Reducing the Tail Risk of CA Compromise by Enabling Trust in Regional CAs Using Language Community and Locale Annotations

Brad Hill
bhill@paypal-inc.com
@hillbrad

Presented at the NIST Workshop on Improving Trust in the Online Marketplace
April 10-11, 2013
A heuristic is a simple procedure that helps find adequate, though often imperfect, solutions to difficult problems.

-Daniel Kahneman
Background

• All Trusted Roots are Equal

• Compromise at any CA can impact all names for all users, globally

• Set of CAs is large and growing
  – Operating in 49 countries, many owned or controlled directly by sovereign governments
Who do I need to trust?

• Microsoft, Mozilla, etc. may have significant user bases or potential markets in many jurisdictions

• But any individual user needs to trust many fewer CAs

• Removing a CA from your root store is a manual process accessible only to experts
Result: Lots of tail risk from Certificate Authorities that most users will never legitimately encounter a certificate from.
Tail Risks

• Persian-speaking users in Iran had no need to trust a small CA serving the Dutch language community and Government of the Netherlands

• One country’s “lawful intercept” is another’s industrial espionage or human rights violation
Microsoft Trusted Root Program


• 352 Root Certificates

• 115 Controlling Organizations
  – 36 Governments
  – 74 Commercial Entities
  – 5 Enterprises
Blanks on the Map

- Only 49 of 206 (24%) sovereign nations have a MSFT-trusted CA within their borders
- Only 27 of 206 (13%) sovereign nations have a trusted, government-operated CA.

- Much room for growth here!
  - Good for the Internet as a whole
  - Bad for any individual user
Given the global nature of the Internet, are there manageable ways to address this risk?
Not with name constraints

• Maybe for a few government CAs:
  – .gov, .gouv.fr, ...

• But the most used gTLDs (.com, .org, .net, ...) are universal
  – Any commercial and perhaps some government CAs will want to support these
  – A “constraint” to .com is effectively meaningless
Related?
Internationalized Domain Names

• IDNs introduced a risk of spoofing using homoglyphs (e.g. example.com with Cyrillic ‘а’)

• IE 7’s algorithm:
  – Display in ASCII encoding by default (punycode)
  – Display in native encoding if the appropriate language pack is installed
    • As consequence of SW version or locale choice
    • As a user-installed add-on
The idea for certificates:

- Annotate CAs with the locales and language communities they serve
- Users have a geographic and language context
- When these contexts clash for names in the global space, alert the user
Example User: Aaron in Seattle

• A USA-based user with US English as the default locale and language

• Also an Israeli immigrant with the Hebrew language pack installed
example.com
Certified by MegaWholeWorld CA
Globally trusted CA: OK!
example.fr
Certified by Fromage CA
French-region CA, .fr ccTLD: OK!
tel-aviv.example.com
Certified by BenGurion CA
User has Hebrew language pack installed: OK!
This site was identified by an authority outside your normal region or language community. Click here to learn more...
The certificate for `shanghai.example.com`

was issued by **Black Cat White Cat Certification Authority (黑貓白貓)**

This Certification Authority normally serves the Chinese language community in The People's Republic of China, Macau SAR and Hong Kong SAR.

- **OK**

  Trust all Certification Authorities serving the Chinese language community.

- Something is wrong. Report this certificate.
“Soft Warning” Enables Situational Trust

- All CAs still installed and enabled by default
  - All CAs can issue in .com without warnings to their own regional + language customer base

- Detective, not Preventative Control

- Warning would be in-context and expected in most situations they occur
  - Booking a foreign hotel, applying for a visa, etc.
NOT ANOTHER DIALOG!!

• Yes... but....this is not meaningless crypto mumbo-jumbo

(no data yet, but my hunch is that...)

• Users already have good working concepts of governments, countries and languages and are able to apply those concepts to most sites they visit
Who will build the lists?

• Governments mandatorily opted-in
  – Perhaps too much legal or geopolitical risk for browser vendors to go farther than this

• Smaller or regional CAs may volunteer in order to reduce their attractiveness as a target

• Community-curated lists an easy possibility

• Or commercially-curated
  – As part of anti-virus/malware or trust broker software
Browsers may eventually set differential requirements directly

• Audit by globally-certified 3rd party vs. possibly unreliable local audit regimes or self-asserted government audits

• As a non-death-penalty punishment
  – E.g. as with revocation of EV bit for TurkTrust incident

• As part of their own community standards
  – E.g. Mozilla might restrict CAs operating in countries where they consider there to exist human rights issues around surveillance, state coercion, etc.
A Band-Aid, not a Panacea

• Top 8-10 global CAs that issue >95% of certificates cannot have meaningful constraints of this type
  – Perhaps few or no commercial CAs will opt-in

• Requires a user at the keyboard to make a decision based on a warning

• Does significantly reduce the attack surface for an opportunistic adversary who wishes to remain undetected
  – “herd immunity” for most users who don’t care from a tiny number who will

• Does “automatically” scale with lots of new gTLDs
  – Though new regional TLDs will need some annotation
A heuristic produces wrong answers sometimes

• Mappings are imperfect, languages and borders are messy
  – North / South Korea
  – Taiwan / China
  – Punjabi in India and Pakistan

• ccTLDs used as *de facto* gTLDs: .tv .ly

• From perspective of US consumer:
  – Is Samsung a Korean or Japanese company?
  – Is Motorola a US or Japanese company?
So, why do it?

• Quick and easy to implement relative to many other solutions on the table

• Can re-use or slightly modify existing technologies like Trust Anchor Management Protocol (TAMP) [RFC 5934]

• Significant, long-term attack surface reduction

• Targets threat scenarios most likely to cause large-scale loss of trust by the public
Work to be done:

• Can be done entirely by any individual user agent
• If interoperability in community-curated annotations is desired:
  – Add to TAMP/CMS to allow conveyance of additional unsigned attributes for Apex Trust Anchors
  – Need additional data mapping regional TLDs to language communities
  – Standardize a subscription mechanism?
  – PKIX WG at IETF retiring – could be done as an AD sponsored experimental draft
QUESTIONS?

Brad Hill   @hillbrad