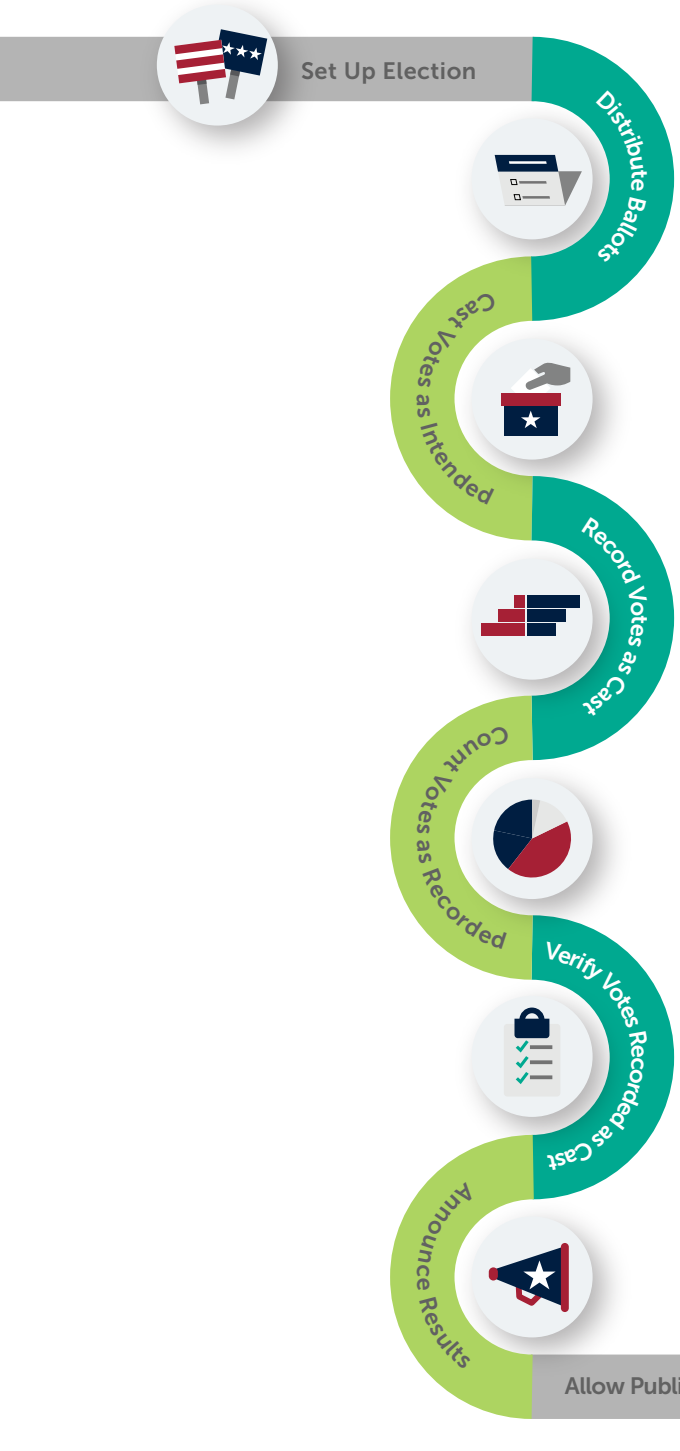


THE FUTURE OF VOTING

END-TO-END VERIFIABLE INTERNET VOTING

SPECIFICATION AND
FEASIBILITY ASSESSMENT STUDY

A PROJECT OF **U.S. VOTE FOUNDATION**
WRITTEN AND PRODUCED BY **GALOIS**

U.S. VOTE FOUNDATION

U.S. VOTE FOUNDATION
SUSAN DZIEDUSZYCKA-SUINAT, PRESIDENT AND CHIEF EXECUTIVE OFFICER
JUDY MURRAY, PH.D.

GALOIS
JOSEPH R. KINIRY, PH.D.
DANIEL M. ZIMMERMAN, PH.D.

DANIEL WAGNER, PH.D.
PHILIP ROBINSON
ADAM FOLTZER
SHPATAR MORINA

July 2015

INTRODUCTION

Societies have conducted elections for thousands of years, but technologies used to cast and tally votes have varied and evolved tremendously over that time. In 2015 many of our essential services have moved online, and some people want elections to follow this trend. Overseas voters are particularly interested in an online approach, as their voting processes can require additional effort and suffer from long delays.

Internet voting systems currently exist, but independent auditing has shown that these systems do not have the level of security and transparency needed for mainstream elections. Security experts advise that end-to-end verifiability—lacking in current systems—is one of the critical features needed to guarantee the integrity, openness, and transparency of election systems.

In this report, we examine the future of voting and the possibility of conducting secure elections online. Specifically, we explore whether End-to-End Verifiable Internet Voting (E2E-VIV) systems are a viable and responsible alternative to traditional election systems.

This project combines the experience and knowledge of a diverse group of experts committed to election integrity. The technical team, comprised of academic and scientific specialists, has long term, proven experience in end-to-end verifiable systems, cryptography, high-assurance systems development, usability, and testing.

INTERNET VOTING TODAY

Internet voting was first proposed over thirty years ago. Since then, many governments and businesses have created Internet voting technologies that have been used to collect millions of votes in public elections.

However, computer scientists, cryptographers, and cybersecurity experts warn that no current Internet voting system is sufficiently secure and reliable for use in public elections.

Part of the problem is that existing systems do not allow third parties to observe the election system and independently verify that the results are correct. In fact, most vendors explicitly forbid such oversight.

SECRET

No existing commercial Internet voting system is open to public review. Independent parties cannot verify that these systems function and count correctly, nor can they audit and verify election results.

INSECURE

Elections for public office are a matter of national security. Researchers have shown that every publicly audited, commercial Internet voting system to date is fundamentally insecure.

NO GUARANTEES

No existing system guarantees voter privacy or the correct election outcomes. Election vendors are rarely held liable for security failures or election disasters.

END-TO-END VERIFIABILITY

An end-to-end verifiable voting system allows voters to:

- check that the system recorded their votes correctly,
- check that the system included their votes in the final tally, and
- count the recorded votes and double-check the announced outcome of the election.

An Internet voting system that is end-to-end verifiable is an **E2E-VIV** system.

The concept of E2E-VIV is decades old. However, most of the required computer science and engineering techniques were impractical or impossible before recent advances. Designing and building an E2E-VIV system in the face of enormous security threats remains a significant challenge.

INTERNET VOTING REQUIREMENTS

Internet voting must be end-to-end verifiable. It must also be secure, usable, and transparent.

SECURE

Security is a critical requirement for Internet voting, and also one of the most challenging. An Internet voting system must guarantee the integrity of election data and keep voters' personal information safe. The system must resist large-scale coordinated attacks, both on its own infrastructure and on individual voters' computers. It must also guarantee vote privacy and allow only eligible voters to vote.

USABLE

Nearly all E2E-VIV protocols designed to date focus on security at the expense of usability. Election officials and voters will not adopt a secure but unusable system. Cryptographers have started to recognize usability as a primary requirement when designing new protocols, and usability is a serious challenge that any future work in this area must address. Any public Internet voting system must be usable and accessible to voters with disabilities.

TRANSPARENT

It is not enough for election results to be correct. To be worthy of public trust, an election process must give voters and observers compelling evidence that allows them to check for themselves that the election result is correct and the election was conducted properly. Open public review of the entire election system and its operation, including all documentation, source code, and system logs, is a critical part of that evidence.

End-to-end verifiability, security, usability, and transparency are only four of many important requirements. This report contains the most complete set of requirements to date that must be satisfied by any Internet voting system used in public elections.

RECOMMENDATIONS

The five key recommendations of this report are:

1. Any public elections conducted over the Internet must be end-to-end verifiable.

2. No Internet voting system of any kind should be used for public elections before end-to-end verifiable in-person voting systems have been widely deployed and experience has been gained from their use.

3. End-to-end verifiable systems must be designed, constructed, verified, certified, operated, and supported according to the most rigorous engineering requirements of mission- and safety-critical systems.

4. E2E-VIV systems must be usable and accessible.

5. Many challenges remain in building a usable, reliable, and secure E2E-VIV system. They must be overcome before using Internet voting for public elections. Research and development efforts toward overcoming those challenges should continue.

It is currently unclear whether it is possible to construct an E2E-VIV system that fulfills the set of requirements contained in this report. Solving the remaining challenges, however, would have enormous impact on the world.

OUTCOMES

The report contains the following:

REQUIREMENTS

We identify a comprehensive set of requirements for an E2E-VIV system.

ARCHITECTURES

We review a variety of ways to build, deploy, and run an E2E-VIV system and the associated engineering issues.

ENGINEERING AND TECHNOLOGY

We present a set of rigorous engineering methodologies, technologies, and tools that are fundamental to building a correct and secure E2E-VIV system.

SECURITY

We lay the foundation for developing a cryptographic system that reflects the ideal functionality of an end-to-end verifiable system, and discuss the technologies that should be used to implement that system.

USABILITY

We present the results of an initial usability study showing that significant effort is needed to develop usable E2E-VIV systems.

CONTENTS

This document is an abridged version, prepared for non-technical audiences. The full report, "THE FUTURE OF VOTING: End-To-End Verifiable Internet Voting", is available from https://www.usvotefoundation.org/E2E-VIV, and contains additional details on cryptographic foundations, architecture, and rigorous software engineering practices.

ACKNOWLEDGMENTS

This project and report would not have been possible without the commitment and tireless hard work of the team at Galois, Inc. Our special acknowledgment and appreciation goes most especially to Joseph Kiniry, who brought his decades of knowledge, skill, experience, and leadership to the project, broadened its scope and led the technical team and writing; and with him, the Galois team members Daniel Zimmerman, Daniel Wagner, Philip Robinson, Adam Foltzer, Shpatar Morina, and Leah Daniels. We are indebted to CEO Rob Wiltbank for the Galois engineering contribution and the long leash he gave to this project.

We would also like to thank the research and technical members of the E2E-VIV Project Team for their contributions to this project from its conception to its completion, with special thanks to Josh Benaloh, Candice Hoke, Keith Instone, David Jefferson, Doug Jones, Aggelos Kiayias, Judy Murray, Ron Rivest, Barbara Simons, and Poorvi Vora.

Equally vital and integral to this report were the reflections, insights and advice from election officials who joined our team, most especially Lori Augino, Judd Choate, Dana Debeauvoir, Mark Earley, Stuart Holmes, Dean Logan, Tammy Patrick, Roman Montoya, and Lois Neuman. We also thank Sean Beggs, Randall Trzeciak, and Andrew Wasser, Carnegie Mellon University, Heinz College Master of Information Systems Management for their support through the CMU ISM Capstone Program.

We are grateful for the generous financial support of the Democracy Fund, as well as their support of collaborative efforts in the realm of civic tech development.

Susan Dzieduszycka-Suinat
President and Chief Executive Officer
U.S. Vote Foundation

For additional information on U.S. Vote Foundation, please visit www.usvotefoundation.org.

For additional information on the Overseas Vote Initiative, please visit www.overseasvote.org.

For additional information on Galois, Inc., please visit www.galois.com.

For additional information on the Democracy Fund, please visit www.democracyfund.org.

CHAPTER 1

INTRODUCTION

Societies have conducted elections for thousands of years, but technologies used to cast and tally votes have varied and evolved tremendously over that time. In 2015 much of our communication takes place online, and many people want elections to follow this trend. Overseas voters are particularly interested in an online approach, as their voting process often requires extraordinary effort.

In March 2013, Overseas Vote Foundation's President and CEO began a discussion with a small group of election integrity advocates to explore what they would do if faced with the challenge of defining an Internet voting system. Despite their concerns about the security of Internet voting efforts to date, they agreed that addressing this challenge is extremely important.

Obstacles to Internet voting range from the risk of hacking to political and policy considerations. Scientists, federal agencies, cybersecurity specialists, and certain organized activists in the U.S. have urged against exposing the ballots of the most powerful nation on Earth to the seemingly endless range of threats that lurk on today's Internet. Election integrity advocates say that secure, tested, certified remote voting systems are not available. Cybersecurity specialists do not consider online ballot return systems secure, and no Internet voting systems have been certified at the time of this writing. Many election administrators have turned to email as a method for ballot transmission, although it does not provide the benefits that a secure, full-featured voting system would. Email is not secure, yet election administrators and voters regularly use it to transmit ballots because no viable alternatives are available.

Existing vendors of Internet voting technologies, whose systems are neither tested nor certified, would like to openly market and sell their systems within the U.S. without meeting resistance from election integrity advocates. A lack of agreement on how to proceed, a long history of mediocre attempts, ongoing animosity among stakeholders, and a general lack of research on the current questions have soured many people on the hope of using the Internet for voting.

Even so, election officials often want to consider Internet-based technologies so they can serve their constituents in modern and efficient ways. In the current economic climate, investment in election innovation is rare. Election officials in the U.S. are stuck with old technology. They devote scarce resources to support outdated voting systems, and they lack the means to certify new ones that would modernize the voting process.

In order to serve all voters, including overseas citizens, military members, and people with disabilities, new and better ways to use technology for voting are needed.

A BETTER TECHNOLOGY

In 1981, security researcher David Chaum published an influential paper describing several applications of *public-key encryption*, a new technology at that time. He suggested a way to use public-key encryption to make a set of ballots anonymous while allowing any observer to verify the accuracy of the tally. This was the first step in the development of *end-to-end verifiable* (E2E-V) election technologies.

Over the following decades, numerous researchers published papers describing and refining election systems that use E2E-V technologies. A unique trait of E2E-V election systems is that they allow voters to verify that their own votes have been accurately recorded. At the same time, they allow any observer to verify that all recorded votes have been accurately counted.

Developers designed many E2E-V election systems for a variety of settings—in-person and remote voting, paper-based and electronic voting, simple majority and instant run-off, etc. Early designs were cumbersome, while more recent E2E-V election systems are easier to use.

Election professionals appreciate the benefits that end-to-end verifiability can bring to election systems. Some are taking early steps toward large-scale deployment of E2E-V election technologies for in-person voting systems. However, it is not yet clear whether the benefits of E2E-V technologies can adequately address the legitimate security concerns inherent to Internet voting.

A PROPOSED STUDY AND OBJECTIVES: THE E2E-VIV PROJECT

Overseas Vote Foundation (OVF),[1] the leading nonpartisan, nonprofit organization dedicated to overseas and military voter participation, developed and wrote the proposal for this project. On December 19, 2013, it was launched as the End-to-End Verifiable Internet Voting: Specification and Feasibility Assessment Study (E2E-VIV Project). The Democracy Fund, a Washington D.C.-based philanthropic organization whose stated objective is to "...invest in organizations working to ensure that our political system is responsive to the priorities of the American public and has the capacity to meet the greatest challenges facing our country", funded the project.

The proposed project had these goals:

- Convene a diverse group of stakeholders to constructively address open questions about how to vote securely online;
- Define a "whole-product" specification for a secure End-to-End Verifiable Internet Voting (E2E-VIV) system;
- Define a set of testing specifications to demonstrate E2E-VIV security;
- Provide a set of guidelines for system usability, accessibility, and testing;
- Produce a report that examines the feasibility of creating a secure E2E-VIV system;
- Include consideration of legal and administrative challenges, and ballot secrecy, privacy, and confidentiality; and
- Release all information produced to the public.

In addition, an unofficial objective of the project was to "change the conversation" about Internet voting by starting a new, constructive dialogue among computer scientists, usability experts, election integrity advocates, and local election officials from key counties around the U.S.

For the purposes of the E2E-VIV project, *end-to-end verifiable* is defined as follows. First, every voter can check that his or her ballot is cast and recorded as he or she intended. Second, anyone can check that the system has accurately tallied all of the recorded ballots.

[1] Overseas Vote Foundation has since been renamed as U.S. Vote Foundation, and their overseas voter program is now referred to as Overseas Vote, an initiative of U.S. Vote Foundation. For the purposes of this project and report, however, we continue to refer to the organization as Overseas Vote Foundation (OVF).

Some concerns about Internet voting are justified. Internet voting takes all the problems with current remote voting systems and adds to them all the security vulnerabilities of the Internet. No participant in this project discounts these concerns or views E2E-V as a magic fix that makes the Internet secure. We believe that E2E-V properties, which apply even when voters use potentially untrusted devices like personal computers and transmit votes over an untrusted medium like the Internet, are important for Internet voting. The E2E-VIV Project does not attempt to make the Internet secure. Instead, it examines whether E2E-V can effectively counter the risks of Internet voting while bringing substantial new benefits not found in today's voting systems.

The E2E-VIV Project also aims to clear up a misunderstanding in the U.S. election community. Our country's scientists are not against technology advancements, nor are they inherently at odds with election officials who seek technology improvements to meet their administrative challenges. Instead, scientists doubt claims of security regarding existing systems that are not publicly tested or vetted. The scientific leaders on this project have often pointed out security vulnerabilities in past systems; however, the E2E-VIV Project has led them to agree that if Internet voting can happen, it must be in a system that takes advantage of end-to-end verifiability and auditability.

SHARED GOALS

Election officials and scientists involved in elections share the same overall goals: that voting systems provide accurate results, protect voters' privacy, are easy to use for all voters, and are robust against both accidental and intentional disruptions. Additionally, election officials must be able to show the public that their voting systems achieve these goals.

This project shows that many scientists care deeply about addressing the needs of election officials as they serve remote voters. These scientists are highly motivated to help when given an opportunity, and they would like to work with election administrators to examine the possibilities in this realm. This project also shows that scientists could improve their understanding of the practical issues that election officials face and find better ways to collaborate and communicate with them to develop technical solutions.

SUCCESS

We hope, that in addition to the concrete outcomes of this project, our research and testing-based approach to examining Internet voting will move beyond the current stalemate and stimulate election development overall. The election industry continues to operate in a traditional way, with only a few vendors able to survive despite demand to move away from outdated, expensive, hardware-oriented solutions. A successful outcome of this project would:

- Help build a specification for a usable, secure E2E-VIV technology;
- Determine the strengths and weaknesses of such a system; and
- Identify reasons to pursue or not pursue this approach.

Ideally, the resulting specification would be:

- Supported by the vast majority of the contributors, including the technical, usability, testing, and research teams;
- Endorsed by the vast majority of the E2E-VIV Project advisory council; and
- Endorsed by the major stakeholders in elections administration as represented by the project's local election officials.

It was acknowledged from the outset that if the project team determined that current techniques were weak and should not be pursued, this would also be an outcome with many useful implications.

The E2E-VIV Project hopes to receive support and endorsement from many members of the election integrity community, as represented by key members of the Election Verification Network, the Verified Voting Foundation and beyond. We intend for the specification to fulfill the following requirements:

INDEPENDENT IMPLEMENTATION The specification must have sufficient detail and clarity that an independent party can implement the election system without having extensive dialogue with project participants.

INDEPENDENT VALIDATION It must be possible for a moderately proficient IT expert to objectively determine, in a reasonable time frame and at reasonable cost, whether a constructed election system fulfills the specification.

EVIDENCE-BASED DECISIONS Every decision made in the crafting of the specification must be objectively justifiable and the evidence for the decision must be traceable.

SCOPE

The original project was limited to system specification and testing only. The project participants did not envision system development in Phase I beyond mock-ups to help test usability. That changed, however, when OVF engaged Galois, Inc. to conduct the technical project management. Galois's management offered to donate engineering time to the project to build "demonstrators" that would be used to prove the concepts of E2E-V and to further examine security and usability. This additional work broadened the scope of the project.[2]

The demonstrators developed using Galois research and development funding are:

- Developed in a completely transparent and public manner within the Galois GitHub Organization;
- Cross-referenced, and thus traceable to and from, all specification aspects (from domain models to behavioral design specifications);
- Replicated into the E2E-VIV GitHub Organization;
- Licensed under either a mainstream Open Source license with a strong community or an alternative license tuned to the elections community.

1.1 PROJECT TEAM

The E2E-VIV Project provided an opportunity to combine the abilities, knowledge, experience, and expertise of a diverse group of technologists, computer scientists, and election officials involved in election integrity. Technical, usability, testing, and local election official sub-teams were created to make communication easier. The project also established an advisory council to open communication with interested members of the election community.

OVF, as the official grantee, was responsible for the overall project conception, proposal development, presentations, communications, management, team recruitment, contractual obligations, public relations, events, and budgeting.

Galois provided the technical and engineering project management, wrote much of and edited the final report, and facilitated the communication and decision-making of the team.[3]

[2] The Galois engineers developed a set of rigorous engineering demonstrators that can be refined to fit into a working election system. Third parties can perform independent verification and validation of these demonstrators.

[3] See the *GaloisInc/e2eviv* GitHub repository at `https://github.com/GaloisInc/e2eviv` to best understand exactly what Galois's contributions are.

1.1.1 TEAM MEMBERS

Project Manager: Susan Dzieduszycka-Suinat, Overseas Vote Foundation

Lead Technical Project Manager: Dr. Joseph R. Kiniry, Galois

Technical Team

- Dr. Josh Benaloh, Senior Cryptographer, Microsoft Research
- Dr. David R. Jefferson, Lawrence Livermore National Laboratory
- Dr. Doug W. Jones, Associate Professor, Department of Computer Science, University of Iowa
- Dr. Aggelos Kiayias, Associate Professor, Computer Science and Engineering, University of Connecticut
- Dr. Olivier Pereira, Professor, Institute of Information and Communication Technologies, Electronics and Applied Mathematics, Ecole Polytechnique de Louvain
- Dr. Poorvi Vora, Associate Professor, Department of Computer Science, The George Washington University
- Dr. David Wagner, Professor, EECS Computer Science Division, University of California Berkeley
- Dr. Dan Wallach, Professor, Department of Computer Science, Rice University

Usability Team

- Keith Instone, User Experience Consultant
- Morgan Miller, Usability Analyst, Experience Lab
- Dr. Judy Murray, Research Consultant

Election Auditing

- Dr. Philip Stark, Professor and Chair of Statistics, University of California Berkeley

Testing Team

- Dr. Duncan Buell, Professor of Computer Science and Engineering, University of South Carolina
- Andrew Regenscheid, Mathematician, National Institute of Standards and Technology

Advisory Council

- Dr. Ben Adida
- Dr. Michael Clarkson, Assistant Professor of Computer Science, The George Washington University
- Dr. J. Alex Halderman, Assistant Professor of Computer Science and Engineering, University of Michigan
- Candice Hoke, Professor of Law, Cleveland State University
- Dr. Ron Rivest, Vannevar Bush Professor of Computer Science, Massachusetts Institute of Technology
- Noel Runyan, Primary Consultant, Personal Data Systems
- Dr. Peter Ryan, Professor in Applied Security, University of Luxembourg
- Dr. Barbara Simons, Research Staff Member, IBM Research (retired)
- John Wack, Voting Systems Standards, National Institute of Standards and Technology
- Dr. Filip Zagorski, Assistant Professor of Computer Science, Wroclaw University of Technology

Local Election Officials

- Lori Augino, Director of Elections, Washington State, Secretary of State

- Rachel Bohman, Former Hennepin County Elections Manager (Minnesota)
- Judd Choate, Director of Elections, Colorado, Secretary of State
- Dana Debeauvoir, Travis County Clerk (Texas)
- Mark Earley, Voting Systems Manager, Leon County (Florida)
- Dean Logan, Los Angeles Registrar-Recorder/County Clerk (California)
- Stuart Holmes, Election Information Systems Supervisor, Office of the Secretary of State (Washington)
- Dr. Lois H. Neuman, Chair, Board of Supervisors of Elections, City of Rockville (Maryland)
- Roman Montoya, Deputy County Clerk, Bernalillo County (New Mexico)
- Tammy Patrick, Senior Advisor to the Democracy Project, Bipartisan Policy Center and Former Federal Compliance Officer Maricopa County (Arizona)

Overseas Vote Foundation Support Team

- Susan Dzieduszycka-Suinat, President and CEO
- Paul McGuire, Legal Counsel and Secretary of the Board
- Richard Vogt, Treasurer and Chief Financial Officer

Galois Team

- Dr. Joseph R. Kiniry, Author and Editor
- Dr. Daniel M. Zimmerman, Author and Editor
- Dr. Daniel Wagner, Chapter Author
- Philip Robinson, Chapter Author
- Adam Foltzer, Chapter Author
- Shpatar Morina, Project Coordination

Capstone Project Team

- Carnegie Mellon University, Heinz College, School of Information Systems & Management; Master of Information Systems Management and Master of Science in Information Security Policy and Management. In early 2014, a Capstone Team was assigned to the project team to assist on the Comparative Analysis of E2E systems.

1.1.2 STAKEHOLDER GROUPS

Although not on the official project team, several communities relevant to the E2E-VIV Project have offered essential input. These communities include:

ELECTION VERIFICATION ADVOCATES Election verification advocates are numerous, well-informed, and strongly connected. They care deeply about election integrity and verifiability. Internet voting is a high-priority issue for many of them.

Election verification advocates tend to be skeptical about Internet voting. This is because several elections vendors have developed Internet voting products that are proprietary, closed-source, and not verifiable. Their products have never had a public audit. Many vendors nonetheless make claims about the security of their products, and election verification advocates reject these claims. Some vendors recommend that elections be outsourced entirely to their own companies—a condition that will never be acceptable to the election verification community, even for an E2E-VIV system.

Some election integrity advocates are in favor of verifiable Internet voting, others are adamantly against Internet voting of any kind, but the bulk of them are undecided. That majority recognizes that significant scientific and engineering challenges must be met to design and develop an Internet voting system. They recognize that the decision to deploy such a system is very much a subjective, political one. In some contexts, such as deciding the winner on a reality TV show, some advocates view using a non-verifiable, outsourced election apparatus as an acceptable choice. However, for government elections of any value, such an option is unacceptable to virtually every advocate.

Being fully transparent with—and listening to the feedback from—the election verification advocate community is mandatory. If the evidence presented in this report does not sway the bulk of that community, the pursuit of any next phase in this project will be contentious.

STANDARDS BODIES Perhaps surprisingly, little national or international election standardization exists. An effort to standardize data interchange formats began about a decade ago and eventually collapsed after agreement on one small standard. This first effort failed for many reasons. Vendors lobby against, and are uninterested in, interoperability. The Election Assistance Commission (EAC) issued Voluntary Voting System Guidelines (VVSG), but these were not geared toward a component-based approach to system design; since devices could not be plugged together, there was little cause for defining interfaces and data file formats. Also, the election research community did not accept that first effort at standardization.

In 2015, the situation changed with the rebirth of the Institute of Electrical and Electronics Engineers (IEEE) 1622 committee and its focus on elections. The IEEE Voting System Standards Committee 1622 (VSSC/1622) creates standards and guidelines around a common data format for election data. The goal is that future election equipment used in U.S. elections and abroad can interoperate more easily. The Voting System Standards Committee intends for their standards and guidelines to be required in future versions of the VVSG.

Many of the top researchers, election advocates, and election officials in the world participate in this committee. Representatives from the major election systems vendors also participate, because they recognize that interoperability will be mandated by future versions of the VVSG.

Standards are critical to any future work on E2E-VIV systems for several reasons. First, given the compositional nature of most E2E-V systems' designs, it is likely that different subsystems will be created and supported by different organizations. Second, in order to enable arbitrary third party verification, clearly defined common data formats must be used. Third, at some point in the future, if E2E-VIV systems are accepted in the mainstream, the EAC must certify them. The EAC, National Institute of Standards and Technology (NIST), and IEEE standards must recognize their core capabilities, subsystems, interfaces, and what constitutes legitimate evidence of correctness and security. A standard means to document these aspects and evidence is necessary to establish a sound, accurate, and expedited certification process.

VENDORS Two types of vendor are relevant to this project: (1) existing vendors of proprietary election systems, and (2) future vendors that support open source election systems.

Existing vendors may be interested in the results of this project, particularly if it moves to a second phase that focuses on the design and development of an open source system. Those that have an existing non-E2E-V Internet voting product (e.g., Scytl, Dominion, and Everyone Counts) could benefit from this work if they take on the tough challenges of verifiability and usability and tackle them accordingly. Any increase in attention on—or any hint of support from the verifiable elections activist community about—Internet voting aligns with their marketing goals.

Vendors can use the requirements contained in this project in various ways. Ideally, they will actively and positively absorb the recommendations. Any investment towards making their commercial systems end-to-end secure and verifiable, as long as there is publicly available evidence of such improvements, would be welcomed by the bulk of the research and activist communities. On the other hand, it is also possible that vendors will simply use these requirements as a checklist, claiming that their systems are E2E-V but providing no evidence. Only time will tell which path each existing vendor chooses to take.

The other type of vendor that is relevant to this project, supporting open source election systems, does not yet exist. We expect such commercial support organizations to emerge to support any E2E-VIV system that occurs as a result of this project. These organizations would not need to have expertise in the underlying cryptography, formal methods, or usability and accessibility. They would rely on the high-assurance development method described in this report, which produces validation and verification artifacts that generate evidence of their correctness and security properties. Additionally, modern formal system specification languages support traceability from requirements to evidence.

Any future mission-critical E2E-VIV system will be robust to any integration, customization, or evolution work by these vendors. That is, systems developed according to the requirements and recommendations in this report cannot be accidentally or purposefully broken without third parties detecting a certification failure. Only these complete, consistent, traceable, evidence-generating artifacts make it possible for such new support vendors to emerge.

HACKERS AND HACKTIVISTS Hackers and election hacktivists are an important audience for this project. Hackers, constructively or destructively, help make open source systems more secure. Hacktivists catalyze movements of like-minded technical individuals. Across the world, their attention has brought to light the flaws of insecure and incorrect electronic voting systems.

Within these sub-communities, it is an undisputed precept that the design and development of a secure system used for public good must be open to critique and improvements from the public. Leveraging that attention is especially valuable for nationally critical systems like public elections. Consequently, direct engagement with these groups, while potentially tempestuous at times, is wise and will have many benefits.

ELECTION OFFICIALS Local elections officials (LEOs) are the core stakeholders in the design and deployment of E2E-VIV technologies. There are over 10,000 election jurisdictions in the United States. That means there are over 10,000 different ways that elections can be run. Smoothly integrating with existing election processes is important. Basic issues like common data formats are simple technical challenges that have straightforward, though potentially politically delicate, solutions.

The enormous variety of technologies, large and small, at the federal, state, and local levels make deploying any new election technology difficult. Traditional IT practices for the design, development, and maintenance of election software cannot work in this setting. No vendor can support 10,000 variants of a single code base to satisfy 10,000 clients, each with slightly different requirements. Some of the software engineering recommendations in this report, particularly those that touch upon feature modeling and software product lines, are directly relevant to the elections setting.

More subtle challenges, such as ensuring that election officials who are uncomfortable with technology can deploy and support a E2E-VIV system for their overseas, military or disabled voters, have little to do with technical solutions. These problems and solutions have more social, political, and psychological roots, and thus require soft solutions.

Tools such as documentation and tutorials, webcasts and screencasts, reports, and demonstration software have a limited reach. Open Source projects often have friendly online forums to welcome and guide newcomers, as well as regularly scheduled and community-organized developer and user conferences. We hope that kind of open, active and supportive community will evolve around E2E-VIV.

VOTERS Despite the importance of all of the aforementioned stakeholders, the most important stakeholders—the ones that hold veto power over the wide-scale deployment of E2E-VIV technologies—are the voters. Many voters want flexible, comfortable voting that is not tied to a particular polling place. However, they may not realize the implications of this desire, particularly with regard to security and privacy. Educating voters about the challenges of Internet voting is important, but it is not possible to make every voter aware of the usefulness of, and critical need for, E2E-V election systems.

Based upon early usability studies of E2E-V election systems, we can expect only a small fraction of voters to understand and use the verifiability features of E2E-VIV systems, even if the user experience of these systems is well-designed. Voters' trust in their election apparatus, and how their voting experience affects their trust in their government, is paramount. Consequently, changes in elections that may impact trust are difficult to make.

Voters are sensitive to changes that are bluntly visible, like electronic pollbooks and electronic voting machines. The past decade, with its introduction of electronic voting machines and the subsequent outcry for a return to a "paper trail", has taught some voters not to trust election technology. A vocal minority may misunderstand changes and be hostile or alarmed. Public reactions are unpredictable, as evidenced by the introduction of voter ID laws across the U.S. and the alarm raised by the use of email for ballot return (even in extraordinary circumstances).

Finally, and perhaps most critically, there is a delicate balance between comprehensibility and security—the twin challenges of digital election systems. People view paper-based elections as transparent and comprehensible. Digital elections have lost those properties. However, in the right circumstances, digital elections benefit from tabulation efficiency, decreases in residual vote count, and facilitation of independent voting for voters with disabilities. Internet voting shifts the balance towards voter convenience, but with a significant loss in general comprehensibility; to the first significant digit, the percentage of voters that are cryptographers is zero.

Choosing to design and deploy an election system that is end-to-end secure and based upon cryptographic principles is a policy decision that firmly delegates trust to a precious few: on the front lines, the elected officials and the politicians voting for modernization, and behind the scenes, the cryptographers, scientists, and engineers responsible for the system's design, development, validation, and verification. Those few assume an enormous responsibility.

1.2 METHODOLOGY

The technical project management of this first phase of the E2E-VIV project was organized in a workflow that focused on delivering an evidence-based report and its complementary Open Source technical artifacts. The methodology is summarized as follows:

- Absorb all input from team members.
- Read all literature on Internet voting.
- Write baseline business and technical requirements and solicit feedback from technical team.
- Write personas as a foundation for user experience studies.
- Interview local election officials based upon requirements, personas, and their current elections framing.
- Outline report and solicit text and reflections from team members.
- Reflect upon the latest advances in cryptography for E2E-VIV.
- Reflect upon the latest advances for reasoning about cryptographic algorithms, protocols, and implementations.
- Craft a parameterized architecture space that reflects underlying requirements and standard cryptographic protocols.
- Integrate all team member text and reflections and develop a final report table of contents.
- Solicit more text and reflections from team members based upon the final report table of contents.
- Write the remaining unwritten chapters.
- Solicit input from all team members on Part 1.
- Solicit input from technical team members on Part 2.

- Solicit initial reflections from technical team members on the feasibility of Part 2 potential recommendations.
- Gather all input from team members and capture it in appendices, citations, and footnotes.
- Identify useful illustrations and figures for report and communicate them to the illustrator.
- Copy-edit, lay out, polish, and release the report.
- Clean up and make public the GitHub repository that includes the report and all associated artifacts of the project.

The outcomes of this process are this report and the reflections of a body of experts in the domain of verifiable elections, as summarized in the following section.

1.3 OUTCOMES

This project has produced a high-level system specification in the form of a set of business and technical requirements. Accompanying that set of requirements are recommendations about the underlying means by which those requirements should be fulfilled.

These recommendations focus on the three dimensions necessary to fulfill the strenuous requirements of any E2E-V system: cryptography, architecture, and engineering. The cryptographic foundation is a formal framework in which to evaluate E2E-V cryptographic protocols. The architecture specification is a formal description of an architecture space, defined by several parameters, in which solutions can be designed, built, and evaluated. Finally, the rigorous engineering necessary to create a high-assurance E2E-VIV product is specified via a recommended software engineering process, methodology, and set of technologies. Used properly, these can fulfill the security and technical requirements while generating the necessary evidence to substantiate that the system is fit-for-purpose.

Fulfilling the usability and security requirements would not be sufficient for a positive assessment by the project team. A full system specification that is usable and secure may, for example, be too expensive to build, too difficult to deploy and manage, or mandate too much expertise from election officials to operate. In the end, social non-functional requirements may trump technical functional requirements.

A positive assessment by the majority of the technical team would mean they agree that the specified election system meets all of the requirements set forth by the charter of the group and that, eventually, an open source E2E-VIV system could be developed, tested, and potentially deployed.

A negative assessment by the majority of the technical team would mean they do not agree that the specified election system meets all of the requirements set forth by the charter of the group, and that designing a usable and secure Internet voting system is still an open scientific, not engineering, challenge.

The final assessment of the team is found in Chapter 9.

1.3.1 USER INTERFACE DESIGN

The user interface (UI) of the E2E-VIV election system is a critical factor in its acceptance. The system must be simultaneously usable, accessible, and secure. Consequently, a detailed UI design informed by user experience (UX) and accessibility testing is a mandatory component of a future detailed system specification.

This report's system specification is focused on high-level requirements for any E2E-V election system (Internet-based or not). As such, several requirements focus on UI and UX and stipulate the necessary framing for UI/UX designs and studies.

Usability and accessibility studies and testing are key components of this report, and the outcome of this first study is meant to inform the UI design of any future E2E-VIV systems. As such, most of the effort relating to UI and UX within the project has focused on developing a technical infrastructure and complementary process that allows efficient definition and execution of usability and accessibility studies.

Researchers conducted an initial usability study, gathering qualitative feedback from several dozen voters. The results of that study, whose full report is included in a separate document [42], led to three conclusions about voters' attitudes regarding Internet voting.

1. *Voters trust the voting system and their election officials.* This trust is both a blessing and a curse. It is a blessing because it means that election officials and the government are working with voters that have a positive attitude; their trust can only be lost and does not need to be won. But it is also a curse because it means that voters will trust Internet voting systems that have no transparency, end-to-end security, or verifiability. As such, this opens the door for vendors to sell their technology and gather naïve voter feedback as "evidence" that their systems are fit-for-purpose for modern public elections, even if that is not the case.
2. *Voters are not interested in learning about verifiability or verification.* Fortunately, only a small fraction of voters needs to actually verify their votes for most E2E-VIV election schemes to generate sufficient independent evidence that the election outcome is correct. The requirements and recommendations reflect this low level of voter interest in verification and suggest several means by which the threshold for election verification may, nevertheless, always be achieved.
3. *Voters expect the Internet voting experience to be somehow different from a traditional voting experience.* Voters expect modern, rich online experiences akin to those they know from popular commercial websites and smart phone applications. This raised expectation opens the door for novel experimentation to develop a "21st Century" voter experience.

CHAPTER 2

REMOTE VOTING

2.1 RATIONALE

Remote voting is becoming increasingly common, necessitated by the growing and diverse needs of voters. It is used to enable overseas citizens and military personnel to participate in elections, reduce access related discrimination domestically, and decrease expensive administrative overhead of polling locations.

In the United States, fewer than 5% of ballots cast in general elections during the 1980s were cast before Election Day. By the 2012 general election, 31% of all ballots were cast early, and 17% were cast by mail. The states of Washington, Oregon, and most recently Colorado have entirely switched over to all-mail voting. For an election system to fully enfranchise the electorate, it must treat remote voting as a first-class capability rather than as a backup system with second-class effectiveness, speed, security, and integrity.

2.1.1 ACCESSIBILITY

According to the International Center for Disability Information and the National Institute on Disability and Rehabilitation Research, 20% of Americans live with disabilities. The Voting Accessibility for the Elderly and Handicapped Act of 1984 mandates that any person with a disability may vote remotely without having to present medical documentation, reducing the barriers to remote voting for those with accessibility needs.

2.1.2 OVERSEAS AND MILITARY VOTERS

In 1986, Congress enacted the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) to address the needs of citizens in the uniformed services, merchant marines, and other overseas civilians. UOCAVA mandates that these overseas and military voters (UOCAVA voters) be able to register and vote remotely in federal elections. It is difficult to calculate an exact number of UOCAVA eligible voters. According to estimates from the United States Elections Project [40], there were 5,127,418 UOCAVA eligible voters for the 2012 U.S. general election and 5,345,814 for the 2014 U.S. general election.

2.1.3 DOMESTIC ABSENTEE

Domestic absentee voters are those who cast their votes by mail because they are unable, or do not want, to be present at polling locations on Election Day; this excludes UOCAVA voters and voters in states that vote exclusively by mail. According to the Election Administration and Voting Survey [20] published by the U.S. Election Assistance Commission, domestic absentee voters cast 16.6% of the ballots in the 2012 U.S. general election and 17.5% of the ballots in the 2014 U.S. general election. As of this writing 27 states allow voters to apply for an absentee ballot without providing a justification, known as "no-excuse absentee voting".

2.1.4 EXPECTATIONS

In 1952, a study by the American Political Science Association defined ten voting rights necessary for members of the armed services [9]. Although initially defined for military voters, these rights have served as the basis for defining the expectations of all remote voters through UOCAVA and other subsequent legislation. Among these rights are:

1. To vote without registering in person;
2. To vote without paying a poll tax or having to meet unreasonable requirements;
3. To use the Federal Postcard Application[1] both to register and to request a ballot, rather than having to use state-specific paperwork;
4. To receive ballots for primary and general elections in time to vote;
5. To be protected in the free exercise of their voting rights; and
6. To receive essential information needed to vote.

These rights first found their way into law in the Federal Voting Assistance Act of 1955 (FVAA) but, due to partisan struggles, the rights were watered down from requirements into recommendations; this left most of the decisions about final implementation to the states. Over time, subsequent legislation has strengthened these recommendations into guarantees and requirements and has expanded rights to include participation by non-English speakers and people with disabilities.

2.2 HISTORY

2.2.1 ARMED FORCES VOTING

Before the American Civil War, U.S. citizens primarily voted in their places of residence and many states legally barred the casting of votes from outside state borders. There was little effort from any state to accommodate absentee voting. In 1864, however, the Civil War displaced soldiers from their residences and Lincoln's re-election was at risk. With much lobbying on behalf of the Republican Party (and opposition from the Democratic Party), nineteen Union states adopted absentee voting procedures for military voters in time for the election. Since the motivation for passing these laws was to secure Lincoln's re-election rather than permanently expand voting access, many states treated absentee military voter laws as temporary and repealed them after the war.

[1] Federal Postcard Application is the Department of Defense name for the official UOCAVA voter registration and absentee ballot request form.

For the 1918 midterm elections, the U.S. War Department decided that it was not ready to support the military vote; the Department prohibited individual states from canvassing overseas soldiers serving in World War I. World War II inspired another push for the military vote in hopes of supporting the re-election of the presidential incumbent. This prompted the Soldier Voting Act (1942). Although it was passed too late for the 1942 midterm elections, this law gave military personnel absentee voting rights for federal elections during times of war without being required to pay a voting tax or postage costs. The act has continuing significance: it stated that all overseas voting would be regulated at the federal level and implemented at the state level, a structure that continues to this day. By 1944, partisan politics led to the weakening of the state mandate from a requirement to a recommendation, leading to a 29.1% turnout rate vs. the 60% domestic turnout rate [52].

2.2.2 REMOTE CIVILIAN VOTING

Progress for civilian absentee voters lagged behind progress for military voters. In 1896, states began to introduce civilian absentee voting legislation. By 1924, only three states had no absentee voting legislation. State laws, however, were a confusing and inconsistent patchwork that limited absentee turnout. Major progress for civilian absentee voters would only come with legislation motivated primarily by military voters such as the FVAA.

In the 1960s, lobbying from overseas civilian groups led to amendments to the FVAA. This effort expanded the number of civilians covered by the law, though the amendments were once again voluntary recommendations to the states. As lobbying pressure increased further, the Overseas Citizens Voting Rights Act (OCVRA) passed in 1974. OCVRA was the first law to guarantee, rather than only recommend, absentee voting rights for overseas civilians.

In 1986, legislators passed UOCAVA, which combined and replaced FVAA and OCVRA. UOCAVA made the rights recommended by the previous acts into requirements for both military and overseas civilian voters.

2.2.3 DISABLED CIVILIAN VOTING

The Voting Rights Act (VRA) of 1965 was the first legislation to allow voters who require assistance to vote—because of blindness, disability, or inability to read or write—to receive help from a person of their choice.

The Voting Accessibility for the Elderly and Handicapped Act of 1984 (VAEHA) improved access for disabled and elderly individuals. Like FVAA and OCVRA, VAEHA did not specify standards of access; individual states set their own standards. VAEHA also limited the disabled voters group to those with *physical disabilities*. It did, however, mandate that "no notarization of medical certification shall be required of a voter with a disability with respect to an absentee ballot or application for such ballot."

The 1990 Americans with Disabilities Act (ADA) requires that people with disabilities have access to basic public services, including the right to vote. ADA does not strictly require that polling locations are accessible, however it did extend the definition of disability to

> "a person who has a physical or mental impairment that substantially limits one or more major life activities, a person who has a history or record of such an impairment, or a person who is perceived by others as having such an impairment."

Over the years, legislators have passed several federal laws to protect voting rights of disabled citizens. The majority of these laws have struggled to clearly define a representative range of disabilities. The laws often focus on in-person access to physical polling locations, which is expensive for states to implement. State-defined policies often ignore rights to voting privacy, and exclude people who have multiple disabilities because technologies that may help them vote are not yet available.

2.2.4 MODERN REMOTE VOTING

In 2002, Congress passed the Help America Vote Act (HAVA) in response to problems found in gathering, counting, and auditing ballots in the 2000 presidential election. HAVA requires that all polling places in elections for federal office anywhere in the United States have at least one voting system capable of assisting disabled voters. This requirement addresses some accessibility concerns.

HAVA was also a response to the large number of rejected ballots in the 2000 election and an inability to sufficiently audit ballots. HAVA recommends that election systems produce a Verifiable Voter Paper Audit Trail (VVPAT) while preserving the privacy of the voter and the secrecy of the cast ballot. HAVA also created the United States Election Assistance Commission (EAC) to oversee the development of new voting machine standards. The National Institute of Standards and Technology (NIST) released the Voluntary Voting System Guidelines (VVSG) to aid in this transition.

The Military and Overseas Voter Empowerment Act of 2009 (MOVE) addresses barriers to overseas voter participation, and specifically attempts to reduce the number of ballots that are not counted due to late receipt. MOVE requires states to send absentee ballots at least 45 days before Election Day, make all registration material and blank ballots available electronically, and remove notarization requirements on voting applications and ballots.

Because state governments enforce existing voting regulations, these regulations are hampered by local political attitudes. In 2010, the Uniform Law Commission oversaw drafting of the Uniform Military Services and Overseas Civilian Absentee Voters Act (UMOVA). UMOVA is designed to identify and standardize the important protections and benefits found in federal legislation like UOCAVA and MOVE in state and local elections. As of April 2015, fourteen states and the District of Columbia have enacted UMOVA.

2.3 SHORTCOMINGS OF CURRENT PRACTICE

Despite years of progressively stronger legislation addressing the needs of remote voters, many shortcomings still exist in current election practices. The topics listed below draw from specific concerns that negatively affect remote voting participants.

2.3.1 USE OF COMMUNICATION TECHNOLOGIES

The majority of remote voting takes place via postal mail, which has many inherent faults that affect the voting process. The 2008 Post-Election UOCAVA Survey Report and Analysis found that voting boards did not count 52% of attempted UOCAVA votes due to problems in the mail delivery process. In addition, maintaining correct voter registration information for military voters and others who frequently change addresses while abroad is expensive and prone to error.

To address differences between states' absentee registration and voting practices, the Federal Voting Assistance Program (FVAP) provides a Voting Assistance Guide (VAG) to support UOCAVA voter registration and ballot request. The VAG supports military Voting Action Officers who assist their units with voter registration instructions.

Since MOVE was passed in 2009, online registration has expanded significantly. OVF and the FVAP offer online voter services to UOCAVA voters through their websites, as do many states and counties. Online blank ballot transmission is becoming routine, and email communications between election officials and voters are flourishing.

Unfortunately, the problem of late ballot receipt and rejection has not been solved.

2.3.2 ACCESSIBILITY AND USABILITY

In 2007, 20% of Americans with disabilities said they were unable to vote in a presidential or congressional election due to difficulty getting to the polls or barriers at polling locations [48]. The voting technologies used, and the physical locations of polling places, often cause such problems. In the 2000 presidential election, 56% of randomly sampled polling places in the United States had at least one barrier to disabled voters [43].

Voters with disabilities often forfeit privacy in order to have someone help them with in-person voting. Polling locations often lack technology that can help, and the assistive technology that is available is often too difficult for voters and poll workers to use. Remote voting still presents obstacles: those with dexterity impairments often have problems handling and marking paper absentee ballots.

2.3.3 AUDITING

Although voter fraud is fairly uncommon, it is a major concern in a bipartisan system. Voter fraud is very difficult to detect without reducing turnout or disenfranchising legitimate voters. Policies intended to reduce fraud or protect identities, such as increasingly prevalent and strict voter ID requirements, often lead to a higher rate of rejected ballots. This is the case even for remote voters. In the 2012 general election, voting boards rejected over 20% of absentee ballots due to non-matching signatures or insufficient identification [20].

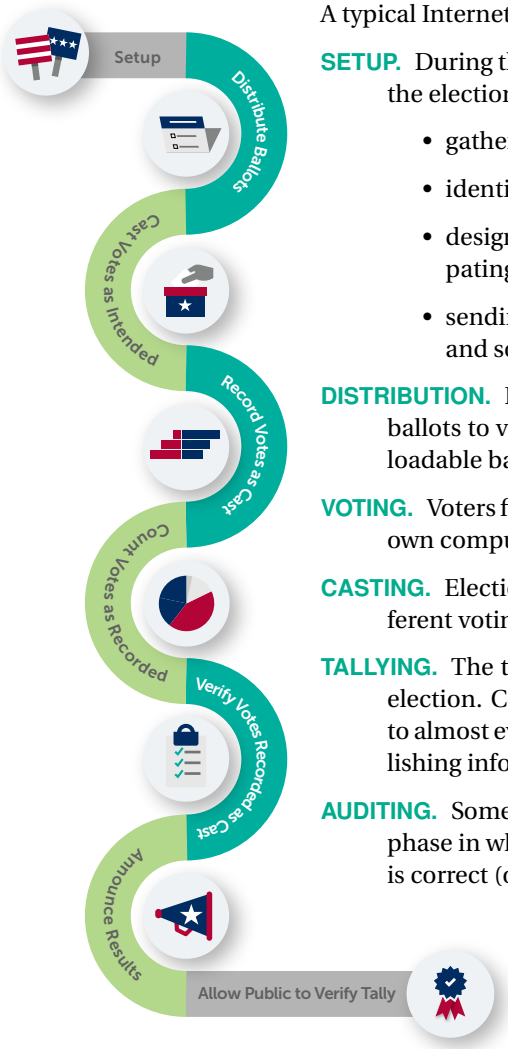
2.3.4 VOTER PRIVACY

A fair voting system must ensure voter privacy. Privacy promotes voter independence and helps prevent voter coercion and vote buying. Most remote voting practices require that voters forfeit independence or privacy because election officials cannot enforce privacy when voting takes place outside of polling locations. Several states require voters to sign a voter privacy waiver when casting a remote ballot [53].

CHAPTER 3

E2E-VIV EXPLAINED

3.1 ELECTION PROCESS AND GOALS



A typical Internet voting election process has six phases:

SETUP. During the setup phase, election officials gather information needed to run the election. This includes:

- gathering registration information for all voters;
- identifying the issues and races that will be voted on;
- designing ballots, often in multiple languages, for all precincts participating in the election;
- sending instructions and other information about the election to voters; and so on.

DISTRIBUTION. Different voting systems use different mechanisms to distribute ballots to voters, such as postal mail, email, or a website that provides downloadable ballots.

VOTING. Voters fill out their ballots, often with the help of software installed on their own computers.

CASTING. Election officials receive the completed ballots. As with distribution, different voting systems use different ballot casting mechanisms.

TALLYING. The tallying phase includes the remainder of the tasks that finalize the election. Counting votes and announcing the election outcome are common to almost every election system, though some include other tasks such as publishing information needed for audits.

AUDITING. Some elections will inevitably be disputed. In such cases, there is a final phase in which interested parties look for evidence that the election outcome is correct (or incorrect).

One major concern for Internet voting involves ballot integrity during the distribution, voting, and casting phases. For the election outcome to be correct, it is important that:

- the blank ballot that is received by and displayed to the voter match the ballot created and sent by the election officials;
- the computer used to fill out the ballot faithfully reports the intention of the voter; and
- the filled out ballot received by the election officials is the same as it was when the voter sent it.

Typical Internet communications involve not just the computers owned by the two parties communicating, but also many intermediary computers controlled by neither party. For example, an email you send from anywhere in the world will travel through multiple servers on its way to its destination. At any point, one of these servers could intercept and modify the email without your knowledge. A good election system needs to account for this, making it impossible for these intermediaries to intercept ballots for viewing or modification during transit.

Another concern is that most voters are not system administration experts, and many of their computers are compromised by malware. A compromised computer may corrupt the voting phase: even if the voter receives an unaltered ballot, malware may change the way the ballot is displayed or the way the vote is recorded before casting the ballot. It can be difficult to design a system that can resist this kind of attack without significantly reducing the usability of the system. Some systems, referred to as dual (or triple) channel systems, use alternative distribution mechanisms as cross-checks. For example, election officials may send a code by postal mail that a voter can use to check that a displayed ballot is correct.

As much as possible, Internet voting should be private and anonymous. It is essential that voters are free to vote the way they choose, and do not feel pressured to vote for a particular candidate or vote a particular way on any issue. The fewer people who know or can find out how a voter voted, the more comfortable the voter can feel about privacy.

At the same time, election systems must only record votes from people who are registered to vote, and must only record one vote from each voter. Election systems must balance the need to keep votes anonymous against the need to ensure that a vote is coming from somebody who should to be able to vote.

One popular approach to this problem in existing systems is to require that each vote be tied to the voter who cast it long enough to decide whether to include the vote in the later tally or not. After it is decided to include the vote, the system records the vote and deletes the information about who cast it. This approach can work; however, audits of systems that take this approach have shown that it is easy to accidentally retain the connection between votes and voters longer than intended. This makes information much more widely visible than intended. It would be better if voters could be confident that the system does not store any connections between their votes and their identities. To accomplish this, the information a voter returns during the ballot casting phase must not include any personally identifying material.

This is a subtle, but crucial, distinction. The overall objective is for Internet voting systems to be correct, private, secure, and so forth. It is important for the people who develop these systems to verify that they are correct and take an active role in seeking out and eliminating defects in the system. However, verifiable Internet voting goes even farther: the system must be *visibly* correct. That is, voters using the system must be able to *check* that it is behaving correctly, without trusting that the system has no bugs or trusting that the system's behavior has not been influenced by third parties. It is especially difficult to prove to voters that their personal information has been deleted in order to protect their privacy, so voters may not want to provide their information in the first place.

This is why it is critical that an Internet voting system not only be correct, but *verifiably* correct. Verifiability is one of the central concerns of Internet voting, and is a critical part of the defense against the software bugs, security vulnerabilities, and sophisticated cybercrimes that history tells us are sure to occur.

The tallying process provides a particularly good example of the difference between correctness and verifiability. Voters certainly want the election system to count the votes correctly, but the goal of verifiability is to provide some *evidence* to voters that the election outcome is correct. Different systems attempt this in different ways. For example, they may allow voters to check that:

- their vote was included in the election outcome;
- the system is recording the content of their votes correctly; or
- the number of people that voted for a given candidate is accurately calculated (this must be proven without revealing any of the individual votes).

Meeting these verification objectives without violating anonymity and privacy is a balancing act. Each of these individual objectives contribute to a single top-level goal: *end-to-end verifiability*. "End-to-end" means that the whole election process produces a result that matches the intentions of the voters.

The verification objectives can be summarized with the catchphrase, "Cast as intended; recorded as cast; and counted as recorded."

- "Cast as intended" is the demand that casting use secure communications and other mechanisms to ensure that malware and outsiders cannot change the vote.
- "Recorded as cast" is the demand that the election system itself correctly interprets a vote.
- "Counted as recorded" is the demand that the tallying process be accurate.

These demands are subject not only to correctness but also to verifiability, so that voters can believe these properties hold even if they suspect that the systems, or the election officials, are corrupt.

3.2 SHORTCOMINGS AND EXPECTATIONS OF E2E-VIV

As discussed in Chapter 2, several difficulties exist with current voting processes:

- voters with disabilities cannot vote unassisted;
- communication channels with remote voters are often slow and unreliable;
- vote tallying is labor-intensive and error-prone;
- election audits are costly; and
- there is little visibility into the election process, so voters (and, in some cases, even auditors) must trust the reports of election officials and voting hardware vendors on election outcomes and processes.

Internet voting may be able to alleviate some of these concerns. Voters with disabilities could potentially use their own familiar hardware, such as Braille displays, screen readers, sip-and-puff input devices, and others, to participate in the election. Internet communications are traditionally speedy (taking seconds rather than weeks) and relatively robust compared to overseas postal mail. In most systems, tallying is automated and fast. Auditing can still be a challenge, though it is expected that verifiable systems can make elections more transparent for this purpose. However, implementation of Internet voting has its own challenges. A system that properly addresses privacy and security concerns may be too complex to use and maintain or too costly to deploy.

3.3 E2E-VIV IN PRACTICE

Several practical voting systems have been developed based on the principles of E2E-VIV. This section describes some systems that communities have used in real elections or pilot tests.

3.3.1 RIES

RIES, the Rijnland Internet Election System [32], was first used in 2004 to support elections to the Rijnland water management board. RIES supplemented the system of postal voting already in use. Election officials used a later version of RIES to allow expatriate voters to participate in the Dutch parliamentary elections [29].

Before a RIES election, credentials—in the form of a very long number—and instructions are sent by postal mail to every voter.

During the election, each voter logs into the election website. The website includes a voting application written in JavaScript; the voting application is a "client-side" application, which means that it runs on the voter's computer and not on the election server. The client-side application processes the voter's authorization code and the public ID of the candidate to create an encrypted vote. The encrypted vote is then placed on a public online "bulletin board" that serves as a ballot box.

At the close of the polls, the election authority releases the final vote tallies along with a codebook containing the encryptions of all valid credentials and all candidate IDs.

The algorithms and protocols used by RIES are public, and each voter has access to all of the inputs and outputs. In principle, each voter may check the computations. This level of verifiability is weaker than the desired individual verifiability of E2E-VIV, but is nonetheless far stronger than conventional voting systems.

In 2006, the Organization for Security and Co-operation in Europe (OSCE) sent an election assessment team to observe the use of RIES. Their report [44] stated that they could not observe many critical security features of the system, and therefore could not be certain of their effectiveness. In 2008, the Eindhoven Institute for the Protection of Systems and Information (EiPSI) revealed several weaknesses in RIES [33]:

- the voter self-check procedure is quite complicated;
- the two-channel (mail and Internet) voting makes the system less transparent;
- too much power is given to the election administrator and the system's Internet host;
- issues arise when modifying the codebook due to a revoked ballot; and
- realistic ways to forge votes via cryptographic means (in particular, using hash collisions) exist.

One of the more important lessons learned through RIES is that when voter authorizations are distributed far in advance of the election, a mechanism must be provided that allows voters to obtain replacement credentials and invalidate lost credentials. This mechanism adds significant complexity to the system, and is a source of some of the problems reported in the OSCE and EiPSI reports.

Another feature of RIES, which has significant tradeoffs, is the ability to perform testing during the election: pre-invalidated test ballots are deliberately added to the bulletin board in order to test the network path from selected Internet clients to the server. While such testing can, in principle, increase confidence in the election integrity, in practice it opens the system to spoofing and denial of service[1] attacks. Moreover, the RIES implementation is aware when it is processing test ballots rather than real ballots, and all of the test ballots are typically voted identically from the same computer. This significantly limits the confidence provided by such testing, at the expense of increased system vulnerability.

Because of these critical reports, election officials discontinued plans to use RIES in the 2008 Dutch parliamentary elections, and the Netherlands banned Internet voting.

[1] A *spoofing* attack deceives the target into believing that an Internet communication came from somewhere other than its actual source. A *denial of service* (DoS) attack is an attempt to make an Internet server unavailable to its intended users.

3.3.2 PRÊT À VOTER

In 2007, the University of Surrey in the U.K. attempted to use the Prêt à Voter system [12, 16] in a student election [10]. This attempt was stopped prematurely, due to system malfunctions and an inability to open polling at all polling stations on time. The failure illustrated many of the pitfalls of adapting a research system to an actual election, such as a short timetable, a lack of clear requirements, and the need for rigorous implementation practices.

Prêt à Voter uses two-part paper ballots. Candidate names appear on one part and voting targets—the areas that voters must mark to cast their votes—appear with a ballot ID number or barcode on the other part. Typically, the two parts are printed as a single sheet with a perforation to divide the sheet after voting.

From the voter's perspective, the order of the candidate names on the ballot is random. The voter makes a mark next to the candidate name she chooses, separates the two parts of the ballot, and destroys the part containing the candidate names. She may take a copy of the voted part home for later verification.

For tabulation, a cryptographically secure mapping exists from the ballot ID numbers to the apparently-random orderings of the candidates. The system uses this mapping to decode the cast ballots into readable ballots with candidate names, while removing the associations between ballots and their ID numbers. The decoded ballots are then posted to a public online bulletin board.

Unvoted ballots may be audited before, during and after the election to ensure that the decoding of cast ballots is being correctly performed. Randomly selected stages in the decoding can be challenged to prove the integrity of the count, and any interested party can easily count the decoded ballots for verification.

Individuals may also search for their voted ballot IDs on the bulletin board. This reveals the positions that were marked on that ballot but, crucially, does not show the corresponding candidate names. A voter can verify that the positions she marked at the polling place were correctly recorded by the system, but because she no longer has the part of the ballot linking candidate names to ballot positions, she cannot prove to anyone else how she voted.

3.3.3 PUNCHSCAN

Punchscan [45, 46] was used for the graduate student association elections of the University of Ottawa in 2007 [25]. It is likely the first E2E voting system with ballot privacy used in a binding election.

The election experience for a Punchscan voter is very similar to that of Prêt à Voter. Punchscan also uses a two-part paper ballot, but the two parts are overlaid one atop the other. The top part has candidate names and candidate numbers (or letters), and the bottom part has numbered (or lettered) voting targets; both parts have an identical serial number. The voting targets on the bottom part are visible through holes punched in the top part. The order of the voting targets for each race appears random to the voter.

The voter casts a vote by marking a choice with a bingo dauber—a thick marker used to fill in circles on bingo cards— and the two halves are separated. Either side can be cast as a ballot, since the bingo dauber marks both: one through the hole and the other around it. The uncast side is destroyed, and the voter may retain a copy of the cast side.

Anybody may inspect the public record of any cast ballot, exactly as with Prêt à Voter; this allows voters to verify that their receipts match the public record. It does not matter which half of the ballot a voter retains, since neither half by itself contains the necessary information to determine the vote. Like Prêt à Voter, Punchscan uses a cryptographically secure mapping from the ballot serial numbers to the apparently-random orderings of the candidate voting positions to decode the ballots for counting. Individual ballots may be audited to ensure that the decoding process is carried out correctly.

3.3.4 SCANTEGRITY II

Scantegrity II (Invisible Ink) [18, 19] was used in the Takoma Park, Maryland municipal elections in 2009 [14]. It was also used in 2011 for in-person voting, along with Remotegrity (Section 3.3.5) for absentee voting. The 2009 Takoma Park election was the first use of an E2E-V system with ballot privacy in binding governmental elections.

Before the election, a *random seed* is generated and shared among election officials. It is very difficult to generate truly random sequences of numbers, so computers use programs called *pseudorandom number generators* to generate sequences of numbers that appear random. Pseudorandom number generators use data called a random seed when they start generating a sequence; every time the same generator is started with the same random seed, it generates the same sequence. The selection of good random seeds is very important in secure computing systems.

The sharing of the random seed is done using a *secret sharing scheme*. In a secret sharing scheme, a computer "splits" a piece of secret information—in this case, a random seed—into multiple parts and distributes these parts to multiple people. Combining some required number of the parts—this could be all the parts, or some smaller number, depending on the secret sharing scheme—reveals the secret information, but combining fewer than the required number of parts reveals nothing.

Using the random seed, the system generates a three-letter alphanumeric code for each choice on each printed ballot. It also generates additional tables so that interested parties can later confirm that the system computed the tally correctly.

During the election, the voter experience is nearly identical to that of conventional optical-scan paper ballots. When a voter marks a choice, the ink in the pen reacts with invisible ink on the paper to disclose the three-letter code in the marked voting target. The ballot ID number and the displayed code are posted to a public online bulletin board.

After the election, members of the public can verify the final tally using the bulletin board in a manner similar to that of Punchscan and Prêt à Voter. In addition to this public verification, individual voters can record their ballot ID numbers and the codes revealed from the invisible ink. They can then use the bulletin board to check that their ballots were tabulated. This information, however, is not sufficient to prove that they voted a particular way.

3.3.5 REMOTEGRITY

Remotegrity [62], which was used for absentee voting alongside Scantegrity (Section 3.3.4) in the 2011 Takoma Park, Maryland municipal elections, is a *code voting* system. Code voting is a common scheme used in unsupervised remote voting systems. Voters enter a cryptographically-generated code corresponding to a candidate in order to vote for that candidate. Each voter gets a different set of codes, so external observers cannot learn which candidate a voter selected from the code the voter entered.

With Remotegrity, voters receive a code voting ballot and an authentication card in the mail. The codes on the ballot are covered by a lottery-style "scratch-off" field. The authentication card contains several authentication codes under scratch-off fields, a lock-in code under a scratch-off field, and an acknowledgment code. Both cards have serial numbers. Election officials can send each voter two ballots so that one can be used for auditing purposes.

To vote, a voter enters both serial numbers, the codes corresponding to her choices, and an authentication code obtained after scratching off a field chosen at random.

The voter can return to the election website a few hours later to check if her codes are correctly represented, and to see if the election authority has posted her acknowledgment code next to her voting codes. This indicates to the voter that the election officials received valid codes for her ballot. She then scratches off the lock-in code and posts it on the website. This affirms to the election officials, observers and other voters that her vote is correctly represented on the website.

Among all the systems discussed here, this is the first one that asks the voter to take positive action to confirm that the vote was correctly posted.

Part of the security of Remotegrity comes from a separation between the computer that generates the authentication codes and voting codes (the "generator") and the computer that collects the votes (the "vote collector"). Because the generator and the vote collector share no information, the vote collector does not know what codes correspond to what candidates. It therefore has no information (other than codes) about how any voter voted and, because it has no information about what codes are valid, cannot change any cast votes. In addition, the vote collector has no information about acknowledgement codes; when a voter's correct acknowledgement code appears on the website, she knows that the election officials have received a valid code for her ballot because only the election officials could have posted the correct acknowledgement code.

The tally in Remotegrity is computed from the codes in a verifiable manner that corresponds to the code voting system used.

If a jurisdiction is concerned about using the Internet for remote voting, Remotegrity ballots can be mailed in, and voters can check for their codes on the election website to be assured that their vote correctly reached election officials.

3.3.6 HELIOS

Helios [5, 6] is a system developed for web-based E2E-V Internet voting. It was used for the election of a Belgian university president in March 2009 and has been adopted by numerous universities and associations since then, including the Association for Computing Machinery and the International Association for Cryptologic Research.

Before an election, officials input the email addresses of the voters who will be participating into the Helios system. The system emails each voter unique randomly-generated login information and the link to the election website.

During the election, a voter enters her choices on the website. After entering her choices, the voter has an option to "spoil" their ballot and request a new one. This invalidates the ballot, so that it is not counted in the final tally, but still allows the voter to verify that it was cast as intended. Spoiling a ballot is also a way to practice using the system and gain confidence in its accuracy. Once the voter casts a ballot that she does not declare to be spoiled, the system sends an email confirming the receipt of her vote, but does not include her choices in the email. At any time before the close of the election, the voter can repeat these steps and the new vote will replace the old vote.

After the election, Helios uses cryptographic techniques to tally the votes without revealing how individual voters voted [11, 55].

Helios does not require voter authentication until after the voter decides to cast a ballot, so any interested party may prepare and audit ballots. All cast ballots are posted in encrypted form on a public online bulletin board so that voters may check that their ballots have been correctly recorded. Similarly, after the polls close, the decryption and vote tally may be checked.

3.3.7 NORWEGIAN SYSTEM

Between 2011 and 2014, the Norwegian government ran a remote Internet voting trial [28] using a cryptographic protocol designed by Scytl, a commercial voting system vendor. The Norwegian system uses a combination of postal mail, the Internet, and SMS text messaging.

Before the election, the voter receives authorization codes to cast a ballot via postal mail. During the election, the voter uses a computer to cast an encrypted ballot. The voter can cast multiple ballots, but only the last ballot cast is counted. If a voter votes both on paper at a polling place and by Internet, the paper ballot overrides the Internet ballot. After casting a ballot, the voter receives a confirmation code offering a partial verification via an SMS text message.

Available descriptions of the Norwegian system are incomplete, so it is not possible to analyze the system in depth. However the system's claims with respect to voter privacy are weak: "If the voter's computer and the return code generator are both honest, the content of the voter's ballot remains private."[2] In addition, the receipt delivered to the voter proves only that the encrypted ballot was received as cast, not that it was counted as cast or that the encrypted vote matches the voter's intent.

The Norwegian system evolved between its first use in 2011 and 2013. Significant complexity was added in an attempt to assure voters that their ballots were stored as cast. In 2013, the Carter Center mounted a serious effort to observe the Norwegian system in action. Their report on the operation of the system and the problems they had observing it offers useful insight into the administration of E2E-V systems in general, as well as the particulars of the Norwegian system [15]. Scytl and the Norwegian government assert that this is an E2E-V system. However, if a voter's encryption software and the return code generator share information, they can lead her to believe that her vote was cast accurately even when it was not. As such, the Norwegian system's property of voter verifiability relies on the voting system software functioning properly. True E2E-V systems can not rely on the correctness of the voting system software for verifiability.

The Norwegian system also does not provide a proof of the tally, and is therefore not universally verifiable. If a voter casts multiple ballots to avoid coercion, she cannot verify which ballot was counted. Since the tally cannot be correct if the correct votes are not included in the count, the voting public also does not have the information to determine that only one vote was counted for each voter. For all these reasons, the Scytl software implementation used in the Norwegian elections is not considered an E2E-V system.

3.3.8 WOMBAT

The Wombat in-person voting system [31] has been used for multiple pilot elections in Israel. A voter fills out her ballot on a touch-screen and receives a printout of both encrypted and unencrypted versions of her vote. She can then choose either to cast or to audit the encrypted vote. If she chooses to audit the vote, she may check that the vote was correctly encrypted. If she chooses to cast it, the unencrypted vote goes into the ballot box and the encrypted vote is posted on a public online bulletin board; the voter can take her copy of the encrypted vote home to verify that it was posted. The encrypted votes are tallied cryptographically, and the unencrypted votes in the ballot box can also be hand-counted.

3.3.9 DEMOS

DEMOS [23] is a code voting system where the voter is given a two-part coded ballot. She uses one part for auditing and the other to vote. Associated with each choice on the ballot is a vote code; the vote code includes the encryption of the vote, which is entered in the voting machine by the voter, and a receipt code, which the voter does not enter, but which is posted online next to the vote code.

The voter can check the receipt to ensure her vote reached the election authorities. The ballot also has a QR code containing all the information on the ballot, which can be scanned by the voter if she prefers not to manually enter the vote code. Once the ballot is entirely represented on the computer, the voter can make her choices. If the voter scans the QR code, the scanning computer knows how she voted. The vote codes are encryptions of the votes, and a verifiable tally is obtained in a standard manner.

[2] This claim is part of the voting protocol description for the Norwegian system [28]. "Honest" means that the software on the computers in question has not been corrupted in an attempt to subvert the election.

A pilot study of DEMOS was carried out during the 2014 European Elections in Greece.

3.4 LIMITATIONS AND TRADEOFFS OF EXISTING E2E SYSTEMS

E2E systems inherit many of the limitations of traditional voting systems. Reliability of equipment, reliance on procedure, trust in insiders, and accessibility are all problems with traditional in-person voting systems. For remote systems, the integrity of postal systems, turnaround time for mailed materials, access to Internet or fax technology, and reliability of Internet servers are all well-documented obstacles to voting.

Existing E2E systems mitigate some of these limitations, but have other limitations of their own. In this section, we examine the limitations of E2E systems with a particular focus on those that are unique to or exacerbated by E2E characteristics.

3.4.1 VOTE SECRECY

Systems like Prêt à Voter (Section 3.3.2) and Punchscan (Section 3.3.3) rely on a randomized candidate order or a code on printed ballots to ensure vote secrecy. Voted ballots must appear on a public online bulletin board in order to verify the election results. To protect secrecy, only the selected position or code is visible on the final ballot along with a ballot ID.

If an insider is able to review the printed ballots before the election, they can record how the candidate positions are arranged for each ballot ID. The insider could then violate secrecy by identifying the candidates marked on the voted ballots [12].

Recent work on Prêt à Voter recommends printing ballots on demand at polling places in order to limit this possibility [49]. However, printing on demand introduces additional problems and expense compared to centralized printing. More printing equipment is required at each polling place, and that equipment can break or be difficult to operate. The printing equipment must also have some way of communicating with the rest of the election infrastructure to ensure that it has the correct cryptographic seeds for generating new ballots.

Scantegrity II (Section 3.3.4) uses invisible ink to hide the vote codes on unvoted ballots, and Remotegrity (Section 3.3.5) can use scratch-off fields to hide vote codes and other information required to cast a ballot. These techniques limit the opportunity for insiders to learn secrecy-compromising information without being detected through the presence of a marked or damaged ballot.

Even with techniques to mitigate insider foreknowledge of the ballots, secrecy can still depend on voters and poll workers correctly following procedures. An important aspect of secrecy is *receipt freedom*: voting systems should not provide receipts (akin to purchase receipts) that allow voters to prove how they voted, because these enable both coercion and vote selling. However, some E2E systems are only receipt free because of procedure; for example, a voter can leave the polling place with a complete Prêt à Voter ballot, failing to shred the half with the candidate order. With both halves of the ballot, she can prove how she voted.

RIES (Section 3.3.1) makes a deliberate secrecy tradeoff by weakening the receipt freedom requirement in exchange for providing universal verifiability and a degree of individual verifiability. The results of an entire election can be independently audited using only the information that is publicly available after the election. However, if a voter discloses her credential or her encrypted vote, the same public information may be used to violate ballot secrecy. The developers of RIES judged this violation to be no more severe than the threats to ballot secrecy inherent in postal voting, and therefore worth accepting for the benefit to verifiability.

3.4.2 BALLOT STUFFING

As when ensuring vote secrecy, many E2E systems depend on correct procedures to defend against ballot stuffing. For example, during the University of Ottawa elections using Punchscan, more ballots were cast than voters recorded in the pollbook. In this case, ballot stuffing can be caught after the fact by poll workers, but it is not an inherently verifiable property of the system and it requires trust in the accuracy of the poll workers.

In the Helios system officials can register voters in the system by email address, so there is limited protection against insider ballot stuffing. Helios relies on individual voters verifying their votes. However, while an interested party may verify the tally for the entire election by checking that the collection of encrypted votes is counted correctly, no provision exists to determine if votes were fraudulently cast on behalf of register voters who did not vote [51].

A pre-election step that publicly publishes tables of valid ballot IDs can help mitigate this problem, but also creates others. All votes in the final tally, even though they are anonymized, can be traced back to before the election began and cross-checked with voter registration rolls. However, having a fixed set of ballot IDs can make it harder to replace lost, stolen, or spoiled ballots, or to provide for late or same-day voter registration.

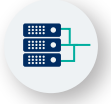
3.4.3 DISPUTE RESOLUTION

E2E systems provide voter verifiability: they enable a voter to determine if her vote was accurately recorded. However, when the vote is not accurately recorded, not all E2E systems provide the voter with evidence that can be used to convince an independent party of the problem. This creates a vulnerability that dishonest voters could exploit. For example, a dishonest voter could raise doubts about the legitimacy of the election by incorrectly claiming that their vote is not accurately recorded.

An E2E system with dispute resolution enables a voter to present evidence to support claims of election fraud. It also enables a third party to resolve a dispute between a voter who claims her vote is inaccurately recorded and the voting system that claims it is accurate.

All cryptographic protocols in the academic literature that provide dispute resolution[3] require either paper or a second electronic method, such as a smartphone, in addition to the machine the voter uses. This is true whether the voter votes in a polling booth or remotely. Therefore, any voting system with dispute resolution should use either paper or a second electronic method.

3.4.4 INFRASTRUCTURE AND EQUIPMENT



Election equipment can fail in practice. An E2E system must be resilient to failures while not giving up E2E properties. A system that lacks recovery mechanisms is not robust; it is only as strong as its weakest recovery mechanism. For example, if a remote voting website fails and election officials resort to accepting voted ballots by email, E2E guarantees are lost for all the emailed ballots.

[3] This includes only the protocols intended for use by voters who vote from untrusted machines.

In addition to being more sensitive to failures, verifiable election systems often require more sophisticated equipment than traditional systems. For in-person voting, a verifiable system might require ballot printers for on-demand printing, a high-quality shredder for two-part ballots, and more sophisticated assistive devices. This adds cost and increases poll worker training requirements.

Many E2E systems post encrypted ballot information to a public online bulletin board during the election. Most of these systems assume that the bulletin board is *write-only*. On a write-only bulletin board, information can never be removed or changed once it has been posted. Moreover, the order in which items are listed on the bulletin board cannot be changed.

In order to update such an online bulletin board in real time, these E2E systems are distributed systems; they can be networked via traditional means, or information transfer among machines can be carried out manually by election officials using USB flash drives or similar devices. Depending on the networking scheme, this can leave the system vulnerable to various security threats and denial of service attacks. At least part of the system must be connected to the public Internet, which increases the possibilities for malicious attacks.

Many systems allow voters to use their own computers to vote. While convenient for voters, this can cause problems because election officials cannot control the voting environment on voters' computers. Threats include:

- malware on the voter's computer, which can undermine security;
- incompatibilities that arise because of the voter's operating system or web browser versions; and
- compromised network infrastructure between the voter and the central election system, which can allow votes to be intercepted or changed by third parties.

In general, it is widely recognized that any E2E-VIV system must be *software independent* [47]. 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. A voting system is *strongly software independent* if, in addition to being software independent, it enables a detected change or error in an election to be corrected without re-running the entire election. A requirement contained in this report insists that any future E2E-VIV system must be strongly software independent.

3.4.5 USABILITY

Traditional election systems struggle with usability. Most often, however, the problems can be addressed with special attention to user interface design. Verifiable systems add steps and complexity to the voting process, presenting usability complications that researchers have not fully studied or overcome. For example, marking a ballot is more complex with code voting, as with Remotegrity, and with position or shape matching, as in Prêt à Voter and Punchscan.

Individual vote verification, not possible with traditional voting systems, is an entirely new process that voters must master in order to take full advantage of the positive E2E-V properties. Many E2E systems have attempted to reduce the additional effort for voters who are not interested in verifying their cast votes.

In 2014, a team of researchers from Rice University studied the usability of three E2E-V systems: Helios, Prêt à Voter, and Scantegrity II [3]. They sought to measure usability by examining effectiveness, efficiency, and satisfaction. Their results show that these systems broadly fail in the area of usability, even for typical voters who are not interested in performing additional verification steps.

The researchers found that a significant number of voters failed to cast a ballot with each of these three systems, rendering them ineffective. Many of those voters thought they had successfully cast a ballot, only to discover that the process had failed them. In a real election, those voters would have left the voting process unfinished without realizing that there was any problem. Traditional voting systems have success rates close to 100% [13].

The E2E-V also lacked efficiency. They all required significantly more time for voting. It took almost twice as long to vote with the E2E-V systems as with a traditional system.

The usability aspects of an election system are crucial. An election system must not disenfranchise voters; on the contrary, it should make voting easy and assist voters in completing the process. Voters must also be confident in the election results. The Rice study shows that adding E2E guarantees can add verifiability at the expense of usability, resulting in a voting system that is unusable by voters. Some researchers do not agree with the Rice study [39]; however, it is an important reference point for E2E-V development.

3.4.6 ACCESSIBILITY

Many E2E systems have requirements for voters' abilities. For example, a typical voter can see where to make a mark for a particular candidate on a Punchscan ballot, but a sight impaired voter cannot do the same without help. In addition to obstacles to marking a ballot, some types of E2E systems lack features to allow disabled voters to participate in individual vote verification without help. Information required for verification is frequently delivered through a paper receipt, an invisible ink code, or receipt data that a voter must write down.

Researchers have proposed accessible verification protocols that protect vote secrecy and allow voters to participate in individual vote verification [17]. These protocols require using accessible devices with an audio, sip-puff, or switch interface to read and mark the unencrypted ballot. The voter must trust that any special device she is using will not create a record of how she voted, which would violate vote secrecy. The device must also represent the ballot faithfully to the voter so that votes are recorded as intended.

Requiring trust in accessible devices is not unique to E2E systems [48]. In non-E2E systems, voters are required to trust many aspects of the election. Because voters must trust the chain of custody of ballots, the integrity of poll workers, and the outcomes of any audits, having to trust an accessible device is a relatively small concession to make in an already-flawed system.

On the other hand, a well-designed E2E system requires a much smaller base of trust for voters to be confident in the election results. The additional requirement of trusting an accessible device is not a flaw of the E2E system; it is part of the nature of using accessible devices. This vulnerability may be lessened by allowing voters to use multiple accessible devices, or by requiring all voters—both those who need help and those who don't—to use similar accessible devices or a universal interface. This ensures that multiple users test the accessible devices or interfaces.

3.4.7 SOCIAL AND POLITICAL

New election systems face a difficult problem. In order to be adopted in large-scale elections, they must have a successful track record. Building a record of success, given the limited financial and human resources available for early small-scale pilot programs, is a major challenge. With limited resources, election officials may be forced to compromise on some aspects of the election systems they implement. This increases the risk that problems with equipment, software, and support will undermine confidence in the system.

Public confidence in election systems in general, and E2E systems in particular, is fragile. When election systems fail during an election or are revealed to have substantial integrity issues, people may believe that all similar systems are flawed. It does not matter if the E2E systems are very different from each other, or if the E2E systems provide guarantees. Failure of an older E2E system can cause the public to reject a new system.

In 2009, there was a hacking demonstration on electronic voting machines used in previous elections [27]. As a result, the Federal Constitutional Court of Germany decided that electronic systems may only be used in elections if "the result can be examined reliably and without any specialist knowledge of the subject." In practice, this is a standard that E2E systems have not been able to meet [13]. Similarly, after reports critical of RIES were released in the Netherlands, a popular movement successfully advocated for a ban on Internet voting in that country as well.

Many people are aware of computer security concerns and vulnerabilities, and are worried by them. Hacking, malicious code, and large amounts of personal data being stolen electronically are almost weekly news. These concerns rightly make people wary of any system with a computerized component, even if the Internet is not involved. The challenge for E2E systems is to overcome this broader skepticism by demonstrating integrity in a way that anyone can understand without making it more difficult to vote.

CHAPTER 4

REQUIRED PROPERTIES OF E2E SYSTEMS

In August 2010, the U.S. Election Assistance Commission issued a set of testing requirements for overseas and military remote electronic voting system pilot projects [57]. However, the EAC requirements have some serious shortcomings. Many of the requirements are arbitrary, inappropriate, or invalid: some set maximum system error rates using specific numbers without justifying the numbers; some set unrealistic limits on the accuracy of computer hardware; and some prohibit developers from programming in ways that are widely used when implementing highly reliable software systems.

If these issues were addressed, the EAC requirements could serve as a solid set of requirements for remote electronic voting systems. However, they are not strong enough to guarantee end-to-end verifiability, which is essential when considering Internet voting systems for use in real elections.

A set of E2E-VIV requirements, which significantly overlaps with the EAC requirements, can be broadly divided into two groups: *technical requirements* and *non-functional requirements*. Technical requirements are those that can be directly addressed by the design and implementation of the system, such as authentication requirements for voters and election officials. Non-functional requirements are those that are imposed on the system by external entities or where the system depends on external behaviors outside its control, such as specific election certification guidelines and operational procedures. The technical and non-functional requirement groups can be further divided into several categories, and Figure 4.1 gives a high-level overview of these.

The following is a high-level description of the E2E-VIV requirement categories and many of the requirements; the full set of E2E-VIV requirements expressed in the Business Object Notation is available as a separate document [36].

4.1 TECHNICAL REQUIREMENTS

There are ten categories of technical requirements for E2E-VIV systems: functional, accessibility, usability, security, authentication, auditing, system operational, reliability, interoperability, and certification.

4.1.1 FUNCTIONAL

The functional requirements of an E2E-VIV system deal primarily with the casting and recording of ballots and associated voter records. One such requirement is that recorded ballots and voters listed as having voted must correspond with each other; a ballot cannot be recorded without a voter casting it, and a voter cannot be listed as having voted without casting a ballot. If the system tells a voter that her ballot has been successfully cast, the system must correctly retain the record that she has voted. The system must keep a voter's cast ballot information even if servers fail.

Another functional requirement is *receipt freedom*: it must be impossible for a voter to prove to anybody any information regarding how she voted, beyond what someone can mathematically deduced from the final distribution of votes. If a referendum passes with 100% of the vote, for example, there is no way to hide the fact that every voter approved of the referendum. If the result is mixed, it must be impossible for any individual voter to prove how she voted. This must be true even when the voter can create digital evidence of her actions by, for example, video recording the ballot casting process or photographing a completed ballot.

No usable E2E-VIV protocol in existing scientific literature has receipt freedom when the voting computer is untrusted. Since the process of casting any individual ballot can be recorded, a protocol with receipt freedom must allow the voter to vote multiple times but only count the last ballot a voter casts. However, it must also ensure that an observer watching any recorded ballot casting process can independently verify that the ballot was cast. This must be ensured even when the voting computer is not trusted to follow protocol, and in a manner that is easy to use and accessible. This represents a significant research challenge for E2E-VIV protocol designers.

In some elections, voters are allowed to cast multiple ballots with only the last cast ballot counting toward the final election tally. In others, voters are prohibited from casting multiple ballots. The system must accommodate both of these election formats.

Maintaining voter anonymity is critical. It must be impossible after the election to reconstruct a link between a cast ballot and any identifying information about the voter who cast it. However, in systems that

Figure 4.1: Requirements hierarchy for E2E-VIV systems.

support the casting of multiple ballots, it is important to maintain links between voters and their ballots *during* the election to ensure that later ballots replace earlier ballots. To balance these concerns, any link between a ballot and the voter who cast it must be irrevocably broken once it is determined that the ballot will be counted toward the final tally.

4.1.2 USABILITY

The usability of an E2E-VIV system is critical to its successful adoption and use. Since user experience is so important, many of the requirements of the system have some relation to usability even though they may be categorized under other headings. There are, however, two requirements that are exclusively related to the usability of the system with respect to vote casting and a general usability requirement that applies to the system as a whole.

If a voter receives a final vote confirmation from the system, such as "Thank you for voting!", the ballot casting process must be complete and the system must have recorded the vote. This allows voters to be certain that their ballots have been recorded and will be counted.

If a voter is uncertain whether or not the system recorded her ballot—for example, she clicked a "submit" button but never got a response from the system—she must be able to vote again.

Researchers must perform usability testing on any E2E-VIV system before it is deployed. The reports of the usability testing must be made public, and the system must achieve satisfactory test results before election officials use it in a real election.

4.1.3 ACCESSIBILITY

Accessibility—the property of being usable by and useful to voters with disabilities—is one of the main goals of an E2E-VIV system. It is closely related to usability, but there are several requirements associated specifically with accessibility that go beyond typical usability requirements.

Users must be involved in the design of the system to identify accessibility problems at each stage of the development process. Developers must consider the system's compatibility with existing technologies designed to help individuals with disabilities. The system should be developed in a way that allows people to use accessible devices such as switches, eye trackers and screen readers in addition to keyboards, mice and touchscreens. The system should present voting options that are optimized for voters' needs by using alternative display fonts, audio representations, braille representations, and other representations as appropriate.

Developers must take all possible measures to ensure that as many voters as possible can use the system. Election officials must provide access to alternative methods of voting for those voters who cannot use the system.

Researchers must perform accessibility testing in addition to mandatory usability testing. The reports of the accessibility testing must be made public, and the system must achieve satisfactory test results before election officials use it in a real election.

4.1.4 SECURITY AND AUTHENTICATION

Security and authentication are closely related. Together, they represent the broadest set of technical requirements. These include requirements on the E2E-VIV system itself, such as data storage and communications, and requirements on the voting and counting processes that the system enables, including voter authorization, voter privacy, vote integrity, and tally accuracy.

Developers must ensure data integrity throughout the system. No data can be permanently lost if the system breaks down or experiences a fault. The system must maintain the integrity of the voters' register, lists of candidates, ballot information, cast ballots, and other critical information. It must authenticate the original source(s) of all information and keep track of where the information came from. All data communications within the system must have associated integrity checks.

System equipment under the control of election officials must be protected against influences that could modify election results. The integrity of the election results must not depend, in any way, upon the security of system equipment that election officials do not control. The system must perform regular "health checks" to ensure that it is maintaining data integrity, all its components are operating in accordance with their specifications, and all system services are available.

Accurate timing information is critical to security, both to provide evidence of compliance with applicable regulations and to detect attacks on and potential breaches of the system. The system must therefore maintain reliable synchronized time sources, with sufficient accuracy to maintain timing data for audit information, election observation data, and time limits for various aspects of the election process. Using the timing information stored by the system, it must be possible to determine whether nominations (and, if required, the candidate's or election officials' acceptance), voter registration, and vote casting occurred within the time limits for those actions.

Authentication and authorization are also important aspects of security. The system must ensure that each individual can be identified uniquely, so that there is no possibility of mistaking one individual for another. The system must also maintain the privacy of individuals, by ensuring that all personally identifiable data is kept confidential as far as legal requirements of the electoral jurisdiction allow. The system must allow access to each of its services only to authorized users; for example, only election officials may be allowed to load ballot information into the system.

The means used to gain access to the system must, as far as possible, protect authentication secrets (passwords, one-time access codes, biometrics, etc.) so that unauthorized entities cannot acquire them. People may not use third party authentication mechanisms, such as existing Facebook, Google and Twitter accounts, to access the system.

Any potential breach of any public or commercial database, such as a credit card database or the Social Security database, must not affect the security of the voting system's authentication mechanism. An attacker should not be able to impersonate a voter even if the entire database used for authentication in the system is compromised. Individual authentication secrets themselves must be changeable or revocable at any time, at the individual voter's or election officials' request. The system should require all individuals to change their authentication secrets at least at least once in every election cycle.

The system must allow only eligible voters to cast ballots, and must ensure that each voter only casts the appropriate number of ballots. A voter must be able to verify that the system has presented her with an authentic ballot and, in the case of remote voting, that she has a secure connection to an official server.

The system must preserve the privacy and integrity of the vote, end-to-end, to the maximum extent possible. Individual voters may not waive the privacy of their votes. In the case of remote voting, the system must preserve vote privacy and integrity even if the voter's computer contains malicious code (corrupted client software, key logging software or devices, etc.). Any client software used in remote voting must not send data to any Internet host except those associated with the E2E-VIV system or provide any information to third parties (such as Facebook or Twitter) regarding the act of voting. The system must destroy any residual information that could be used to discover a voter's choices after a ballot has been cast. If a voter uses a computer outside the control of election officials to cast her vote, she must be provided with instructions for destroying the residual information on that computer.

The system must accurately count the votes, and the counting process must be reproducible. The system must also maintain the availability and integrity of all information used to generate the final tally and all information regarding the counting process itself for as long as required. Vote tabulation must be *strongly software independent*; it must be possible to detect any compromise of the election system software that causes a change in the tally, and to reconstruct a correct tally from some record in the event of such a compromise.

A deployed E2E-VIV system will likely be an attractive target for highly capable adversaries who wish to influence election results or to disrupt election processes. System designers and testers must assume that an adversary has a budget of US$10 per voter per election that they can apply toward any subset of votes or voters of they choose. This means that designers and testers of an E2E-VIV system for use in a U.S. presidential election must assume that an adversary has a budget of approximately US$1,300,000,000.

Election officials shall have overall responsibility for compliance with these security requirements, and independent bodies will assess compliance as appropriate.

4.1.5 AUDITING

The ability to perform comprehensive audits of system activity is one of the important distinguishing aspects of an E2E-VIV system. compared to other voting systems. In addition to those security requirements (such as the tracking of accurate timing information) that touch on auditing, several system requirements relate specifically to auditing.

Developers must design and implement audit features as part of the E2E-VIV system from the beginning; they cannot be added as an afterthought to an existing system. Developers must implement audit and monitoring capabilities into all levels of the system, from low-level communications among individual computers to high-level interactions with election officials. The system must keep audit logs of all activity relevant to the conduct and outcome of the election. These logs must be locked, incapable of being modified by anyone, once they are written. They must also be as complete as possible without violating voter privacy.

The audit system must actively report potential issues and threats, rather than merely serving as a passive repository of system logs. It must record at least the following events and actions with accurate timing information:

- all voting-related information, including the number of eligible voters and votes cast, the number of invalid votes, count and recount results, etc.;
- any detected attacks on the operation of the system or its communication infrastructure; and
- any system failures, malfunctions, or other detected threats to proper system operation.

The audit system must provide sufficient information to election observers in real time, and after the election's conclusion, to verify that the election is carried out in accordance with applicable law.

The audit system must also be able to:

- cross-check and verify the correct operation of the voting system and the accuracy of the election results;

- detect voter fraud; and
- prove that all counted votes are legitimate and that all ballots have been counted.

In situations where the system cannot verify the legitimacy of all the votes, it must be able to report how many ballots may be affected.

If a tradeoff must be made between maintaining voter privacy and identifying the perpetrators of fraud, the system must resolve that tradeoff in favor of voter privacy.

For voters to trust an E2E-VIV system, its auditability must extend to its own source code as well as the activities it performs during an election. Developers must publish the E2E-VIV system software and any official monitoring and auditing applications in source form. They must include full documentation, instructions for building and running the software, and a digital signature as a proof of authenticity.

4.1.6 SYSTEM OPERATIONAL

System operational requirements ensure that the system is configured, updated, and run in a transparent, accountable way. One important requirement is that election officials must publish manifests of the system used to run any election. These manifests must include details of the software and versions they used, the dates they installed the software, and brief descriptions of the software's functionality. Well-defined procedures must exist to update the manifests to reflect changes to the installed software and to check the installed software against the manifests to detect tampering. Election officials must follow these procedures before every election period, and must also check all equipment and approve it for use.

During an election period, election officials must keep key equipment in a guarded, secure area at all times. They must have a contingency plan for system failures, including provisions for backup systems. The backup systems must conform to the same standards and requirements as the systems they replace. In addition, election officials must make sufficient arrangements to backup data; backup systems must be continuously monitored, and backup data must always be available during the election. Election staff must be ready to intervene rapidly, according to well-defined response procedures, if problems occur during an election.

The election officials and election system vendors must be accountable for the performance of the system. To ensure this, election staff must prepare a report after every election containing every software manifest change and every violation of data security, system security, physical security or control procedures that occurred during the election period. This report must be published within a reasonable amount of time after the election.

4.1.7 RELIABILITY

E2E-VIV systems must satisfy strict reliability requirements that ensure their behavior is reasonable, both under normal conditions and while under attack.

In general, the back-end (i.e., non-voter-facing) components of the system must be able to run continuously, for at least a week, at the highest rate that election officials expect voters to participate. Multiple actual tests of mock elections must be run to demonstrate that the system satisfies this requirement. It applies only to normal operation, not while the system is under attack.

The system must also be highly available during the election period; voters should be able to access it 99.9% of the time. It must be able to recover from any failure, other than a regional natural disaster or malicious attack, in less than 10 minutes. This must be demonstrated by inducing failures in actual mock election situations, for example by unexpectedly unplugging servers or disconnecting storage devices. In order to ensure the 10-minute maximum recovery time, all critical parts of the system must have redundant backup systems that can take over if failures occur.

An E2E-VIV system is likely to be a tempting target for distributed denial of service (DDoS) attacks.[1] It must be able to continue correct operation during a sustained DDoS attack at a specified level (that is, a specified number of machines performing the attack or a specified amount of data being used in the attack), without slowing down by more than a specified amount during the attack. The specified attack level and acceptable slowdown will vary among election types. For example, a system running a national election must be able to resist a significantly higher level of attack than a system running a county election. Security experts' initial suggestions for the thresholds for a national election are that the system must continue operating correctly under a DDoS attack at a level of 100 gigabits per second, with no more than a 15 second slowdown.

The network configuration used during an election must show that the system can survive DDoS attacks and continue an acceptable level of operation. Election officials should re-evaluate the network configuration every election cycle to keep pace with advancing attack technology.

4.1.8 INTEROPERABILITY

E2E-VIV systems must use open, rather than proprietary, data and communication standards for interoperability among their various components and services. Whenever possible, developers should use the Election Markup Language (EML), or a similar standard ratified by an international standards body, for data interchange and configuration within the system. The standards used within the system should allow for localization of election data, such as translation to different languages, where required.

Election officials must publish the log data for the system, and documentation describing its meaning and format, so that anybody can download, inspect, and publish concerns based on the system logs.

4.1.9 CERTIFICATION

In order to provide sufficient evidence for certification of an E2E-VIV system, each functional requirement must have an associated set of automated tests. Election officials must be able to run these tests on demand. Test results should be unambiguous and easy to understand.

To the extent possible, system developers must provide formal proofs of correctness and security for the communication and cryptographic protocols implemented by the system.

[1] A distributed denial of service (DDoS) attack is an attempt to make an Internet server unavailable to its intended users by attacking the server from many other systems on the Internet at the same time.

4.2 NON-FUNCTIONAL REQUIREMENTS

There are five categories of non-functional requirements for E2E-VIV systems: operational, procedural, legal, assurance, and maintenance/evolvability.

4.2.1 OPERATIONAL

The operational requirements on E2E-VIV systems deal with several distinct issues: voter assistance, election and registration timing, voter registration, candidate nominations and lists, receipt freedom, voter assistance, election integrity, and openness.

VOTER ASSISTANCE Election officials must inform voters, in clear and simple language, how electronic voting will be organized and what steps voters will need to take in order to participate and vote electronically. Election officials must make support and guidance on voting procedures available to all voters. For remote voting, support and guidance must be available through a different, widely-available communication channel (such as a dedicated phone number) in addition to being available on the Internet. Voters must receive clear guidance on hardware platforms, operating systems, browsers, browser plug-ins, other applications that the E2E-VIV system requires. They must also be told what what common components, plugins, or other software, such as pop-up blockers and script blockers, may interfere with voting. Voters must receive clear guidance about configuration choices they can make to more strongly protect their privacy, such as:

- disabling cookies and browser history logging;
- running privacy-protecting browser plugins;
- voting from temporary virtual machines;
- logging out of social networks; and
- disabling non-election-related Internet communications.

ELECTION AND REGISTRATION TIMING In any election carried out using an E2E-VIV system, legal provisions in the election jurisdiction must state clear timetables concerning all stages of the election. The period during which a vote may be cast electronically must not begin before election officials notify the public of the election. In jurisdictions that allow remote electronic voting, the voting period must be defined and made known to the public well in advance of its start. In jurisdictions where remote voting takes place concurrently with voting at supervised polling stations, remote voting should not be allowed after the period for supervised voting has ended.

VOTER REGISTRATION An E2E-VIV system must have a publicly accessible voters' register that election officials regularly update. Each voter must be able to check that her information as recorded on the register is accurate, and must be able to request corrections. Election officials must authenticate all modifications to the voters' register.

CANDIDATE NOMINATIONS AND LISTS On any electronic ballot, all voting options must be presented equally. An electronic ballot must not contain any distinguishing fonts, sizes, styles, or other embellishments that could cause a voter to think that one or more of the voting options are preferred. The ballot must not contain any information about the voting options, such as biographical information about candidates or interpretations of and statements about ballot initiatives. Only the information required for casting the vote or required by law (for ex-

ample, candidate party affiliation) must be on the ballot. The system must not display any messages that may influence voters' choices. If additional information about voting options is available from an electronic voting site as part of an E2E-VIV system, it must be separate from the actual electronic ballot and presented without bias.

RECEIPT FREEDOM E2E-VIV systems must exhibit receipt freedom, which was described earlier as part of the functional requirements. Operationally, receipt freedom has two different meanings depending upon whether the voting apparatus is supervised (in a polling place) or unsupervised (as is the case in most remote voting systems).

In a supervised environment, voting information—images, sounds, etc.—should disappear from the voting apparatus as soon as the voter casts a vote. When the system provides paper proof of an electronic vote at a polling place, the voter must not be allowed to show it to any other person or remove it from the polling place.

In an unsupervised environment, the situation is different. An adversary or coercer can digitally record the voting process, or voters can record themselves with the intention of selling their votes. Third parties must not be able to use such recordings to prove, either during or after the election, that the votes shown in the recordings are counted in the final tally.

ELECTION INTEGRITY Developers will likely make E2E-VIV systems available for testing by voters and election officials, both before and during elections. To preserve election integrity they must indicate clearly, before the final casting of any ballot, whether the ballot is part of a real election or part of a test. If a test occurs simultaneously with a real election, the system should direct individuals casting test ballots to the appropriate voting channel so they can cast real ballots.

An E2E-VIV system must not disclose preliminary results to anyone, including election officials, until after the system has stopped accepting electronic ballots. The system must not disclose tally information to the public until after the end of the voting period, including all polling station voting. The system should perform any decoding required for the counting of the votes as soon as practicable after the end of the voting period. Election officials must be able to participate in, and observers must be able to observe, the counting process. The system must keep a record of the counting process, including timing information and identifying information for everybody involved in the counting process. If any irregularity affects the integrity of votes, the system must record that the affected votes had their integrity violated. The effect of integrity violations on the election results will vary depending on the legal provisions of the involved jurisdictions.

OPENNESS Any deployed E2E-VIV system must function correctly as an open system, where large parts—specifically, any remote client hardware and software—are unknown, unsecured, uncertified, and completely out of the control of election officials. Researchers must be able to audit the system to the extent possible given this requirement. Developers and election officials should be able to apply the conclusions drawn from the audit process when developing systems and procedures for future elections.

4.2.2 PROCEDURAL

Successful deployment of E2E-VIV systems requires certain procedures relating to provisioning, certification, maintenance, availability, and use. Because such systems are critical pieces of public infrastructure, information about their functioning must be publicly available. Information about the specific components of a system must be disclosed, at least to the relevant election officials, as required for verification and certification purposes. Before an E2E-VIV system is introducted, at appropriate intervals after its introduction, and whenever any changes are made to the system, electoral officials must call upon an independent body to verify that the system is working correctly. The independent body must also verify that election officials have taken all necessary security measures.

After introducing an E2E-VIV system, election officials must take steps to ensure that voters undesrtand its use and have confidence in the system. These steps may include outreach, practice elections, and any other measures to educate voters. In particular, election officials must give voters an opportunity to practice any new electronic ballot casting method before, and separately from, the time voters cast electronic ballots during a real election.

Election officials must take steps to ensure the reliability and security of the E2E-VIV system. For example, they must guard equipment and provide suitable reliable power supplies. They must make every effort to avoid the possibility of fraud or unauthorized intervention during the voting process. Election officials must be satisfied that the E2E-VIV system is genuine, and is operating properly, before using it to conduct a real election.

Only election officials or individuals appointed by them should have access to the central infrastructure, the servers, and the election data. Election officials should establish clear rules for such appointments. Critical technical activities must be carried out by teams of at least two people, and the composition of these teams must be changed regularly. As far as possible, critical technical activities should take place outside of election periods.

To the extent permitted by law, election officials must allow observers to watch and comment on the conduct and results of any election carried out using an E2E-VIV system. During an election period, any authorized intervention affecting the system must be monitored by both election officials and election observers.

The system must maintain the availability, integrity, and confidentiality of the votes. It must also keep the votes sealed until the counting process begins. Any votes stored or communicated outside controlled environments must be encrypted. Recounts must be possible, and any features of the system that may influence the correctness of the result must be verifiable. The system must also support partial or complete re-runs of elections.

Election officials must establish clear technical and legal procedures to follow if voters can prove that the system did not accurately receive or count their votes. They must also establish procedures to follow if the official election verification application does not verify that the results of the Internet portion of the election are correct.

4.2.3 LEGAL

Legal requirements arise primarily from the application of existing law to E2E-VIV systems. These include requirements on accessibility and availability; on the counting of votes, number of votes per voter, and anonymity of votes; and on restrictions with respect to reverse engineering or testing of E2E-VIV systems.

To comply with accessibility and availability requirements, an E2E-VIV system must be understandable and easy for voters to use. Registration requirements for electronic voting must impede voter participation. E2E-VIV systems should be designed, as much as possible, to maximize the opportunities they provide for voters with disabilities. Unless remote electronic voting channels are universally accessible, they must be used only as an additional and optional means of voting beyond polling places or more traditional remote voting methods.

In all jurisdictions—those that use an E2E-VIV system exclusively and those that combine electronic and traditional voting systems—election officials must ensure that only one vote by each voter is counted. In jurisdictions that combine electronic and traditional voting system, there must a secure and reliable method to aggregate all votes and calculate correct results.

The way in which voters are guided through the process of electronic voting should be designed to discourage their voting precipitately or without reflection. Voters must be able to alter their choices at any point during an electronic voting process before casting their vote. They must also be able to stop the voting process without the system recording their previous choices or making them available to any other person under any circumstances. The electronic voting system must not enable any manipulative influence to be exercised over the voter during the voting process, must provide the voter with a means of participating in the election without exercising a preference (for example, by casting a blank ballot), must indicate clearly to the voter when the voting procedure has been completed, and must preserve voter anonymity.

There must be no legal impediments to interested parties who want to study the E2E-VIV system. In particular, no nondisclosure agreement or contract of any kind may be required for download and study of, or for building, testing and publishing test results for, the E2E-VIV system.

4.2.4 ASSURANCE

There are several assurance requirements related to the implementation, documentation, and licensing of E2E-VIV systems. First, client side software—that is, any software that is expected to be used on a system serving as a voting terminal, whether a supervised machine at a polling place or an unsupervised machine belonging to a voter—must be free of known bugs on a wide range of platform and software stack combinations. The system must exhibit strong security with respect to voter authentication, such that there is no way to automate forging or invalidation of voter authentication credentials without compromising the cryptographic protocols or secrets used in the system.

All aspects of the design, architecture, algorithms and documentation for the entire Internet voting system (not just the E2E-V core) should be published and available for free download by anyone. As the system changes, all associated public documentation must be kept up to date, and no new version of an E2E-VIV system should be certified until it has up-to-date documentation.

The source code, build scripts, issue tracking system, security features, and related development information for the entire Internet voting system—all versions, for all supported platforms—should be made publicly available for free download and inspection, under a license that permits anyone to download, build, instrument, and test the system.

4.2.5 MAINTENANCE AND EVOLVABILITY

Maintenance and evolvability requirements are closely related. Election officials, or any entity engaged by election officials for this purpose, must have the right and the ability to update the election system to conform to changes in applicable law, available technology, or threats to system integrity independent of the original vendors of the system.

Election officials must also have the right and ability to patch election systems to correct flaws discovered in the algorithms, implementation, or deployment, subject to the documentation update requirement described above.

CHAPTER 5

CRYPTOGRAPHIC FOUNDATIONS

This chapter is not included in the abridged version of the report for non-technical audiences. It is included in the full report, available from https://www.usvotefoundation.org/E2E-VIV.

CHAPTER 6

ARCHITECTURE

This chapter is not included in the abridged version of the report for non-technical audiences. It is included in the full report, available from https://www.usvotefoundation.org/E2E-VIV.

CHAPTER 7

RIGOROUS SOFTWARE ENGINEERING

This chapter is not included in the abridged version of the report for non-technical audiences. It is included in the full report, available from https://www.usvotefoundation.org/E2E-VIV.

CHAPTER 8

FEASIBILITY

In Chapters 1 through 4 of this report, we described the motivation for, history of, and requirements on a remote voting system that experts can approve and the public can trust. In Chapters 5 through 7 of the full report, we described the necessary cryptographic, architectural, and engineering foundations, tools, and techniques necessary to design and build a system that fulfills the requirements set forth in Chapter 4. However, the fact that it seems *possible* to design and develop such a system does not mean that it is *feasible* to do so.

This chapter analyzes the question of feasibility in several areas, some of which are *technical* (correctness, security, usability, availability) and others *non-technical* (law, politics, fiscal, research, development, operational, and business). After discussing each of these areas, we summarize with an integrated feasibility analysis, focusing on the question: "Is it practical to tackle the problem of E2E-VIV at this time?"

To determine feasibility, we took multiple approaches. We examined current knowledge of these systems as discussed in peer-reviewed literature. We talked extensively with election officials, and had discussions over multiple years with both election verification activists and other experts who have decades of experience designing and developing secure, high-assurance systems.

The feasibility of E2E-VIV will ultimately be determined by those organizations with the resources to invest in E2E-VIV research and system development. Given how quickly unverifiable Internet voting systems are being deployed worldwide, such investments are time critical.

8.1 TECHNICAL FEASIBILITY ANALYSIS

We first examine technical feasibility. If designing and constructing a formally verified, secure E2E-VIV system is not possible, analyzing any other feasibility area is unnecessary.

Since this section focuses on technical feasibility, it refers back to the technical chapters of this report. If you are reading the non-technical version of this report, or you are uninterested in technical matters, we recommend skipping to Section 8.2.

8.1.1 PROTOCOL

A secure and usable E2E-V protocol is an essential component of any E2E-VIV system. However, E2E-V alone does not provide many of the necessary properties for public election systems, including:

- **COERCION RESISTANCE.** It is difficult to design a coercion-resistant E2E-V protocol where the voter votes from an untrusted computer. Coercion-resistant protocols exist where the voter votes from a trusted computer; however, these require the voter to vote multiple times, indicating each time whether or not the vote should be considered valid. Current coercion-resistant protocols pose significant usability and accessibility challenges.
- **DISPUTE RESOLUTION.** An E2E-V protocol enables a voter to determine whether her vote was correctly recorded. If she discovers that it was not, the protocol does not necessarily provide her with evidence to convince a third party of the problem. It is therefore difficult for election officials, observers and the general public to determine the extent of fraud if there are multiple complaints. Existing protocols that do provide the voter with evidence of fraud require the use of paper or a second independent communication channel, as well as the use of physical election security procedures. Such procedures cannot be used for remote voting. Additionally, the use of paper or a second communication channel presents usability and accessibility challenges.
- **RESISTANCE TO CLIENT MALWARE AND DENIAL OF SERVICE.** If a voter follows all the steps for voter verification of an E2E-V protocol, she should be able to determine if her vote has been manipulated by malware. However, denial of service attacks might limit her ability to perform the verification procedure. Additionally, if the protocol does not support dispute resolution, she would not be able to provide evidence of a problem. In particular, client malware could replace her vote with another valid vote in many E2E-V designs. She would recognize this if she were able to perform voter verification, but she would not be able to prove it. The use of multiple channels or paper can provide additional protection against these types of attacks, but dilutes the usability and accessibility of the system.
- **UNIVERSAL DESIGN.** E2E-V protocols with a number of the above properties have been developed, but the use of second channels (or paper) and multiple complicated steps are difficult to achieve in an accessible system. A protocol that cannot be used properly by most voters is not necessarily secure, no matter how well it is designed. For example, if voters find it difficult to verify their votes, voter verification cannot be relied upon to contribute to the correctness of the election outcome.

Experts are divided on whether a protocol that has some of these properties would be an improvement over existing vote-by-mail systems. Further, most experts agree that it is not clear how to develop a protocol that has all of these properties. As such, this remains one of the most uncertain and challenging areas for progress on Internet voting.

8.1.2 ENGINEERING FOR CORRECTNESS AND SECURITY

As previously mentioned, formal verification capabilities have advanced tremendously over the past fifteen years. Scientists were barely imagining high-assurance or formally verified operating systems and hypervisors such as seL4 [37], Mirage [41], and HaLVM [54] in the year 2000. The same is true of formally verified compilers (such as CompCert [21]), static analysis tools (such as Verasco [58]), verification tools (such as VST [59]), and verification-centric programming languages (such as Dafny [22]). Incredible advances in mechanical theorem proving, particularly for SAT, SMT, constraint solving, and logical frameworks, support all of this technology.

Design, development, and analysis of secure systems have also progressed tremendously. Powerful open source static analysis tools (such as Uno [30]), fuzzers (such as AFLFuzz [7]), and protocol specification and reasoning frameworks (such as EasyCrypt [24] and F [26]) are all publicly available and can be applied to commercial systems.

The only thing preventing the design and development of formally verified, correct and secure evidence-based systems is market pressure. Only a very small number of organizations have the necessary resources—primarily in the form of people and knowledge—to tackle such challenges, and they cannot do it without clients who provide requirements, funding, and time.

As such, if an appropriate protocol is developed, *designing and developing an E2E-VIV system is technically feasible*. We can estimate—based upon the size and complexity of the relevant protocols and subsystems—the effort necessary to build an E2E-VIV system. We can determine cost based on the estimate of effort. This analysis is provided below in Section 8.2.3.

8.1.3 DESIGN AND ENGINEERING FOR USABILITY

Striving for security and usability often presents conflicts. Design features that offer security often decrease usability, and features that offer usability often decrease security. This problem is very apparent in early E2E-V election systems such as Helios, Prêt à Voter, and RIES. Because of this conflict, scientists are faced with a difficult question: Is it feasible to design and develop an E2E-VIV system that is secure and usable? More specifically, is it feasible to design and develop an E2E-VIV system that follows universal design principles?

Usability experts claim that universal design of election systems is reasonable and necessary. Several organizations have extensive experience in this area, such as the Center for Civic Design. Some new voting systems that are under development, such as Los Angeles County's VSAP project and Travis County's STAR-Vote system, mandate universal design.

While researchers are still studying certain aspects of usable E2E-VIV systems—particularly those of voter ritual and verifiability—usability experts agree that a universal design for an E2E-VIV system is possible in principle. The experts agree that, in order to achieve such a universal design, it is necessary to conduct a long-term, in-depth, qualitative and quantitative usability study based upon a working demonstration system.

QUALITATIVE EXPERIMENTS. In an interactive, *qualitative* experiment, a facilitator and a voter communicate using a video chat system such as Skype. The voter shares their desktop with the facilitator. The facilitator should be very familiar with the issues of E2E-VIV systems. The facilitator should also have usability and accessibility knowledge. The voter uses one of several versions of the E2E-VIV system. While using the system, the voter shares their thoughts and feelings about the experience in real-time. After the voter has finished participating in the demonstration election, the facilitator uses a script to ask the voter what they thought.

QUANTITATIVE EXPERIMENTS. For a non-interactive, *quantitative* experiment, voters are solicited via social media, mailing lists, etc. to experiment with (variants of) an E2E-VIV system. Sample voters in these experiments are given ample information about what kinds of information are being collected about their behavior, so they can make a fully-informed judgement about their participation.

Various quantitative measures related to voter participation and interaction can be measured automatically, both within voters' web browsers and on the E2E-VIV server. Most of this data is similar to the analytics that any professional website collects about its users: How do voters navigate the site? Where does a voter pause for a long time to read? When does a voter ask for help? When does a voter hover over a button a long time before they decide to click it? How often do voters challenge ballots or verify their votes? How often do voters examine the bulletin board? Is there a correlation between the interactive behavior of a voter while voting and their likelihood of voting, challenging, or auditing correctly?

8.1.4 AVAILABILITY

A system that is correct, secure, and usable is still not useful to voters if it is unavailable during an election. Many government websites are unreliable, especially during a distributed denial-of-service (DDoS) attack or just after a security breach.

Many companies whose businesses depend on having highly available and secure websites have effectively solved this problem. Companies like Amazon, Google, and Facebook have uptimes comparable to those necessary to run a public election, even if threatened by DDoS attacks.

The necessary network, server, and security infrastructure—and the consequent cost—to fulfill the availability demands of these companies and their customers is significant. The cost is so significant that every government that has attempted to build a facility dedicated to running Internet elections has spent many millions of dollars per election.

Today, however, there are many robust, inexpensive, public and private cloud computing platforms built to work with pre-existing infrastructure. Strong, large-scale DDoS protection services are now available. Because E2E-VIV systems do not need to run on dedicated, physically secure hardware—as long as suitable roots of trust are available—it should be possible to run highly available elections systems on existing hardware.

We believe a highly available E2E-VIV system can be deployed and maintained with current highly-available networked services. This is especially true if elections are run over a reasonable time frame (such as many days to a few weeks) and are built using a peer-to-peer network model.

8.1.5 OPERATIONAL

Operational feasibility presents other challenges. Creating a correct, secure, usable E2E-VIV system that can be deployed with high availability is not enough. If that system is too difficult or expensive to integrate into existing election workflows, or is too complex for LEO IT staff to understand and support, it will not be used.

Software such as an Internet voting system is usually delivered for deployment as a bundle of source code with many dependencies. That stack of software must be hand-built, carefully customized, and installed on a server. Because of the complexity of Internet voting systems, the core application typically depends on dozens of other large pieces of software. These dependencies include databases, application servers, web servers, authenticatation servers, and dozens of libraries for processing configuration files, communicating over networks, and performing cryptography.

The vast majority of jurisdictions has neither the expertise nor the resources to deploy such a system. Deploying a traditionally designed and developed Internet voting system is not feasible.

Packaging and delivering complex distributed processing systems in cloud deployments, however, has become commonplace in recent years. Complex deployments by non-technical staff are now possible and widely available due to the creation of new technologies invented specifically to fulfill this need.

The key technologies that solve this problem are discussed in Chapter 7 of the full report. These include continuous integration systems and configuration management tools for development and deployment. They also include cloud deployment and management technologies, such as those available from Amazon, Google, Microsoft, Heroku, and other major cloud providers.

If an E2E-VIV system is constructed using these specific technologies, then point-and-click deployment and management becomes a possibility even for LEO offices that have limited IT resources. In this technical setting, the operational aspects of E2E-VIV are feasible.

8.2 NON-TECHNICAL FEASIBILITY ANALYSIS

Non-technical feasibility of E2E-VIV systems will be primarily decided in the realms of law, politics, finance, public perception, and business interests. In particular, if any of these sectors is fundamentally opposed to any of the key features of E2E-VIV systems, then deployment of E2E-VIV systems is infeasible. The examples below are based upon discussions within the election integrity community, media reporting about Internet voting, and and reflections upon past activities within legislatures worldwide.

8.2.1 LAW

In the U.S., legislators must change the legal framework of elections in nearly every jurisdiction that wishes to use Internet voting. Historically, legislatures are comfortable with introducing Internet voting trials, particularly for UOCAVA voters. Providing technology that helps disabled voters is commonplace.

However, legislatures often permit or mandate the use of new election technologies with little restriction on their form, substance, and impact. This creates serious problems. Legalizing Internet voting without mandating end-to-end verifiability, or permitting large-scale Internet voting without first evaluating the impact and success of E2E-V in polling places and in small-scale Internet voting trials, could have disastrous consequences.

Based upon historical evidence, a gradual evolution of state and local election law—particularly facilitated by the local nature of elections—seems feasible in a 5–10 year time frame.

A subsequent research and development phase of this project should include concrete legal recommendations for state and local legislators. These recommendations must ensure that the legal framework for Internet voting deployment is rational, evidence-based, and legally mandates the requirements set forth in this report.

8.2.2 POLITICS

In the main, politicians and elected officials want to be perceived as forward-thinking and modern. Thus, it is not uncommon for those running for office to support new election technologies such as Internet voting. On the other hand, political parties and powerful political special interest groups are motivated by other factors.

The hypothetical implications of widespread trustworthy use of E2E-VIV—particularly the possibility of increased broad-spectrum voter participation—are potentially at odds with the agendas of some political actors.

As a result, the political feasibility of E2E-VIV is an open question. Only time will tell.

8.2.3 FISCAL

The cost of developing and deploying previous non-E2E Internet voting systems is often not part of the public record. Evidence indicates that the cost of each voting system deployed in the U.S. (SERVE), The Netherlands (KOA and RIES), Norway (with Scytl), Estonia, France, Switzerland, and Australia (iVote in New South Wales and vVote in Victoria) ranges from approximately one and a half million to tens of millions of dollars. It is reasonable to expect that creating an E2E-VIV system as stipulated in this report would cost several million dollars.

Given the continuous flow of investment into elections, and the comparatively similar development cost of an E2E-VIV system, it could be considered fiscally feasible to invest in this type of innovation. Just over 3 billion dollars have been spent on elections via HAVA, the cost of non-E2E voting machines from traditional vendors is several thousand dollars per machine, and the average cost per vote in today's elections, depending upon the jurisdiction, ranges from $2 to $10 per vote.

With current election costs, an open source E2E-VIV system—even if licensed and supported at reasonable costs by commercial organizations—will likely be extremely cost-effective in the medium-to-long term. Unfortunately, federal and state funding for election technology is currently difficult to find. The U.S. Congress has no interest in expanding budgets for elections. The debate around the elimination of the Election Assistance Commission, whose yearly budget is only just over ten million dollars, illustrates this fact. States and local municipalities have tight budgets. We cannot expect any single state or municipality to fund future phases of the E2E-VIV project.

The fiscal feasibility of E2E-VIV depends, then, on non-governmental enetities that have both financial resources and an interest in the speculative impact of widely available E2E-VIV. These include non-profit foundations, wealthy individuals, and existing and new vendors that are willing to invest millions of dollars into the research and development of E2E-VIV.

8.2.4 INTEGRATION

Regarding the operational issues discussed in Section 8.1.5, an important question is whether jurisdictions' IT staff or their contractors (see Section 8.2.5, below) will be capable of integrating an E2E-VIV system into their existing technical and election workflows.

Existing Internet voting products have serious integration challenges because of their own proprietary designs and the many proprietary data formats and protocols in Election Management Systems. This situation is, in part, the motivation for the interoperability requirements of Section 4.1.8, which state that open protocols and data standards must be used and respected in any E2E-VIV system.

This idea is further strengthened by the rapid progress of the IEEE 1622 working group that focuses on standardizing election data formats and protocols [34]. Existing and new vendors are planning to revise their products to conform to the IEEE standards, especially since it is likely that a future VVSG revision will mandate their use.

For this reason, integrating E2E-VIV systems with existing local and state elections systems seems feasible.

8.2.5 BUSINESS

Election officials have historically been reluctant to develop their own technology or to rely upon technologies that do not have a significant commercial support business infrastructure. Any new IT system requires support services to cover system evolution, support, maintenance, integration, and training.

A healthy systems market will sustain the growth of an IT support infrastructure and surrounding services, including value-added resellers, system integrators, and consultants. A distribution channel and value-added support infrastructure is necessary for E2E-VIV systems to be widely accepted and deployed.

Whether such a market will develop and, if so, whether it will be a competitive market is a critical question. Given recent shifts in the elections marketplace, especially with the entrance of a new generation of vendors and technologists, we believe it is feasible that a healthy business ecosystem will emerge over the next decade.

8.2.6 PUBLIC ACCEPTANCE

The final and most crucial feasibility question for E2E-VIV is that of public acceptance. Independent of any technological or political decision, if voters do not trust the election system, they will not trust their elected leaders or their democracy.

Our initial usability study, as well as case studies in the U.S. and elsewhere, shows that the general public usually welcomes new election technology. In general, voters believe that election officials know what they are doing and that if they have chosen to deploy a new election technology, the technology must be a good one.

Trust, however, can easily break. Much of the public currently distrusts IT systems that are responsible for citizen data or services, especially since security failures of government systems and those of private companies are often in the news.

Government agencies responsible for these systems have an even harder time earning and maintaining trust. Distrust is prevalent both in government employees that must use government systems and in citizens whose private information is stored in government systems.

Earning and maintaining public trust in E2E-VIV systems will require an extraordinary amount of transparency and strategy, and will take a long time.

Because E2E-VIV systems' correctness and security rely upon deep mathematical and computer science foundations, very few citizens can directly understand them and come to trust them by reading the literature for themselves. Non-experts will always have to trust in the work of experts who develop E2E-VIV systems. The feasibility of public acceptance therefore depends on the trustworthiness of those experts and the evidence that they, and the E2E-VIV system itself, can produce.

8.3 INTEGRATED FEASIBILITY ANALYSIS

This chapter's analysis provides us with the necessary components to evaluate the overall feasibility of building and deploying a practical E2E-VIV system for U.S. elections.

All technical aspects—engineering for correctness and security, design and engineering for usability, availability, operational—are feasible, though difficult.

Feasibility of the non-technical aspects ranges from unknown to entirely possible. With respect to law, feasibility is contingent upon legislators, election officials, and social pressure from voters. The financial, research, integration, and business aspects are relatively straightforward, and thus feasible.

The most important open question relates to the main challenge of any modern IT system: how do people and software relate?

The politics and public acceptance of Internet voting are open questions. We believe that only the disciplined, transparent, scientific, and practical pursuit of E2E-VIV can convince the public that E2E-VIV systems deserve their trust.

In summary, it is feasible to pursue future phases of this project. We discuss our final recommendations in our concluding chapter.

CHAPTER 9

CONCLUSION

There is tremendous pressure to build Internet voting systems and use them in public elections. Researchers, developers, and election officials must take the time to understand the requirements for secure and trustworthy elections so that they can evaluate systems—both good and bad—and make well-informed decisions. The use of flawed election systems in public elections can result in significant and irrevocable harm.

This report presents the most complete set of requirements to date that must be satisfied by any Internet voting system for public elections. This set of requirements, described in Chapter 4 and published in complete detail in a separate document [36], is useful to several audiences:

- *legislators* and their staffs who may craft laws that relate to remote elections, particularly Internet elections and elections for overseas, military, and disabled voters;
- *election officials* who may specify, evaluate, or purchase Internet voting products or services;
- *activists* who wish to better understand, and advocate for, E2E-VIV systems;
- *standards bodies* that may standardize various classes of Internet voting technologies, and specify the level of rigor for certifying Internet voting systems;
- *testing organizations* that may test Internet voting systems for compliance with technical standards;
- *researchers and engineers* who may continue working toward viable E2E-VIV systems.

This report and the expanded technical report also contains additional information useful to a subset of these audiences, including:

- a basis for developing the cryptographic foundations with which to evaluate and compare various E2E protocols and E2E-VIV systems (Chapter 5),
- an analysis of the architecture space of E2E-VIV systems (Chapter 6),
- precise recommendations on the state of the art for rigorous engineering of E2E-V systems (Chapter 7),
- a framing for an ongoing discussion about the feasibility of designing, constructing, certifying, legalizing, and deploying E2E-VIV systems (Chapter 8), and
- a reflection upon the outstanding issues that must be addressed in future stages of E2E-VIV development, including political, legal, research, and engineering challenges (Section 9.2).

Following are recommendations and possible next steps.

9.1 RECOMMENDATIONS

The E2E-VIV Project team does not assert that Internet voting *must* be pursued, nor does it assert that Internet voting must *never* be pursued. There is no consensus among the team members for either of these positions. With this understanding, the project team recommends the following.

Recommendation: E2E-V **Any public elections conducted over the Internet must be end-to-end verifiable.**

The use of Internet voting systems without end-to-end verifiability—including all Internet voting systems that jurisdictions are experimenting with and using at the time of this writing—is irresponsible. Any voting systems used to conduct public elections over the Internet must be E2E-VIV systems.

Recommendation: SUPERVISED FIRST **No Internet voting system of any kind should be used for public elections before end-to-end verifiable in-person voting systems have been widely deployed and experience has been gained from their use.**

It is critical to gain experience with E2E-V in the simpler in-person setting before attempting to deploy it in the vastly more complex Internet setting. Using E2E-V for in-person elections will also improve the integrity of existing in-person voting systems.

If election officials and election system vendors ignore these first two recommendations, we expect that deficient, unverifiable Internet voting systems will be widely used within ten years. Vendors will claim to have solved the security problems, and eager officials will believe these claims. Elections may be altered with no public awareness. If election officials manage to find evidence left by a careless attacker after altering an election, the damage will have already been done.

In making these first two recommendations, we realize that we have created a difficult path to follow. We assert that no attempt at Internet voting should deviate from this path. Building an in-person E2E-V system is no small task. Building an E2E-VIV system that satisfies the requirements in this report is even more ambitious; it may even be impossible. However, if it is possible, the resulting system will be far better than the vulnerable Internet voting alternatives.

Recommendation: HIGH ASSURANCE **End-to-end verifiable systems must be designed, constructed, verified, certified, operated, and supported as high-assurance systems according to the most rigorous engineering requirements of mission- and safety-critical systems.**

A software independent voting system does not rely on high-assurance software to detect errors in the election outcome. However, high-assurance software engineering tools and techniques can make such errors much less likely to occur, and can also reduce the risk of the following problems:

1. **PRIVACY VIOLATIONS.** While E2E-V systems can identify and mitigate issues of election integrity, they cannot do the same for privacy issues. A poorly-implemented E2E-V system will allow observers to detect certain issues with the election (such as votes not being counted correctly), but not to detect when voter identification details are stolen from an insufficiently secured server.
2. **PROGRAMMING ERRORS.** A low-quality E2E-V system is far more likely than a high-quality one to have software engineering flaws in design, functionality, security or other areas that trigger failures in verification. These will increase the burden on election administrators to deal with partial failures. This could also significantly impact the voters' trust in the election process, as well as the election administrators, apparatus, and outcome.

3. **SECURITY ISSUES.** Low-quality implementations of any type of software system are extremely difficult—and often impossible—to secure in the presence of insider or outsider attack. Security is not a band-aid to apply to a poorly-implemented system; it can only be achieved through a combination of rigorous process, method, design, implementation, validation, verification, deployment, and operation.

High-assurance software engineering is the only reasonable way to attempt to implement an E2E-V system that is correct, secure, and does not have enormous fiscal and trust implications for election officials after deployment. A less rigorous development approach will almost certainly lead to costly defects.

Recommendation: UNIVERSAL DESIGN **E2E-VIV systems must be usable and accessible.**

It is not feasible to make voting easy for voters with the most extreme disabilities. However, it is essential that we at least serve voters who have challenges in vision, hearing, comprehension, or motion yet can still use some kind of computing device. We should use a qualitative and quantitative testing-based experimentation platform to assess usability and accessibility, and follow best practices [2], recommendations [50, 60, 61], and standards [4] in accessible UI design and implementation. By doing so, we will be able to service nearly every overseas and military voter and, in the long term, the more than 84 million disabled voters in the U.S. [56].

We must also look to, and learn from, the AnywhereBallot and EZ Ballot experiments [8, 38] of the Accessible Voting Technology Initiative [1]. We must engage with the researchers and attendees at the annual California State University, Northridge International Technology and Persons with Disabilities Conference [35]. Only through direct engagement with voters, both abled and disabled, can we have any hope of understanding how to develop a usable, accessible E2E-VIV system.

Recommendation: MOVE FORWARD **Many challenges remain in building a usable, reliable, and secure E2E-VIV system. They must be overcome before using Internet voting in public elections. Research and development efforts toward overcoming those challenges should continue.**

Building a usable, reliable, and secure Internet voting system may be impossible. Solving the remaining challenges, however, would have enormous impact on the world. Continued research and development efforts must be conducted transparently, with all results and artifacts open to peer review. Internet voting systems, including E2E-VIV systems, must not be deployed in public elections before all the key security problems are resolved.

9.2 NEXT STEPS

To carry out these recommendations, legislators, researchers, and engineers face several challenges.

9.2.1 POLITICAL AND LEGAL CHALLENGES

The greatest concern voiced by election verification scientists, election integrity advocates, and E2E-V researchers is that legislators will mandate the experimentation with—or use of—Internet voting before a correct, secure, open, usable, accessible E2E-VIV system exists. Using the current untested and unverified systems opens the door to wholesale election manipulation or failure. Aggressive early adoption of election technology must be tempered by a clear understanding that voters' trust in their elections is hard-won and easily lost.

Scientists and election integrity advocates are also very concerned that well-meaning legislators and election officials will push to deploy Internet voting systems too early and too quickly, based on misleading information from prospective vendors and other advocates that is not balanced with *independent* advice from cybersecurity experts. They may also misunderstand how the security risks grow with the scale and significance of the election, and how these risks change over time as the threat environment changes. Such misjudgments may sometimes induce legislators and election officials to weigh political goals more highly than the security risks.

The political and legal challenges—and related opportunities—should focus on how to legislate the evidence-based measured introduction of new elections technologies. This includes Internet voting. *Defining an appropriate pace, milestones, and success criteria for the introduction of E2E-VIV systems must be a primary focus of any next phase of this project.*

9.2.2 RESEARCH AND ENGINEERING CHALLENGES

Although E2E-V is necessary for a viable Internet voting system, use of E2E-V does not ensure that an Internet voting system is free from vulnerabilities. Also, the definition of an E2E-VIV protocol for U.S. elections is very challenging. In particular, the research community must determine how to address five key challenges:

- how to handle large-scale dispute resolution;
- how to authenticate voters for public elections;
- how to defend an E2E-VIV system against denial-of-service attacks and automated attacks that aim to disrupt large numbers of votes;
- how to make verifiability comprehensible and useful to the average voter; and
- how to avoid voter coercion and vote selling in the context of digital observation of voting and verification.

The usability facets of E2E-VIV are also challenging. The main issues with usability are:

- how to ensure usable vote privacy and vote integrity in the presence of client-side malware and
- how to ensure that verification is usable and accessible to the typical set of voters.

While some of these issues can be addressed by current technologies, further research is necessary to determine if all of these concerns can be adequately addressed, as discussed at length in the preceding chapters and as codified in our requirements. *Until researchers adequately address these challenges, Internet voting systems should not be used in public elections.*

The development and deployment of a high-assurance distributed system of the scale and import of a public E2E-VIV election system has never been attempted. It involves considerable engineering challenges in addition to the fundamental research challenges already mentioned. *If the research issues can be solved, current best practices for building high-assurance distributed systems should be sufficient to address the engineering issues.*

9.2 CODA

Many people believe that Internet voting will increase voter participation, help with voter decision-making and engagement, provide equal opportunity for voters with disabilities, and decrease election costs.

Proponents of E2E-V election systems hope that their adoption will prevent corrupt election officials and governments from manipulating election outcomes, and will truly capture the voice of the people and increase confidence and trust in government.

Trustworthy democracy is a worthwhile goal, and we should strive to achieve it. The only responsible way to make progress is to continue peer-reviewed research and experimentation.

Appendix A

EXPERT STATEMENTS

The following expert statements are all included unedited, in their entirety.

A.1 JOSH BENALOH AND CONCURRING EXPERTS

RONALD L. RIVEST, PHILIP STARK, VANESSA TEAGUE, CONCURRING

THE VIABILITY OF RESPONSIBLE INTERNET VOTING

Remote voting[1] entails significant risks above and beyond those of in-person poll-site voting. Included among these are risks to integrity – as remotely-cast ballots may pass through numerous hands without independent observation – and risks to privacy – as voting takes place without the benefit of publicly-enforced voter isolation.

Internet voting substantially exacerbates the risks of remote voting by making it possible for small problems to be magnified and replicated on a large scale. Careless or malicious errors, intrusive malware, and unforeseen omissions – all of which can be caused by individuals or very small groups – can cause very large numbers of votes to be changed and the privacy of large numbers of voters to be compromised.

The technology known as end-to-end (E2E) verifiability allows individual voters to verify that their intended votes have been properly recorded and that all recorded votes have been properly counted. When applied to in-person voting, E2E-verifiability provides new assurances to voters by allowing them to check for themselves that the results of an election are correct. When applied to Internet voting, E2E-verifiability mitigates some of the risks described above – but does not eliminate them: voters are able to check that their ballots are properly recorded and counted, but malware can still compromise privacy, prevent voters from casting their ballots, and otherwise hinder voters.

Although E2E-verifiable election technologies have existed for more than thirty years, their use has thus far been limited to small demonstration systems and private elections for student governments, professional societies, and the like. E2E-verifiable elections produce new challenges and complications for implementers and administrators. They represent a new and different paradigm for elections – substantially replacing the notion of verification of election equipment with that of verification of the integrity of individual elections. As such, it is important to act deliberately and gain experience with E2E-verifiability in more manageable environments before attempting to deploy E2E-verifiable elections in their most challenging environment: the Internet.

These realities lead us to two principal conclusions.

[1] Remote voting is defined here as voting without the benefit of the public monitoring that takes place in a traditional poll site.

- Public elections should not be conducted over the Internet using systems that are not end-to-end verifiable.
- End-to-end verifiable Internet voting systems should not be used before end-to-end verifiable poll-site voting systems have been widely-deployed and experience has been gained from their use.

The second of these two principles is also necessitated by the fact that an E2E-verifiable election must have a tally to verify, and if an E2E-verifiable system is used only for remote voters, then the votes of these remote voters must be separately tallied and reported. Few jurisdictions are willing to segregate and report the tallies of local and remote voters separately.

We take no position here as to whether the integrity benefits of E2E-verifiability and the privacy benefits it makes possible outweigh the risks of remotely-executed large-scale corruption of an Internet-based election, but we are agreed upon the conclusions that "naked" Internet voting is dangerous and irresponsible and that E2E-verifiability should be deployed in the less risky and more manageable scenario of in-person poll-site voting before it is deployed in the wilds of the Internet.

A.2 DAVID JEFFERSON AND CONCURRING EXPERTS

CANDICE HOKE, RONALD L. RIVEST, BARBARA SIMONS, PHILIP STARK, AND VANESSA TEAGUE, CONCURRING

A.2.1 ELECTION SECURITY IS NATIONAL SECURITY

In a democracy election security is a key part of national security. The very legitimacy of government depends on the fact, and also the public perception, that the outcome of every election fairly represents the will of the people. We must be assured that no part of the voting process is unfairly manipulated to produce a different outcome, that all and only those who are eligible to vote have the opportunity to do so, that no one votes more than once, and that the privacy of the ballot is not compromised.

In this paper we demonstrate that while end-to-end verifiable (E2E-V) voting systems have a great deal to offer, but when they are embedded in an Internet voting context (E2E-VIV) they still do not provide sufficient security to prevent remote attackers from silently modifying votes and changing the outcome of elections undetectably, or from disrupting the election and disenfranchising a large number of voters. Fundamental security problems remain with E2E-VIV systems for which there are no practical solutions in sight and that will not be resolved in the foreseeable future.

A.2.2 VERIFIABILITY

Election security depends on *verifiability*. After an election is closed there must remain enough evidence for anyone who doubts the results to re-examine and rationally determine whether the winners were called correctly. We need to verify that only eligible voters voted, that no votes were lost, or duplicated, or modified, that no phony votes were inserted, that every eligible voter who tried to vote was able to do so, and that all the votes were counted correctly, once and only once. That evidence trail has to be *end to end*, spanning the entire data path through which the ballot data travels, from the voters' heads to the final result. We must be able to reconstruct the vote totals (or statistically audit them) from the original unmodified ballots or copies of those ballots that are provably identical to the originals as intended by the voter.

The traditional approaches to verifiability are all based on physically secured and indelible paper ballots (or paper cast vote records) that can be recounted or audited by humans without having to trust any software or complex machines. The goal of end-to-end verifiable (E2E-V) systems is to use cryptographic protocols to achieve for all-electronic voting systems the same (or higher) level of confidence in the election outcome for electronic voting systems as is achievable with paper-based systems. The goal of end-to-end verifiable *Internet voting* (E2E-VIV) systems is the same, but specifically extended to the much more difficult security context of remote voting from private platforms and devices over the public Internet.

Some approaches to end-to-end "verification" at first sound great, but fall far short. It is not sufficient, for example, to provide a feature whereby each voter can verify that her own ballot was correctly transmitted to the server over the Internet. First, it is difficult to provide verification capability without also making it possible for the voter to prove to a third party how she voted, thereby enabling automated vote selling and voter coercion. But even if that problem were resolved and if every voter verified that her voted ballot was properly received, it would still not be possible to demonstrate that no phony votes, unassociated with any actual voter, were inserted.

A.2.3 THE POWER OF E2E-V SYSTEMS

End-to-end verifiable voting systems are a major conceptual and mathematical step forward from conventional voting systems. Through advanced cryptographic techniques these varied systems, while differing in many ways in their architecture and in the roles of insiders, share the following fundamental security properties:

a) **INTEGRITY.** Once a voter successfully enters her ballot into the E2E-V system it cannot be undetectably lost or modified in any way, even in the presence of bugs or malicious logic.

b) **PRIVACY.** Once a ballot enters the E2E-V system it is encrypted, so that there is no way that the privacy of the ballot to be violated subsequently.

c) **COUNTING ACCURACY.** The ballots cannot be miscounted without that fact being detectable.

d) **UNIVERSAL PUBLIC VERIFIABILITY.** The systems output and publish sufficient verification data so that *anyone* can verify that no ballots were lost or modified and that the votes were properly counted. The verification data provides essentially a *cryptographic proof* that ballot integrity was preserved and the counts are correct. Anyone is free to run a verification program over the verification data to confirm it. You don't even have to trust the official verification program—you can use one from a source you trust, or if you have the skill you can write your own.

e) **OPENNESS AND TRANSPARENCY.** The code for E2E-V systems is generally open source. The mathematical principles underlying the E2E-V security guarantees have been vetted by many cryptographic experts and are open and public. And the specifications for proof checkers are also publically documented so that mutually suspicious political groups can hire their own experts whose independent election verification programs, if correct, must agree.

These powerful E2E-V security properties are not shared by any traditional voting system. In a precinct voting context they make E2E-V systems essentially invulnerable to ordinary software bugs, to malicious code inside (but not outside) the voting system, to transient hardware faults, and to most kinds of insider fraud (at least without a large conspiracy). Such failures will at least be detected because any lost or modified ballots and any miscounts will be flagged whenever anyone runs a verification program. This is in strong contrast to other forms of purely electronic voting systems which are unverifiable, and in which bugs or malicious logic can cause errors that are totally undetectable. The wrong people may wind up taking office without anyone knowing that the election results were incorrect.

For these reasons it is appropriate to consider E2E-V systems in any electronic voting situation. E2E-V adds truly powerful security guarantees, particularly in a precinct voting situation where voter authentication is done in person and where we have good reason to presume that the certified software in the voting machines is not malicious.

But as we explain in the next section, these E2E-V security guarantees *do not fully extend to Internet voting systems*. E2E-V Internet voting systems (E2E-VIV) have exploitable security holes for which there are no good solutions today and that preclude them from being suitable for use in public elections for the foreseeable future.

A.2.4 REMAINING UNSOLVED SECURITY ISSUES WITH E2E-VIV SYSTEMS

Once the voters' choices are safely input to a precinct-based E2E-V system many, but not all, of the security guarantees described in the last section follow directly. But that is a key qualification: these guarantees begin *once the voters' choices are safely input to the E2E-V system*, but not before. Unfortunately, when an E2E-V system is embedded into the Internet voting context as an E2E-VIV system, new security problems appear that the E2E-V guarantees do not address and that cannot, with any current technology, be fixed. The problems with E2E-VIV systems arise *before the votes even enter the system*. In this section we enumerate the remaining difficult security problems that will have to be solved definitively before we can consider deploying an E2E-VIV system.

VOTER AUTHENTICATION

A central issue with all remote, online voting systems is voter authentication. The voting system must be able to positively identify the voter in strong a way, so that it is essentially impossible to avoid the authentication process, and impossible to fool it so that an ineligible person is allowed to vote or that someone can fraudulently impersonate another voter.

Voter authentication is not part of an E2E-VIV system, but is a separate security issue. Unfortunately it is a very difficult and complex problem that remains unresolved (in the U.S. at least) for the foreseeable future.

Strong voter authentication is required for several reasons. Any online voting system must:

- verify that potential voters are duly registered or eligible to vote in the jurisdiction they attempt to vote in;
- prevent anyone from voting more than once; and
- resist vote selling, vote coercion, and proxy voting insofar as possible in a remote voting situation.

In an online voting system it is not sufficient to use the kinds of authentication commonly used in ecommerce situations, e.g. passwords, challenge-response systems based on personal information, or email-confirmations. These very weak authentication systems are more or less sufficient in commercial situations where secrecy is not so important, and where fraudulent transactions can be detected eventually and frequently be reversed or at least can be absorbed as a cost of doing business.

But in the national security context of an online election such weak authentication mechanisms will not suffice. If an attacker has the technical means to impersonate one voter, he can generally automate and amplify his methods to impersonate thousands of voters with very little additional effort. Almost every month we hear of huge data breaches at commercial or government institutions that have already allowed vast amounts of personal information on tens of millions of people to fall into the hands of criminals or foreign powers. Thus, any authentication mechanisms based on merely presenting personal information (name, address, account number, driver's license or social security number, mother's maiden name, etc.) is hopelessly compromised already, and way too weak for use in an election. Unfortunately some states have implemented such embarrassingly weak online authentication systems and have been forced to strengthen them, though they are still not sufficiently strong.

The traditional voter authentication method is based on wet ink signature matching. The voter is required, either in person at the precinct or on the envelope of a mail-in ballot, to duplicate with a new ink signature the old signature image on file from the time she registered to vote. In some states this is augmented with VoterID requirements at the polls. But there is no way to securely (unforgeably) input a wet ink signature image to a computer or mobile device and transmit it over the Internet for authentication with the ballot. Nor is there yet a way to securely and unforgeably transmit any of the usual VoterID documents.

Many people have suggested voter authentication systems based on biometrics such as fingerprints or retinal scans. For very good reasons too numerous to fully explain here none of these mechanisms is suitable for online voting. And it is important to note that while some mobile phones and tablets have fingerprint authentication devices built in, such systems authenticate the user to the device only. They do not authenticate the user to any remote service over the Internet, nor can they easily be extended to do so securely.

Other stronger, more technical authentication methods could be considered. Voters could be issued cryptographic ID cards such as the CAC cards issued to DoD personnel or like the national ID card of Estonia. Cryptographic ID cards would in principle enable voter authentication from any Internet-connected computer or device that could read them. But no U.S. state issues such IDs to its citizens or voters, and it seems unlikely that any will do so in the foreseeable future. Even if the security climate changes and people are willing to accept such an ID system, the startup and maintenance costs will be very high. Voters would have to buy computers or devices that could read the cards, and they would almost certainly have to be useful for other online purposes besides just voting in order to justify the costs involved to both the government and the voter.

The fact is that the U.S. has no strong, universally deployed online citizen identification and authentication system, and none is on the horizon. While strong remote voter authentication is not a fundamentally unsolvable problem, it is an immense practical problem that has to be dealt with before we can consider deploying any online voting system, including E2E-VIV systems.

CLIENT SIDE MALWARE

In an E2E-VIV system voters compose and input their vote choices on a privately owned (hence unsecured) platform, either a PC or mobile device. If the voting platform is infected with malware or spyware, it is complicated to prevent the votes from being modified or reported to a third party, and impossible to prevent them from just being thrown away by the malware before the ballot is encrypted and enters the E2E-VIV system.

The malware threat is ubiquitous now and is fundamental to all online voting systems. No device is safe from malware infection. No software safeguards such as commercial antivirus systems are very effective against it. There are hundreds of ways that malware can infect a voting platform, sometimes by sophisticated technical means and sometimes by tricking users into taking unsafe actions. There are hundreds of places in the huge multilayered software ecosystem of a PC or mobile device where malware can hide and be launched from. And there are thousands of hardware, OS, browser, combinations, and countless configuration choices—way too many for any possible comprehensive defense against malware. A modern PC or mobile device can easily contain software elements from a hundred different companies or open source development groups, any one of which may either be malicious or contain critical vulnerabilities that enables malicious code. Such vulnerabilities are so numerous that more are discovered all the time and vendors release security updates on a regular basis to plug the more recently discovered holes. E2E-VIV systems have no ability to prevent or even detect the actions of malware before the votes are safely submitted into the E2E-VIV software.

Malware in voters' computers can undermine the election in three fundamental ways.

i) **MALWARE MODIFICATION OF VOTES.** Malware may actually modify the voter's choices surreptitiously, before they are submitted to the E2E-VIV system. The techniques for accomplishing this without tipping off the voter will depend on the detailed architecture of the voting system, e.g. whether the client side is packaged as a full-blown application, or as a mobile app, or a Javascript script, or a browser plugin, or some other form. But in all cases the voter's choices must be input to the PC or mobile device in the clear, unencrypted, and be processed by a large amount of system software and application/browser/script software *before* it is encrypted and submitted to the E2E-VIV system. Regardless of the E2E-VIV architecture, with today's software tools it is reasonably straightforward for malicious code to modify votes undetectably before they are encrypted.

   Depending on the design of the E2E-VIV system, it may be possible for some voters to discover after the fact that different votes were recorded for them than the ones they thought they cast. But even so, there will generally be no way to prove to election officials that the voter did not cast the votes recorded for her by mistake, or cast them deliberately and then change her mind. Whether there is a remedy for voters who claim their votes are modified by malware and falsely recorded is an unresolved question.

We cannot generally eradicate the threat of malware. But in the special case of online voting there are techniques that in theory can prevent malware from surreptitiously modifying votes. Unfortunately they all involve additional burdens on the voter in the form of code voting, or special hardware devices independent of the PC, or a second independent communication channel to the election server that does not use the Internet, or at least is guaranteed to use an independent path from the one the votes travel. All known methods of working around client side malware involve some complication in the voting process that will be enough of a barrier, at least for the time being, to discourage many voters.

ii) **MALWARE VOTE PRIVACY VIOLATION.** Malware on a voter's computer or mobile device could allow her completed ballot to enter the E2EVIV system unmodified, but prior to that it could *also* send a copy of her votes to a third party. Unless a voter has considerable expertise and has special instrumentation running during the voting transaction there is no way for her to know it. And if the instrumentation was not in place before voting there is no after-the-fact test that can determine whether this happened, and certainly no way to reverse the privacy violation. If the voter is voting from a mobile device, as opposed to a PC, often no such instrumentation even exists today.

In any remote voting situation there is always the possibility that someone can physically look over a voter's shoulder and watch her vote. That is a risk we live with also with paper mail-in ballots. But the main concern is not with individual cases of privacy violation, but with widespread automated spying on many online votes.

Widespread vote privacy violation can undermine democracy in two major ways. First, in situations where some people have power over others (e.g. employers, commanding officers, union supervisors, parents, nursing home management) revealing who cast which ballot can be the basis for coercion or retaliation. This may not (yet) be a widespread concern in the U.S., but it certainly is in other countries.

Also, automated privacy violation can enable large scale, automated vote buying and selling. It is easy to imagine a scheme in which many voters are induced to sell their voting credentials, or to run a particular program while voting for a particular candidate in exchange for PayPal dollars or some other crypto currency such as Bitcoin that can be transmitted entirely online. The vote buying transaction would likely be totally undetectable by authorities. Even if the scheme eventually comes to the attention of authorities, the buyers may be long gone, or may be on foreign soil out of reach of U.S. law. In any case there would be no way to know how many votes were sold or who the sellers are. Technical tricks, such as allowing voters to vote multiple times online with only the last cast vote actually counting, are not effective when the attacker knows how the system works or when the voter cooperates in a vote sale.

As with malware that intends to modify ballots surreptitiously, there are workarounds that can prevent malware from surreptitiously revealing how someone votes to a third party. But again, they complicate the process of online voting sufficiently to be a barrier that will discourage many voters from voting

iii) **MALWARE DENIAL OF SERVICE.** The easiest and most intractable malware attack is one that simply prevents the voter from successfully voting. That can be done in many ways. The malware could make it appear that there was an error of some kind, which might be frustrating but hardly surprising to voters who might either blame themselves or their own flaky computers or attribute it to just another buggy online service. Alternatively, the malware might perfectly mimic a completed voting transaction, so that the voter believes she has successfully voted, whereas the malware would simply throw the ballot away.

Such a denial of service attack might not be very politically effective if it is applied to a random set of voters. But if it can be applied *selectively* to voters who would be likely to vote in a way that the attacker does not like, then it becomes a powerful partisan fraud tool. The malware writer may want to make a good guess as to how the voter will likely vote before deciding whether of not to block her from voting. Fortunately, there are many clues in a voter's computer or mobile device, such as browser history, to indicate at least a likely party preference or social class, and that is probably all the information the malware would need.

Some voters may be sophisticated enough to detect that their ballots were never included in the count, especially during the post-election verification stage when some might discover that there is no record that they voted. But any particular voter would find it almost impossible to prove to election officials that she actually tried to vote online but that malware prevented it. Perhaps she simply never really tried to vote, or

for some other technical reason not related to malware she had been prevented from successfully voting. There would be no evidence anywhere accessible to officials that could help them diagnose the situation. Even if the voter brought her computer in for forensic examination by experts, chances are that the malware would have erased evidence and erased itself, leaving no trace.

And finally, even if an obvious widespread malware denial of service attack were somehow discovered, there would be no way to estimate how many ballots were lost and how many voters were disenfranchised. The E2E-VIV system does nothing to help with such an estimate because the ballots are discarded by the malware before they ever enter the E2E-VIV system.

Unfortunately, while there are (at best inconvenient) workarounds for malware that aims to surreptitiously modify a ballot or send it to a third party, *there is fundamentally no workaround for malware designed to just prevent voting*. Well-designed malware would make the voter believe she had successfully voted, and she might never discover until it was too late that she did not. Even if she did discover it, the only recourse would be to vote from a different, uninfected PC or device, *but she almost certainly would not know that malware was the cause of the problem and would likely not know to vote from a different machine!*

Malware is a profound, absolutely fundamental problem that has been with us since the dawn of the PC age or before and will be with us for as far into the future as we can see. There is fundamentally no way to totally eradicate client side malware, or totally immunize against it, or even detect its presence. Malware is getting ever easier to write because templates, kits, libraries, and exemplars of successful malware are widely available to aid attackers, and because the payoff far exceeds the risks of getting caught. It is estimated that anywhere from 10 to 30 percent of all PCs in the world are infected with malware, and even more when spyware is included. And there are probably no reliable estimates as to the fraction of mobile devices similarly infected.

Finally, even if an easy to use, accessible workaround for client side malware is invented that preserves vote integrity and privacy, it will still not be possible to prevent a malware denial of service attack that just blocks voting. Such denial of service attacks are in a theoretically different category and there will never be a general way to thwart them all, nor a general way for voters or election officials to unambiguously recognize one. Even if it is recognized, there will be no way to estimate how many voters were affected.

The conclusion therefore, is that client side malware remains a fundamental threat that E2E-VIV systems cannot fully defend against.

NETWORK ATTACKS AND DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

E2E-VIV systems are client-server protocols that execute on top of several layers of other software, including the operating system and browser on the client side, the operating system and server complex on the server side, and the various levels of TCP/IP protocol stack all through the Internet, as well as routing protocols, DNS, NTP, DHCP, and also numerous other protocols used in wireless or mobile devices. The E2E-VIV system cannot work properly unless all of this other software works properly also. We have already discussed the problem of malicious logic on the client side. But E2E-VIV software is also attackable from the server side or from the Internet infrastructure software that the E2E-VIV software depends on.

There are many ways to attack an E2E-VIV election by maliciously modifying or configuring the software in the Internet. Such attacks are called *network attacks*. Any IT person who controls a router, DNS server, or another element of Internet infrastructure is in a position to prevent votes from getting to their destinations. On the positive side, E2E-VIV systems are partly robust against such network attacks in that they cannot result in votes being falsely injected or modified without detection. This is a clear advantage that E2E-VIV systems have over other Internet voting systems. However, there is no way to prevent a network attack from disrupting the E2E-VIV protocols in a way that causes ballots to be lost, i.e. undelivered. While this will also be detectable, the malicious loss of votes in transit cannot be prevented by an E2E-VIV protocol, and it may not be possible even to estimate the number of votes affected.

One especially dangerous form of network attack is the *distributed denial of service* (DDoS) attack. In this attack, an attacker floods the server (or some other subsystem) with so much traffic or other work that it either crashes the system or else slows it to such a crawl that it is effectively down. Voters would experience a DDoS attack on a vote server as either *extreeeeemly* long waits between steps in the voting process, or total nonresponsiveness of

the server, or some other error. The net effect is that large numbers of voters would simply be disenfranchised. The attack can be directed pointedly at the server side, in which case all online voters would be affected, or it could be selectively directed at certain parts of the Internet infrastructure that would affect only a subset of the voters.

We have to be able to defend online elections against DDoS attacks for two key reasons. First, they are about the easiest of all network attacks to perpetrate. There are many different kinds of DDoS attack against different parts of Internet infrastructure and different levels of software, and there are many kits available on the dark net to allow anyone from anywhere in the world to perpetrate a DDoS attack against almost any target. In fact, the means of DDoS attack are so routinized and ubiquitous that there are illegal businesses online that will conduct an attack to your specifications against any target you choose for a moderate price. You can ask for, say, a 50 gigabit per second attack for the last 4 hours on Election Day against the IP address of the (hypothetical) Cook County vote server. That would probably prevent anyone from voting online in that jurisdiction during those hours. All of those voters would be disenfranchised, but none of them would be able to prove that they were among of the victims, and election officials would not even be able to make a decent estimate of the number of ballots lost.

DDoS attacks have actually been used in real public elections around the world at least four separate times that have been made public. (Arizona Democratic Primary, 2000; Ontario NDP, 2003; Hong Kong people's election, 2012; NDP of Canada 2012). While there are various tools that can be used to *ameliorate* some DDoS attacks, there is no *general solution*, and the DDoS problem is so fundamental that there will probably never be one with the current architecture of the Internet. Vulnerability to DDoS attacks is effectively built in to its design. Hence, all E2E-VIV systems are vulnerable to network attacks that can result in disenfranchising a large number voters with no way of even measuring how many were affected. There is no fundamental defense against DDoS attacks.

A.2.5 CONCLUSION

E2E-V offers a dramatic improvement in the security of voting systems. While it is necessary for *any* online voting system for public elections, it is by no means sufficient. Once it is embedded in a larger *Internet voting* context fundamental new security vulnerabilities appear for which there are no solutions today, and no prospect of solutions in the foreseeable future. These include vulnerability to authentication attacks, client side malware attacks, and DDoS attacks that can be perpetrated by anyone in the world. Unless and until those additional security problems are satisfactorily and simultaneously solved—and they may never be—we must not consider any Internet voting system for use in public elections.

REFERENCES

[1] *Accessible Voting Technology Initiative*. URL: http://elections.itif.org/ (visited on 07/01/2015).

[2] *Accessible Voting Technology Initiative: Election Design Guidelines*. URL: http://elections.itif.org/resources/guidelines/ (visited on 07/01/2015).

[3] Claudia Z. Acemyan et al. "Usability of Voter Verifiable, End-to-end Voting Systems: Baseline Data for Helios, Prêt à Voter, and Scantegrity II". In: *The USENIX Journal of Election Technology and Systems* (2014), p. 26.

[4] *ADA Standards for Accessible Design*. URL: http://www.ada.gov/2010ADAstandards_index.htm (visited on 07/01/2015).

[5] Ben Adida. "Helios: Web-based Open-Audit Voting". In: *USENIX Security*. 2008. URL: https://www.usenix.org/legacy/events/sec08/tech/full_papers/adida/adida.pdf (visited on 07/01/2015).

[6] Ben Adida et al. "Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios". In: *USENIX EVT/WOTE*. 2009. URL: https://www.usenix.org/legacy/event/evtwote09/tech/full_papers/adida-helios.pdf (visited on 07/01/2015).

[7] *American Fuzzy Lop*. URL: http://lcamtuf.coredump.cx/afl/ (visited on 07/01/2015).

[8] *Anywhere Ballot*. URL: http://anywhereballot.com/ (visited on 07/01/2015).

[9] American Political Science Association et al. "Findings and recommendations of the special committee on service voting". In: *American Political Science Review* 46.2 (1952), pp. 512–523.

[10] David Bismark et al. "Experiences Gained from the first Prêt à Voter Implementation". In: *First International Workshop on Requirements Engineering for e-Voting Systems (RE-VOTE)*. IEEE. Aug. 2009, pp. 19–28. DOI: 10.1109/RE-VOTE.2009.5.

[11] Philippe Bulens, Damien Giry, and Olivier Pereira. "Running mixnet-based elections with Helios". In: *USENIX EVT/WOTE*. 2011. URL: http://www.usenix.org/events/evtwote11/tech/final_files/Bulens.pdf (visited on 07/01/2015).

[12] Craig Burton et al. "Using Prêt à Voter in Victorian State elections". In: *USENIX EVT/WOTE*. 2012. URL: https://www.usenix.org/system/files/conference/evtwote12/evtwote12-final9_0.pdf (visited on 07/01/2015).

[13] Michael D. Byrne, Kristen K. Greene, and Sarah P. Everett. "Usability of voting systems: Baseline data for paper, punch cards, and lever machines". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM. 2007, pp. 171–180.

[14] Richard Carback et al. "Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy". In: *USENIX Security*. 2010. URL: https://www.usenix.org/legacy/events/sec10/tech/full_papers/Carback.pdf (visited on 07/01/2015).

[15] Carter Center. *Internet Voting Pilot: Norway's 2013 Parliamentary Elections*. Mar. 2014. URL: http://www.cartercenter.org/resources/pdfs/peace/democracy/Carter-Center-Norway-2013-study-mission-report2.pdf (visited on 07/01/2015).

[16] David Chaum, Peter Y. A. Ryan, and Steve Schneider. "A Practical Voter-Verifiable Election Scheme". English. In: *Computer Security – ESORICS 2005*. Ed. by Sabrinade Capitani di Vimercati, Paul Syverson, and Dieter Gollmann. Vol. 3679. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2005, pp. 118–139. ISBN: 978-3-540-28963-0. DOI: 10.1007/11555827_8.

[17] David Chaum et al. “Accessible voter-verifiability”. In: *Cryptologia* 33.3 (2009), pp. 283–291.

[18] David Chaum et al. “Scantegrity II: End-to-End Verifiability by Voters of Optical Scan Elections Through Confirmation Codes”. In: *IEEE Transactions on Information Forensics and Security* 4.4 (Dec. 2009), pp. 611–627. ISSN: 1556-6013. DOI: 10.1109/TIFS.2009.2034919.

[19] David Chaum et al. “Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes”. In: *USENIX EVT*. 2008. URL: https://www.usenix.org/legacy/event/evt08/tech/full_papers/chaum/chaum.pdf (visited on 07/01/2015).

[20] U.S. Election Assistance Commission. *Election Administration and Voting Survey*. URL: http://www.eac.gov/research/election_administration_and_voting_survey.aspx (visited on 07/01/2015).

[21] *CompCert*. URL: http://compcert.inria.fr/ (visited on 07/01/2015).

[22] *Dafny: a language and program verifier for functional correctness*. URL: http://research.microsoft.com/en-us/projects/dafny/ (visited on 07/01/2015).

[23] Alex Delis et al. *Pressing the Button for European Elections 2014: Public attitudes towards Verifiable E-Voting In Greece*. June 2014. URL: https://drive.google.com/file/d/0B-mtbRwyPn_SdnpMRzBKcEZWUm8/view?usp=sharing (visited on 07/01/2015).

[24] *EasyCrypt: Computer-Aided Cryptographic Proofs*. URL: http://www.easycrypt.info/ (visited on 07/01/2015).

[25] Aleks Essex et al. “Punchscan in practice: an E2E election case study”. In: *Proceedings of Workshop on Trustworthy Elections*. 2007.

[26] *F*: A higher-order effectual language designed for program verification*. URL: https://fstar-lang.org (visited on 07/01/2015).

[27] Federal Constitutional Court of Germany. *Docket Nos. 2 BvC 3/07 & 2 BvC 4/07*. 2009. URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html (visited on 07/01/2015).

[28] Kristian Gjøsteen. “The Norwegian Internet Voting Protocol”. English. In: *E-Voting and Identity*. Ed. by Aggelos Kiayias and Helger Lipmaa. Vol. 7187. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, pp. 1–18. ISBN: 978-3-642-32746-9. DOI: 10.1007/978-3-642-32747-6_1.

[29] Rop Gonggrijp et al. “RIES - Rijnland Internet Election System: A Cursory Study of Published Source Code”. English. In: *E-Voting and Identity*. Ed. by Peter Y.A. Ryan and Berry Schoenmakers. Vol. 5767. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2009, pp. 157–171. ISBN: 978-3-642-04134-1. DOI: 10.1007/978-3-642-04135-8_10.

[30] Gerard J. Holzmann. *UNO: Static source code checking for user-defined properties*. 2002. URL: http://www.spinroot.com/uno/uno_long.pdf (visited on 07/01/2015).

[31] *How to Vote: Wombat Voting System*. URL: http://www.wombat-voting.com/how-to-vote (visited on 07/01/2015).

[32] Engelbert Hubbers, Bart Jacobs, and Wolter Pieters. “RIES - Internet Voting in Action”. In: *29th International Computer Software and Applications Conference (COMPSAC 2005)*. IEEE. 2005, pp. 417–424.

[33] Engelbert Hubbers et al. “Description and analysis of the RIES internet voting system”. In: *Report of the Eidhoven Institute for the Protection of Systems and Information*. Faculty of Mathematics and Computer Science Eindhoven University of Technology, June 2008.

[34] *IEEE 1622-2011 - IEEE Standard for Electronic Distribution of Blank Ballots for Voting Systems*. URL: http://ieeexplore.ieee.org/servlet/opac?punumber=6130554 (visited on 07/01/2015).

[35] *International Technology and Persons with Disabilities Conference*. URL: http://www.csun.edu/cod/conference/index.php (visited on 07/01/2015).

[36] Joseph R. Kiniry and Daniel M. Zimmerman. *E2E-VIV BON Specification*. URL: http://www.usvotefoundation.org/E2E-VIV/bon-specification.pdf (visited on 07/10/2015).

[37] Gerwin Klein et al. “seL4: Formal verification of an OS kernel”. In: *Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles*. ACM. 2009, pp. 207–220.

[38] Seunghyun Lee et al. “EZ ballot with multimodal inputs and outputs”. In: *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility*. ACM. 2012, pp. 215–216.

[39] Neal McBurnett et al. *Scantegrity Responds to Rice Study on Usability of the Scantegrity II Voting System*. Dec. 2014. URL: http://vote.caltech.edu/content/scantegrity-responds-rice-study-usability-scantegrity-ii-voting-system (visited on 07/01/2015).

[40] Michael P. McDonald. *United States Elections Project*. URL: http://www.electproject.org/.

[41] *Mirage OS*. URL: http://www.openmirage.org/ (visited on 07/01/2015).

[42] Judy Murray and Keith Instone. *E2E-VIV Usability Study Report*. URL: http://www.usvotefoundation.org/E2E-VIV/usability-study.pdf (visited on 07/10/2015).

[43] United States General Accounting Office. *Voters with disabilities: access to polling places and alternative voting methods*. 2001. URL: http://www.gao.gov/products/GAO-02-107 (visited on 07/01/2015).

[44] *OSCE/ODIHR Election Assessment Mission Report*. Nov. 2006. URL: http://www.osce.org/odihr/elections/netherlands/24322?download=true (visited on 07/01/2015).

[45] Stefan Popoveniuc and Ben Hosp. “An introduction to Punchscan”. In: *IAVoSS Workshop On Trustworthy Elections (WOTE 2006)*. Robinson College United Kingdom. 2006, pp. 28–30.

[46] Stefan Popoveniuc and Ben Hosp. “An Introduction to PunchScan”. English. In: *Towards Trustworthy Elections*. Ed. by David Chaum et al. Vol. 6000. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2010, pp. 242–259. ISBN: 978-3-642-12979-7. DOI: 10.1007/978-3-642-12980-3_15.

[47] Ronald L. Rivest and John P. Wack. *On the notion of “software independence” in voting systems*. Prepared for the TGDC, and posted by NIST at the given URL. July 2006. URL: http://vote.nist.gov/SI-in-voting.pdf.

[48] Noel H. Runyan. *Improving access to voting: A report on the technology for accessible voting systems*. 2007. URL: http://www.demos.org/publication/improving-access-voting-report-technology-accessible-voting-systems (visited on 07/01/2015).

[49] Peter Y.A. Ryan et al. “Prêt à Voter: a Voter-Verifiable Voting System”. In: *Information Forensics and Security, IEEE Transactions on* 4.4 (Dec. 2009), pp. 662–673. ISSN: 1556-6013. DOI: 10.1109/TIFS.2009.2033233.

[50] *Section508.gov: Opening Doors to IT*. URL: https://www.section508.gov (visited on 07/01/2015).

[51] *Security Review: Helios Online Voting*. Mar. 2009. URL: https://cubist.cs.washington.edu/Security/2009/03/13/security-review-helios-online-voting/ (visited on 07/01/2015).

[52] Claire M. Smith. *Convenience Voting and Technology: The Case of Military and Overseas Voters (Elections, Voting, Technology)*. Palgrave Macmillan, 2014. ISBN: 1137398582.

[53] Claire M. Smith. *Time to Move: Overseas and Military Voter State Policy Innovation*. 2011. URL: https://www.overseasvotefoundation.org/files/Time_to_MOVE_March2011.doc (visited on 07/01/2015).

[54] *The Haskell Lightweight Virtual Machine (HaLVM)*. URL: https://galois.com/project/halvm/ (visited on 07/01/2015).

[55] Georgios Tsoukalas et al. “From Helios to Zeus”. In: *USENIX Journal of Election Technology and Systems* 1.1 (Aug. 2013). URL: https://www.usenix.org/jets/issues/0101/tsoukalas (visited on 07/01/2015).

[56] *United States Census Bureau*. URL: http://www.census.gov/ (visited on 07/01/2015).

[57] U.S. Election Assistance Commission. *UOCAVA Pilot Program Testing Requirements—August 25, 2010*. Aug. 2010. URL: https://www.fvap.gov/uploads/FVAP/VSTL_AppendixB.pdf (visited on 07/01/2015).

[58] *Verasco*. URL: http://verasco.imag.fr/ (visited on 07/01/2015).

[59] *Verified Software Toolchain*. URL: http://vst.cs.princeton.edu/ (visited on 07/01/2015).

[60] *Web Accessibility Evaluation Tool*. URL: http://wave.webaim.org/ (visited on 07/01/2015).

[61] *Web Accessibility Initiative*. URL: http://www.w3.org/WAI/ (visited on 07/01/2015).

[62] Filip Zagórski et al. “Remotegrity: Design and Use of an End-to-End Verifiable Remote Voting System”. English. In: *Applied Cryptography and Network Security*. Ed. by Michael Jacobson et al. Vol. 7954. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2013, pp. 441–457. ISBN: 978-3-642-38979-5. DOI: 10.1007/978-3-642-38980-1_28.

ABOUT U.S. VOTE FOUNDATION

U.S. Vote Foundation (US Vote) and its initiative, Overseas Vote, are dedicated to bringing a comprehensive range of best-in-class voter services to U.S. citizens residing within the U.S., living abroad or serving in the military. US Vote's exclusive Voter Account application supports voters' ongoing participation in the electoral process. Through its hosted systems program, US Vote helps states, campaigns and voter outreach organizations offer their own customized online voter services. US Vote is poised to respond to the growing need for research and development of alternatives to polling place voting. U.S. Vote Foundation is a 501(c)(3) nonprofit, nonpartisan public charity incorporated in Delaware.

For additional information on U.S. Vote Foundation, please visit www.usvotefoundation.org.

For additional information on the Overseas Vote Initiative, please visit www.overseasvote.org.

ABOUT GALOIS

Galois specializes in the safety, security and reliability of critical hardware and software systems where failure is unacceptable. We apply a solid foundation of mathematics, applied formal methods, and science to advance cryptography, language design, scientific computing, software correctness, mobile security, cyber-physical systems, and computer security.

For additional information on Galois, please visit www.galois.com.

ABOUT THE DEMOCRACY FUND

The Democracy Fund invests in organizations working to ensure that our political system is responsive to the public and able to meet the greatest challenges facing our nation.

For additional information on the Democracy Fund, please visit www.democracyfund.org.

WITH GENEROUS SUPPORT FROM THE

DEMOCRACY FUND

OF, BY, AND FOR THE PEOPLE