Revocation Timelines

Discussion lead by Ben Wilson

Current Baseline Requirements

Section 4.9.1.1 of the TLS Baseline Requirements (TLS BRs) states,

“The CA … SHALL revoke a Certificate within 5 days if one or more of the following occurs:

… (12) The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA’s Certificate Policy or Certification Practice Statement.”

Section 4.9.1.1 of the Code Signing Certificate Baseline Requirements and of the S/MIME Certificate Baseline Requirements are very similar.

Problem

Recently numerous incidents of delayed revocation beyond the CA/Browser Forum's 5-day period.

The BRs are absolute; they don't contain any exceptions or mitigations.

Ignoring a problem does not make it go away – the Forum needs to address the issue of delayed revocation.

Total automation and eliminating issuance to "critical" services are only partial solutions.

Still, incidents such as Heartbleed highlight the importance of being able to quickly revoke certificates on a massive scale.

Examples of Critical Industry Sectors and Systems Affected by Immediate Revocation

Context: Without talking yet about delayed revocation, here are some sectors/systems that are likely affected by immediate revocation:

- Government (tax, revenue, law enforcement, postal services)
- Financial (banking, payments, insurance)
- Healthcare (medical devices)
- Transportation (planes, trains, and automobiles)
- Telecommunications
- Economic (supply chains)
- Energy

Mozilla Guidance on Delayed Revocation Incidents

Mozilla does not grant exceptions to the revocation timelines in the Baseline Requirements, but does acknowledge that CAs might face “exceptional circumstances” where revocation might cause “significant harm”.

Immediate revocation is challenging for CAs who are required to comply, yet balance the need for security with the potential harm of revocation.

- **What are “exceptional circumstances”?**
- **What is “significant harm”?**

Better Requirements; Clearer Guidelines and Definitions

Questions:

Can BR Section 4.9.1.1 be unambiguously modified?

- Should the Forum revise deadlines for revocation?

How should critical infrastructure and sensitive environments be treated?

Can “exceptional circumstances” and “significant harm” be defined, or can other criteria be developed?

- Could CAs provide sufficient detail to support assertions of “exceptional circumstances” and “significant harm”?

What other things might the Forum do to enhance incident reporting and auditing to ensure CAs are accountable for delayed revocations?

What can CAs do to improve timeliness of revocation?

Can CAs provide better, more comprehensive explanations and justifications for delayed revocations, along with clearer timelines for when problematic certificates will be revoked?

How can CAs engage more with their Subscribers with training and education on certificate replacement and automation?

Should CAs be required to assess where a certificate will be used?

Why & Why not?

How can CAs promote the use of automated certificate management tools and ensure that Subscribers adopt these methods?

What other things can be done?

Conclusions (Ben's High-Level Observations)

We cannot control how Subscribers will use or misuse Certificates, but Subscribers need to be educated about revocation and take on responsibility, and CAs need to take on compliance obligations. Automation needs to be promoted.

We should amend parts of the Baseline Requirements (sections 3.2.2.4, 4.9.1, and 9.6) re: domain validation methods, certificate revocation drivers (e.g. security vs. compliance), subscriber agreements, etc.

In the BRs, we might be able to improve upon Mozilla's guidance re: potential impact and significant harm, but we do not have clear consensus on how to address all the issues associated with "critical systems".

Not every claim of critical infrastructure uses TLS properly. While some critical public sites use TLS to communicate with Relying Parties, guidance could differentiate those uses that are "legitimate" or "proper" and those that are not.