

Response for
California SOS Top-To-Bottom Review of Electronic Voting Systems

Prepared by:
Neil McClure, Chief Technology Officer
Hart InterCivic, Inc.
July 30, 2007

Thank you very much for the opportunity to present an oral response before this panel on behalf of Hart InterCivic. My name is Neil McClure and I am the Chief Technology officer for Hart InterCivic, Inc. and have been involved with the development of the Hart voting system since its inception.

The Hart voting system was certified by NASED in the summer of 2000, following a three-year development effort, our DRE system, the eSlate™ Electronic Voting System. The system was first used in live elections during the 2000 General Election. Since the November 2000 elections, the eSlate System is now installed in over 300 jurisdictions in 11 states including two of the largest counties in the U.S. that have purchased and successfully implemented electronic voting systems.

Since the initial introduction of the eSlate System, we have released new eSlate System applications to support storage and warehouse management of the equipment, distributed collection of cast vote records, candidate rotation, and multiple language support. These features, along with version upgrades for our other applications, represent the focus of our development resources over the first three years of the system's life and the priorities of this development had been determined by market and customer requirements. In 2003, it became clear to Hart InterCivic that the public was calling for greater security of electronic voting

systems however, there were no standards in place and some key policy decisions had not been acknowledged nor addressed. Nonetheless, Hart set out on an accelerated development and implementation effort for additional and enhanced security features, many which were a part of our original system architecture.

Despite a lack of guidance from within the election industry, Hart made a substantial investment in 2003 and embarked on a focused development effort to incorporate current information technology techniques using industry best practices to implement a high security architecture for the Hart voting system. To assist us in the achievement of this goal, we retained the services of a highly respected company in the systems security industry to develop a security architecture that was appropriate for the election industry. The company's name was @Stake (pronounced "At Stake"), and employed a number of well known and well respected security experts in the field of application security. Prior to the completion of our engagement, @Stake was purchased by Symantec and became a part of Symantec's professional services division.

Security is not a one-off effort, but an on-going commitment that is integrated into the business processes of a company. Hart InterCivic's structured software development environment and our ISO certified quality and facility security systems were an ideal foundation to integrate security practices within the organization. The @Stake representative spent one month on-site conducting interviews on the engineering staff, reviewing code and revising business processes while assisting us with the integration of a security culture for the Hart voting system. The first effort completed by the Hart/@Stake team was to define the framework of a threat model for an electronic voting system.

A threat model attempts to encompass as many factors as possible surrounding the operation of a system. A threat model is not just about technology but includes other system relevant elements, such as the operating environment, characteristics of typical users, functional requirements and motivation of attackers to name a few. The intent of the threat model is to define an environment that a system can be applied to for evaluation of potential vulnerabilities, mitigation, procedural requirements and other elements that collectively make up the security architecture. System security is not a yes or no question but must be evaluated in terms of probability and likelihoods, so without some form a threat model, there is no reference frame to perform a security assessment. Furthermore, implementation of security features can have a significant impact on system cost and usability. Higher security typically results in increased system cost, increased operating cost and increased complexity yielding reduced usability. The threat model helps to evaluate these trade-offs as the system designers attempt to find an acceptable and reasonable balance between these important aspects.

The Red Team explicitly states that no threat model was used in their testing. Without “making assumptions about compensating controls or procedural mitigation measures that the vendor, the Secretary of State, or individual counties may have adopted” the findings of the Red Team are not surprising.. This outcome is made further obvious by the fact that the Red Team was provided all the technical information, including the source code for the system. By ignoring the operating environment, the Red Team tested the system out of context so taking actions based solely on their findings would produce an unrealistic result, generating unintended consequences and potentially reducing the overall security of the system.

The Red Team findings also highlight where trade-offs were made in the face of system costs and usability. Several suggestions are made in the report that can raise the level of security but the real question is whether it is necessary. Is the cost-benefit ratio acceptable when applied to the probability of a successful attack? Cost is define here as both system cost and increased complexity in system operation.

This points to the need to develop and adopt a threat model so that vendors, election officials and public have common reference point for voting system security. Until a threat model or at least key aspects of the operational environment can be agreed to by the election industry, there will be no agreement on what is reasonable or acceptable security. These key aspects of the operational environment also need to be applied equally to all types of voting methods as well, including electronic, optical scan and paper ballots. Electronic voting systems have been typical held to an absolute standard, which is unreasonable while the vulnerabilities of other voting methods have been ignored. Without some agreed-to parameters surrounding security, the security debate will continue without resolution and all parties will suffer, including the public through their lack of confidence in the U.S. election process.

This is exemplified by an illustration from our security development effort. Since there was no standards or guidance provided by the election community, Hart needed to define the operating environment and establish some binding parameters for our security architecture. In order to make these decisions and have some form a reference, we analyzed what had been practiced and accepted for many years for paper ballot voting methods. Some fundamental results of that

analysis were that the polling place is supervised and trusted, the central election office is supervised and trusted while information in transit it is at risk. These are the same conditions that are, and have been used, for paper systems for years and are reasonable assumptions that can be stated for electronic systems. Naturally, when the Red Team testing is not subject to these conditions, perceived vulnerabilities will be discovered.

A case in point is the Attack Scenario 1, where additional Access Code were allegedly gained by a malicious voter using a surreptitious device. This attack requires distracting the poll worker for a sufficient amount of time to plug in a device to piece of election equipment, which sits in full view of the entire polling site, undetected. After being connected for thirty seconds, the malicious voter removes the device, again undetected. In the Hart voting system, Access Codes simply allows access to a particular ballot style at an eSlate device. Having an Access Code is identical to having a blank ballot so the same vulnerability exists for paper ballot systems. But an attack on the paper system requires the malicious voter to distract the poll worker for only a few seconds, enough time to steal additional ballots.

There are some inconsistencies in the Red Team report surrounding this attack scenario that we need to investigate with the Red Team. The JBC prints Access Codes for Early and Election modes and the Access codes are not active until the codes are printed. From the description in the report, we are unclear how the attack is successfully carried out once the Access Codes are surreptitiously collected, as the Access Codes are not active without printing.

The threat model takes into account technology, operating environment and human factors. To address the premise that information is at risk when in transit, we needed to use some form of cryptographic keys. When faced with the use of cryptographic keys, we were challenged with our customer's experience with the use of such technology or anything similar. Enough challenges exist with poll workers and we determined it would be an unacceptable situation to require poll workers to be responsible for a private key. The risk to the system when introducing a cryptographic key infrastructure is that the system can be rendered inoperable if the keys aren't managed properly. This is why we choose a symmetric key pair to authenticate information at the termination of transit. Symmetric keys are easier to manage and provide a reasonable level of security when evaluated within the threat model. Yes, our system can use public/private keys pairs – yes, it is stronger security. Is it a requirement? Is the increased complexity a trade-off that will be understood by the public when the key management gets out of synchronization? We don't have those answers, that is why we need to work together.

This raises an interesting issue worth consideration. The vendor community has been asked to develop increased security for electronic voting systems ahead of the establishment of standards or determination of other public policy issues. The issue of authentication verses encryption is an excellent example of a public policy that the vendors have been forced to answer without guidance from the election community. Is ballot data public information? If so, can it be obscured from public view? We have been asking these questions for several years with no definite answer from the election community and generally believe it will only get answered in a court room some day. In the absence of guidance from the election industry (and not wanting to be in court as part of the judicial test), we took the conservative position that ballot data is public

information and it can not be obscured from public view. Hence, our current system security is built on the premise that information can only be digitally signed and authenticated (visible) and not encrypted (obscured) for transfer between locations of election operations.

We understand that the Red Team was given a limited amount of time in which to test our system. Our preference would have been to provide some level of training on the use of the Hart voting system as we believe it would have saved time on the learning curve and made them aware of other features of the system. An example of this is in regards to SERVO, a system application that provides equipment management, warehouse functions, data back up for the voting devices (JBC, eSlate and eScan) and system verification. This latter function, system verification, was not understood by the Red Team.

One of the fundamental security elements of the Hart voting system is the distributed storage of Cast Vote Records in physically separate memory devices. The Hart voting system was designed such that there are three independent storage locations, creating triplicate originals. For the DRE, this includes the MBB, the JBC and eSlate and for our digital scanner it includes the MBB, the eScan unit and the paper ballots. It can be practically guaranteed that in the conduct of election that at least two of these storage mediums will be under separate custodial care and travel different pathways back to election headquarters. As mentioned above, SERVO will back up the data stored on the hardware devices, other than MBBs, that contain originals of the Cast Vote Records. SERVO also reconstructs each MBB from the data contained on the JBC, eSlate and the eScan to create duplicate original MBBs. These duplicate original MBBs can be read by Tally, the tabulation application, to produce a second set of original results that must match those

produced from the MBBs that were removed from the polling location. This is not a lengthy audit process and provides for system verification.

This functional capability nullifies Attack Scenario 2 contained in the report. Not only would an attacker need to modify all three triplicate originals for the attack to go undetected, but must modify all three identically.

It has been a difficult couple of years for the voting system vendors. Federal attention, new standards, requirements for additional voting methods, accelerated time frames, media focus and a whole new community of election experts has presented many new challenges, as it would for companies in any industry. Federal officials, State officials, public outcry, academic community and a thirsty media, all with different perspectives, objectives and agendas, all pointing at us, the vendors to solve their individual problems and yet we rarely get invited to the table to work out solutions. County officials understand the importance of working with the vendors to solve our election issues and there are some lessons to be learned from this working model. But being forced to work in a vacuum, we'll never solve issues faced by the election community.

We applaud your Red Team Review, however maybe not in the manner that it was conducted. Having spent a large sum of money on the development of a security infrastructure, we had nobody to review it that would yield a creditable outcome in the view of public. If Hart paid for the review, it would have tainted the results in the eyes of the vocal critics of electronic voting. We'd also like to point out that the attacks were defined as single point penetrations and were not conducted as part of an election cycle. This approach avoided many of the interlinked

parameters that are designed into the system to ensure integrity of the election process. For example, over-writing firmware is a detectable event if were to occur as part of an election cycle and the system operated in a manner where an election was actually in process.

Hart believes there is great value for our product to continue the kind of testing performed as part of this review. We'd like to suggest a possible approach for future such reviews and would be interested in helping to establish national program that would be satisfactory to all interested parties.

The biggest issue surrounding open inspection and review of our system by third parties is disclosure. We have a duty to our customers, and the public, to protect the integrity of our system, This includes being mindful of the possibility of malicious claims being made against our system that are not factual, defamatory or otherwise intended to prompt an alternate agenda (yes, it happens). We are interested in continually improving our system and an excellent source of input is from third-party independent reviewers. However, it is very difficult for us to agree to open inspection if we are not allowed the time to address any findings resulting from the inspection before they are made public. This is not in the best interest of our customers or the public. We'd like to suggest that we our open inspection protocol be based on a model developed by the Organization for Internet Safety (OIS), and detailed in their "Guidelines for Security Vulnerability Reporting and Response".

The process developed by the member organizations is multi-step process, where a vulnerability is identified, confirmed and then the clock starts counting down toward the disclosure date. Our

biggest concern about independent review is being provided an appropriate amount of time to address any issue discovered prior to public disclosure and agreeing to such a review without the opportunity to address any issues jeopardizes the integrity of our product, is a disservice to our customers and threatens public confidence. We understand the public disclosure is the leverage historically used to motivate a manufacturer to correct a problem, but it must be used responsibly to conduct open inspections in a cooperative manner.

There is also an issue of funding for the on-going conduct of open inspections. The vendors can't pay for the reviews as it will taint the outcome, state and counties don't have the budget for on-going financial support. Short of a federal appropriation, there is another possible source of funds. If we, the election community, developed a clear, concise, documented process for the on-going effort of independent, third-party open inspection of voting systems, we believe there are a number of philanthropic organizations whose charter is fund efforts for the public good and this program may well fit within their guidelines. This solution is worth pursuing but it requires the cooperation of all parties to work toward an acceptable process.

The current Red Team report, their findings and related observation requires additional review and discussions between the Team and our company. We have found several inconsistencies, alternate conclusions, omissions and a few errors in the report. It is critical these be addressed before any action is taken based on the report. It was also disappointing, and a disservice to the public, that none of the well-designed security aspects of the system were acknowledged in the report.

We look forward to continuing to work with the Red Team to address the unresolved open issues in the report. We also understand that this process is not complete and that, with the Red Team, it is necessary to work with the SOS to apply the operating environment so that responsible actions, if any, can be identified as a result of this review. This report is an important tool and must be used responsibly.

Thank you for your time.