The Security of Remote Online Voting

A Thesis

In TCC 402

Presented to

The Faculty of the

School of Engineering and Applied Science

University of Virginia

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science in Computer Science

By

Daniel Rubin

March 27, 2001

On my honor as a University student, on this assignment I have neither given nor received unauthorized aid as defined by the Honor Guidelines for Papers in the TCC courses.

____

Approved ____________________________ Date __________________

Technical Advisor- David Evans

Approved ____________________________ Date __________________

TCC Advisor- Matthew Mehalik

Table of Contents

Abstract

The infeasibility of remote online voting can be shown through a security analysis of its previous uses and technological risks. My project focuses on two cases where voters cast their ballots over the Internet – the 2000 Arizona Democratic Primary and the University of Virginia Student Council Elections. I ran Student Council elections for two semesters and will recount my experiences as an elections administrator; Arizona will be evaluated based on reports and commentary of their online election. This project will also review the underlying technology that makes remote online voting possible and assess the security risks.

1 Introduction

"[It is] by their votes the people exercise their sovereignty." - Thomas Jefferson

America votes using antiquated technology. Equipment developed as early as the 1890s gets trucked out each November for the people to participate in democracy. 'One person, one vote' – a guiding principle of American suffrage – is devalued when votes are lost, miscounted, or erroneously discarded. Surely modern technology can save the country from this awful electoral predicament[HM00].

In light of the Florida 2000 Presidential Election, new technology can usher in an age of reliable and efficient voting systems. Elections should be rid of hanging chads, dimpled chads, and month-long recounts. A potential savior to voting technology could be the Internet. As 'www' and .com's become ubiquitous in American culture, voting online might seem realistic in the near future. But fears of automated voter fraud and electronic disenfranchisement could keep this from getting off the ground.

Previous uses of online voting demonstrate significant flaws, making it unsafe for legally binding public elections. The security risks related to remote online voting will prevent its deployment until a more secure online infrastructure can be developed. Two case studies emphasize the impotence of remote online voting to be both a secure and successful election medium - the 2000 Arizona Democratic Presidential Primary and the University of Virginia Student Council Elections. I learned first-hand about the flaws and risks of Internet voting from running the Student Council election and I have seen how professionals failed to run a secure online election from researching the Arizona case.

1.1 Problem Definition – What is Remote Online Voting?

This project will evaluate feasibility of remote online voting – which includes forms such as Internet voting. Remote online voting allows voters to cast their ballots from any Internet-connected computer or handheld device. This offers voters valuable convenience, allowing people to vote from their home or anywhere else they can access the Internet.

Electronic voting, which has been certified and used in elections, differs significantly from remote online voting. About 30 percent of voting precincts use electronic systems, including optical scanners and ATM-style interfaces[HM00]. None of the current electronically tabulated voting schemes provides remote voting except some forms of absentee voting. This report will focus only on Internet-based remote online schemes.

1.2 Rationale

How can the Internet help voting?

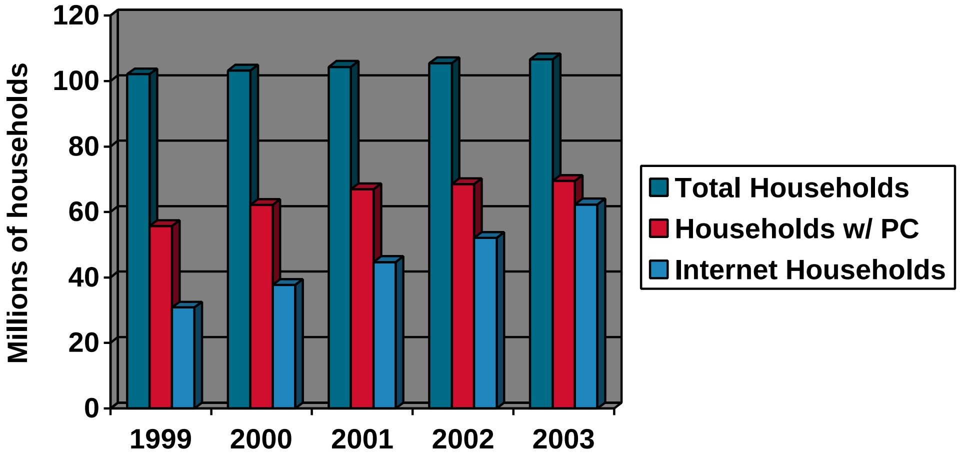
The Internet has achieved fast growth and a wide acceptance rate among Americans. Due to its broad acceptance, the Internet can reach a lot of voters and have positive influence on their voting preparation and participation[CAL00].

With the rise of Internet popularity, remote online voting can be seen as a natural progression, adapting our society to the best available technology. This technology can streamline the process and return results much faster than the mechanical systems currently in use [DR00].

Internet voting would be very convenient. As Figure 1 shows, the percentage of United States households with Internet access is projected to rise from 30% in 1999 to 58% in 2003[CAL00]. Convenient remote elections would lead to larger voter turnouts and a "stronger" electorate[DR00].

Figure 1 - Projected American Households with Internet Access (Millions)

[Dataquest and The Yankee Group, qtd. in CAL00]

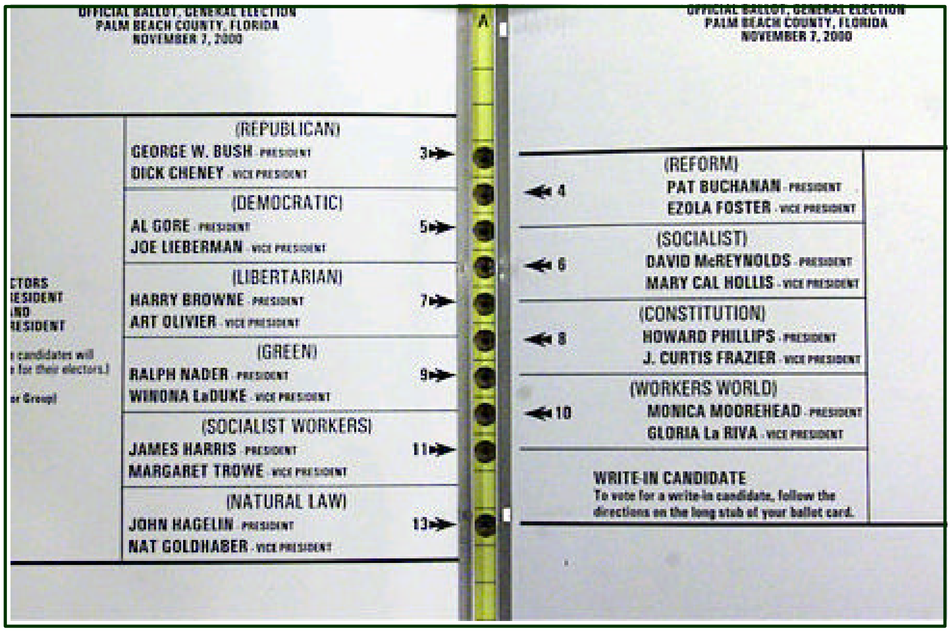


Any electronic voting method, including remote online voting, provides the means for fast and accurate tabulation of votes and does not have the known and accepted error present in physical voting methods[MN01]. Internet ballots can reduce the confusion of paper ballots. Computerized ballots can ensure voters do not vote for too many candidates and warn voters if they do not vote in a particular race[No00]. Simple, available tools can guarantee that the ballot represents the true intent of the voter. A well-designed Internet ballot should easily avoid the problems resulting from Palm Beach County's now infamous Butterfly Ballot, shown below[Sut00].

Figure 2 – The Palm Beach County Butterfly Ballot

The Palm Beach County Butterfly Ballot supposedly confused some voters by placing voting options on both sides of the ballot holes.

Image from [Wash00].



OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

CTORS
ESIDENT
ND
ESIDENT

candidates will
for their electors.)

or Group)

(REPUBLICAN)
GEORGE W. BUSH - PRESIDENT
DICK CHENEY - VICE PRESIDENT 3 ➤

(DEMOCRATIC)
AL GORE - PRESIDENT
JOE LIEBERMAN - VICE PRESIDENT 5 ➤

(LIBERTARIAN)
HARRY BROWNE - PRESIDENT
ART OLIVIER - VICE PRESIDENT 7 ➤

(GREEN)
RALPH NADER - PRESIDENT
WINONA LaDUKE - VICE PRESIDENT 9 ➤

(SOCIALIST WORKERS)
JAMES HARRIS - PRESIDENT
MARGARET TROWE - VICE PRESIDENT 11 ➤

(NATURAL LAW)
JOHN HAGELIN - PRESIDENT
NAT GOLDHABER - VICE PRESIDENT 13 ➤

OFFICIAL BALLOT, GENERAL ELECTION
PALM BEACH COUNTY, FLORIDA
NOVEMBER 7, 2000

◄ 4 (REFORM)
PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

◄ 6 (SOCIALIST)
DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

◄ 8 (CONSTITUTION)
HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

◄ 10 (WORKERS WORLD)
MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE
To vote for a write-in candidate, follow the directions on the long stub of your ballot card.

Why is security so important?

Remote online voting must prevent automated voter fraud. Fraud exists in most current paper voting systems because of the balance between eradicating fraud and a non-intrusive authentication system[CAL00]. For example, the 1993 National Voter Registration "Motor Voter" Act made voter registration extremely easy while accepting the possibility of having a few fraudulent voters registered as well[US00]. We should accept a nominal increase in fraudulent votes if it results from a larger voter turnout.

The secret ballot concept must be preserved for remote online voting. No one should be able to prove how a voter cast his or her vote, protecting secrecy and preventing vote selling[Cra96b]. Unfortunately, by taking the voter out of the poll site, election officials can not know if voters are being intimidated or influenced by third parties while casting their vote[HC01].

Malicious code attacks have the ability to undermine the entire system regardless of cryptographic protocol effectiveness. Viruses, worms, and Trojan horse attacks are difficult to prevent or detect, leaving a voter's ballot vulnerable to corruption without their knowledge[CAL00, Ru00]. These attacks can be automated and distributed quickly, tainting an entire election.

The immediacy of results, a benefit of electronic schemes, may be lost if the election does not provide a significant audit trail for conducting recounts. Any election equipment certified for public elections needs to have an accurate means for conducting recounts[CAL00]. The importance of audit trails can not be underestimated in light of the Florida recount of 2000.

Internet voting opens itself up to a host of security problems because the Internet is an insecure medium for communication [Cra96a, CAL00, MM00, Ru00]. Election officials "will not have full end-to-end control of the infrastructure for voting." [CAL00].

1.3 Project Scope

Condemning the feasibility of complex technology such as remote online voting cannot be done through research of purely theoretical models. Real world deployment of remote online voting shows how the weaknesses dominate, making remote online voting a risky proposition. This project will examine two uses of remote online voting – two schemes that fail if we consider security a paramount requirement.

The Case Studies

The first case study is the 2000 Arizona Democratic Primary – the first major use of Internet voting in a legally binding political election. I based my evaluation on accounts and commentary regarding what took place in Arizona during March 2000. Many things went wrong, prompting critics to declare remote online voting too risky for use in public elections[PS01]. However, the vendors claimed success and declared their product could be used for elections in the near future[MG01]. Controversy swirled as a watchdog group filed a lawsuit, customer service lines were perpetually busy, and people with old browsers or no computers were left out in the cold[Phi99]. This first real test of remote online voting left a lot of questions to be answered on what will be a hot topic for years to come.

The second case study strikes closer to home – the University of Virginia Student Council Elections. Running this election for two semesters has given me a better perspective on what makes an election work and how requirements fail in the real world. I managed the website, the Internet ballots, the Unix backend database MiniSQL, and worked with the Elections Committee to keep everything running smoothly.

In this case, a woefully insecure system succeeds because the University uses it on a small scale and the students trust the system. The University's honor system plays a much larger role than the web site for security, as the system cannot legitimately prevent automated voter fraud. The ballot options are clear and overvoted ballots cannot be cast. The elections committee can easily set up, manage, and tabulate votes on this system.

The Technology

This report will analyze the mathematical foundations to the cryptography used in remote online voting protocols. Remote online voting has its own computer security risks and many difficult obstacles to overcome before it can truly become a legitimate voting option[Ru00].

Analysis will begin with the RSA public key encryption algorithm – the basis of almost all voting protocols[FOO92, Cra96a, Sche96]. This report will look at some theoretical and practical protocols and how they satisfy voting security requirements. The requirements themselves will be examined, along with tradeoffs made when voting schemes get implemented.

Malicious attacks – the most significant technological risk to remote online voting – will be analyzed to determine the extent of the threat and possible consequences[Ru00]. Comparing attacks and defense mechanisms can shed some light on ultimate feasibility of remote online voting[MM00].

1.4 Project Roadmap

Our current voting scheme gains security through its physical nature – physical ballots, audit trails, and end-to-end supervision from voting officials. Internet voting takes those ends and blindfolds the government to exactly what goes on. The ends of the protocol that require human interaction open up security vulnerabilities. The future of remote online voting lies in securing those ends so legal ballots can safely make the trip and illegal ballots cannot.

Bruce Schneier, one of the nation’s authorities on cryptography and computer security, once said, “if you give me bits, I can secure them. It’s that human-bit interface that is going to cause you hardship. That’s where things are going to break”[Sche99].

The feasibility of Internet voting is a story about human-bit interfaces.

2 The 2000 Arizona Democratic Primary

A successful failure using online voting

"The image is that it was a successful process. [It was] successful only if you compare it to nothing. If you compare it to any official election held in the country, it would have been labeled a disaster." – Election Center director Doug Lewis [Bu00]

"Lacking clear and explicit guidelines, we therefore went to great lengths in Arizona to implement rigorous procedures and protocols to ensure ballot sanctity and universal accessibility." – election.com CEO Joe Mohen [MG01]

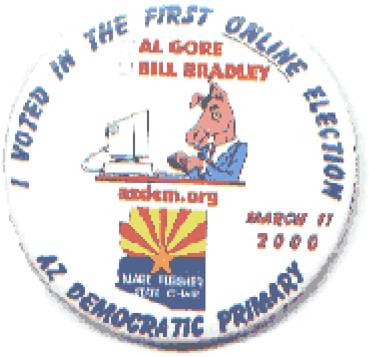


Image permission granted by www.azdem.org.

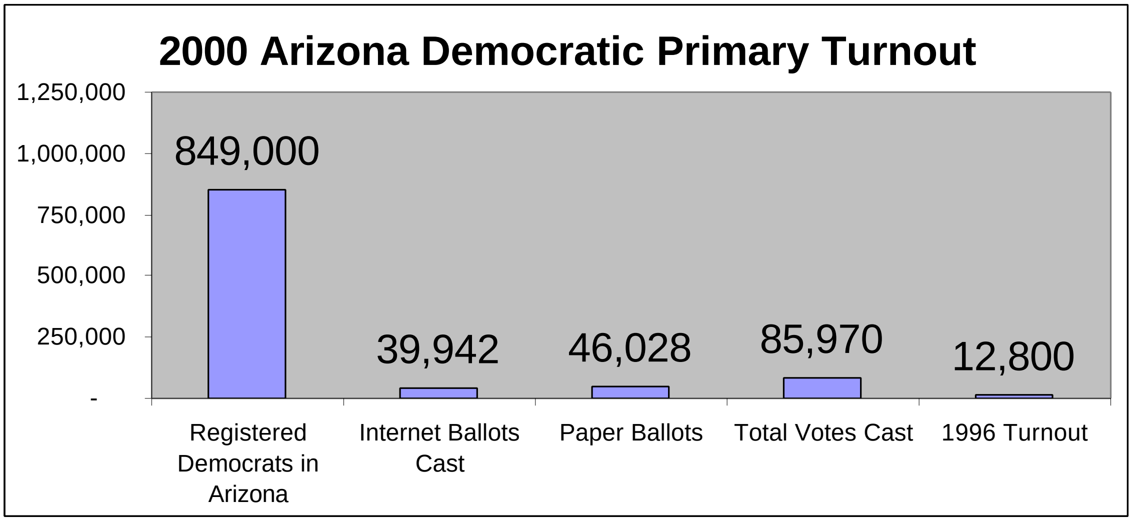
The 2000 Arizona Democratic primary brought America into a brave new world of Internet voting. Arizona Democratic leaders and their online election vendor ignored the requests of technological experts who warned that we were not ready for online voting. Minor technological aspects broke down, but claims of success resounded from the aftermath. Picking up the pieces of what went on reveals a lot about the feasibility of remote online voting.

In a state with a Republican governor, two Republican senators, and Republicans holding five of six seats in the House, the Arizona Democrats needed to do something to reinvigorate their party[Mat00]. When paired with an online election vendor that wanted to publicize its product, the result was lots of money being spent to generate excitement about Internet voting and the Arizona Democratic party[Led00b].

2.1 Four days in March that changed voting forever

March 7 began a new era for American elections. Registered Democrats in Arizona could cast legally-binding ballots for their presidential primary across the Internet from anywhere in the world. Up until March 10, voters could cast their ballots remotely across the Internet, all before the official Election Day of Tuesday March 11. On the 11th, voters could only cast ballots at polling locations, either physical or Internet ballots[MG01].

Figure 3 – Turnout in the 2000 Arizona Democratic Primary [Leb00b], [MG01], [Mat00].



As Figure 3 shows, the 2000 turnout was barely 10% and Internet votes only accounted for 46% of the votes cast. But comparing these numbers to the 1996 election, the turnout increase was six-fold. Internet voting can not assume all of the credit for the getting more voters out – Bill Clinton was unopposed in that essentially meaningless election[Led00b].

To bring online voting to their constituents, the Arizona Democrats contracted election.com to administer the election. Election.com sent registered voters their Online Voting Certificate in January 2000, providing each voter with a personal identification number (PIN) to authenticate themselves to the election.com website[MG01]. Because the election was technically private, the voting system was not subject to voting standards that apply to the November general election[Mat00].

Between March 7 and 10, Democrat voters could log onto election.com and authenticate themselves to vote in the Arizona election[MG01]. The election site was also mirrored on the party website, www.azdem.org. The site asked for the voter's PIN, name, address, and an additional randomly chosen question to deter fraud. Questions such as date of birth or the last few digits of social security number were used. Upon success, the voter could cast their ballot from the convenience of wherever they choose to access the Internet[Led00a].

2.2 What went right in Arizona

Vendors and party officials most often cite high voter turnout to prove the success of Arizona’s online election. They rally behind claims of increased participation from all demographic groups. The absence of a major technological failure gets played up as well[MG01]. However, most of these claims fail to tell the whole story objectively.

Aside from boosting turnout nationwide, Internet voting has the potential to reinvigorate the most apathetic of all voting blocs – young people. As Figure 3 showed, turnout did increase in the primary from 12,800 to 85,970. The turnout among young voters was key. Of the Internet votes cast in Arizona, 75 percent of them were from people between 18 and 24 years old[Lee00]. During the 1996 presidential election, less than one-third of the people between ages 18 and 24 voted[Bur00].

To help minority turnout, the Democrats and election.com had an extensive campaign to raise voter awareness about the Internet election, to educate them about the process, and to provide accessible computers for people to use. The Democrats even went out to assist Native Americans participate in the online process[MG01]. Despite these efforts, several voter’s rights groups considered the online results diluted by rich computer users[PS01].

Party officials and election.com executives claimed that their election was secure, implying that any Internet election would therefore be secure. Party executive director Cortland Coleman said the security threats are “being overstated,” concluding that Internet elections are more secure than their physical counterparts[Mat00]. Joe Mohen, election.com CEO, said that his security was “airtight”[La00].

Looking beyond the biases of those who ran the election reveals a different story altogether.

2.3 What went wrong in Arizona

The Arizona election avoided a major catastrophe and vendors claimed security succeeded against all hacking attempts. But many parts of the election protocol failed, and these aspects of failure in Arizona bring to light the

Image permission granted by election.com.

Election.com’s online election demonstrated many of the risks of remote online voting.

potential disaster that accompanies remote online voting.

On the first day of voting, the election web site was down for over an hour[La00]. Election.com said the failure was due to a router malfunction and the site was up for 95 out of the 96 scheduled hours[MG01]. Those who were able to connect to the site had problems if their computers and software were not current enough[Ka00]. Old web browsers could support online voting, nor could most Macintosh computers. People who were not very computer literate also had problems using the web site[Ra00]. A lack of technical support hampered the election; two phone lines were constantly busy throughout the entire election, leaving many without assistance[Ka00].

Computer expects criticized the robustness of the security systems, asserting that large-scale fraud could not have been prevented and that small-scale fraud occurred[La00]. Voters used PINs to authenticate themselves, having received the PIN in the mail prior to the election. Some voters lost their PINs, others received PINs from previous residents or tenants, allowing them to vote more than once[Le00a]. Election.com could have violated the secret ballot since they assigned voters their PIN[La00]. Another weakness was the cryptography system – election.com used a proprietary "cascading" encryption algorithm[Lee00]. By not allowing public and academic scrutiny of their cryptography, we can not accurately gauge its effectiveness.

The election was not a public election, allowing the Arizona Democrats and election.com to circumvent standard certification processes[Ra00]. The election did not have to comply with the rigorous laws that apply to regular political elections. Being a private election, election.com was not forced to reveal their costs to the public[La00]. Some speculate that election.com "spent like mad" to have the election succeed – not out of public duty, but because of a planned IPO[Le00b].

2.4 Was the election fair?

Allowing Internet users five days to cast their ballot compared to one day for polling place votes sparked a federal lawsuit from the Voting Integrity Project. The suit claimed the this disparity violated the 1965 Voting Rights Act[Whi00]. Minorities had less access to online voting - African-Americans and Hispanics are about half as likely as whites to have Internet access [PS01]. The courts allowed the election to take place, but the lawsuit is still pending[Whi00]. An April 2001 trial date has been set[PS01].

Election.com cited increased turnouts among blacks and Latinos to conclude that their voting system did not discriminate[He00]. They also claimed to have made great efforts to increase turnout for Native Americans, bringing computers to the reservations[MG01].

But regardless of minority outreach efforts, the five day voting period was considered by many a violation of the law. “It just wasn’t fair to give people who had web knowledge and web access four more days to vote,” said Michael Cornfield, a professor as George Washington University[Whi00]. Deborah Philips, VIP president, said she can immediately see how a “disproportionate number of white voters” were able to cast their ballots online[Whi00].

Many of the glitches discovered in Arizona can be eliminated with more preparation and attention to detail. For example, election.com forgot to provide audio cues for blind voters[PS01]. More help lines should be accessible and cross-platform Internet voting needs to be available. As Alfie Charles, assistant secretary of state in California said, “We can learn from the mistakes in Arizona”[Ra00].

We learned a lot about some of the problems related to the nature of remote online voting, such as security, fairness, and educating the public through Arizona’s experimentation. The Internet’s infrastructure lacks security demanded for a public election.

3 Student Council Online Elections

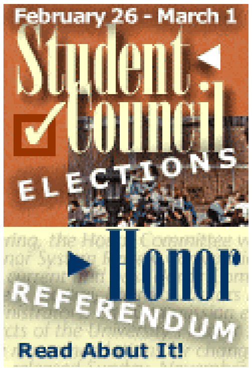


Image permission granted by www.virginia.edu.

Convenience succeeds in a small community of trust

"It's now 8:50 p.m. on Monday night, and the voting site is totally non-functional. What the hell is going on?" –Student Council President Joe Bilby, in an election night email

The website for Student Council elections at the University of Virginia is not secure, but its Internet basis makes it extremely accessible and convenient for the student body. Students spread out geographically in Charlottesville as well as those studying abroad all over the world enjoy the convenience of voting from almost anywhere.

Paper ballots, the only alternative, would be a terrible hassle. They would be expensive to print, time consuming and error-prone to count, and maintaining convenient poll sites would be impractical. The website solves most of those problems – giving almost all students an easy means to participate in student government.

Running this election website has taught me a lot about the usability and security risks of remote online voting. Even though this system succeeds for University elections, its failures are indicative of Internet voting's weaknesses in general, showing that it is not a safe medium for real elections.

3.1 *Small, simple, successful*

The Student Council election system consists of two basic parts: the website and the database. The website breaks down into two sections – the user side and the administrator side, which I used to manage the election. The web interfaces provides almost all of the functionality to cast ballots and administer elections. The database primarily serves to manage student information.

Students can easily vote in one session with minimal computer skills, satisfying Cranor's definition of a convenient election[Cra96a]. Authenticating a student merely requires their email login and the last four digits of their social security number – a very thin layer of security.

The website maintains a running tally of all the votes, making it easy for the elections committee to determine which candidates win or lose. The results page posts a full listing of all write in candidates. Student Council's voting system does not support a robust interface for voter turnout through the website. I needed to generate those tallies manually through the elections database.

The elections database, a Unix system call MiniSQL, worked well throughout the elections. It's primary use was importing the full listing of University students and then modifying it to correct candidate names and other student data. I easily ran INSERT and UPDATE queries to fix all information. Its biggest weakness was that it failed to implement all standard SQL queries and there was not an easy way to count how many voters cast ballots.

This election system succeeds because it is convenient and simple to use. The system has become well accepted as turnout has increased significantly over the last three years[Mar00]. Despite prevailing security flaws, the system serves its purpose well and virtually eliminates all manual counting from the process.

3.2 Student Council's scheme highlights Internet voting's drawbacks

The Student Council elections provide good insight into the overall inability for the Internet to be a safe medium for legally binding political elections. Some of its failures are unique, but many are strikingly similar to the Arizona experiment. This small election failed in many ways despite being carried out in a community of trust. A viable remote online voting scheme would have to correct these errors and scale to work for a large population of untrusted users.

90-minute downtime first day

Hours before the start of voting, a job on the Student Council server consumed almost all the system resources. Within minutes of the 8:00 PM start of the elections, about 200 students attempted to vote. Almost all of them received Server Error 500 messages and at about 8:25 the server crashed. Student Council and Information Technology and Communication (ITC) worked to get the server restarted and back online. At about 9:55 the server was back online, with a capacity of 50 students established. Since the first downtime, no reports were made of problems accessing the site.

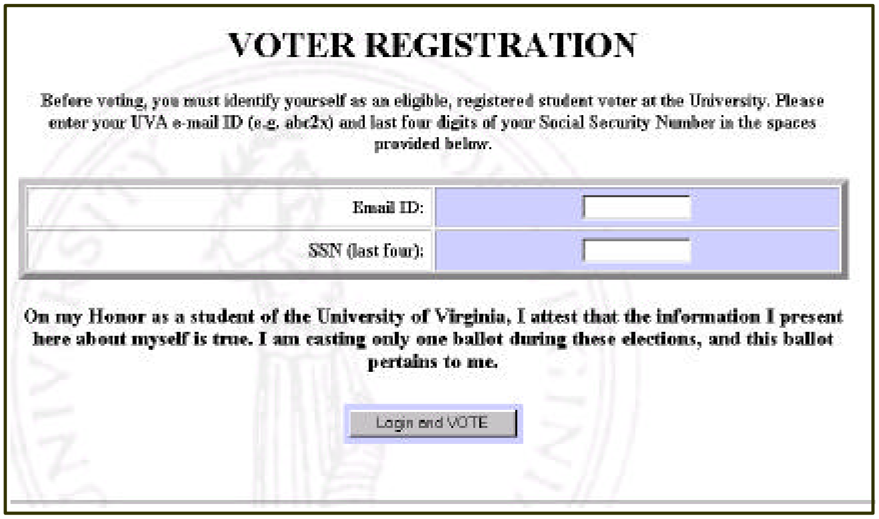
Arizona had a 60 minute downtime on the first day of their election, and they had stand-alone servers and professionals monitoring the system[MG01]. Both of these failures were internal – if these systems accidentally fail from the inside, a motivated attacker should have little trouble trying to force some sort of availability failure.

Secret data was not well protected

The information students used to authenticate themselves failed to ensure many requirements that any secure system must follow, as shown in Figure 4. The data, for the most part, is publicly available. Student email logins are publicly available through www.virginia.edu's whois system. The "key" for students was the last four digits of their social security number. Although not publicly available, these are not hard to find. Students often submit assignments with their full identification number on them and class rosters have identification numbers on them. Anyone with access (legitimate or otherwise) to assignments, rosters, grade postings, and the like can easily masquerade as another student to the election system.

Figure 4 –Student Council's Voter Registration Page

The registration page prompts the voter for information that is not well protected. The honor system plays a large role in the site's security.



VOTER REGISTRATION

Before voting, you must identify yourself as an eligible, registered student voter at the University. Please enter your UVA e-mail ID (e.g. abc2x) and last four digits of your Social Security Number in the spaces provided below.

Email ID:

SSN (last four):

On my Honor as a student of the University of Virginia, I attest that the information I present here about myself is true. I am casting only one ballot during these elections, and this ballot pertains to me.

While voting, a student's identifying information becomes a hidden input on the cgi page. When a voter transmits their ballot, their identification number and all of their choices are passed along the Internet unencrypted. Anyone who views the packets can see how a voter cast their ballot.

Ballot ordering was inconsistent

All candidates were entered into the election system alphabetically for all offices and most of these appeared on the ballot in reverse-alphabetical order. The ballot appearance on the website was consistent with normal stack operations, pushing in candidates and leaving the last one on top. Several times the ballot ordering deviated from this pattern, causing some candidates to feel slighted, insinuating that the elections committee was favoring some candidates by placing them at the top or grouping certain candidates together. No one on the elections committee, including the website administrator from 1999-2000, could determine the cause of the ballot ordering. The actual Perl code that generates the ballots was posted on the website and a student mailed in a suggestion to fix the ordering. The elections committee will attempt to make this correction for Fall elections.

School of Continuing and Professional Studies students could not vote online

Although not a significant voting bloc, SCPS students could not use the website to vote in University-wide elections or for their own representatives. The data from the registrar indicated that 48 out of 18,000 students, or 0.26%, were classified as SCPS students. Due to a parsing error, when the student data was imported, these students were rejected. We allowed them to vote over email so they could vote without needing a paper ballot.

This problem was not simply an elections problem – some of the candidates for the SCPS offices were listed as university staff and would never appear in the student database, implying that their size may be significantly underestimated.

Students studying abroad were not in the election database

University students studying abroad did not appear in the roster that the elections committee uses to authenticate the students. These students needed to email the elections committee, which had their names added to the database so they could vote.

Some students were confused by their voting options

First, second, and third-year law and medicine students were prompted to vote for undergraduate second, third, and fourth-year class councils. The system could not distinguish between a first-year undergraduate and a first-year law student. To remedy this, all graduate students were raised to at least fourth-year standing, making them ineligible for all class council races.

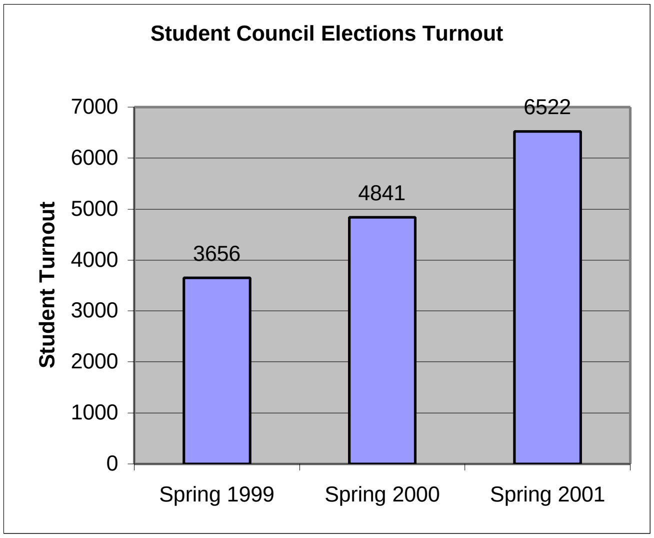
Students with too many credits could not vote for their class officers. For example, third-year students who came to the University with Advanced Placement credit may have accumulated enough credits to appear as fourth-years. The data came straight from the registrar, giving Student Council no means of distinguishing between real fourth-years and third-years with a lot of credits. These students were required to email the elections committee if they wanted to change their class affiliation.

This particular failure could be devastating in a remote online scheme. Under physical schemes, everyone at a particular polling station votes on the same ballot with the same options. Removing that consistency could make it difficult to ensure that voters are presented with the correct options for local elections, as well as provide people who move to vote in whatever races they are legally allowed to vote in.

3.3 What remote online voting provides for Student Council

Eliminating paper ballots and switching to an online scheme dramatically reduces the effort required by the elections committee. The website housed voter guides, information, and the actual mechanism to vote. The turnout increases, as shown in Figure 5, reveal the site's success and ubiquity.

Figure 5 – Overall Student Council election turnout since 1999 [Mar00]



Easy access

Almost all students either own a computer or have easy access to one at any of the computer labs spread out across the University grounds. The voting website received over 19,000 visits during election week

This extensive accessibility makes the Internet a prime location to conduct elections. For the general public, this universal accessibility is not the case, potentially diluting the vote with rich computer users[PS01]. Therefore, what helps make the Student Council election successful could make a public Internet election unfair.

Easy ballot generation

Many races are on the ballot, but any one student can only vote in a small percentage of them. Most races are broken down by year or school. Maintaining paper ballots for all permutations of schools and years would be overwhelming. This step is nearly trivial for the online system, although it is not robust enough to satisfy every voting specification.

Links to voter guides and notes

The site has links to unbiased Student Council voter guides, allowing students to inform themselves better before voting. The site also provides an easy means to post notices to the voters about any known problems or bugs. The Spring 2001 election encountered several non-fatal errors and posting them made voters more aware, facilitating prompt resolutions to individual concerns.

Sample ballots educate voters of their options

Sample ballots are posted, allowing students to preview what they will be presented with when they actually vote. This service allows students to know when they will be asked to vote for one or more candidates and to inspect the actual voting interface. Students from Florida can actually practice voting to alleviate the mishaps similar to the 2000 presidential election.

3.4 The fundamental tradeoff – security for convenience

Proponents of online voting assume that Internet security measures can replicate those used when people vote in person. For someone to vote at a poll site, they need to register, show up, and prove their identity. These steps take time and effort. To vote in Student Council elections, none of the steps are required.

Students do not specifically register to vote. If the registrar considers them a student, so does the election system. Students submit no additional paperwork. The remote nature of online voting obviously does not demand showing up, as students can vote from home, computer labs, or Europe, as several voters did. Voter identity is not proven, considering the weak authentication system employed.

The layer of security is so thin, yielding two consequences – one, students can very easily vote, and two, attackers can very easily to forge votes. Any voting system that had multiple stages of authentication would discourage most student voters; such a process would probably take too long and could make voting not seem anonymous. Mailing students identifying information, either postal mail or email, would be risky, as many people would throw it away or delete it, thinking it was junk mail. The very same problem occurred in the Arizona primary when many voters complained about never receiving their PIN only to realize they accidentally threw it away [Led00a].

The Student Council voting system cannot legitimately defend against attackers forging votes or masquerading as voters. The system does not log information about the computers it receives votes from, allowing a single user to taint an election without their identity being revealed. The main defense the site has is the student-run honor system. Students click on a button that they are on their honor to not vote illegally. This scheme succeeds in our community of trust but would fail if used among untrusted users. The system can only check if a student has voted, preventing a single email login and social security number from double voting.

The election server does maintain a secret ballot. The server uses the identification information to note that a particular student has voted and prevent double voting. The database saves the ballot without any identifying information. From the votes cast, the elections committee could determine the school and year of the voter, but not who actually cast the ballot.

3.5 Success that does not scale well

The success of the system can only continue if the size of the election remains about the same size. This system can not scale to a larger body – it would become totally unmanageable if the size increased by a considerable margin. For example, in the ballots table of the elections database, over 80,000 individual entries were stored for 6522 voters. The system relies on too much manual troubleshooting and the database would grow exponentially. Aside from growing too large, the election would be vulnerable to this single point of failure – a failure that could wipe out the entire canvas.

Despite its shortcomings, the Student Council system still succeeds. Student leaders have been very impressed with the increased turnout[Mu01]. The system places simplicity and convenience above security so students can vote in a hassle-free environment. No paperwork or special passwords are required – a student can just sit down and vote at any Internet-ready computer. Some candidates see campaigning moving online as well.

4 Technology and Technological Risks for Online Voting

"It is unreasonable to assume that average Internet users who want to vote on their computers can be expected to understand the concept of a server certificate, to verify the authenticity of the certificate, and to check the active ciphersuites to ensure that strong encryption is used. In fact, most users would probably not distinguish between a page from an SSL connection to the legitimate server and a non-SSL page from a malicious server that had the exact same look as the real page." – Avi Rubin [Ru00]

Remote online voting grew from a solid mathematical and technological foundation. Algorithms developed over twenty years ago support the most important cryptographic principles in voting protocols. Over the years, security requirements were developed to improve the effectiveness of these protocols. This chapter will investigate the technology that makes online voting happen, drawing evidence from the previous case studies.

A host of technological risks plague the feasibility of remote online voting. These risks, such as malicious attacks, highlight the weaknesses in online security, especially voting. A common theme occurs among the probable failure points – human interaction. Whether it's a malicious attacker or an ignorant user or administrator, attacks rarely involve brute force attacks on cryptographic algorithms.

4.1 Cryptographic Foundations

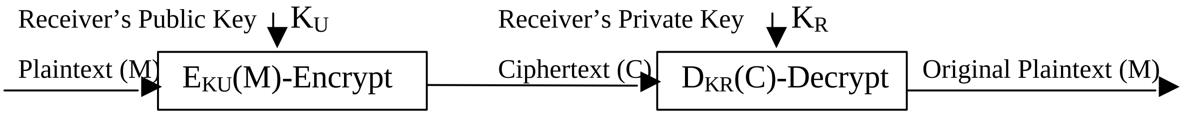
Remote online voting naturally draws fundamental principles from public key cryptography (PKC) because it provides simple means for authentication and confidentiality.

Public key cryptography originated from the desire for people to communicate privately without the need to meet and agree on a secret key. With the invention of the Diffe-Hellman public key exchange algorithm in 1976, cryptography was changed forever[DH76, Sche96]. The Diffie-Hellman scheme provided a means for two people to generate a secret key based on the presumed difficulty in computing discrete logarithms[Stal99]. There is a recurring theme in much of cryptography where security exists because a particular problem is very difficult to solve.

Encryption Algorithms and Techniques

Rivest, Shamir, and Adleman took a monumental leap in cryptography and computer science with their paper "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems" [RSA78]. Their proposed RSA encryption algorithm used two separate keys – a public key and a private key to encrypt and decrypt messages. The basic protocol is illustrated below in Figure 6.

Figure 6 – Encrypting and decrypting a message using public key cryptography

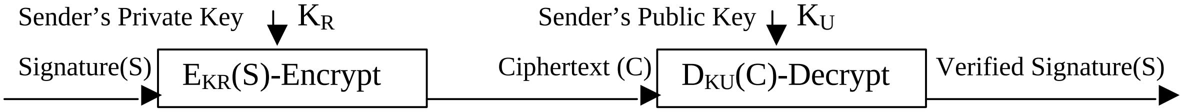


Revealing the public key does not give an attacker enough information to determine the private key. The RSA encryption security depends on factoring large numbers, 100 to 200 digits in length, which is believed to be computationally difficult[CLR98].

Digital Signatures

The RSA algorithm provides another major feature for secure communications – digital signatures. Only the owner of the private key can read a message encrypted with the complementary public key, but he has no way of ensuring who sent the message. Using the RSA algorithm backwards, a user can 'sign' the message by encrypting a textual signature with their private key[RSA78]. Anyone can decrypt this message to confirm who sent it, but only someone who knew the private key could have encrypted it, authenticating the message, as shown in Figure 7.

Figure 7 – Generating a digital signature with public key cryptography

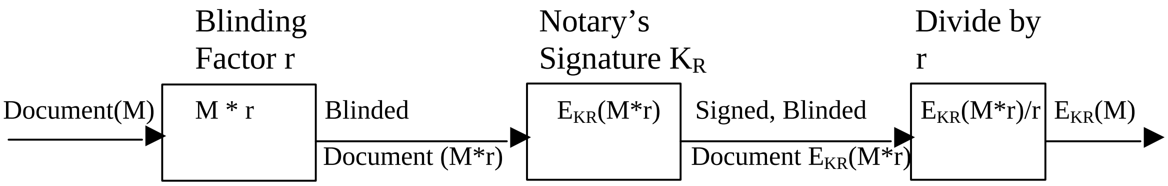


4.2 Theoretical protocols and PKC

The authentication and confidentiality of PKC makes much of theoretical voting possible, but another important element is required – blind ballots. Without being able to blind ballots, an identity can be matched to a ballot, violating the secret ballot.
PKC facilitates a successful model for secret ballots by allowing a ballot to be blinded.

A blinding scheme, illustrated below in Figure 8, is paramount to protocols discussed by [FOO92, Cra96a, Sche96]. David Chaum first introduced the notion of blind signatures in his 1982 paper "Blind Signatures for Untraceable Payments"[Ch82].

Figure 8 – Generating a blinded document with public key cryptography



The resulting document, E_{KR}(M), has the notary's signature, but signer does not know the contents of document M. This process works when the signing process is commutative with multiplication[Sche96].

Blinded ballots generally include a PIN that the voter received during registration, allowing the voting authorities to ensure double voting does not occur. In [Cra96a], the Sensus scheme guarantees a secret ballot and prevents double voting with two administrators – a validator and a tallier. The validator receives an identifiable, blinded ballot, and the tallier receives an anonymous ballot that was signed by the validator.

The protocol begins when the voter sends the validator a ballot with the concatenation of a PIN and a blinded ballot. The validator checks that the voter's PIN has not voted yet. Having only received a blinded ballot, the validator can not violate the secret ballot. The validator separates the PIN and signs the blinded ballot, passing it back to the voter. The voter removes the blinding and passes the signed ballot on to the tallier anonymously[Cra96a].

Although successful in theory, practical failures would occur, delaying the deployment of remote online voting. Anyone with access to PINs that were not used during voting could taint the election. An administrator could cheat the system by casting ballots for all voters who abstain[Cra96a]. The Student Council scheme has the exact same vulnerability, worsening the situation by making it obvious which students have not voted. These schemes further assume that ballots are passed across an anonymous channel and that administrators cannot trace packets back to their sender[Cra96a].

4.3 Online Voting Security Requirements

A secure voting system must thoroughly satisfy four major requirements: authentication, availability, confidentiality, and integrity[Stal99]. Theoretical models like [FOO92] have claimed success, but this project has shown how real-world examples have failed. Any remote online voting scheme that strives to be used in public elections must be able to satisfy these constraints in a practical manner – quite a challenge given the insecure nature of the Internet[CAL00, MM00, Ru00].

There are additional requirements from literature – convenience, flexibility, mobility[Cra96a]. Convenience dominates the discussion – voting should only take one session and require minimal skills. Most security sacrifices are in the name of convenience, as is the case for Student Council.

The chart on page 25 at the end of this section reviews how the Arizona and Student Council elections fulfill the four main requirements. For contrast, the chart stacks up a conventional paper ballot scheme against the same requirements.

4.4 Malicious Attacks and defense mechanisms

Malicious attackers pose a serious threat to remote online voting. Many potential attacks can alter or destroy a voter’s ballot without any indication that an attack was made[Ru00]. Encryption strength becomes meaningless as Trojan horse attacks and viruses do their damage before a user encrypts their a ballot. Distributed denial of service attacks could render an election site useless, as similar attacks did just that to popular commercial sites in February 2000[Ru00, MM00].

Motivated attackers have a big target with the Internet and Microsoft users. Attacks like the IloveYou bug and the Melissa virus have caused enormous damage in lost data and productivity, exploiting weaknesses in the Windows operating system and mail programs[Gl00, Pe99]. A similar virus could infect computers on election day, either preventing voting or manipulating the results[Ru00].

Fortunately, these attacks have improved the response of security experts. The Internet Worm, which shut down 10 percent of the 1988 Internet brought about CERT – the Computer Emergency Response Team[Pe99]. Techniques such as blacklisting known viruses and monitoring code execution has brought some success in thwarting attackers, but the tools are having trouble keeping up with newer applications[MM00]. Adhering to the most fundamental security design principles and policies, as stated by Saltzer and Shroeder in 1975, could resolve most of the problems[SS75, MM00].

Prevailing Issues

Security professionals must address many holes in Internet security. As long as malicious computer users have many options in selecting which weaknesses in the Internet to exploit, remote online voting is infeasible[Ru00]. An election website must prevent malicious attacks in order to protect the trust of the voters[CAL00, DR00].

4.5 It all comes down to human interaction

All the security in the world cannot prevent the weakest part of the system from failing – human interaction. People choose bad passwords, lose their PINs, accidentally compromise their private keys, and unknowingly pass on emails with viruses attached[Gl00, Le00a, Ra00]. Users ignore warning messages, do not check certificates and site authenticity, and get fooled into going to a fake web pages[Ru00, Sub00]. Someone must provide better education and more accessible help for the average computer user[Ka00, Ra00].

Users are not the only humans to blame. Software companies need to design error messages that are less esoteric, allowing users to understand their options. Viable remote online voting technology may in fact be available, but until engineers go the extra mile to make it safe and usable, it will not be a legitimate option for conducting elections.

Remote Online Voting Security Requirements

	Authentication	Availability	Confidentiality	Integrity
AZ Democratic Primary	PINs were mailed to registered Democrats. The PIN in conjunction with identifying (but by no means secretive) questions allowed voting[MG01].	With the exception of a one-hour downtime, the election was available[La00]. Customer service help lines were not available and voting was not available to old browsers and some Macintosh computers[Ka00].	Election.com may have had access to the PINs that would have allowed them to link votes to a voter[La00]. Their encryption was not known to be compromised, but it was a proprietary algorithm that did not undergo public scrutiny[Lee00].	I have not found evidence of integrity failure, but the election's private nature allows election.com not to release all relevant information regarding their procedure[Ra00].
Student Council Elections	Student Council authenticates voters with their email login and student identification number. Email logins are publicly available and student id's are not well protected, as they are associated with class rosters and assignments.	Prior to elections, a student consumed all of the server's resources before the elections began. Within 30 minutes of the start of elections, the workload crashed the server, resulting in a 90 minute downtime.	The system does not use encryption, allowing attackers to steal or modify data in transit. Although records cannot match votes to a voter, all individual ballots are saved.	The plaintext nature of the ballots makes them vulnerable. Legitimate officials have too much access to the voting canvas, including the ability to prevent a voter from voting or allow them to vote multiple times.
Paper Ballots	Voter presents identification to poll worker who checks their name against the roll.	Polls are open at times specified and mandated by county, state, and federal laws.	The voting booth allows the voter to exercise their franchise in privacy, casting a ballot that cannot be linked back to them.	All ballots are transported to the official election site where they are tabulated by elections officials and saved for recounts and audits.
Definition	Officials correctly identify the authenticity of a voter. All stages of voting can guarantee that a ballot is authentic. The voter is eligible to vote and only votes one time.	The voting system must be available to the voters at its specified times. An online voting system must be able to resist denial of service attacks, viruses, and the like.	Only legitimate officials have access to ballots. The secret ballot must be maintained and eavesdroppers must not be able to view a cast ballot.	Only legitimate officials have access to the election canvas and only the individual voter has access to their personal ballot. Ballots would not be tampered with en-route to the election server.

5 Conclusion

“You think about [Internet voting] for five minutes and it sounds like a good idea. You study it for 10 months, and you find a lot of reasons that it may not be such a good idea.” – President of the California Voter Foundation Kim Alexander [La00]

Internet voting can solve a lot of problems that exist in our current voting system, but if it were implemented now, it would create a host of new problems, more severe than the current problems. Improved convenience and tabulation speed would come at the cost of security, fairness and validity of results. Despite its failures, the case studies also showed how Internet voting can succeed, depending on what is at stake for the election. The American presidency would be a big target for attackers, not the Student Council presidency.

5.1 Summary

The Internet is an insecure medium, making it infeasible to hold secure elections online. Malicious attacks are too serious of a risk, considering their potential for destruction. If defense mechanisms cannot prevent automated voter fraud, remote online voting cannot be implemented. Aside from infrastructure woes, flawed protocols and user error add to the challenge of making a viable online election system. Fortunately, most of the technology for voting exists – the most fundamental components are provably effective.

Internet voting had significant failures in the case studies, but many areas of success indicate hope for non-public online elections, where security requirements are not as high. The convenience can not be surpassed as more and more people get online. Paper ballots would be expensive and error prone for smaller organizations, such as Student Council.

5.2 Interpretation

All of the systems – theoretical and practical – have shown that a robust system is hard to build. It’s problematic when theoretical protocols have documented points of failure. Any practical system must be full of weaknesses, just like those found in the Arizona and Student Council systems. Considering the flaws in the current voting system, a fully robust system may unfortunately be impossible.

A superfluous barrier to success lies with the online election vendors and computer security experts. Their stubbornness to see other perspectives could inhibit progress in the field. I see this more on the vendor side, but both need to be more open.

Vendors need to be more critical of the risks involved. Some make awful comparisons, rationalizing that Internet voting is safe because electronic commerce is safe. This is a poor comparison because vendors manage commerce in the open, with detailed descriptions of all transactions from purchase to payment to delivery. Election officials conduct voting secretly and anonymously – dramatically more challenging. Another poor conclusion drawn from Arizona, for example, states that because no known major attacks took place, none are possible. Proof by example bears no weight.

Experts need to be more open to the fact that someday, Internet voting will be a reality. Being critical of our current, premature schemes and protocols is fine; do not write off the technology just yet. They should work to fix the problems rather than criticize them. Luckily, some experts are doing just that.

With respect to the smaller systems like Student Council's election scheme, the future looks bright. Smaller groups should consider using Internet voting for non-public elections – it is convenient and secure enough for organizations like Student Council. The products sold by companies like election.com offer services that can facilitate elections for groups geographically spread out or those that want to eliminate postal fees and paper ballots from their elections process.

Student Council can create a much better system with some minor changes. For example, a more granular office and candidate system, the ability to modify student data on web site, sorting the candidates on the ballot, and generating turnout results would make their system much stronger. Moving more management to the web site and away from the Unix side can significantly reduce the effort and man-hours required. I know I spent way too much time searching for the syntax to modify students' year so they could vote in the fourth-year class council race.

Users need computer literacy education. Perhaps this will not be as significant as the voters of tomorrow will have grown up using personal computers all their lives. The average American does not understand enough about using Internet to safely maneuver through an online election. Actually, the average American does not have Internet access, the focus of a different, yet equally important issue.

5.3 Recommendations

Before remote online voting can become a reality, we need to build computer defense mechanisms to catch up with the attacks. As long as the malicious users have the advantage, there is too much risk involved. New techniques and policies could usher in an era of safe, reliable software, providing the infrastructure for remote online voting.

I think it is safe to assume that voter turnout and participation would increase if we have online voting. Increased voting convenience would reduce many barriers that prevent several groups from having large turnouts, such as: students, handicapped people, military stationed abroad, and busy professionals. Absentee voting helps the problem, but Internet voting would serve these groups better and aid millions of other voters at the same time.

We obviously cannot stop here – and we will not. Improvements in Internet security, cryptography, voting protocols, and computer interfaces will one day bring a successful remote online voting model to public elections. Internet voting is a good idea and done right can help a lot of people in a lot of ways.

But we’re not ready yet. We’re not ready technologically, and we’re not ready socially. One day we will, but on Tuesday, November 6, 2001, we’re going to vote on the same machines we’ve been using all along. Except hopefully not using the Butterfly Ballot.

6 Bibliography

[Bu00] Burke, Lynn. "The Tangled Web of E-Voting." WIRED Magazine. http://www.wired.com/news/politics/0,1283,37050,00.html. June 26, 2000.

[CAL00] California Secretary of State. A Report on the Feasibility of Internet Voting. California Internet Voting Task Force. Sacramento: 2000.

[Cam00] Camp, L. Jean. Trust and Risk in Internet Commerce. Cambridge: The MIT Press, 2000.

[CLR98] Cormen, Thomas H., Charles E. Leierson, and Ronald L. Rivest. Introduction to Algorithms. Cambridge: The MIT Press, 1998.

[Cra96a] Cranor, Lorrie Faith, and Ron K. Cytron. "Sensus: A Security-Conscious Electronic Polling System for the Internet." http://ccrc.wustl.edu/~lorracks/sensus/, 1996.(30 Sept 2000)

[Cra96b] Cranor, Lorrie Faith. "Electronic Voting." http://www.acm.org/crossroads/xrds2-4/voting.html, 1996. (30 Sept 2000)

[Cra96c] Cranor, Lorrie Faith, and Ron K. Cytron. "Towards an Information-Neutral Voting Scheme That Does Not Leave Too Much To Chance." http://www.research.att.com/~lorrie/pubs/mpsa/mpsa.html, 1996. (24 Oct 2000)

[DH76] Diffie, Whit and Martin E. Hellman. "New Directions in Cryptography." IEEE Transactions on Information Theory. Vol. IT-22, No. 6, November 1976.

[DR00] Dictson, Derek, and Dan Ray. "The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections." The George Bush School of Government and Public Service, Texas A&M University. January 18, 2000.

[FOO92] Fujioka, Atsushi, Tatsuaki Okamoto, and Kazui Ohta. "A practical secret voting scheme for large scale elections." *Advances in Cryptology – AUSCRYPT '92.* Springer-Verlag, Berlin, 1993.

[Gl00]. Gleick, James. "Love, Microsoft - Who's to blame for the 'ILOVEYOU' virus? Who else??" The Slate. http://slate.msn.com/Features/lovebug/lovebug.asp. May 9, 2000. (March 14, 2001)

[Go99] Goldman, Ralph. "Internet Voting Testimony of Ralph Goldman" Workshop on Election Technology, State Government Committee, House of Representatives, State of Washington. http://www.netvoting.org/Resources/Workshop10-14-9.doc, 1999. (24 Oct 2000)

[He00] Hershey, Robert L. "Firm says it can hold elections on line." The Washington Times. October 15, 2000.

[HM00] Hiltzik, Michael A. and Greg Miller. "Fiasco Reveals a Ballot System Full of Holes." The Los Angeles Times. 11 November 2000.

[HC01] Hoffman, Lance J. and Lorrie Cranor. "Internet Voting for Public Officials." Communications of the ACM. Vol. 44, No. 1, January 2001.

[Ka00] Kamman, Jon. "Dems hail success of online election." The Arizona Republic. March 12, 2000.

[La00] Ladd, Donna. "Casting Your Vote On The Internet: Yea Or Nay." ZDNet Interactive Week. http://www.zdnet.com/intweek/stories/news/0,4164,2597347,00.html. July 3, 2000.

[Led00a] Ledbetter, James. "Net Out the Vote." The Standard. http://www.thestandard.com/article/display/0,1151,13004,00.html. March 20, 2000

[Led00b] Ledbetter, James. "'Virtual Voting' Faces Real-World Concern." The Slate. http://slate.msn.com/netelection/entries/00-03-16_77458.asp. March 16, 2000.

[Lee00] Lee, Lydia. "Vote naked in the privacy of your own home!" Salon Technology. http://www.salon.com/tech/view/2000/03/20/election. March 20, 2000.

[Mar00] Marchetti, Sarah. "Bilby, Dignan to face run-off election." The Cavalier Daily. http://www.cavalierdaily.com/CVarticle.asp?ID=3454&Date=3/3/00. March 3, 2000.

[Mat00] Matthews, William. "Can the Net revive the vote?" Federal Computer Week. http://www.fcw.com/fcw/articles/2000/0904/cov-vote-09-04-00.asp. September 4, 2000.

[MM00] McGraw, Gary and Greg Morrisett. "Attacking Malicious Code: A Report to the Infosec Research Council." IEEE Software. September/October 2000.

[MN01] Mercuri, Rebecca T. and Peter G. Neumann. "System Integrity Revisited." Communications of the ACM. Vol. 44, No. 1, January 2001.

[MG01] Mohen, Joe and Julia Glidden. "The Case for Internet Voting." Communications of the ACM. Vol. 44, No. 1, January 2001.

[Mu01] Murphy, Deirdre Erin. "Students elect Fifer." The Cavalier Daily. http://www.cavalierdaily.com/CVArticle.asp?Date=Mar+2+2001&ID=7684. March 2, 2001.

[No00] Norr, Henry. "Time to Digitize Elections." San Francisco Chronicle. November 27, 2000.

[Pe99] Pethia, Richard. "The Melissa Virus: Inoculating Our Information Technology from Emerging Threats." Testimony before the Subcommittee on Technology, Committee on the Science, U.S. House of Representatives. http://www.cert.org/congressional_testimony/pethia9904.html. April 15, 1999. (March 14, 2001)

[Phi99] Phillips, Deborah M. "Are We Ready for Internet Voting?" The Voting Integrity Project. http://www.voting-integrity.org. Arlington, VA, 1999.

[PS01] Phillips, Deborah M. and Hans A. Von Spakovsky. "Gauging the Risks of Internet Elections." Communications of the ACM. Vol. 44, No. 1, January 2001.

[Ra00] Raney, Rebecca Fairley. "After Arizona Vote, Online Elections Still Face Obstacles." The New York Times. March 21, 2000.

[RAND96] Hundley, Richard, Robert Anderson, John Arquillam and Roger Molander, ed. Security in Cyberspace: Challenges for Society. Proc. of RAND and the Ditchley Foundations. Santa Monica, 1996.

[RSA78] Rivest, R.L., A. Shamir, and L.M. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Communications of the ACM. Vol.21, No. 2, Feb 1978.

[Ru00] Rubin, Avi. "Security Considerations for Remote Electronic Voting over the Internet." http://avirubin.com/e-voting.security.html, 2000. (25 October 2000)

[SS75] Saltzer, Jerome H. and Michael D. Schroeder. "The Protection of Information in Computer Systems." Proceedings of the IEEE. September 1975. http://www.cs.virginia.edu/~evans/cs551/saltzer/

[Schd99] Schneider, Fred B, ed. Trust in Cyberspace. Washington, D.C.: National Academy Press, 1999.

[Sche96] Schneier, Bruce. Applied Cryptography. New York: John Wiley & Sons, 1996.

[Sche99] Schneier, Bruce. "Security in the Real World: How to Evaluate Security Technology." Computer Security Journal, Volume XV, Number 4, 1999.

[Stal99] Stallings, William. Cryptography and Network Security: Principles and Practice. 2nd ed. Upper Saddle River, New Jersey: Prentice Hall, 1999.

[Sub00] Sullivan, Bob. "Paypal alert! Beware the 'Paypai' scam!" MSNBC. July 21, 2000. http://www.zdnet.com/zdnn/stories/news/0,4586,2606152,00.html?chkpt=zdhpnews01. (March 14, 2001)

[Sut00] Sullivan, T.J. "Casting votes via Internet coming, but still years off." Ventura County Star. http://www.insidevc.com/elect2000/stories/20001111co1.shtml November 11, 2000.

[US00] United States Department of Justice, Civil Rights Division, Voting Section. About the National Voter Registration Act. http://www.usdoj.gov/crt/voting/nvra/activ_nvra.htm. February 11, 2000.

[Whi00] White, Ben, "Online Balloting: A Question of Fairness", The Washington Post, March 19, 2000: A9.

[Wash00] The Washington Post. Picture of the Butterfly Ballot. http://washingtonpost.com/wp-srv/onpolitics/elections/ballot110800.htm. November 8, 2000.