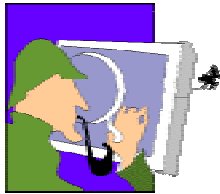


Security Requirements for Internet Voting Systems

**Presented By:
Ed Rodriguez**

**ACSAC '01
December 13, 2001**



Booz | Allen | Hamilton
delivering results that endure

© 2001, Booz Allen & Hamilton Inc.

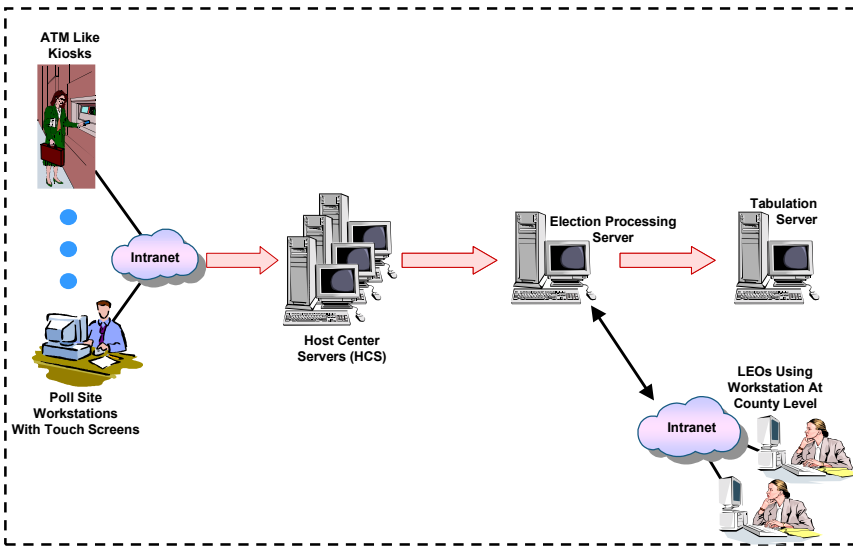
Outline

- What is Internet Voting?
- Why is Internet Voting Different?
- Unique Internet Voting Security Considerations
- Framework to Develop Security Requirements
- Discussion of Internet Voting Security Attributes
- Observations & Final Words

What is Internet Voting?

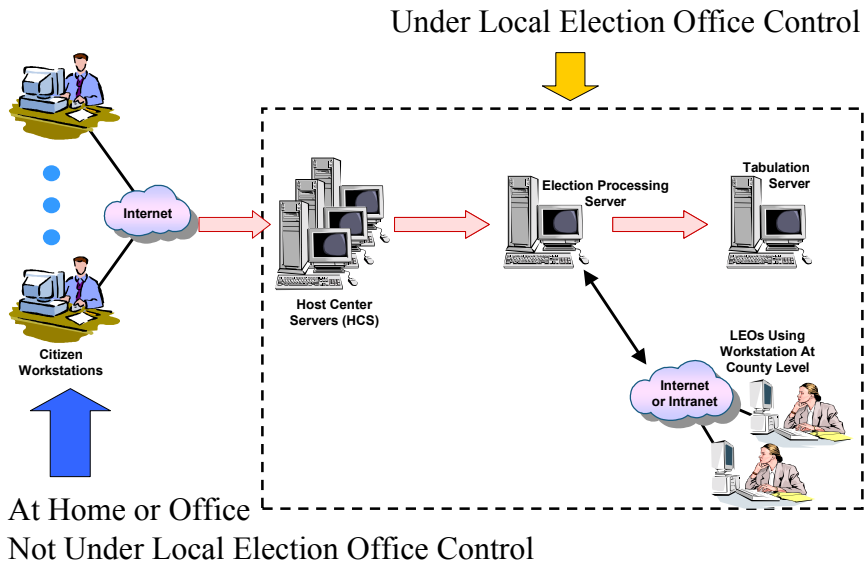
- Internet Voting is the act of casting a vote using a system that employs internet based protocols.
- Currently there are two flavors:
 - Poll site internet voting
 - Remote internet voting

Poll Site Internet Voting



Under Local Election Office Control

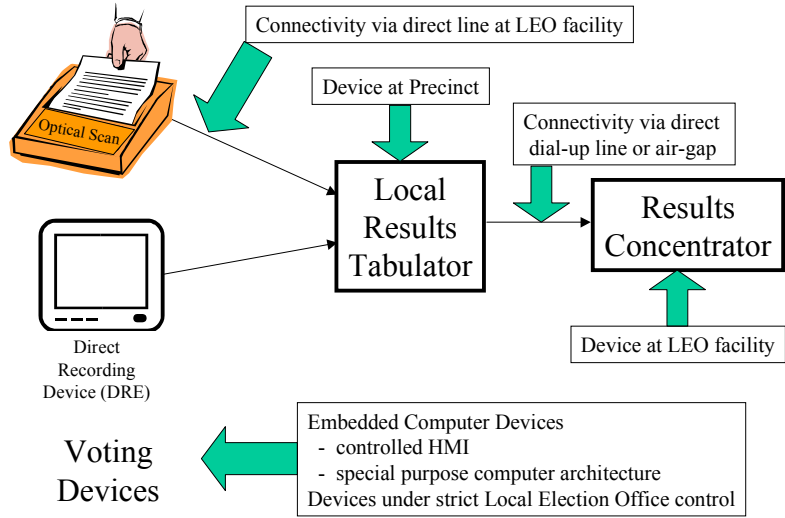
Remote Internet Voting



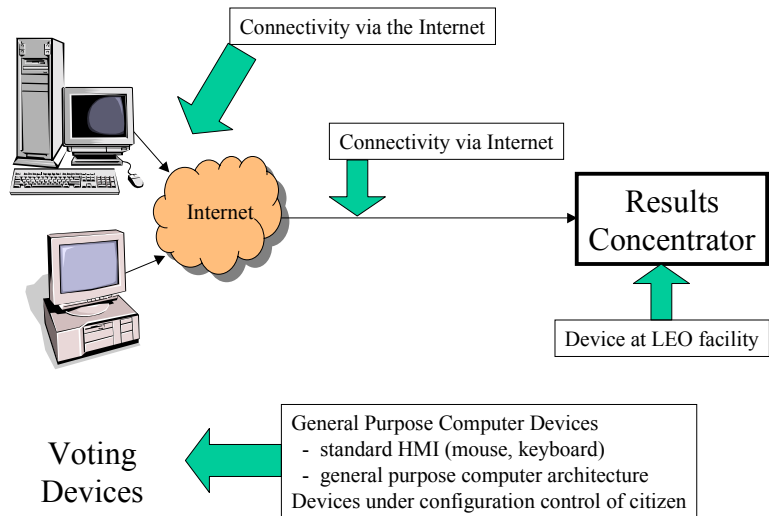
Community View

- Various reports have stated that poll site internet voting is feasible in the mid term while remote internet voting is not feasible
 - “we can’t accept any risk at all”
 - there are new risks that don’t exist in current systems
- If the two are architecturally very similar then **why are there two vastly different views on this matter?**
- Let’s investigate further...

Why is Internet Voting Different From Electronic Voting



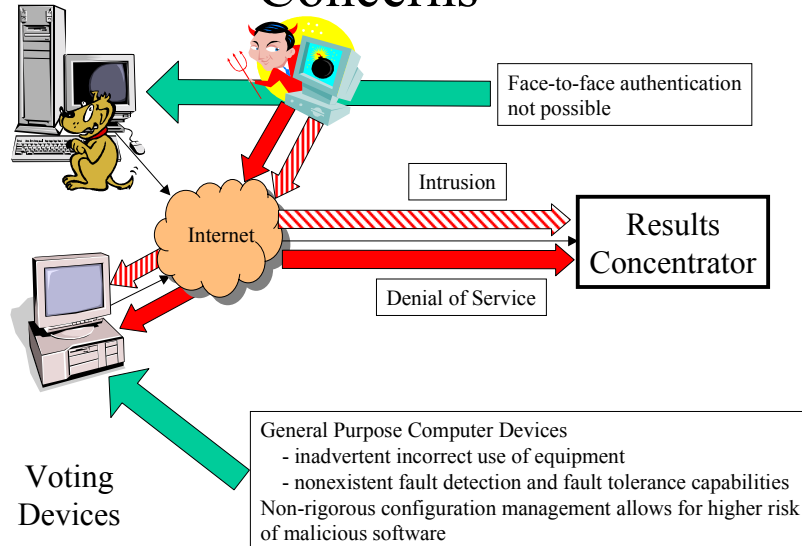
Why is Internet Voting Different From Electronic Voting



Why is Internet Voting Different From Electronic Voting

The environment that Internet voting operates within creates unique security concerns

Unique Internet Voting Security Concerns



Therefore, We Assert...

- Internet Voting security requirements MUST account for environments with different sets of threats even though the system architectures are similar/identical!
- To date no clear view or articulation of security requirements has been made
 - Current Revised FEC Voluntary Standards for Computer Based Election Systems (VSS) standards are first cut at this issue but being developed without broad industry participation (vendors or security community)

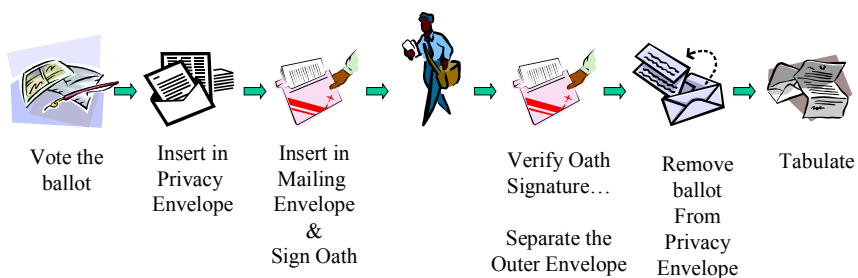
Development of Security Requirements

- Develop a notional concept of operations
 - How would an Internet Voting System work from a *user* perspective?
- Identify the required security attributes for security-related objects and operations
 - What security things do we have to worry about?
- Define security requirements categories?
 - What is the high level set of security requirements?

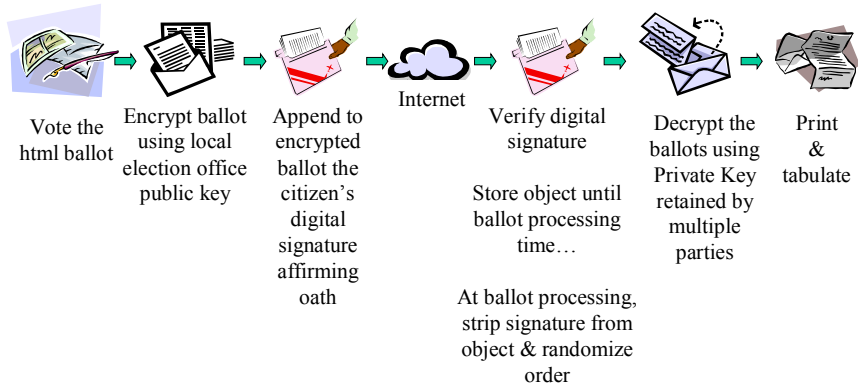
Concept of Operation

- Discussion based on the “Voting Over the Internet” (VOI) model implemented and used during the 2000 General Election
- VOI’s model was based on the absentee voting process
- California Internet Voting Task Force Report cited the absentee voting model as the most suitable for internet voting

Absentee Voting Process



VOI Voting Process



Security Attributes

- Four Primary Security Services Provided Through the Use of Cryptography

	Registration	Voting
Data Integrity	✓	✓
Identification & Authentication	✓	✓
Non-repudiation	✓	✓
Confidentiality		✓

Security Attributes

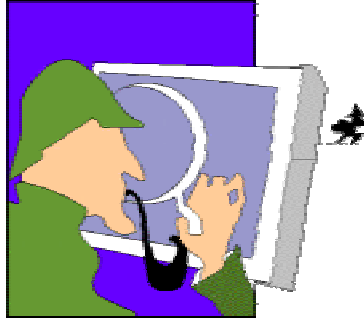
	Electronic Voting	Remote Internet Voting
Data Integrity	<ul style="list-style-type: none"> • Non-cryptographic techniques used (CRC) 	<ul style="list-style-type: none"> • Cryptographic techniques required (digital signatures)
Identification & Authentication	<ul style="list-style-type: none"> • Personal address (no proof reqd) • Driver's license 	<ul style="list-style-type: none"> • Identity digital certificate (w/ face-to-face validation) • Emailed ID & password?
Availability	<ul style="list-style-type: none"> • Equip uses best commercial practices w/ some reliability enhancements 	<ul style="list-style-type: none"> • COTS Equip • Network DoS concerns • Network availability
Non-repudiation	<ul style="list-style-type: none"> • Limited (no proof of vote being counted) 	<ul style="list-style-type: none"> • Extensive logs • Residual objects exist
Confidentiality	<ul style="list-style-type: none"> • Citizen's choices are anonymous at entry time 	<ul style="list-style-type: none"> • Encrypted e-ballot is unencrypted only by LEO

Page 17

Observations & Final Thoughts

- Internet Voting provides opportunity to provide enhancements beyond current systems.
 - Strong I&A (benefits extend to registration)
 - “Proof of Vote”
- Does Internet Voting Demands Perfect Security?
 - So Say the “Experts”
 - Higher Standard or Pessimistic Viewpoint?
 - Should Be Defined by Standards (FEC? IEEE?)
- Perfect Anything Is Unattainable
 - Need for a Managed Risk Approach to Security
 - Some Security Risks Remain
- Require active participation of security community to integrate security into stds!

Page 18



Ed Rodriguez
rodriguez_ed@bah.com