E-Voting

Physical Security, Human Factors

Paolo Falcarin

Ca' Foscari University of Venice

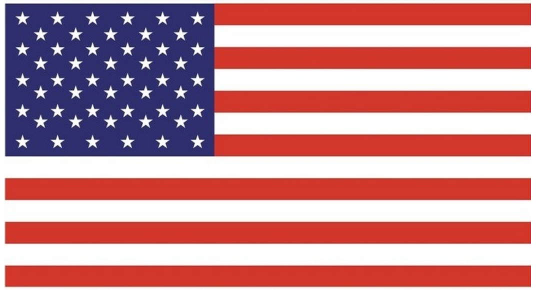
Department of Enviromental Sciences, Informatics and Statistics

paolo.falcarin@unive.it

CM0626 – Software Security

18 March 2025

In the world's oldest continuous democracy



- Humboldt County, CA: voting machines dropped 197 votes
  - Wired, 12-8-2008
- Florida's 13th Congressional District (2006): One in seven votes recorded on voting systems was blank
  - US Government Accountability Office, 2-8-2008
- Franklin County, Ohio: computer error gave Bush 3,893 extra votes in one precinct
  - – WaPo, 11-6-2004
- In a North Carolina County: 4,500 votes were lost –WaPo, 11-6- 2004

Software Independence

- Rivest and Wack: “A voting system is software independent* if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome.”

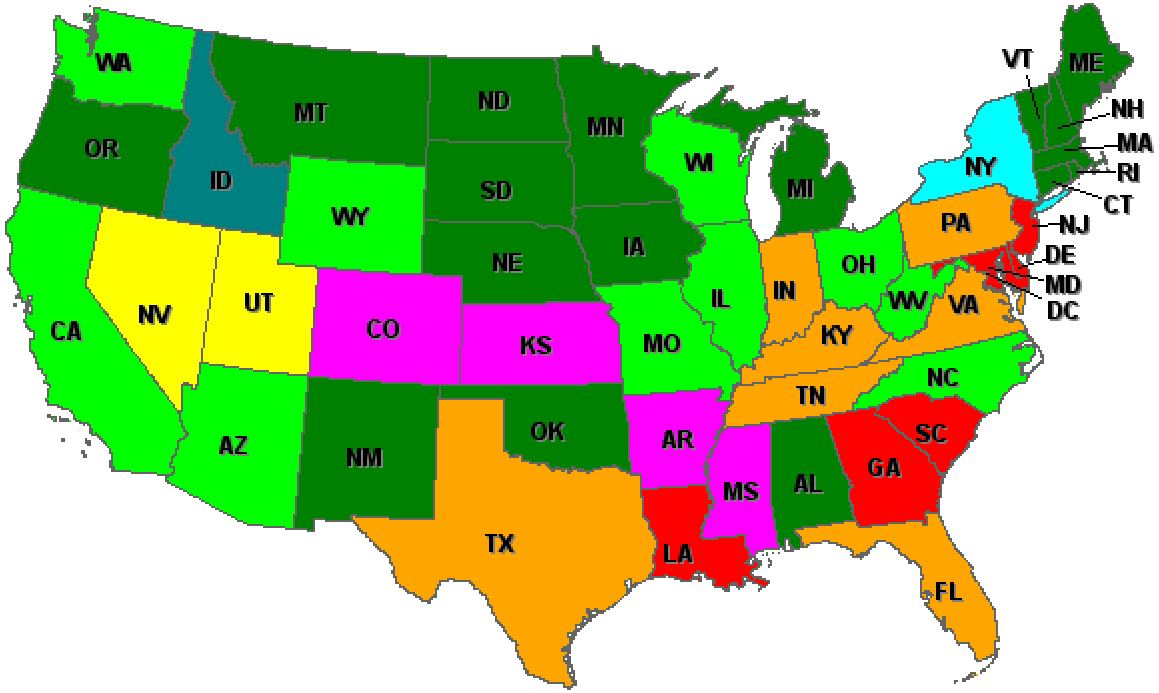
- Different from “Don’t use software”
- It means “Error-free software is not an assumption”
- Should check the output of software

Shift the Focus

- Audit the Election Not the Equipment
- Instead of checking
  - all the software, and
  - that it will perform several operations correctly every time
- Determine that only the **tally** is correct, only this time

Voting Technology: 2008 US Election

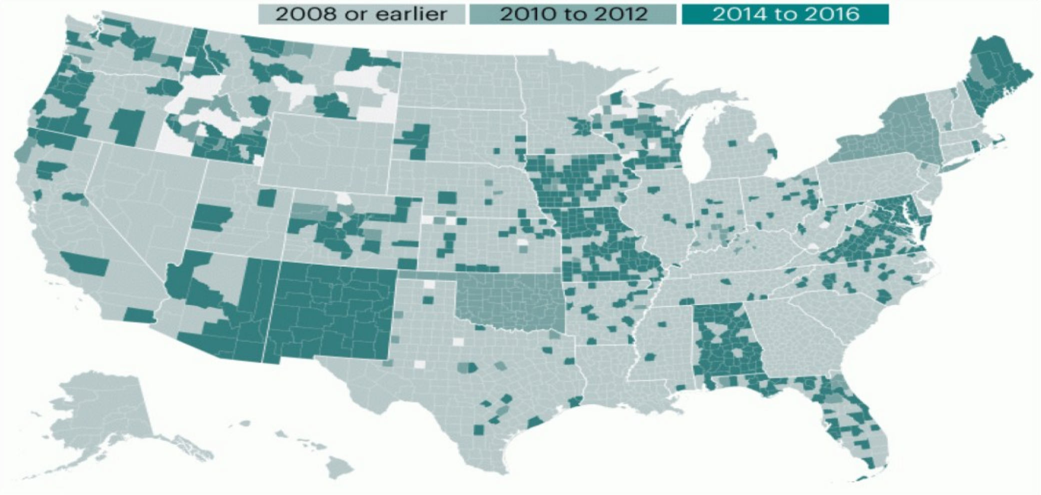
- Paper Ballot (also Puerto Rico)
- Paper Ballot and Punch Card
- Mixed Paper Ballot and DREs with VVPAT (also Hawaii and Alaska)
- DREs with VVPAT
- Mixed Paper Ballot and DREs with and without VVPAT
- Mixed Paper Ballot and DREs without VVPAT
- DREs without VVPAT
- Mechanical Lever Machines and Accessible Ballot Marking Devices



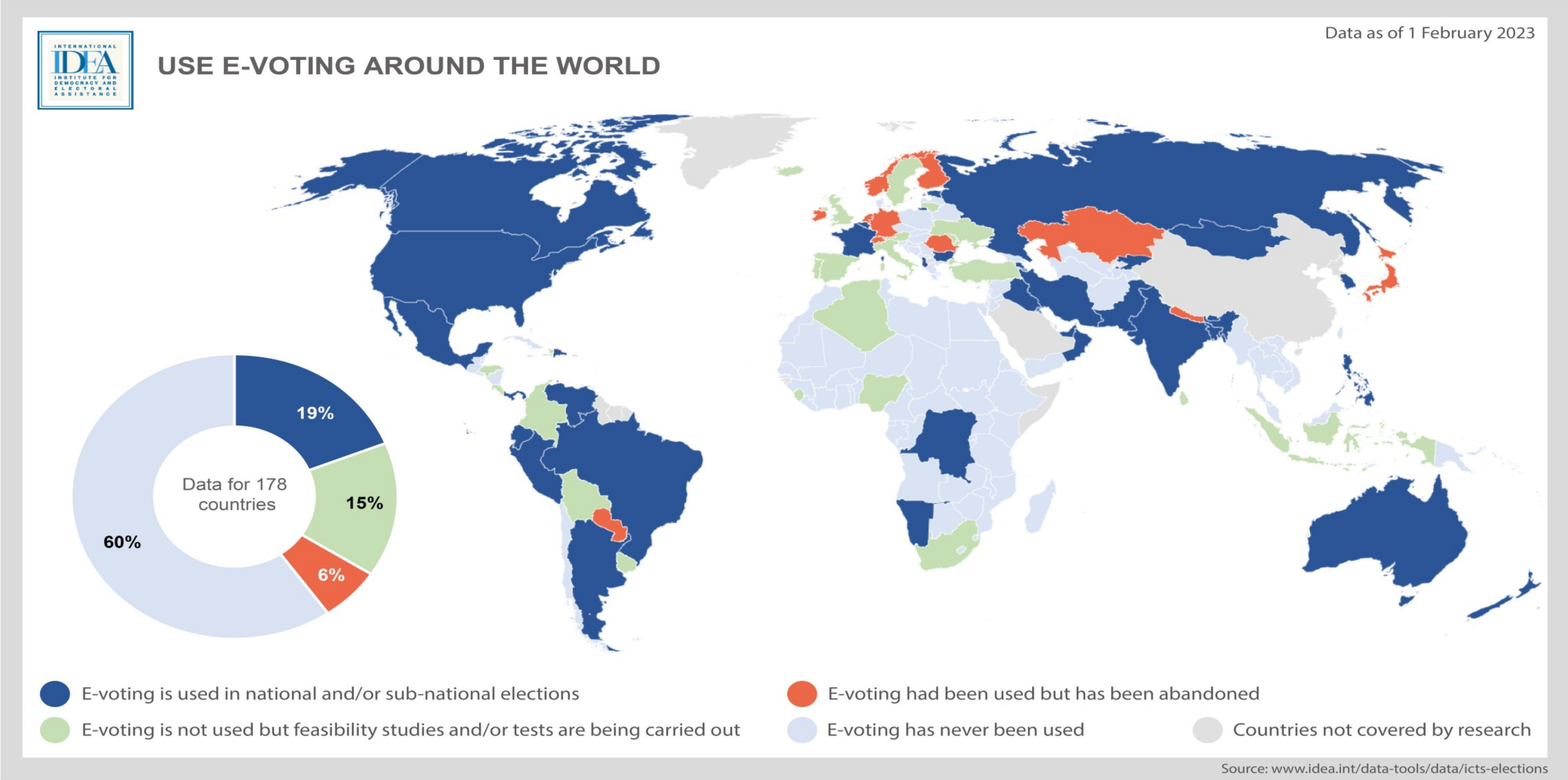
Source: Verified Voting Foundation

Example: E-Voting in USA

- Machine malfunctions are a regular feature of American elections.
- Many local jurisdictions depend on aging voting equipment based on frequently obsolete and sometimes insecure technology.
- Voting and tabulation equipment are not connected to the internet, making it difficult to hack systems remotely to change votes.



World Map of e-Voting (2023)



USE E-VOTING AROUND THE WORLD

Data as of 1 February 2023

INTERNATIONAL IDEA INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE
19%
15%
6%
60%
Data for 178 countries
E-voting is used in national and/or sub-national elections
E-voting had been used but has been abandoned
E-voting is not used but feasibility studies and/or tests are being carried out
E-voting has never been used
Countries not covered by research

Source: www.idea.int/data-tools/data/icts-elections

E-Voting Security Requirements

- Anonymity of the votes
  - The voter’s choice shall be confidential
- Accuracy of the votes
  - The integrity of the votes and number of votes cannot be altered
- Eligibility
  - only votes of legitimate voters shall be taken into account

Wang, K., Mondal, S.K., Chan, K., & Xie, X. (2017). A Review of Contemporary E-voting : Requirements , Technology , Systems and Usability. In Data Science and Pattern Recognition, ISSN 2520-4165 V1, N 1, 2017

E-Voting Security Requirements

- Un-reusability
  - Each voter is allowed to cast only one vote
- Public Verifiability
  - Anyone should be able to check the validity of the voting process
- Fairness
  - No Partial results can be computed before the end of the election

Wang, K., Mondal, S.K., Chan, K., & Xie, X. (2017). A Review of Contemporary E-voting : Requirements , Technology , Systems and Usability. In Data Science and Pattern Recognition, ISSN 2520-4165 V1, N 1, 2017

Remote E-Voting Security Requirements

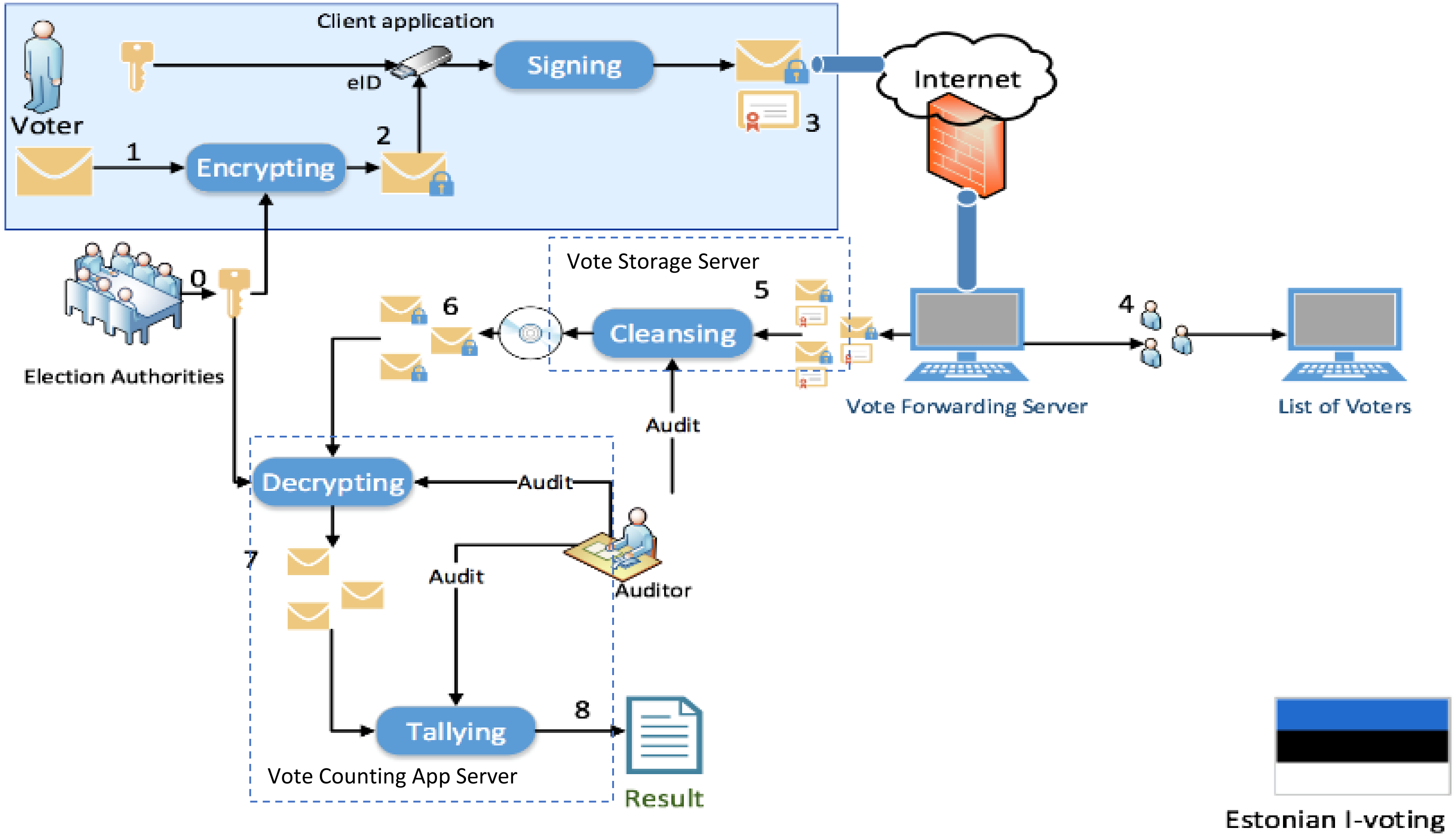
- Receipt-free
  - No voter is able to construct the contents of his vote
  - Prevent vote-buying and vote-coercion
- Reviseability
  - Voters can change their vote (prevent coercion of attacker looking over voters shoulder)
  - Necessary when voting location is not controlled by the election administrators

I-Voting system

- In 2005, Estonia became the first country in the world to hold nation-wide elections using I-Voting system
- It allows voters to cast their ballots from any internet-connected computer anywhere in the world
- During a designated pre-voting period (7 days), the voter logs onto the system and casts a ballot using
  - an ID-card in a personal SmartCard Reader
  - or a Mobile-ID in a mobile app
- The voter's identity is removed from the ballot before it reaches the National Electoral Commission for counting, ensuring anonymity.

1. https://e-estonia.com/solutions/e-governance/i-voting/
2. Nurse, J. R., Agrafiotis, I., Erola, A., Bada, M., Roberts, T., Williams, M., ... & Creese, S. (2017, July).
   An assessment of the security and transparency procedural components of the Estonian internet voting system.
   In *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 366-383). Springer.

Estonian I-Voting



1. Encrypt vote with Public Key of Election Authorities
2. Sign vote with eID Voter private key
3. Send Vote to the Vote Forwarding Server
4. Authenticate Voter using their eID public key

Image from R. Verbij. "Dutch e-voting opportunities." Master thesis, University of Twente, 2014

Estonian I-Voting

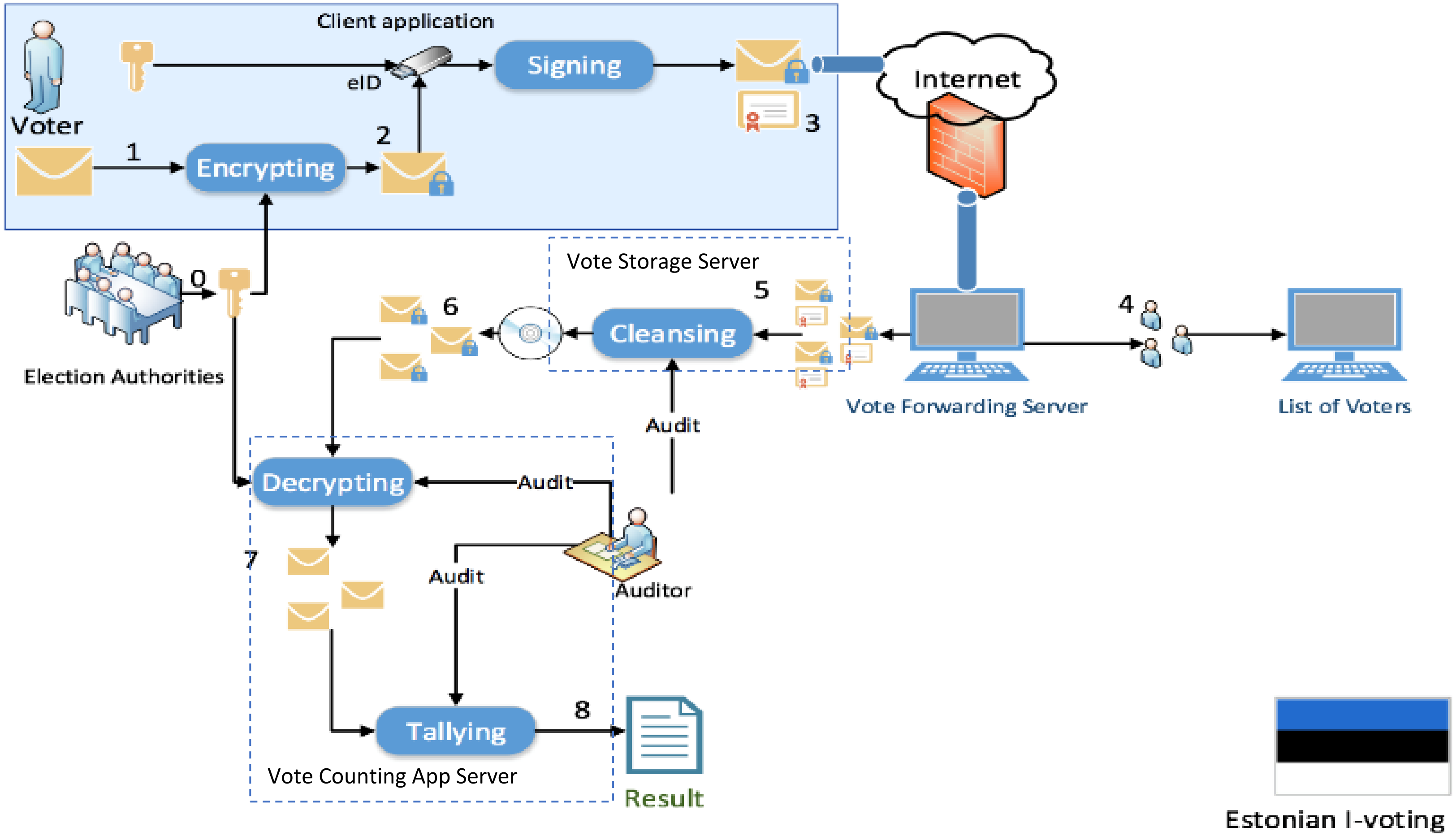


Image from R. Verbij. "Dutch e-voting opportunities.“ Master thesis, University of Twente, 2014

5. Send ballots to the Vote Storage Server for cleansing
6. Store ballots on a DVD
7. Delivery DVD to offline air-gapped server with Vote Counting App (VCA)
8. Publish results and then audit data and process

Estonian I-Voting: Analysis

- Audit process support verifiability and user trust in the system
- In I-Voting new vote overwrite the previous ones
  - Physical vote overrules any electronic vote
- Verify integrity of devices
  - Firmware-level malware checks
  - Advanced Persistent Threat
- Physical Security Requirements for election facilities
  - Server rooms with security seals and tamper-checks

Estonian I-Voting: Analysis

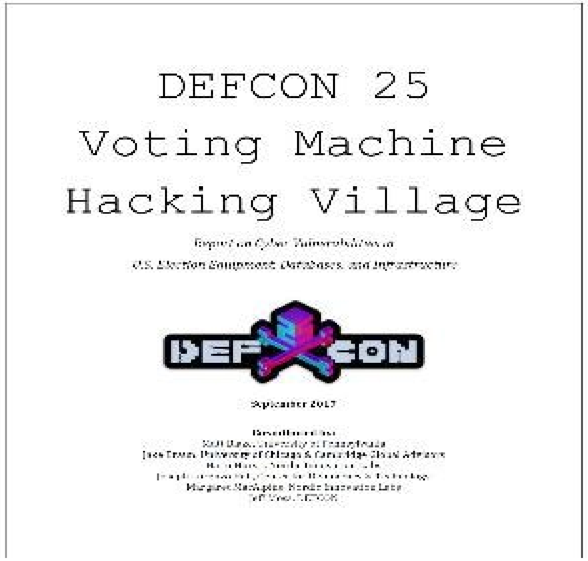
- Computer incident-handling processes during elections
- Analysis, checks, and investigations during and after elections
    - incoming ballots, server logs, etc.
- Main concern: resilience against highly sophisticated attacks
    - via large-scale compromise of voter machines
    - or attacks on hardware before reaching the system
- Vote Collection System (interact with client) to be outsourced
    - Possible additional integrity issues

What can go wrong

- Malware and Hacks
- Lack of Physical Security
- Side Channel Attacks to air-gapped server
- Human Errors

E-Voting Hacks

- Election hacking has recently gained prominence at DefCon.
- In 2017 the “Voting Machine Hacking Village” area revealed the cyber vulnerabilities of US election equipment, databases and infrastructure.

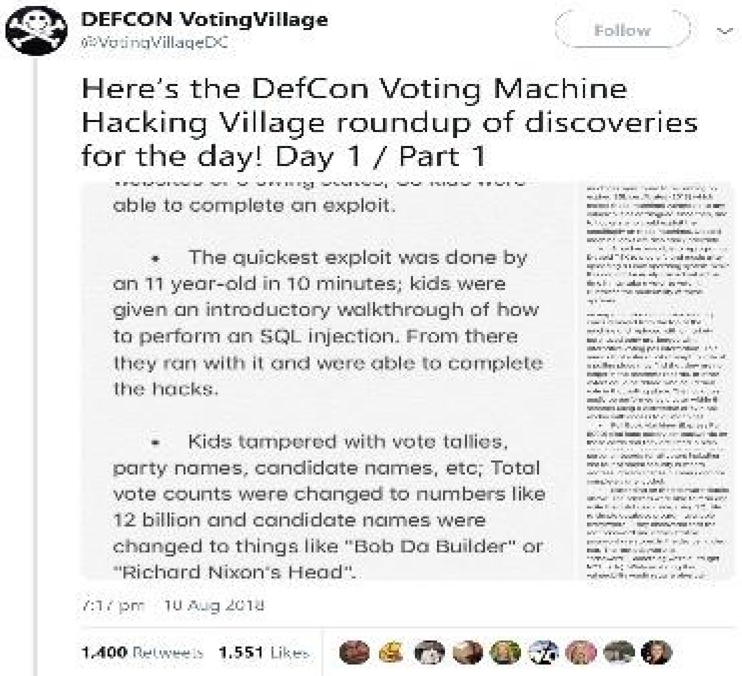


DEFCON 25
Voting Machine
Hacking Village

Report on Cyber Vulnerabilities in
U.S. Election Equipment, Databases, and Infrastructure

September 2017

Report Authors:
Matt Blaze, University of Pennsylvania
Jake Braun, University of Chicago & Cambridge Global Advisors
Harri Hursti, Nordic Innovation Labs
Joseph Lorenzo Hall, Center for Democracy & Technology
Margaret MacAlpine, Nordic Innovation Labs
Jeff Moss, DEFCON



DEFCON VotingVillage
@VotingVillageDC

Here’s the DefCon Voting Machine Hacking Village roundup of discoveries for the day! Day 1 / Part 1

able to complete an exploit.

- The quickest exploit was done by an 11 year-old in 10 minutes; kids were given an introductory walkthrough of how to perform an SQL injection. From there they ran with it and were able to complete the hacks.

- Kids tampered with vote tallies, party names, candidate names, etc; Total vote counts were changed to numbers like 12 billion and candidate names were changed to things like "Bob Da Builder" or "Richard Nixon's Head".

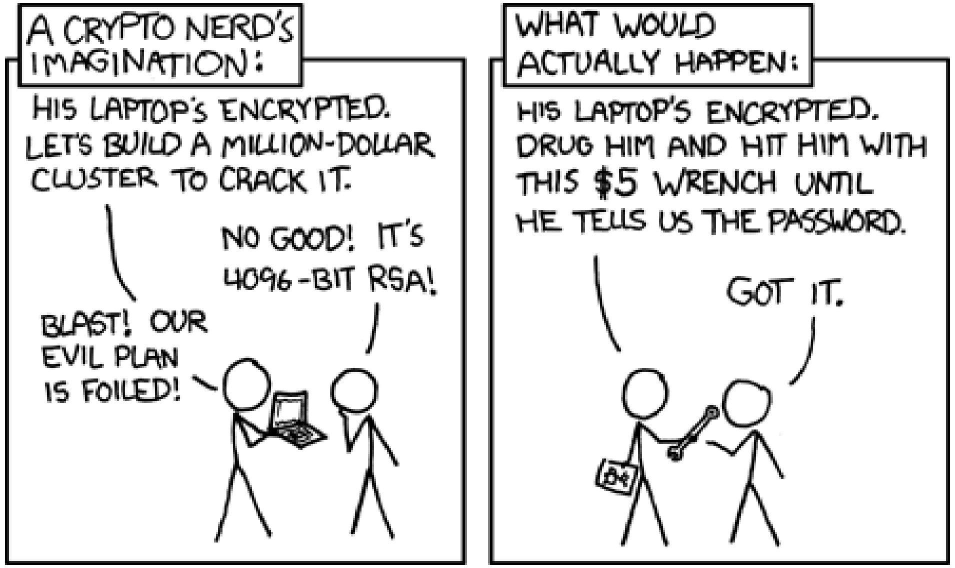
7:17 pm · 10 Aug 2018

1,400 Retweets 1,551 Likes

https://nakedsecurity.sophos.com/2018/08/14/11-year-old-hacker-changes-election-results/

Human Errors

- Social Engineering
- Weak passwords
  - Unisyn Voting Solution in USA: weak passwords for all devices written in the manual
- Poor physical security at the voting location
- Coercion


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

https://xkcd.com/538/

Vote Hijacking (Malware)

```
Class VoterApp {
....
int vote (int choice) {
          choice = BAD_GUY_CANDIDATE;
        String ballot = encrypt (choice, NEC_Public_Key);

        String signature  = sign (ballot, Voter_Private_Key)

        VFS.sendVote(ballot, signature, eID);
} }
```

Air-Gapped Computer

- Air gapping is a security measure to ensure that a computer network is physically isolated from unsecured networks like the internet and LANs.
- A true air gapped computer is also physically isolated
  - Data can only be passed to it physically
  - via USB, removable media, HDMI, firewire with another machine

Air-Gapped Computer breaches

- Social engineering
  - Human access the computer and attach a USB device or a Wi-Fi dongle [1]
- Electromagnetic
  - Eavesdropping on EM radiation from the computer’s memory bus
  - Monitoring leakage from USB ports and cables
  - EM shielding has become a common defensive measure

[1] https://www.wired.com/2016/11/wickedly-clever-usb-stick-installs-backdoor-locked-pcs/

Air-Gapped Computer breaches

- Acoustic Channels
  - hackable smartphones capable of picking up audio signals that the human ear can’t differentiate from background noise
  - RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis [1]
  - The most cutting-edge area involves the use of ultrasonic sound waves with higher frequencies that are both inaudible and provide greater bandwidth [2]
- Optical Transmission with easily-hacked surveillance cameras [3]

[1] Genkin, Daniel, Adi Shamir, and Eran Tromer. "Acoustic cryptanalysis." *Journal of Cryptology* 30.2 (2017): 392-443. https://www.cs.tau.ac.il/~tromer/acoustic/

[2] https://www.wired.com/2016/11/wickedly-clever-usb-stick-installs-backdoor-locked-pcs/

[3] https://abcnews.go.com/GMA/video/smart-home-devices-vulnerable-hackers-48446108

Air-Gapped Computer: tips for security

- Secure the machine off-site or in a fully-secured room
- Make sure all cables to the machine are properly shielded
- Use USB Port Blockers to plug any unused USB ports
- Turn the machine off and unplug it from the power source when not in use
- Replace all standard drives with SSD
  - No more acoustic leaks
- Encrypt all data

https://www.thesslstore.com/blog/air-gapped-computer/