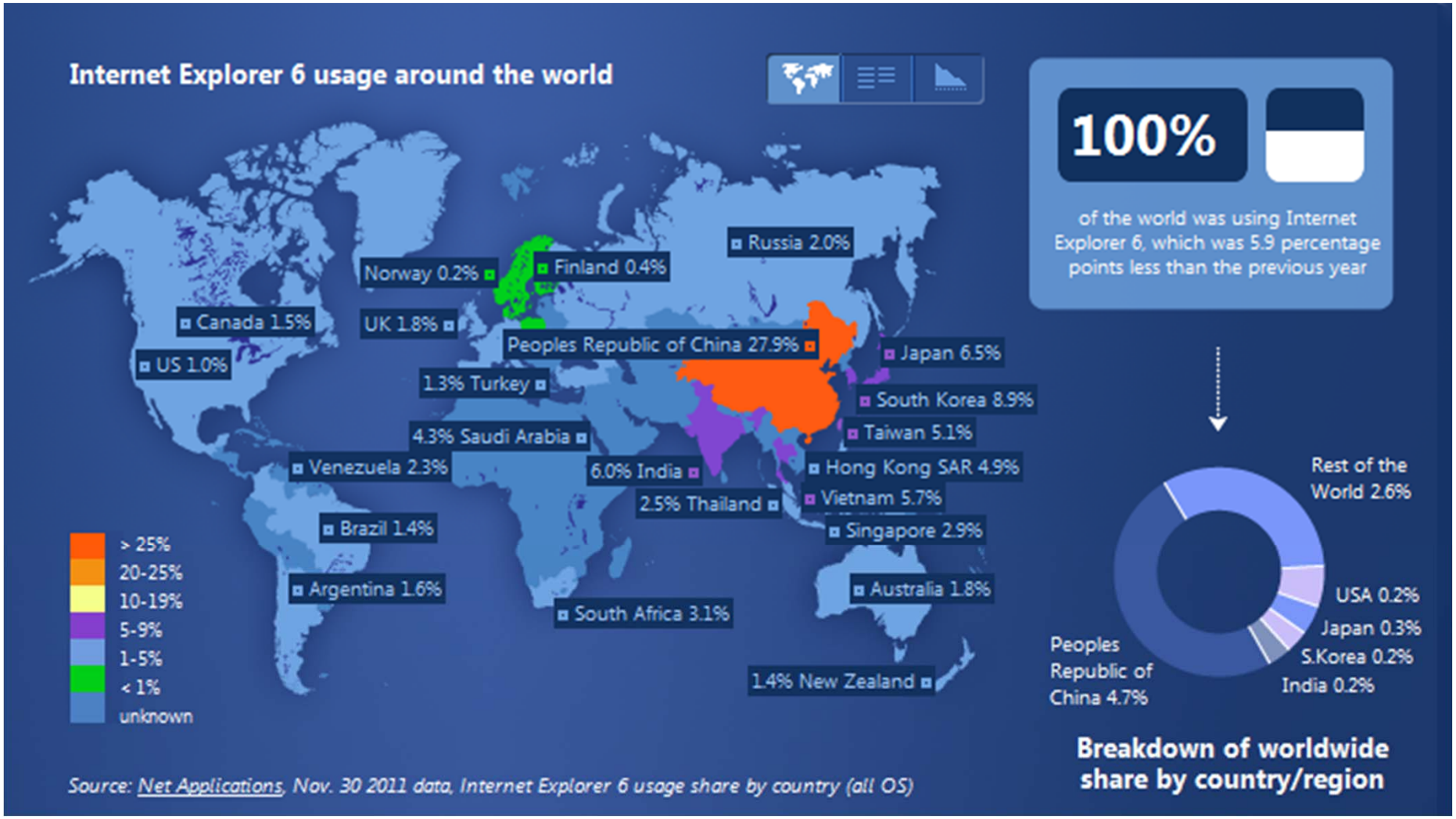
Jul 23, 2010

```
# Disable SSLv2
SSLProtocol all -SSLv2
# Choose cipher suites
SSLHonorCipherOrder On
# Use only strong authentication and ciphers; prioritise RC4 to mitigate BEAST
SSLCipherSuite RC4-SHA:HIGH:!ADH
```

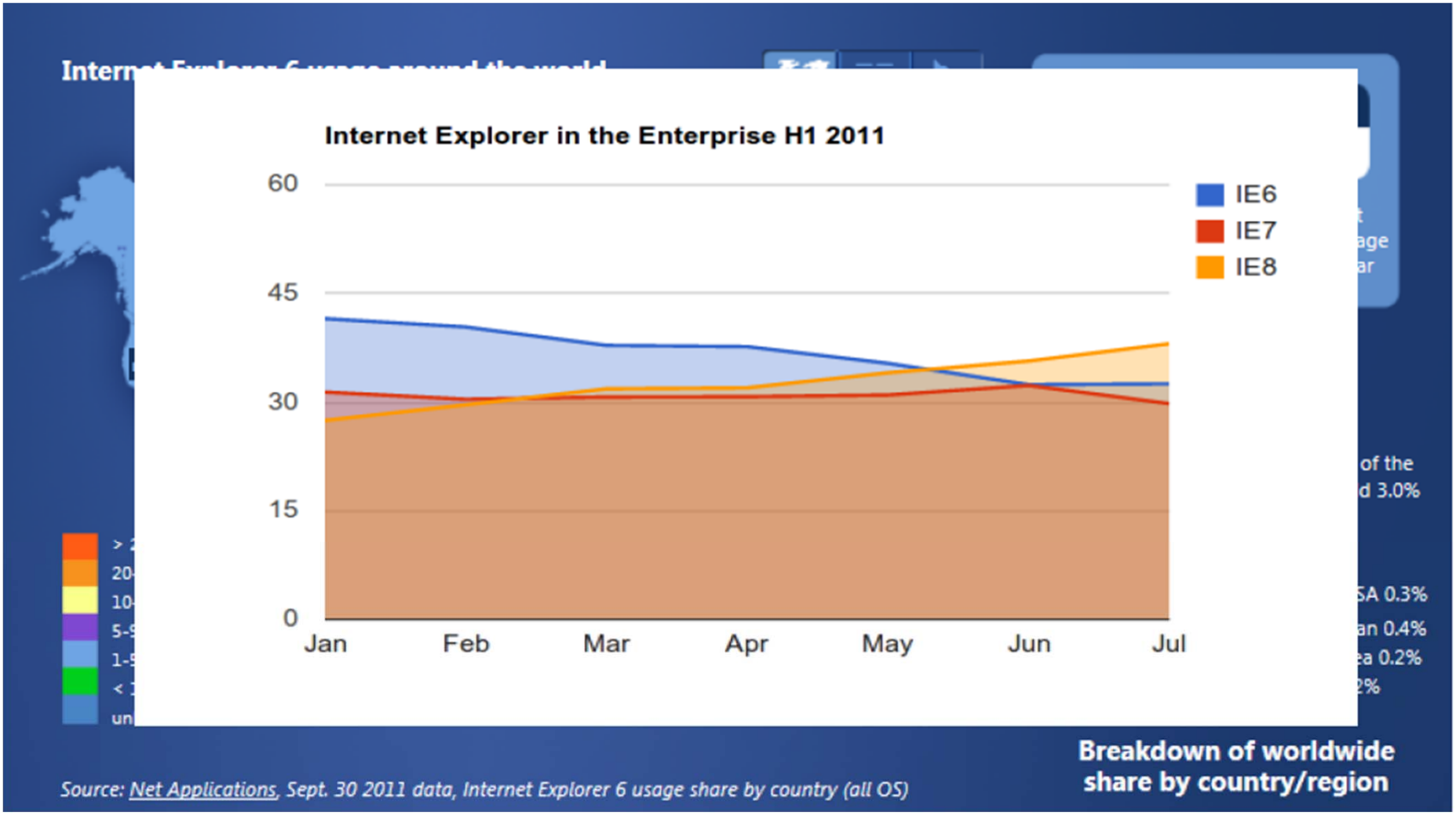
By the way, we are currently working on a Best Practices for SSL Deployment document, which should tell you all you need to know to properly deploy SSL. It will be published during the RSA Conference in February next year.

Report Abuse Like (0) Reply

Is Internet Explorer 6 a Problem? No?

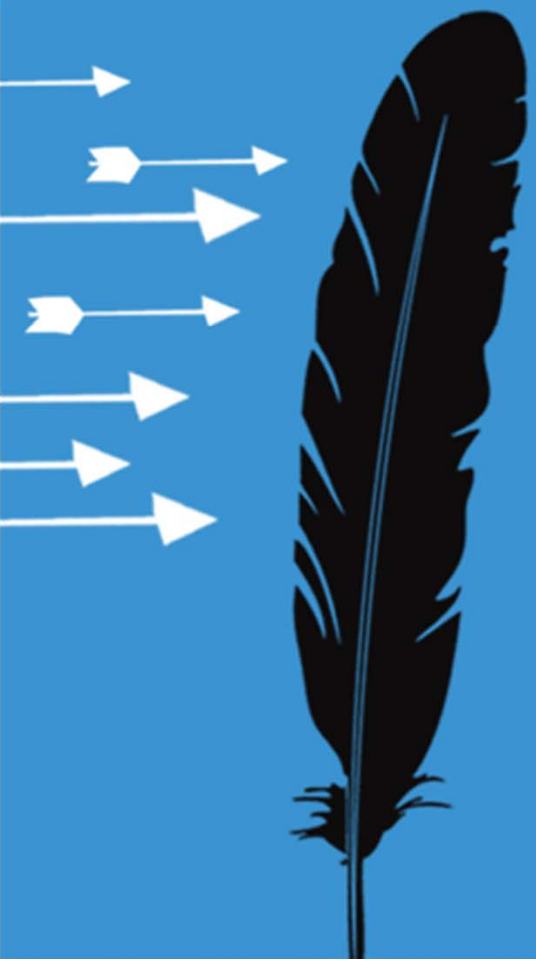


Actually, yes. IE6 Still In Wide Use



Lessons Learned

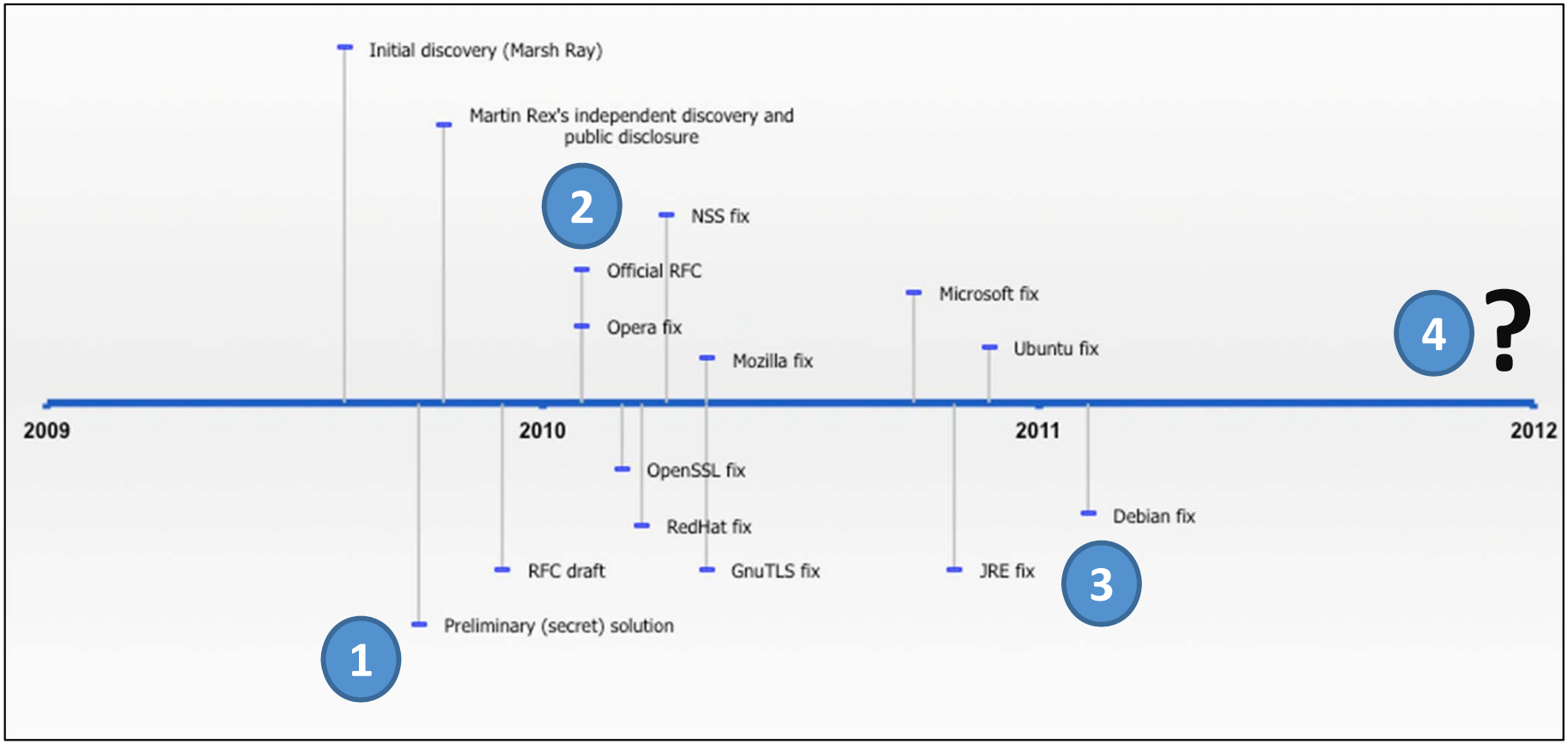
- If a system allows for an insecure configuration, the majority of the installations will be insecure
  - Vendors must actively prune libraries and products to remove obsolete features
  - Ship secure by default
  - Bug fix-only maintenance not good enough
- End-user products have a very long life, and will not be replaced even if insecure



Protocol Attacks

SSL/TLS Authentication Gap Timeline

- Flaw in the protocol that allowed one TCP connection to carry multiple independent SSL/TLS streams
- A rare example that allows us to follow the fix timeline:

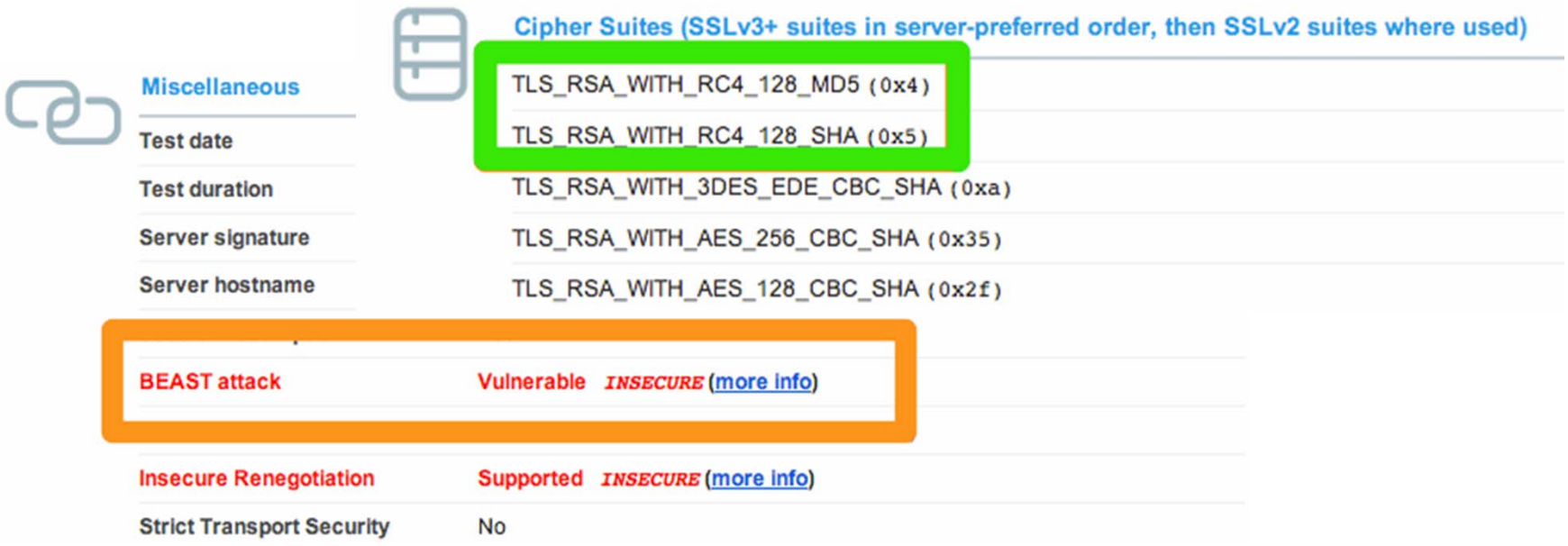


Lessons Learned

- Fixing flaws in protocols takes time:
  1. Allow 6 months to fix the protocol itself
  2. Further 12 months to fix implementations
  3. Further 24 months for “everyone” to patch

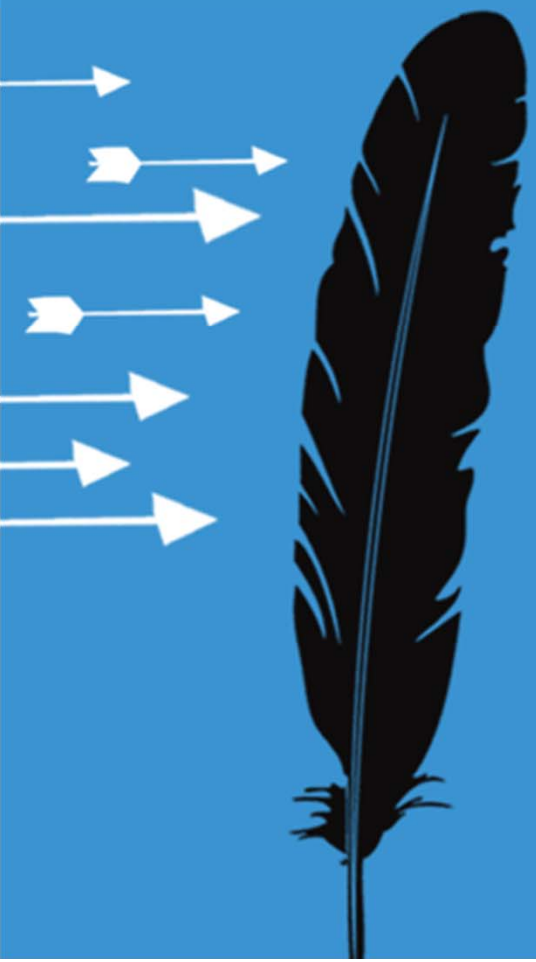
BEAST Attack Against CBC Suites

- Vulnerability in SSL 3.0 and TLS 1.0
- Decrypts small parts of traffic (e.g., cookies)
- **Fixed a long time ago in TLS 1.1 (2006)**
- **But TLS 1.1+ ignored by majority ("Attack not practical")**



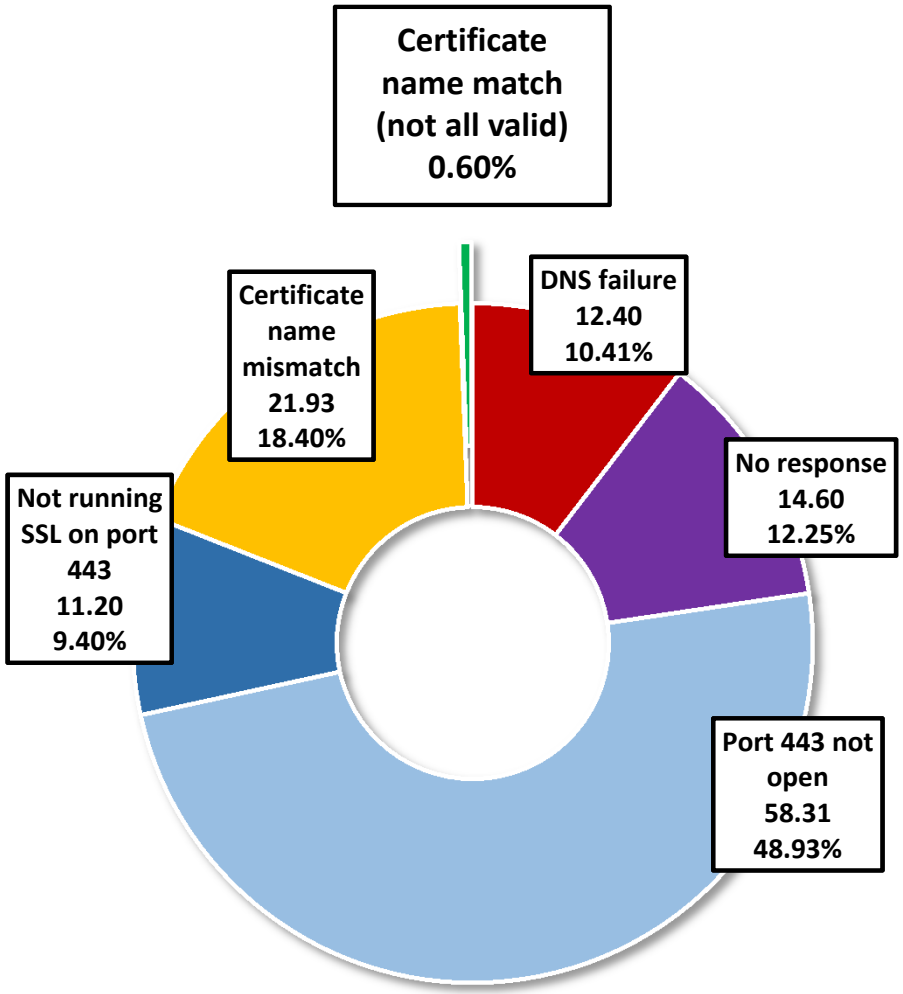
Lessons Learned

- Attacks get only better over time
  - Do not leave obvious flaws without a fix, even if an exploit is not currently available
  - Someone will find a way to exploit the flaw, if it is important or interesting enough



SSL/TLS Application Issues

Very Few Sites Actually Use SSL

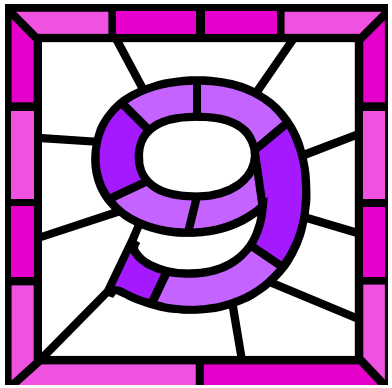


- The pie chart on the left represents a scan of about 120 million domain name registrations
- SSL is not very common, across all registrations
- Today, we are at **0.4%** across registered domains and **1%** across active sites
- However, about **10%** of the Alexa's Top 1M sites support SSL

Sites With SSL Use It Incorrectly

Virtually all sites are a mix of HTTP and HTTPS.

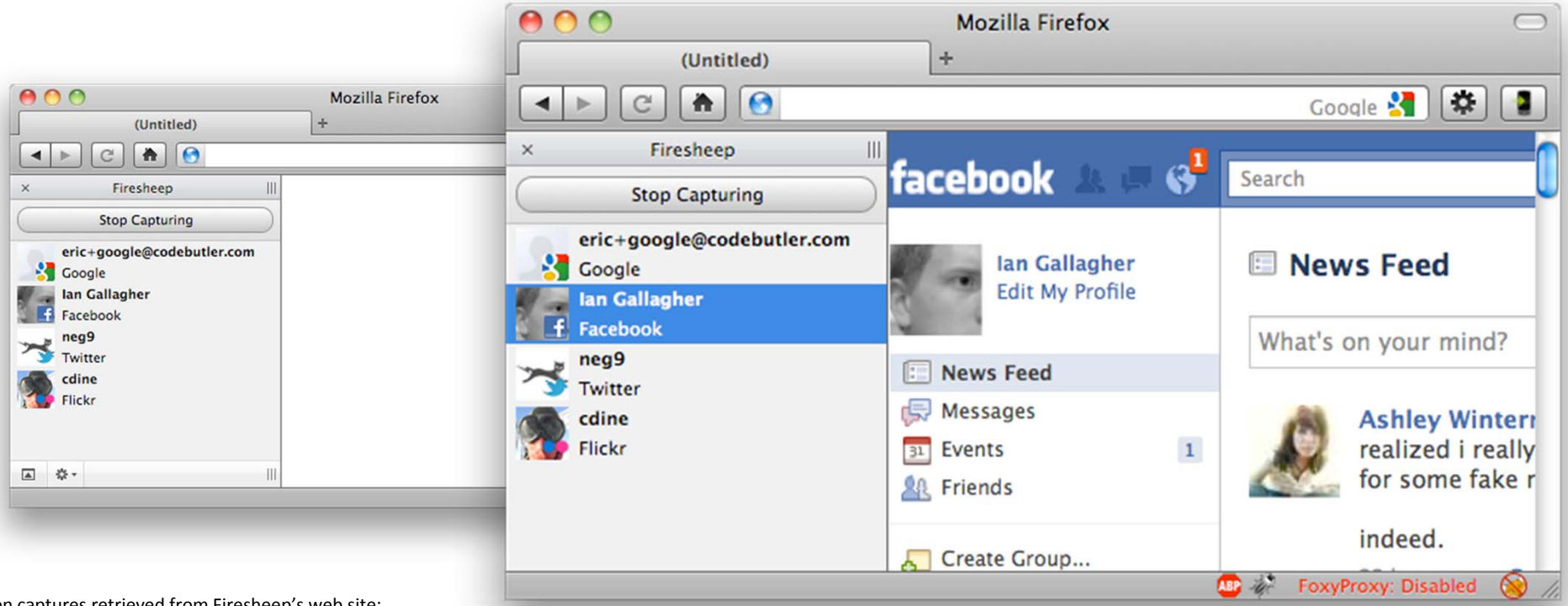
- User's first request to a site is virtually always unprotected, which means it can be hijacked
- Over **67%** not well configured
- Nearly **54%** support SSLv2
- About **20%** mix content within the same page
- About **54%** do not use SSL to protect authentication
- About **15%** use session cookies that are not secure



We found only 9 properly secured SSL sites among Alexa's top 1 million

Firesheep: Account Hijacking Made Easy

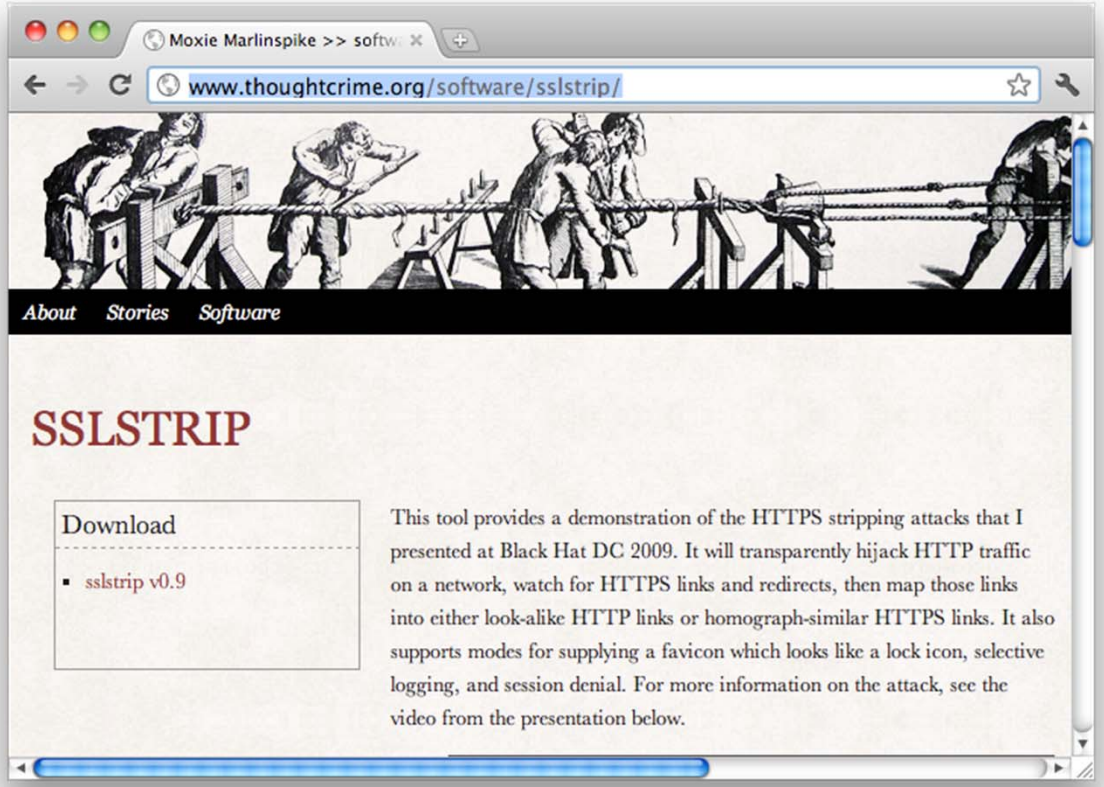
1. Install Firefox plug-in
2. Press “Start Capturing”
3. Choose account to hijack



Screen captures retrieved from Firesheep’s web site:
http://codebutler.com/firesheep

SSLStrip: HTTP Users Stay With HTTP

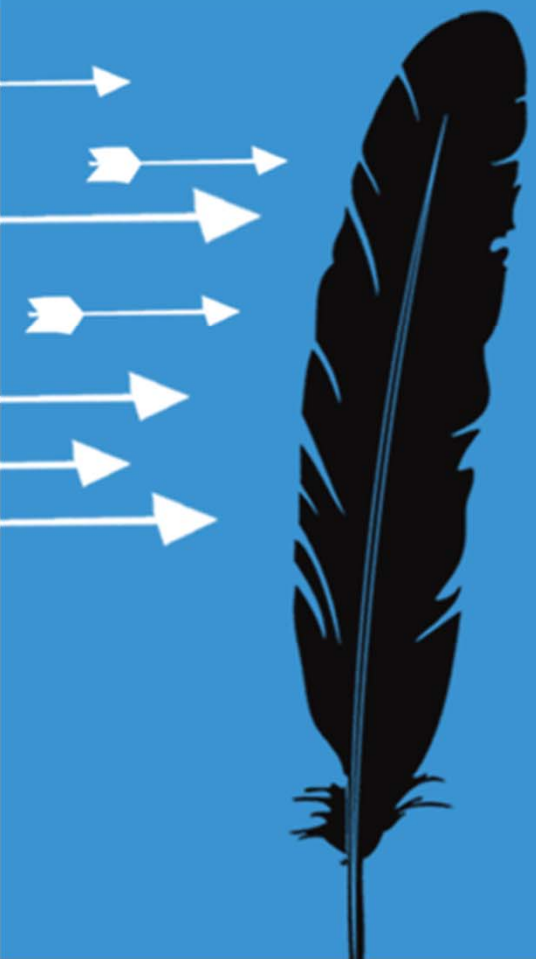
1. Victim's traffic re-routed through attacker's machine
2. Links to HTTPS are stripped
3. Victim stays in HTTP, under full control of attacker



The attack can be fully automated

Lessons Learned

- Developers are too busy adding features to do the right thing when it comes to security
- The path of least resistance always wins



PKI Trust Issues

Where Does Trust Come From?

- Users trust browsers and operating systems
- They, in turn, trust a number of CAs
- In practice, the trust comes from:
  - Hundreds of certificate authorities
  - Their resellers and partners
  - Other organizations (typically large organizations) that have purchased *intermediate certificates*
- **Any one of these can sign any domain name**

Recent Attacks Against PKI

- Comodo (March 2011)
  - One successful attack and at least one unsuccessful one that we know of
  - Reseller compromise lead to issuance of certificates for 7 high-profile domain names
  - No reports of successful use of the rogue certificates
- DigiNotar (July-August 2011)
  - Full CA compromise (and without a timely notification)
  - Over 500 rogue certificates issued; some used
  - *DigiNotar blacklisted by all major vendors*

Mitigation: Certificate Authority Pinning

- CA pinning: require specific CA for domain name
- The DigiNotar compromise was detected by the CA-pinning feature in Chrome
  - There is no standard way to do that
  - Google used it for themselves because they could
- You *may* be able use the same mechanism:
  - Adam Langley (Google): *"If you run a large, high security site and want Chrome to include pins, let me know."*
- RFC: Public Key Pinning Extension for HTTP
  http://tools.ietf.org/html/draft-ietf-websec-key-pinning-01

Possible Future: DANE (DNSSEC)

- DNSSEC is a secure version of the DNS protocol
- DANE* leans on DNSSEC to add support for *out-of-bound certificate validation*
- It provides support for:
  - Certificate Authority pinning
  - Certificate pinning (has to be signed by valid CA)
  - Self-signed certificates
- Problems to overcome:
  - No support for DNSSEC in clients
  - DNS registrar hack can hijack your domain name

(*) DNS-based Authentication of Named Entities

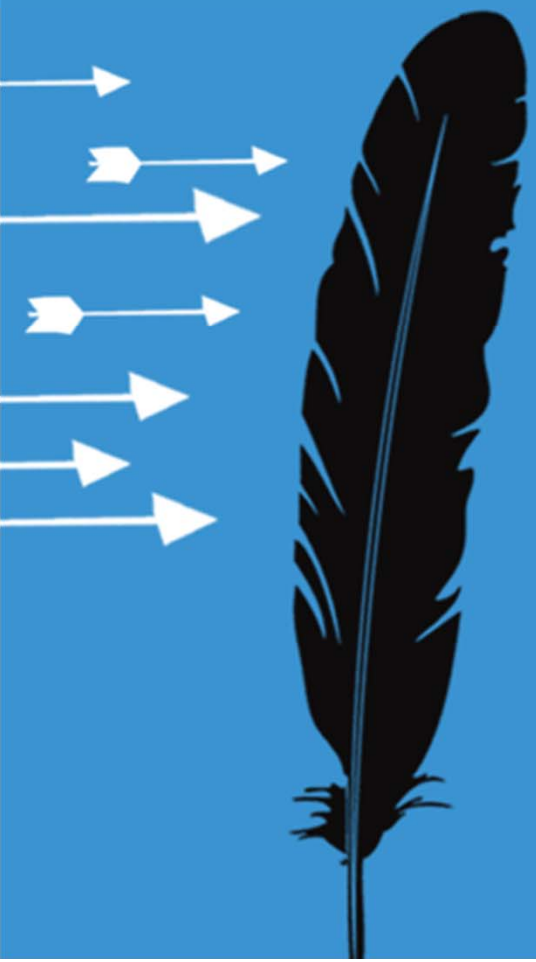
PKI Alternative: Convergence

- Introduced by Moxie Marlinspike* in August 2011
- Not a replacement for PKI, but a method of *abstracting trust decisions on the client side*
  - Client asks remote notaries to make trust decisions
  - Notaries are free to implement own decision logic
  - Clients are free to choose what notaries they trust
- Problems to overcome:
  - Needs reliable infrastructure, which may be very expensive

(*) Author of sslsniff and sslstrip

Lessons Learned

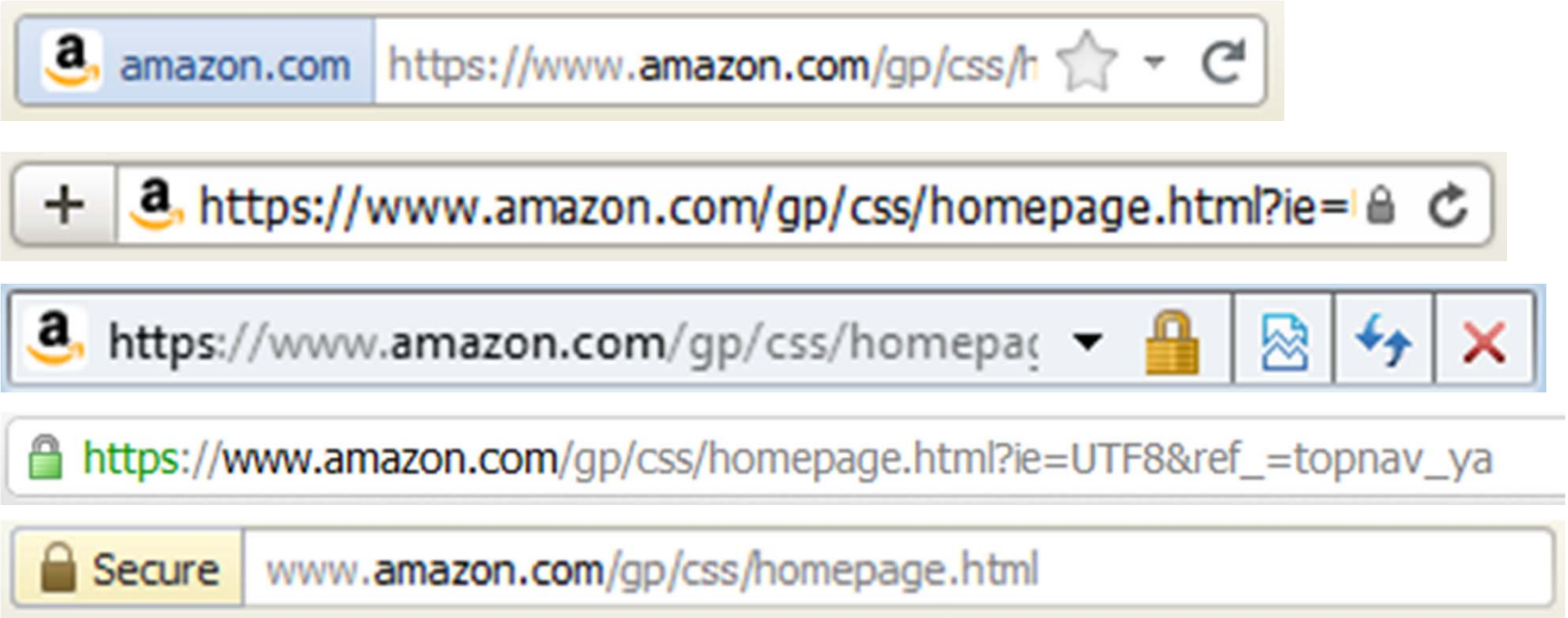
- Embedded trusted certificate stores are a liability for everyone: users, browser vendors, and certificate authorities
- At present, there are few incentives for CAs to improve the security of the current system
  - CAs do not compete on security
  - If you're large enough, no one can touch you
  - Little guys will burn



Browser Problems

SSL Indicators

- The padlock changes location with every new browser version
- Firefox does not use it any more



Extended Validation Certificate Indicators

- EV certificates want to be “the new padlock”
- Some browsers try to differentiate

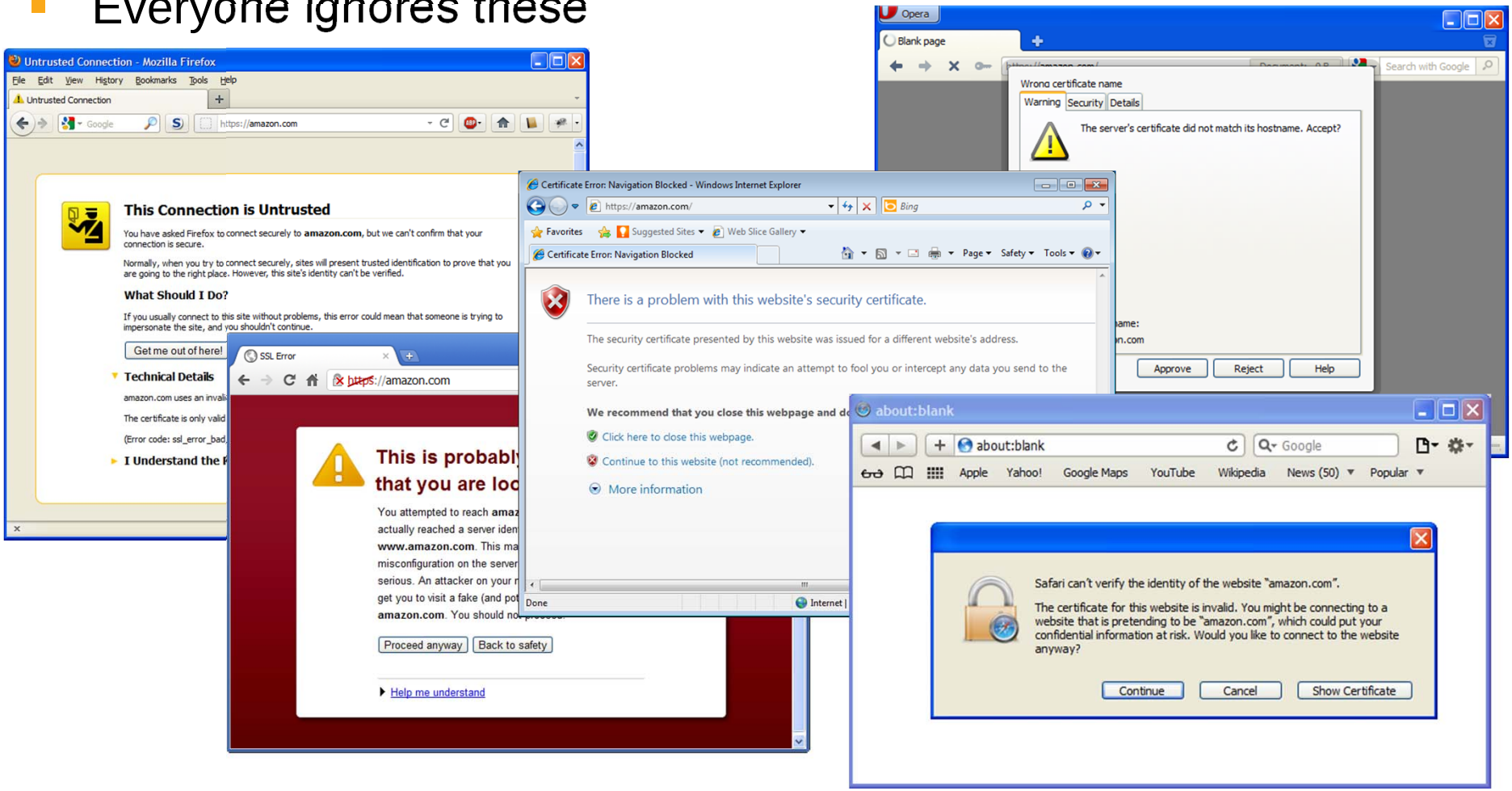
- Others, not so much

- No one cares, anyway

SSL Certificate Warnings

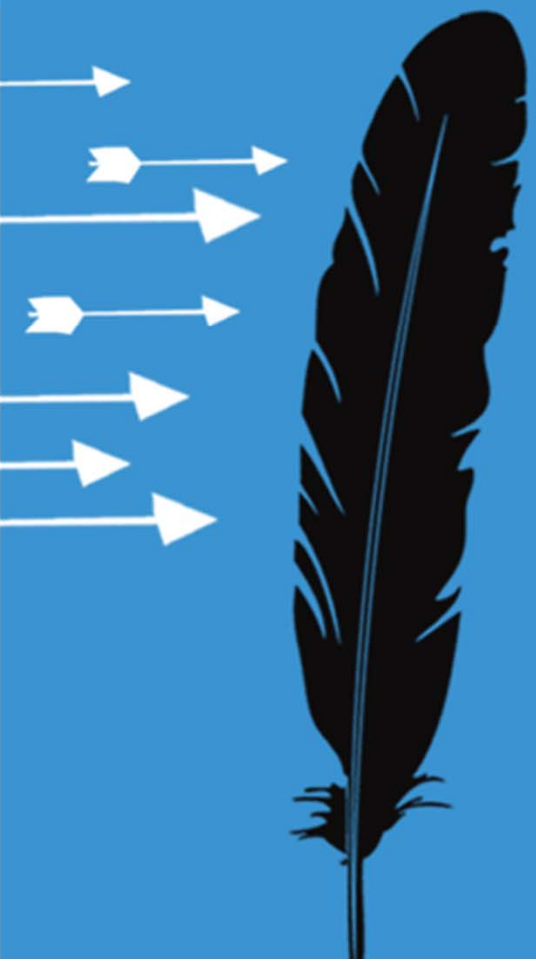
All browsers will accept invalid certificates, most with one click; Firefox requires that you do a little dance

- Everyone ignores these



Lessons Learned

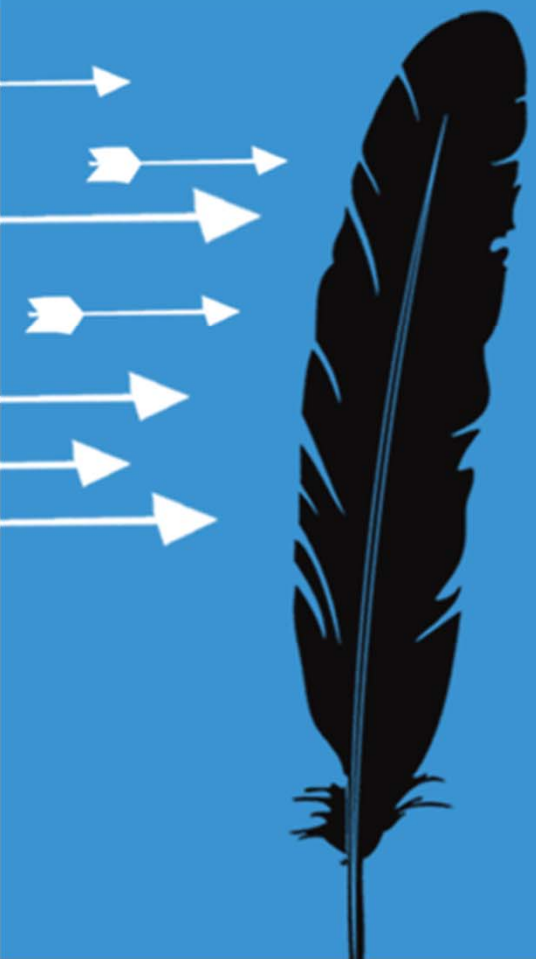
- Vendors of consumer products cannot afford to be strict when it comes to security
- They tend to be conservative, in order to preserve product usability and their market share



Lessons Learned

Summary of Lessons Learned

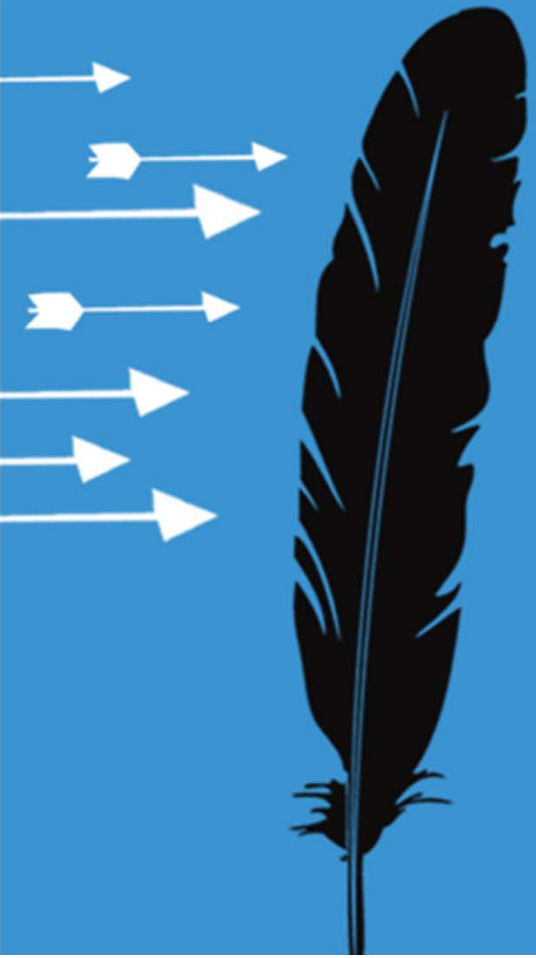
- Security must be **invisible** and **always enabled**, as well as **resilient** to configuration and programming errors, and consumer bypasses
- Complex security systems need constant supervision and guidance
  - We need independent bodies, free of financial conflict, that can **focus on security**
  - The ecosystem must be designed so that every participant has an **incentive to do better** when it comes to security



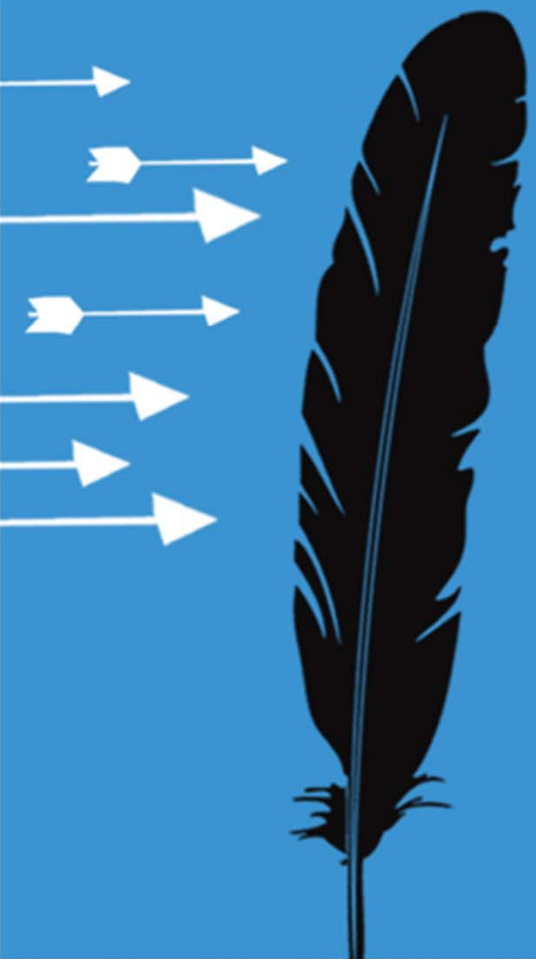
How to Apply What You Have Learned?

How To Apply What You Have Learned

- In the first 3 months following this presentation you should:
  - Identify business-critical public-facing web sites
  - Test each site for common certificate and configuration issues, as well as the renegotiation vulnerability
  - Instrument change to fix discovered weaknesses
- Within 6 months, you should:
  - Publish a checklist for secure SSL web deployment
  - Initiate a HSTS adoption program



Questions?



Bonus slides

Sources of SSL/TLS and PKI Data

- SSL Labs
  - Tested nearly all public SSL servers, checking certs, configuration and application-level flaws
  - Reports and raw data available
- SSL Observatory
  - Scanned entire IPv4 space looking for certificates
  - Reports and raw data available
- Opera Security Group
  - Weekly large-scale assessments
  - Findings on their blog