E-voting Security Perspectives: Globally and in Switzerland

Prof. Bryan Ford
Decentralized and Distributed Systems Lab (DEDIS)

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Swiss Cyber Storm – October 18, 2017

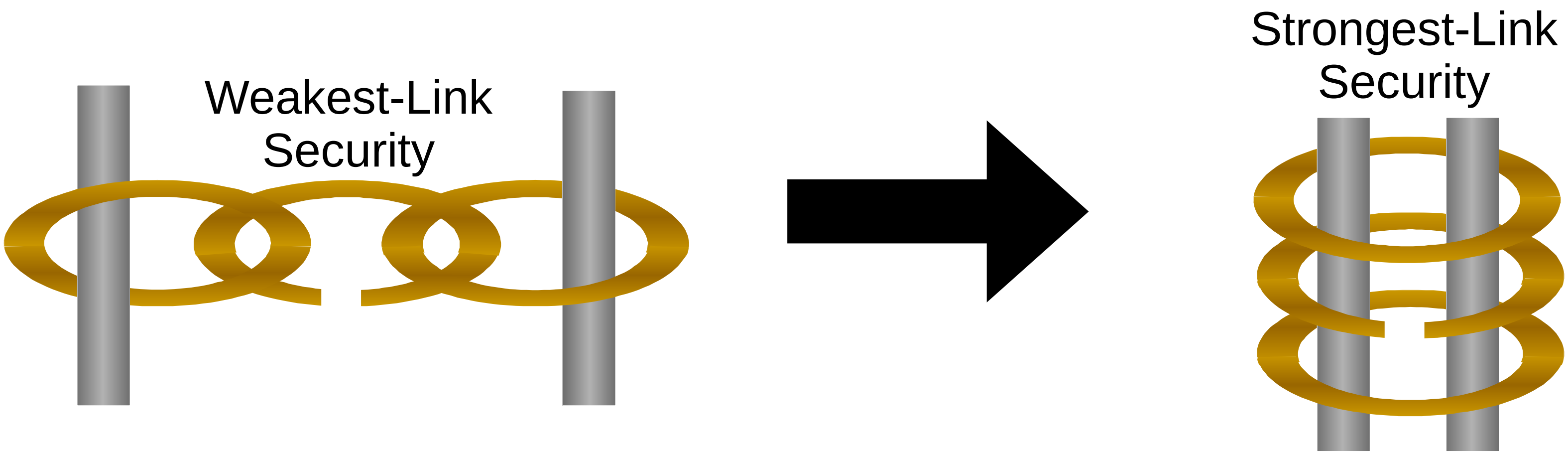
Introducing the DEDIS lab at EPFL

Design, build, and deploy secure privacy-preserving
Decentralized and Distributed Systems (DEDIS)

- **Distributed:** spread widely across the Internet & world
- **Decentralized:** no single points of failure or compromise

Overarching theme: building decentralized systems
that **distribute trust** widely with **strongest-link security**

- Accountable anonymity systems, next-gen blockchains, …



Talk Outline

- Basic concepts and types of E-voting systems
- E-voting workflow and security challenges
  - Voter registration, vote casting, counting & reporting
  - Integrity, availability, and privacy/coercion threats
- Reasons E-voting might be worth the risk
  - Comparative evaluation against paper-based voting
  - Available tools to address security challenges
  - Potential security advantages and opportunities
- Conclusion: what is the future of E-voting?

Introduction to E-voting

What is “E-voting”?
Voting with the help of
electronic systems

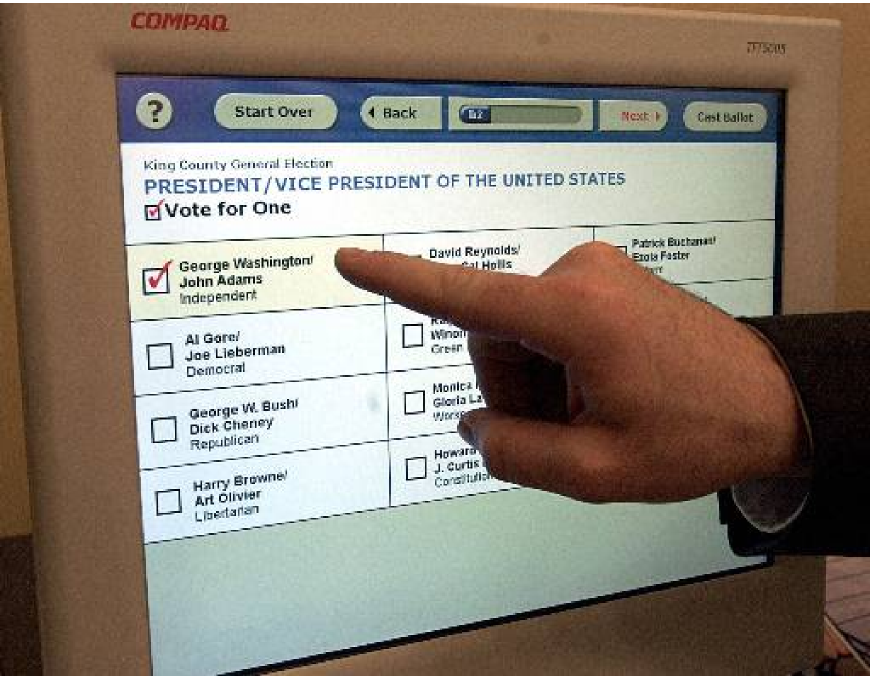
Huge variety of approaches around the world, but generally fall into a few major categories

- Paper-based electronic voting systems
- Direct-recording election (DRE) systems
- Online electronic voting systems

Paper-based E-voting Systems

Still produce and/or count **paper ballots**

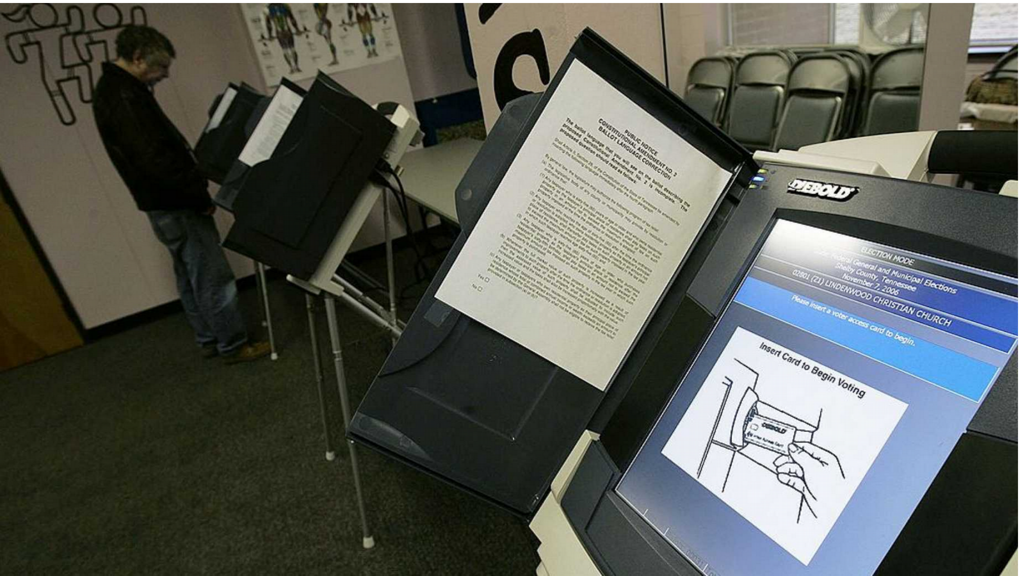
- Convenient user interface to print paper ballot
- May automate counting, with paper "audit trail"
  - But paper may not help if auditing is too costly

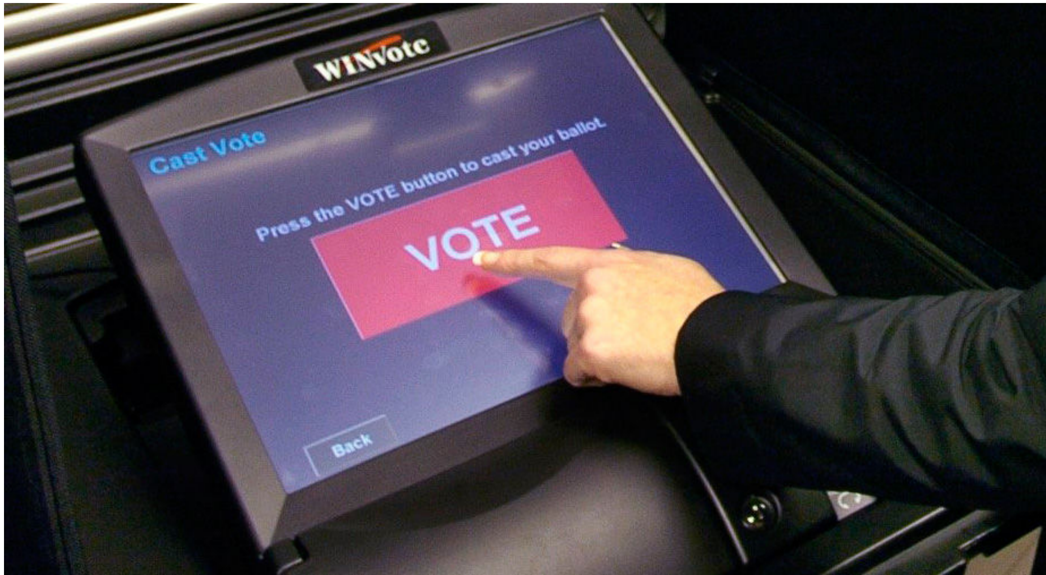

COMPAQ
?
Start Over
Back
Next
Cast Ballot
King County General Election
PRESIDENT / VICE PRESIDENT OF THE UNITED STATES
☑ Vote for One
☑ George Washington/ John Adams Independent
□ Al Gore/ Joe Lieberman Democrat
□ George W. Bush/ Dick Cheney Republican
□ Harry Browne/ Art Olivier Libertarian
David Reynolds/ Cal Hollis
Patrick Buchanan/ Ezola Foster

Direct-Recording Election (DRE)

Ballots are **entered and counted** electronically

- Increase user convenience, counting speed
- Users must still “show up” and vote in person
- Major risks of undetectable tampering
  - Must “just trust” vendors, election officials


DIEBOLD
ELECTION MODE
Please insert a voter access card to begin.
Insert Card to Begin Voting



Online E-voting Systems

Allow users to vote **remotely** over the Internet

- Convenience: vote from home with own device
- But hard to secure client device or environment
  - Malware could compromise vote integrity, privacy

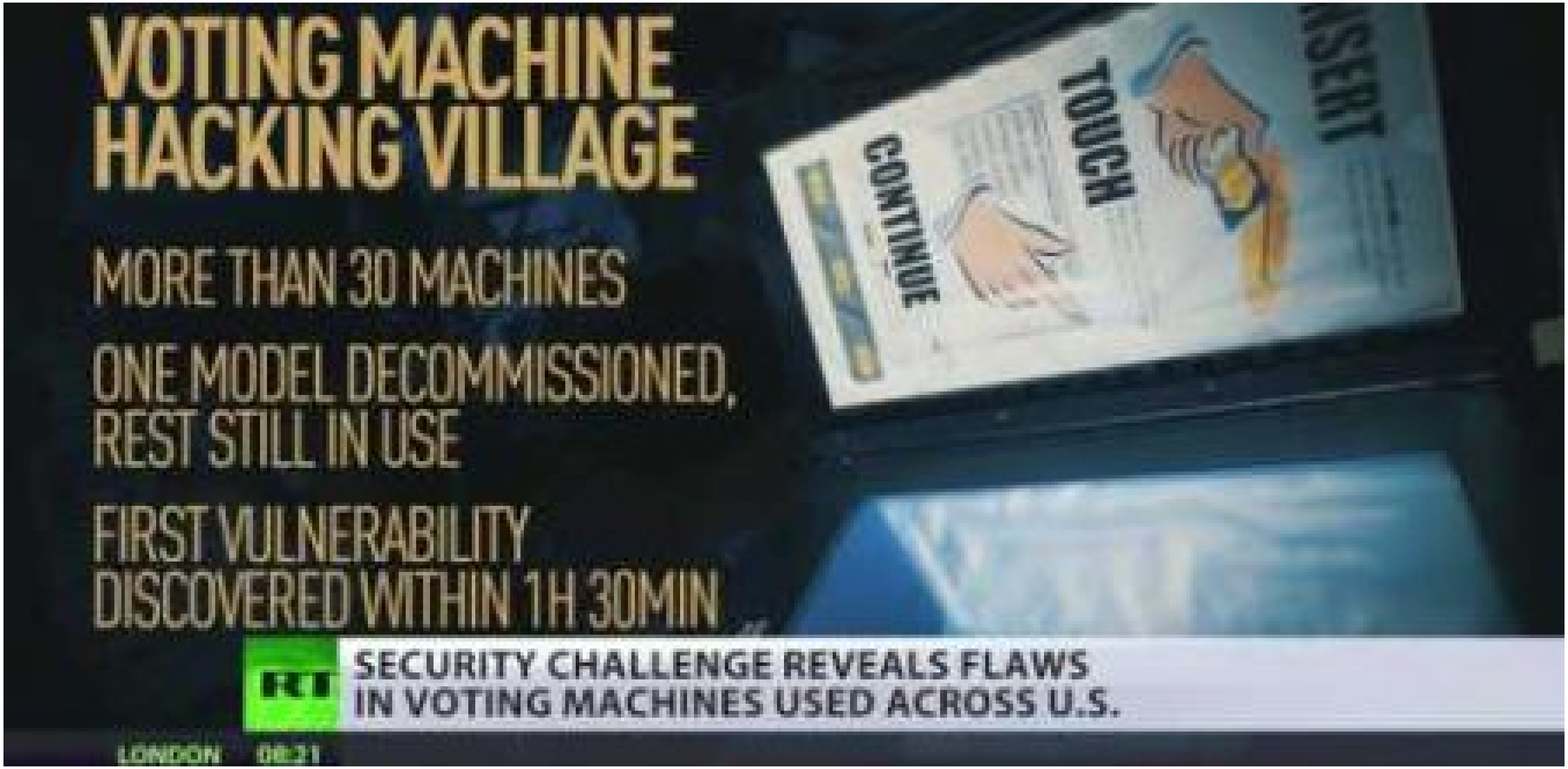
E-voting Security Horror Stories

Experiences from E-voting systems in the US

- Found to use obsolete, never-updated software
- Often vulnerable to malware compromise
  - Via local tampering (USB) or remote (wireless)
- Frequent reliability and availability failures
  - Inopportune crashes, potentially lost votes
- Usability issues: voter confusion, miscast votes
- Weak evaluation, certification requirements
  - “Seems to work” is definitely not good enough

E-voting Security Horror Stories

Many issues long known by security researchers, but recently highlighted at DEFCON 2017



VOTING MACHINE HACKING VILLAGE

MORE THAN 30 MACHINES

ONE MODEL DECOMMISSIONED, REST STILL IN USE

FIRST VULNERABILITY DISCOVERED WITHIN 1H 30MIN

SECURITY CHALLENGE REVEALS FLAWS IN VOTING MACHINES USED ACROSS U.S.

The State of Global E-voting

Much of the E-voting technology currently in use around the world is horrendously insecure…

- But that doesn’t mean it *needs* to be insecure: research points to many ways to improve

Poorly-informed policy decisions, weak standards, funding/business model failures equally to blame

- Limited transparency, accountability for security
- Insufficient incentives to drive strong security

State of E-voting in Switzerland

15 years of experimentation, 150+ pilots

- Cantons choose, Federal Chancellery certifies
  - Criteria depends on usage: 10%, 30%, 50%, 100%
  - Strong security requirements, e.g., trust-splitting
- Currently two active competitors in market
  - Third de-certified in 2015 over security concerns
- Encouraging E-voting access for 50% of voters
  - Pending proposal for 4-year E-voting moratorium
  - Pending proposal for E-voting CTF competition

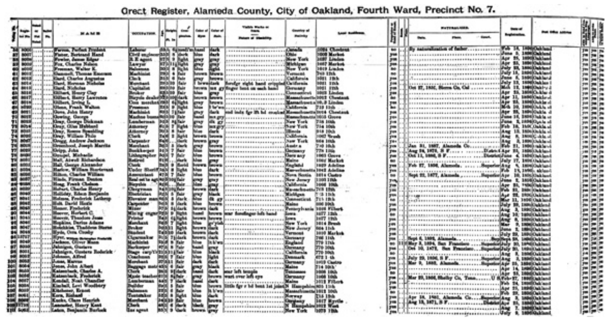
Talk Outline

- Basic concepts and types of E-voting systems
- **E-voting workflow and security challenges**
  - Voter registration, vote casting, counting & reporting
  - Integrity, availability, and privacy/coercion threats
- Reasons E-voting might be worth the risk
  - Comparative evaluation against paper-based voting
  - Available tools to address security challenges
  - Potential security advantages and opportunities
- Conclusion: what is the future of E-voting?

Generic E-Voting Workflow

Three fundamental phases:

- Voter registration (in-person or automated)
- Vote casting and recording
- Results tallying and certification



Grect Register, Alameda County, City of Oakland, Fourth Ward, Precinct No. 7.

Voter Registration

Determines:

- Who is allowed to vote?
- Where? At what polling station (US)? By mail
- What all is on ballot? Local, regional, national?

May be a separate process (e.g., US) or integrated with citizen registry (Switzerland)

- Local registries must be recorded, aggregated, delivered to E-voting systems securely

Voter Registration Security Issues

Small-scale risks, requiring (risky) action per vote

- Registering fake relatives, pets, dead people
- Feasible in either physical or electronic world
  - Physical: “social engineering” authorities in person
  - Electronic: hacking, tampering with voter records
    - Electronic registration attacks may be feasible even without E-voting, if voter/citizen records are electronic
- Rare in practice, hard to use to tip an election
  - The more fake records, the more likely detected

Voter Registration Security Issues

Larger-scale risks to be (more) worried about

- More sophisticated electronic attacks to create many fake “voters” *and hide their existence*
  - Harder to detect if no one ever sees fake records
  - Feasible if attacker controls voter database server
- Large-scale disruption or disenfranchisement
  - Prevent/discourage whole communities from voting
  - Systems offline, too few, confusing interfaces, must vote in particular location, voter ID laws (see US)

Both *security* and *usability* are equally critical!

Vote Casting Security Issues

- **Integrity attacks:** subverting the vote itself
  - Modifying cast votes: user votes A, device casts B
  - Casting multiple votes per user (ballot stuffing)
  - Dropping or spoiling ballots of “undesirable” users
- **Privacy attacks:** subverting voters’ free choice
  - Leak decisions to family, hackers, government, …
  - Coercion by family, abusers: “Let me help you vote”
  - Vote-buying: offer voters “anonymous donation” in exchange for proof that they voted attacker’s way

Security of Online Vote-Casting

Remote Internet-based voting adds challenges

- Election authorities can’t control client devices
  - May be old, rarely/never updated, malware-infested
- Risk partly depends on prevalence of devices
  - A few compromised devices unlikely to tip election
  - But a 0-day exploit of a *popular* device could…
- Can’t control environment in which users vote
  - May be more susceptible to coercion

Vote Counting and Reporting Issues

Tallying and reporting integrity risks:

- Modify counts (in obvious or less-obvious ways)
- Tamper with reporting, aggregation across sites
- Selective disenfranchisement of populations via vote-counting or reporting failures

Tallying and reporting privacy risks:

- Leak voter privacy via time or order votes cast
- Coercion via uniquely-identifiable ballots (e.g., in rank-choice or preference-order ballots)

Economic, Business Model Issues

Public vs private competition-driven funding?

- Competition may potentially drive faster innovation
- But “race to market” can incentivize *lower* security

Open source or closed/proprietary designs?

- Expose systems to broader scrutiny earlier
- But no guarantee that critical flaws will be found

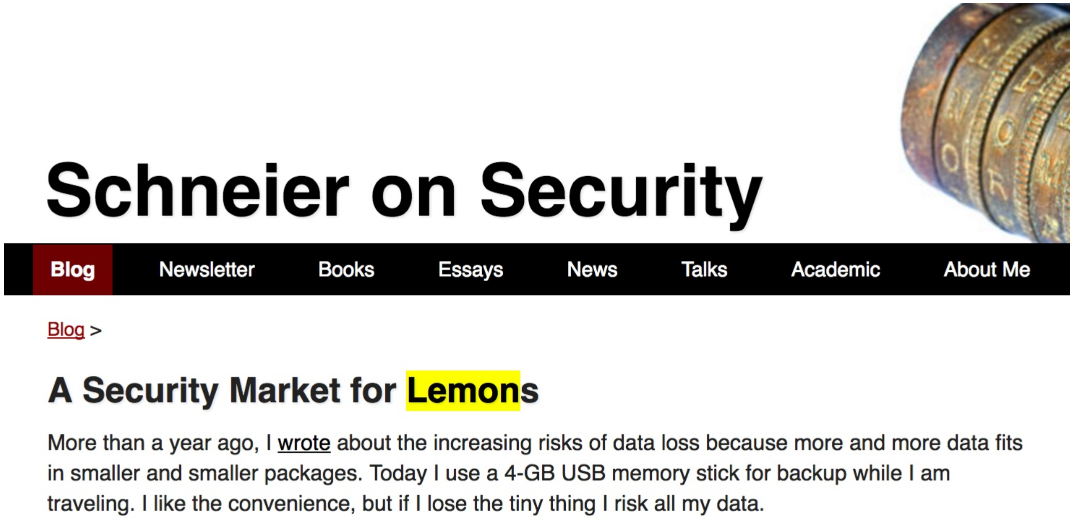
How to incentivize innovation, quality, diversity?

The Market for [Cyber] Lemons

George A. Akerlof won Nobel Prize in economics for observing:

If buyers have less information than sellers about product quality, incentives lead to reduced quality

Unfortunately, cybersecurity in general – and E-voting security in particular – tends to be a market for lemons.



Schneier on Security

A Security Market for Lemons

More than a year ago, I wrote about the increasing risks of data loss because more and more data fits in smaller and smaller packages. Today I use a 4-GB USB memory stick for backup while I am traveling. I like the convenience, but if I lose the tiny thing I risk all my data.

Talk Outline

- Basic concepts and types of E-voting systems
- E-voting workflow and security challenges
  - Voter registration, vote casting, counting & reporting
  - Integrity, availability, and privacy/coercion threats
- **Reasons E-voting might be worth the risk**
  - Comparative evaluation against paper-based voting
  - Available tools to address security challenges
  - Potential security advantages and opportunities
- Conclusion: what is the future of E-voting?

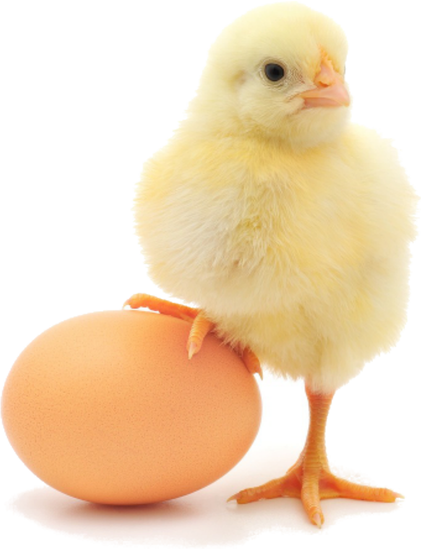
Voting: a Comparative Perspective

E-voting is (currently) a security/privacy disaster,
but *so is traditional paper-based voting*

- Paper-based registration, casting, tallying, reporting vulnerable to many analogous security risks
  - Must “just trust” election officials to behave honestly
  - Long tradition of “fishy” paper elections globally
- E-voting presents *opportunity* (if not yet realized) for greater transparency and security
  - If known technological tools are used properly
- Potential for greater convenience, participation

Can we trust paper ballot counts?

A paper-based “audit trail” isn’t so useful if you never actually count or audit the paper ballots!



Experiences from US election in 2016:

- Only 1 of 3 recount attempts “completed”
- Costly: not authorized unless convincing public evidence of tampering *already exists*
  - But a recount or audit is the only way to get that evidence!
- Procedures excluded many districts from recounts
  - Attacker could hide tampering simply by breaking a seal
- Sampled risk-limiting audits could lower costs
  - But more complex, politically and legally “not a thing”

Disruption and Disenfranchisement

Disruption from inconvenience, under-provisioning

- Make voters in “undesirable” districts wait hours, impose confusing rules on where & when to vote
  - Result: many people give up and just don’t vote

Disruption via cumbersome “security” provisions

- Example: “Photo ID” requirements in the US
  - Ostensibly to prevent voting fraud, but no evidence
  - In reality, disproportionately prevents poor, minority, handicapped, or elderly voters from voting

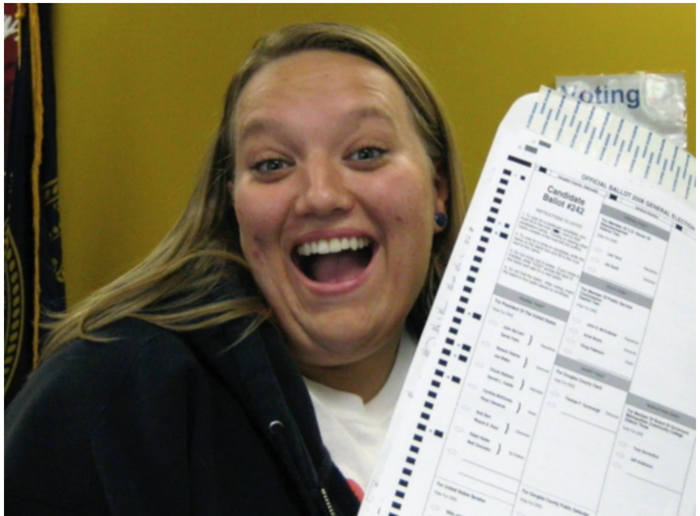
Privacy, Coercion Risks with Paper

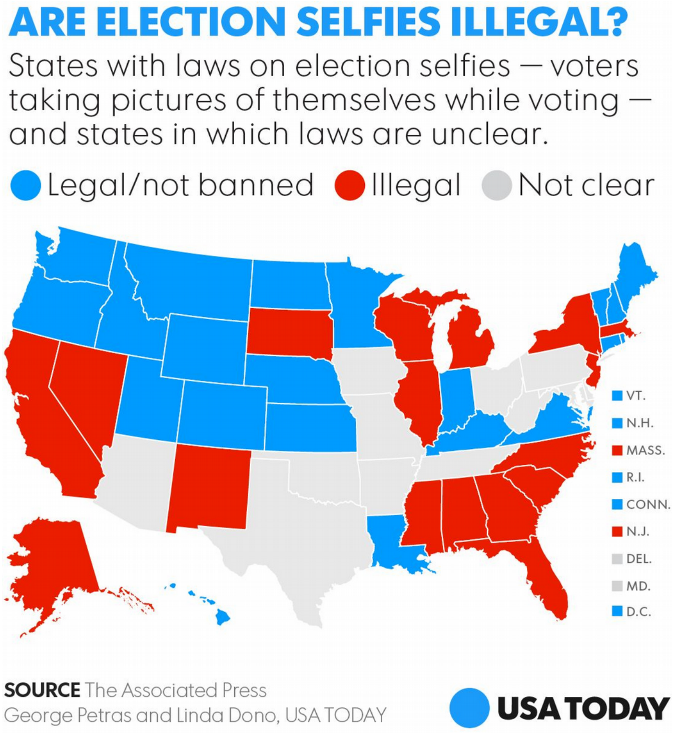
Much of Europe (including Switzerland) routinely uses mail-based “voting from home” anyway

- Less cultural concern for coercion risks

US-style ballot booth privacy is far from perfect

- “Ballot selfies” are popular, but present coercion risk




ARE ELECTION SELFIES ILLEGAL?

States with laws on election selfies — voters taking pictures of themselves while voting — and states in which laws are unclear.

SOURCE The Associated Press

George Petras and Linda Dono, USA TODAY

Tools to Improve Voting Security

We have many **mature technologies** to increase the security and transparency of voting systems

A few examples:

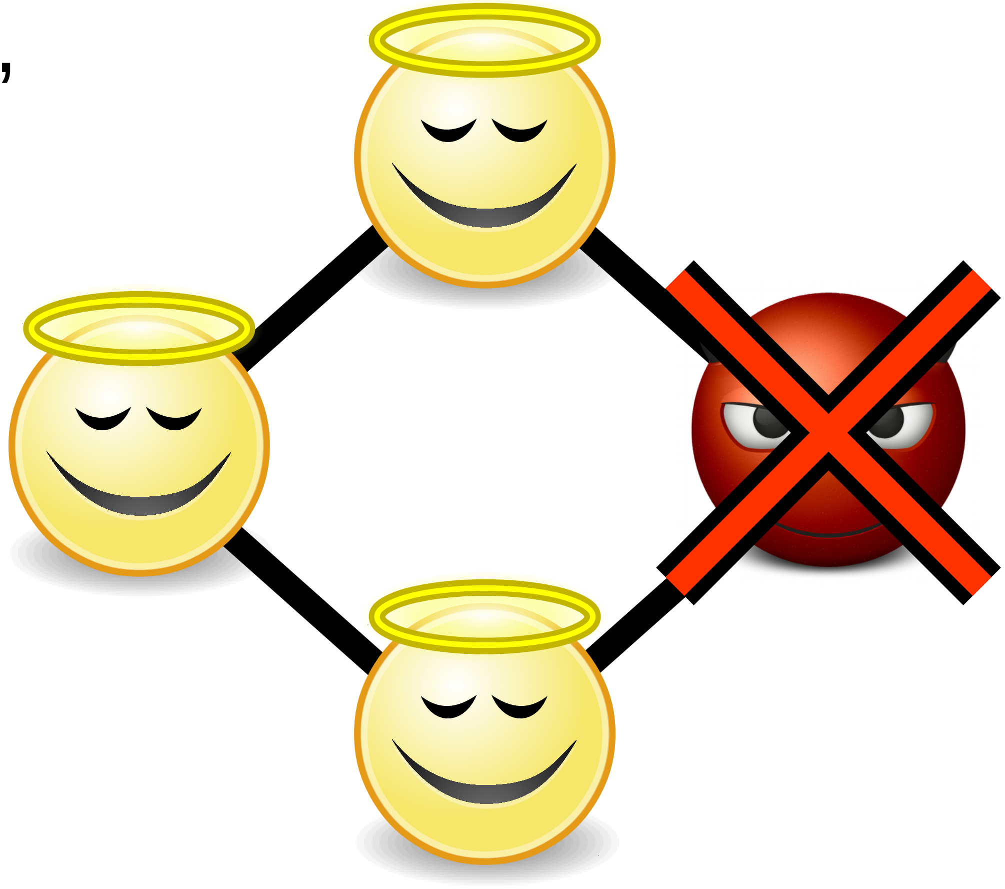
- **Cryptographic verifiable shuffles:**
  prove ballots were permuted without tampering
- **Homomorphic encryption:**
  add up all encrypted ballots *before* decrypting
- **Distributed ledgers (aka “blockchain”):**
  ensure public transparency of ballots, results

Properly used, could improve security over paper

Fundamental Tool: Distributed Trust

Computer science theory, algorithms, crypto has long known *principles* of decentralized security…

- Threshold cryptography, Byzantine consensus
- Tolerate any one (or several) arbitrary failures or compromises



Fundamental Tool: Distributed Trust

Computer science theory, algorithms, crypto has long known *principles* of decentralized security…

- Threshold cryptography, Byzantine consensus
- Tolerate any one (or several) arbitrary failures or compromises

Already a requirement in E-voting systems for Switzerland

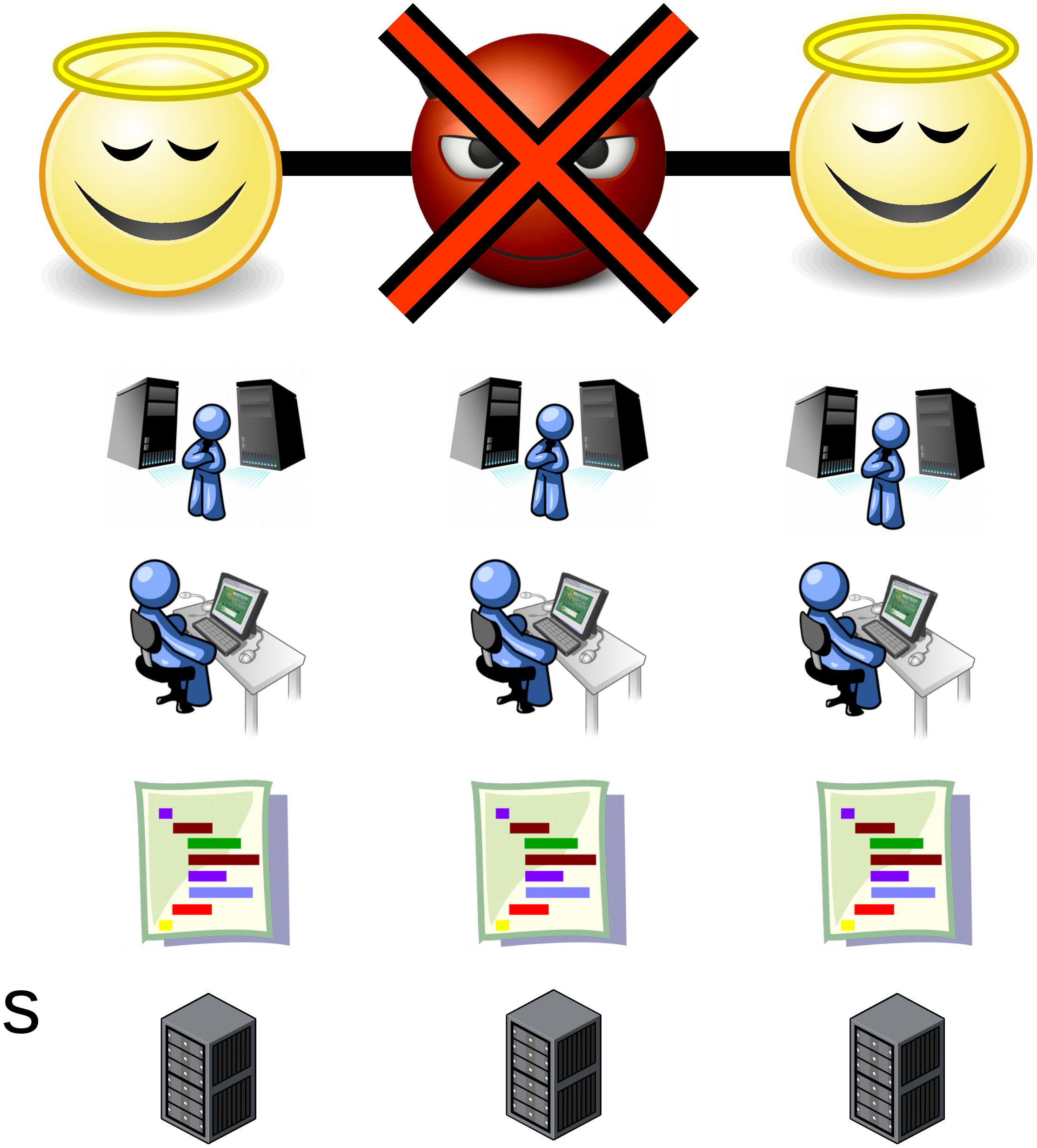
Distributed Trust is Work in Progress

Avoid single points of failure, compromise

But risks come at many levels…

- Operators
- Developers
- Software
- Hardware

Must address all levels



Opportunities for “Coopetition”

Competition can help drive *functional* innovation

- More convenient interfaces, features, etc.

Standards & cooperation is better to drive security

- Well-known principle: don’t compete on security
  - It’s like mud-wrestling a pig: everyone gets dirty
- Cooperation could potentially improve resilience, diversity
  - Example: cross-vendor cryptographic verification of critical voting processes
    - each keeps the other honest

Incentives for Security Hardening

Robust, well-run “bug bounty” programs can help

- Discover, fix flaws before attackers can exploit
- Increase public confidence in system security

Long-term: Evolution of Democracy

E-voting offers potential to enable users to participate more regularly and directly in decisions

- Promising experimental participatory models feasible only if users have direct online access

Example: **Delegative** or **Liquid Democracy**

- Give users a *choice* to participate directly or via representative on a given topic
- Many challenges, but we must evolve

Direct + Representative = Delegative Democracy

Talk Outline

- Basic concepts and types of E-voting systems
- E-voting workflow and security challenges
  - Voter registration, vote casting, counting & reporting
  - Integrity, availability, and privacy/coercion threats
- Reasons E-voting might be worth the risk
  - Comparative evaluation against paper-based voting
  - Available tools to address security challenges
  - Potential security advantages and opportunities
- **Conclusion: what is the future of E-voting?**

Conclusion: Challenges and Opportunities

E-voting presents **huge security challenges**

- Risk of undetected manipulation, disruption, …
- Critical, but many are not unique to E-voting

E-voting also presents **significant opportunities**

- Conveniences demanded by today’s users
- Long-term: more participatory democracy

Conclusion:
What’s the Path Forward?

We have many **technical tools** to mitigate risks

- Modern cryptography, distributed ledgers, etc.
- Proper designs could offer *stronger* security, and require less “blind trust” in authorities, than conventional paper-based voting

Must **innovate vigorously** but **deploy cautiously**

- Technically-informed, security-focused policy
- Combine benefits of competition & cooperation