TrustFull: Trustworthy Fullstack Computing

Mads Dam

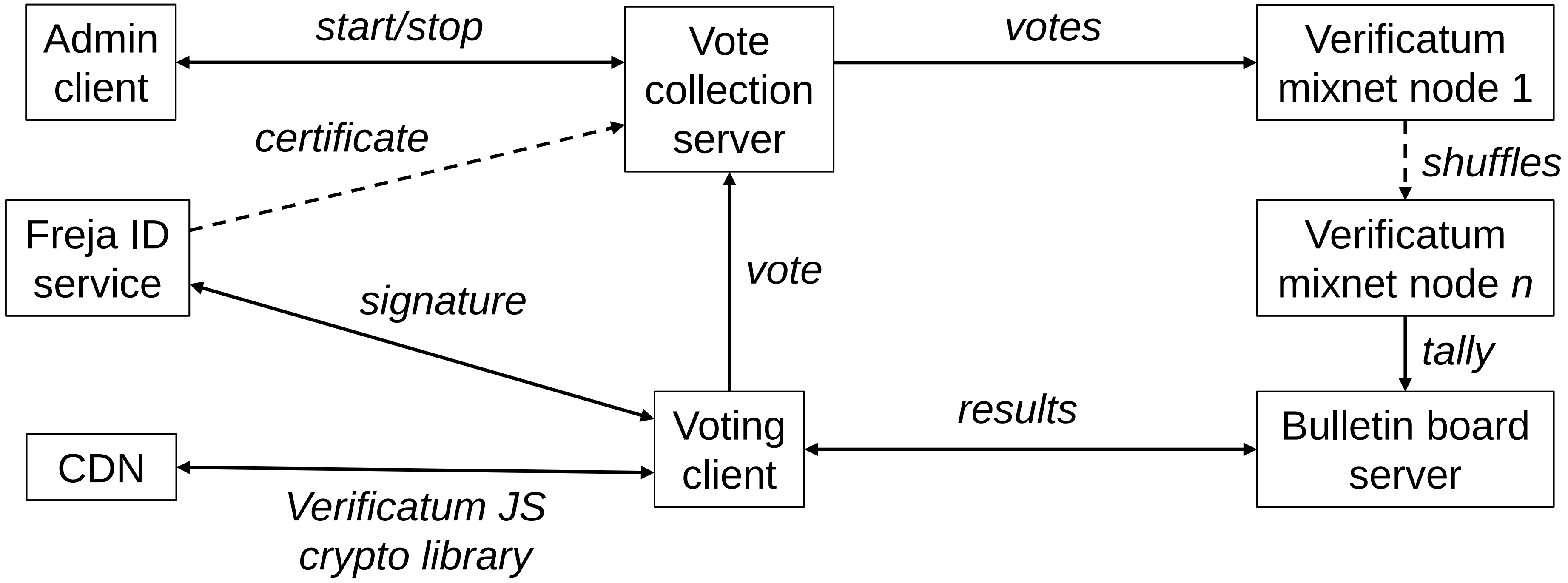
Benoit Baudry, Roberto Guanciale, Martin Monperrus, Musard Balliu, Douglas Wikström,
Karl Palmskog
Postdocs, PhD students, MSc students
KTH/EECS/TCS

SSF-Vinnova samverkanskonferens för cybersäkerhet 2023

Purpose and Goal

Methods to build systems with strong security across the entire HW-SW stack

Example: The TrustFull e-voting demonstrator



Other Recent Highlights

- Multi-variant Execution at the Edge
- Cabrera-Arteaga, Laperdrix, Monperrus, Baudry
- Automatic sandboxing and diversification of WASM binaries
- 9th ACM Workshop on Moving Target Defense

- Neural Transfer Learning for Repairing Security Vulnerabilities in C Code
- Chen, Kommrusch, Monperrus
- Automatic repair of of C vulnerabities using deep learning
- IEEE Transactions on Software Engineering

- HOL4P4: semantics for a verified data plane
- Alsshnakat, Lundberg, Guanciale, Dam, Palmskog
- Formal semantics of P4 data plane language in the HOL4 theorem prover
- EuroP4’22

- SoK: Confidential Quartet - Comparison of Platforms for Virtualization-Based Confidential Computing
- Guanciale, Paladi, Vahidi
- Comparing confidential computing HW platforms
- SEED’22

- Special Soundness in the Random Oracle Model
- Wikström
- Non-interactive proofs of knowledge with applications to mixnets and e-voting
- Submitted

- Silent Spring: Prototype Pollution Leads to Remote Code Execution in Node.js
- Shcherbakov, Balliu
- Injecting properties into object root prototypes to trigger remote code execution, privilege escalation, etc.
- Usenix 2023

- Validation of Side-Channel Models via Observation Refinement
- Buiras, Nemati, Lindner, Guanciale
- Guided relational testing to refine models of side channels.
- Micro 2021

- Formally verified isolation of DMA
- Haglund, Guanciale
- Modelling and security analysis of direct memory access controllers
- FMCAD’22

Thank you!