Estonia: A First Peek

Joe Kiniry
DTU, ITU, DemTech

DemTech Auditing

- DemTech is archiving and analyzing publicly released election software for correctness, security, and software engineering practices
  - examined Norway (v2), Scantegrity II, KOA
  - recently looking at Helios
  - in the queue: Pret-a-Voter, Solon, LiquidFeedback, ACT, Victoria
  - we are happy to look at your design, architectures, and implementations!
  - during VoteID Joe looked at Estonia's system

Estonia's Software

- (some) server software published as a code drop from Sven Heiberg on 11 July to https://github.com/vvk-ehk/evalimine
- code release was mandated by government, not technologists responsible
- unclear what role activism in Estonia had
- DemTech fork for analysis in out GitHub Organization found at https://github.com/demtech/evalimine

Big Picture

- nearly typical code drop: no docs, no harness, no tests, no protocol description
- evidence of very poor software engineering practices (looks like a one man hack job)
- code is medium sized

  python: 9892 (59.46%)
  cpp: 6487 (38.99%)
  sh: 257 (1.54%)

Documentation

- documentation coverage is embarrassing
  2.3% coverage for Python code
  1.2% coverage for C++
- The majority of comments are in reused library code, not in Estonia's code (proper).
- No non-source documentation (architecture, requirements, test plan, etc.)

Engineering Practices

- 2 assertions in C++ code
- 1 assertion in Python code (for a default case in CLO processing)
- 1 function comment (in the whole system!)
- on the other hand, the build system does use Python lint and the Python syntactic static checker
- evidence that that there perhaps is validation code, but it is not included (and as such, causes the build system to fail)

Dependencies

- Tons of implicit dependencies in Python code that are nearly undocumented. They are mentioned offhandedly in debian/changelog.
  - bdocpython (http://wpki.eu/wiki/upload/8/82/BDoc-1.0.pdf)
  - Mobiil-ID (http://mobiil.id.ee/)
  - Uus HSM (hardware security module?)
  - kontrollitavus (BSc thesis?)

Server Configuration

- Example Apache server config looks fine.
- SSL configuration looks ok.
- SSL is only used for HES.
- Certificates are included in the code drop.

Code Borrowing

- Large amount of included code is lifted from libraries and is used for handling server-side crypto (particularly certificate management).

- "Borrowed" code has no attribution of source, authorship, or license.
  - base64 from John Walker and in the public domain.
  - countLines taken from GNU's wc (!).

Main Issues Found

- vote auditing does not exist
- vote validity is a stub and only logged
- malformed votes will be logged and stored and detected during decryption

Vote Analysis

```
def analyze(ik, vote, votebox):

    #   TODO: implement security checks
    #   such as verifying the correct size
    #   of the encrypted vote

    return []
```