NDNCERT-v2: Deploy, Debug, Dominate

Ashlesh Gawande

Alex Afanasyev

Summary

- Deploy
  - /ndn/edu/memphis/agawande/CA
  - Lack of documentation to setup with repo
- Debug
  - Crashed the server multiple times
  - Discovered multiple problems in client and server
  - Found out unimplemented critical things in the server
- Dominate
  - Skeleton of PyNDNCert client
  - Still on the way (far away) to domination

Crashes

- Ndncert-client
  - Type enter on step 0 -> Crashes: stoi
  - Crash when entering any other string by exact challenge name
    - What would you expect to enter to the question
      - `Step 3: Please type in the challenge ID from the following challenges`
    - `          Email`
- NDNCert Server
  - Crash when receiving interest with incorrect sha256-params
    - Discovered by GSoC student earlier: https://redmine.named-data.net/issues/4982
  - Crash on invalid input
    - wrong request, incorrect encryption, missing blocks in parameters TLV, anything non-conformant

Critical Unimplemented Things

- Hkdf derived key not used
    - In both client and server code, m_aesKey being initialized and derived using hkdf function, but not actually used anywhere.

- PROBE not implemented
    - Probe function is neither fully documented (as a spec) nor implemented anywhere in the server code. The code only include functionality to set a “handler”, but no uses of that (except the test cases).
    - Effectively, it is now hard-coded to return randomly generated number as identity.

Other (unexpected) things

- Local-ndncert-anchor not used
  - m_localNdncertAnchor (local-ndncert-anchor)
- Client tool asks for email twice (?!?)
- Why json for NEW/and other exchanges requires “\n” at the end ?!?
  - Not having it crashes the server
- Minor: JSON_CA_EQUEST_ID -> typo

Roadblocks to Domination

- Problems related to encryption/decryption
- Stuck with decrypting JSON:
  - IV, payoload, algorithm seem to be the same outputted in Python and received in C++, but C++ crashes with a mystery error from security::transform::blockCipher
- https://github.com/9th-ndn-hackathon/pyndncert