March 13, 2014

1. Scantegrity
2. Process Modeling
3. Internet Voting

Scantegrity

- Goal: allow detection of both ballot chain of custody and software system compromise that will affect election integrity
- Builds on optical scan systems
- Allows voters to verify their ballots counted correctly
- Used in some small civic elections in Maryland
- Structure:
  - Vote casting procedure
  - Election audit procedures
  - Dispute resolution process

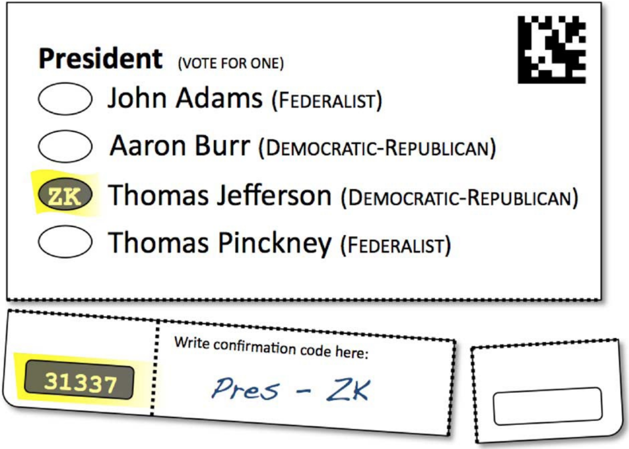
Vote Casting Procedure

- The ballots
  - Ovals have background with reactive ink with confirmation code printed in the oval
  - Detachable part to note confirmation codes
  - Serial number that is hard to read (eg, QR code)
- Marking the ballots
  - Voter given ballot enclosed in a privacy sleeve
  - Fill in oval with special pen; background immediately turns dark, leaving visible confirmation code
  - Voter can record confirmation code on detachable part
  - After 5–7 minutes, oval turns completely dark, obscuring confirmation code

Vote Casting Procedure

- The ballots
  - Ovals have background with reactive ink with confirmation code printed in the oval
  - Detachable part to note confirmation codes
  - Serial number that is hard to read (eg, QR code)
- Marking the ballots
  - Voter given ballot enclosed in a privacy sleeve
  - Fill in oval with special pen; background immediately turns dark, leaving visible confirmation code
  - Voter can record confirmation code on detachable part
  - After 5–7 minutes, oval turns completely dark, obscuring confirmation code

Picture of Ballot



President (VOTE FOR ONE)

○ John Adams (FEDERALIST)

○ Aaron Burr (DEMOCRATIC-REPUBLICAN)

● ZK Thomas Jefferson (DEMOCRATIC-REPUBLICAN)

○ Thomas Pinckney (FEDERALIST)

31337

Write confirmation code here:

Pres - ZK

Election Audit Procedure

- Auditing a printed ballot
    - Done by voter before they vote
    - Select printed ballot from pile
    - Given main body, one half of detachable part, serial number on that part
    - Voter fully marks ballot at his/her leisure to reveal *all* confirmation codes
- Checking confirmation numbers
    - Voters go to web site, enter detachable serial number
    - Web site reports confirmation codes *not candidates* in positions (it believes) marked for voted ballots

Dispute Resolution Process

- Voter provides confirmation code they believe should be on ballot
- Likelihood of guessing a correct code is low

Election Process

- Elections are a *process* composed of specific tasks
- Tasks related to one another
  - Temporal order (one must follow another)
  - Dependency (output from one task used as input to another)
  - Exception handling (handling problems)
- Machines may perform these tasks

Continuous Process Improvement

1. Create a precise, accurate model of the real-world election process
2. Use formal analysis methods to automatically identify potential problems in the model
   - We focus on single points of failure
3. Modify process model to ameliorate problems
   - Verify the modification makes things better
4. Deploy improvements in real-world process
5. Repeat steps 2–4

Fault Tree Analysis

- Fault trees show how problems could arise
- Can automatically generate fault trees from process model and a hazard
  - Hazards are conditions under which undesired, possibly dangerous events may occur
- Analyze fault trees automatically to identify points of failure
  - Especially Single Points of Failure (SPFs)

Compute Cut Sets

- Combination of events such that, if all events in the cut set occur, the hazard occurs
    - Minimal if removal of any event causes the resulting set not to be a cut set
- Can be computed automatically from the fault tree

Use Them!

- Process
  - Change process to reduce number of SPFs
  - Gives changes to procedures to detect, handle failures
- Machine
  - Determine inputs to, outputs from particular tasks
  - Compare existing systems to existing process to find discrepancies

Internet Voting

- A generic term for many different possible ways to handle the casting and transmission of votes over the Internet
- First version: voter votes at home on a PC using a web browser connected to a server at Election Central
- Second version: voter votes at special kiosk that then transmits the votes to Election Central over the Internet
    - This is like the first, but the PC—the kiosk—is (essentially) trusted
    - So only talk about first

First Version: How to Do It

- PC transmits authentication information of voter to Election Central
- Election Central transmits ballot to PC
- PC displays ballot
- PC records vote
- PC transmits vote to Election Central server

First Version: How to Do It

- PC transmits authentication information of voter to Election Central
- Election Central transmits ballot to PC
- PC displays ballot
- PC records vote
- PC transmits vote to Election Central server

Every step can be compromised

First Version: How to Attack It

- PC transmits authentication information of voter to Election Central
    - PC contacts fake Election Central site
    - PC has a Trojan horse that constructs bogus data
    - User requests wrong ballot
- Election Central transmits ballot to PC
    - Ballot is a PDF with malicious content
    - Wrong ballot is sent
- PC displays ballot
    - Display does not match underlying ballot

First Version: How to Attack It

- PC records vote
  - User cannot cast vote for desired candidates, races
  - Displayed votes on ballot do not match votes stored in computer
- PC transmits vote to Election Central server
  - PC cannot contact Election Central
  - PC again contacts fake Election Central site
  - PC sends incorrect votes to EC
  - Attacker intercepts ballot in transit, either deletes it or changes it
- Software, hardware maybe compromised by vendors, third parties

Server at Election Central

- As is on the Internet, *anyone* can access it
- Standard server side technology riddled with holes
  - Need to write your own server *from scratch*
- Even if server carefully written, relies on flawed libraries, operating systems, and network infrastructure
- Small configuration errors may create gaping vulnerabilities
- Procedures and policies may also cause security problems
- Attacker only needs to find one problem

Bottom Line

- NASDAQ, Pentagon, government sites regularly penetrated
- If those experts cannot stop compromises, why should we assume election servers will be invulnerable?

Bottom Line

- NASDAQ, Pentagon, government sites regularly penetrated
- If those experts cannot stop compromises, why should we assume election servers will be invulnerable?

Key Question:
as a citizen and a voter, are you comfortable that your vote will not be altered or discarded undetectably?