


Swiss Cybervoting PIT(falls)



Author

- CTF Player
- Independent Security Researcher
- Reverse Engineer & Exploit Dev
- Software Engineer

Views are my own and not related to my employer

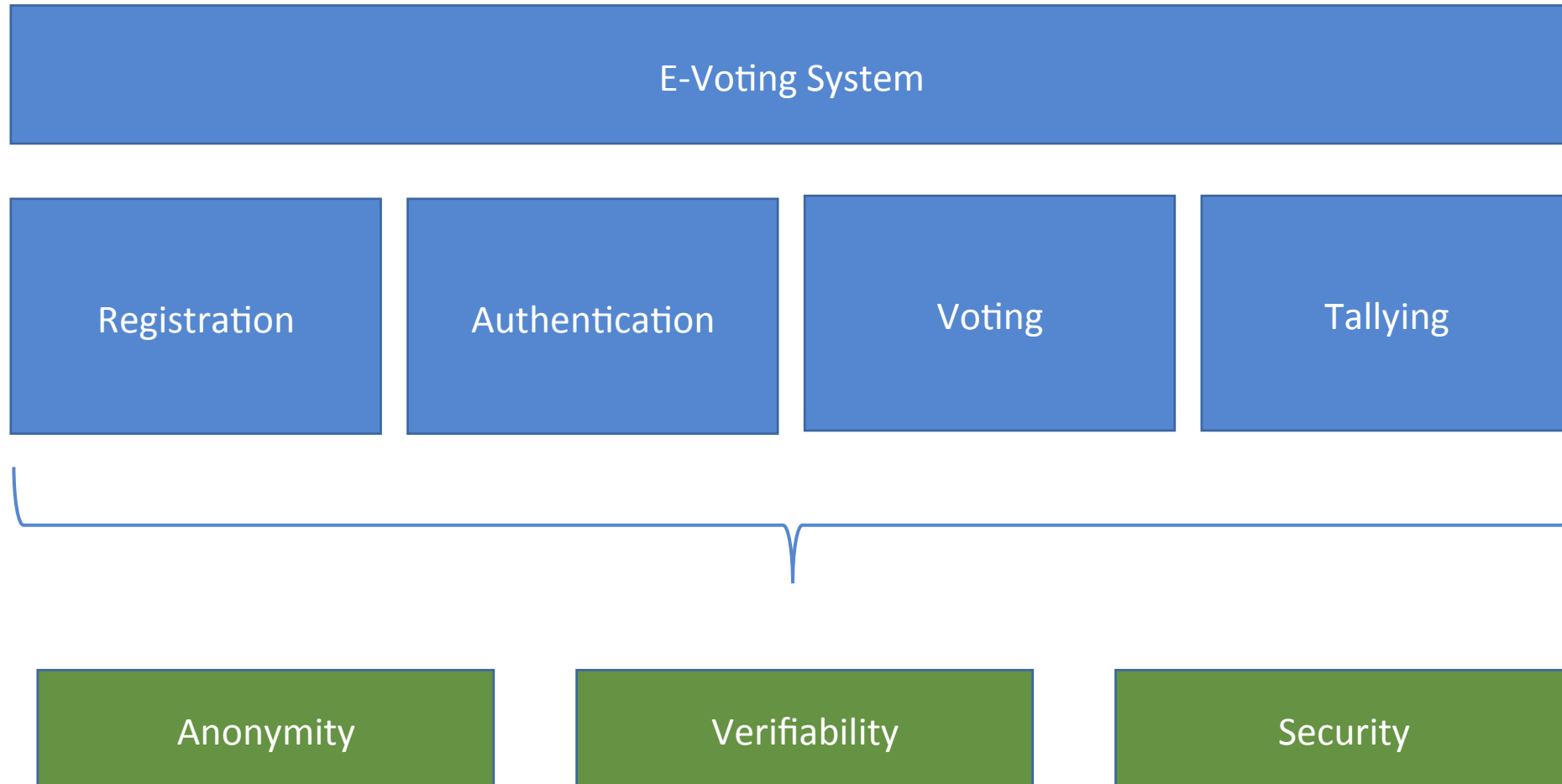
 @ xorkiwi

 /in/janniskirschner

Jannis Kirschner



Components of an e-voting system



Where's e-voting present?



European Union Parliament
Europe



Canton of Neuchâtel
Switzerland



Swiss Canton of Fribourg
Switzerland



Canton of Basel-Stadt
Switzerland



US Elections
USA



McDonalds Franchises
Spain



Department of Defense
USA



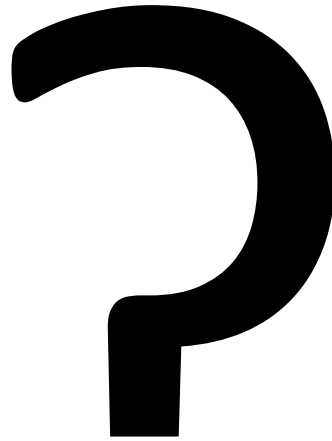
City of Barcelona
Spain

Why cybervoting

- + Comfortable to use
- + Accessible
- + Might attract young voters
- + Citizens living abroad
- + Less invalid votes

- Security risks on scale
- Very expensive to maintain
- System must be trusted by users
- Hard to verify

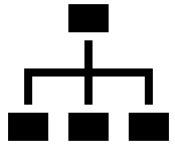
„Open Code“



General details



250'000 LOC



5 Components



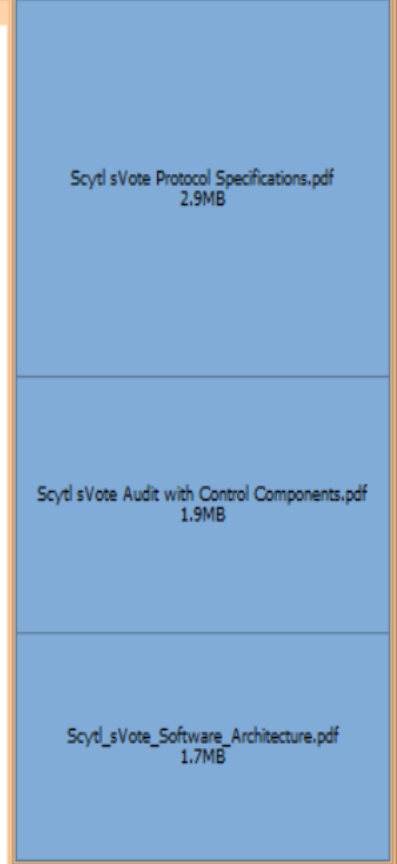
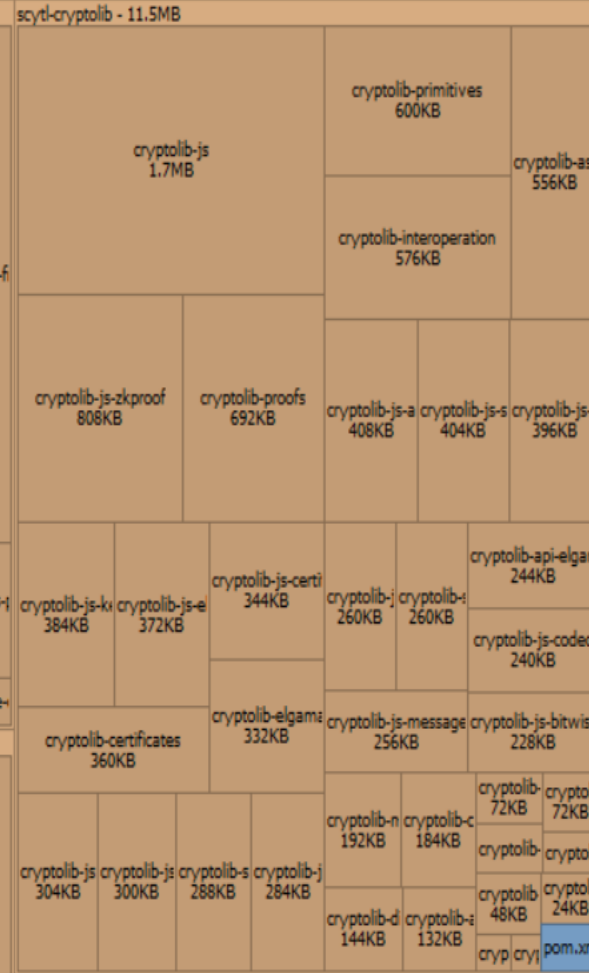
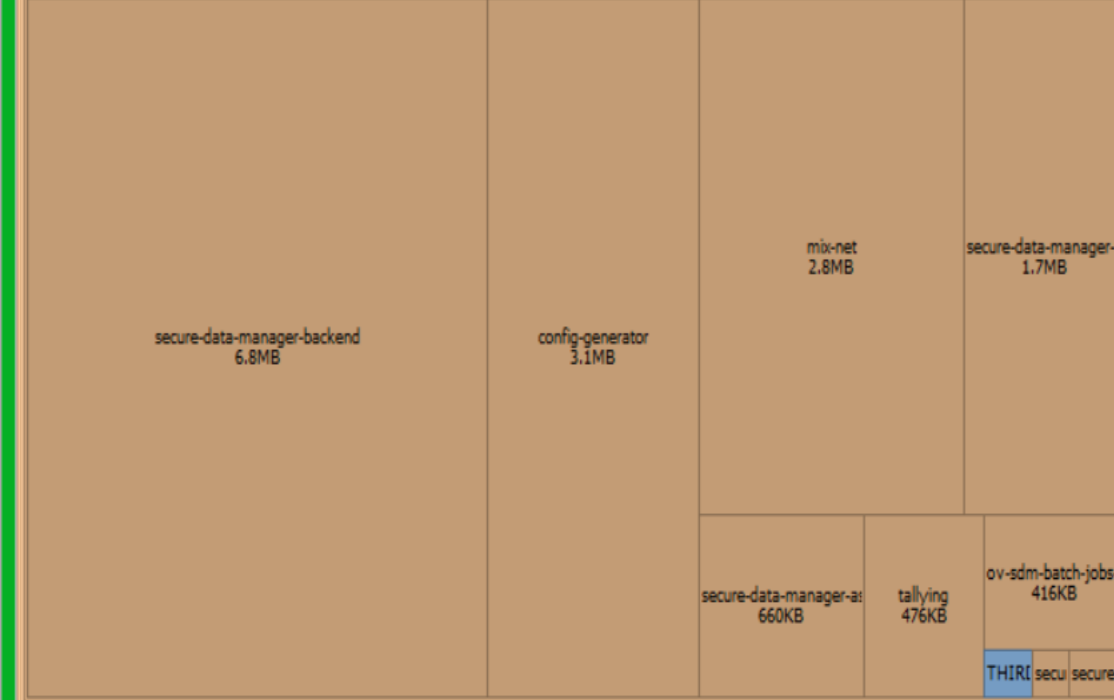
300 External Dependencies



55MB

source-code - 60.0MB

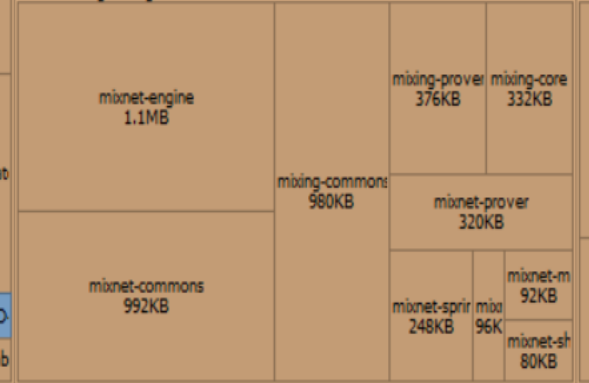
online-voting-secure-data-manager - 16.2MB



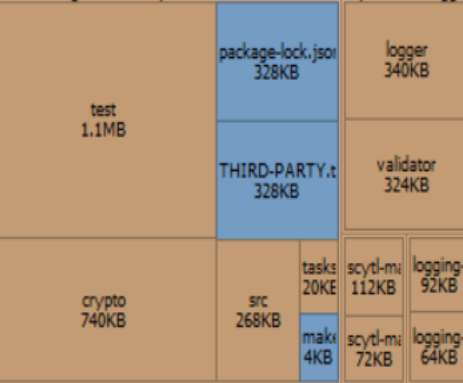
online-voting-channel - 14.5MB



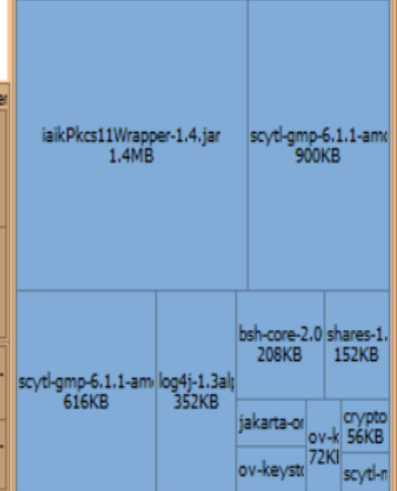
online-voting-mixing - 4.6MB



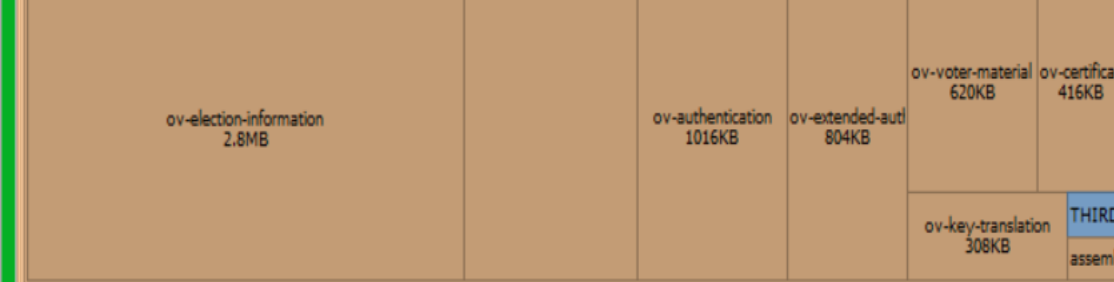
online-voting-client-library - 2.9MB



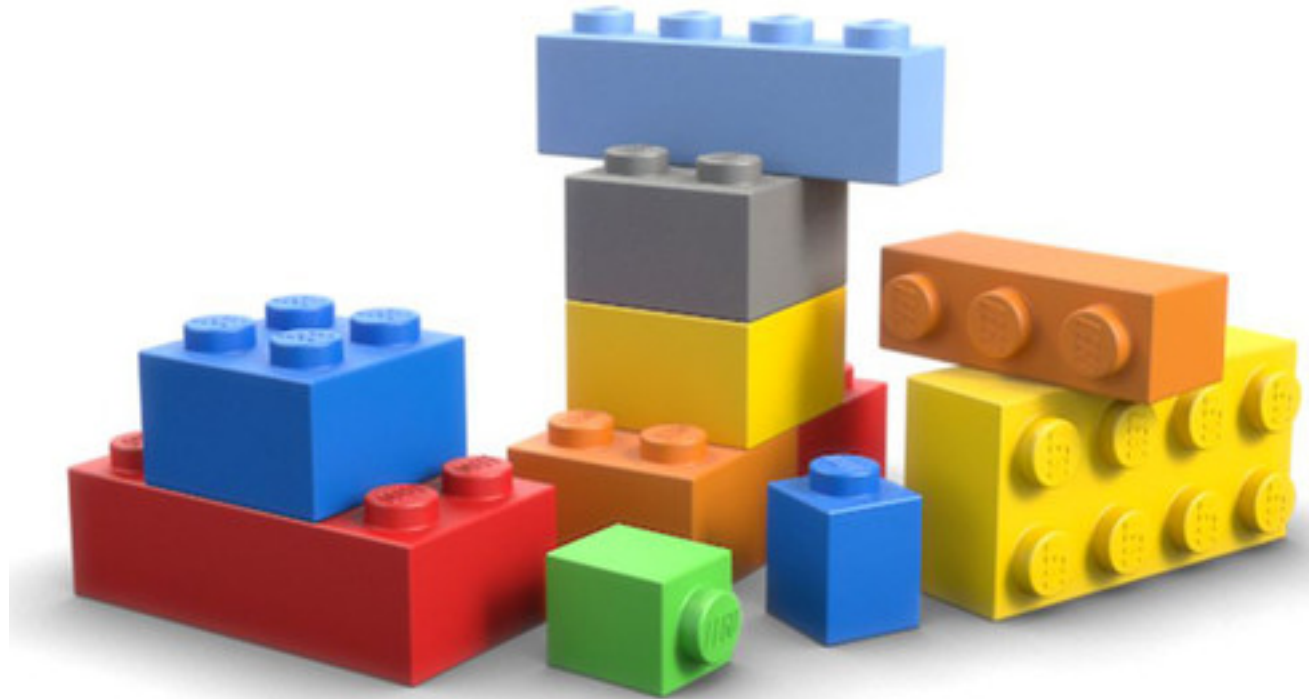
dependencies - 3.9MB



ov-election-information - 2.8MB



To build or not to build



Documentation



Incomplete (Security) Audits



PIT Scope

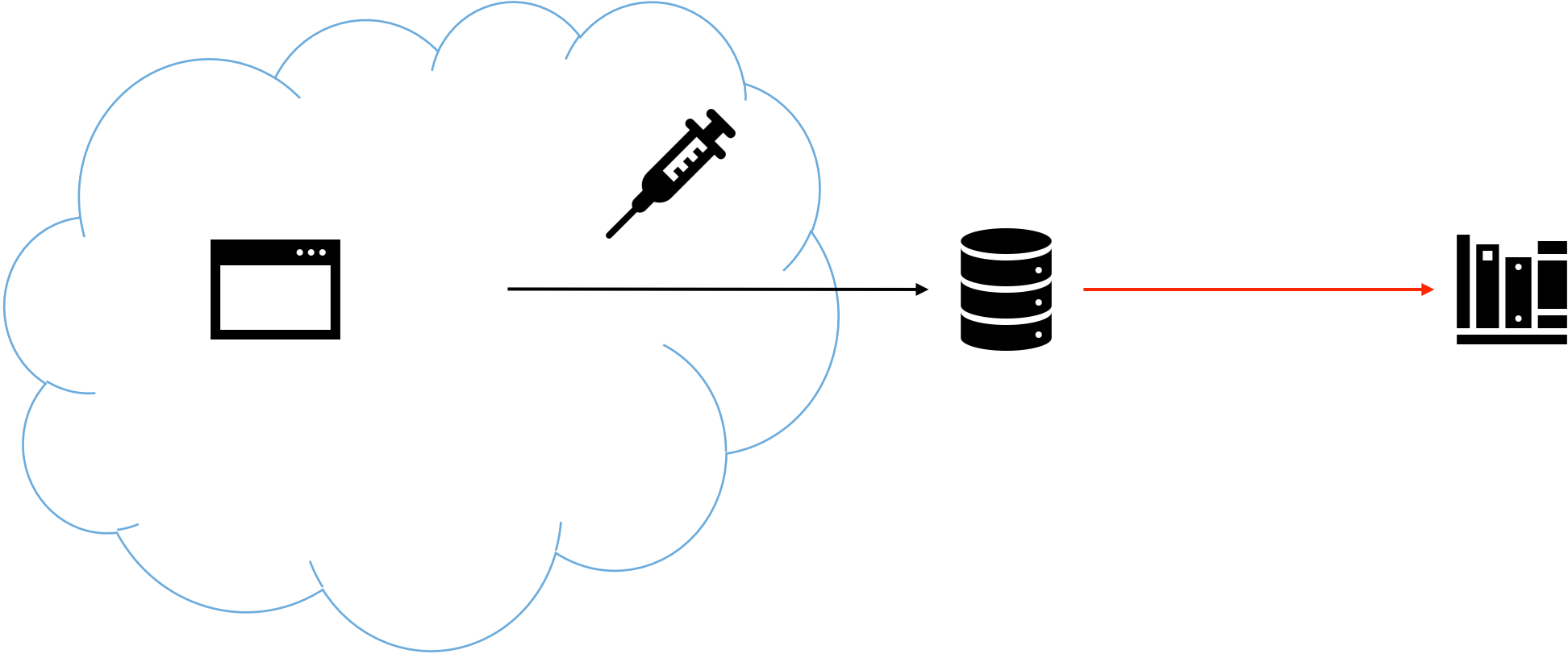


SDM Command Injection



```
Java.lang.getRuntime.exec()
```

Crafted X-Forwarded-For HTTP Header Injection



Discussion points

- „Should critical code be made public or stay private?“
- „Is an unexploitable vulnerability still a vulnerability?“
- „How secure is secure enough for critical systems?“