Election Systems Threat Landscape

- Voting Systems
  - highly visible, depended upon for ballot integrity
  - main subject of HAVA
  - targeted by corrupt candidates & supporters - aim to alter outcome

- Election Management Infrastructure
  - less visible, less standardized, built and maintained by counties
  - depended upon for election logistics, voter registration
  - targeted by hostile state actors - aim to disrupt election & legitimacy
Most attention has been on Voting Systems

- Many voting systems (especially DREs) depend on complex software and hardware for integrity of vote
  
  - early focus was on evaluating and hardening this critical software & firmware - a herculean task

- Current approach focuses on voting architectures that can tolerate inevitable defects & vulnerabilities
  
  - “Software Independence” (Rivest & Wack)

  - Paper ballots + post-election audits (RLAs)
Some open issues in Voting Systems

• Usability and Ballot Design
• Role of “Ballot Marking Devices”
• Post election audit practices
• Chain of custody / interactions among security mechanisms
• Disaster recovery
• Public confidence
• Software update / bug fixing vs. certification
• Practical issues: Deployment, funding, vendor marketplace, incentives
Election Management Infrastructure

- Much less visible and receives much less attention than voting systems, but at least equally critical

- Largely ad hoc, bespoke systems maintained by each (county/township) election jurisdiction (5000+ in US)

- Voter registration, precinct pollbook creation, machine provisioning, ballot design, tally, results reporting, public communication

  - Potentially exposed to remote access (and attack)

- Many functions outsourced to contractors and vendors
Consequences of infrastructure compromise

- Disruption of election day logistics
- Disenfranchisement of large numbers of voters
  - provisional ballots mostly don’t scale
- Incorrect outcomes reported
- Loss of confidence in outcome / legitimacy of election
- Can be tailored to favor candidates