The Best Election
Money Can Buy

Joe Kiniry
Galois

NASED 2016
Our Mutual Expertise

• you are the election experts
  
  • your little finger probably knows more about elections than I have learned in my fifteen years of elections work

• I am a security and critical systems expert
  
  • I hacked my first internet voting system in 2003 and have analyzed dozens of election systems

  • I built my first high-assurance election system in 2003 and it was used in EU elections in The Netherlands

  • I have advised four governments on matters related to the use of computers in elections, esp. security
“Perfect” Elections

• we—you and I—want our elections to run smoothly

• we want evidence so there is no contested result

• we want the outcome to represent the will of the electorate

• we want the public to trust in the election’s outcome

• elections officials must provide “perfect” elections that satisfy the electorate—but also other forces—including candidates, political parties, and media

• here are some simple, cheap recommendations for significantly improving our elections in the 21st century
Recommendations

- introduce a security mindset into your team

- mandate risk-limiting audits and parallel testing

- demand that election technologies provide evidence of their correctness and security, preferably in both the RFP and contracting process
Recommendations

• introduce a security mindset into your team

๏ mandate risk-limiting audits and parallel testing

• demand that election technologies provide evidence of their correctness and security, preferably in both the RFP and contracting process
Recommendations

• introduce a security mindset into your team

• mandate risk-limiting audits and parallel testing

○ demand that election technologies provide evidence of their correctness and security, preferably in both the RFP and contracting process
The Security Mindset

• find or introduce someone in your organization that can “turn on” a security mindset

• hire an intern that is a computer science student

• speak with your local university’s computer science department to find a public employee willing to donate their time for public good

• encourage your local IT support organization to facilitate an employee to do on the job training
RLAs and Parallel Testing

• risk-limiting audits are the least expensive way to audit which candidates won the election

• they only work in jurisdictions with a paper record

• they are mandated by law in CA and CO

• perform inexpensive experiments with risk-limiting audits and parallel testing in sensible jurisdictions

• advocate for new state laws that mandate audits
Evidence

• evidence comes in many forms, from scientifically peer-reviewed papers to legal guarantees

• certification is the only form of evidence widely understood and used today

• the VVSG is working toward a better understanding of what constitutes legitimate evidence that is third party verifiable
Why Make These Recommendations?

• 21st century elections are fundamentally different
• technology has tremendously impacted…
  • …what is possible for new elections solutions
  and
  • …what is possible for hackers with ill intentions
Today’s State of Affairs

- our elections are critical systems
- the technology that we use is often out-of-date
- there is little budget to replace systems
- evolution in federal standards takes time
- the security of elections is often not top priority
technology is everywhere in our elections
election management systems
voter registration
ballot distribution
remote ballot marking
electronic poll books
DRE voting machines
internet voting
vote tabulation
elections auditing
results reporting
Technology’s Impact

Technology...

...is meant to help run “perfect” elections

...changes the very nature of elections

...empowers voters

...empowers campaigns

...empowers bad actors
Finance and Security

• historically we find that, in every industry where there is money to be made, bad actors get involved

• >$1B dollars will be spent this year for the election

• the majority of those funds flow to the media

• some funds are used by campaigns for computer science—from artificial intelligence to online advertising—to optimize their campaigns

• this security expert’s hypothesis: some campaigns, or their proxies (e.g., Super PACs), are using computer science—in the form of hackers—in this election
WASHINGTON — In the latest cyberattack targeting the federal government, an intruder gained access to information for thousands of employees at the Justice Department and the Department of Homeland Security, but officials said Monday that there was no indication that sensitive information had been stolen.
Nothing Classified or Hip in C.I.A. Director’s Hacked Email  OCT. 20, 2015

Hacking of Government Computers Exposed 21.5 Million People  JULY 9, 2015

White House Weighs Sanctions After Second Breach of a Computer System  JUNE 12, 2015

U.S. Was Warned of System Open to Cyberattacks  JUNE 5, 2015

Hacking Linked to China Exposes Millions of U.S. Workers  JUNE 4, 2015

Russian Hackers Read Obama’s Unclassified Emails, Officials Say  APRIL 25, 2015
Let’s look at some core maxims of security, reinterpreted for elections.
Maxims of Secure Systems

**Shannon’s maxim**
The enemy knows the system.

**Kerckhoff’s principle**
A system must be secure even if the code is public.

**The NSA and DOD’s recommendation**
Assume you are hacked.
Maxims of Secure Elections

**Shannon**
Hackers already have the code for your election systems and know your processes.

**Kerckhoff**
An election should be secure even if everything about the election is public knowledge.

**NSA/DOD**
Assume bad actors or hackers work for you, work for your vendor, and already have backdoors on your election systems.
Internet Voting

• internet voting is a case study in insecure elections

• no existing internet voting product or research prototype is secure, usable, and accessible

• we should not call today’s remote voting systems “internet voting”, but instead “machine voting”

• they only have a chance at working if no hackers are interested in your election, you completely trust the vendor and all of their employees, and you are lucky
E2E-VIV

• internet voting as a case study in secure elections

• recalling our maxims, this new kind of voting system is…

  • …a technology platform about which the enemy knows everything (Shannon), and

  • …created and maintained in a completely transparent and open fashion (Kerckoff),

  • … is one that operates property even assuming breach

• the only path forward is to turn “machine voting” into end-to-end verifiable internet voting (E2E-VIV), which is the focus of the U.S. Vote Foundation’s report “The Future of Voting” published last year, which I co-authored
Recommendations

• introduce a security mindset into your team

• mandate risk-limiting audits and parallel testing

• demand that election technologies provide evidence of their correctness and security, preferably in both the RFP and contracting process
do not make the trustworthiness of your election depend upon the trustworthiness of your staff or your vendors