SSITH/SHIELD Voting System Demonstrator

DARPA Briefing

Joe Kiniry & Dan Zimmerman, Galois

August 2018

Our Experiences with Demonstrations for DARPA

- DARPA demonstrators that are compelling vs. uninspired
  - Attractive, redeployable demonstration with physical artifacts
  - Use cases for underlying technology that obviously relate to DoD application
- HACMS experience (live drone hacking) pros and cons
  - Public demonstration that viewers immediately understand; Coolness factor of demonstration
  - Authenticity of live hack
- New wrinkle for SSITH/SHIELD: Public Red Team
  - Technology in the hands of the public vs. with a red team under NDA
- A core concern for DARPA is public embarrassment
  - How to align confidence of performers and evidence of security with DARPA goals
- Pros and Cons of Voting as a DARPA demonstrator
  - DoD application of secure SoCs and silicon (indirect); DoD support for military voters (direct)
  - Legislative inaction on responding to election meddling by our adversaries

Verifiable Paper as a Compelling Use Case

- Paper-based artifacts are manifest in DoD processes and procedures
- Paper artifacts are often the basis for critical decision-making
- Provenance of paper artifacts is difficult to manage

- Paper-based artifacts are the foundation for trust in elections
  - Ballots, receipts, logs, manifests, manuals, rules, statutes, etc.
- Insider attack on traditional elections in the USA and abroad focuses on the manipulation and control of paper artifacts
- Physical security and the four eyes principle are the only remediations today
- Verifiable paper is a killer application for a physical root of trust in elections
- *Verifiable paper plus an end-to-end verifiable voting scheme is ideal*

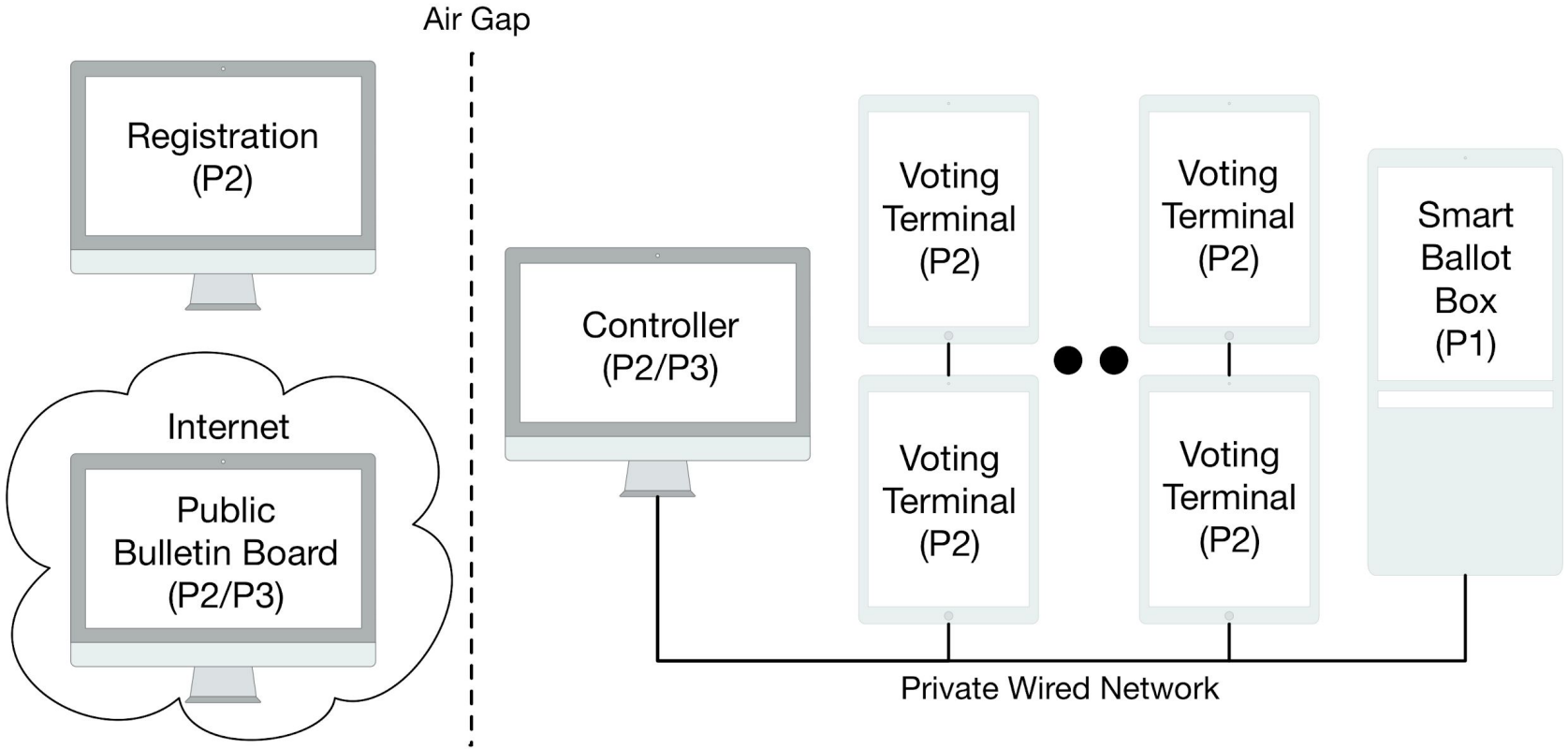
End-to-End Verifiable Technologies

- An *End-to-End Verifiable* (E2E-V) system is a computing system that...
  - ...is based upon cryptographic protocols
  - ...that provide evidence about the system's operation and security
  - ...that is cryptographic/mathematical and consequently checkable by 3rd parties
  - ...and is independent of the implementation's nature, platform, or assurance
  - ...and is fit-for-purpose for the requirements of the system
- An *End-to-End Verifiable Voting System* is a digital voting system that…
  - ...is based upon cryptographic protocols involving the principals and principles of elections
  - ...that provide evidence that each voter's vote is captured correctly and is included in the final tabulation, and that no vote is lost, missing, added, or altered,
  - ...that is checkable with small, simple proof checkers written by arbitrary parties
  - ...and ensures that voters cannot reveal how they voted, voters cannot be coerced or sell their vote, and election officials cannot collude to violate system security
- *The right E2E-V voting system to deploy on SHIELD/SSITH is STAR-Vote*

STAR-Vote Pedigree

- History
  - The County Clerk of Travis County, TX became interested in elections integrity in 2006
  - In 2011 she decided to challenge the community to design a next generation voting system
  - In 2012 STAR-Vote (**S**ecure, **T**ransparent, **A**uditable, and **R**eliable Voting System) was designed with academic experts in cryptography, audits, system security
  - The STAR-Vote design was published at USENIX 2013 and subsequently as a journal paper
- Technical Inventors
  - Josh Benaloh, Microsoft Research and Olivier Pereira, Catholic University of Louvain (cryptography)
  - Dan Wallach, Michael Byrne, and Philip Kortum, Rice University (cryptography, system security, and usability and accessibility of voting systems)
  - Neal McBurnett, ElectionAudits and Philip Stark, Berkeley (risk-limiting audits)
- Implementations
  - Rice University student implementation in Java
  - Galois demonstration commercial implementation in Haskell
  - Microsoft-funded high-assurance E2E-V SDK

System Overview



Microsoft Project

- E2E-V SDK
  - The largest project of the Defending Democracy Program under President Brad Smith
  - Evolve our existing open source SDK for E2E-V to match Microsoft requirements
    - Technical lead at Microsoft is Josh Benaloh
  - Provide formal specification and assurance case for entire protocol and its implementation
  - Current implementation is in C and Java; specification will be in Cryptol, ACSL, and Coq
  - Build a demonstrator COTS system using Microsoft Surface, Windows, and Linux
- Risk-Limiting Audits for America
  - Evolve the Risk-Limiting Audit system we built for the State of Colorado to work for the USA
    - ColoradoRLA becomes RLA4All
  - Make the RLA4All system available for free to all jurisdictions and states in the country
  - Does not involve SSITH/SHIELD technology at the moment

Layered Security for SSITH/SHIELD Demonstrator

- E2E-V system
  - Protocol and implementation assurance case
  - Implementations directly synthesized from Cryptol and Coq specifications
- SSITH Secure RISC-Vs
  - 8 different teams producing 3 secure CPUs that match STAR-Vote's architecture
- Formally Assured Secure Boot
  - A hardware root of trust that grounds red team boundary tightly (no FPGA hacking permitted)
- SSITH Secure Compilation of OSs and system software
  - Ensure kernel, core OS, and voting system software is compiled with performers' compilers
- SHIELD Dielets and Reader
  - Hardware root of trust in paper artifacts, SRI reader integrated directly into demonstrator
- SHIELD in paper (Verifiable Paper) and Voting System Equipment
  - Provides physical and cryptographic evidence about paper and physical artifact provenance

SRI Component: SHIELD in Paper Prototype

- SOW
  - Work with Galois on development of Verifiable Paper IP
  - Initial stock of 50 units of verifiable paper, with a per-batch cost thereafter
  - Modification of reader front-end to work with Verifiable Paper
  - SHIELD technical support to Galois for development of Voting System demonstrator
  - Per unit cost for readers for integration into Voting System demonstrators (2 per system)
  - Demonstration support at DEF CON, university road show, etc.
  - Periodic travel to Galois to support system engineering
- Technology
  - Galois works with multiple SRI teams on the development of secure systems and tools for the DoD, thus we have a long and healthy working relationship
- Expertise
  - SSITH PI Peter Neumann has worked with Joe Kiniry for years on elections
  - SRI led a top-to-bottom review of commercial voting systems for California in 2007
  - SRI leadership including CTO Greg Kovacs, Lab Director Pat Lincoln, and PI Peter Neumann are extremely enthusiastic about this application of DARPA technology

Threats and Mitigations

- Internal Red Team
  - We will bring in a hardware security red team that has deep experience with secure hardware and election systems for an intense private red team exercise
- Layered Security Architecture
  - We have unmatched layered security: a formally assured E2E-V protocol, the formally verified implementation of the E2E-V protocol, the SSITH secure CPUs, and the secure compilation of the entire firmware, OS, drivers, libraries, and minimal application stack
- Threat Model
  - The demonstrator threat model is exactly the SSITH threat model, extended to the SHIELD domain: red team access to equipment is UART and Ethernet and API for loading arbitrary userland binaries on device (SSITH) & arbitrary SHIELD reader interactions via RF
- Contest Goals
  - We will frame the red team goals as a cybersecurity contest
  - A checklist of winning conditions is coupled directly to formally/rigorously assured security properties about the system—participants win if they defeat the security properties of the voting system that run through all six layers previously discussed

Public Red Team Exercises

- DEF CON Voting Village 2019 and 2020
  - 2019: Smart ballot box with SSITH P1 processor and SHIELD verifiable paper; other components E2E-V but with no DARPA technology
  - 2020: Complete system with SSITH P1/P2/P3 processors and SHIELD verifiable paper (possibly 2nd-generation writable)
- University Road Show
  - After DEF CON 2019, one or both of...
    - Autumn 2019/Spring 2020 with partial system
    - Autumn 2020 with complete system
- CrowdSupply Voting System
  - Small, affordable FPGA capable of running a portion of the voting system (smart ballot box software and a lightweight version of voting terminal software, without SHIELD tech), for broader public engagement

SSTAR-Vote

- This system will be a spectacular demonstrator for SSITH and SHIELD
- It pushes all of the buttons for what constitutes a compelling demonstrator
- It is tightly framed for a red team exercise and made-for-TV hacking event
- The system's layered security has unprecedented depth and assurance
- The potential positive impact of a DARPA-based voting system for the DoD is immeasurable and icing on the cake

- The combination of STAR-Vote, Microsoft's funding, and DARPA funding for this system turns STAR-Vote into *SSTAR-Vote: The SSITH/SHIELD Transparent, Auditable, Reliable Voting System*