DANE COUNTY CLERK

City-County Building, Room 106A
210 Martin Luther King, Jr. Boulevard
Madison, Wisconsin 53703
(608) 266-4121

SCOTT McDONELL
COUNTY CLERK

Recently, the integrity of our elections has been called into question. I want to be clear that Dane County has the most rigorous system in place to ensure election integrity in the state of Wisconsin. For example:

Coding:

- Dane County codes our own elections, unlike many counties who outsource this duty to the vendor.
- The vendor does not touch our equipment or software. There are no updates or patches.
- Our election servers and scanners are not connected to the internet.

Testing:

- The County Clerk's office marks and tests 100's of ballots, making sure the totals are correct.
- After the election supplies and ballots are distributed throughout the County, municipal clerks then do their own testing in an open meeting to again ensure the equipment is recording the vote correctly.

Board of Canvass (BOC) Review:

- The BOC checks to see if there is a large under-vote (for example 1000 people vote, but there are only 700 votes for President).
- The BOC checks to see if the historical results of each ward is reasonably consistent.
- If there is a suspicious result, the BOC can vote to pull either the paper ballots or digital ballot images in order to inspect them.

Post-Election Audits

- Dane County is the only county in the state which routinely audits random wards for election anomalies. The digital images are compared to the election results posted to verify that the equipment is working properly and to ensure that voters are properly filling out their ballot.

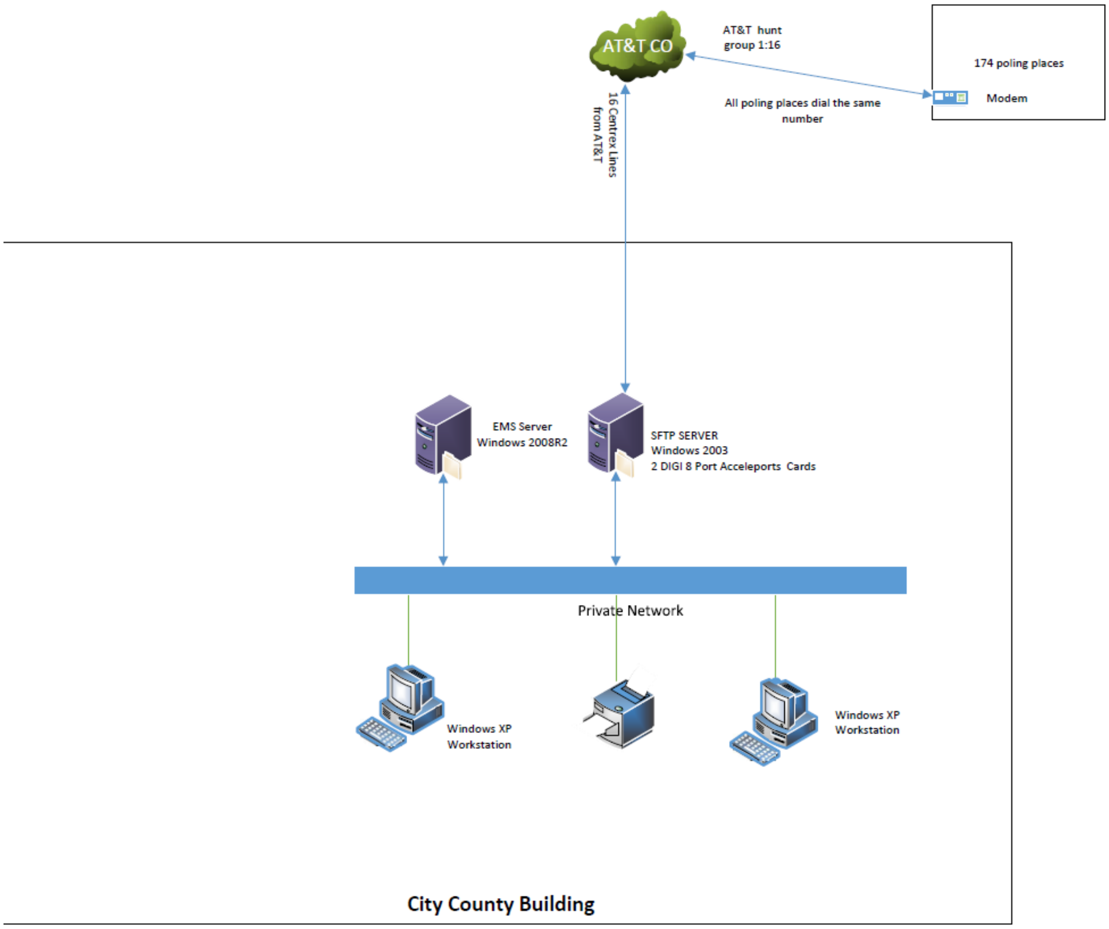
Paper Ballot Trail:

- In the end, there is a paper ballot filled out by the voter. Any attempt to commit fraud would be very risky due to the fact that there is a paper record of the election.

Research has shown that some voters think that their vote is not secret or that their vote won't be counted. They then decide that voting is pointless. As you can see we ensure that every vote is counted. Let's work to get the word out that our elections are secure.

Security Details

This diagram shows the how the election system is set up.


AT&T CO
AT&T hunt group 1:16
174 poling places
Modem
All poling places dial the same number
16 Centrex Lines from AT&T
EMS Server Windows 2008R2
SFTP SERVER Windows 2003 2 DIGI 8 Port Acceleports Cards
Private Network
Windows XP Workstation
Windows XP Workstation
City County Building

Page 38`

Hardware

Unofficial early results transmission is accomplished using the following hardware: DS200 Precinct Tabulator with its optional imbedded modem, a server at the jurisdiction, and a Firewall at the jurisdiction. In this version of the system, the modem in the DS200 is a "land line" modem that communicates over the public telephone network. The server houses a telephone modem bank to receive the transmissions, and Remote Access Service (RAS) software to manage the connection requests from those modems. The server will also host a secure file transfer COTS software package (alternatively, this service can be run on a separate server). The firewall provides a buffer between the network segment where the server is located and the rest of the network (other internal virtual networks or external networks)."

...

- The server is to allow no remote devices other than the DS200 tabulators (via the RAS modems) and the results transfer service (which runs on the EMS Results PC) to connect to it.

Page 39

ES&S Software Encryption

The data that is transmitted is encrypted using the CAVP certified AES algorithm and it is digitally signed using the CAVP certified ECDSA digital signature algorithm. The CMVP certified Open SSL cryptography module is used for these cryptography functions.

Page 43 - 45

Dial-up Communications Security

When wired, i.e. dial-up communications is deployed as part of the system, various countermeasures are deployed in place of an Intrusion Detection System (IDS). Even when dial-up communication is being used, the system is not connected to any other internal or external network except through the phone system. A dial-up connection is considered to be much safer and secure than a broadband connection. Each time the Tabulator dials in, a unique IP address is assigned. Since the IP address constantly revolves, it essentially makes your dial-up connection more secure and reduces the threats from hackers.

Various Countermeasures Deployed:

The steps below, combined with a thorough set of policies and an educated user community, can significantly enhance the security of a dial-up environment. In order to reduce the threat from hackers, the following countermeasures are deployed:

Encryption

If an unauthorized dial-up user penetrates the identification and authentication defenses of a computer system, encryption is used to prevent data modification and deter theft. Encryption is technically a privacy measure, as opposed to a pure security precaution. It is intended to make the information unintelligible to anyone who does not have the proper decryption capability (key, algorithm, or decryption device). This prevents unauthorized personnel who do access a system from being able to read the data that they may want to alter, destroy, or circulate.

For data communications, data is encrypted both at the application layer and at the point of transmission and must be decrypted at both the data transmission layer and at an EMS terminal (application layer) where the key used in the encryption process has been installed. ES&S uses encryption for all data transmissions. The encryption used for dial-up eliminates sending cleartext.

Although the encryption and decryption process is primarily used for data transmission, the encryption process done by the application protects critical files and programs from external threats. Encrypted data and program source code make it very difficult for an unauthorized user to determine what information or code is contained in a file.

Encrypting files also protects file relationships that can be determined by reading the source code of programs that use such files. For the intruder unfamiliar with an organization's data components and flow, such an obstacle can discourage any further unauthorized activity. Even for authorized users, encrypted files bear no relationship to the information the users are accustomed to seeing.

Page 95

Modeming results: NIST asserts that encrypting modem results offers a reasonably secure transmission mode for unofficial results.

Page 32

Data Transfer Security

ES&S optical mark recognition systems exchange information only with the EMS PC. Removable media is the primary method used for this exchange. Alternate methods of data transfer are not available in this version of the ES&S OMR systems. Data transferred between ES&S's Digital Scan OMR systems and the EMS PC is protected using digital signatures to ensure its authenticity. Encryption is used to protect the information in the key exchange package. The RSA Crypto Library is used for these services; it is CMVP certified. The AES algorithm and AES algorithm and EC-DSA algorithm in that library are NIST CAVP certified.