CALTECH/MIT
VOTING TECHNOLOGY PROJECT

A multi-disciplinary, collaborative project of
the California Institute of Technology – Pasadena, California 91125 and
the Massachusetts Institute of Technology – Cambridge, Massachusetts 02139

Potential Threats to Statewide Voter Registration Systems (PREPARED FOR NIST "THREATS TO VOTING SYSTEMS" WORKSHOP)

R. MICHAEL ALVAREZ
CALTECH

Key words: ***voting systems threats, voting attacks***

VTP WORKING PAPER #40
October 2005

Potential Threats to Statewide Voter Registration Systems

Prepared for NIST "Threats to Voting Systems" Workshop

R. Michael Alvarez[1]
Caltech/MIT Voting Technology Project
October 6, 2005

The Help America Vote Act (HAVA), passed in 2002, requires that states implement "… a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and assigns a unique identifier to each legally registered voter in the State." Many states are now rushing to meet these requirements by January 1, 2006, and by the time of the November 2006 federal elections it is likely that virtually all states will have their statewide voter registration system operational.

These new statewide voter registration systems pose new risks for election administration, for a number of reasons. In most states voter registration processes and data prior to HAVA were primarily a local activity, controlled by a local jurisdiction, typically a county election official. Such decentralization meant that effectively in most states there multiple voter registration processes and systems, and that mounting a systematic attack on the voter registration process in most states implied attacking a variety of different voter registration systems, operating in many different locations, using different types of hardware and software, and so on. The post-HAVA reality in most states will be a single centralized system, and thus, a single place where attackers can focus their energies.

One critical problem regarding threats to statewide voter registration systems is that there are no existing standards for these databases, nor is there a corresponding testing and certification process to insure that the databases comply with these standards. Here I offer some analysis of potential threats to statewide voter registration systems, which might help fuel further analysis and discussion of the development of standards, testing and certification for HAVA-compliant statewide voter registration systems. I

[1] Thanks to Ben Adida, Doug Chapin, Jr., and Ron Rivest for very helpful comments.

conclude that one important way to mitigate some of these risks is through the development of standards, and that we clearly need close study of statewide voter registration systems as they are implemented in 2006.

The threats to statewide voter registration systems fall into four categories: authenticity of the registration file, secrecy of the registration file, integrity of the registration file, and potential voter registration system failures.[2] I discuss each in turn briefly below.

Authenticity of the registration file

A first threat to authenticity of the statewide voter registration file arises due to the centralization of the voter registration list. The new centralized statewide voter registration systems required by HAVA will involve some form of data transfer between the local election officials, who in many states will retain some responsibility for the voter registration data and who will need the voter registration data for a wide range election administration tasks. This means that these statewide systems will involve voter registration data being passed from state to localities, which implies new points of vulnerability --- during the data transmission process and in the local election office. So while there is a centralized statewide list, it is possible that attackers could isolate points of vulnerability in the transmission path, or in one of many local election offices and possibly access the state list via local vulnerabilities that might be outside the direct control of state election officials.

Second, the statewide voter lists will be interactive with other databases, as required by HAVA, in particular state Department of Motor Vehicle and Social Security Administration databases. Again, the statewide voter data will be transmitted for comparison to those lists, and thus again be potentially vulnerable in transmission and when in places potentially outside the state election official's control. There has also been much talk recently about potential interoperability of statewide voter registration lists between states, which depending upon how implemented again may open the door for new vulnerabilities not experienced in the former decentralized voter registration systems in place throughout most of the nation before the passage of HAVA.[3] Thus, these potential vulnerabilities imply that attackers could have access to voter registration information and the ability to alter that information or add entries to the file.

Secrecy of the registration file

There are potential privacy concerns with the new statewide voter registration lists. There will be a great deal of information in statewide voter lists, including voter addresses, birthdays, and contact information; voter history data; and other identifying

[2] Ben Adida suggested this useful framework.

[3] See, for example, the recent report by the Commission on Federal Election Reform, "Building Confidence in U.S. Elections" (http://www.american.edu/ia/cfer, last touched October 6, 2005).

information including either partial or complete social security numbers, drivers license numbers, or other state identification numbers. This data could be of great use for commercial purposes, or for other more nefarious purposes (identify theft, stalking, or other illegal purposes). On the other hand, we clearly desire that voter registration information, at least at some level, be available for use by academics, political organizations, and other observers of elections to allow for external scrutiny of these data to insure the databases have high integrity. Thus a balance must be struck, between the need to insure the privacy of the centralized statewide voter registration list (especially elements in that file that might be attractive for identity theft), and the need to allow public access to voter registration data for external analysis and review.

Integrity of the registration file

Prior to the development of statewide voter registration lists, responsibility for the voter registration files typically resided at the local level. With the state-centralized voter registration files under HAVA, it is unclear how responsibility for the integrity of the information in the files will be distributed between state and local election officials. If much of the responsibility for the information rests at the state level, which might make the job of verifying local registration status more difficult than if local officials controlled the information. If the responsibility is somehow shared between the state and local levels, the possibility arises that the voter registration data could be corrupted if file updating is not done correctly. These threats to the integrity of the new statewide voter registration lists need further examination, especially as new state systems are implemented.

Potential voter registration system failures

These threats run from unintentional system malfunctions to malicious attacks. For example, we have all experienced computer failures of various sorts in our experience; centralized statewide voter registration files should be implemented using systems that seek to minimize these failures and which will prevent data loss or corruption when system failures occur (this is an example where standards would be very helpful). At the other end of the spectrum would be a general "denial of service" attack on a statewide voter registration system, where the attacker would attempt to make it difficult or impossible for local election officials to access the statewide voter registration list immediately before, during, or after the election. There is thus need to study these risks and vulnerabilities and to insure that voter registration systems are robust and hardened.

Need for understanding the threats to statewide voter registration files

Unfortunately, unlike the technologies that are used for ballot casting and tabulation, the technologies that are being put in place to satisfy the HAVA requirements have not been developed necessarily consistently with any national or state standards, nor

with any necessary state or federal testing and certification process in place. While the current state and federal testing and certification process for ballot casting and tabulation technology is not perfect (in fact the federal Voluntary Voting System Guidelines are now under revision), the state and federal processes now in place do provide some level of assurance that certain standards have been met. We simply do not necessarily have that level of assurance for the new statewide voter registration systems that will be in place throughout the nation after January 1, 2006.

While this analysis of potential threats is by definition somewhat vague, because either the statewide files are not operational yet or they have not been operational long enough to determine in more precise detail their vulnerabilities, there is reason for analysis and study of attacks on statewide voter registration systems. The incentives to attack a statewide voter registration list are great:

- An attacker could, with access to the statewide list, engage in various types of election fraud. The attacker could register fictitious voters, and could attempt to cast ballots using the fictitious via by-mail absentee voting. This could be very difficult to detect, if done as part of a careful and sustained attack on the voter registration system.

- The attack could instead focus on disenfranchising registered voters, effectively mounting a "denial-of-service" attack on precinct voting. With access to the statewide voter list, the attacker could potentially remove voters from the list, move them to inactive status, alter their address information --- or do any number of things with the file to make it difficult or impossible for the voter to be allowed to cast a ballot when he or she tried to vote.

- The attack could be a "denial-of-service" attack on the voter registration system itself; if local election officials try to access voter registration data in the days immediately before or after an election, the attacker could mount a "denial-of-service" attack on the local officials computer system --- or the system where the statewide list is controlled. This could lead to significant disruption of early or absentee voting, election day activities, or pre- and post-election administration tasks. This risk could be mitigated somewhat by providing the voter registration data to the local officials before election day.

- A similar attack could focus on "electronic pollbooks", especially those that are used in precincts on election day. An attacker could mount a "denial-of-service" attack on a server that distributes voter registration data before the election to "electronic pollbooks", and thereby possibly cause a serious disruption in the election if voter registration data is not easily available in polling places.

- As noted earlier, the attack could focus on obtaining voter registration data for other purposes, either commercial data mining or identity theft (for two possible examples), especially if the attacker could access the database at levels where important data like drivers license or social security numbers are stored. But

> voter registration data, even without that sort of identifying information associated with it, could still be vulnerable to theft and inappropriate use, as there still are many purposes that voter registration data with names, addresses, birth dates, and other contact information could be used for.

These are just some of the potential threats to statewide voter registration lists. No doubt, as these files become operative and are used, other potential or real threats to these systems will arise. We clearly need more analysis of the security vulnerabilities of these systems as they are implemented in 2006 and beyond. We also need development of standards for these systems, and processes for testing and certification to those standards.