

Technology at the Ballot Box

Secure Systems Engineering Fall 2024

 EE G7701

October 23, 2024

Tushar Jois



Questions

- When will the exam scores be posted?
- Is there any extra credit available?
- Is there starter code for the ballot machine?
- Can we use the backdoors taught in lecture as a part of the project?
- What should be included in the project installation/user manual?
- How complex should the backdoors be?
 - If the red team doesn't find our back door, how would that impact the final grade?

Recap

- Secure systems can be backdoored in a myriad of ways
- Even though cryptography can be subverted in subtle ways
- The use of computing systems requires accepting large chains of trust

Lesson objectives

- Describe e-voting systems and their potential flaws
- Understand the design considerations inherent to e-voting
- Explain the societal implications of using e-voting systems

Takeaways on Trump, Voter Fraud and the Election

A New York Times Magazine investigation finds that misleading and false claims about widespread voter fraud are part of a long disinformation effort that the president has taken to new extremes.



Early voting in Ann Arbor, Mich., on September 24. Emily Elconin/Reuters



By Daniel Victor

Sept. 30, 2020



The specter of widespread [voter fraud](#) has been a cornerstone of



There was

Can we do better?

no credible evidence
of voter fraud in the
2020 US election.



It all started in 2000...



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

ELECTORS
FOR PRESIDENT
AND
VICE PRESIDENT

(A vote for the candidates will
actually be a vote for their electors.)

(Vote for 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 GOLDBABER - VICE PRESIDENT

13 ➡

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

(REFORM)

PAT BUCHANAN - PRESIDENT
EZOLA FOSTER - VICE PRESIDENT

4 ⬅

(SOCIALIST)

DAVID McREYNOLDS - PRESIDENT
MARY CAL HOLLIS - VICE PRESIDENT

6 ⬅

(CONSTITUTION)

HOWARD PHILLIPS - PRESIDENT
J. CURTIS FRAZIER - VICE PRESIDENT

8 ⬅

(WORKERS WORLD)

MONICA MOOREHEAD - PRESIDENT
GLORIA La RIVA - VICE PRESIDENT

10 ⬅

WRITE-IN CANDIDATE

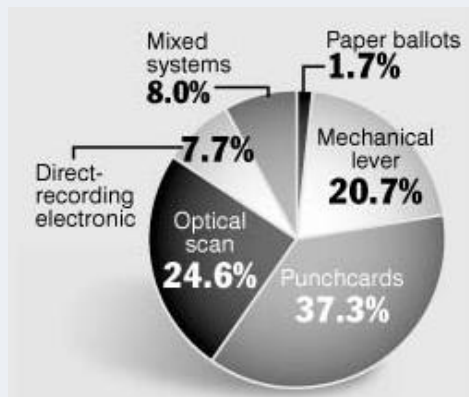
To vote for a write-in candidate, follow the
directions on the long stub of your ballot card.

There has to be a better way, right?



Voting systems

1996 Presidential election



Type of voting system	How the system works	Advantages	Disadvantages
Paper ballots	Voters mark choices on ballots and drop them in a sealed box.	Inexpensive; used mostly in rural areas.	Counting votes is slow and labor-intensive.
Mechanical lever	Voters pull a lever assigned to a candidate.	Easy to use; prevents multiple votes for the same race.	Machines can weigh 900 pounds and are no longer manufactured.
Punchcards	Voters punch holes in a ballot; ballots are then read by a computer.	Cheaper; more portable.	Can be inaccurate and unreliable; hand recounts pose problems.
Optical scan	Voters darken an oval or rectangle next to their choice; ballots are then read by a computer.	Easy to use; the process is similar to marking lottery tickets or standardized tests; hand recounts are possible.	Improperly marked ballots may not be recorded; high cost.
Direct-recording electronic	Touch-screen electronic display.	Easy to use; vote totals can be instantly printed on tape and recorded on a cartridge.	Computers provide no external way to verify vote accuracy.

Desirable properties of voting systems

Voter feels that:

- Vote was counted
- Vote was private
- Nobody else can vote more than once
- Nobody can alter others' votes

People believe that the machine works correctly and that its behavior cannot be modified

These have to do with perception.

It is also important that these perceptions are true.

“The purpose of an election is to convince the supporters of the losing candidate that they lost”

J. Alex Halderman, University of Michigan

Audit trail

- It is important that all phases of the vote casting and counting be auditable
- Recounts must be possible
 - If results come into question
- For electronic systems, need to audit
 - Hardware and software development
 - System deployment
 - All system binaries (compiled code, as well as compiler)
 - Use of system

Currently, such audit of hardware and software is not common, and is considered very difficult, if not impossible.

Voter verifiable audit

An audit trail (probably involving paper) that enables recounts and makes it harder to tamper with an election. The very piece of paper that is verified by the voter is used in the recount.



What could possibly go wrong?

Failure modes of electronic systems

- Several well understood concepts
 - The more software, the more flaws
 - Electronic systems are expected to fail at times
- Software security
 - It is very difficult to examine software and understand its behavior
 - Especially with a malicious programmer
 - It is difficult to know that a particular source code matches a particular binary
 - It is difficult to know that a particular binary is installed on a particular platform
- Many anecdotes of voting systems failing
 - To be clear, a *failure*, is not necessarily a *vulnerability*
 - To the right attacker, this is a distinction without a practical difference, though



Fairfax Judge Orders Logs Of Voting Machines Inspected

By **David Cho**
November 6, 2003

School Board member Rita S. Thompson (R), who lost a close race to retain her at-large seat, said yesterday that the new computers might have taken votes from her. Voters in three precincts reported that when they attempted to vote for her, the machines initially displayed an "x" next to her name but then, after a few seconds, the "x" disappeared.

In response to Thompson's complaints, county officials tested one of the machines in question yesterday and discovered that it seemed to subtract a vote for Thompson in about "one out of a hundred tries," said Margaret K. Luca, secretary of the county Board of Elections.

Software dangers

- Software is complex
 - top metric for measuring number of flaws is lines of code
- Windows/Mac/Linux Operating Systems
 - tens of millions of lines of code
 - new “critical” security bug announced every week
- Unintended security flaws unavoidable
- Intentional security flaws undetectable



Insider threats

- Easy to hide code in large software packages
- Virtually impossible to detect back doors
- Skill level needed to hide malicious code is much lower than needed to find it
- Anyone with access to development environment is capable
- Requires:
 - background checks
 - strict development rules
 - physical security

Example insider threat

- Ronald Harris
 - A computer programmer for the Nevada Gaming Control Board in the 1990s
 - Wrote anti-cheating code for slot machine for casinos
- Malicious code in testing unit
 - When testers checked slot machines, it downloaded malicious code to slot machine
 - A special sequence of coins activated the “winning mode”
- He and an accomplice walked away with thousands of dollars
 - Remained undetected
- Caught when greed sparked investigation
 - \$100,000 jackpot

What are some other insider threats?

- Instagram
- City College of New York
- Intelligence agency (NSA/CIA)
- New York City board of elections

Analysis of a voting machine



Avi Rubin

*Professor Emeritus
Johns Hopkins University
My PhD advisor*



DIEBOLD

We won't rest.

Code analysis

- 56-bit DES in CBC mode with static IVs used to encrypt votes and audit logs

```
#define DESKEY ((des_key*)"F2654hD4")
```

- Unkeyed public function (GPG) for file integrity protection
- No authentication
 - (the PIN authentication)
- Insufficient code



THE TECHNOLOGY

Behind crack.sh is a system with 48 [Xilinx Virtex-6 LX240T FPGAs](#). Each FPGA contains a design with 40 fully pipelined DES cores running at 400MHz for a total of 16,000,000,000 keys/sec per FPGA, or 768,000,000,000 keys/sec for the whole system. This means that it can exhaustively search the entire 56-bit DES keyspace in:



$$2^{56} / 768,000,000,000 = \sim 26 \text{ hours}$$



```
// LCG - Linear Congruential Generator  
// used to generate ballot serial numbers  
// A psuedo-random-sequence generator  
// (per Applied Cryptography,  
// by Bruce Schneier, Wiley, 1996)
```

BallotResults.cpp

Diebold Election
Systems

"Unfortunately, linear congruential generators cannot be used for cryptography"

Bruce Schneier

Applied Cryptography (Wiley, 1996)

Page 369

```
/* this is a bit of a hack for now. */
```

AudioPlayer.cpp

```
/* the BOOL beeped flag is a hack so  
we don't beep twice. This is really a  
result of the key handling being  
gorped. */
```

WriteIn.cpp

```
/* the way we deal with audio here is  
a gross hack. */
```

BallotSelDlg.cpp

```
/* need to work on exception *caused  
by audio*. I think they will  
currently result in double-fault. */
```

BallotDlg.cpp

```

void CBallotRelSet::Open(const CDistrict* district, const CBaseunit* baseunit,
const CVGroup* vgroup1, const CVGroup* vgroup2)
{
    ASSERT(m_pDB != NULL);
    ASSERT(m_pDB->IsOpen());
    ASSERT(GetSize() == 0);
    ASSERT(district != NULL);
    ASSERT(baseunit != NULL);
    if (district->KeyId() == -1) {
        Open(baseunit, vgroup1);
    } else {
        const CDistrictItem* pDistrictItem = m_pDB->Find(*district);
        if (pDistrictItem != NULL) {
            const CBaseunitKeyTable& baseunitTable = pDistrictItem->m_BaseunitKeyTable;
            int count = baseunitTable.GetSize();
            for (int i = 0; i < count; i++) {
                const CBaseunit& curBaseunit = baseunitTable.GetAt(i);
                if (baseunit->KeyId() == -1 || *baseunit == curBaseunit) {
                    const CBallotRelationshipItem* pBalRelItem = NULL;
                    while ((pBalRelItem = m_pDB->FindNextBalRel(curBaseunit, pBalRelItem))) {
                        if (!vgroup1 || vgroup1->KeyId() == -1 ||
                            (*vgroup1 == pBalRelItem->m_VGroup1 && !vgroup2) ||
                            (vgroup2 && *vgroup2 == pBalRelItem->m_VGroup2 &&
                                *vgroup1 == pBalRelItem->m_VGroup1))
                            Add(pBalRelItem);
                    }
                }
            }
        }
    }
}

```

zero comments

Disclosure

- Researchers retained an EFF Attorney (Cindy Cohn)
 - Worry about Diebold suing for copyright violations, leaking of trade secrets (DMCA)
- Also worked with general counsels at Johns Hopkins, Rice
- No election pending at the time of disclosure
- Technical paper eventually published at IEEE S&P

This paper, copyright the IEEE, appears in *IEEE Symposium on Security and Privacy 2004*. IEEE Computer Society Press, May 2004. This paper previously appeared as Johns Hopkins University Information Security Institute Technical Report TR-2003-19, July 23, 2003.

Analysis of an Electronic Voting System

TADAYOSHI KOHNO*

ADAM STUBBLEFIELD†

AVIEL D. RUBIN‡

DAN S. WALLACH§

February 27, 2004

Potential solutions

Separate vote casting from tabulating

A touch screen machine produces paper ballot that a voter can use or destroy. Then, a scanning and tabulating machine (with a small, open-source, verified code base) tallies the screen-generated ballot.

Design transparency

Require machine design and source code to be public and verified by security experts. Create standardization bodies that vet voting machine manufacturers and the machines themselves.



Some
thoughts
on e-voting

Threat modeling

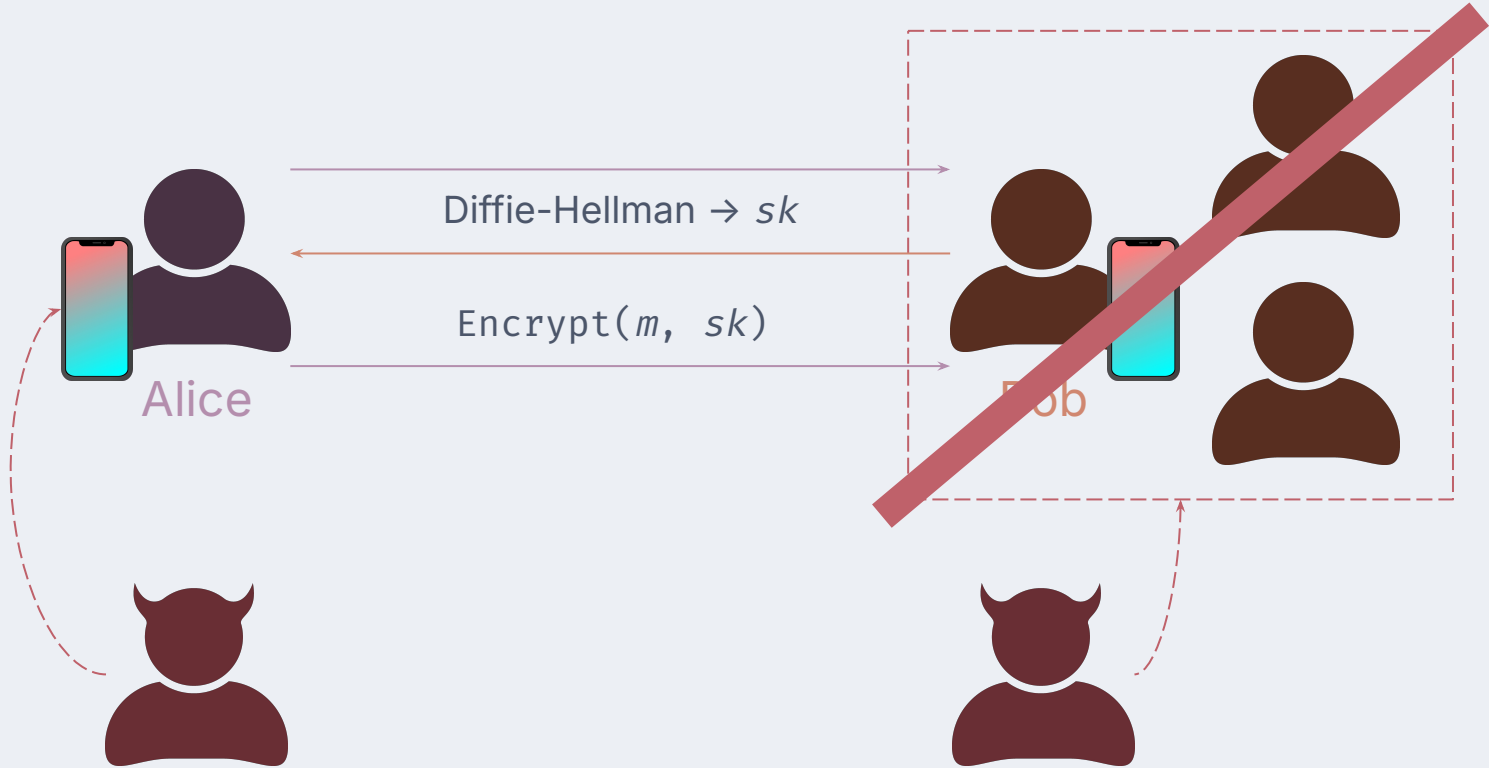
- Type of election (public vs. private)
- Consequences of a successful attack
- Value of election outcome to potential adversaries
- Expertise, skill & resources needed to disrupt
- Level of motivation of potential attackers
- Amount of disruption needed to sway the election or call its outcome into doubt
- Consequences of a perception of unfair outcome

Platform issues

- Hardware manufacturer
- OS vendor
- Applications (Office, web browser, remote control, anti-virus)
- Physical access (insider threat, forensic adversary)
- Software bugs/vulnerabilities

Would these be used to subvert an election?

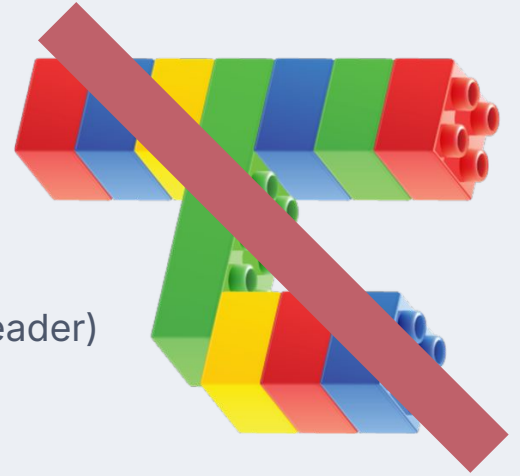
It depends on the threat model, the importance of the election, and the resources of the adversary.



Internet voting in public elections

- Social issues:
 - Vote coercion
 - Vote sale
 - Vote solicitation (click here to vote, banner ads)
- Technical issues:
 - Securing the platform
 - Securing the communications channel
 - Assuring availability of the network
 - Registration issues, one vote per person, no dead voters
 - Authentication in each direction
 - Maintaining equitable costs (no poll tax, e.g. smartcard reader)

Please never do this



Opinions

1. The Windows/Mac/Linux/Mobile environments are totally inadequate as a voting machine in public elections.
2. The current Internet is totally inadequate as a communications infrastructure in public elections.
3. The *level of threat* to *difficulty of attack* ratio for public elections in today's environment is too high.
4. Even if we could solve the technical issues, there are still social issues that are deal breakers for Internet voting in public elections.
5. Stick to optical scanning with poll-site tallying!

The security of voting should be a non-partisan issue.
Too much is at stake for party politics.

Looking ahead

- Exam 1 grades are available on Blackboard
 - To get back your exam and rubric, email me from your CCNY email with the subject line “EE G7701 Exam 1 [LastName]”
- Lab 6 deadline extended to **Thu Oct 31, 10p**
- **Today's activity:** project check-in 1 with your group
 - Checking see if you're making enough progress each week
 - Due tomorrow 10p, but you can/should probably finish it in class today

Lesson objectives

- Describe e-voting systems and their potential flaws
- Understand the design considerations inherent to e-voting
- Explain the societal implications of using e-voting systems