U.S. VOTE FOUNDATION

THE FUTURE OF VOTING

End-to-End Verifiable Internet Voting: Specification and Feasibility Research Study

Susan Dzieduszycka-Suinat,
President and CEO, U.S. Vote Foundation

Joseph Kiniry
Principal Investigator, Galois, Inc.

THE FUTURE OF VOTING

Brought to you through the
generous support of

U.S. VOTE FOUNDATION

THE FUTURE OF VOTING

PART I
End-to-End Verifiable Internet Voting and the Project

- - -

PART II
Discussion and Feedback

Goals for Today's Meeting

- Answer your questions about Internet Voting
- Identify the challenges
- Familiarize you with End-to-End Verifiable Internet Voting (E2E VIV)
- **Inform you of the** E2E VIV project
  - Our project's goals
  - Findings and Recommendations
- Garner your feedback!

Please tell us about your expectations for our session today

What does the Future of Voting look like to You?

Let's answer the 3 most common questions first....

If I can bank online, why can't I vote online?

Banking ≠ Voting

- In banking, the bank…
  - Knows who you are
  - Knows every transaction you make
  - Has a ledger on all transactions in the bank
  - The bank and the federal government insure loss
- In elections…
  - Voter identity and vote are private
  - No ledger of all transactions
  - No insurance if something goes wrong

Why not just use email to transmit ballots?


VIDEO

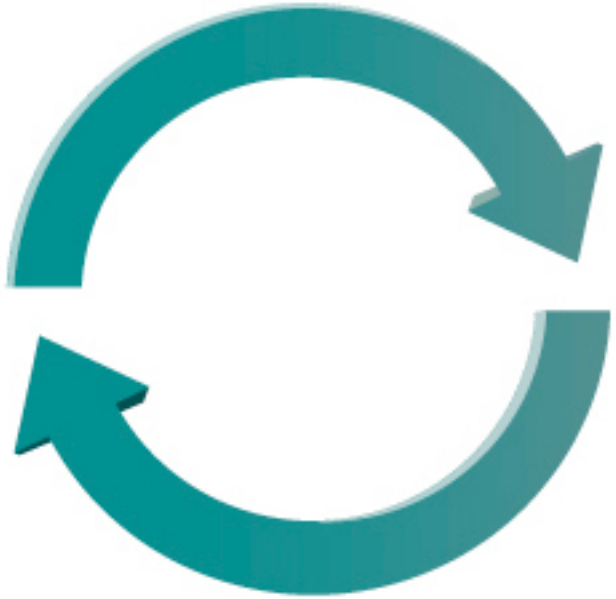
Aren't there a lot of existing vendors already out there selling Internet Voting already....

How are they successful, if Internet Voting is so risky?

Today's Internet Voting Vendors

- No Existing Vendor…
  - Permits public disclosure of their source code
  - Has publicly-documented protocols or formats
  - Provides evidence of election correctness verifiable by any individual or organization
  - Permits public discussion of their pricing or contracts
  - Has an End-to-End Verifiable system:
    a property that every elections security expert in the world insists is mandatory for voting systems

Before we move on....
What does End-to-End Verifiable really mean?



Or better yet…
What precisely is Internet Voting and when can I use it?

It's Internet Voting if...

- Voter is permitted to submit their completed ballot over the Internet in any manner (email, web site, iPhone app, desktop app, etc.)...

  Then the voter is using Internet Voting

- Election official is using technology which transmits voter choices over the Internet (whether it is over a VPN, implicitly by reporting ballots after the election, etc.)...

  Then the election official is using Internet Voting

But We Want Internet Voting!

- It will raise election participation rates!
- It will decrease election costs!
- It will permit the disabled greater independence in participating in democracy!
- It will be more convenient for voters!
- It will be make elections easier to manage!

None of these statements are true today - Were an open source E2E VIV system to exist, perhaps they could be true tomorrow

Challenges of Internet Voting

- Think how difficult it is to secure a single service available over the internet - even for governments and large corporations
- For Internet Voting to work using traditional IT, you must secure every computer, phone, cable modem of every voter in your election!

A bespoke, open source E2E VIV system designed by the world's experts is the only possible way to have a secure, trustworthy internet election

Verifiable Elections

- An election is ***verifiable*** if independent third parties can confirm the election outcome
- Traditional elections are verifiable…
  - Quality election processes
  - Independent election observers
  - Public participation in elections
  - A public tally

No existing commercial
Internet Voting system is verifiable

End-to-End

- An end-to-end secure system means …
  - System designed to be secure from threats from the beginning to the end of the system's purpose
  - For elections, that means from brain of the voter to the announcement of the election result
- An end-to-end secure election system is secure from hackers, insider-attack, and simple mistakes in running the election

No existing commercial Internet Voting system is end-to-end secure

End-to-End Verifiable Elections

- Consequently, an End-to-End Verifiable Election system is both
  - Verifiable (independent third party verification of the election outcome is possible)

+

  - End-to-End (secure from the voter's brain to the election outcome)

No existing commercial voting system (of any kind) is end-to-end verifiable

E2E Verifiable Internet Voting - 1

- An E2E Verifiable Internet Voting system is both end-to-end and verifiable, and moreover…
  - Must not require that voter's devices are secure
  - Must not require that your servers have security better than the likes of the IRS and Sony
  - Must be open source and prove to the world that you are using the audited software everywhere
  - While…

E2E Verifiable Internet Voting - 2

- An E2E Verifiable Internet Voting system is both end-to-end and verifiable, and moreover…
  - Permits voters to check that their votes are recorded properly, but not violate their privacy
  - Permits voters to check that their votes are included in the final tally
  - Permits anyone to check that all of the cast ballots have been tallied correctly

E2E VIV System Benefits

- E2E Integrity - digital manifestation of processes and controls that you know and understand used in paper-based elections
  - The system protects the election from hackers, malicious insiders, and administrative errors
- Software Independent - you need not trust vendors' software or hardware for a correct election outcome
  - If something goes wrong, election officials are guaranteed to detect it, determine the cause, and remedy the situation

No existing commercial Internet Voting system has E2E integrity or software independence

Sounds Magical

...

Is it possible?

E2E VIV is Complex, but…

- R&D on E2EV election systems has been ongoing for *20+ years*
- Creating a *correct* E2EV system is *difficult*
- Creating and operating a *secure* E2EV system is *very difficult*
- Creating and operating a correct and secure E2EV *Internet Voting* system is…

only possible with the right team
at the right time…
and that time is now

Let's Have a Look

• • •

An E2E System in Action:
Turning Theory into Practice

E2EV in Action – STAR-Vote

- Introducing a "Secure, Transparent, Auditable, and Reliable" Voting System – The STAR-Vote ballot marking System
- Designed by election officials in Travis County, Texas in tandem with top academic experts in E2EV systems
- The STAR-Vote Team – The *"Avengers for Elections"*: cryptographers, security experts, statisticians, election auditing experts, etc.

STAR-Vote Prototype Demo

STAR-Vote as an Internet BMD

- Why not use STAR-Vote as an end-to-end internet ballot marking device?
  - Design is bespoke to supervised voting, not an internet ballot marking device
  - User Interface – particularly relating to vote verification – is hard to use
  - Ensuring the product is correct and secure is an extremely difficult R&D task

Can use STAR-Vote as case study in how to design and build an E2E VIV system and perform usability experiments

Designing an E2E VIV System

- Cannot use STAR-Vote for Internet Voting or as a home BMD…

  We must precisely understand exactly what is necessary for a E2E VIV that is useful, accessible, correct, and secure

- How do we use the latest research in…

  End-to-end secure systems, verifiable elections and systems, and usable secure systems to design the world's first E2E VIV system for the public?

End-to-End Verifiable Internet Voting: Specification and Feasibility Assessment Study (E2E VIV Project)

• • •

Take on the Internet Voting Challenge

Informal Goals – E2E VIV Project

- Convene a "Team of Rivals"
- Change the Conversation → Constructive
- Fill in the Research Gaps
- Approach a difficult, 'stuck' topic from a research perspective
- Create New, Current Reference Points
- Drive Positive Messaging

Formal Goals – Success Targets

- Produce Written Report
- Develop System Specification
- Product Recognized by LEOs
- Public Hearings, Advocacy Groups
- Inform Public of Study Results
- Identify Path to Next Phase/s

Address IV Challenges Head-on

- Anonymity of Voter / Ballot
- Usability / Accessibility
- Cyber Security Threats
- Auditability
- Testing / Certification

Team and Organization

- U.S. Vote Foundation – organization, management and communication
- Galois – technical project management, execution, and engineering
- Academic and Scientific Experts
- Usability and Accessibility Experts
- Local Election Officials

Report Contents

Executive Summary

- 5 Pages, Illustrated

Part 1: For the Public

- Introduction
- Remote Voting
- E2E VIV Explained
- Required Properties of E2E Systems

Part 2: For Technologists

- Crypto Specification
- Architecture
- Rigorous Engineering
- Verification & Validation

Part 3: Looking Forward

- Feasibility
- Conclusion
- Appendices

Phase I Project Outcomes

• • •

Specification and Feasibility

Study Outcomes – 1 of 3

- *Complete set of requirements* for an E2E VIV system have been crafted
  - Any system which fulfills those requirements and provides evidence of such is an E2E VIV system
- *Collection of alternative architectures* for E2E VIV systems has been specified
  - The precise solution architecture will depend upon the threats that governments care to address
- *Set of rigorous engineering methodologies, technologies, and tools* have been identified that are fundamental to building an E2E VIV system

Phase I Outcomes – 2 of 3

- The *security foundations* (both theoretical and practical) of the E2E VIV system have been identified
- A *long-term usability study* has been designed to ensure the E2E VIV election system is usable by all voters

Phase I Outcomes – 3 of 3

- Experts have determined that it is ***technically feasible*** to design, develop, and support an open source E2E VIV system if there is…
  - sufficient political will
  - financial support
  - the right international team is engaged

Additional Findings / Outcomes

- E2E systems built with these cutting-edge technologies are 1/10th the size and complexity of previous products
- Voters and elections officials are interested in verifiability due to the cyber-threats they witness in the media.
- *Usable security is at the crux of the entire solution - more experiments needed to better understand voters*

Usability Study

- Qualitative, interactive usability study conducted with 30 participants
- Study consisted of live use of STAR-Vote prototype as mimic for an E2E VIV system
- Study results include information about the voters thought processes and their reflections about their voting experiences (past and future)

Usability – Some Findings

- Voters tend to intrinsically trust the voting system and election authority
- Very few voters are interested in verifying their votes or the election
- Voters expected the IV experience to be different than traditional elections

Usability Study - Main Subtext

- Internet Voting may offer the opportunity to break away from the "old" voting experience
  - *Flexible:* Vote on your own schedule
  - *Comfortable:* Use your own devices with which you are familiar and comfortable
  - *Location Agnostic:* Vote from home or in early voting centers over days or weeks

Prototype 21st Century Voting Experience

• • •

Maybe voting could be something like this?

E2E VIV Challenges Remain

- Significant-but-achievable research and engineering challenges remain:
  - Cryptographic protocols
  - User interface for usability and accessibility
  - Secure and highly-available deployment
- Main engineering issues focus on high-assurance software engineering for nationally critical systems

Recommendations

- Phase II R&D to implement and experiment with high-assurance E2E VIV variants
- Rigorous analysis of cryptographic scheme
- Determine feasibility of assurance and availability for large-scale elections
- Run large-scale, advanced usability studies
- Design, development, and review must be open to peer-review and the public

In Conclusion….

- Phase I – a great step forward
- Let’s move forward to Phase II

Discussion and Feedback

...

Questions and Comments Welcome

U.S. VOTE FOUNDATION

THE FUTURE OF VOTING

Thank You for Joining Us Today!

Brought to you through the generous support of

DEMOCRACY FUND
OF, BY, AND FOR THE PEOPLE