Georgia Voting System

Security Features

Brit Williams

Bwilliam@kennesaw.edu

770-630-9433

KSU Center for Election Systems

Http://elections.kennesaw.edu

elections@kennesaw.edu

1-866-KSU-VOTE

1-866-578-8683

Principal Organizations

- Diebold Elections Systems Division
- NASED Independent Test Agencies (ITAs)
- KSU Center for Election Systems
- Local Election Jurisdictions

Diebold Election Systems

- Prepares the Election System
- Mates the Election System with the Operating System
- Submits the combined Election System/Operating System (SYSTEM) to the ITA
- After ITA and State approval, installs the SYSTEM in the local jurisdictions
- Maintains the SYSTEM hardware

NASED ITAs

- Reviews the SYSTEM for compliance with the FEC Voting System Standards
- Monitors the ‘Final Build’ of the SYSTEM object code
- Submits the Final Build, which includes the SYSTEM source code and object code, to the KSU Center for Election Systems

KSU Center for Election Systems

- Reviews the SYSTEM for compliance with State of Georgia Election Code and Rules.
- Tests the SYSTEM for the presence of any unauthorized/fraudulant code.
- Develops a validation program to use to test the SYSTEM as installed in the Local Jurisdictions.
- Verifies that the SYSTEM installed by Diebold in the Local Jurisdiction is identical to the system received from the ITA and certified by the KSU Center.

Local Election Jurisdictions

- Maintain and protect the SYSTEM
- Use the SYSTEM to program and conduct elections.

Security Functions

There are three distinct functions that must be performed to protect the integrity of the Voting System:

1. Verify that the SYSTEM as delivered from the ITA is free of extraneous or fraudulent code.
2. Verify that the SYSTEM as installed by Diebold in the Local Jurisdictions is *identical* to the SYSTEM received from the ITA and certified by the KSU Center.
3. Verify at specified and random times that the SYSTEM has not been modified in any way.

Security Function 1

Verify that the SYSTEM as delivered from the ITA is free from extraneous or fraudulent code.

- Set up and conduct sample elections with known outcomes that are representative of Georgia general and primary elections.
- Conduct high-volume tests to determine capacity limits of the SYSTEM.
- Conduct tests to determine the SYSTEM's ability to recover from various types of errors.

Security Function 2

Verify that the SYSTEM as installed in the Local Jurisdictions is *identical* to the SYSTEM received from the ITA and certified by the KSU Center.

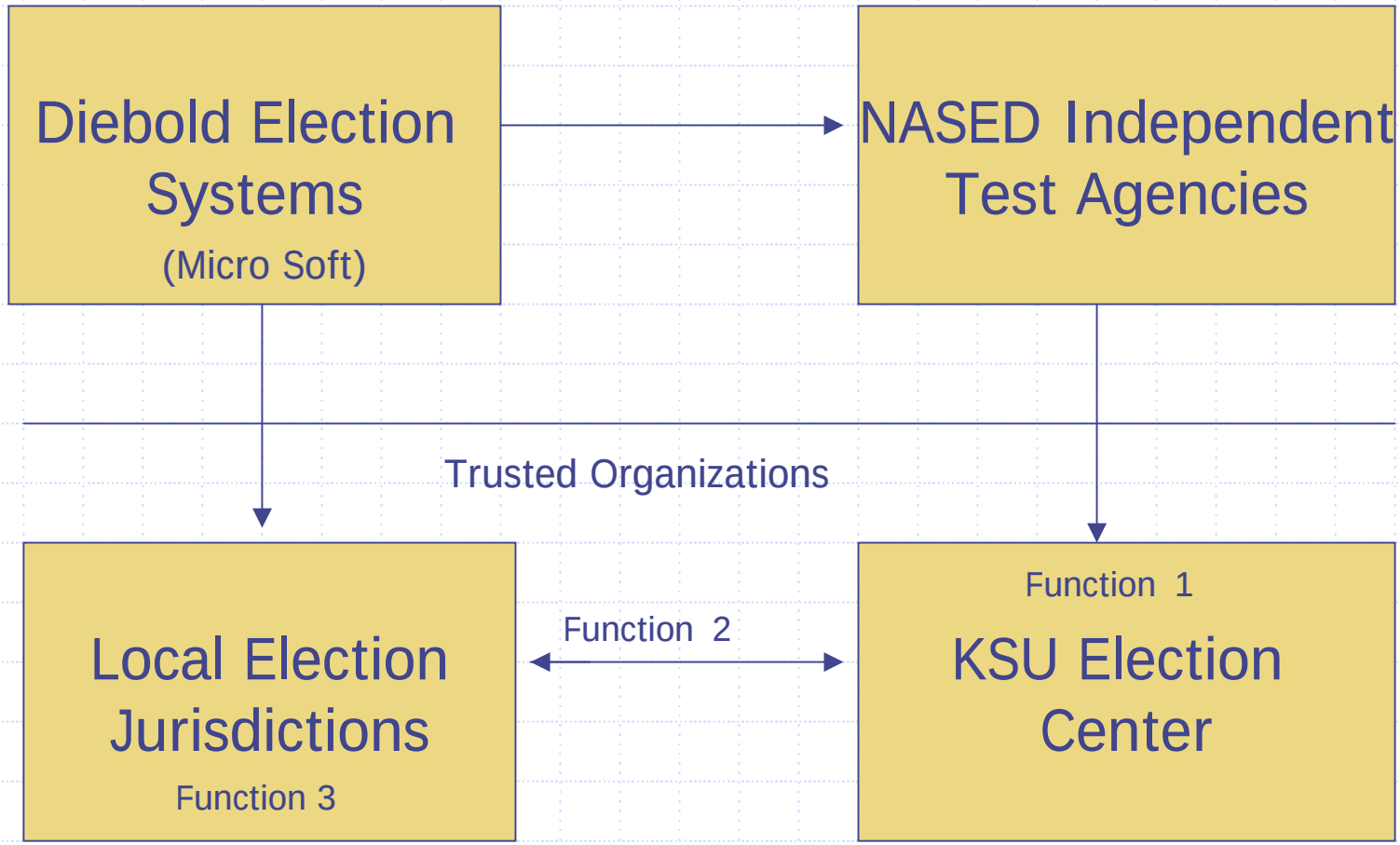
- Prepare a verification program that will detect any changes to the SYSTEM installed in the Local Jurisdictions.
- Run the validation program against the SYSTEM installed in the Local Jurisdiction (after Diebold installation).
- Provide the Local Jurisdiction with a copy of the validation program.

Security Function 3

Verify at specific and random times that the SYSTEM has not been modified in any way.

- Run the verification program immediately before beginning to define an election.
- Run the verification program immediately upon the completion of an election.
- Run the verification program after any suspicious event.
- Run the verification program at random times as desired.

Overview of Security Relationships



Validation Program (Hash)

- Based on NIST certified SHA-1 contained in FIPS 180-2, August 2002.
- Run ‘hash’ on the SYSTEM certified by the KSU Election Center. This creates File 1.
- Run ‘hash-comp’ to compare File 1 with a new ‘hash’ on the SYSTEM in the Local Election Office.
- They should be identical. Any differences are logged.

The chance that a modification will not be detected is less than 1 in 1,000,000,000.

Hash Program

- Based on FIPS 180-2, Secure Hash Statement.
- Computes:

  32 bit CRC,

  128 bit MD5 Hash,

  160 bit SHA-1 Hash.
- www.dmares.com/mareswares/gk.htm

  (See HASH and HASHCOMP)

Procedural Security Features

Procedures that control:

- who can access the system,
- when they can access the system,
- what components they can access,
- what functions they can perform.

Physical Security Features

- Locked offices and warehouses
- No network connections
- No concealed voting booths
- Public posting of precinct results
- Open view of precincts and election offices on election day

Specific Threats

- Trojan horse
- Counterfeit voter cards
- Altering GEMS or AVTS code
- Altering memory cards

Future Considerations

- Download AVTS firmware during precinct setup.
- Implement SAIC high threat features:
  - Dynamic passwords on voter card and Poll Manager's card,
  - Randomize records on one file,
  - Encrypt modem transmission.

Brit Williams

Bwilliam@kennesaw.edu

770-630-9433

KSU Center for Election Systems

Http://elections.kennesaw.edu

elections@kennesaw.edu

1-866-KSU-VOTE

1-866-578-8683