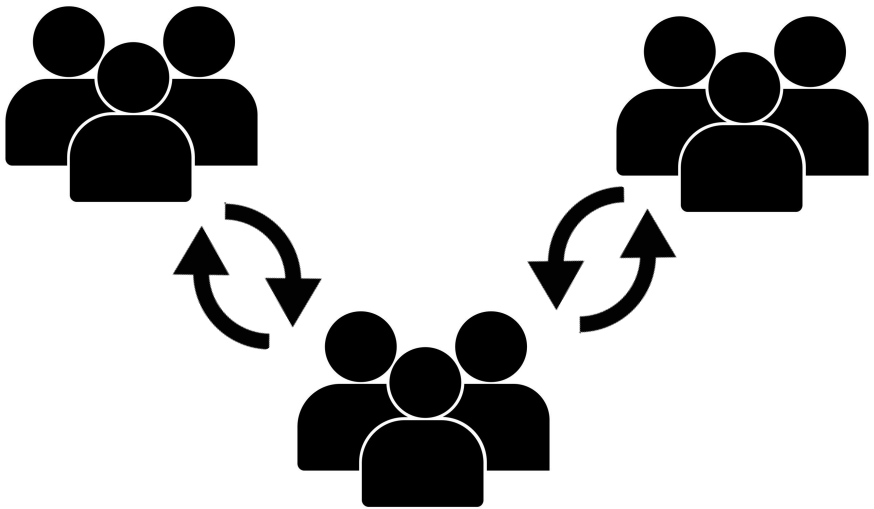
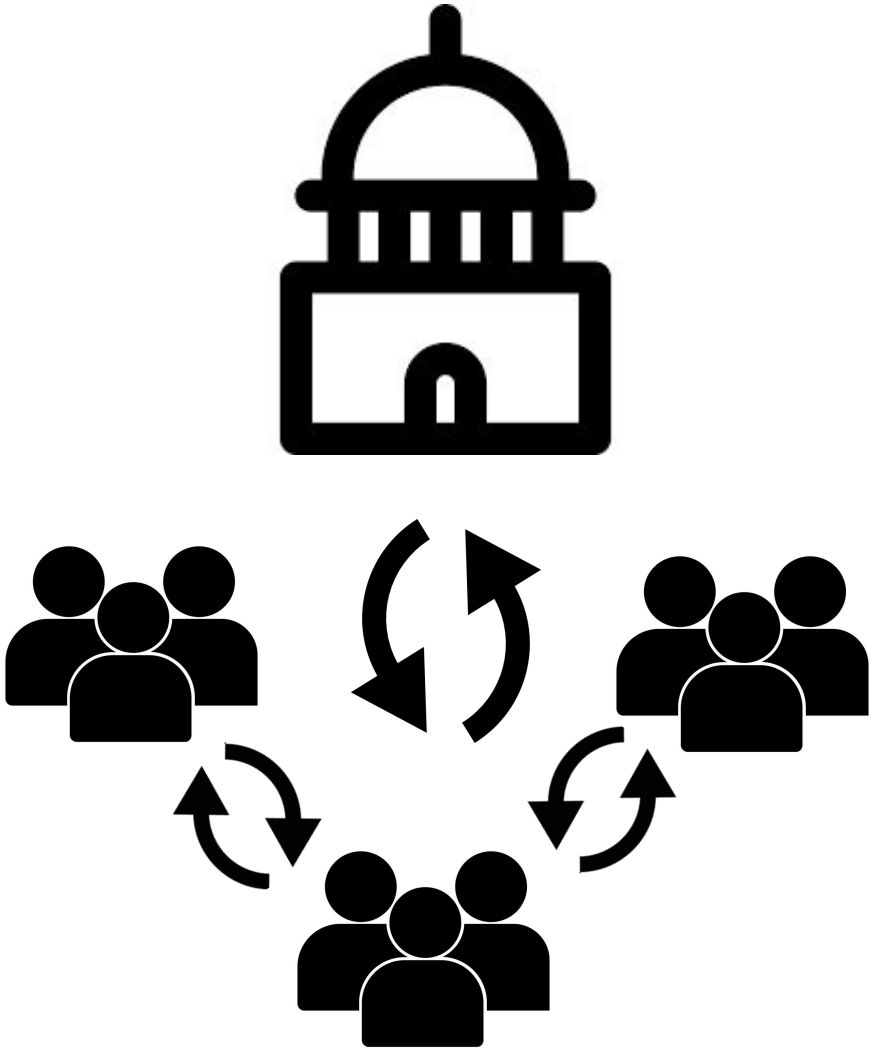
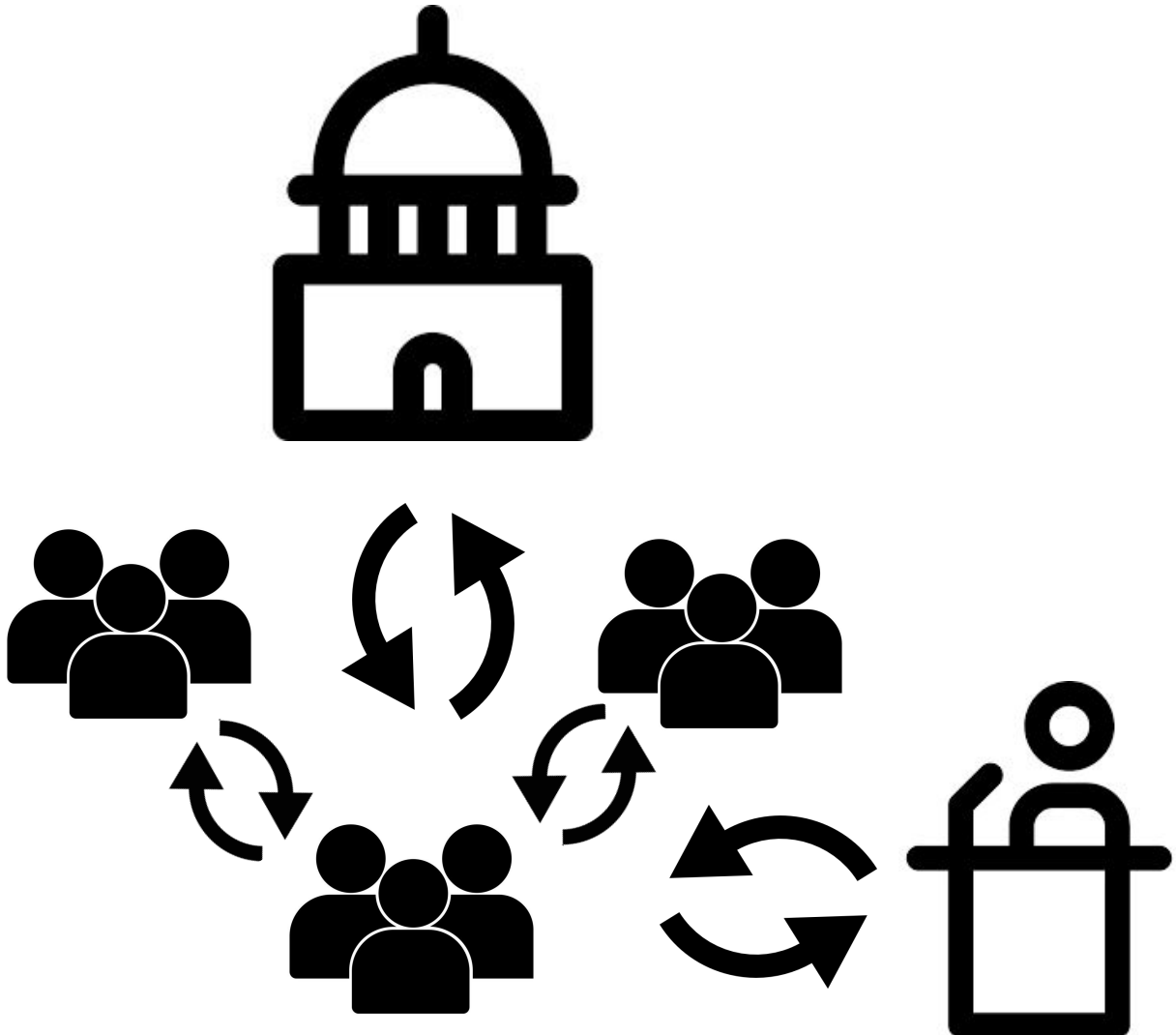
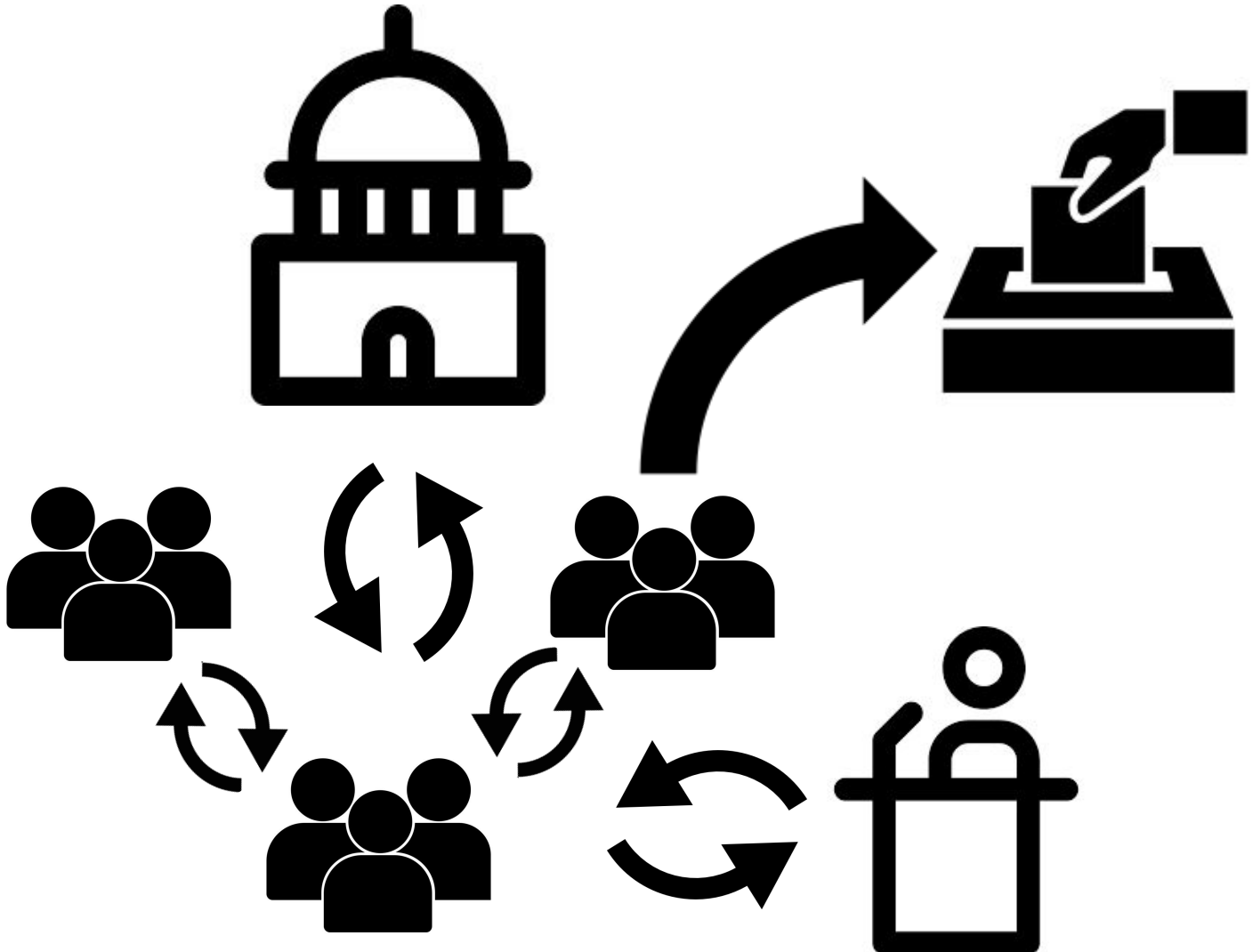
Election Security

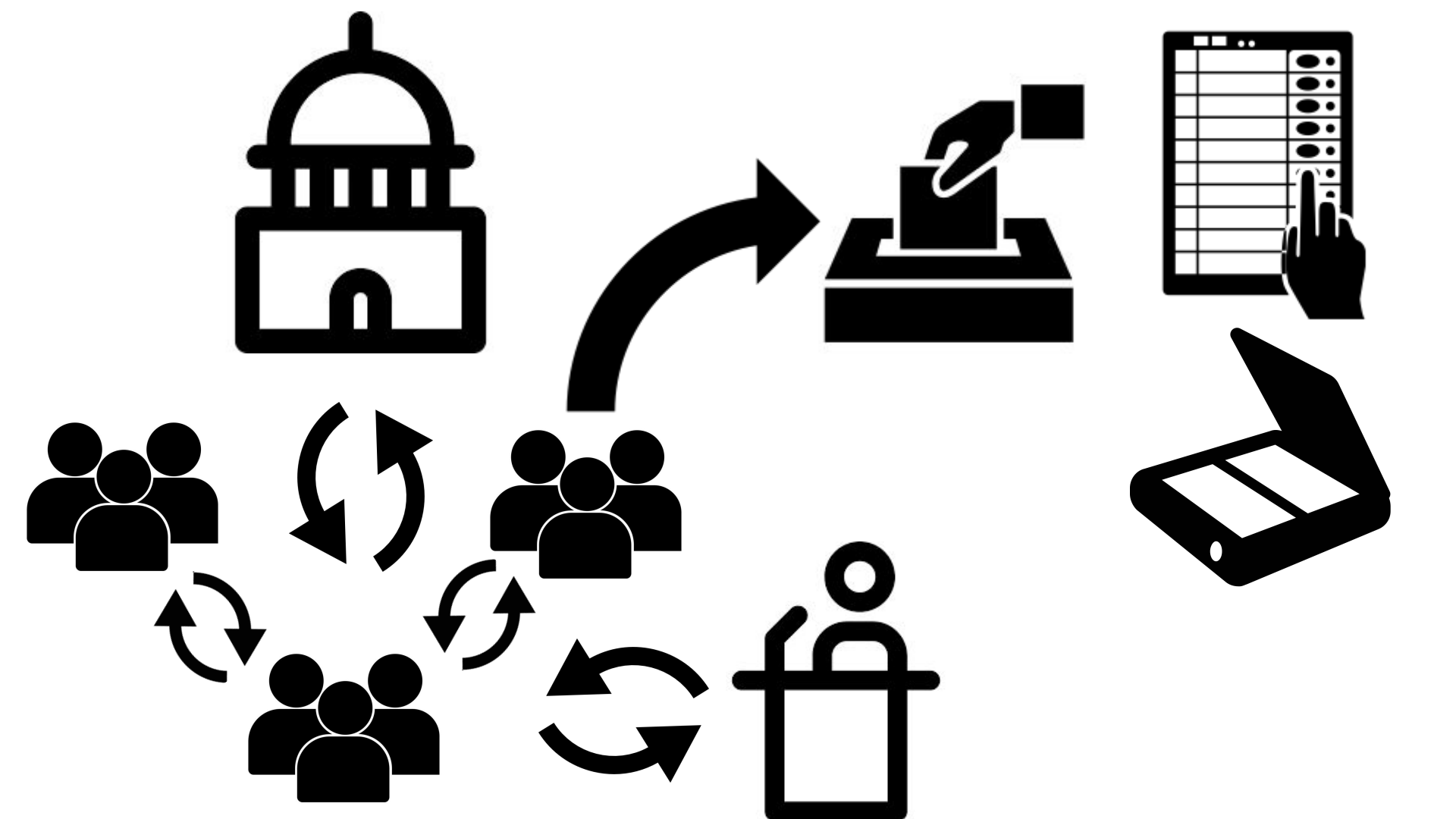
Leah Namisa Rosenbloom
Brown University
CSCI 1660 Guest Lecture
Spring 2018

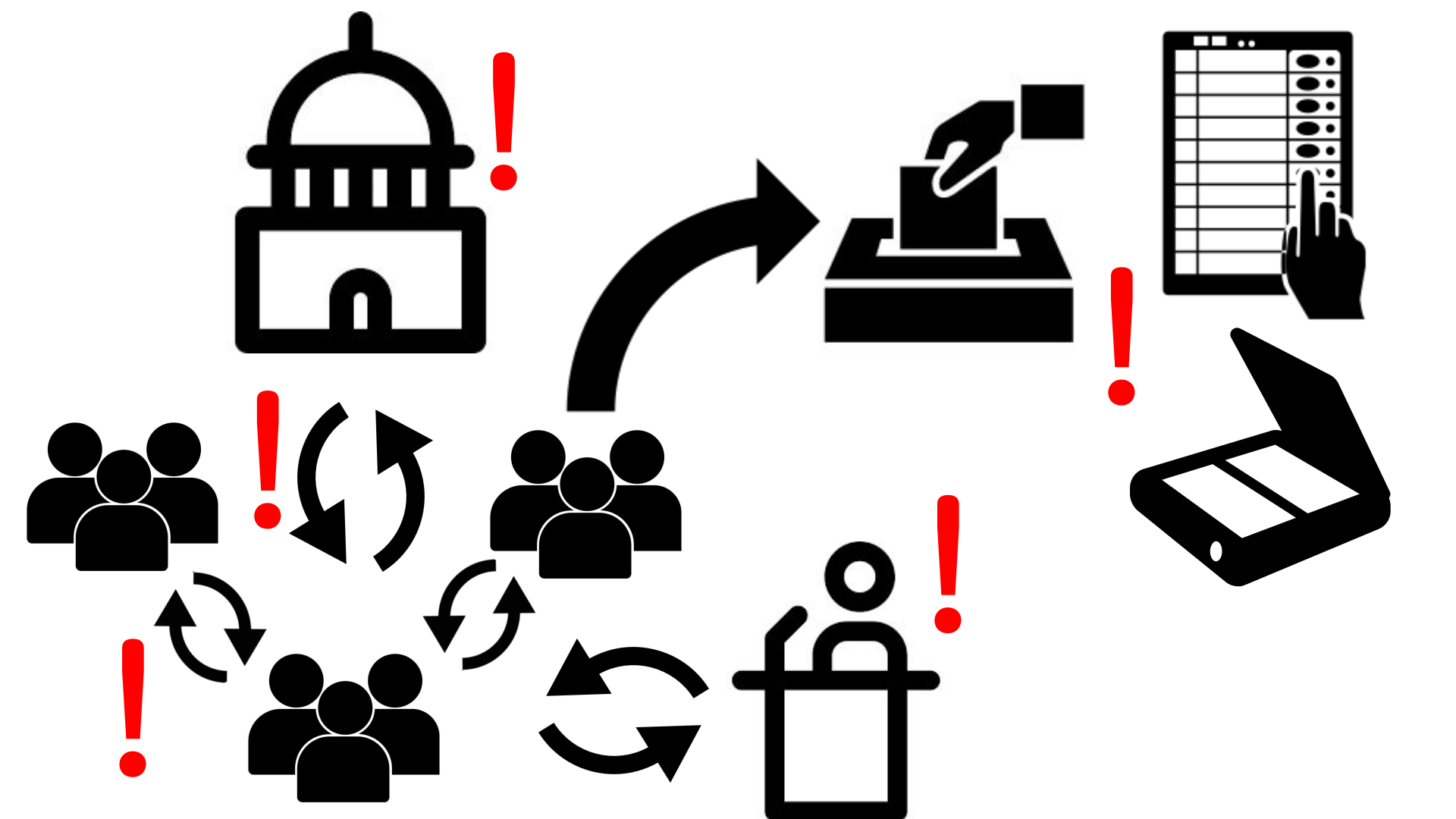












But what is Election Security?

- “Free and Fair” process
- Faith in results
- Peaceful transfer of power

But what is Election Security?

- “Free and Fair” process
- Faith in results
- Peaceful transfer of power

Your opinion matters.

Lecture Overview

- Electoral process ✓
- Electronic voting systems Then (2006) and Now (2017)
- Regulation v. certification
- Security beyond voting systems
- Security beyond technology

2006: Diebold AccuVote-TS(x)

- *Security Analysis of the Diebold AccuVote-TS Voting Machine*,

  Ariel Feldman, Alex Halderman, Edward Felten (2006)
- Diebold AccuVote-TS(x) widely deployed in US (10%) and Canada
  - Direct Recording Electronic (DRE) voting system:

    general-purpose computers running specialized election software
- First comprehensive analysis of deployed DRE
- Found to be extremely vulnerable

Why? Here's the Setup (Part 1):

- ★ Hardware
  - power switch, keyboard port, two PC Card slots behind lightweight, uniform lock
    - PC Card slot 1: removable flash memory card
    - PC Card slot 2: modem card for transferring ballot definitions and results
  - two switches and jumpers on motherboard control source of bootloader
    - Source 1: on-board flash memory (default)
    - Source 2: erasable programmable (EP) ROM chip in motherboard socket
    - Source 3: proprietary flash memory in "ext flash" slot

Why? Here's the Setup (Part 1):

- ★ Hardware
  - power switch, keyboard port, two PC Card slots behind lightweight, uniform lock
    - PC Card slot 1: removable flash memory card
    - PC Card slot 2: modem card for transferring ballot definitions and results
  - two switches and jumpers on motherboard control source of bootloader
    - Source 1: on-board flash memory (default)
    - Source 2: erasable programmable (EP) ROM chip in motherboard socket
    - Source 3: proprietary flash memory in "ext flash" slot
- ★ Software: Windows CE, Diebold BallotStation

Why? Here's the Setup (Part 1):

- ★ Hardware
  - power switch, keyboard port, two PC Card slots behind lightweight, uniform lock
    - PC Card slot 1: removable flash memory card
    - PC Card slot 2: modem card for transferring ballot definitions and results
  - two switches and jumpers on motherboard control source of bootloader
    - Source 1: on-board flash memory (default)
    - Source 2: erasable programmable (EP) ROM chip in motherboard socket
    - Source 3: proprietary flash memory in "ext flash" slot
- ★ Software: Windows CE, Diebold BallotStation
- ★ On Boot
  - bootloader copies self into RAM, initializes hardware
  - if memory card in PC Card slot 1, search for update files
    - if fboot.nb0 found, replace bootloader in on-board flash memory with contents
    - if nk.bin found, replace OS image in on-board flash memory with contents
    - if EraseFFX.bsq found, erase file system area in on-board flash memory
  - uncompress OS image, copy to RAM, release control to OS kernel (see Part 2)

Why? Here's the Setup (Part 1):

- ★ Hardware
  - power switch, keyboard port, two PC Card slots behind lightweight, uniform lock
    - PC Card slot 1: removable flash memory card
    - PC Card slot 2: modem card for transferring ballot definitions and results
  - two switches and jumpers on motherboard control source of bootloader
    - Source 1: on-board flash memory (default)
    - Source 2: erasable programmable (EP) ROM chip in motherboard socket
    - Source 3: proprietary flash memory in "ext flash" slot
- ★ Software: Windows CE, Diebold BallotStation
- ★ On Boot
  - bootloader copies self into RAM, initializes hardware
  - if memory card in PC Card slot 1, search for update files
    - if fboot.nb0 found, replace bootloader in on-board flash memory with contents
    - if nk.bin found, replace OS image in on-board flash memory with contents
    - if EraseFFX.bsq found, erase file system area in on-board flash memory
  - uncompress OS image, copy to RAM, release control to OS kernel (see Part 2)

Points of Discussion (5 min)**:**

1. what are the vulnerabilities?
2. what is the severity/scope?
3. what are the solutions?

Bootloader Blues

- bootloader can reprogram itself and the entire OS, overwrite flash memory
- overwriting is permanent (excluding hard reset)
- takes orders from removable media in PC Card Slot 1
- removable media port is behind flimsy lock

⇒ attacker with access to PC Card Slot 1 can permanently reprogram machine

Mitigation

- authenticate updates with digital signatures
- increase physical security and tighten chain of custody

Why vulnerable? Here's the Setup (Part 2):

- ★ On OS init
  - kernel runs Filesys.exe, which unpacks registry and runs programs in \Init
    - shell.exe (Debug Shell), device.exe (Device Manager), gwes.exe (Graphics, Windowing, and Events Subsystem), taskman.exe (Task Manager)
  - Device Manager mounts filesystems
    - on-board flash mounted at \FFX
    - memory card (if present) mounted at \Storage Card using FAT or FAT32
    - root file system mounted at \ in RAM
  - if memory card inserted, Task Manager searches for files
    - if files ending in .ins (proprietary scripts) found, confirm with user and run scripts
    - if explorer.glb found, launch Windows Explorer
      - else, launch BallotStation.exe from \FFX\Bin

Why vulnerable? Here's the Setup (Part 2):

- ★ On OS init
  - kernel runs Filesys.exe, which unpacks registry and runs programs in \Init
    - shell.exe (Debug Shell), device.exe (Device Manager), gwes.exe (Graphics, Windowing, and Events Subsystem), taskman.exe (Task Manager)
  - Device Manager mounts filesystems
    - on-board flash mounted at \FFX
    - memory card (if present) mounted at \Storage Card using FAT or FAT32
    - root file system mounted at \ in RAM
  - if memory card inserted, Task Manager searches for files
    - if files ending in .ins (proprietary scripts) found, confirm with user and run scripts
    - if explorer.glb found, launch Windows Explorer
      - else, launch BallotStation.exe from \FFX\Bin
- ★ BallotStation procedures
  - determine mode from \Storage Card\CurrentElection\election.brs (see Part 3)
  - if card is replaced, transition to mode specified by newly inserted card
  - if machine is rebooted, return to mode specified by currently inserted card

Under New Management

- Windows Explorer gives full access to file systems, control panel

  ⇒ attacker with access to PC Card Slot 1 gets access to file systems, control panel
- root file system mounted in RAM ⇒ reboot destroys evidence
- multiple stack-based buffer overflows in .ins script handling
- BallotStation takes orders from removable media in PC Card Slot 2

Mitigation

- authenticate Windows Explorer, BallotStation, script requests
- mount file systems in nonvolatile memory

Why vulnerable? Here's the Setup (Part 3):

- ★ BallotStation modes: Pre-Download, Pre-Election Testing, Election, Post-Election
- ★ Election Setup
  - machines stored in facility with access control, delivered to poll workers pre-election
  - poll workers configure BallotStation with ballot description
    - Option 1: insert memory card into PC Card Slot 2
    - Option 2: download ballot definition by connecting to Windows PC running Diebold's Global Elections Management System (GEMS) server software
  - poll workers test machine for "logic and accuracy" by simulating election, get zero tape

Why vulnerable? Here's the Setup (Part 3):

- ★ BallotStation modes: Pre-Download, Pre-Election Testing, Election, Post-Election
- ★ Election Setup
  - machines stored in facility with access control, delivered to poll workers pre-election
  - poll workers configure BallotStation with ballot description
    - Option 1: insert memory card into PC Card Slot 2
    - Option 2: download ballot definition by connecting to Windows PC running Diebold's Global Elections Management System (GEMS) server software
  - poll workers test machine for "logic and accuracy" by simulating election, get zero tape
- ★ Voting: poll workers authorize voter with smart card, voter approaches machine & casts vote, machine invalidates card, poll workers re-enable card for new voter

Why vulnerable? Here's the Setup (Part 3):

- ★ BallotStation modes: Pre-Download, Pre-Election Testing, Election, Post-Election
- ★ Election Setup
  - machines stored in facility with access control, delivered to poll workers pre-election
  - poll workers configure BallotStation with ballot description
    - Option 1: insert memory card into PC Card Slot 2
    - Option 2: download ballot definition by connecting to Windows PC running Diebold's Global Elections Management System (GEMS) server software
  - poll workers test machine for "logic and accuracy" by simulating election, get zero tape
- ★ Voting: poll workers authorize voter with smart card, voter approaches machine & casts vote, machine invalidates card, poll workers re-enable card for new voter
- ★ Tallying Results
  - poll workers insert "Ender" card, get result tape, check voter count against votes cast
  - results transferred to central tabulator PC running GEMS software
    - Option 1: transfer over LAN, phone line, or serial cable
    - Option 2: "accumulate" results into one machine using memory cards of others
  - if recount, check tape v. memory cards and re-tabulate; if needed examine on-board FS

Cross Contamination

- Network awareness
- Accumulation ⇒ shared removable media
- *Number* of votes consistent ⇒ result tape consistent
- Result tape, memory cards, logs always consistent but not necessarily correct

  ⇒ attacker can tamper with votes and election results will pass audits, recount

Mitigation

- Authenticate updates, restrict communication, limit memory card sharing
- Voter Verified Paper Audit Trails (VVPAT)

Three-Layer Offense (Harri Hursti, 2006)

1. Application software (replace instructions)
2. Operating system (replace person reading instructions)
3. Bootloader (replace supreme entity that creates person)

Three-Layer Offense (Harri Hursti, 2006)

1. Application software (replace instructions)
2. Operating system (replace person reading instructions)
3. Bootloader (replace supreme entity that creates person)

Successful Attacks (Feldman et al., 2006)

- Targeted and infectious vote-stealing (stealth mode)
  - check for Election mode, “secret knock”
  - suspend BallotStation, scan result files, alter them arbitrarily
  - simulate normal procedure (pretend to update, confirm changes, etc.)
  - spread like a virus via infected memory cards
- Denial-of-Service (havoc mode)
  - overwrite file system contents of on-board flash memory, memory card(s)
    - destroys all current election results
    - renders machine inoperable
  - modify, corrupt ballot description

Gems from the Diebold Timeline

- 2000: Diebold linked to disappearance of 16,000 votes for Al Gore in Florida
- 2000-2001: Diebold gives $125,000 to the Republican National Committee
- 2003: Diebold deploys untested machines in California, subsequently banned
- 2004: Diebold CEO pledges commitment to Ohio victory for Bush in Republican fundraising letter, Diebold linked again to voting irregularities
- 2010: Diebold settles SEC accounting fraud charge for $25 million
- 2013: Diebold indicted for using bribery, falsifying documents to get business in China, Indonesia, and Russia

2017: A “Sobering” State of Affairs

- *DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, Matt Blaze, Jake Braun, Harri Hursti, Joseph Hall, Margaret MacAlpine, Jeff Moss (2017)
- 4 days, 25 pieces of election equipment, all breached in some way
  - participants had limited prior knowledge, tools, and resources
- Breaches included remote control, unauthorized access to files and configuration data, default passwords, removable media exploitation, voter data theft
- vulnerabilities threaten confidentiality, integrity, and availability of vote

AVS WinVote (2003-2014)

- remote access over WiFi possible using 2003 exploit
- hacker used Metasploit to gain access to filesystem and escalate privileges to admin
- two unobstructed USB ports on back of machine allow similar access
- unchangeable, universal default password of “adminabcde”

AVS WinVote (2003-2014)

- remote access over WiFi possible using 2003 exploit
- hacker used Metasploit to gain access to filesystem and escalate privileges to admin
- two unobstructed USB ports on back of machine allow similar access
- unchangeable, universal default password of “adminabcde”

Premier/Diebold AccuVote-TSx

- EPROM chip socketed not soldered
- lack of access control on .ini configuration files
- JTAG debugging interface still active

AVS WinVote (2003-2014)

- remote access over WiFi possible using 2003 exploit
- hacker used Metasploit to gain access to filesystem and escalate privileges to admin
- two unobstructed USB ports on back of machine allow similar access
- unchangeable, universal default password of “adminabcde”

Premier/Diebold AccuVote-TSx

- EPROM chip socketed not soldered
- lack of access control on .ini configuration files
- JTAG debugging interface still active

ES&S iVotronic

- red Personal Electronic Ballot (PEB) security fuses intact; tampering possible

AVS WinVote (2003-2014)

- remote access over WiFi possible using 2003 exploit
- hacker used Metasploit to gain access to filesystem and escalate privileges to admin
- two unobstructed USB ports on back of machine allow similar access
- unchangeable, universal default password of “adminabcde”

Premier/Diebold AccuVote-TSx

- EPROM chip socketed not soldered
- lack of access control on .ini configuration files
- JTAG debugging interface still active

ES&S iVotronic

- red Personal Electronic Ballot (PEB) security fuses intact; tampering possible

Sequoia AVC Edge

- firmware protected by 8-bit cipher

Diebold ExpressPoll 5000

- units not properly decommissioned; contained 650,000 voter records
- physical security of removable media thwarted by standard screwdriver
- default username and password available online
- obsolete OS (Windows CE 5) with no input or software validation
  - same bootloader and OS reflashing issue as AccuVote-TS(x)
- pollbook software reads ExPoll.resources to obtain election parameters
  - same unauthorized re-parametrization issue as BallotStation
- possible smart card ID tampering

Diebold ExpressPoll 5000

- units not properly decommissioned; contained 650,000 voter records
- physical security of removable media thwarted by standard screwdriver
- default username and password available online
- obsolete OS (Windows CE 5) with no input or software validation
  - same bootloader and OS reflashing issue as AccuVote-TS(x)
- pollbook software reads ExPoll.resources to obtain election parameters
  - same unauthorized re-parametrization issue as BallotStation
- possible smart card ID tampering

General Concerns

- this was a limited-scope study; imagine what real attackers could do
- supply chain compromised by foreign-made (hardware and software) components
- voting systems in urgent need of further consideration, regulation

Managing DREs

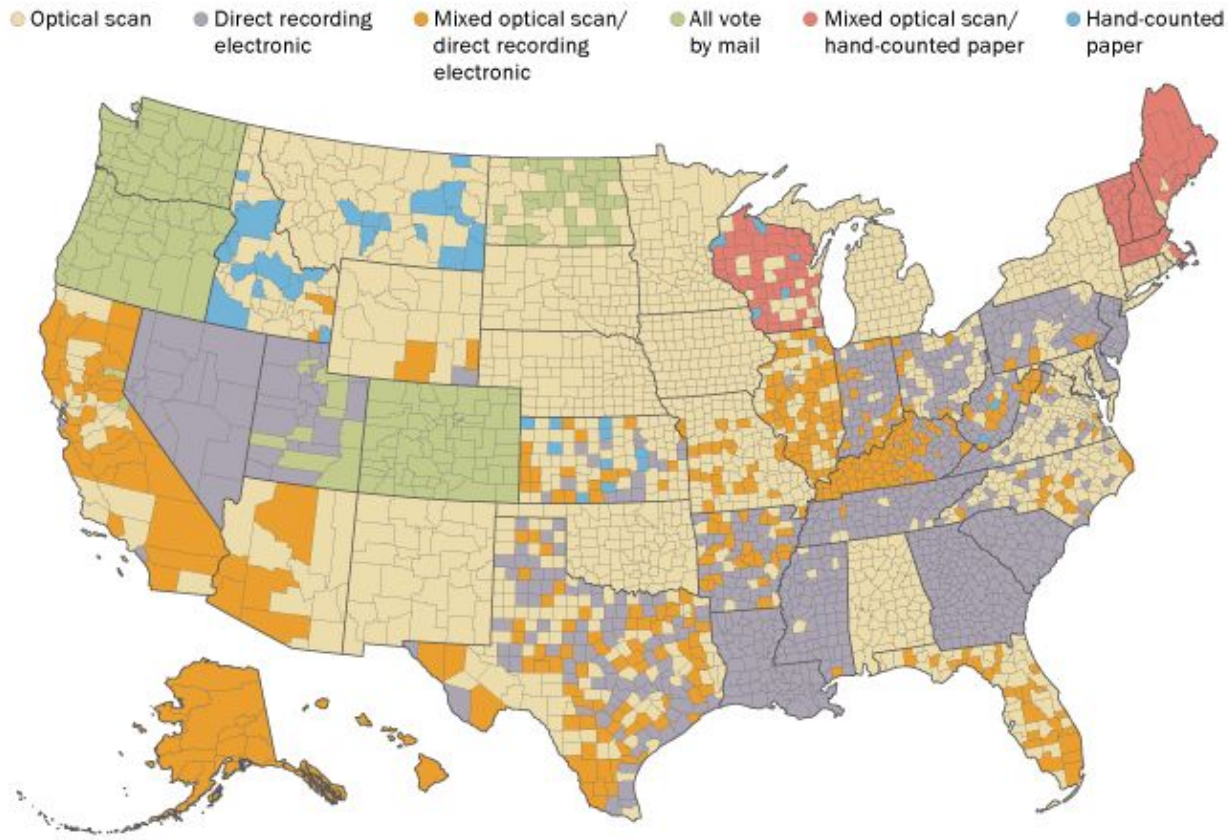
- Voter Verified Paper Audit Trail (VVPAT)
  - voter sees print-out of result, checks for accuracy
  - printed results saved for auditing
- Risk-Limiting Audits
  - random samples taken until results are confirmed with high probability
  - minimal effort if results are correct
  - if incorrect, recount already in progress

Alternatives

- Optical scan paper ballot systems
  - voters mark paper ballots
  - votes tabulated by scanning devices
  - PRO: ideal security-efficiency ratio
  - CON: expensive
- Hand-counted paper ballots
- Vote by mail
- Mechanical lever voting systems (RIP 2010)
- Punch card voting systems (RIP 2016)

Across the U.S., a patchwork of voting methods

Principal voting system, by county



Source: Pew Research Center analysis of data from Verified Voting Foundation.

PEW RESEARCH CENTER

Regulation v. Certification in the US (Gorcenski 2016)

- Regulation: law that carries civil and/or criminal penalty for non-compliance
- Certification: quality assurance standard
- no codified federal voting system regulation; yes federal certification
- states regulate, can mandate federal certification
- software certification standards: style over substance
    - most use automated code-checkers
    - small fraction of code reviewed by humans
- 20 states have no regulations
- $4 billion Help America Vote Act (2002) introduced more tech, failed to fix flaws

Election security: beyond voting systems

- Voter data
  - Russian hackers use spear-phishing to access voter information in 39 states
  - Federal government prosecutes leaker; Republicans vote to eliminate EAC
  - Facebook sells ~~50~~ 87 million users' private data to Cambridge Analytica
- Political party and campaign security
  - DNC hack, Clinton emails
- Social media and "fake news"
  - "Skip the line, vote by SMS" tweets

Election security: beyond technology

- Targeted voter suppression
  - gerrymandering
  - voter ID laws
- Systematic disenfranchisement
  - mass incarceration
  - banning groups based on race, gender, etc.
- Traditional voter fraud
  - ballot-stuffing in Russia