OpenElect® and FreedomVote's Security Features

OpenElect FreedomVote Tablet (FVT)

OpenElect FreedomVote Scan (FVS)

The OpenElect Voting System's in-precinct ballot marking device, the FreedomVote Tablet (FVT), and ballot scanner, the FreedomVote Scan (FVS), are protected by a multi-tiered security policy that encompasses software, hardware and voting procedures on the systems.

The in-precinct units are physically locked and secured to the ballot box. Tamper evident seals are placed on the ballot box and FVS and FVT to ensure security. All access doors to the units themselves are protected via physically locked doors. The system runs an optimized and hardened Linux operating system, which verifies the software components and election data at multiple points throughout the day.

The OpenElect software stores all election definition data and vote files using a 256-bit[1] Advanced Encryption Standard (AES) encryption schema that is unique to each election. The election specific keys are in turn protected with a customer specific AES key of equal strength.

[1] 256-bit encryption refers to the length of the encryption key used to encrypt a data stream or file. A brute force attack on this level encryption would require 2^{256} different combinations, taking 27 trillion trillion trillion trillion trillion years on a current state of the art computer, making it impossible to decrypt without the key.

Typically, 256-bit encryption is used for data in transit, or data traveling over a network or Internet connection. However, it is also implemented for sensitive and important data such as financial, military or government-owned data. The U.S. government requires that all sensitive and important data be encrypted using 192- or 256-bit encryption methods.

Unisyn Voting Solutions

www.unisynvoting.com

All units are set-up for the individual customer and will only communicate with systems that are similarly configured. Additionally, on startup, the system verifies all software against a signature file to verify that the software binaries have not been tampered with, this is then followed by a comprehensive check that the election definition files are valid and unchanged. The system will only allow “whitelisted” files to be executed on the system. FVS and FVT units have no modem, Wi-Fi or Bluetooth capability and are never connected to the internet for any reason.

Each FVS and FVT unit has a unique asymmetric key. The public keys for all valid machines are uploaded to the Election Manager module. When the election is exported, it is signed by the Customer Private Key, and the data is encrypted with a randomly generated AES 256 key. This key is in turn encrypted with the machine public key if the machine is assigned to that election, so that only assigned machines can access the election definition data.

On startup, all systems will first use the Customer Public Key to validate the digital signature on all files to ensure the election data came from a trusted source and is unchanged. The system then uses its own private key (which never leaves the device) to extract the election definition. Simply stated, an election cannot be loaded on an unauthorized machine, nor can a machine use data from an untrusted source.

Unisyn continues as the leader in implementing secure and reliable voting systems. Our systems are designed from inception to meet the security requirements of the U.S. Election Assistance Commission (EAC) Voluntary Voting System Guidelines (VVSG). Unisyn was the first voting system vendor to take full advantage of the wide variety of cyber services offered by the Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA). These cybersecurity service offerings include:

- Voluntary participation in the National Cybersecurity Assessment
- Cyber Hygiene Vulnerability Scan
- Risk and Vulnerability Assessment

In July of 2018, Unisyn became the first DHS election industry partner to undergo end-to-end voting system vulnerability and penetration testing. During the National Cyber Assessments and Technical Services (NCATS) Product Cybersecurity Assessment, a cybersecurity research team from Idaho National Labs (INL) performed a cybersecurity assessment of the Unisyn election system that was completed on October 31, 2018. The purpose of the assessment was to understand the functionality of the system in relation to the current cybersecurity risk assessments and make recommendations to address these items in the interest of protecting the critical infrastructure controlled by Unisyn election systems from a cyber or physical attack.

Cybersecurity is a constantly changing landscape, and Unisyn is committed to providing state of the art secure systems, adding enhancements and protection from newly identified threats with every release.

Contact us for more information:

Unisyn Voting Solutions, Inc.
2310 Cousteau Court, Vista, CA 92081
Tel: +1-760-734-3233
Email: mktg@unisynvoting.com
Website: www.unisynvoting.com