Voting Systems Security: A Rope of Sand

G.D. Ritter & Nick Tiller

February 8, 2012
Table of Contents
The Paper

Our Story So Far:

- The Help America Vote Act of 2002 mandated use of electronic voting systems.
- Many of these voting systems were put in place before adequate security testing took place.
- Problems range from obvious debug code left in place in the production systems to major problems with the architecture.
Methodology

To elucidate problems in the relevant systems:

- Time-limited access to source code
- More than 300,000 lines of code per system
- Understanding of architecture critical
- Independent confirmation necessary for including a vulnerability in paper
Before the election...

- eCM (eSlate Cryptographic Module Manager) creates a master key, which is stored on every eCM token (a USB thingy.)
- The BOSS (Ballot Origination Software System) creates the database representing the precincts, electoral race, &c and write it to MBBs.
- MBBs are PCMCIA storage cards containing vote information.
- SERVO (the System for Election Records and Verification of Operations) resets the JBCs, eSlates and eScans for use, and transfers the key onto these devices.
During the election...

- The eScan system uses paper ballots. These are fed into the eScan machine, which writes them to an MBB.

- The eSlate machine requires a 4-digit code, which is generated by the JBC (Judge’s Booth Controller) and provided by a poll worker. Paper confirmation is printed by the VBO (Verified Ballot Option) attached to the machine.

- Absentee ballots are processed together by Ballot Now, which records the results to another MBB.
After the election...

- MBBs are taken to election headquarters.
- Loaded onto a machine running *Tally* or a machine running *Rally* that is attached via network to a machine running *Tally*.
- Votes are added and logs are verified by the machines.
Problems

- Failure to effectively protect election data integrity.
- Failure to eliminate or document unsafe functionality.
- Failure to protect election from malicious insiders.
- Failure to provide trustworthy auditing.
MBB Images

- If an attacker gets a hold of the MBB, they can tamper with the data by replacing the contents of the MBB with earlier contents of the MBB.
- As the MBBs are used for the final tally, these votes may be simply ignored.
- 100 lines of C code are sufficient to copy the data from the MBB, which can then be rewritten.
BOSS, Ballot Now, SERVO, and Tally require a username and password.

An attack allows access to the secure database in which these data are stored, whereupon they can be deleted.

Accessing any of these applications then allow you to create a new administrator account, giving you full access.

You can then modify... just about anything.

Ballot Now checks with another database using a stored procedure; if this stored procedure is modified, you can log in to Ballot Now with any username and password.
Third-Party Software

- The cryptographic functionality in many third-party components is never verified by Hart’s systems (e.g. the eCM tokens are Spyrus Rosetta USB devices.)

- More worringly, there is a great deal of reliance on Windows, e.g. the eCM keys rely on CryptGenRandom in Windows 2000, which contains vulnerabilities.

- Flaws in these cannot be fixed by the Hart system, as they rely on third-party fixes in order to repair problems.
The eScan configuration file can be uploaded via Ethernet using a simple, unauthenticated protocol. (Can be accessed by a standard socket API.)

The config file contains a commented-out “allow duplicate ballots” option; if uncommented, this allows someone to scan multiple copies of the same ballot, effectively voting multiple times.

(Butler & al also attached tape to a single ballot, allowing it to be pulled back out and rescanned multiple times.)

This can be detected by various logging mechanisms.

There is also an undocumented telnet server running on the eScan machine.
JBC and eSlate

- Both of these devices are susceptible to “soft” button presses.
- A soft button press is an input event which is delivered by serial port that the OS delivers to the application as though it were a typical keyboard interrupt, making it indistinguishable from a real key press.
- Butler & al wrote a program that attached to a JBC via serial port and simulated button presses, retrieving a voter code from the JBC and then using it to vote multiple times by simulating key presses on the eSlate.
- No indication that these votes were faked in the logs; all were counted by Tally.
The EMS applications (BOSS, Ballot Now, Tally, SERVO, and eCM manager) can all write the eCM key to a debug file in cleartext.

The Spyrus library used by these applications checks the Windows registry for a debug file, and if it exists, writes all or part of the eCM key to that file.

Brief access to the registry is all that’s needed to enable this, and the attacker could then return to access the key.
The “Autovote” feature allows for reproduction of a large number of pre-filled-in ballots. It is enabled through the Windows registry.

The ballots are randomly distributed, but ballots with undesired properties can simply be discarded.

Autovote ballets say “Autovote” on the front and back, but this can be removed with image processing software.

Results from autovote ballets are indistinguishable otherwise.
Polling Place Insiders

- A polling place worker can use access to the machine to access or replace memory cards in the eScan machine. (Tamper evident seals may make this more difficult.)
- A polling place worker can correlate the order of ballots cast with the votes cast and relay information to an election official with access to them.
- The JBC’s serial port can be used to access voter access codes without printing by disabling the printer in the menus. The number of outstanding codes is supposedly limited but Butler & al could generate over 10,000 within an expiration period that could be set as high as 16 hours.
Tally maintains a record of which MBBs are tallied. If an MBB is marked as tallied, then Tally will refuse to count the results.

Tally is *wholly* configurable via the Windows registry. Modification of the registry can lead to subtle errors nearly impossible to detect.
EMS Audit Logs

- The EMS audit logs are databases containing entries for every action performed in the EMS programs, including a date and time, the name of the user, an identifier for the action, and data pertaining to the log entry.

- This can be accessed by an unprivileged attacker and freely modified to e.g. hide evidence of tampering. Butler & al accessed it via an ODBC interface and used SQL directly.
The VVPAT Record

- VVPAT (Verified Voter Paper Audit Trail) is the generated paper record to go with voting activity.
- The VBO is attached via 1/8-inch port that is accessible if the VBO is removed. Commands are sent via the port in an unauthenticated fashion. An attacker could print arbitrary data via this port.
- An attacker could modify the VBO’s serial number—calling into question the validity of its printed records—or sever the VBO entirely, preventing voting for a period of time.
- It is trivial and fast to access the interior of the VBO and access or replace the paper.
The VVPAT Record (Cont’d)

- The resulting VVPAT papers use the standard PDF-417 barcode format and plain text, making the resulting paper easy to fake.
- No authenticating information is included.
- An attack needs to know the serial number of the VBO, in which case the paper roll can be replaced in a minute.
Open Interfaces

- Both JBC and eScan listen on TCP port 4600 for commands from SERVO. No authentication is used.
- An attacker with a handheld device and an ethernet cable can mimic SERVO during a live election and cause votes audit logs to be destroyed from an eScan device.
- The JBC uses a parallel port for similar purposes.
Premier Analysis

- Failure to effectively protect vote integrity and privacy
- Failure to protect election from malicious insiders
- Failure to validate and protect software
- Failure to provide trustworthy auditing
- Failure to follow standard software & security engineering practices
Premier Architecture

- Administrator uses the Global Election Management System server (GEMS) to define a ballot.
- Over the LAN, the GEMS server has the Central Office AV-TSX or Election Media Processor, which encode the 128 MB PCMCIA memory cards which are used in the polling places’ AV-TSX.
- The GEMS server also has the 128 KB Epson memory cards created for use at with the polling places’ AV-OS.
- Memory cards are sent to the polling place or pre-inserted into the machines, depending on policy.
At the polling place, the precinct admin opens an election by inserting the *Supervisor Card*.

Voters receive their *Voter Card* from a poll employee who use either the *Voter Card Encoder* or *ExpressPoll*.

Voter uses their card to vote and then returns it.

Supervisor reinserts their card and closes the election.

Optionally, a precinct may instead use optical scan units, wherein the voters simply use paper ballets.

Memory cards are then shipped back to the central office for tabulation.
Table of Contents
Casting Unlimited Ballots

- **Goal:** If the user votes, followed by reinserting their card, it is spit out.

- **Reality:** Vulnerabilities allow users to use successfully use an unlimited number of ballots.

- A user approaches the machine with a stack of smart cards containing the default Smart Card Key.

- Using a previously-discovered exploit, the user is able to access and modify the log to cover their tracks. This takes just over a minute.

- Using another exploit, the user gains access to the Supervisor Menu (again in under a minute) and encodes the Voter Cards (each of which takes a few seconds).
Exposing Voter Choices

- By gaining access to the log, it is not difficult to narrow down and expose voter choices.
Malicious Insiders

- Previous studies on the security of the Deibold/Premier systems resulted in the addition of third-party software *Verdasys Digital Guardian*, *Sygate Security Agent* firewall, and *McAfee VirusScan*.

- DG was designed for Win 2000 or XP and is created to allow an admin to remotely specify policies using special laptop referred to as the Digital Guardian console.

- Each GEMS server runs the Digital Guardian Agent that enforces these consoles. This agent can only be disabled by being connected directly to the DG console.

- The GEMS server has 3 users created: The *Administrator*, *GEMSAdmin*, & *GEMSUser*. 
Circumventing Digital Guardian

- Due to misconfiguration, the GEMSUser is in the Windows Administrators group.
- Another misconfiguration resulted in the GEMS database files being renamable by Nero CD burning application.
- The blacklist policy for apps does not extend to C:/ntldr, which allows the user to change the boot file.
Software Update Authentication Vulnerabilities

- ExpressPoll’s software update is performed by inserting a memory card, which the system scans for either EBOOT.BIN or NK.BIN. EP does not verify these files, and thus a malicious user merely needs to reboot the system after inserting a memory card with a malicious form of either file.

- VCE’s system is similar, except by using a serial cable.

- Digital Guardian’s update can be broken by replacing whitelisted applications with malicious versions (this includes GEMS applications).
Trustworthy Auditing

- ExpressPoll’s logging software is stored in an unsecured .xml file which can be easily modified or deleted, with no indication to the user.
- Digital Guardian’s logging default does not log when a user attempts a malicious activity, despite warning that it will. Thus, auditing shows no indication.
- EMP was similar to ExpressPoll, in that the proper user could simply edit the log file.
- AV-TSX VVPAT uses a paper trail. However, the structure of the VVPAT causes a couple issues. One, it was possible to simply remove the paper log. Two, it was possible to use a syringe to simply inject a liquid that would ruin the ink into the enclosure.
# Table of Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td>Voting Systems Basics</td>
</tr>
<tr>
<td>3</td>
<td>Security in Voting Systems</td>
</tr>
<tr>
<td>4</td>
<td>CASE STUDY: Florida's New Voting System</td>
</tr>
<tr>
<td>5</td>
<td>CASE STUDY: Wisconsin's Voting System</td>
</tr>
<tr>
<td>6</td>
<td>CASE STUDY: Kansas' Voting System</td>
</tr>
<tr>
<td>7</td>
<td>CASE STUDY: Iowa's Voting System</td>
</tr>
<tr>
<td>8</td>
<td>CASE STUDY: Ohio's Voting System</td>
</tr>
<tr>
<td>9</td>
<td>CASE STUDY: Missouri's Voting System</td>
</tr>
<tr>
<td>10</td>
<td>CASE STUDY: Pennsylvania's Voting System</td>
</tr>
<tr>
<td>11</td>
<td>CASE STUDY: Wisconsin's Voting System (Continued)</td>
</tr>
<tr>
<td>12</td>
<td>CASE STUDY: Kansas' Voting System (Continued)</td>
</tr>
<tr>
<td>13</td>
<td>CASE STUDY: Iowa's Voting System (Continued)</td>
</tr>
<tr>
<td>14</td>
<td>CASE STUDY: Ohio's Voting System (Continued)</td>
</tr>
<tr>
<td>15</td>
<td>CASE STUDY: Missouri's Voting System (Continued)</td>
</tr>
<tr>
<td>16</td>
<td>CASE STUDY: Pennsylvania's Voting System (Continued)</td>
</tr>
<tr>
<td>17</td>
<td>Discussion and Conclusion</td>
</tr>
<tr>
<td>18</td>
<td>References</td>
</tr>
</tbody>
</table>

*Note: The table of contents is based on the contents page of the book, which is not provided here.*
Web-Based Voting in Washington, D.C.

*Attacking the Washington, D.C. Internet Voting System* by Scott Wolchuk, Eric Wustrow, Dawn Isabel, and J. Alex Halderman
In a move praised for its transparency, the city of Washington D.C. introduces a new web-based voting system in 2010.

The system is open-source, built on Ruby on Rails, hosted on Apache, uses MySQL.

Uses a public key to encrypt ballots and only a private key, off the internet, can decrypt them.

Multiple firewalls between web and web server, and between web server and application server.
Attacking the Web Application

- The web application’s codebase being open source revealed a vulnerability that allowed arbitrary shell script to be executed.
- By using a filename like foo.$(cmd), the Bash shell on the server would execute whatever cmd was needed.
- Outbound traffic was filtered, but outbound communication could be achieved by writing to the publicly accessible /images directory.
- There was an intrusion detection system, but it did not monitor HTTPS, making the attack feasible.
Secrets were revealed by several means, as simple as finding passwords via bash history and looking for the temporary unencrypted files in the /tmp directory, which were left unchanged.

The encryption code was changed to leave future submitted ballots in the /images directory, and with all previous ballots accessible from the temporary directory, plus other voter credentials, all security was lost.

The (University of Michigan-based) team then added HTML that would play the University of Michigan fight song after the vote completed as a “calling card” of sorts.

Other vulnerabilities existed in the web application, such as failing to use a new encryption key for cookies and basing browser session ids on the sequential rid value from MySQL rather than a random number.
Attacking the Network Infrastructure

- Using network utilities like Nmap and cracking software like “John the Ripper”, the team was also able to gain administrator access to a terminal server.

- Other attackers—at random, most likely not for the vote—were trying to access the server, so they blocked IP addresses and made the password more difficult to guess.

- Installed a keylogger so they could find the other passwords for the attached Cisco switches; locked the admins out of the network as soon as that was done.

- Found publicly accessible webcams—security cameras—attached to the network monitoring the servers and server room. (Photos are included in the paper.)
The Aftermath

- Attack not discovered until mailing list participant asked what the tune they played for successful voters was.
- D.C. officials unable to determine that attack had occurred without “calling card,” and were days away from going through with real use of the system.
- Moral: digital and internet voting is hard.