UOCAVA Remote Voting Systems Workshop

Sponsored by:
NIST/EAC/FVAP

Notes for Framing Breakout Groups

Primary Goal:

Establish a comparative threshold for an acceptable level of risk by identifying accepted risks of the current UOCAVA voting process (mail delivery and return of ballots), and developing measures and/or criteria for comparing risks of remote electronic absentee voting systems (focusing on unsupervised remote voting from personally-owned devices over the Internet) to those of the current system.

Stretch Goal:

Identify any current, emerging, or future technologies for remote electronic absentee voting systems capable of providing a comparable level of risk to the current UOCAVA voting process.

Breakout Groups

Group 1: Voter Authentication and Privacy

The breakout group will:

- Identify voter authentication and privacy characteristics and risks of the current UOCAVA voting process.
- Identify potential risks related to voter authentication and privacy of remote electronic absentee voting systems. For example, the breakout group may consider:
    - Ballot secrecy
    - Coercion and/or vote selling
    - Voter registration databases and voter lists
    - Strength of authentication mechanisms
    - Susceptibility to phishing/social engineering
    - Usability and accessibility of authentication mechanisms
    - Voter autonomy
    - Other potential risks
- Develop measures and/or criteria for assessing and quantifying identified risks and their potential impacts. How do these compare to those of the current UOCAVA voting process?
- Identify properties or characteristics of remote electronic absentee voting systems that could provide comparable authentication mechanisms and privacy protections as the current UOCAVA voting process.

Stretch Tasks:

- Evaluate currently available technologies that can mitigate the identified risks. How do the properties or characteristics of these technologies compare to those of the current UOCAVA voting process?
- Identify and discuss emerging or future research areas that hold promise for improving voter authentication and/or privacy. For example:
    - Biometrics, such as speaker identification
    - Novel authentication methods
    - Cryptographic voting protocols, and other cryptographic technologies

Group 2: Auditability

The breakout group will:

- Identify the audit capabilities of the current UOCAVA voting process.
- Identify audit capabilities and potential risks to the auditability of remote electronic absentee voting systems. For example, the breakout group may consider:
    - Necessary and desirable auditing capabilities
    - Trustworthiness of election records
    - Usability and accessibility of voter verification
    - Other potential risks
- Develop measures and/or criteria for assessing and quantifying identified risks and their potential impacts. How do these compare to those of the current UOCAVA voting process?
- Identify properties or characteristics of remote electronic absentee voting systems that could provide audit capabilities comparable to those of the current UOCAVA voting process.
    - How would the audit properties and characteristics of remote electronic voting systems augmented with paper compare to those of purely electronic systems?
    - Are there other technologies or architectures that could provide improved audit properties or characteristics?

Stretch Tasks:

- Evaluate currently available technologies that can mitigate the identified risks. How do the properties or characteristics of these technologies compare to those of the current UOCAVA voting process?
- Identify and discuss emerging or future research areas that hold promise for improving remote electronic voting system auditability? For example:
    - Cryptographic voting protocols (e.g., end-to-end voting systems)
    - Trusted Computing and Trusted Platform Modules
    - Transaction processing systems
    - Open source voting systems

Group 3: Network and Host Security

The breakout group will:

- Identify problems and risks associated with the transmission of blank and voted ballots through the mail in the current UOCAVA voting process.

- Identify risks associated with electronic transmission or processing of blank and voted ballots. For example, the breakout group may consider:
    - Reliability and timeliness of transmission
    - Availability of voting system data and functions
    - Client-side risks to ballot integrity
    - Server-side risks to election integrity
    - Threats from nation-states
    - Other potential risks
- Develop measures and/or criteria for assessing and quantifying identified risks and their potential impacts. How do these compare to those of the current UOCAVA voting process?
- Identify properties or characteristics of remote electronic absentee voting systems that could provide for the transmission of blank and voted ballots at least as reliably and securely as the current UOCAVA voting process.

Stretch Tasks:

- Evaluate currently available technologies that can mitigate the identified risks. How do the properties or characteristics of these technologies compare to those of the current UOCAVA voting process?
- Identify and discuss emerging or future research areas that hold promise for improving network and host security? For example:
    - Trusted Computer and Trusted Platform Modules
    - End point security posture checking
    - Cloud computing
    - Virtualization
    - Semi-controlled platforms (e.g., tablets, smart phones, etc.)
    - Use of a trusted device (e.g., smart card, smart phone, etc.)