WHITE PAPER: CONSULTING SERVICES

Securing the eSlate Electronic Voting System

Application Security Implementation

By Brad Arkin
brad_arkin@symantec.com

White Paper: Symantec Enterprise Solutions

Securing the eSlate Electronic Voting System

Application Security Implementation

Contents

Executive summary

Hart InterCivic, Inc. engaged @stake, recently acquired by Symantec™ to be integrated into Symantec Consulting Services, as part of its efforts to raise the level of security provided by the eSlate electronic voting system. Symantec @stake consultants advised Hart in making significant changes to the latest version of the eSlate system code and the Hart development process. The enhancements to the overall eSlate design and implementation aim to provide a consistent and robust security level across the system. Hart has applied Symantec's @stake Secure Development Lifecycle to its software engineering process to elevate security to a key driver in the ongoing development of the eSlate voting system.

Overview

The security of electronic voting systems is an issue that is receiving increased national attention. Security researchers, academics, and the general media are raising serious questions about the level of security provided by Direct Record Electronic (DRE) voting systems. The media attention and conflicting expert commentary make the task of securing a DRE voting system particularly challenging. Hart InterCivic ("Hart") has recognized the need to deploy a voting system with appropriate risk mitigation strategies that can be easily described.

Hart engaged @stake, now a part of Symantec Consulting Services, the global leader in information security, to perform a security risk assessment of the eSlate e-voting system and a review of the Hart development process. With guidance from Symantec @stake consultants, Hart implemented a tailored version of the Symantec @stake Secure Development Lifecycle "S@SDL" (see Figure 1) to promote security in Hart's eSlate voting system applications and to address issues identified during Symantec's security assessment of the eSlate system.[1]

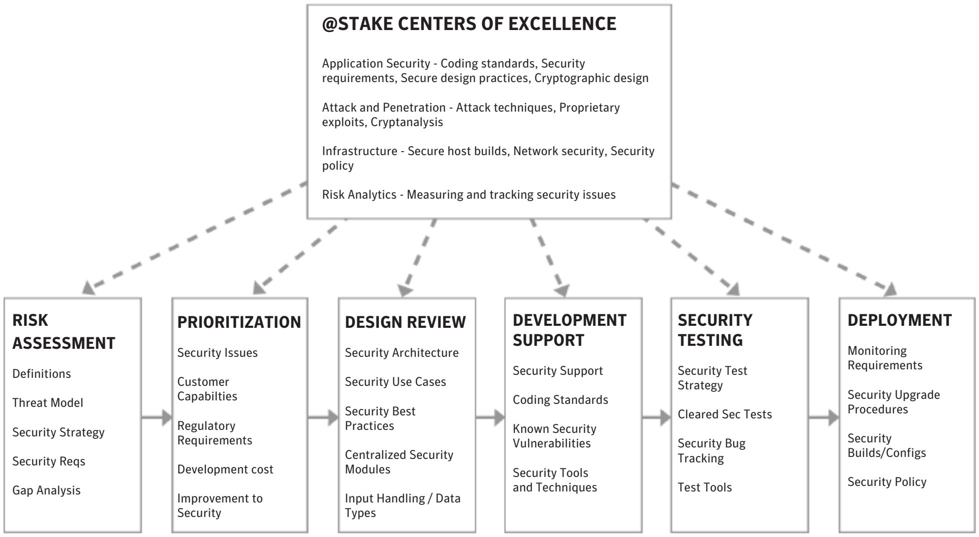
@STAKE CENTERS OF EXCELLENCE
Application Security - Coding standards, Security requirements, Secure design practices, Cryptographic design
Attack and Penetration - Attack techniques, Proprietary exploits, Cryptanalysis
Infrastructure - Secure host builds, Network security, Security policy
Risk Analytics - Measuring and tracking security issues
RISK ASSESSMENT
Definitions
Threat Model
Security Strategy
Security Reqs
Gap Analysis
PRIORITIZATION
Security Issues
Customer Capabilties
Regulatory Requirements
Development cost
Improvement to Security
DESIGN REVIEW
Security Architecture
Security Use Cases
Security Best Practices
Centralized Security Modules
Input Handling / Data Types
DEVELOPMENT SUPPORT
Security Support
Coding Standards
Known Security Vulnerabilities
Security Tools and Techniques
SECURITY TESTING
Security Test Strategy
Cleared Sec Tests
Security Bug Tracking
Test Tools
DEPLOYMENT
Monitoring Requirements
Security Upgrade Procedures
Security Builds/Configs
Security Policy

Figure 1: The Symantec @stake Secure Development Lifecycle (S@SDL)

In the fall of 2003, Symantec @stake consultants performed a comprehensive risk assessment to determine areas for security improvements within the eSlate voting system. The first step in the assessment was a threat modeling exercise. The Symantec @stake assessment was not limited to individual components such as the voter terminal, but identified, ranked, and categorized the risks facing the entire voting system. After completing the threat modeling exercise, a review of the Hart design and implementation was conducted to determine how well the existing countermeasures and risk mitigation techniques addressed the identified threats. The final step in the Symantec @stake risk assessment was the generation of prioritized recommendations for new security features, design enhancements, and development process changes to improve the security posture of the overall system.

Hart integrated the S@SDL into their software development methodology in order to permanently include security as one of the fundamental drivers in the software engineering process. (See Table 1 for an example of this inclusion of security into the development process.) The S@SDL includes risk assessment and prioritization exercises as the first steps in each new release cycle. These steps enable Hart to continuously determine the existing security level of the eSlate system and identify necessary security improvements based on the needs and technical capabilities of eSlate customers. Applying the S@SDL throughout the lifecycle ensures that the security requirements for the system are defined at the start of a new development cycle and tracked throughout the project.

Table 1: eSlate secure design principles

Hart InterCivic established the following principles to drive product development. They are incorporated at every level of the eSlate system and component design.

Design Principle	Description
Defense in Depth	Security is only as strong as its weakest link. Hart products have multiple layers of protection instead of relying on a single defense mechanism.
Segmentation	Components must be isolated from each other and hardened individually against attack.
Stand-alone Security	Each component must be secure in its own right without relying on the security of other components.
Least Privilege	Every component or user in the system is given the minimum set of privileges required to perform a task.
Default to Deny All	By default each component must deny access to resources or information unless the request is explicitly authorized.
Monitor the Environment	The system must support auditing and monitoring processes to detect any attempts to compromise the system. The system must maintain secure audit records to allow forensic investigations into system activity.

Hart identified key points throughout their development process that required security review and support. The S@SDL calls for security reviews to be conducted concurrently with existing events such as software requirements generation, application design, code reviews, and software testing. These reviews provide constant feedback and allow Hart engineers to maintain a focus on application security throughout the development process.

The rigorous software engineering process currently practiced by the Hart software team made it easier to implement the S@SDL approach at Hart. Hart's institutional commitment to quality and security has enabled the company to achieve ISO9001:2000 and BS7799-2:2002 certifications.[2, 3] The following list describes each step in S@SDL in more detail:

- **Risk assessment** – Each new major development cycle begins with an assessment of the current system based on the latest attack techniques, academic research advances, feedback from Hart customers, and new secure development tools. Best security practices are carefully evaluated in the context of the environment where a DRE voting system operates. The output of this step is a set of risks, which are rated according to impact and likelihood, and a set of recommendations for raising the overall level of security.

- **Prioritization exercise** – Hart employs an iterative approach to security that allows the continuous improvement of overall system security with each development release. This evolution of the product suite enables Hart customers to steadily gain experience with new security features and terminology instead of overwhelming election operators with an unfamiliar and unwieldy system. Hart prioritizes recommendations using this iterative philosophy and seeks to make changes that yield the greatest improvement in the system security level. The output of the prioritization exercise is a set of new security requirements that are identified and scoped for the upcoming design cycle.

- **Security design review** – Hart developers interpret and understand the security requirements. They remove ambiguities, verify that the requirements are supported in harmony with the existing security architecture, and evaluate the impact to usability. An emphasis is placed on removing complexity during design and improving the testability of new and updated software components. The output of the design review process is a set of specifications and other documentation artifacts to support the developers during coding and testing.

- **Secure development support** – The Hart security architect provides a variety of development support services to Hart's software engineers. In addition to communicating secure coding standards and detailed information such as cryptographic implementation techniques, the security architect informs Hart developers of advances in tools and techniques for improving security during the development process. The security architect works with developers to resolve any implementation-level roadblocks identified during coding.

- **Security testing** – The Hart test team develops security test cases to exercise end-to-end aspects of the system as well as individual security features. The test team also generates appropriate component-level security testing strategies.
- **Deployment** – The Hart development team works with the implementation personnel who deploy and train users of the eSlate voting system to include security in the operating specifications. The development team also produces policies and guidelines to help customers make use of the latest eSlate security enhancements during an election. In conjunction with the security mechanisms supported by the eSlate system, adherence to these operational guidelines is absolutely critical to the secure operation of an election.

eSlate system architecture

The eSlate system architecture is composed of the eSlate DRE used by voters on Election Day and other components used by election officials to create, manage, and report elections. The eSlate system was designed with multiple discrete components to ensure distributed data processing. The distributed architecture establishes multiple, independent data paths through the system that are cross-verified throughout the election process. Figure 2 shows the eSlate system architecture with all major election functions represented.

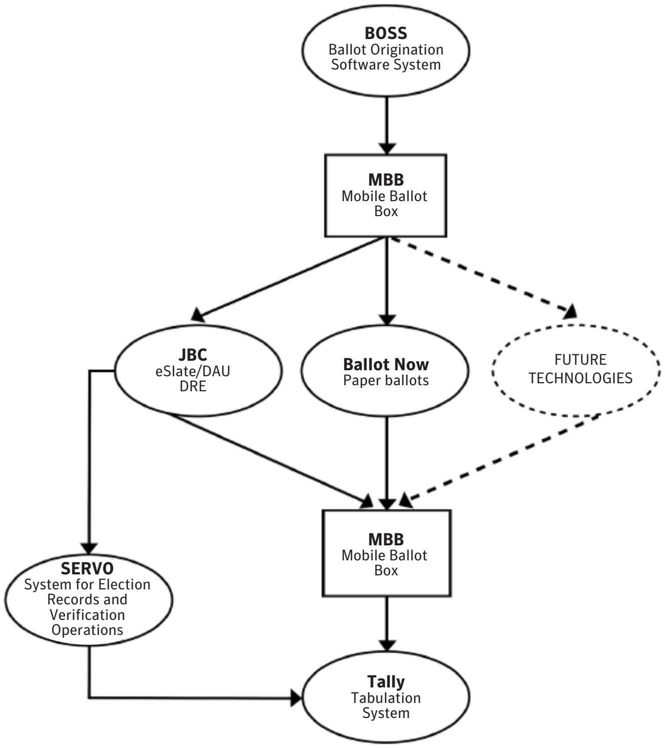

Figure 2: eSlate System Architecture

The three components that comprise the eSlate DRE or Polling Place system are:

1) **eSlate™** – The terminal used by the voter to cast votes.

2) **Disabled Access Unit™ (DAU)** – The unit that modifies an eSlate to provide alternative access features, including an audio ballot reader, for disabled and literacy-challenged voters.

3) **Judge's Booth Controller™ (JBC)** – The polling place control console that manages up to 12 eSlate voting terminals, prints Access Codes and voter receipts, and records Cast Vote Records (CVRs) on the Mobile Ballot Box (MBB).

Election officials use the components identified below to generate ballots, transfer information between devices, and tabulate and report vote totals.

- **Mobile Ballot Box™ (MBB)** – The PC memory card that carries the election database and formatted ballots to the Judge's Booth Controller, Ballot Now, and SERVO and stores CVRs and audit information.
- **Ballot Origination Software System™ (BOSS)** – The software application that enables users to build election databases, format ballots, and electronically write multiple ballot styles to the Mobile Ballot Boxes.
- **Tally™** – The software application that tabulates and reports accumulated totals using the CVRs recorded on Mobile Ballot Boxes.
- **Rally™** – A satellite tabulation application that includes functionality for MBB verification, reading, election data storage, and communication from a satellite facility to a central tabulation function.
- **Ballot Now™** – An application that supports printing absentee/mail ballots on ballot stock from a Secretary of State-certified printer, scanning and digitally imaging the voted ballots, resolving unclear ballots, and capturing CVRs and writing the CVRs to an MBB.
- **SERVO™** – An election records and asset management system that maintains ongoing equipment history and supplies election records as required. This application also supports the ability to produce “recount MBBs.” These recount MBBs can be read by Tally for comparison against the original MBBs and are generated separately, based on both eSlate and JBC internal memory. SERVO also manages backup and storage of CVRs and audit data for election record retention requirements.

Security architecture

The System 4.0 release of Hart’s eSlate Electronic Voting System contains significant new enhancements to provide further assurance of integrity for cast votes. These additions to the system architecture are based on the Symantec @stake security risk assessment recommendations and the integration of the S@SDL with Hart’s development methodology. This release is scheduled for use in live elections starting in 2005.

Combined with the existing security features, the overall security architecture of the eSlate System 4.0 comprises the following major components:

- **Triple redundant storage of vote records** – When a voter casts a ballot, the information is recorded in three locations: eSlate internal memory, JBC internal memory, and on the MBB (the PCMCIA flash card in the JBC device). The different handling and usage profiles of these data storage components yield different risk profiles. These diverse risk profiles significantly increase the difficulty of compromising vote records in all three locations. Triple redundancy of data allows election officials to recover polling place "recount" data from the different storage sources using SERVO. They can then investigate and reconcile any claims of fraud or device malfunction.

- **User account management and password storage** – A role-based access control model and password-based user account authentication protect the workstation components that manage election data, from creating ballot definitions to tallying final vote counts. The system maintains user passwords in one-way salted hash format (PBKDF2).[4] The role-based authorization model allows administrators to easily apply the principle of least privilege by assigning users only those privileges necessary to carry out their job function.

- **Digital signatures of data** – Digital signatures protect all data maintained on the MBB, including ballot definitions and cast-vote records. These cryptographic signatures are generated according to the HMAC specification.[5] This allows the device receiving a MBB to verify the integrity and origin of the data before it is processed. This feature enforces existing policy and legal requirements that protect vote data in transit.

- **Two-factor authentication** – A two-factor authentication system secures all cryptographic key material. Workstation components require cryptographic keys to generate and verify MBB digital signatures. These keys are stored on the eSlate cryptographic module (certified to FIPS-1 Level 3) and are further protected by the eSlate cryptographic module PIN.[6] In order to access the key material, the two-factor authentication requires both: (1) something you have (the eSlate cryptographic module) and (2) something you know (the eSlate cryptographic PIN).

- **Network encryption of data** – Network transfer of data occurs only in specific, limited circumstances between customer-managed facilities. These transfers occur over either dial-up connections on the public telephone network or temporary local private networks composed of a few peer-to-peer machines where all cabling is visible. All client-server connections are protected using SSL and mutual digital certificate authentication.[7] The eSlate System employs the Sybase SQL Anywhere Database and the Sybase network encryption features are enabled with mutual digital certificate authentication to secure connections to a remote database.[8]

- **Individual DB credentials for every customer** – Common design practice for workstation-based commercial applications accessing a bundled DB usually involves the use of a hard-coded DB password in the application binary. This practice introduces a number of risks that are mitigated in the eSlate design by the use of customer-specific DB credentials. The application generates a random set of strong authentication credentials at installation time. These credentials are unique to the jurisdiction and are completely subject to the election authority's control. There are no hard-coded passwords or encryption keys in the eSlate application binaries or source code.

- **Audit logs for all components** – All components in the system, including workstation devices and voter terminals, support a persistent logging mechanism to capture and record all security-related system events.

- **Continuous DRE integrity checks** – The eSlate and JBC components run continuous background monitoring to ensure the integrity of the executable firmware. Firmware is stored internal to the device in non-volatile memory along with a verification table that provides a cyclic redundancy check (CRC) code for each of several code sections. When the embedded, real-time operating system begins code execution, a system task performs a CRC calculation of each code section. The system is halted with a failure message if the calculated CRC does not match the expected value from the verification table. This verification operation is performed continuously while the system is active and provides protection against hardware failures and attempts to corrupt the eSlate or JBC application.

- **Code verification** – The firmware resident in the eSlate components is audited against unauthorized changes by SERVO, both before and after the election. A cryptographically-secure digital hash provides verification that the eSlate firmware is identical to the certified version on file with the National Software Reference Library (NSRL) which is managed by the National Institute of Standards and Technology (NIST). This provides an additional technical protection against attempts to modify election software on voter terminals.

Data flows in an election

Figure 3 shows the flow of data through the DRE function for the eSlate system. The ballot definition software application, BOSS, is located at the jurisdiction central headquarters. When an election begins, BOSS writes multiple MBBs in a quantity sufficient to support the election (i.e., more MBBs than the number of polling places). The MBBs are distributed to the various pieces of equipment in use for a particular election. Figure 3 shows MBBs going to the JBC and SERVO.

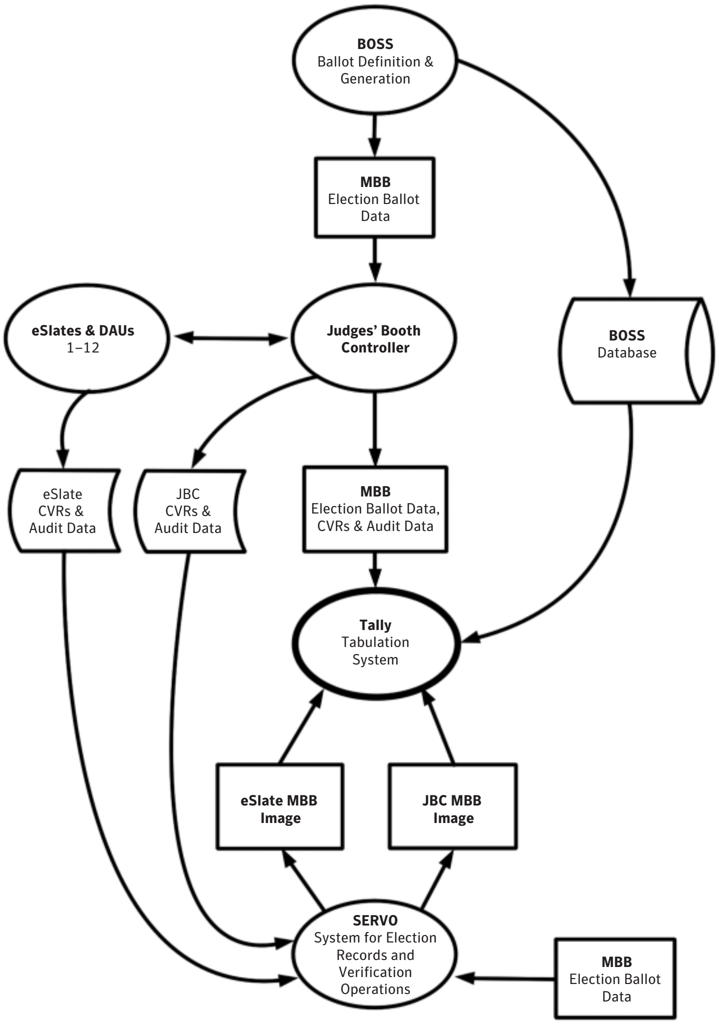

Figure 3: eSlate Data Flows

The JBCs are deployed to the polling locations, connected to as many as 12 eSlate and/or DAU devices, and used to run the election on Election Day. As votes are cast, the Cast Vote Records are redundantly written to the JBC, eSlate, and MBB. The JBC and MBB create a cumulative record of activity that occurs on all connected eSlates. The eSlate creates the records of its specific activity. At the close of the polls, the JBC produces printed records that include accumulated totals from the polling location and an accounting of voted ballots throughout the day. The MBB is removed and securely transported, according to local procedures and elections laws, to the tabulation center to be read by Tally.

The JBCs and/or eSlates are also secured and transported according to local procedures and election laws. The equipment is processed at the warehouse where each unit is connected to a SERVO station. SERVO verifies the integrity of each device’s internal memory, calculates the hash of the firmware, and stores an exact copy of the cast vote and audit records contained on each unit. SERVO maintains this data in a local database.

Once all units have been backed up by SERVO, a system verification record is created. SERVO, using identifying data contained in the redundant records from the eSlate or JBC hardware, compiles and accounts for all equipment and data from the election. SERVO assembles the data into MBB groupings so that each MBB is represented using the records from the JBCs. This process is also performed for the eSlate records.

The result is a complete and independent set of CVRs for the entire election with all equipment and data accounted for by the SERVO process. SERVO verifies the data on the units based on data from an MBB that has been in the possession of election officials at all times. This information is burned to CDs, one for the JBCs and one for the eSlates. These CDs are then delivered to the central tabulation center for system verification.

The primary data path for tabulating vote counts is via the MBBs delivered to Tally. A copy of the BOSS database is used to initialize Tally. This provides the tabulation function with a complete record of every MBB produced for the election. Each MBB is uniquely serialized for each election. As Tally reads each MBB, the integrity of the MBB data is verified and the origin is authenticated before the data is copied to the Tally database.

When the MBB images are delivered to Tally from SERVO, Tally reads each CD containing redundant CVR data from eSlate and JBC memory, populates a separate database, and produces a set of reports. These reports are then compared to the reports produced directly from the MBBs. This is done as an audit check to verify that the totals from the three different CVR storage locations are identical.

Conclusion

Hart has worked to raise the security level of the eSlate electronic voting system and improve the internal processes Hart uses to develop and build software. The comprehensive Symantec @stake risk assessment was the initial step that led to a series of changes in both the Hart development process and the eSlate applications. Hart's use of the S@SDL provides opportunities for security review and feedback at key points throughout the development cycle. The changes in the latest eSlate software release (System 4.0 and above) advance the security assurance and integrity throughout an election. The primary goal of these efforts is to create the best possible balance of security features and usability.

About Hart InterCivic

From electronic voting to the most effective technologies for automating local government processes, Hart InterCivic's name stands for exceptional expertise, absolute accessibility, and trusted transactions. Hart InterCivic is a leader in providing products and services that help redefine the relationship between state and local governments and the citizens they serve. Based in Austin, Texas, Hart InterCivic has offices throughout the U.S. and is working nationwide to bring governments closer to citizens through complete electronic government (eGovernment) solutions and election management solutions. More information about Hart InterCivic is available from the company's Web site at www.hartintercivic.com.

About the author

Brad Arkin is the Technical Manager for Symantec's New York office. Brad holds a MS in computer science with an emphasis in computer security from The George Washington University and a BS in computer science and mathematics from The College of William and Mary. Brad is an MBA candidate at the London Business School and Columbia University.

References

[1] R. Hansen, “@stake Secure Development Lifecycle,” http://www.atstake.com/research/strategic_security/acrobat/atstake_secure_dev_cycle.pdf, March 2004.

[2] Hart InterCivic, “Hart InterCivic Achieves Prestigious Information Security Certification,” http://www.hartintercivic.com/news/press_releases.asp?id=132, May 2004.

[3] Hart InterCivic, “Hart InterCivic Achieves Advanced Quality Certification,” http://www.hartintercivic.com/news/press_releases.asp?id=118, January 2004.

[4] B. Kaliski, “PKCS #5: Password Based Cryptography Specification,” RFC 2898, September 2000.

[5] H. Krawczyk, M. Bellare, and R. Canetti, “HMAC: Keyed-Hashing for Message Authentication,” RFC 2104, February 1997.

[6] Federal Information Processing Standards 140-1, “Security Requirements For Cryptographic Modules,” http://www.itl.nist.gov/fipspubs/fip140-1.htm, January 1994.

[7] T. Dierks and C. Allen, “The TLS Protocol,” RFC 2246, January 1999.

[8] Sybase, “Encryption Technologies in Adaptive Server Anywhere 8,” http://www.sybase.com/detail?id=1026265, October 2003.

About Symantec

Symantec is the global leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions. Headquartered in Cupertino, California, Symantec has operations in 35 countries. More information is available at www.symantec.com.

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 408 517 8000
1 800 721 3934
www.symantec.com