Last-Minute Addendum:
Breaking News on Namecoin TLS Development

Jeremy Rand
Lead Application Engineer, The Namecoin Project
https://www.namecoin.org/

OpenPGP: 5174 0B7C 732D 572A 3140 4010 6605 55E1 F8F7 BF85

Presented at Grayhat 2020 Monero Village

Building Certificate Chains is Hard

- In theory, a TLS server is supposed to send a chain of certificates that starts with the server's own certificate, and ends with a root CA that the client trusts.
- TLS client software is quite diverse.
- Different clients might have different sets of trusted root CA's.
- CA's cross-sign each other regularly, adding to the entropy.
- The server operator has no reliable way to be certain that the client will build the expected certificate chain.

An escape hatch!

- If the TLS client has trouble chaining the certificates back to a trusted root CA, there's a fallback mechanism to help the client get whatever intermediate certs they might be missing.
- A certificate can include some extra data:
  - "Oh, you're looking for the certificate of the CA who signed me? No worries, here's a URL where you can download it!"
- This is called the Authority Information Access (AIA) extension.

How common is AIA support?

- Microsoft CryptoAPI (Windows) supports AIA for all applications.
- Chromium and Safari support AIA on all desktop and mobile OS's.
- Firefox doesn't support AIA.
  - It uses other heuristics to find missing intermediate certs, e.g. caching intermediates between different handshakes (which CryptoAPI and some other clients also do).
- Most smaller clients don't support AIA.

Deja vu?

- Recall:
  - We made ncp11 feed intermediate name-constrained CA's to NSS…
  - Signed by the Namecoin root CA that NSS already knows about…
  - So that NSS will determine the certificate chain to be valid.
- This is what AIA does!

Introducing Encaya!

- Encaya is an alternate frontend for ncp11's intermediate CA lookup engine.
- Instead of exposing the intermediate CA's as PKCS#11 objects…
- It exposes them as AIA-compatible URL's.
- So now the positive override functionality of ncp11 can work with anything that supports AIA.

In other words…

- Censorship-resistant (and layer-2-scalable, attack-surface-minimized) Namecoin TLS for:
  - Most Windows applications.
  - Chromium on all desktop and mobile OS’s.
  - Safari on all desktop and mobile OS’s.

No local code execution needed

- Just change your DNS settings…
  - Easy to do, supported by basically all platforms since enterprises need to do it routinely.
- Import the Encaya root CA…
  - Ditto.
- And your machine can use Namecoin TLS.
- Even if your Namecoin-DNS bridge and Encaya server are running on a completely different machine.

Tivoization is no longer a problem

- We had always said that Tivoized platforms like iOS would never get Namecoin support, because we can’t run our own code on them.
- But now we don’t need to.
- So supporting Namecoin (with TLS) on iOS is now feasible.
  - (If you’re okay with running Namecoin on another machine.)

You don’t even need a secure network path

- If DNS gets hijacked, you’ll wind up navigating to an IP that can’t produce a valid TLS certificate.
  - Because the impostor server doesn’t control a certificate that Encaya will chain to the Encaya root CA.
  - So you’ll get a TLS error, but no security issue.
- If the AIA traffic gets hijacked, you’ll also just get a TLS error.
  - Because the AIA certificates are authenticated by the Encaya root CA that you imported.
  - Still no security issue.

Demo of Encaya in Chrome on Windows

Code status

- Very much in “proof of concept” stage.
- Hot off the press.
  - This literally worked for the first time on Oct 29 (day before yesterday).
- It will take nontrivial work+time to get this ready to deploy to users.

Caveat

- Negative overrides are explicitly out of scope for Encaya.
  - But I think this is okay.
  - You can combine Encaya with a separate negative override method if one exists for your platform.
- Ubiquitous positive overrides are a bigger barrier to Namecoin adoption than ubiquitous negative overrides.
  - Users who need MITM-resistance can choose their platform accordingly, but website owners want assurance that anyone can view their website.

Etymology?

- “Encaya”: phonetic spelling of “ncaia” (Namecoin Authority Information Access) when pronounced as an acronym.
- Also happens to be a portmanteau of “Encrypt” and “Xaya”.
  - Xaya is the flagship product of Autonomous Worlds, Ltd., which employs some Namecoin developers.
- (Yes, I put too much time into that name.)

Contact Me At...

- https://www.namecoin.org/
- OpenPGP:
  5174 0B7C 732D 572A 3140
  4010 6605 55E1 F8F7 BF85
- jeremy@namecoin.org
- Questions? Ask me on #namecoin on Freenode IRC.
- Thanks to the Monero Village for inviting me here!