Context Description: Posted Dec. 1, 2006

This draft report was prepared by NIST staff at the request of the Technical Guidelines Development Committee (TGDC) to serve as a point of discussion at the Dec. 4-5 meeting of the TGDC. Prepared in conjunction with members of a TGDC subcommittee, the report is a discussion draft and does not represent a consensus view or recommendation from either NIST or the TGDC. It reflects the conclusions of NIST research staff for purposes of discussion. The TGDC is an advisory group to the Election Assistance Commission, which produces voluntary voting system guidelines and was established by the Help America Vote Act. NIST serves as a technical advisor to the TGDC.

The NIST research and the draft report's conclusions are based on interviews and discussions with election officials, voting system vendors, computer scientists, and other experts in the field, as well as a literature search and the technical expertise of its authors. It is intended to help in developing guidelines for the next generation of electronic voting machine to ensure that these systems are as reliable, accurate, and secure as possible. Issues of certification or decertification of voting systems currently in place are outside the scope of this document and of the TGDC's deliberations.

Wireless Issues and STS Recommendations for the TGDC

November, 2006

Acronyms and Terms Used in This Paper

The following acronyms and terms are used in this paper. Some of these terms are also defined in the draft VVSG 2007 glossary, located at http://vote.nist.gov/TGDC/VVSG2007-glossary-20061011.doc.

- **DRE** – Direct Record Electronic
- **IR** – Infrared
- **Kbps** – kilobits per second
- **LAN** – Local Area Network
- **PEB** – Personal Electronic Ballot (used by ES&S)
- **PKI** – Public Key Infrastructure
- **RF** – Radiofrequency
- **STS -** Security and Transparency Subcommittee
- **TGDC -** Technical Guidelines Development Committee
- **VVSG** – Voluntary Voting Systems Guidelines
- **WAP** – Wireless Access Point

1. Introduction

This paper discusses issues with wireless communications used with voting systems and presents STS recommendations for wireless-related requirements in VVSG 2007. For VVSG 2005, the TGDC recommended that use of radiofrequency (RF) wireless and infrared (IR) wireless be permitted, but that all wireless communications be authenticated and encrypted, that it be restricted in several other ways, and that the requirements be accompanied by a warning that use of wireless is extremely risky and should be avoided (the VVSG 2005 was published without this warning).

Since then, there has been much opposition to use of wireless from the computer security community. Various voting system threat analyses, notably the initial NIST Threat Analysis Workshop (http://vote.nist.gov/threats/index.html) and the Brennan Center report[1] (http://www.brennancenter.org/programs/downloads/Full%20Report.pdf), have listed threats associated with wireless and recommended against using it. A handful of states now ban wireless usage on voting systems during Election Day.

The purpose of this paper is to inform the TGDC about the issues regarding use of wireless and present rationale for the associated STS recommendations.

1.1 Summary of STS Recommendations

The primary STS recommendations discussed in this paper are as follows:

1. **No radiofrequency wireless permitted on voting systems:** STS recommends against permitting use of RF wireless in conjunction with voting systems or, for that matter, any system used in a polling site while polling is taking place.

2. **Place modems on special devices:** STS recommends that wireless modems used to upload election night results be located on separate devices that are specially configured for this purpose.

3. **Restricting use of infrared wireless:** STS recommends that IR wireless continue to be permitted, but that its use be limited to applications where the IR port can be shielded from external observation; that is IR devices may be used in situations where a device is plugged into a shielded slot as a substitute for a physical electrical contact.

The following sections discuss these recommendations and other surrounding issues in more detail.

[1] Found respectfully at http://vote.nist.gov/threats/index.html and http://www.brennancenter.org/programs/downloads/Full%20Report.pdf.

2. How is Wireless Used Today in Voting Systems?

Wireless communications is a category that represents a broad spectrum of wireless signals, strengths, ranges, and applications. For voting systems, two types of wireless have been used: (1) radiofrequency, typically represented by wireless LANs and wireless modems, and (2) infrared, typically represented by television remotes and laptop wireless connections to peripherals such as printers. Radiofrequency waves can travel relatively large distances (hundreds of feet to many miles) and penetrate through walls and other objects (with some degradation of signal), while infrared wavelengths are shorter than that of radio waves, between approximately 750 nm and 1 mm.

Thus far, use of wireless in voting systems includes the following (there may be other uses not documented here):

- **Loading software and ballot information prior to the election (RF and IR):** wireless cards are used along with IEEE 802.11 communications protocols such that the voting systems can be connected via a wireless LAN to a software distribution server. This can be done at the factory or in other locations, e.g., county warehouses to make last minute changes to ballot definitions. IR connections can be used for the same purposes.

- **Wireless LANs on Election Day (RF):** at least one vendor[2] uses a wireless LAN throughout voting operations; the LAN is used to broadcast signals to voting stations for opening the polls and closing the polls, as well as for collecting stored votes after the close of polls (to meet the wireless requirements of VVSG 2005, this equipment will require modifications).

- **Wireless modems to transmit election night results (RF):** a number of voting systems come supplied with wireless modem cards that are used after the close of polls to transmit unofficial election night results to election headquarters.

- **To activate the ballot (IR):** at least one vendor[3] uses IR in conjunction with a PEB to access supervisor functions and to activate the ballot. Other vendors use ISO 7816 smart cards with electrical contacts for this purpose.

The Diebold TS DRE contains an IR port which is not presently used (apparently a use was planned at one point but was never implemented). It has been reported but unsubstantiated by vendors that wireless is being considered for use with electronic poll books to connect them together on wireless LANs at the polling site and to connect them to a state voter registration database[4]. Doug Jones states that in response to rising pressure to update and test voting systems

[2] The Winvote system from Advanced Voting Systems, Inc., http://www.advancedvoting.com/index.php.

[3] ES&S, whose site contains no relevant information; verifiedvoting.org has a description found at: http://www.verifiedvoting.org/article.php?id=5165.

[4] Electronic poll books, if used to activate the ballot, arguably would fall within the VVSG 2007 definition of a voting system (found in http://vote.nist.gov/TGDC/VVSG2007-glossary-20061011.doc) and would be subject to its *general* requirements, i.e., communications, cryptography, quality, etc. Devices that similarly implement other functions of a voting system as covered in the definition would also be subject.

faster, some vendors have proposed that their next-generation voting systems will use wireless technology for remote-control initialization and testing of voting machines[5].

3. Risks Associated With Wireless

There are a number of issues and risks associated with using wireless. The following sections focus on these issues and link them to various voting applications in which wireless is or can be used.

3.1 Inherent Vulnerabilities of Wireless (RF and IR)

Wireless, regardless of the type, is inherently a security risk because the signals cannot be contained or restricted except though their signal strength or via obstructions that block the signals. Encryption can be used as a means for securing the data content represented by the wireless signals, but there is still the inherent risk of the signals being blocked or disrupted. Attackers are readily able to do this: someone nearby a polling site with a small laptop or possibly a PDA can use widely available software to jam and disrupt wireless signals, and there is little if anything that can be done about it (this sort of attack is called a "denial of service" attack). Thus, encryption is necessary if one wants to restrict who can read or send wireless communications, but communications (whether encrypted or not) can still be jammed, and the jamming can be done surreptitiously.

VVSG 2005 includes a requirement that there be a backup mechanism in place for any function that uses wireless. If a voting device used wireless, for example, to automate the collection of voting records from each voting systems at the end of the day, there would need to be a backup mechanism so that the collection of voting records could still be accomplished. In this case, the backup mechanism might be a manual collection of the removable media that stores the records. It would be necessary for the backup mechanism to be easily executed, e.g., by poll workers.

3.2 Expansion of Attack Range

If a computer system is connected to an external network, for example the Internet, then an attack is potentially possible from anywhere on that network, possibly anywhere in the world. But there is no reason to operate an election system on an external network, except, possibly, to report election results to a central counting facility after polls have closed, or to distribute software patches, or upgrades, or election configuration files to the election machine from some remote location. But while the election is under way, there is no reason to expose the voting system to the risks of an external network connection.

Wired networks, or often "sneaker-nets," clearly can accommodate the communications needed within a polling place, since they generally are set-up in a single room. With wired communications even a non-technical person can see what is connected to the network by following cables. As soon as we introduce wireless, the ability to verify the network configuration visually disappears, and the potential attack range goes up dramatically. An

[5] http://www.cs.uiowa.edu/~jones/voting/nist2004.shtml.

attacker (or more precisely her antenna) can potentially be in another room, on the floor above or below, even outside the building. The normal operating range of the voting machine wireless equipment is no guide to how far away the attacker may be, because she is not constrained to use similar equipment to the voting machines, particularly antennas, nor even is she constrained to follow legal power limitations.

3.3 Complexities of Secure Wireless Networking

Many technically unsophisticated users manage to set up home or small business wireless LANs and make them work fairly reliably. Most laptops come with built-in wireless capability and wireless access points (WAPs) are relatively cheap (e.g., $50.00). Wireless LANs are increasingly offered by coffee shops and airports or even train cars as a way of enticing customers. While these networks are often configured so as to allow anyone to access them, this often doesn’t matter since the networks aren’t generally used for important communications.

While this spread of easy-to-use, low-cost wireless networking is often very convenient, many people are really quite familiar with the basic insecurity of wireless LANs. We know that our neighbors may be using our access point, or we may be using theirs. We know that the kid next door could be intercepting our e-mails, but we also know how uninteresting most of our e-mail is, and some of us know how to set up e-mail clients to use encryption. We may be using a carefully aimed $50 directional antenna to deliberately allow a neighbor 100 yards away to use our access point. We often accept this insecurity for convenience sake, but that doesn’t mean that most of us will be willing to accept insecure voting systems.

Business is often another matter. The facts are that business-grade wireless, in which reliability, speed, integrity, and security are highly important, are expensive and complicated. Business-grade wireless access points can cost tens of thousands of dollars and often have to be positioned by trial and error so that the signals reach around columns and walls. Wireless intrusion detection systems are necessary to detect routine errors or deliberate attacks that can completely bring down the network. Security is still largely a manual process in which end-user systems use a shared encryption key; when the key changes, each end-user system has to be updated by hand with the new key.

With careful, expert setup and supervision this allows tolerably safe routine business applications over wireless LANs. But, election systems are commonly set up in widely dispersed locations and operated for one day then torn down and returned to a warehouse, so it hardly seems practical or sensible to key the voting stations, verify the configurations and monitor the network in such a security critical application, in an area where hundreds to thousands of untrusted people (voters) have access to the polling place.

A lot of work is currently being done in IEEE and IETF standards groups to provide for better, more automated wireless authentication and key management, to better facilitate secure commercial use of wireless communications. Doing this well probably requires a public key infrastructure, with the complexities that implies. As these standards for 802.11, Bluetooth and similar technologies (now in their infancy) mature, it may be sensible to revisit the use of wireless in voting systems. But there is no good reason for a voting system, a security critical application, exposed to outside attack, with an extraordinarily disadvantageous ration of setup to use, to be on the bleeding edge here.

And in any event, wireless opens up a whole new avenue of attack, which really isn't necessary; over the distances required for polling places, electrical cables are practical, and what is connected to what is easily verified with cables. How will we convince the security conscious element of the public that we are serious about voting system security if we even try to accommodate wireless during polling, when we plainly don't have to do so? Private citizens may have a right to sacrifice security for convenience in their personal lives, or business to sacrifice security for their customer's convenience, and they often knowingly or unknowingly do that, but elections should not be run that way.

3.4 Risks in Loading/Configuring Voting Systems via Wireless

Voting system today are often loaded with new software and configured prior to the election via wireless LANs. This can be done at the vendor's site when the system is initially configured as well as at local county warehouses when the system is updated or ballot information is loaded.

Simply put, this is directly against NIST guidance. Software loading and configuration must be done on a closed network, i.e., one that can't be accessed except by authorized personnel, because when systems are loaded or configured, security controls often are disabled and thus the systems are more vulnerable to attack. A wired LAN, e.g., connected via Ethernet cabling that doesn't connect to any other networks, forms an effective closed network, but a wireless network is inherently open: access to the radiofrequency signals cannot be easily managed and anyone within range is capable of accessing or jamming the network. The complexity factor of manually loading encryption keys again works against the convenience factor of wireless networking. If we use a single key for all the voting machines in a good sized jurisdiction, as a convenience to set-up, how long will the key remain a closely held secret? If we try to use more elaborate and secure methods for keying voting machines, how often will we find that the voting system won't work because it isn't keyed correctly?

IR could also be used to update voting systems; a shielded IR port that has been specially designed to accommodate the requisite IR equipment may constitute a closed network.

3.5 Risks in Using Wireless for Transmitting Election Results

Modem cards are often included in voting stations so that they can be used afterwards to phone in the election results. Wireless modems are used frequently because of the advantages of not needing to connect directly to a phone line (that often is not working or located out of reach). The modems are commonly labeled and marketed as "Broadband Access," specifically the widely marketed Verizon and Cingular wireless data access products that offer transfer rates up to several hundred kbps, and fall back to "cellular" rates (about 14 kbps) where the broadband service is not available.

It should be mentioned, though, that the communications path between the wireless modem at the polling site and the central server is likely to include a number of different networks, including the Internet. Thus, the voting station is participating in a network and is vulnerable to potential eavesdropping (which may not be an issue with unofficial election night results) or various other forms of attack such as changing the results. For those reasons as well as those reasons stated previously, the communications should be via an authenticated channel (i.e., the voting station will connect end-to-end to "its" specific central server and vice versa, and all the communications between will be capable of being encrypted if necessary). This likely would require issuing digital certificates to the voting stations used in polling places and to the central tabulation facilities.

As one may see, the preparations and the cryptographic mechanisms needed to secure the wireless transmissions are complicated and, if misconfigured, could permit other systems on the same network to access the voting station. The STS believes that election officials are better served by placing the modem on a device that is separate from the voting station; this device would be loaded with the election results and would then perform the requisite cryptographic connection to the central server and then transmit the results. Essentially, placing the modem and communications software/hardware on a separate device makes it easier to "get it right" and removes the necessity and complexity of the voting station needing to connect to a network to transmit election night results.

Some individuals have argued that, since the election results are unofficial, no special security is required. STS considers this argument as highly specious, as it is important that the election results be accurately received by the correct recipients and that the wireless interfaces at the end points be protected against attack.

3.6 Risks Associated with Use of Infrared

Infrared transmissions share many of the same vulnerabilities and complexities of RF. But, IR transmissions can be shielded and protected from interference. VVSG 2005 permits IR, even on Election Day, but requires shielding and authentication/encryption.

However, its unauthenticated usage is as risky as for RF. Its usage needs to be authenticated end-to-end, which may require digital certificates on the voting systems and any devices using IR to communicate with the voting systems.

4. Conclusions for VVSG 2007

The conclusions of this white paper are that use of wireless in voting systems is very risky and that securing and maintaining wireless connections is so difficult as to be impractical for users such as poll workers and election officials often relying on limited technical assistance.

The complexity alone of configuring and operating wireless networks effectively rules them out for voting equipment or for any equipment that needs to be operated at the polling site. Poll workers or technicians can't be expected to configure these networks the night before an election and make them work correctly throughout the next day. Encryption keys cannot be shared on a widespread basis; they would have to be assigned per polling site and managing these keys would add significantly to the burdens that election officials and poll workers already have.

Usage of wireless networks before or after elections to upload software or make changes to ballot definitions is a tremendous risk, as the wireless capability can be eavesdropped or used fraudulently to make changes to voting systems. Again, securing these connections adequately can be so difficult as to be impractical.

The STS recommendations for wireless in voting stations are as follows:

4.1 No RF Permitted on Voting System

Voting systems shall not include any RF wireless capability nor shall they be designed to potentially accommodate RF wireless capability. Thus, software loading must be conducted on closed networks or via insertion of removable media. Wireless modems require specialized equipment (see below).

4.2 Transmitting Election Results on Specialized Equipment

Modems (wireless or otherwise) required for transmitting election night results shall be contained on separate, special communications devices that shall be configured to use requisite cryptographic and communications protocols. These protocols must be implemented as basically recommended in VVSG 2005 and in the communications and cryptography requirements being drafted for VVSG 2007. The authentication must be end-to-end and encryption must be provided as an option.

4.3 Restrictions on Use of IR

Use of IR is unnecessary and inherently risky, therefore its usage is not encouraged or promoted. Vendors shall include well-documented justifications for its inclusion on voting devices. Its use shall be restricted as per the requirements in VVSG 2005 and additional restrictions: the connections must be authenticated end-end and encrypted and completely shielded via special-purpose enclosures. In addition, it may be necessary to specify what types of applications IR can be used an not used for.

4.4 No Wireless on Polling Site Systems

No wireless should be used at all in other polling site systems during elections, including electronic poll books. If the voting devices implemented functions covered in the VVSG 2007 voting system definition, they would be subject to VVSG 2007 general requirements and therefore wireless capability could not be included with the exception of IR. Wireless is difficult to configure and is not reliable. Poll workers or election officials should not be burdened with having to configure or maintain any use of wireless or deal with backup procedures in case it fails. The only exception should be for well shielded infrared ports used as a contactless substitute for smartcards.