Checking the List Twice

State Certification Testing of Voting Systems National Conference

Indianapolis, Indiana
June 14-15, 2012

Joshua Franklin

Matthew Masterson

Danielle Sellars

Overview

- Introduction
- Purpose
- What, When, and How to Verify?
- Team Effort
- Relevant Facts
- The Plan
- The Process
- The Results
- Examples
- Conclusions
- Next Steps

Purpose

To explain our experiences in verifying the physical, software, and set up configuration for the voting systems in Ohio's 88 counties.

Why Verify?

- Keep the system safe, secure, and certified.
- Software is the same during distribution, installation, setup. [1]
- Supports a chain of custody
- “Software integrity: ensuring that the software programs have not been altered, whether by an error, a malicious user, or a virus.” – Bruce Schneier

When to Verify?

There is no single answer:

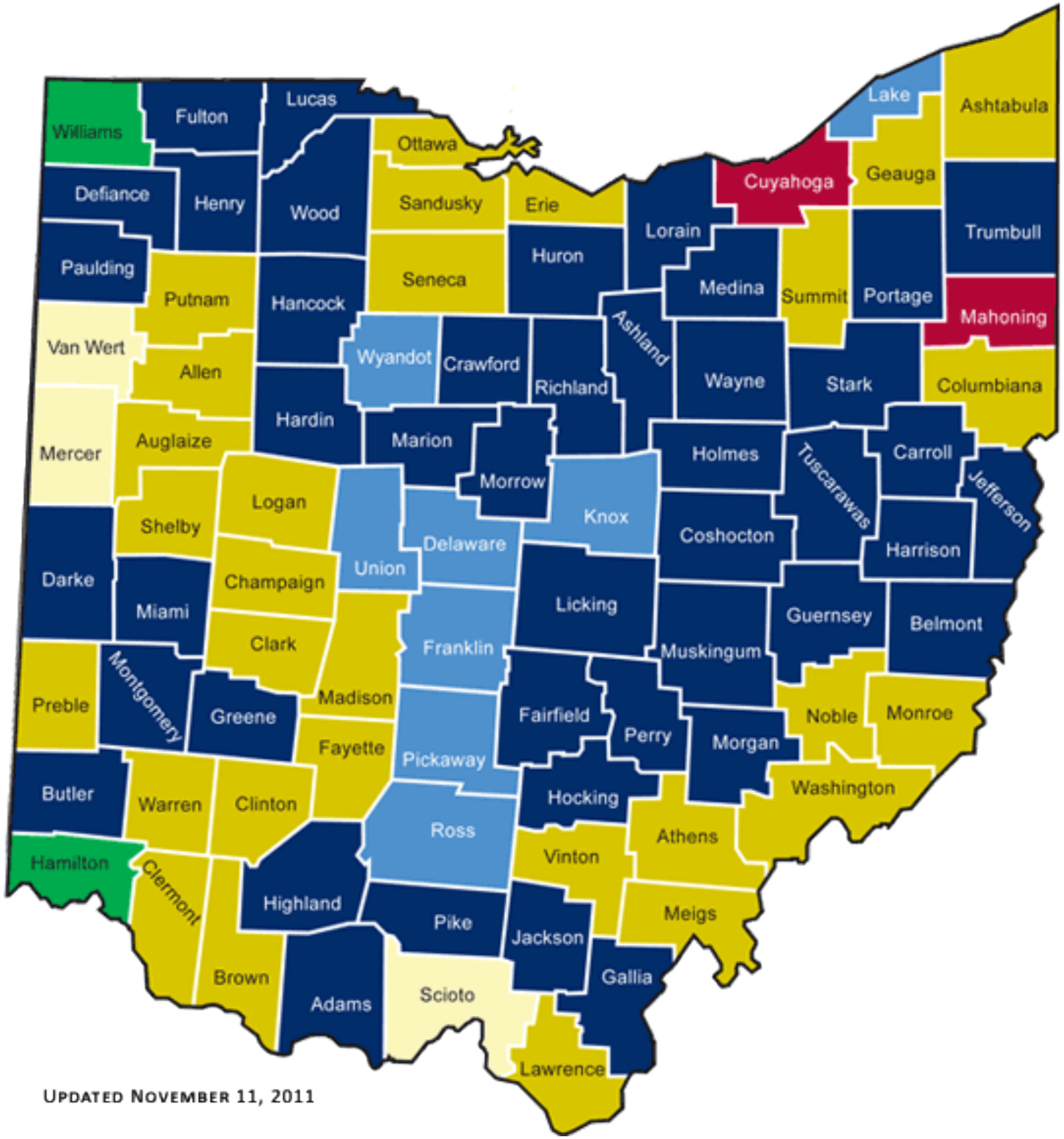
- At time of installation?
- Before the election?
- At the polling place?
- After an election?
- After canvass?
- Part of post-election audit?

What and How to Verify?

- Check the:
  - Installation media
  - Software already on the machine
- System Identification Tools from manufacturer
  - Validate the hashes of the static software files
  - Provides high level of assurance that the software is unchanged

Team Effort

- Accomplishing this is a bumpy road
- Required federal, state, and local efforts
- Danielle Sellars provided the footwork and onsite technical know-how



Updated November 11, 2011

Relevant Facts

- Since being purchased in 2002 systems have not been validated
- Numerous upgrades to every fielded system has been performed since then
- OH requires newly purchased systems to be EAC certified

The Plan

- Start with Premier Assure 1.2 counties
  - All Assure counties were mandated to upgrade to Assure 1.2
  - EAC certified system
- Don't swallow the entire elephant
  - GEMS servers only
- Work with the EAC and vendor to understand what system should look like

The Process

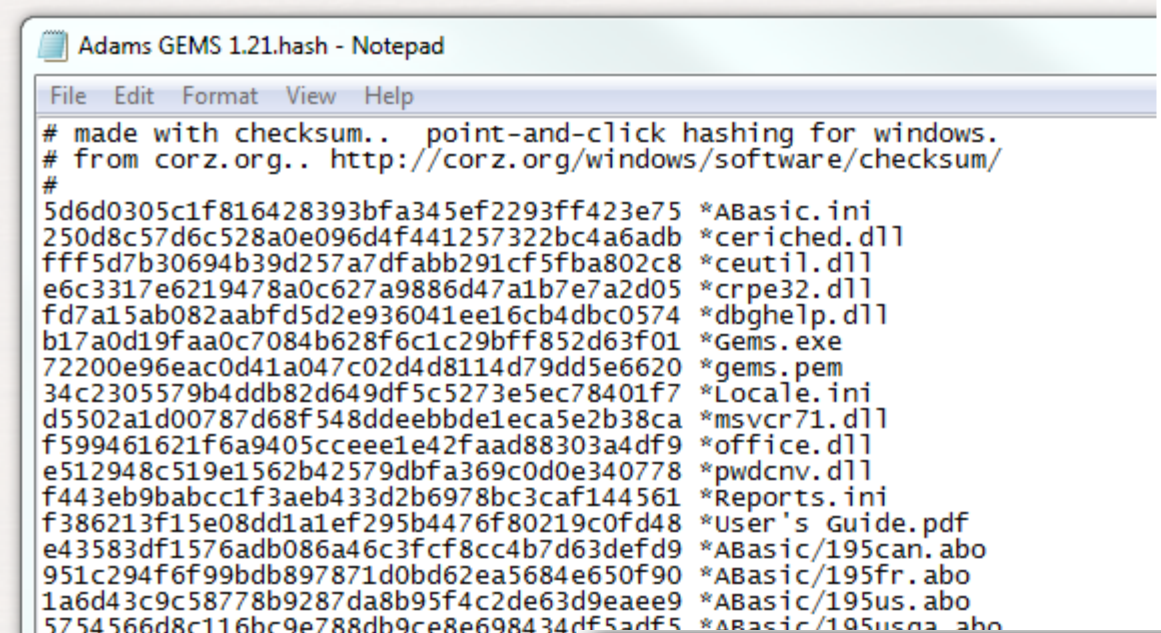
- Process the vendor provided verification tools (uneditable pdf) to a useable format (raw text)
- Run SHA1 hash check on GEMS program directory using portable COTS software
- Confirm hash values match EAC certification through the use of text comparison software
- Identify Windows 2003 Server security configuration (User accounts, Rights, Running Services)

The Results

- Hash checks of GEMS servers show no differences across counties
- Physical checks of the systems show no differences across counties
- The system setup and rights vary greatly from one county to the next
    - Possibly uncertified configuration
    - Possibly significantly less secure

	GemsAdmin	ILS anon	Gems User	IUSR	IWAM	LocalAdmin	LocalGuest	Support	Aspnet	Accutouch TS	IUSR_county	IWAM_county	localadmin	localguest	nonadmin	support
Adams													L	y		y
Ashland																
Belmont																
Butler																
Carroll																
Coshocton																
Crawford																
Darke																
Defiance	y					L	y	y								
Fairfield										y	y	L	L	y	L	y
Fulton										y	y	L	L	y	L	y
Gallia										y	y	L	L	y	L	y
Greene										y	y	L	L	y	L	y
Guernsey										y	y	L	L	y	L	y
Hancock																
Hardin																
Harrison																
Henry																
Highland											y	L	L	y	L	L
Hocking										y	y	L	L	y	L	y
Holmes																
Huron																
Jackson													L	y		y
Jefferson																

County Data

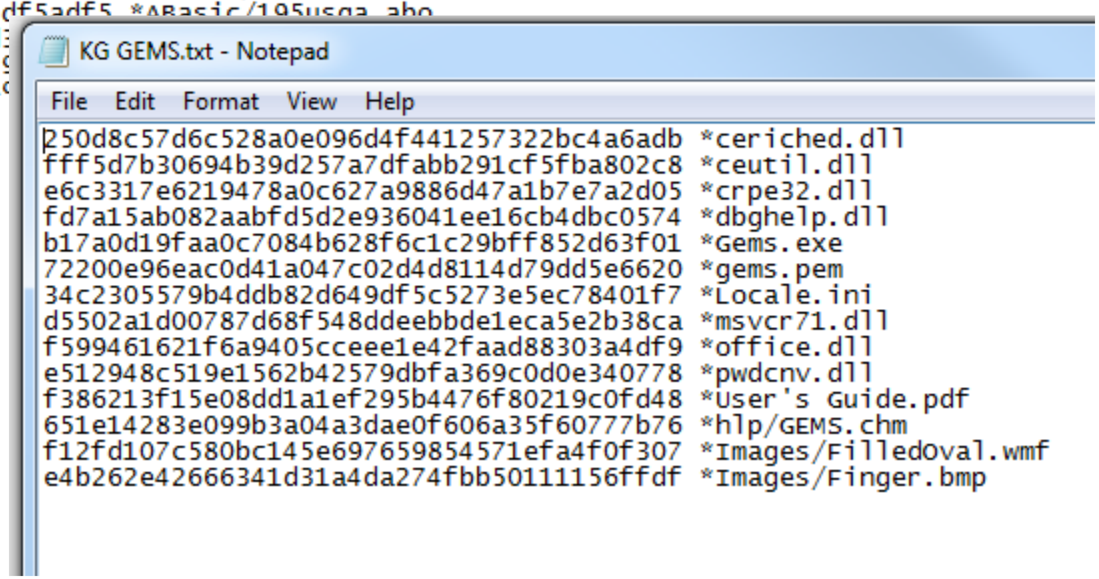


```
# made with checksum..  point-and-click hashing for windows.
# from corz.org.. http://corz.org/windows/software/checksum/
#
5d6d0305c1f816428393bfa345ef2293ff423e75 *ABasic.ini
250d8c57d6c528a0e096d4f441257322bc4a6adb *ceriched.dll
fff5d7b30694b39d257a7dfabb291cf5fba802c8 *ceutil.dll
e6c3317e6219478a0c627a9886d47a1b7e7a2d05 *crpe32.dll
fd7a15ab082aabfd5d2e936041ee16cb4dbc0574 *dbghelp.dll
b17a0d19faa0c7084b628f6c1c29bff852d63f01 *Gems.exe
72200e96eac0d41a047c02d4d8114d79dd5e6620 *gems.pem
34c2305579b4ddb82d649df5c5273e5ec78401f7 *Locale.ini
d5502a1d00787d68f548ddeebbde1eca5e2b38ca *msvcr71.dll
f599461621f6a9405cceee1e42faad88303a4df9 *office.dll
e512948c519e1562b42579dbfa369c0d0e340778 *pwdcnv.dll
f443eb9babcc1f3aeb433d2b6978bc3caf144561 *Reports.ini
f386213f15e08dd1a1ef295b4476f80219c0fd48 *User's Guide.pdf
e43583df1576adb086a46c3fcf8cc4b7d63defd9 *ABasic/195can.abo
951c294f6f99bdb897871d0bd62ea5684e650f90 *ABasic/195fr.abo
1a6d43c9c58778b9287da8b95f4c2de63d9eaee9 *ABasic/195us.abo
5754566d8c116bc9e788db9ce8e698434df5adf5 *ABasic/195usga.abo
8196184c77021ae48c74f5f9bfd67b37d3
40f9fab171cf1fd3e6d3f299096d591c39
4ffa71b4c52a973cce93bc0827684d0f89
```

Certified Values

(manually extracted

from PDF)



```
250d8c57d6c528a0e096d4f441257322bc4a6adb *ceriched.dll
fff5d7b30694b39d257a7dfabb291cf5fba802c8 *ceutil.dll
e6c3317e6219478a0c627a9886d47a1b7e7a2d05 *crpe32.dll
fd7a15ab082aabfd5d2e936041ee16cb4dbc0574 *dbghelp.dll
b17a0d19faa0c7084b628f6c1c29bff852d63f01 *Gems.exe
72200e96eac0d41a047c02d4d8114d79dd5e6620 *gems.pem
34c2305579b4ddb82d649df5c5273e5ec78401f7 *Locale.ini
d5502a1d00787d68f548ddeebbde1eca5e2b38ca *msvcr71.dll
f599461621f6a9405cceee1e42faad88303a4df9 *office.dll
e512948c519e1562b42579dbfa369c0d0e340778 *pwdcnv.dll
f386213f15e08dd1a1ef295b4476f80219c0fd48 *User's Guide.pdf
651e14283e099b3a04a3dae0f606a35f60777b76 *hlp/GEMS.chm
f12fd107c580bc145e697659854571efa4f0f307 *Images/FilledOval.wmf
e4b262e42666341d31a4da274fbb50111156ffdf *Images/Finger.bmp
```

Storage Requirements of Election Equipment (2008-56)	
Climate controlled location	
Security Requirements (2008-56)	
Access to secure rooms kept to minimal number of privileged BOE personnel	
Minimum Access Control Requirements (2008-56)	
Entry/Exit log	
Security Requirements Tabulation Server Room (2008-56)	
Access to secure rooms kept to minimal number of privileged BOE personnel	
Room secured by a double lock system	
Minimum Access Control Requirements (2008-56)	
Entry/Exit log	
Password Management on Tabulation Server	
BIOS Password in place, Split R/D	
Windows Account Password, Split R/D	
Password Complexity (2008-73)	
12+ characters, 2+ numbers, 1 non-alphanumeric, max 2 repeating, mixed case	

State Conclusions

- Establish the baseline configuration for each voting system, regardless of vendor
- Baseline includes tabulation software and system configuration
- Confirm deployed systems match that configuration
- Work with vendors and jurisdiction to bring systems into proper configuration

State Conclusions

- Provided validation tools did not include mechanism for comparison, nor a simple way to compare only static files.
- Produces additional overhead in confirmation process.
- Hash codes must be manually transcribed for visual and/or text comparison
- An automatic utility would be preferable: faster and more accurate

EAC Conclusions

- The tools were not a form that could readily be used. (e.g., received in pdf file format)
- The state would need to procure a COTS hashing tool to compare against the PDF.
  - No automatic comparison. A person would have verify each hash by sight or manually transcribe the values.
- Poor quality hardware pictures requiring special tools and knowledge.

EAC Conclusions

- The EAC's program did not require the tools to be checked for functionality or usability by any parties.
- Vendors basically submitted whatever they wanted under the heading of “System ID Tools".

EAC & State Next Steps

- Validate the voting systems
- EAC work with state and jurisdictions to understand their needs
- Talk with other states to learn their process
- Work with vendor to understand differences and certified configuration

References

[1] Report to U.S. Election Assistance Commission, NSRL, 2004. http://www.nsrl.nist.gov/Documents/vote/July132004-EAC.pdf

[2] Ohio SOS, System Verification Documentation

Questions?

Joshua Franklin

Matthew Masterson

Danielle Sellars