moz://a

CRLite

Scalable, Reliable Revocation

June 2018

What is CRLite?

Academic research presented at the 2017 IEEE Symposium on Security and Privacy

“A Scalable System for Pushing All TLS Revocations to All Browsers”

Scheme for achieving extremely high compression of CRLs, making it practical to maintain a complete set of revocation information on the client

Alternative revocation checking mechanism being implemented in Firefox that:

- eliminates (mostly) the need for costly OCSP queries
- is highly reliable
- doesn’t suffer from false positives

How does it work?

1. We rely on existing CT logs to gather all serverAuth certificates from enrolled CAs

1. We download the CRLs pertaining to these certificates

1. We generate a series (cascade) of bloom filters based on this data and ship it to the browser

Initially, all of this happens on a daily basis

- ○ Firefox may rely on existing revocation checking mechanisms (OCSP) for newly issued certs

More detail can be found in the original research paper: https://mislove.org/publications/CRLite-Oakland.pdf

How will Firefox change?

- By default, Firefox will check for revocation using CRLite for all opted-in certs
- Firefox will also continue to use OneCRL for revocation checking
  - OneCRL is primarily used for revoking intermediate CA certificates
- OCSP checking will typically not occur - even for EV certificates - if the certificate is opted-in to CRLite
  - OCSP (including stapling) and CRL checking will still be available as a fallback mechanism when CRLite is unavailable (opt-out, newly issued certificate, failure retrieving CRL)
- A revoked certificate will block the page from loading
  - Error can be overridden unless HSTS enabled
- If CRLite data on client has not been updated for a while, then Firefox will fall back to OCSP

Information for CAs

- We need to know about every certificate you issue for this to work properly!
  - This currently only applies to certificates that are trusted for TLS in Mozilla products
- We're scanning CT logs for this purpose
  - Haven't yet decided which logs we'll scan
    - But we recognize the need for consistency with requirements of other root programs
- CAs can opt-out for all certs issued by a given intermediate CA certificate
  - By default, we plan to opt-in every intermediate
  - By default, we'll opt-in all end-entity certs issued after May 1, 2018
  - We know that a few CAs still aren't CT logging - you'll need to opt-out
  - We know that some CAs started logging all certs prior to May 1st - you can tell us when
- What if a CA's customers can choose not to log particular certificates?
  - We are still deciding how we'll handle this situation. Options are
  - (1) require CT; unlogged certificates trigger an error before revocation checking occurs
  - (2) accept false positives in this scenario
  - (3) fall back to OCSP if no SCTs are received in handshake

Next Steps

- We plan to test this in the Fall
  - We'll run it in report-only mode to ensure that it works as expected
  - We may ask for CAs to volunteer for the testing

- We will send an official communication with final information, including instructions for opting out of CRLite

Questions?

moz://a

Thank You