Certificate Revocation With CRLSet

Keith Bogart

CCIE #4923

- kbogart@ine.com
- @keithbogart1
- linkedin.com/in/keith-bogart-2a75042

CCIE Routing & Switching

Topic Overview

- CRLSet Functionality
- CRLSet Example
- CRLSet Challenges

CRLSet

- Google Chrome does not utilize CRLs or OCSP, it utilizes CRLSets.
- Google Chrome's method of checking for revoked Certificates.
- CRLSet is;
  - A carefully selected collection of revoked-certificate serial numbers published by many different certificate authorities.
  - Google's own, compiled/curated CRL which is automatically downloaded into Chrome browser.
  - Lists are auto-updated by regularly crawling the CRLs from the major CAs around the world.

The "Chromium Project" states that CRLSets, "are fetched infrequently (at most once every few hours)"

CRLSet Example

The first part is a short JSON-format file header identifying the file version, content type, the CRLSet's sequence number, the count of certificate authority CRL sets appearing after the header, a short list of explicitly blocked certificates, and an expiration date for the data.

-

What differentiates the “explicitly blocked” serial numbers from the larger list? From the Chromium Project, “…CRLSet can quickly block certificates in emergency situations. As a secondary function they can also contain some number of non-emergency revocations.” So apparently the smaller list of explicitly blocked certs were done so due to some “emergency situation” (which is left to your imagination. Chromium developers won’t say what their criteria is.)

-

As of 2014 Microsoft had a total of 353 Trusted Root Certificates (CA’s). Compare that to the 53 in the list above.

CRLSet Challenges

- CRLSet is only composed of a subset of the hundreds of Certificate Authorities that exist globally.
- CRLSet is space-constrained to about 24k Revoked Certificates (there are millions of revoked Certificates worldwide)
- Chrome implicitly trusts Certificates that are not within their CRLSet
- More information can be found at:

  https://www.grc.com/revocation/crlsets.htm

To keep the CRLSet manageable, its size is strictly limited to 256k bytes. Consequently, an oft repeated admission by Google's engineers and spokespeople is that their CRLSet "does not contain all revoked certificates".

-

Chrome will blindly trust every revoked certificate that was originally signed by more than four fifths of the certificate authorities Microsoft trusts.