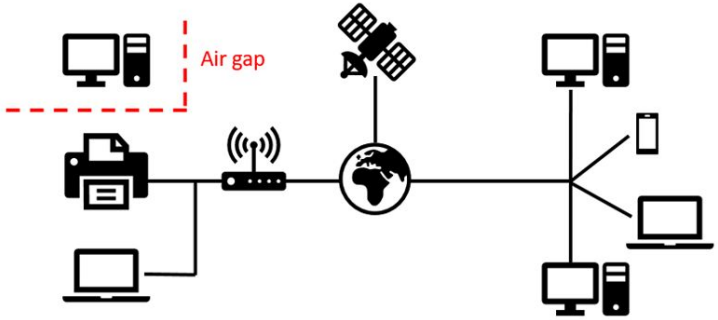
Security Flaws in Online Voting

By Alex Chen and Michael Yu

Background



- Pennsylvania's Venango County voting system report by CMU
  - Used digital touch-screen voting machines
  - Voters reported votes being switched
  - CMU discovered remote-access software preinstalled, going against the practice of air-gapping election systems
  - Voting machines from Election Systems & Software (ES&S) were found to be preinstalled with remote-access software in several other locations

Why is this worrying?

- Remote-access software exposes voting machines to manipulation
- Digital systems often leave no paper trail that can expose discrepancies between actual votes and those reported by the machines
- Remote-access software was sometimes installed by officials on the advice of ES&S
    - Exposes vulnerabilities that could be exploited by social engineering attacks

Online voting

- The internet is even more exposed than the machines mentioned earlier
- Case Study: Voatz voting app
  - Governance and Compliance
  - Internal Processes
  - Voting Processes
  - External Storage
  - Infrastructure and Administration
  - Mobile Application

Relevant parts of the threat model

- Voting Processes
  - Manual identity verification and long term storage of voter information
- External Storage
  - Use of third party systems to store data (AWS)
- Mobile Application
  - Lack of trusted root

How exactly does Voatz work?

Mobile Application:

- Uses Zimperium Mobile Threat Defense services to detect things like rooted/jailbroken devices
- MDT checks for applications that have not been digitally signed by Apple or Google
- MDT flags suspicious connections (ex: man-in-the-middle attacks)

Voatz network security

- Asymmetric encryption for network data
  - Exchange public keys
- Perfect Forward Secrecy (PFS)
  - Frequently change keys used to encrypt/decrypt
- Application Key Sequencing
  - Ensure that only one device is used by a user
- Input sanitization and validation
  - Prevent attacks such as buffer overflow attacks

Voatz network security cont.

Network Security	
Man-in-the-Middle Attacks	HTTPS (AES\GCM) Application Key Sequencing, Certificate Pinning, Certificate Transparency
Data leakage	Perfect Forward Secrecy (PFS)
Multiple registrations by the same voter on different phones	Application Key Sequencing
Data injection, memory attacks	Sanitization and Validation
Distributed Denial of Service (DDoS)	Cloudflare services
DNS flood attacks	DNS Redundancy DNSSEC
HTTP flood attack	Multiple points of presence (PoPs), geo-Blocking, Web Application Firewall
UDP amplification or SYN flood attacks	Elastic load balancing

Voatz storage security

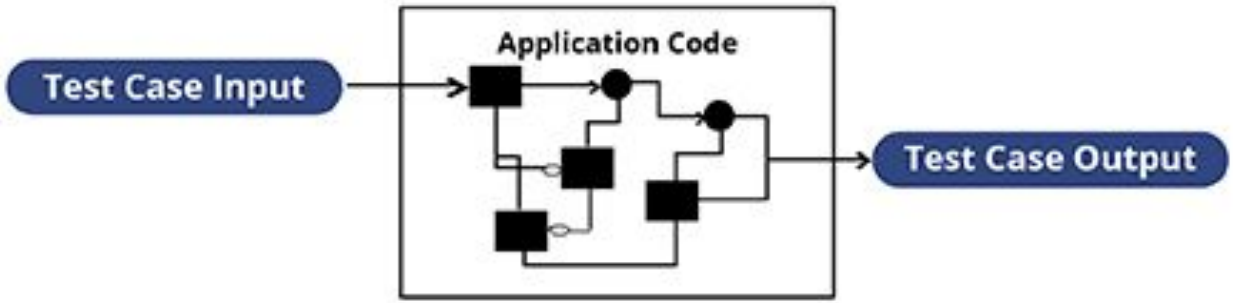
- Permissioned blockchain: Hyperledger Fabric
  - Distributed ledger technology
  - All participants must be authenticated
  - Ledgers
    - stored immutable historical records
  - Clients, endorser, orderer, validator
    - Endorser mentions identity when endorsing transactions

Factors of a promising solution

- General:
  - Defining the issue
  - Time and effort
    - More than just a few years needed
    - Engineers well-versed in system security
- Align with federal standards
  - “Voluntary Voting System Guidelines Version 2.0”
- Both black and white box testing
  - Consult independent experts instead of vendors
  - Disregard non-commissioned reports

Black box Testing

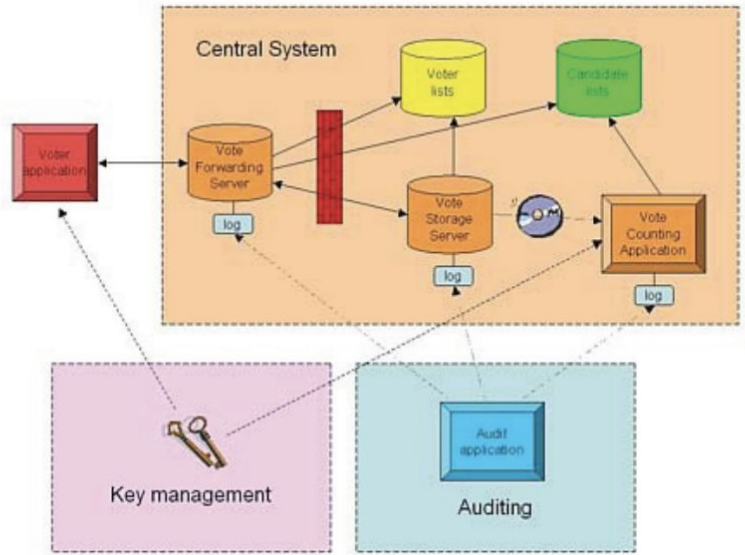
WHITE BOX TESTING APPROACH



Is security the only technical challenge?

- Secrecy and verifiability
  - Risk-limiting audits
  - Just as essential as security

Architecture of online voting



What does this all mean?

- Much room for improvement in creating online voting applications
  - Skilled engineers given a few years were not able to create a secure online voting system
  - Solutions in other countries are also under-developed
- Technological advancements have societal requirements to meet

Works Cited

- https://www.govtech.com/biz/Detailed-Audit-of-Voatz-Voting-App-Confirms-Security-Flaws.html
- https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines
- https://www.researchgate.net/publication/276198111_Black_Box_and_White_Box_Testing_Techniques_-_A_Literature_Review
- http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.857.8662&rep=rep1&type=pdf
- https://pdfs.semanticscholar.org/4bbf/ed889f9b25f93304fbdd8b035975d4a5881a.pdf
- https://medium.com/blockchannel/mind-the-crypto-air-gap-89dd8650cba7
- https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html
- https://iotbytes.wordpress.com/dial-up-modems-and-iot/
- https://asmed.com/comptia-network-osi-model/
- https://voatz.com/voatz-security-whitepaper.pdf
- https://opensource.com/article/19/9/introduction-hyperledger-fabric
- https://www.researchgate.net/publication/334405589_Vulnerabilities_on_Hyperledger_Fabric
- https://github.com/trailofbits/publications/blob/master/reviews/voatz-threatmodel.pdf