

Testimony
to
The Election Assistance Commission
Hearing on the Use of Wireless Capabilities

July 28, 2005

by
H. Stephen Berger

Introduction

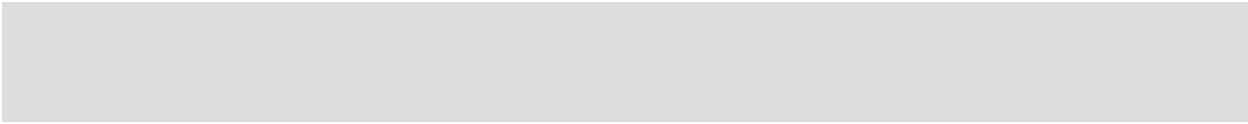
I would like to thank the Election Assistance Commission, the commissioners and staff for this opportunity to present these thoughts on the use of wireless technology, as it is presented in the Voluntary Voting System Guidelines (VVSG). It is a privilege to contribute to the deliberations of the Commission on this topic and more generally to the development of the VVSG.

When introducing any new technology to a security sensitive environment, such as voting, the simple but difficult question, "Do the benefits outweigh the risks?" must be asked. In developing a satisfactory answer to this question, subordinate questions must be asked. Among these questions are:

1. Do we fully understand the risks?
2. Can the use of the new technology be limited and its risks safeguarded or otherwise mitigated to acceptable levels?
3. In a system with distributed responsibility and authority, including federal, state and local officials, what is the certainty with which risk mitigation measures will be consistently implemented?
4. What are the public relations or public confidence risks and can these be adequately addressed?

Conclusions

It is my conclusion that the use of wireless can be properly limited and its risks mitigated sufficiently so as to allow its use under these controlled conditions and its benefits obtained. This does not say that the indiscriminate and uncontrolled use of wireless should be allowed in voting systems. Indeed I know of none who advocate the use of wireless in voting systems except in limited applications and with carefully constructed safeguards. The carefully applied and safeguarded use of wireless would appear to provide a potential benefit when used in voting



systems. I suppose that this means I am not a “wireless teetotaler”, we can use wireless responsibly.

However, while it is possible from a technical perspective to limit and safeguard the use of wireless sufficiently to allow its use the issue of public perception and public confidence must be judged separately. Particularly troublesome in the voting system is the fact that many of the safeguards that must be implemented must be done on the local level. One must ponder the ability to retain a high degree of voter confidence if even one jurisdiction does not implement prudent safeguards and a significant security failure occurs. The risk to public confidence may be enough to decide the question or at least the manner in which some aspects of this decision are made.

Analytical Framework

My further remarks will elaborate on those limits and safeguards and the degree to which the VVSG appropriately reflects them.

Technologists generally agree that wireless communication is both less reliable and secure than wireline communications. However the benefits of wireless communications in many applications have produced tremendous advances, improving both its reliability and security. Today wireless communications are routinely used in a wide variety of security sensitive applications, including this nation’s defense, banking, personal and business communications of all kinds. In these applications, and many others, safeguards and mitigation techniques have been identified that are generally judged as sufficient to allow the benefits of wireless to be delivered.

In December of 2002 Dr. Ron Ross of the National Institute of Standards and Technology (NIST) made a presentation to the IEEE P1583 committee titled, “Assessing the Security of Federal Information Technology Systems”. In that presentation a slide titled, “The Security Chain” listed the technical and non-technical elements of an information security system.

The slide ends with the statement, “Adversaries attack the weakest link...where is yours?” This statement and the slide have significant application for the topic of this discussion. If wireless is the weakest link in the security chain of a voting system it should be strengthened. However, if greater weakness exists at some other point then time and resources are more properly applied at that point.

The metaphor may be taken further. If there are limited resources available to address the security needs of a voting system then resources used to improve one aspect of the system security will diminish the resources available to address other potential vulnerabilities. In the extreme an inordinate focus on one risk may result in a chain with a single link strong enough to anchor a battleship and the rest of the chain left a diminished and delicate series of jewelry links.

The Security Chain



Links in the Chain

(Non-technology based examples)

- ✓ Physical security
- ✓ Personnel security
- ✓ Procedural security
- ✓ Risk management
- ✓ Security policies
- ✓ Security planning
- ✓ Contingency planning

Links in the Chain

(Technology based examples)

- ✓ Access control mechanisms
- ✓ Identification and authentication devices
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls
- ✓ Smart cards
- ✓ Biometrics

Adversaries attack the weakest link...where is yours?

National Institute of Standards and Technology

If one of the benefits of wireless is that it saves time and money in configuring systems then the possibility exists that resources will be saved so that more resource will be available in the system to address areas of greater risk. *If labor savings through the use of wireless allows more stringent pre-election logic and accuracy testing or poll worker training, it may provide a net increase in system security.*

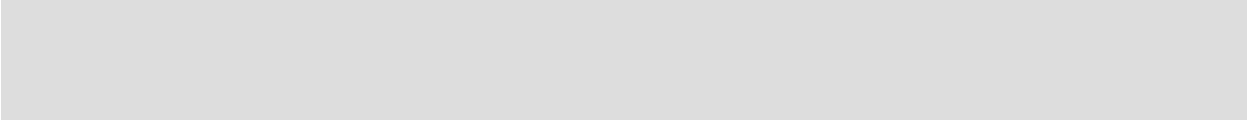
This logic postulates that the use of carefully controlled wireless may introduce a moderate additional risk but result in a net increase in the security of the voting system. This, perhaps, surprising outcome would result if the labor savings benefits allow greater attention to security at other critical points in the system.

We must ask, "What is the risk we are concerned about?" There are two risks:

1. Tampering
2. Confidentiality
3. Denial of Service

Tampering with the outcome of an election is the more serious of the two. If votes can be surreptitiously changed through a wireless link then there is indeed a very serious risk to deal with. Confidentiality is a significant risk but is secondary to the risk of tampering.

In considering the risk of tampering there is a chain of increase risk:

- 
1. Risk of tampering with a single vote.
 2. Risk of tampering with all the votes on a single machine.
 3. Risk of tampering with a precinct's vote tally.
 4. Risk of tampering with a county's vote tally.
 5. Risk of tampering with a state's vote tally.

It is clear that security should be increasingly stringent as the impact of tampering increases.

In a similar fashion concern increases about the risk for confidentiality as opportunity increases to compromise the confidentiality of more votes. In discussing the requirements on wireless in the current draft of the VVSG this hierarchy of risk will be utilized.

A denial of service occurs when the wireless link is disrupted, intentionally or unintentionally by electromagnetic energy or by other means. To affect the voting process wireless the wireless link would have to be used in an essential way, without an alternative for system communication.

We now turn to the current draft of the VVSG and ask the question, "Are sufficient safeguards incorporated in the VVSG to protect against each of these risks?"

Wireless Requirements in the VVSG

The requirements on wireless contained in the current draft of the VVSG are found in Volume 1 Section 6.7. Other sections of the VVSG also apply and several are specifically identified by Section 6.7 as applying. Among the other sections that apply to wireless are the requirements on telecommunications, Volume 1 Section 5. Through that citation the same requirements for accuracy, durability, reliability, maintainability, and availability are applied to wireless as are requirement for other portions of the voting system. VVSG Volume 1 Section 6.7 then proceeds by providing a number of specific requirements for wireless.

The question becomes, are these safeguards sufficient?

Denial of Service Attack

Taking the concerns for denial of service, confidentiality and tampering in reverse order, we begin by examining the safeguards provided for denial of service. Section 6.7.6 is specifically provided to mitigate the effects of a denial of service attack. The first three requirements of Section 6.7.6 are:

- 6.7.6.1 The voting system shall be able to function properly throughout a DoS attack, since the DoS attack may continue throughout the voting process.
- 6.7.6.2 The voting system shall function properly as if the wireless capability were never available for use.
- 6.7.6.3 Alternative procedures or capabilities shall exist to accomplish the same functions that the wireless communications capability would have done.

These requirements would appear to be sufficient that a wireless communications link will not be essential to the voting process. It would appear that a denial of service attack is not a realistic possibility if these requirements are met.

An issue then arises, “How confident are we that these requirements will be met?” This question goes first to the adequacy of the testing or evaluation used to judge system compliance with the VVSG and later to the quality of the entire Voting System Conformity Assessment System. That is, the system that will voting systems are properly tested to the requirements of the VVSG and that delivered systems are within manufacturing tolerances to the system tested.

On this and the VVSG in general the need to specific and thorough test methods the various requirements is observed. It is in the details of the testing and evaluation that many requirements will be fully realized or perhaps undone. So we may conclude that if the testing and evaluation is done well a denial of service attack is not a realistic possibility.

Confidentiality

Confidentiality of the transmitted data is the next point of concern. This issue is dealt with in Section 6.7.4, "Protecting the Transmitted Data". The requirements of Section 6.7.4 are:

- 6.7.5 All information transmitted via wireless communications shall be encrypted and authenticated, with the exception of wireless T-coil coupling, to protect against eavesdropping and data manipulation including modification, insertion, and deletion.
 - 6.7.5.1 The encryption shall be as defined in Federal Information Processing Standards (FIPS) 197, "Advanced Encryption Standard (AES)."
 - 6.7.5.1.1 The cryptographic modules used shall comply with FIPS 140-2, Security Requirements for Cryptographic Modules.
 - 6.7.5.2 The capability to transmit non-encrypted and non-authenticated information via wireless communications shall not exist.
 - 6.7.5.2.1 If wireless communication (audible) is used, and if the receiver of the wireless transmission is the human ear, then the information shall not be encrypted (i.e., this specifically covers the case of the wireless T-Coil coupling for assistive devices used by people who are hard of hearing - see Volume I, Section 2.2.7.2 DRE standards item c)

Using the security chain metaphor, these requirements would seem to reduce the risk to confidentiality to a level far below that presented by other means. Simply stated, there are easier ways to gain access to confidential data than through tapping into the wireless transmission, as guarded by these requirements.

In addition most of the common wireless protocols provide additional security measures to protect the confidentiality of the data being transmitted. If it can be assumed that the implementers of a wireless link will utilize the security features provided with that link then further safeguards, beyond those required in the VVSG will be provided. The VVSG requires that the vendor document these features and explain their application and use. This would appear adequate to safeguard the proper protection of the confidentiality of the data.

Tampering

The draft VVSG guards against the possibility of tampering by . The requirements providing these protections are contained in:

- 6.7.2 Controlling Usage
- 6.7.3 Identifying Usage

6.7.10 Authentication

If properly implemented, these requirements will assure that an election official will know when a wireless link is in use, can control its use and that the use of the link will require proper authentication.

The controlled and limited use of wireless is a critical element. Few argue for the advisability of active wireless links during the voting process for transmitting voting data. The consensus seems to be to restricting wireless to pre and post election functions and if used at all during elections, then only for ancillary functions.

The question then becomes, “Can an election official forbid the use of wireless from the opening of the polls to the closing of the polls and know that this restriction is observed?” A critical element is contained in Section 6.7.3.2 of the VVSG:

6.7.3.2 If a voting system provides wireless communications capabilities, then there shall be an indication that allows one to determine when the wireless communications (e.g., radio frequencies) capability is active.

6.7.3.3 The indication should be visual.

The test for these requirements will be critical. How reliable is the required indication? This requirement could be very robust or relatively ineffective. A robust implementation may place the indicator on the power provided to the wireless circuitry. If the wireless circuitry receives power then the indicator will be active. In this implementation the indicator will only be inactive if there is no power to the wireless circuitry. The requirement contained in Section 6.7.3.2 could be rewritten in this more stringent manner.

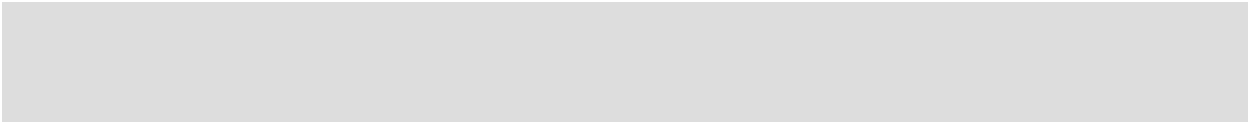
Even more critical will be the test or evaluation used to judge compliance. At a minimum the evaluation of compliance should preclude indicators that can be surreptitiously manipulated with relative ease. A robust requirement and evaluation will give confidence that the use of wireless is under the control of election officials.

As a further observation the accessibility requirements would be well applied here. The indicator of an active wireless link could be required to be both visual and audible. This would support the ability of an election official with a visual disability to perform their function. However, it would also allow an official who is visually or audibly distracted to have a redundant alert to an active wireless link.

The next topic is the control of the wireless link. Section 6.7.2.6 requires:

6.7.2.6 If a voting system includes wireless capabilities, then the system shall have the ability to turn on the wireless capability when it is to be used and to turn off the wireless capability when the wireless capability is not in use.

The critical element here is how much confidence can there be that this requirement is met?



Here again the test and evaluation is critical. If the test requires that the wireless circuitry be on a removable module or that power to the circuitry be physically turned off then there can be great confidence that the wireless circuitry will only be used when the election official intends for it to be used.

Alternately, if the control of the wireless circuitry is indirect and subject to multiple means of control there will be far lower confidence that the intent of this requirement has been met.

Authentication is the third element in protection against tampering. The requirements of Section 6.7.10, Authentication, would appear to be adequate to protect the use of wireless to authorized users. The requirements of Section 6.7.10 do not remove all risk but appear to reduce them to the point where an unauthorized user will find other avenues more promising.

The Role of State and Local Officials

The VVSG and these remarks are written with the belief that state and local election officials will and must play a critical role. The VVSG requirements provide latitude in the equipment which will support local control. This latitude requires that local officials properly fulfill their function if the use of wireless is to be properly limited and safeguarded.

The VVSG could go further.

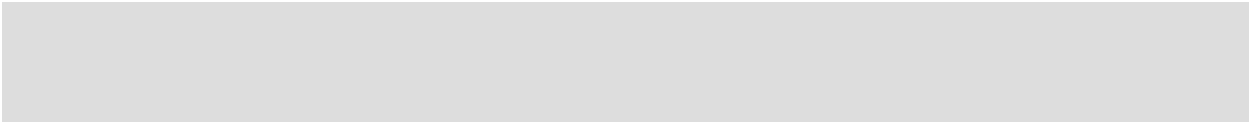
For example, if there was wide agreement that the risks outweigh the benefits during the active voting process then a requirement could be added to the VVSG that a positive interlock be provided that would assure that a wireless link could not be active during active voting and equally that voting could not be conducted if the wireless link were active. Such a requirement could be met with relative ease by removable wireless modules or physical switch between the power provided wireless circuitry and that provided to vote recording circuitry.

The interdependence between management best practices and equipment requirements is extremely important. There is a flexible boundary between what is placed in the equipment requirements of the VVSG and what is provided in management guidelines and best practices. To the degree requirements for wireless security are adequately safeguard in one there may be less stringent requirements in the other. Of course, some degree of redundant requirement provides greater assurance that the system is being used appropriately and securely.

At this interface between equipment requirements and management guidelines uniformity provides positive benefits. To the degree all systems that employ wireless are required to do so in similar ways by the VVSG then the ability to provide more specific and detailed management guidance is increased. Further uniformity of implementation allows for the safeguards placed on those implementations to receive wider review and scrutiny. There would appear to be opportunity for further development in this area. If the VVSG required a more uniform structure for the location or type of indicators used or the manner in which wireless functions are controlled then management guidelines will be able to be more specific and useful.

Benefits of Wireless

Wireless communications offers a number of potential benefits to the voting system. It offers the possibility of significant labor savings in updating voting stations and preparing them for an



election. When this automated update is then confirmed by a following logic and accuracy test that adequately assures that the updates are correct, unaltered and uniform, the benefit delivered would appear significant.

The use of wireless eliminates the need for redundant human actions, with its high error rate, at some points in the pre and post election process. This application increases accuracy by replacing an error prone human process with a more reliable automated process.

Wireless also allows for more timely updates. Particularly in ancillary functions, such as providing voter registration data to polling locations, wireless communications would appear to offer positive benefits. It is to be noted that such ancillary functions may be offered on equipment that is entirely separate from voting equipment. Hence, it is possible to use wireless communications completely separate from voting equipment.

Conclusions

In these remarks I have offered the following conclusions:

1. The use of wireless can provide positive benefits to the voting system if properly limited and protected.
2. The VVSG, as currently drafted appears to provide sufficient safeguards to the use of wireless.
3. The tests and evaluations used to certify equipment as compliant to the VVSG will be critical. It is imperative that uniform, thorough and detailed test and evaluation methods be provided to assure the careful and rigorous evaluation of the VVSG requirements.
4. The VVSG relegates significant security issues to election officials and the election management process. This boundary between equipment requirements and election management could be drawn differently. On several points observations are offered on how it could be drawn differently.

The critical elements to be addressed, based on these conclusions, are the rigor of the equipment evaluation process and the coordination of election management with the equipment specifications of the VVSG.

I thank the Election Assistance Commission, its commissioners and staff for the opportunity to offer these remarks. It is truly a privilege to contribute to this deliberation. I wish the commission every success in its efforts to safeguard and protect the election system of this nation.

Sincerely,

H. Stephen Berger