Discussion Topic: Wireless Technology & Internet Connectivity

This document highlights the cybersecurity working group discussion around the wireless technology and internet connectivity used by a voting system. Wireless and Internet technology are noted as an open area due to concerns around auditability, data protection, and system integrity. This document will list the current and potential use cases, identify the threat concerns, and discuss current VVSG 2.0 related requirements. See, document titled, *Wireless and Internet Use Case Analysis*, for more detailed information.

Decision Points

- Is wireless/internet technology appropriate for use within voting systems?
- Is the presence of wireless technology appropriate within voting systems?
- Is internet connectivity appropriate for use within voting systems?
- Is the presence of internet connectivity technology appropriate within voting systems?

Wireless Technology

This is not an exhaustive list of wireless and internet technology types. This is just a list of the more common types for reference in understanding what technologies are used in context with the use cases described below.

- **Wi-Fi** – WiFi is a wireless technology that uses the IEEE 802.11x standard. It is used in wireless local area networks (WLANs) which are a group of devices wirelessly connected to a network that is restricted to a limited geographical area.
- **Bluetooth** - Bluetooth is shorter range, low power, radio communications protocol. Bluetooth technology creates small wireless networks known as personal area networks (PANs).
- **Near field communication (NFC)** - Of the wireless technologies discussed in this document, NFC has the shortest range of communication, which is typically less than 4 inches. NFC is a radio communication technology based on radio-frequency identification (RFID) technology.

Internet Technology

- **Cellular/Cellular Modems** - Cellular technology is a wireless technology used for wide area networks (WANs). Cellular allows data to be transferred wirelessly across large geographical areas and often carries data over the internet.
- **Public Switched Telephone Networks** – Telephone networks were originally a set of fixed analog telephone systems, but today they are mostly digitally and traverse many different networks including, cellular networks.

Use Cases

This section does not cover all use cases of wireless and internet technology in elections. This list is intended to capture the interest in the technology and assist in explaining the concerns.

*Current Use of Wireless/Internet Technology Inside the Polling Place*
Device level management from a centralized EMS to other election devices

Activation card used to activate a ballot and voter’s session

Transmit general election data/elections results to the central election office

Peripheral input/output devices such as a keyboard, mouse, headset, or printer.

Current Use of Wireless/Internet Technology Outside the Polling Place

Device level management from a centralized EMS to other election devices

Receive general elections results at the central election office

Future Use of Wireless/Internet Technology in Elections

Assistive technologies, such as a Bluetooth headset or hearing aid

The following sections describe the general concerns with using in the voting system and potential mitigations to those concerns. The concerns and mitigations are illustrated through the impact on elections. The concerns and mitigations do not represent a consensus opinion, but rather an aggregation of what was discussed by the cybersecurity working group.

General Concerns

Concern A. Remote/Nation-state attacks on the voting system

The use of cellular expands the attack surface even further than other wireless technologies because the data traverses over the internet. The internet itself touches all over the world. This type of access allows a malicious actor to attack from various distances, meaning they do not have to be in close proximity of a polling place or near a specific jurisdiction.

Exposure to the internet could allow nation-state attackers to gain remote access to the voting system. With remote access an attacker may be able to view all files within a voting system and make modification to files within the voting system. These files may include, election results and ballot records.

Additionally, exposure to the internet may also enable nation-state attackers to remotely inject malware that maliciously modifies or deletes files within the voting
system. Malware injected into the central count system could impact the integrity of the election results received from all precincts within an entire State. This could have a severe impact on the integrity of the election. The malware may also impact the behavior and function of the voting system, such as by rerouting information from the voting system to the computer of a nation-state attacker.

This type of exposure could also make voting systems vulnerable to ransomware. Ransomware is a type of malware that could deny access to election data or functionality, usually by encrypting the data with a key known only to the hacker who deployed the malware. Ultimately an attacker, could render a voting system non-operational, until a ransom is paid.

**Concern B. Loss of confidentiality and integrity of the voting system and election data**

Information sent wirelessly may be susceptible to interception by a malicious actor to eavesdrop or have unauthorized access to view the wirelessly transmitted information. In addition to viewing the transmitted election data, the attacker could also maliciously modify the election data, such as tabulation totals, causing the receiving device to obtain false tabulation results.

Wireless technology can also provide entry points for attackers to access and/or harm the voting system. By accessing a vulnerable wireless point within the voting system, an attacker may be able to remotely inject malware. This malware could be used to send election data to the remote attacker, modify files (e.g., tabulation results) within the voting system, or delete files (e.g., ballot records). The malware could also be used to maliciously modify how a voter’s input is recorded within the voting system and falsely output the voter’s ballot selections.

**Concern C. Loss of availability to perform election functions and access election data**

If wireless is required to perform elections functions, such as sending election data between two devices or printing ballots, a jamming attack could block all wireless transmissions. This could halt election processes within polling place and disrupt the election.

**Concern D. Loss of ballot secrecy**

This concern was discussed with regards to the use of wireless technology to activate a voter’s ballot through an activation card. Eavesdropping on wireless traffic could allow an attacker to intercept information that may be used to identify a voter. This could violate ballot secrecy if that information can be used to a link a voter to their ballot selections.
Concern E. Lack of technical expertise required to apply secure configuration of wireless technologies
Proper configuration of wireless technology is essential to ensure that the appropriate security controls are applied to protect the voting system. Without proper configuration, the voting system could be left open to potential vulnerabilities. This secure configuration may require technical staff to be available at every polling place throughout an election.

Potential Mitigations:

Mitigation A. No Wireless hardware
The voting system does not contain any wireless hardware. The intent of this mitigation is to limit the attack surface. This mitigation may require manually managing and configuring each device, physical connections to peripheral devices, and other alternative methods to transmit information.

With this mitigation, voting systems would not have a cellular transmission capability within their architecture. Alternatively, elections results could be transmitted through other out-of-band methods including...
- The manual sneaker-net process, where the data is transferred via USB/printed results, and sent to the central tabulation center
- Telephone communication to send election results via a phone call or text message
- Using an encrypted mobile application to send election results to the central tabulation center
- Scanning a QR-code to transfer the results and embedded the QR-code with a digital signature to verify the election results

Note: A Senate Intelligence Committee report states the following, “Paper ballots and optical scanners are the least vulnerable to cyber attack; at minimum, any machine purchased going forward should have a voter-verified paper trail and remove (or render inert) any wireless networking capability.”

Mitigation B. Enable/Disable Wireless
Turn on/off the wireless interface so that it is only used when necessary. This may be done manually or automated based on the voting state (e.g., activated state).

1 This reference can be found on page 59 of the report. Here is the link to the document: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf
**Note:** This was not listed as a potential mitigation for the use of cellular technology or internet connectivity.

**Mitigation C. Sophisticated security awareness and ongoing secure configuration management**

In the scenarios where wireless technology is allowed, there is a need to ensure the voting system and devices interacting wirelessly with the voting system have the appropriate security configurations. This requires secure configuration and implementation in every jurisdiction, and it must be maintained and updated over the life of the system in every jurisdiction. This mitigation is meant to ensure the highest security configurations for encryption, authentication, and data signing are performed. Additionally, to maintain the security of the wireless technology, there should be a process to review and update the technology.

For peripheral devices used within the polling place, this requires election workers to be aware of the Bluetooth specs of their own personal devices. The technical expertise of election workers varies. To properly ensure this mitigation is applied it may require additional technical staff to be present at each polling place.

**Note:** This mitigation is mostly procedural and does not directly apply to VVSG requirements and certification. Within the VVSG requirements, documentation could be provided to explain the secure configuration process and needs.

**Mitigation D. Airgap at both ends of communication + Sophisticated security awareness and ongoing secure configuration management**

This mitigation applies to the use of cellular technology to transfer unofficial election results. The first mitigation is that an airgap (no physical connection) is applied between the voting system and the device used to send the unofficial election results. Also, at the central tabulation center, the receiving device would be kept separate/airgapped from the machine that performs the final tabulation. Information must be manually transferred from the tabulation system to the election reporting machine. This protects the information on the voting system from malicious tampering.

The transmission of this information requires secure configuration and implementation. The voting system would use methods to keep communications private, such as using a trusted virtual private network (VPN) to encrypt the data and traffic. This does not prevent a user from downloading malware from the internet but protects the confidentiality of the data sent. Another method is to use secure file transfer tools that encrypt the data in transit and sends to authorized recipients. This requires secure configuration and implementation in every jurisdiction, and it must be maintained and updated over the life of the system in every jurisdiction.
The following section describes additional thoughts on the potential benefits to using wireless or internet technology in the voting system. The potential benefits do not represent a consensus opinion, but rather an aggregation of what was discussed by the cybersecurity working group.

**Potential Benefits**

*Note:* The following do not imply that wireless technology is the only solution to these achieve these benefits.

**Benefit A. Automation and Efficiency.**

Wireless technology can be used to simultaneously send device configurations and ballot style updates from an EMS to several voting devices. The wireless transmission of this information requires less hardware and less physical setup. Also, this wireless method prevents the need to manually configure and apply updates to each device one by one.

In addition to configuration updates, wireless technology may also be used to provide software updates to devices. This use may apply to some uses of wireless technology, but as an example, may not include cellular connectivity to the voting system.

**Benefit B. Assist with Geographical Restrictions**

The use of cellular or internet transmission of unofficial election results, is useful for jurisdictions that may have geographical challenges (e.g., mountainous or rural) or barriers to quickly sending election night reports to the central tabulation center.