Security Analysis of InnoVote Products

Risks, Mechanisms, and Vulnerabilities

By
Erin Thead
Software Engineer
erin@erinthead.com

Table of Contents – Security Analysis of InnoVote Products

1. Introduction

1.1. Purpose.

The purpose of this document is to analyze the security of the InnoVote System of software and hardware components. The document provides a detailed description of security risks to the data that InnoVote products use and store, an explanation of security features of the software and hardware that help mitigate these risks, and an analysis of vulnerabilities that remain in the system.

The intended audience of this document is the developer and any other persons interested in the project, including election reform activists, computer security professionals, political figures with an interest in election reform, and potential buyers of the design.

1.2. Scope.

InnoVote Election Products are designed to be secure and reliable. Software products are designed with secure practices in mind, and hardware protection is designed into certain parts of a complete InnoVote System of products.

A complete InnoVote System consists of the following products:

- Some combination of MyVotronic DRE machines with SecureDRE software and CardReader scanners with CardReader Software
- ReliaVote Precinct Edition software at the precinct or voting site level
- Precinct- or voting-site-level products networked securely in such a way as conforms to the design of reference [6]
- ReliaVote Central Server software at the county tabulator level
- County-level network that conforms to the design of reference [6]
- Secure databases (conforming to the specification of references [3] and [4]) on every machine running an InnoVote software product

This document analyzes this configuration *only*. It does not attempt to analyze the security of InnoVote products mixed with compatible third-party products.

1.3. References.

[1] Thead, E. *InnoVote CardReader Hardware Requirements Overview,* 2005.
[2] Thead, E. *InnoVote CardReader Functional Design*, 2005.
[3] Thead, E. *InnoVote Database Access Matrix*, 2005.
[4] Thead, E. *InnoVote Database Detailed Design*, 2005.
[5] Thead, E. *InnoVote MyVotronic Hardware and Operating System Overview*, 2005.
[6] Thead, E. *InnoVote Network Detailed Design*, 2005.
[7] Thead, E. *InnoVote ReliaVote Central Server Functional Design,* 2005.
[8] Thead, E. *InnoVote ReliaVote Precinct Edition Functional Design*, 2005.
[9] Thead, E. *InnoVote SecureDRE Functional Design*, 2005.

1.4. Overview.

The remainder of this document is organized in the following fashion:

Section 2: Provides a description of confidentiality, availability, and integrity risks to data stored and used by InnoVote products.

Section 3: Provides a description of software and hardware mechanisms in InnoVote Systems to provide protection against the threats described in §2.

Section 4: Provides a description of security vulnerabilities that could not be resolved by the mechanisms of §3, a threat assessment of each, and suggested good practices to mitigate the risk. Also provides a description of the hardware and software components that are considered a high risk.

2. Security Risks

This section describes the security risks of conducting an election electronically, in whole or part. It does not describe security risks of the proposed design of InnoVote products.

2.1. Risks to Data Confidentiality.

The risks described in this section are associated with the privacy of data and with protecting sensitive data from unauthorized viewing. Confidentiality of sensitive data is important in an election because if a third party obtained incomplete voting results before an election was over, the attacker could release it to the public and potentially affect the final outcome. The section assumes that an attacker does not obtain privileges to modify data but merely to read it.

2.1.1. Risk CR1: Data interception over a network

2.1.1.1. Description of Activity

This activity consists of an unauthorized person's intercepting election data that are being transmitted from a precinct to a Board of Elections in a county or parish.

2.1.1.2. Threat Type

The threat associated with this activity is the release of sensitive private data to the public or to unauthorized third parties.

2.1.1.3. Severity of Threat

This threat is of moderate severity. An unauthorized person could take actions, such as releasing the data he or she obtained, that might result in an election result's being different from what it might otherwise have been; however, the intruder is not directly altering the results.

2.1.2. Risk CR2: Local unauthorized viewing of stored data

2.1.2.1. Description of Activity

This activity consists of an unauthorized person's viewing vote results that are stored on the hard disk or memory of a voting device or tabulation computer, or a person viewing such results before an election has been declared over. This unauthorized viewing is performed locally, at the machine in question, rather than across a network communication line.

2.1.2.2. Threat Type

The threat associated with this activity is the release of sensitive private data to the public or to unauthorized third parties.

2.1.2.3. Severity of Threat

This threat is of moderate severity. It is assumed that any person who obtains access to locally stored vote data is either a voter or an election official. If either person obtains access to such data, he or she could release it to the public or to other unauthorized persons, potentially affecting the final outcome.

2.1.3. Risk CR3: Remote unauthorized viewing of stored data

2.1.3.1. Description of Activity

This activity consists of an unauthorized person's viewing vote results that are stored on the hard disk or memory of a voting device or tabulation computer. This unauthorized viewing is performed over a network communication line.

2.1.3.2. Threat Type

The threat associated with this activity is the release of sensitive private data to the public or to unauthorized third parties.

2.1.3.3. Severity of Threat

This threat is of moderate to high severity. It assumes that the intruder is not a person who is voting or an election official, but rather, an outsider. If such a person obtains access to the data, he or she could release it to the public or to other unauthorized persons, potentially affecting the final outcome.

2.2. Risks to Data Availability.

The risks described in this section are associated with availability of election data to software and human users who need it. Availability of data is important during an election because certain attacks on data availability could result in severe delays in restoring the affected systems, possibly causing some voters to leave the voting site and therefore potentially affecting the outcome. The section assumes that an attacker does not obtain read or write privileges to the data but is able to prevent *others* from using it.

2.2.1. Risk AR1: Network flooding

2.2.1.1. Description of Activity

This activity consists of "jamming" network communication lines between election systems with useless data. Important data can be dropped or delayed significantly.

2.2.1.2. Threat Type

The threat associated with this activity is denial of service.

2.2.1.3. Severity of Threat

This threat is of low to moderate severity. Proper implementation of data communication protocols will ensure that the data are *eventually* received by their intended recipient, if possible, and that the sender of the data will not assume that the recipient has received the data until all data are acknowledged thus.

If the attack is carried out at the precinct level while an election is in progress, and the voting equipment is configured to transmit votes in real-time to a tabulation system in the precinct, then the attack conceivably could result in delays at the precinct level that might frustrate individuals who have not yet voted. Such voters might choose to leave the site, potentially affecting the final results. However, if the attack is carried out after an election is ended, then it will not affect the final results, only the time to report the results.

2.2.2. Risk AR2: Loss of a critical network node

2.2.2.1. Description of Activity

This activity consists of preventing a node from transmitting and/or receiving data, either by terminating its connection to the network via a network flooding attack or by executing some instruction on the machine itself that prevents it from connecting. The node in question is considered critical, because it either receives election results, transmits them, or does both, and if it goes down, the transmission of the data to the county's central tabulator cannot be completed.

2.2.2.2. Threat Type

The threat associated with this activity is denial of service.

2.2.2.3. Severity of Threat

This threat is of low to moderate severity. As with flooding attacks, proper implementation of a valid protocol will ensure that the data are either acknowledged as being received or that the sender is made aware that the data could not be received.

As with flooding attacks, if this attack is carried out in a network that requires real-time transmission of election results while an election is in progress, it could result in severe delays and frustration of voters. However, if it is carried out after an election is over, the worst case is that it would delay the reporting of results.

2.3. Risks to Data Integrity.

The risks described in this section are risks to the integrity of important election data. This class of risks is the gravest when it relates to an election. In the best case, a *detected* security breach that compromised data integrity could invalidate the election results on every computer or voting device where it occurred and require a recount or re-vote. An *undetected* integrity violation could result in a fraudulent final outcome.

2.3.1. Risk IR1: Local unauthorized modification of votes and tallies

2.3.1.1. Description of Activity

This activity consists of an unauthorized person's modifying vote results and/or tallies, or an authorized person's doing so at a time at which it should not be done. The intruder has direct, local access to the computer or voting device on which the results are stored and is not using the machine over a data communication network.

2.3.1.2. Threat Type

The threat associated with this activity is the falsification of valid election results and thus potentially the wrong candidate or candidates being declared winners.

2.3.1.3. Severity of Threat

This threat is of high severity. If the computer on which the activity occurred has no means of detecting that the data were modified and no means of alerting other authorities to the modification, then this activity could have extremely severe consequences.

2.3.2. Risk IR2: Remote unauthorized modification of votes and tallies

2.3.2.1. Description of Activity

This activity consists of an unauthorized person's modifying vote results and/or tallies. The intruder does not have local access to the computer or voting device and has gained access to it over a network connection.

2.3.2.2. Threat Type

The threat associated with this activity is the falsification of valid election results and thus potentially the wrong candidate or candidates being declared winners.

2.3.2.3. Severity of Threat

This threat is of high severity. If the computer on which the activity occurred has no means of detecting that the data were modified and no means of alerting other authorities to the modification, then this activity could have extremely severe consequences.

2.3.3. Risk IR3: Modification of data in transit on a network

2.3.3.1. Description of Activity

This activity consists of an attacker's modifying sensitive election data while the data are being transmitted from one machine to another over a network. It is assumed that the sender and recipient of the data cannot detect the modification.

2.3.3.2. Threat Type

The threat associated with this activity is the falsification of valid election results and thus potentially the wrong candidate or candidates being declared winners.

2.3.3.3. Severity of Threat

This threat is of high severity. If the sender and receiver have no means of detecting that the data were modified and no means of alerting other authorities to the modification, then this activity could have extremely severe consequences.

2.3.4. Risk IR4: Impersonation of a legitimate network node

2.3.4.1. Description of Activity

This activity consists of an attacker's using a computer which should not have access to election data (a "malicious node") and impersonating a computer that has legitimate access to election data. Typically this activity is performed by "spoofing" the legitimate node's IP address on packets. The malicious node can either modify the data illicitly and pass it to a valid node that believes it to be the node it is impersonating (risk IR3) or fail to transmit data to some other computer that is expecting it, giving the appearance that it has lost its connection.

2.3.4.2. Threat Type

This activity is associated with two distinct threats, depending on the course of action that the impostor takes. If the malicious node modifies data, the threat is the falsification of valid election results. If the malicious node does not modify data but instead does not transmit it when another computer is expecting it, the threat is denial of service because the other computers will report the "loss of a critical network node" (risk AR2).

2.3.4.3. Severity of Threat

The threat is of high severity. If the other computers in the network have no means of detecting that the node is an impostor, then data transfers from it will be treated with the same privileges as data transfers from the node it is impersonating.

3. Security Mechanisms

3.1. Network Security Mechanisms.

This section describes hardware and software mechanisms of InnoVote products that are designed to mitigate the risks to data that are being transmitted from one machine to another over a network.

3.1.1. NSM 1: Encrypted transmissions

3.1.1.1. Description of Mechanism

When an InnoVote software product initiates a data transmission to an InnoVote software product installed on a different machine, the data transmission will be encrypted. This is true whether the sender and receiver are located on public networks or private. The mechanism for this (the Kerberos protocol) is described in detail in reference [6], *Network Detailed Design*, section 4.

3.1.1.2. Risks Mitigated by This Mechanism

This security mechanism alleviates the following risks:

- CR1: Data interception over a network. An intruder will be unable to read the data because the data will be encrypted and the intruder will not have the keys to decrypt it.
- CR3: Remote unauthorized viewing of stored data. The computer with the stored data will not accept an unencrypted connection. It should be noted that this security mechanism is not sufficient to minimize this risk, as an intruder may be able to initiate a secure socket connection.
- IR2: Remote unauthorized modification of votes and tallies. The computer with the stored data will not accept an unencrypted connection. It should be noted that this security mechanism is not sufficient to minimize this risk, as an intruder may be able to initiate a secure socket connection.
- IR3: Modification of data in transit on a network. An intruder will be unable to read the data because the data will be encrypted and the intruder will not have the keys to decrypt it.
- IR4: Impersonation of a legitimate network node. An intruder will not be able to impersonate a legitimate machine for the purpose of collecting data unless he or she has gained access to and compromised the machine. It should be noted that this security mechanism is not sufficient to minimize this risk, as an intruder may be able to do this.

3.1.2. NSM 2: Kerberos infrastructure

3.1.2.1. Description of Mechanism

The InnoVote machines will be networked in a way that conforms to the network architectures of reference [6], *Network Detailed Design*. Voting machines and ballot scanners will be connected over a private network to the precinct computer. The precinct computers will have public connections to the county's central computer.

For every such private precinct network, there will be a Kerberos infrastructure that gives a private password or key. For every public county-wide network, there will be a similar Kerberos infrastructure. A precinct computer will not use the same key for data transmission over the two networks that it may access; it will have separate keys or passwords for the precinct and county networks.

The Kerberos servers for the precinct networks will be located at a private IP address in each precinct's network and the Kerberos server for a county will be located at a public IP address. The key management systems will conform to the Kerberos version 5 protocol.

3.1.2.2. Risks Mitigated by This Mechanism

This security mechanism mitigates the following risks:

- CR3: Remote unauthorized viewing of stored data. A machine with locally stored sensitive data will not accept packets from unauthorized machines. It should be noted that this security measure itself does not protect against a malicious instruction from a compromised machine that still has a recognized key pair.
- IR2: Remote unauthorized modification of votes and tallies. A machine with locally stored sensitive data will not accept packets from unauthorized machines. It should be noted that this security measure itself does not protect against a malicious instruction from a compromised machine that still has a recognized key pair.
- IR4: Impersonation of a legitimate network node. The machines in a given network will not allow unencrypted packets to be stored as data or executed as instructions. If a malicious node spoofs the IP address of a legitimate one, it will not have access to the legitimate node's key and thus cannot forge an encrypted packet.

3.1.3. NSM 3: Private networks

3.1.3.1. Description of Mechanism

Every precinct network will be private. The only machine with access to the public Internet will be the precinct computer. All voting machines and ballot scanners will have private IP addresses. The precinct computer will mediate traffic to and from the private network. Also, any machine that attempts to connect to the physical network in a precinct will have to be recognized as a valid network node or it will not be granted access to the private network or the machines thereon.

3.1.3.2. Risks Mitigated by This Mechanism

This security mechanism mitigates the following risks:

- CR3: Remote unauthorized viewing of stored data. Data that are stored on voting machines and ballot scanners are viewable only from within the private network. Only recognized machines will be allowed to use the network communication lines.
- AR1: Network flooding. The establishment of a private network at the precinct level makes it extremely difficult to impossible for the private network to experience denial of service from traffic flooding. The precinct computer will mediate traffic in and out of the network, and only valid machines will be allowed to use the network lines.
- IR2: Remote unauthorized modification of votes and tallies. With the voting equipment located on a private network with no access to or from the public Internet, it will be extremely difficult to impossible for an intruder to gain access to the databases.
- IR3: Modification of data in transit on a network. The establishment of a private network makes it extremely difficult to impossible for an intruder to obtain and modify data.
- IR4: Impersonation of a legitimate network node. The virtual private network management system will not allow a node to enter the network and claim it is some other node.

3.1.4. NSM 4: Firewalls

3.1.4.1. Description of Mechanism

As described in reference [6], *Network Detailed Design*, numerous firewalls will be present to restrict traffic to and from machines in a network. Section 3 of that document gives a detailed description of the placement and configuration of these firewalls.

3.1.4.2. Risks Mitigated by This Mechanism

This security mechanism mitigates the following risks:

- CR1: Data interception over a network. The firewalls will prevent unauthorized machines from sending or receiving data on the network and will therefore prevent such machines from intercepting confidential data.
- CR3: Remote unauthorized viewing of stored data. The firewalls will limit network traffic destined for any InnoVote machine, and the firewalls that protect the private networks will limit the traffic that can enter the networks in the first place.
- AR1: Network flooding. Some firewalls have "learning" mechanisms by which they can often detect a denial-of-service attack and restrict traffic from the machine or machines that are generating the excessive traffic.
- AR2: Loss of a critical network node. Firewalls that can detect denial-of-service attacks will inherently help to prevent a successful denial-of-service attack.
- IR2: Remote unauthorized modification of votes and tallies. A firewall that mitigates Risk CR3, "Remote unauthorized viewing of stored data," is inherently mitigating the risk of having such data modified as well.
- IR4: Impersonation of a legitimate network node. The firewalls control access to the network, making impersonation of a good node very difficult to impossible.

3.2. Local System Security Measures.

This section describes hardware and software mechanisms of InnoVote products that are designed to mitigate the risks to data that are being stored on the hard disk or memory of a machine.

3.2.1. LSM 1: Prohibition of remote access to databases

3.2.1.1. Description of Mechanism

Every InnoVote machine will contain a database, as is described in reference [4], *Database Detailed Design*. The database management system for a database will be configured to allow local access only. The database management system will not be allowed to initiate connections to or accept connections from a remote system. All ports will be closed except the port(s) over which InnoVote software products make connections with each other and with the Kerberos server.

3.2.1.2. Risks Mitigated by This Mechanism

This security mechanism mitigates the following risks:

- CR3: Remote unauthorized viewing of stored data. The database program will not be listening on a data port for connection attempts. The only open ports will be used by InnoVote software programs, therefore requiring that any data received over these ports be handled by that software. The database will not allow the remote login of users.
- IR2: Remote unauthorized modification of votes and tallies. The database requires user authentication to view any tables. If users cannot login remotely, then they will not be able to view the data stored in the database.

3.2.2. LSM 2: Duplication of sensitive election data

3.2.2.1. Description of Mechanism

As is described in the *Functional Design* documents for each InnoVote software product, the database tables containing information about specific ballots and the votes thereon will be duplicated, both locally on the voting device and in transfer to the precinct computer. As soon as a ballot is finalized and cast—whether electronically or by paper scan—the voter's choices are transmitted to the precinct computer in real-time and stored, both on the precinct computer and the voting device where the ballot was cast. On the voting device, the vote is also copied into a duplicate table that is transmitted in full to the precinct computer when the election is declared over.

Additionally, when a vote is finalized, the voter's choices are determined and increments are made to the tallies of the correct candidates or ballot options. As is described in reference [4], *Database Detailed Design*, a separate table exists for candidate/option tallies.

3.2.2.2. Risks Mitigated by This Mechanism

This security mechanism mitigates the following risks:

- IR1: Local unauthorized modification of votes and tallies. This security feature does not make it *impossible* to modify sensitive data, but it—in combination with LSM 3—makes it much more difficult for tampering to go undetected. As is described in the *Functional Design* documents for the InnoVote software products, each product contains functions that will check these tables for tampering.
- IR2: Remote unauthorized modification of votes and tallies. If the security mechanism prohibiting remote logins were undermined, this security feature—while not making it *impossible* to modify sensitive data—would, in combination with LSM 3, make it very difficult to tamper with data without being detected.

3.2.3. LSM 3: Encryption of sensitive database elements

3.2.3.1. Description of Mechanism

The tables in a database that store information about votes, real-time votes, and (if necessary) votes retallied during a recount will be protected with strong encryption. The tables as a whole will be protected, rather than individual entries, so as to prevent all forms of tampering. A detailed description of this system is given in §4 of reference [4], *Database Detailed Design*. To decrypt one of these tables, the database management system will have to authenticate the software operation that is requesting the decryption. An access matrix is provided in reference [3] that describes which software operations will need access to these sensitive tables, and *when* they may have such access.

3.2.3.2. Risks Mitigated by This Mechanism

This security mechanism mitigates the following risks:

- CR2: Local unauthorized viewing of stored data. It will not be possible for an unauthenticated human user or unauthenticated program or program operation to obtain access to the data in plain-text readable form.
- CR3: Remote unauthorized viewing of stored data. If the feature prohibiting remote logins were undermined, it would not be possible for an unauthenticated human user or unauthenticated program or program operation to obtain access to the data in plain-text readable form.
- IR1: Local unauthorized modification of stored data. This feature, in combination with LSM 2, provides not just protection against tampering, but a detection mechanism. The candidate tally table will not be encrypted, but the vote tables will. As is described in the *Functional Design* documents, the InnoVote software products retally totals from the real-time votes and finalized votes. The software programs check all three sources of tallies—the unencrypted tally table, the real-time vote table, and the finalized vote table—against each other. Any differences trigger an alert.
- IR2: Remote unauthorized modification of stored data. If the feature prohibiting remote logins were undermined, this feature, in combination with LSM 2, would provide protection against tampering and a detection mechanism. The candidate tally table will not be encrypted, but the vote tables will. As is described in the *Functional Design* documents, the InnoVote software products retally totals from the real-time votes and finalized votes. The software programs check all three sources of tallies—the unencrypted tally table, the real-time vote table, and the finalized vote table—against each other. Any differences trigger an alert.

3.2.4. LSM 4: Authentication of software operations that use a database

3.2.4.1. Description of Mechanism

Although the developer has proposed two user-authentication policies for the database management system (found in §5 of reference [4], *Database Detailed Design),* she strongly advises potential users of the InnoVote product line to require that individual software *functions,* rather than the products taken as wholes, be authenticated by the database management system when they need to use a table. The database management system will store authentication data for every valid software function, as well as a list of operations that the software function will be allowed to perform on the table. A detailed description of these privileges is given in reference [3], *Database Access Matrix*. A software function will be granted the appropriate access until it informs the database management system that it is about to complete execution, at which point the DBMS will log out the "user" associated with that software function.

3.2.4.2. Risks Mitigated by This Mechanism

This security mechanism mitigates the following risks:

- CR2: Local unauthorized viewing of stored data. This mechanism is highly effective in ensuring that no unauthorized human users or software programs can even read the database tables.
- CR3: Remote unauthorized viewing of stored data. If the mechanism to prohibit remote logins to the database were undermined, this mechanism would prevent unauthorized entities from viewing the database.
- IR1: Local unauthorized modification of stored data. By preventing unauthorized individuals and unauthorized software from reading the database, this mechanism also prevents unauthorized entities from writing to the database.
- IR2: Remote unauthorized modification of stored data. If the mechanism to prohibit remote logins to the database were undermined, this mechanism would prevent unauthorized entities from writing to the database.

3.2.5. LSM 5: Time constraints on data access

3.2.5.1. Description of Mechanism

In an election, certain operations may be performed on database tables only at particular times. For example, the candidates that will appear on a ballot may be changed at any time prior to the day of the election, but not while an election is taking place. Stored vote data may be deleted from the database after a given period of time following the election (as prescribed by the laws of the state in which the election is taking place), but not before. For this reason, the database management system will control access to tables based not only upon the privileges that a software operation requires to execute correctly, but also upon the date and time at which the access request is taking place. The database management system will have its own internal clock to determine the date and time.

3.2.5.2. Risks Mitigated by This Mechanism

This security mechanism mitigates the following risks:

- CR2: Local unauthorized viewing of stored data. A time-limited access system prevents a software operation from viewing the database during a time period when such viewing would be potentially damaging to the confidentiality of the data.
- CR3: Remote unauthorized viewing of stored data. Even if the security mechanisms to prevent remote access to the database were undermined, a time-limited access system prevents viewing of the database during a time period when such viewing would be potentially damaging to the confidentiality of the data.
- IR1: Local unauthorized modification of stored data. A time-limited access system prevents a software operation from making modifications to the database during a time period when such modifications would be potentially damaging to the integrity of the data.
- IR2: Remote unauthorized modification of stored data. Even if the security mechanisms to prevent remote access to the database were undermined, a time-limited access system prevents modifications to the database during a time period when such modifications would be potentially damaging to the integrity of the data.

3.2.6. LSM 6: Packet analysis and filtering

3.2.6.1. Description of Mechanism

This mechanism allows an InnoVote software product to analyze the data segment of an authenticated and decrypted packet and determine whether the data in the packet contains a command to view or modify an encrypted database table. The encrypted database tables contain information about real-time votes, finalized votes, and (if necessary) recounted votes. Only certain systems should be requesting access to these sensitive tables, and even when the packet appears to have come from a trusted source, if it is requesting to use a database table that it has no need to use, the request should be denied. Such an event would indicate that either the key management server or the software product requesting the modification was compromised.

This very powerful feature is integral to each InnoVote voting and tabulation software product. For each product, it behaves slightly differently, depending on the product's requirements, but the concept is the same: Machines can accept modification requests from lower-level machines but not higher-level ones. They can accept viewing requests from higher-level machines but not lower-level ones. The specification for ReliaVote CS also contains this security feature, although the county's server does not "report to" any higher-level node and would not need to block modification requests from it. The security feature provides protection not just against compromised *software* programs, but also against a compromised key server, and this is why it appears in ReliaVote CS. As is stated in §4 of this document, the county's Kerberos server is at a higher risk for attacks than other machines.

3.2.6.2. Risks Mitigated by This Mechanism

This mechanism mitigates the following security risks:

- CR3: Remote unauthorized viewing of stored data. This feature provides a fail-safe mechanism in case the key server or another InnoVote software product is compromised. The mechanism prevents any system other than the local one from viewing the sensitive election data.
- IR2: Remote unauthorized modification of votes and tallies. This feature strongly limits the ability of an intruder to modify vote results. As has been described elsewhere in this document, it would be extremely difficult to make modifications to the encrypted tables on any InnoVote product, but it is especially hard to do so to the machines with private IP addresses (the voting devices), and, with this feature in use, the precinct PC as well, since any changes to the precinct PC's vote tables would have to have originated from within the private network. Therefore an attacker would likely attempt to modify results on the county's tabulator and "cover his tracks" at the lower levels so that the modification would not be noticed. This feature makes such activity impossible.

3.2.7. LSM 7: Event and error recording

3.2.7.1. Description of Mechanism

As is described in the *Functional Design* documents for each InnoVote software product, when an error or a significant event occurs, an entry is created in the Events table of the Database. Among the events considered "significant" are modifications to vote tables, reprogramming a voting device, and (for voting machines and scanners) locking the hardware from input or output.

This mechanism is not preventive, but rather, detective, in case some other security mechanism is compromised. The event table would indicate what had occurred and when it happened.

3.2.7.2. Risks Mitigated by This Mechanism

This mechanism mitigates all of the security risks described in section 3 of this document. It does not provide means of preventing any of these events from occurring, but if they do occur, it provides a means of detecting them and potentially recovering from them. In an election, a security breach can be minimized if an uncompromised "paper trail" of ballots exists—which will be the case if InnoVote voting devices are used—and the security breach can be detected. If the uncompromised paper ballots exist, then a security breach that is detected in time will be effectively neutralized because the paper ballots will be counted in a secure manner. The real risk to an election's legitimacy is *undetected* tampering.

4. Vulnerabilities and High Risks

In spite of the extensive security measures taken to ensure the confidentiality, integrity, and availability of data on InnoVote products, the data cannot be considered completely secure. The security system that the measures of §3 establish places certain components at a high risk for being attacked. Additionally, although InnoVote software products themselves are designed to be secure, third-party operating systems of computers on which some InnoVote software products reside may not be secure.

4.1. Components with High Risk of Being Attacked.

4.1.1. Kerberos key management servers

The security design of the InnoVote System places considerable responsibility on the Kerberos key management servers. These servers, most particularly Kerberos servers on a public network, store the cryptographic keys that allow InnoVote products to determine whether to accept incoming data from a given source or not. The InnoVote products check to ensure that data packets received on their ports *are* encrypted before processing the packets further, but they have no means of determining whether a particular key is valid other than the information that they may receive from the key server. An attacker that succeeded in compromising the key server would have seriously undermined the network security of an InnoVote system.

It should be noted now that, were this done, the InnoVote products still have restrictions on what software operations a packet can initiate and what operations can be performed on sensitive data. Security measure LSM 6, "Packet analysis and filtering," provides this level of extra protection in the event of a Kerberos server failure. However, that security measure would be invoked only in a scenario in which some component—most likely the Kerberos server but also possibly another InnoVote software product—were compromised.

The key servers for the precinct networks have private IP addresses and are located on networks that require authentication for data sent by them to be accepted by other machines on the network. These servers are highly secure. However, the key server for the county must be located on a public network in order to provide access to the central server and all the precinct computers. As is stated in reference [6], *Network Detailed Design*, the Kerberos server for the county will be protected by a very strict firewall. This firewall severely limits the traffic that will even be allowed to reach the server, and the Kerberos protocol itself provides means of authentication before the server allows a connecting machine to use another machine's public key in encrypting a data transfer.

4.1.2. Central tabulation server for a county

There is a hierarchy of databases in a network of InnoVote products. Voting machines and ballot readers are at the bottom, precinct computers are in the middle, and the county's central server is at the top. Machines on a lower level need to request modifications to a higher-level machine's local database as they transmit their vote tallies to the higher level, but there should be absolutely no modification requests in the opposite direction. Likewise, machines on higher levels need to request copies of a lower-level machine's data, but lower-level machines do not need copies of higher-level data.

Because a precinct network is private and precinct computers will block modification attempts from higher-ranked or unknown computers, an attacker would most likely attempt to modify results on the county's tabulator. Such an attacker might attempt to "cover his tracks" at the lower levels so that the modification would not be detectable, but the security measure LSM 6 ("Packet analysis and filtering") would prevent such activity from succeeding, thereby keeping an intact copy of the election results distributed across the county on the precinct computers and again on the individual voting devices located in every precinct. However, as is shown in the next paragraph, such activity is not even necessary to perpetrate undetected election fraud.

The software specification for ReliaVote CS provides no mechanism for definitively determining that a change was made to the vote results. Also, it is assumed here that any intruder who compromised the system to such a degree as to [(1)] break down the firewalls, [(2)] compromise the Kerberos system for the county and impersonate a precinct computer, and [(3)] successfully decrypt and modify all the vote results, could also modify any timestamps placed on his activities. Were such an event to occur, the intruder would not have to backtrack and modify the uncompromised data that exist in the precincts, because after the precinct computers transmit their final election data to the county's server, they assume that the data is safe on that server. There is no further checking of data unless it is required by law or election officials take the initiative themselves to do so. This means that data stored on the county's central server are more vulnerable to integrity attacks than data stored elsewhere.

The developer of the system considers it highly improbable that an attacker could successfully penetrate the multiple layers of security and modify the sensitive data on a county's server without being detected. As is stated in §4.2, even with the assumption that the computer's operating system contains security flaws that theoretically would allow a person to gain full access to the hard disk, the network security features and the encryption of the sensitive database tables provide excellent protection for the county's tabulation server.

4.1.3. Firewalls that control access to private networks

The private networks that exist in every precinct are protected by a strong system of firewalls, as well as a "mediator" computer (the precinct computer) that has the only public IP address. The security of this network restricts the amount and type of data that can enter or exit the network.

The firewalls that protect the private networks are not "vulnerable" in the sense of necessarily having known flaws that could be exploited, but because of the responsibility that they have, the developer believes that they are at a higher risk for attempted attacks. Any person who manages such a network should ensure that, should the firewall system for a private network be disabled by some means, that the precinct computer should detect it and all machines with private IP addresses lose their connections to the Internet immediately.

4.2. Operating System Privilege Vulnerability.

It must here be noted that a vulnerability exists on the computers that have ReliaVote Precinct Edition and ReliaVote Central Server. These computers, despite their firewall protection and cryptographic protection, are more vulnerable than others because they have public IP addresses. (This vulnerability does not extend to the kiosk machines that will have CardReader Software because these machines are located on private networks and do not have access to the public Internet, nor do they have keyboards or mice attached.)

The database management system on such computers is a separate piece of software and is not controlled by an InnoVote software product. It is controlled by the computer's operating system. Were an intruder to exploit a security flaw in the operating system of one of these computers and gain system-level access, the intruder could conceivably bypass the security measures of the database management system to gain access to the stored data on the hard disk. The vote tables are encrypted, but since the hypothetical intruder has full access to the system in our worst-case scenario, he or she could "hijack" a legitimate InnoVote software function that the database management system would recognize as one that needs the tables decrypted. The intruder could then, perhaps through a Trojan horse acting as the InnoVote software function, make modifications to the database tables.

In truth, this scenario is highly unlikely to occur. It would require the simultaneous breakdown of all the network access mechanisms, including traffic-restricting firewalls, and the compromising of the Kerberos server so that the intruder could impersonate a machine whose instructions in the data packets would be granted write access to the sensitive data. This scenario would also require the attacker to have a ready-made script or program that would exploit a security flaw in the computer's operating system and grant him or her system-level privileges, and another ready-made program that would impersonate a valid InnoVote software operation and trick the database management system into decrypting the sensitive database tables. These events are extremely unlikely to occur simultaneously. Nevertheless, this is a recognized security vulnerability of the InnoVote election system and must be documented so that appropriate measures can be taken to prevent it, such as keeping the operating system up-to-date on any security upgrades and "bugfixes" that are offered by the vendor.

4.3. Necessary Steps for Altering the Reported Results of an Election

An attacker wishing to alter the reported results for an election would have to perform the following steps and fail to be detected at each step:

1. Obtain the public IP address of the county's central tabulator. This is trivial.
2. Obtain the port number over which ReliaVote CS is listening for connections. Once an IP address is found, this is trivial.
3. Bypass the firewall that limits traffic to specific IP addresses, either by spoofing a valid IP address or by "hacking" the firewall itself. This is more difficult but doable.
4. Initiate a connection on the ReliaVote CS port to the Kerberos server. Discovering the IP address for the Kerberos server is trivial, but the completion of a connection again requires spoofing a whitelisted IP address and port or "hacking" the firewall that protects this server.
5. Penetrate the Kerberos server for the county and obtain a fraudulent "ticket" that would fool the central tabulator into identifying it as one from a recognized computer. This is extremely difficult, and most attacks that made it this far would fail in this step. If an unauthenticated computer attempted to communicate with the county server, it would be rejected.
6. Forge data packets with instructions that will be accepted by ReliaVote CS. Since this action is presumed to take place after voting has occurred but before the results are reported, the only action that the software will allow is for new votes to be added to the table. This means that the data packets must contain perfectly formed unique entries to the vote tables. The packets must also contain modifications to the tally table. This requires the attacker to have extensive knowledge of the database structure. This step is difficult but doable with a knowledge of the system.

This list shows that the burden of protection from this attack falls on the Kerberos server. It is highly unlikely, given strong keys that are not known to or retrievable by humans, that the Kerberos system could be circumvented, but if this were to happen, then the integrity of the election data is dependent on the attacker's ability to modify the county server's database.