Securing Digital Democracy

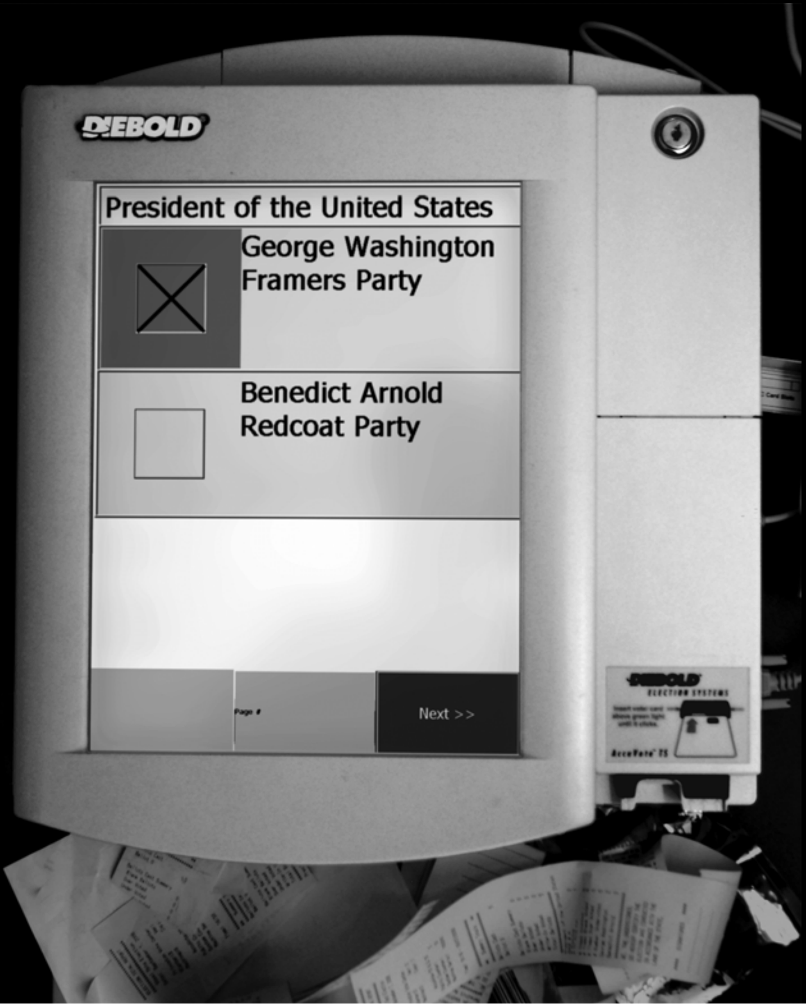
Lecture 1 | *Voting as a Security Problem*

J. Alex Halderman
University of Michigan

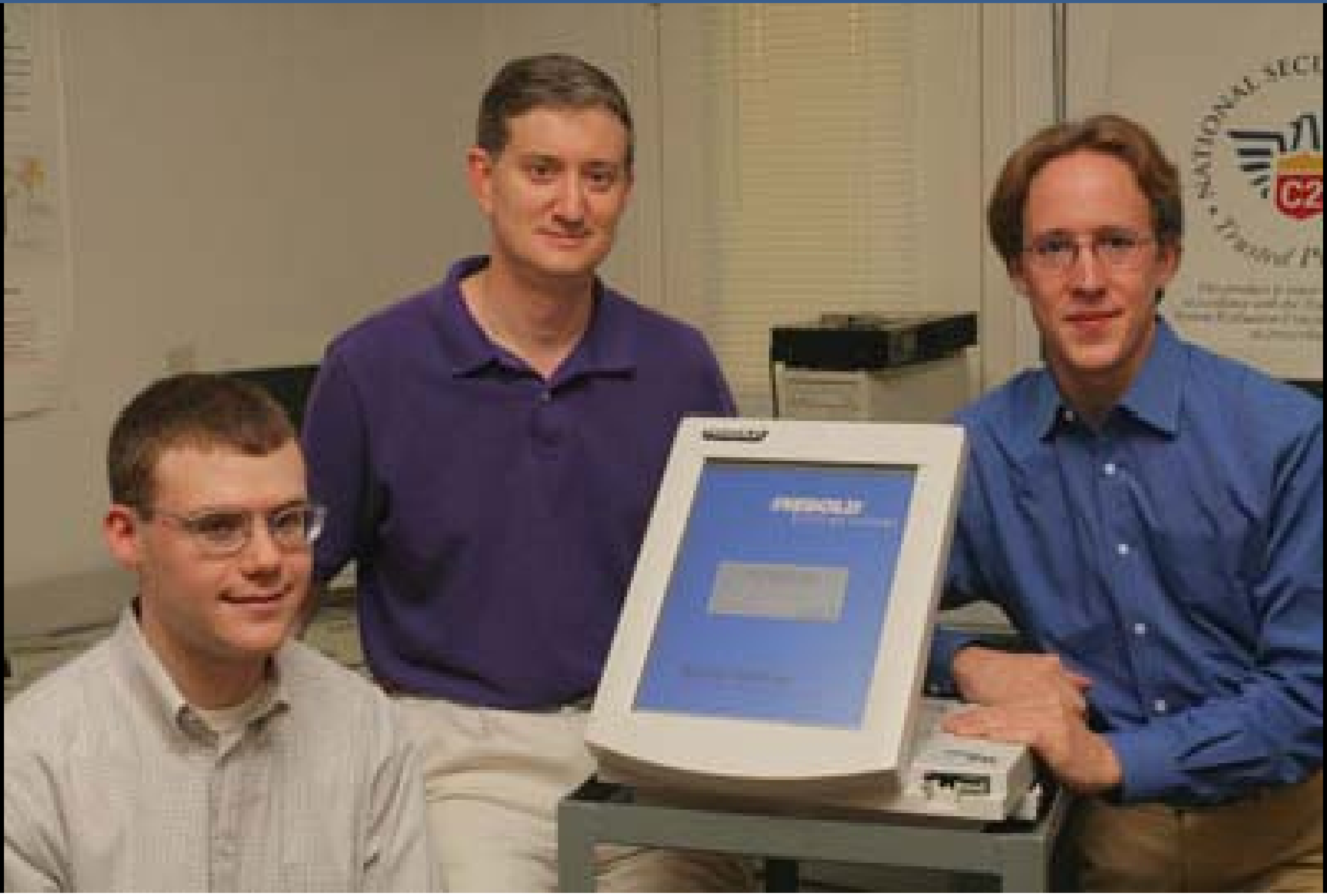
1.1 Welcome

Welcome!

1.1 Welcome


DIEBOLD
President of the United States
☒ George Washington
Framers Party
□ Benedict Arnold
Redcoat Party
Page #
Next >>
DIEBOLD
ELECTION SYSTEMS
AccuVote TS

1.1 Welcome



1.1 Welcome

DUPLICATION PROHIBITED
2 Volta
Street
VChat
Lookup
Monitoring?
Save
MICHIGAN ENGINEERING

Deny entry to India
and notify originator

Goals for the Course

Understand how your vote is counted.
You should have confidence in the results…or not?

Learn to apply the security mindset to reason about attacks and defenses, in elections and beyond.

Critically examine the role of technology in elections, including results of recent research.

Find out what you can do to make elections fair and accurate.

Syllabus

1. Voting as a Security Problem
2. How We Got Here
3. Computers at the Polls
4. Problems with DREs
5. Security Procedures
6. E-Voting around the World
7. Human Factors
8. Internet Voting
9. Using Technology Wisely
10. E-Voting and Public Policy

The Security Mindset

The Adversary

Computer security studies how systems behave in the presence of an *adversary*.

"*The adversary*"

a.k.a. "*the attacker*"

a.k.a. "*the bad guy*"

Know your enemy.

Thinking like an Attacker

Understand techniques for circumventing security.

Look for ways security can break, not reasons why it won’t.

Sun Tzu
author of
The Art of War

Thinking Like an Attacker

- Look for weakest links – easiest to attack
- Identify assumptions that security depends on – are they false?
- Think outside the box: not constrained by system designer's worldview

Practice thinking like an attacker:
For every system you interact with, think about what it means for it to be secure, and image how it could be exploited by an attacker.

Practice Thinking Like an Attacker

In your college math course,
Prof. Rote is giving the final exam:

> Write the first 100 digits of pi:
> 3.________________________________

Available in advance.
Closed book, closed notes.

How would you cheat?

WHAT COULD GO WRONG?

Thinking as a Defender

Security policy

- What are we trying to protect?
- What properties are we trying to enforce?

Threat model

- Who are the attackers? Capabilities? Motivations?
- What kind of attack are we trying to prevent?

Risk assessment

- What are the weaknesses of the system?
- What will successful attacks cost us?
- How likely?

Countermeasures

- Costs vs. benefits?
- Technical vs. nontechnical?

Challenge is to think rationally and rigorously about risk. *Rational paranoia.*

What **Security Requirements** do election systems need to enforce?

Integrity

The outcome matches voter intent.

Votes are cast as intended.

Votes are counted as cast.

Security Requirements

☑ Integrity

Ballot Secrecy

Weak form:

Nobody can figure out how you voted…

Strong form:

…even if you try to prove it to them.

Security Requirements

☑ Integrity

☑ Ballot Secrecy

Voter Authentication

Only authorized voters can cast votes,

and

each voter can only vote up to the permitted number of times.

Security Requirements

☑ Integrity

☑ Ballot Secrecy

☑ Voter Authentication

Enfranchisement

All authorized voters have the opportunity to vote.

Security Requirements

- ☑ Integrity
- ☑ Ballot Secrecy
- ☑ Voter Authentication
- ☑ Enfranchisement

Availability

The election system is able to accept all votes on schedule and produce results in a timely manner.

Security Requirements

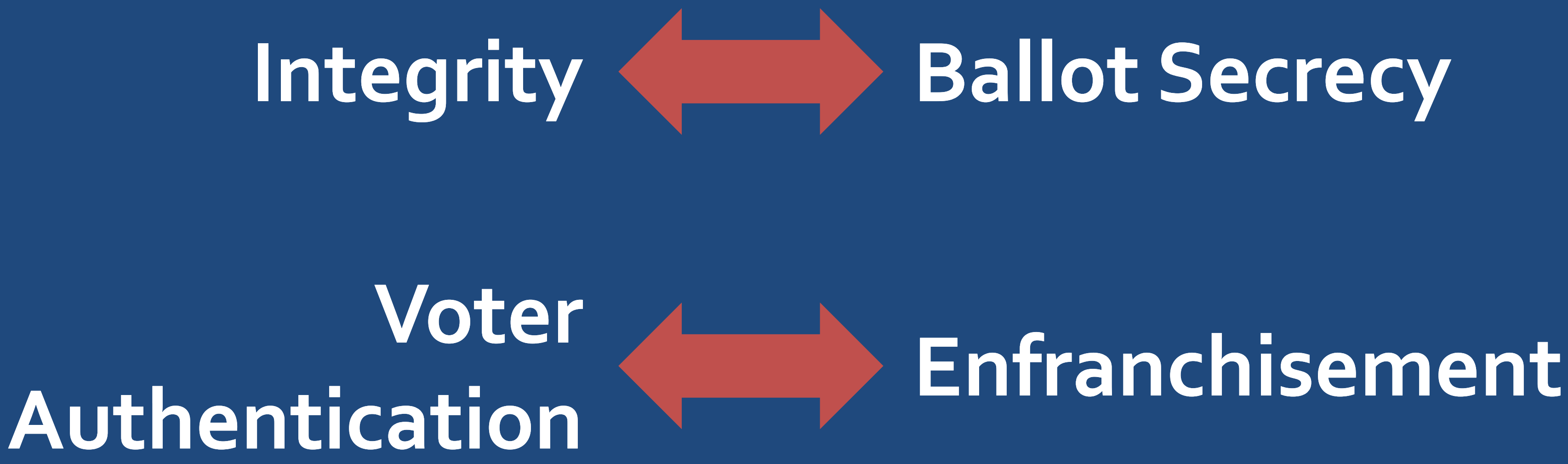
☑ Integrity

☑ Ballot Secrecy

☑ Voter Authentication

☑ Enfranchisement

☑ Availability



Integrity ⟷ Ballot Secrecy

Voter Authentication ⟷ Enfranchisement

1.3 Security Requirements for Voting

Security Requirements

☑ Integrity

☑ Ballot Secrecy

☑ Voter Authentication

☑ Enfranchisement

☑ Availability

Other Important Properties

☑ Cost Effectiveness

☑ Accessibility

☑ Convenience

☑ Intelligibility

Securing Digital Democracy

Lecture 1 | *Voting as a Security Problem*

J. Alex Halderman
University of Michigan