



# Combining E2E Voting with Trustworthy Computing

Russell A. Fink (JHU / APL and UMBC)

Alan T. Sherman (UMBC)

NIST E2E Voting Systems Workshop

October 13, 2009



## Our Position

- E2E integrity is not sufficient
  - Electronics and software are necessary for accessibility, usability, efficiency
  - Malicious software can violate privacy, sow confusion, disrupt availability
  - Many problems caught late - only after polls close
- *Trustworthy Computing (TC)* can help plug gaps
  - *Trusted Platform Modules (TPM)* protocols
  - Application attestation
  - Secure key storage and key sealing

## ● ● ● | Examples – Gaps in E2E Systems

- Privacy attacks
  - Malicious software in scanners, touch screen interfaces can violate voter privacy
- Disruptive attacks
  - Malicious software can disable machines, swap votes, fake evidence of fraud
- Avoiding electronics hinders accessibility, usability
  - Scantegrity lacks accessibility interface for blind
  - Some Scantegrity voters will have difficulty writing down codenumbers, especially for long ballots

## ● ● ● | Examples – TC adds value

- Platform attestation helps assure correct software is running
  - Shuts down many privacy and disruptive attacks
- TPM protocols and secure key storage can help enforce policies, chain of custody of election data
  - TPM can bind vote to ballot presented and measurement of software
- Increases assurance of electronic improvements to usability, accessibility
  - Electronic intent capture, multi-media I/O, Scantegrity printer for codenumber



## Costs and Limitations of Trustworthy Computing

- Costs
  - Key management
  - More complex system design, administration
- Limitations
  - Does not enhance understandability, transparency
  - Must trust TPM and other hardware
  - Platform attestation through static TPM measurement of software is imperfect