The view from a Browser Vendor: Reliable Root-Stores

Tom Albertson

Microsoft Corporation

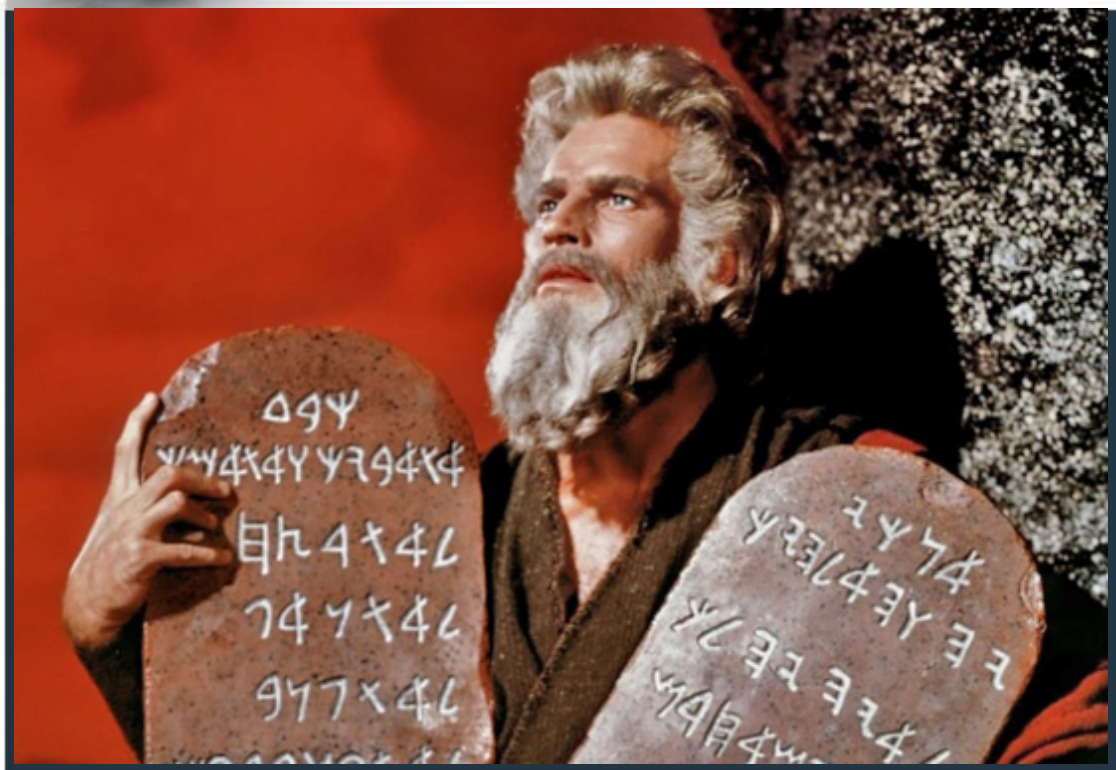
ETSI - European CA-Day

29. November 2012,
Bundesdruckerei
Oranienstraße 91 10969 Berlin

Agenda

- Where We Began
- Where We Are
- Where We Are Going

In the Beginning



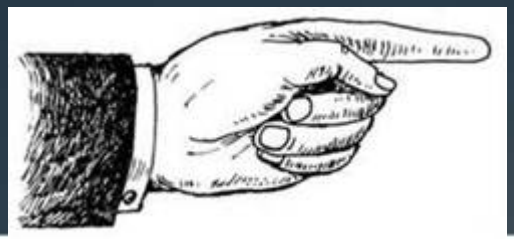
1. There was the Internet
2. And there was a CA (or two)…
3. ~~We wrote some rules~~
4. And distributed their root certificates (~~in Windows~~)
5. The Internet Grew
6. And Grew
7. And Grew
8. Suddenly there were *lots* more CAs!
9. Everywhere!
10. So we wrote a few more rules…

And Before We Knew It

There were LOTS and LOTS of CAs
And it was Basically Good

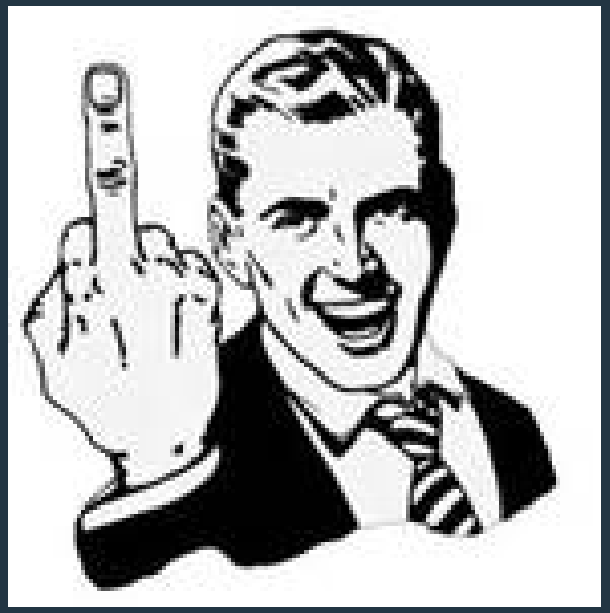
Our Rules were Few

- A few technical requirements (for our mutual protection)
- A few general requirements (for our sanity as distributors)
- A means of verifying that the first two requirements were true
  - Audit
- The Same Rules for Everyone, Rigorously Enforced



Then Came the Rains

- ALONG CAME THE HACKERS!
- WHO MESSED UP SEVERAL CAs
- And harmed our customers



COMODO
Creating Trust Online™

And there was a Flurry of Activity

14 December 2011

CA/Browser Forum Approves Baseline Requirements for SSL/TLS Certificates

First industry-wide standard for the issuance and management of SSL/TLS digital certificates

DOWNLOAD THE DOCUMENT

Network Security Controls

Network and Certificate System Security Requirements (adopted on 3 August 2012 with an Effective Date of 1 January 2013)

F. **Certification Authority Pra**

Section F is introduced to collect interim the Windows Root Certificate Program. Requirements under Section F are enforced until such a time that they may be incorporated into the audit criteria of qualified audit authorities (WebTrust, ETSI). Technical Requirements in this Section may be modified in the process of incorporation into those audit criteria.

1. The CA will implement multi-factor authentication (ex. smartcard and password, biometric and password) for system or user accounts that can cause issuance or approval of certificates on behalf of the Program CA.

   Multi-factor authentication tokens will not be left in a permanent or semi-permanent state (ex. plugged into a device that accesses the root certificate chain and enables authorization of certificates), such that the integrity of the physical security separating root certificates from the organization's systems or authorized employees and accounts is compromised.

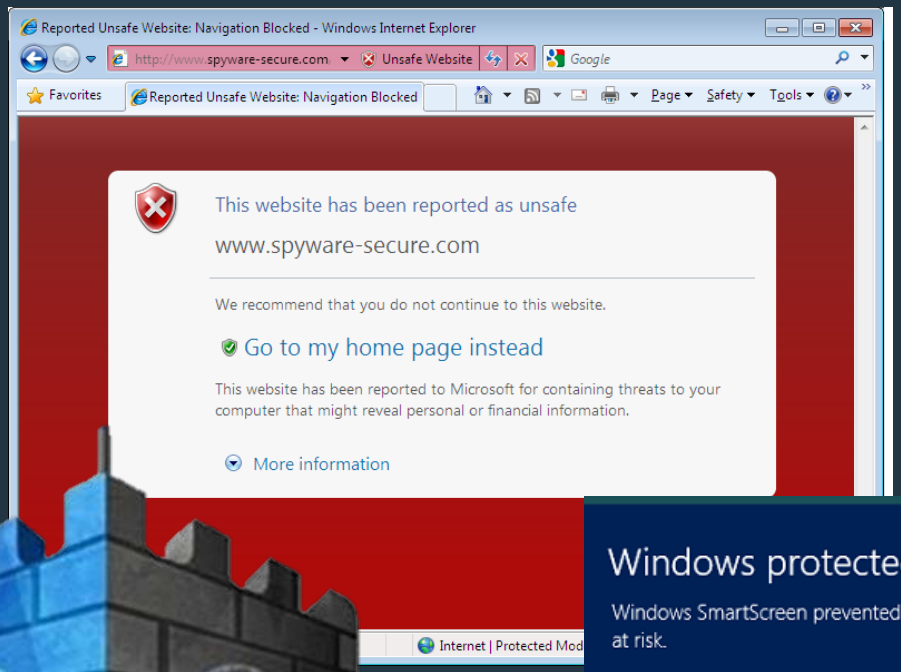
2. All root certificates distributed by the Program must be maintained in an offline state – that is, root certificates may not issue end-entity certificates of any kind, except as explicitly approved from Microsoft.

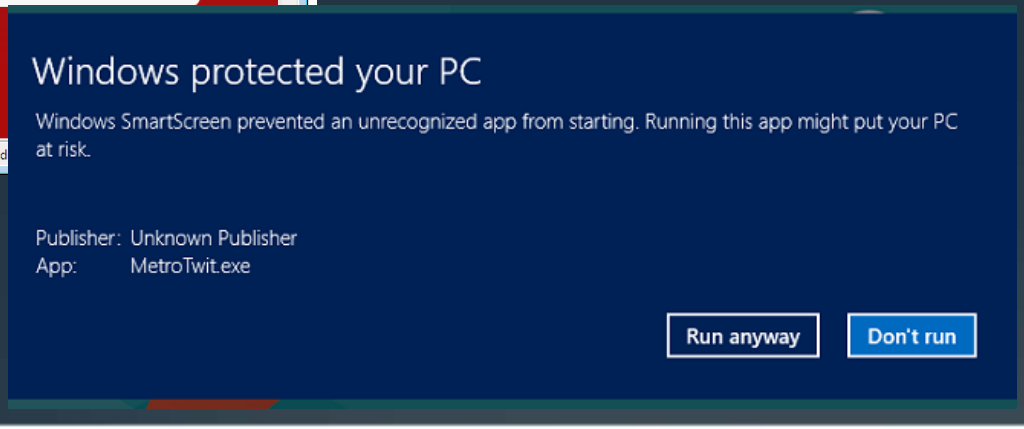
However

- The attention to the Problem was Good

So – Where Are We (Microsoft) Now?

- Much More Aware – and Effective against Bad Certs

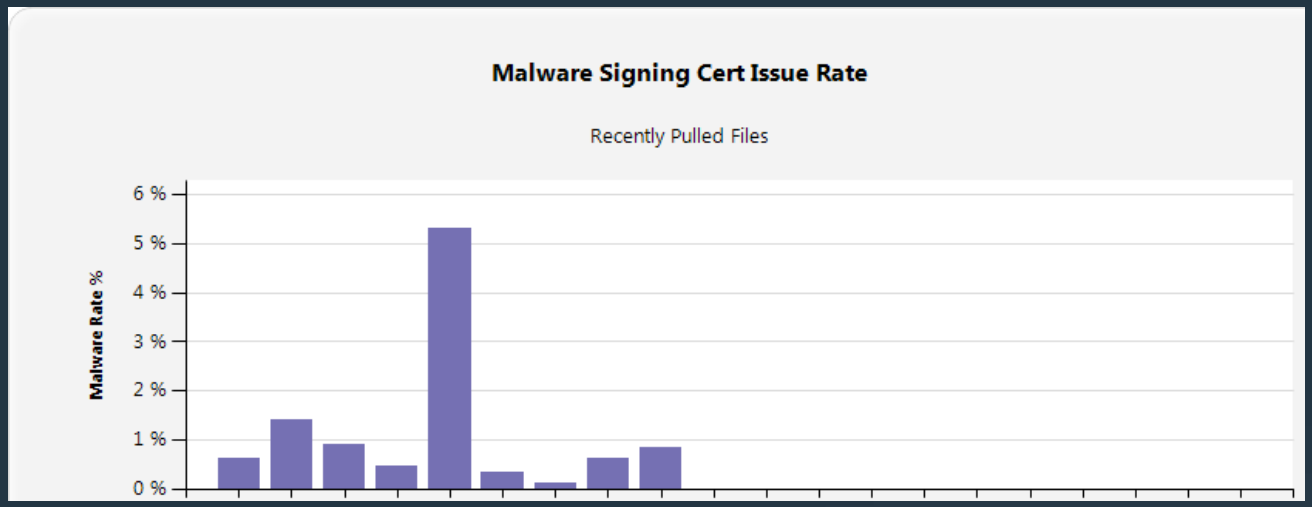




SmartScreen Filters on Internet Explorer & Windows 8, Treating Bad Certificates = Malware

Where is Microsoft Now, cont.?

Much more Active (but Still Reactive)
Utilizing Big Data (Bing, Windows Update, SQM)
Yielding Interesting Results



And Equivalent Data for SSL Sites (via Cert Tracking alpha, a la EFF – except far larger and more dynamic sample set)

And we have some more Tools

Automatic updater of revoked certificates (Disallowed CTL) - KB2677070, see http://support.microsoft.com/kb/2677070

- FAST response to bad roots and intermediates
- Effective Revocation within hours of release to Windows installed base *

*Windows Vista and later

* Provided users employ the Windows Update mechanism

So, Where Should We (Microsoft) Go?

(Doorway to Hell Cavern, Turkmenistan)

OR…

Maybe We Can Help Attack Bad Certs

Technical means will have to await future announcements

But based on what we're learn we are looking at:

1. Making Changes to the Windows Root Certificate Program
2. Making qualitative distinctions between CAs
   a. Based on actual threat profile (threat to Windows users)
   b. Based on actual observed certificate activity and validity
      - SSL and code signing issuers
      - qualified certificates
3. Making recommendations on PKI network security practices (hard lessons learned)

Questions, Links and Contacts

- Windows Root Certificate Program

  http://technet.microsoft.com/en-us/library/cc751157.aspx

  And

  http://social.technet.microsoft.com/wiki/contents/articles/3281.introduction-to-the-microsoft-root-certificate-program.aspx

  KB931125 on the Auto Root Update Mechanism, http://support.microsoft.com/kb/931125

  Tom Albertson, Program Manager, Trustworthy Computing (TwC)

  tomalb@Microsoft.com

  casubmit@Microsoft.com