

Electronic Voting Machines (DREs)

- Voter inserts a smartcard that encodes which races the voter can vote in
- Voter selects choices on a touchscreen monitor
- Votes are stored on an electronic storage device

Lots Of Advantages

- Easy to use - voters love them
- Support for multiple languages
- Support for voters with disabilities

Privacy

Integrity

Privacy

- Nobody should be able to figure out how anyone else voted
- Some programs for overseas voters already compromise privacy

Integrity

- The winner of the election should be the candidate that received the most votes
- There's always going to be some errors due to everything from user error to machine malfunction

Dealing With Errors

- If the election is within the margin of error, from a scientific perspective it's a tie
- Nobody's happy with this, so our laws essentially assign a winner
- This is only reasonable if the errors are random

Errors

- If the problem is that some voting machine just isn't able to read some small percentage of votes
 - The error is essentially random
 - Assigning a winner is like flipping a coin

Errors

- If the error includes any malicious activity, like intentionally flipping a small number of voters on a small number of machines
 - The error is no longer random
 - Assigning a winner is like flipping a weighted coin - someone's more likely to win

Privacy

Integrity

Privacy

Integrity

Preventable

Detectable

Undetectable

Preventable

- Can be caught before any damage is done
- Poll worker can check to make sure that nobody tries to stuff multiple ballots into the box

Detectable

- Can be detected after the damage is done, but generally some sort of corrective action is required
- If we count the number of ballots in the ballot box, and it doesn't match the number of voters something went wrong

Detectable to Preventable

- If we know about the attack, detectable attacks can become preventable
 - The smartcards on some electronic voting machines have been shown to be insecure
 - If we know this, poll workers can watch to make sure that someone doesn't insert their own smartcard

Undetectable

- Cannot be detected, even after the election is over
- If a small number of machines switch a small number of votes from one candidate to another

Why Undetectable?

- How could we hope to detect an undetectable attack?
 - Certification
 - Logic and accuracy testing
 - Parallel testing

Certification

- We don't know how to verify that complex software systems are secure
- Not a problem with incomplete specifications
- Not a problem of not enough time or money
- We just don't know how to do it

What About Airplanes?

- Avionics systems are designed to be *reliable*, not *secure*
- If a pilot wants to crash a plane, the plane doesn't stop him

What About ATMs?

- ATMs are *auditable* (and have a paper trail)
- Because they don't have to forget any information, all errors are detectable
- We can easily build auditable voting machines too, they just can't be private

Logic and Accuracy Testing

- Great for making sure that the ballot looks right
- Completely worthless for security
 - Doesn't look like a real election, the machines can tell the difference

Parallel Testing

- Taking a very small percentage of machines and trying to run a parallel election on them will only detect problems if:
 - You get lucky in choosing the machines
 - The parallel election looks exactly like the real election does
 - Still doesn't detect "knock" attacks

Privacy

Integrity

Preventable Detectable Undetectable

Privacy

Integrity

Preventable Detectable Undetectable

Large Conspiracy

Single Attacker

Single Attacker

- We can't verify that software is secure
- We can't detect if a few random machines flip a few selected votes when it looks like a real election is going on
- It only takes one person to change the software to do this

Privacy

Integrity

Preventable

Detectable

Undetectable

Large Conspiracy

Single Attacker

Solutions

- Paper trail
 - Ensures that no vote flipping can occur - still need good procedures for other attacks
- Cryptographic tricks
 - Ensure not only that every votes is cast correctly, but that every vote is counted - currently still need paper though