Security Seals on Voting Machines: A Case Study

ANDREW W. APPEL, Princeton University

Tamper-evident seals are used by many states' election officials on voting machines and ballot boxes, either to protect the computer and software from fraudulent modification or to protect paper ballots from fraudulent substitution or stuffing. Physical tamper-indicating seals can usually be easily defeated, given they way they are typically made and used; and the effectiveness of seals depends on the protocol for their application and inspection. The legitimacy of our elections may therefore depend on whether a particular state's use of seals is effective to prevent, deter, or detect election fraud. This paper is a case study of the use of seals on voting machines by the State of New Jersey. I conclude that New Jersey's protocols for the use of tamper-evident seals have been not at all effective. I conclude with a discussion of the more general problem of seals in democratic elections.

1. SEALS AND PROTOCOLS

Tamper-evident seals are widely used in elections, applied to ballot boxes, voting machine components, bags for transmittal of election results, and so on. What is the intended purpose of these seals, and are they effective in achieving that purpose?

Generally speaking, a seal is a device that is not difficult to remove, but is supposed to leave evidence of tampering if it is removed. Seals must have a physical design that will show some difference in appearance or behavior if they are removed and reapplied. Seals are generally serial-numbered (or otherwise marked with a unique identifier), so that if someone removes the seal and replaces it with a fresh one, the new one will have a different number.

The purpose of seals attached to a ballot box is to assure that ballots are not tampered with (or replaced) between the time that voters deposit them and the time they are counted. Seals attached to voting machines are meant to protect against many attack vectors, in particular to assure that the vote-counting software is not replaced (with fraudulent vote-miscounting software) between the time the vote-counting software is installed (e.g., when the machine is manufactured) and the time that election results are reported. Clearly, in the latter case the seals have a much more difficult job

to accomplish, since they must protect for a period of years during which many more people may have access to the voting machine.

Simply slapping seals on a device does not magically protect it. Physical seals in general can be defeated with simple techniques and at low cost [Johnston and Garcia 1997]. In addition the effectiveness of seals depends on having a protocol for their application and inspection [Johnston 1997]; otherwise, no one will notice if a seal has been replaced with a different one.

In order for seals to be effective, the seal user (e.g., election officials) must keep organized records of what serial number is applied to what device (e.g., ballot box, voting machine); the seal user must protect these records from tampering; and the seal user must inspect the seals at appropriate times (e.g., when a ballot box is opened for vote counting) to make sure that the right serial number is in place and that the seals have not been physically tampered with. Furthermore, if the inspection determines that tampering may have taken place, there must be a procedure to take appropriate action, otherwise the inspection is useless.

Seal inspection is not a trivial process: different seals show evidence of tampering in different ways, sometimes in quite subtle ways. Seal inspectors must therefore be trained, on each kind of seal they are inspecting, to know what to look for. For example, a pressure-sensitive adhesive (PSA) tape seal may show evidence that it has been removed and replaced, just by the fact that it no longer sticks as firmly as before to the substrate, so a good inspection requires the removal and replacement of the seal [Johnston 2006, p. 7]. A seal may be attacked by replacing it with a fresh seal whose serial number has been erased and reprinted with a laser-printer, so the inspection protocol requires a careful examination.

The choice of seals to effectively protect a given device requires expertise or experience; a tape seal that's effective on corrugated cardboard packaging may lift easily from the steel cabinet of a voting machine. A simple strap seal that's effective as a reminder to a (well intentioned) registered nurse not to open a bin of used syringes, may be ineffective against a (dishonest) attacker who means to steal an election for ideological or pecuniary reasons.

The process of reasoned selection, organization, recordkeeping, training, and oversight of seals forms *a seal use protocol*.[1] Designing, implementing, and operating a seal protocol is expensive and requires significant expertise and motivation. In this paper I will present my observations of New Jersey's use of seals in elections, and conclude that although New Jersey uses seals, there is no effective seal use protocol, nor do election officials have the required expertise and motivation. Consequently, seals in New Jersey elections are not effective for a useful purpose.

In the last two sections of the article I will explain why elections pose a particular challenge for seal use protocols: the "seal user" is not just election officials, the "seal user" who needs assurance of nontampering is really the public at large.

2. DIRECT-RECORDING ELECTRONIC VOTING MACHINES

By 2008, most counties in New Jersey were using Sequoia AVC Advantage voting machines. The AVC Advantage is a direct-recording electronic (DRE) computer. (See Figure 1.) That is, a voter indicates votes by pressing buttons on user-interface; the

---

[1]"Seal use protocols are the formal and informal procedures for choosing, procuring, transporting, storing, securing, assigning, installing, inspecting, removing, and destroying seals. Other components of a seal use protocol include procedures for securely keeping track of seal serial numbers, and the training provided to seal installers and inspectors. The procedures for how to inspect the object or container onto which seals are applied is another aspect of a seal use protocol. Seals and a tamper-detection program are no better than the seal use protocols that are in place." [Johnston 2010, Section 24].

Fig. 1.   AVC Advantage.

computer gives feedback by lighting corresponding lights; the computer stores those votes in an internal memory and in a removable cartridge. (Other models of DRE voting machine use a touch-screen instead of buttons and an LCD display instead of lights.) At the close of the polls, the machine prints out the election results for that precinct, and the cartridge is removed for tabulation (i.e., accumulation with other precincts).

DRE voting machines are very vulnerable to software-based fraud: if an attacker replaces the firmware (software) that determines how the computer interprets button-presses on the user interface, then he can make the machine fraudulently miscount votes according to an algorithm he determines. He can choose the algorithm so as to resist detection by blackbox testing, that is, not to cheat in circumstances other than in real elections. In real elections, of course, the privacy of the ballot prevents interviewing the voters to learn how they voted, so unlike (for example) bank ATMs there is no end-to-end way to audit a "paperless" DRE. (DREs have been proposed, and some produced, with a voter-verified paper audit trail (VVPAT), but the AVC Advantage studied here does not have a VVPAT.) All of this is well established as a matter of computer science, and is established for the AVC Advantage in particular by our own research [Appel et al. 2008, 2009].

During 2008 and 2009, in the course of a lawsuit over the constitutionality of using DREs to conduct elections in New Jersey, it became apparent that New Jersey intended to rely on tamper-evident seals as the main means of protection against software-based election fraud. I served as an expert witness in this lawsuit, and as such I had the opportunity to examine the seals that had been in use and the seals that were proposed (by the State) for use in the future. I also observed several aspects of the State's protocols for inspecting seals. In this article I will describe several successive seal regimes either used or proposed by the State. As I will show, each one that I examined is ineffective for the purpose of protection against software-based election fraud.

A physical security mechanism, such as a lock or a seal, provides protection if either (1) it significantly slows down unauthorized access to the protected item or (2) there is a significant likelihood that unauthorized access will later be detected. In the case of a DRE voting machine, there are many vulnerabilities that need to be protected, such as: computer chips or ports that permit replacement of the software; user-interface components; and vote data; "later detection" will be significantly more useful if it

Fig. 2.   Rear of AVC Advantage cabinet with door open (hinge at right).

occurs before election results are certified. The attack itself may come hours, days, months, or years before the election in question: once fraudulent software is installed, it may stay in place to affect election after election.

3. PHYSICAL ACCESS TO AVC ADVANTAGE ROMS

The AVC Advantage weights over 200 pounds, and unfolds to over 6 feet in height for elections. The rear cabinet door opens to reveal three sheet-metal enclosures (Figure 2). Inside the large sheet-metal enclosure at top left (17" wide by 14" high) is a circuit-board containing the "motherboard" computer; in the metal enclosure at lower left (17" wide by 8" high) are batteries to provide reserve power; in the small enclosure (6" by 9") is a second "daughterboard" computer. The side of the motherboard enclosure visible in Figure 2 is a sheet-metal circuit-board cover, held in place by 10 screws.

The motherboard computer (Figure 3) counts the votes and interprets voters' button-presses, so an important pathway to software-based election fraud is via replacement of the motherboard firmware [Appel et al. 2009]. The firmware of the AVC Advantage motherboard computer is located in three read-only memory (ROM) chips, mounted in sockets on the motherboard (Figure 4). The ROM chips are in a vintage-1980-standard 40-pin DIP package. By replacing just one of these chips, the attacker can make the voting machine fraudulently alter results before reporting them at the close of the polls. As we have reported [Appel et al. 2009, 2008] there are no significant digital or cryptographic protection or detection mechanisms for ROM replacement. In this article we concentrate on physical protections or tamper-evidence.

The simplest way to replace a ROM chip is to (1) unlock the cabinet door; (2) un-screw 10 screws that hold the circuit-board cover in place; (3) unhook (but not other-wise open) the daughterboard box to get it out of the way of the circuit-board cover; (4) remove the circuit-board cover; (5) pry out one ROM chip; (6) press into place a replacement ROM; (7) replace the circuit-board cover; (8) replace the daughterboard box on its hook; (9) replace the screws; (10) lock the door.

This process can be reliably and repeatedly done in under 7 minutes. Steps 1 and 10 are easily accomplished using the simplest of ordinary lock-picking tools. Steps 2 and 9 are done using an ordinary Phillips screwdriver. Steps 3, 4, 6, 7, and 9 require no tools at all. Step 5 requires a flat-blade screwdriver. Steps 2 and 9 take the majority of the time.

The cabinet door is secured by a cheap wafer-tumbler lock. Someone with no experience in lock-picking can easily be taught to pick this lock. In particular, I had no previous experience in picking locks. I received a few minutes of advice about lock-pick tools and instruction on their use from a Princeton University graduate

Fig. 3. Circuit-board cover removed from motherboard enclosure. Bottom center, panel for on/off knob. Top center (just to the right of "batteries"), a green strap seal remaining after the circuit-board cover has been moved past it (see discussion of seal regime #1). Slightly to the lower right of center, 1 configuration ROM and 3 program ROMs with white labels. At top left and top center of enclosure, one can see two of the 10 threaded holes for the screws that hold the circuit-board cover in place.

Fig. 4. Close-up of ROM chips (with white labels).

student. I found that lock-picking tools are easily available on the Internet. I bought a set of lock-picking tools for less than $40. With an hour or two of practice, I could reliably pick the lock of the AVC Advantage cabinet. After more practice, I could pick the lock in an average of 13 seconds (measured over 10 trials on two different voting machines). Therefore the cabinet-door lock does not provide substantial protection against ROM replacement.

The AVC Advantage was apparently designed by its manufacturer to accommodate two different kinds of seals, a circuit-board-cover seal and a results-cartridge seal.

Fig. 5.   Hole for circuit-board-cover seal.

Fig. 6.   Cartridge with strap seal.

These design elements are shown in Figures 5 and 6, and consist of holes in the circuit-board cover, circuit-board case, cartrige-holder, and cartridge.

A circuit-board-cover seal can secure the circuit-board cover to the circuit-board enclosure, in an attempt to protect the circuit-board from tampering. There is a $1/4$-inch diameter hole near the upper right corner of the circuit-board cover, and a corresponding hole in the enclosure. In principle, one can loop a strap seal through these two holes. The hole is visible in Figure 5, next to the label "DO NOT REMOVE".

The ROM chips are not the only devices underneath the circuit-board cover: there are also 4 AA batteries that provide battery backup for data in RAM memory on the motherboard. These batteries are visible at top center in Figure 3. Thus, the circuit-board cover must be removed not only for infrequent maintenance events, such as installing firmware upgrades by replacing ROM chips; every year or two the batteries must be replaced. In any seal protocol that uses the circuit-board-cover seal, it must be replaced at least when the batteries are replaced.

The Results Cartridge holds electronic ballot definitions (i.e., which candidates are running) and electronic vote data (i.e., how many votes they got). It is installed by election workers several days before the election; it is removed by pollworkers at the polling place right after the polls close. The cartridge is then transported to a central site for tabulation. The cartridge is about the size of a VCR tape; it has a half-inch by one-sixteenth-inch slot, and the metal cartridge-socket enclosure has a corresponding slot on each side, through which a strap seal can be looped. See Figure 6, with a

blue plastic strap seal looped through the slot at the top of the cartridge-holder and cartridge; the serial-numbered tag of the strap seal is partly visible at left.

4. A MODEL OF THE ATTACKER

A security protocol can be evaluated against an *attack model,* that is, a characterization of the motivation of the attacker, resources available to the attacker, how much time and effort the attacker is willing to spend, willingness of the attacker to use unlawful means, how much authorized access does the attacker to the protected material, and so on.

Motivation. In the case of an attack on a voting machine, the attacker's motivation is (presumably) to commit election fraud, to steal an election by altering vote totals inside the voting machine during the election. Historical studies show many instances of persons willing to commit election fraud by means such as ballot-stuffing, tampering with mechanical voting machines, coercing voters, altering vote totals after they are reported by the precincts, and so on. Another motivation for altering vote totals is not necessarily to win, but to get enough votes to qualify for matching funds, ballot status in future elections, and so on.

Resources. Candidates for the presidency of the United States routinely spend hundreds of millions of dollars to get elected; candidates for governor of New Jersey sometimes spend tens of millions. Independent groups not associated with the candidates routinely spend millions of dollars. Volunteers and party workers routinely devote hundreds of hours to political campaigns, even separately from the flow of money. Even candidates who are quite honest can sometimes attract supporters who are willing to use unethical or fraudulent means. If there is a limitation on resources, it is not in "How much is it worth to get elected?," but more in "How many people can be involved in an election fraud before word leaks out?"

Time. Election campaigns go on for months or years; attackers have substantial time to prepare.

Skills. In this article I am assuming that the attacker has no special knowledge about security seals. The attacker is assumed to know the general purpose of the seal as applied to the voting machine; to be resourceful enough to look for seal samples on the Internet; and to be moderately handy with simple workshop tools.

Access. Some insiders—election workers who are employees or contractors of county election officials—may routinely have access to AVC Advantage voting machines with the circuit-board cover removed. This is necessary approximately once per year to change the battery. Any seal protocol may be entirely useless in preventing these insiders from fraudulently replacing ROM chips. The same may be true of insiders working for the manufacturer of the voting machine.

Other insiders may have routine access to the warehouse where the voting machines are stored, and where they are prepared for each election, under circumstances where the circuit-board cover is in place. Such an insider may have access to 500 or more voting machines at the same place, for long periods of time. The seals (or other security measures) must protect against an insider who has such access.

Outsiders—ordinary members of the public—have access to voting machines when they are left in public places for several days before and after elections. Because AVC Advantage voting machines are big and heavy, it is impractical for election workers to transport them to the polling places on the day of the election. Instead (according to trial testimony by election officials) they are delivered by truck up to a week before

the election (it takes several days for a county to deliver hundreds of voting machines to hundreds of polling places), and they are picked up in the week after the election. Polling places include elementary school gymnasiums, university academic buildings, church basements, lobbies of municipal buildings, and volunteer firehouses. In many of these locations, a member of the public can easily gain access to unattended voting machines during weekdays and weekends before and/or after the election, at times when no other person is present [Felten 2006, 2008a, 2008b, 2009].

An alternate model for the attacker. The very seal protocol that is put in place to protect the votes and vote-counting software from vote-stealing attackers, becomes a target for a quite different form of attack: denial of service. An attacker who simply cuts, removes, or destroys tamper-indicating seals (without doing anything else) can attempt to call the legitimacy of the election into question. This is a fundamental problem with the use of seals to secure elections.

5. EVALUATION CRITERIA FOR SEAL PROTOCOLS

Unless all of the following criteria hold, serial-numbered tamper-evident seals cannot provide effective protection. (Even so, there is no guarantee that this list is exhaustive in a particular application; security is difficult!)

(1) The seal must be in place at times when the attacker has access to the container. (In this case, the container is the AVC Advantage motherboard enclosure.)
(2) The attacker cannot bypass the seal entirely, that is, in order to gain access to the protected item, the attacker must remove (or otherwise defeat) the seal.
(3) It must be difficult for the attacker to remove and replace the (same) seal without leaving evidence of tampering.
(4) It must be difficult for the attacker to remove the seal and replace it with a different one without leaving evidence of tampering. This is usually accomplished by
    (a) Manufacturing each seal with a serial number (or other unique identifier)
    (b) Refusing to manufacture the same serial number on two different seals
    (c) Designing the seal so that the erasure and rewriting of the serial number will leave evidence of tampering.
    Implicit in this criterion is that it must be difficult for the attacker to counterfeit a seal "from scratch," that is, manufacture close-enough looking seals. I am not sure how much experience with injection-molding of plastics one needs to be able to do this, but really that is rarely the point: in the vast majority of cases there are much easier attacks—either the simple removal and replacement of the original seal, or the purchase of extra (legitimate) seals and changing their serial number, or the purchase of extra seals to re-use some of their parts with the serial number of the original seal.
(5) The seal user (in this case, county election officials) must implement and execute a protocol for applying the seals, with organized records of which serial-numbered seal is attached to which serial-numbered container; and the records themselves must be protected from tampering.
(6) As part of this protocol, the seal user must regularly inspect the seal for evidence of tampering, and compare its serial-number with the records.
(7) The seal user must train the inspectors [Johnston 1997]
    (a) to understand the purpose of the inspection;
    (b) to detect the kinds of tampering that are plausible for each specific kind of seal used;
    (c) to understand what conditions in the seal are normal, caused by variation in manufacturing, or in application of the seal, or in wear and tear;

Fig. 7.   Unattended voting machines in public places the weekend before an election.

  (d) to perform the necessary recordkeeping;
  (e) to report anomalies.
(8) Finally, it must be the case that if anomalies are detected and reported, some appropriate action will be taken.

If any one of these conditions is missing, the seals are likely to be ineffective in detecting unauthorized access to the container. I will evaluate New Jersey's use of seals with respect to these criteria.

6. SEAL REGIME #1, 1990–2008

Between 1987 and 2005, one New Jersey county after another adopted the AVC Advantage voting machine; 19 out of 22 counties are now using it. The use of seals may have differed slightly from one county to another. I observed the seals in use, and the manner in which they were used, during the 2004 presidential election in Mercer County, by visiting the polling place and watching the procedures that pollworkers used in closing the polls; during this time I also observed the inside of the cabinet with the door open. In July 2008 I examined voting machines from Union County that had been used in the February 2008 presidential primary; in this examination I had full access to two voting machines for 30 days. In 2008–09 there was extensive deposition and trial testimony from several county and state election officials about the use of seals. Based on these observations and testimony I can describe how seals were used during that period.

No circuit-board-cover seal was used during this period. That is, the hole labeled "DO NOT REMOVE" had no seal; if there was one, it had been removed.

Based on representations from the manufacturer in court documents from 2004 and 2008, I conjecture that a circuit-board-cover seal may perhaps have been installed by the manufacturer; I further conjecture that no advice was given by the manufacturer to county election officials about the use, inspection, and replacement of this seal; I further conjecture that (if this seal was ever installed at all) it was removed during routine maintenance (battery replacement) and not replaced. Without conjecture, I observed that no such seal was present in 2004 or 2008 on Mercer County machines, or in 2008 on Union County machines.

Conclusion: No circuit-board-cover seal was used in Seal Regime #1.

Various different plastic strap seals were used during this period as Results Cartridge (RC) seals. The seal used by Mercer County in 2004 was a plastic band (i.e., the strap was not axially symmetric), perhaps similar to the one shown in Figure 9 (I did not take contemporaneous photographs and am relying on my memory). The (exact) seal used by Union County in February 2008 is a plastic strap seal shown in Figure 8.

The main purpose of the Results Cartridge seal is to secure the RC against removal (as shown in Figure 7). The RC seal is installed before the voting machines are transported to the polling place. After the close of the polls, typically at 8 p.m. on election
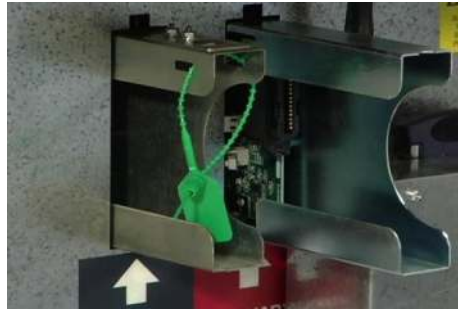
Fig. 8.   Plastic strap seal on Union County voting machine.

day, pollworkers are supposed to perform these steps: (1) Cut the seal with a scissors; (2) write down the seal's serial number on the precinct's election-results form; (3) sign the form; (4) place the seal, the form, and the cartridge in a special zippered pouch; (5) seal this pouch with a plastic tab seal; (6) transport this pouch to a central location, where the electronic data in the cartridge will be uploaded into a computer for tabulation.

Figure 8 shows that an RC seal was installed by Union County in an empty cartridge-slot on one of the two voting machines that they delivered to me in mid-2008 for examination (the other of the two machines had no seal at all). This use does not serve the purpose of detecting unauthorized removal of a cartridge. It could, in principle, detect the unauthorized insertion of a cartridge.

A secondary, perhaps unintended, purpose of the RC seal is to prevent removal of the circuit-board cover. Figure 8 shows that the circuit-board cover has two rectangular holes, with a sheet-metal cartridge holder poking through each one. (Each of the two white arrows on the machine's label points to one of these holes.) Even after the screws holding the circuit-board cover are removed, one might think that a strap seal through the two slots in the cartridge holder could prevent the circuit-board cover from sliding off of the cartridge holder.

Therefore, we can perform the exercise of evaluating the RC strap seal as a means of protecting the ROM chips on the circuit board.

(1) Is the seal in place at times when the attacker has access to the container?
   No. After pollworkers remove the seal on election night, the voting machine remains in a public place for several days until a truck comes to collect it. Replacement of ROM chips during this period will permit fraud in the *next* election(s).
   No. Insider attackers have access to voting machines in the warehouse between elections. At such times, the RC seal is not present.
   No. With respect to protecting the RC itself (as opposed to the circuit-board cover), there is a serious danger of tampering with the RC after it has been removed from the voting machine [Appel et al. 2009].
(2) Must one remove (or otherwise defeat) the seal to gain access to the protected item?
   No. The seal used by Union County is so flexible that I was able to remove the circuit-board cover without removing the seal. The same is true of the RC seal used by Mercer County in 2008. It is possible that a band-type seal (as in Figure 9) used by Mercer County in 2004 would prevent this.
(3) Is it difficult for the attacker to remove and replace the (same) seal without leaving evidence of tampering?

Fig. 9.   Band-type plastic strap seal.

No. The seals used by Union County are very easy to defeat in a few seconds, by poking a jeweler's screwdriver into the opening and thereby disengaging the teeth. Strap seals in general are easy to defeat with simple tools [Johnston and Garcia 1997]. The jeweler's screwdriver is not necessarily even the best or fastest way to defeat this seal; it is the one that occurred to the author, who was (at that time) entirely an amateur at defeating seals.

(4) Is it difficult for the attacker to remove the seal and replace it with a different one?

No. The seal was marked "INTAB 0000585". INTAB is the name of the manufacturer. Union County has approximately 800 voting machines. This very strongly suggests that Union County ordered a batch of seals from INTAB, and that INTAB started the serial numbers from 0000000 for each batch. Thus, there is evidence that INTAB manufactures seals with duplicate numbers, and that an attacker would be able to purchase a batch of seals from INTAB with the same serial numbers as all the seals used in Union County's 2008 Presidential primary election. In fact, many (though not all) seal manufacturers will sell seals with any desired range of serial numbers, regardless of the ranges ordered in the past and who ordered them.

(5) Did the seal user (county election officials) implement and execute a protocol for applying the seals, with organized records of which serial-numbered seal is attached to which serial-numbered container?

No. Subsequent deposition and trial testimony by New Jersey election officials showed that they had not taken significant steps in seal regimes #2, #3, and #4 to design a seal use protocol. I do not know how or if the election officials organize the records of seal serial numbers, but in a trial which ended up with significant focus on seal effectiveness, they were able to offer no testimony on this topic.

(6) Did the seal user inspect the seal for evidence of tampering, and compare its serial-number with the records?

No. Pollworkers are supposed to remove the seals and record their serial numbers. Two different kinds of evidence show that they do this only about half the time. First, a sample of 50 different paper results-reports from several counties in the February 2008 primary election show that in just 50% of the cases, a seal number is written down in the blank provided for that purpose. In the other half of the cases, the blank is left empty, or a voting-machine serial number is erroneously entered instead. Second, I sent a team of observers (including myself) to watch 5 different precincts perform their close-of-polls duties on the evening of the November 2008 Presidential election. About half of the precincts' pollworkers did not know what to do with the seals; in two precincts they left the seals on the floor. In my observation, both in 2004 and 2008 in Mercer County, the pollworkers did not closely examine the seal for evidence of tampering.

Precinct pollworkers are not given access to the records showing what seal number should be on each voting machine. If any comparison is done at all, it is by election workers who receive the forms on which the pollworkers wrote the serial number. The fact that about half the forms lack the serial number suggests that the comparison is not taken seriously.

(7) Are seal instructors trained (a) to understand the purpose of the inspection, (b, c) to understand the physical properties of the seal and modes of tampering, (d) to perform recordkeeping, (e) to report anomalies?

  No. Pollworkers are hired from among the general public to work 15 hours on election day for $200, with two hours of training before election day. This training covers how to run a polling place and conduct elections; it is not specific to seals. I have inspected the pollworker instruction manuals from three different counties; these manuals give no instruction in the purpose of the seals or in inspecting them for tampering.

(8) If anomalies are detected and reported, is some appropriate action taken?

  No. As observed, the rate of failure for inspectors to record any serial number at all is about 50%. This is likely consistent from year to year (though the only quantitative evidence we have is from February 2008 and November 2008), and yet, no corrective action in the seal-inspection process was made; no county clerk failed to certify an election based on missing seal numbers.

Thus, seal regime #1 is ineffective in almost every possible way. Even for the purpose of detecting tampering with the Results Cartridge (as opposed to the circuit-board cover), seal regime #1 is ineffective with respect to criteria 1, 3, 4, 6, 7, and 8.

7. SEAL REGIME #2, NOVEMBER 2008

In litigation over the constitutionality of using paperless DRE voting machines in New Jersey, on September 2, 2008, Plaintiffs delivered to the Court an expert report describing the vulnerability of the AVC Advantage to software-based election fraud. The report explained the ineffectiveness of seal regime #1, and added that merely adding more seals would not be a panacea, citing the work of Johnston [1997].

In a pretrial conference in September, the Court expressed concern and asked the Defendant (the State of New Jersey) what they were going to do to secure the voting machines for the November 2008 presidential election. The State responded that they would add more seals to secure the circuit-board cover. The State's solution, which I will call "seal regime #2", is described in October 2008 by the manufacturer of the voting machine, Sequoia Voting Systems [Sequoia 2008]. It is well summarized by Figure 10, taken from the document published on Sequoia's web site. This seal regime was in use during the November 2008 general election. In mid-November 2008, I obtained samples of these seals from the State and I was able to examine them.

The Results Cartridge seal is essentially the same as before. The three new seals are a cup seal, a wire, and a pressure-sensitive adhesive (PSA) seal. I will consider each in turn.

Cup seal, $3/4$-inch diameter, manufactured by American Casting and Manufacturing, with an engraved serial number. This kind of seal is sometimes called an "E-cup" seal; Sequoia here calls it a "security screw cap". The seal is used over one of the 10 screws that hold the circuit-board cover onto the circuit-board enclosure. The base (at left in Figure 11) is placed over a screw hole; the screw is screwed through the base, through the clearance hole in the circuit board cover, and into a threaded hole in the enclosure. Then the cap (at right in Figure 11) is pressed into the base, where it is gripped by radial spring prongs in the base.

The $3/4$-inch ACM cup seal has a serial number on the cap, but no serial number on the base. Therefore, any method of attack that destroys the base but leaves the cap undamaged will defeat this seal, as long as the attacker can obtain a supply of undamaged bases. I found that it is generally easy to obtain seal samples from American Casting and Manufacturing, and to purchase seals. ACM advertises its seals on

Fig. 10. Sequoia Voting Systems's proposed seal regime, September 2008.

Fig. 11. Cup seal (3/4 inch).

the Internet, including this cup seal. An attacker could easily obtain additional seals in quantity, at a price of about 75 cents each.

I found two methods of defeating this seal. The first method leaves both the seal and the base intact, but I did not perfect this method to the point where I consider it entirely reliable. The attacker cuts a rectangle of aluminum roof flashing (that is, thin sheet aluminum, though not nearly so thin as aluminum foil) about 2.3 inches by 5 inches. This is rolled into a tube, $3/4$ inches in diameter by 5 inches long. The tube fits in between the base and the cap, where it is hammered into place. The end of the tube deforms, gripping underneath the base. Then a twist of the wrist (often) removes the cap.

The second method is much simpler. The attacker inserts a thin flat-blade screw-driver vertically between the cap and the base, and then bends it down to a horizontal position. This flattens the base but does not damage the cap. After doing this several times around the perimeter of the base, it is easy to pry off the cap. If there is any damage at all to the cap, it is at the bottom of the cap in a place that will be invisible once the cap is replaced onto a new base. The attacker then removes the screw, which is straightforward. After the circuit-board cover is removed and then replaced, a fresh base is installed, and the original (serial-numbered) cap is pressed into place.

Roger Johnston has a third method that defeats this seal without needing any fresh parts (such as the replacement base that my attacks use), in just a few seconds. [Johnston 2010]

Wire rope lock seal. The wire rope lock seal has a metal component that looks like a padlock, and a long braided steel cable (Figure 12). The padlock is about one inch in height, 1/4 inch in thickness.

Fig. 12.   Wire cable seal (E. J. Brooks Co.).

In use on the AVC Advantage, the cable is threaded through a hole in the circuit board cover and one in the enclosure underneath, tying them together. Then the cable is pushed through a hole in the "padlock." Inside the padlock there are two steel balls and a spring, in a configuration that makes it "impossible" to pull the wire back out.

I found that this seal is quickly and easily defeated. The padlock body is soft metal. The base of the "padlock" is (probably the same) soft metal, about 1 millimeter thick, press-fitted into place. There are two holes, just larger than the wire diameter. When the seal is locked, the wire protrudes through one of these holes, and the other is empty. By threading a #4 wood screw though the empty hole, one can yank out the entire base with a pair of pliers. This leaves almost no marks at all on the base, and absolutely no marks at all on the serial-numbered padlock. When the base is removed, the internal components (balls and spring) can be removed. Then the cable easily comes out. Later, the padlock can be reassembled, and the base can be pressed into place. This leaves the cable lock seal as good as new, easily reinstalled. The first time I tried this on an actual voting machine, it took 50 seconds.

The cable lock seal can be used in either of two configurations.

In the first configuration, one pulls the cable through the padlock, and one leaves the end of the cable untrimmed. In this configuration, the attack as described above works straightforwardly.

In the second configuration, after the cable is pulled through the padlock, one cuts off the extra cable. This makes the end of the cable fray. If the attacker naively applies the attack as described above, the cable will fray all the way (throughout its length). I found various ways that the attacker can still defeat the seal. For example, while the padlock is in its disassembled state, I have found that I can twist the frayed cable end together enough to feed it through. The trick is to pull the wire through the different components of the padlock *before* reassembling the padlock.

Thus, the padlock seal is easy to remove and reinstall with simple tools, in either of these two configurations.

Johnston has an alternate attack on this seal [Johnston 2010] which is probably faster than mine.

Pressure-sensitive adhesive (PSA) tape seal. The PSA tape (Figure 13) is sold by E. J. Brooks Co. as "type KR" [Brooks 2008]. The tape is attached, at the left of the cabinet (when viewed from the rear) half on the outside cabinet of the AVC Advantage and

Fig. 13.   Pressure-sensitive adhesive tape. At left, as first installed; at right, when (mostly) peeled back and pressed down again.

half on the circuit-board cover. A second identical PSA seal attaches the circuit-board cover to the daughterboard box, and a third seal attaches the daughterboard cartridge to the daughterboard box. The third seal need not be touched when unhooking the daughterboard box and removing the circuit-board cover.

The tape is printed with the Great Seal of the State of New Jersey, at left, and a serial number, at right. The adhesive is designed to show tampering: if one peels off the seal, part of the adhesive remains on the sheet metal (and detaches from the plastic tape) to display the words "OPEN VOID OPEN VOID".

Although I had not had previous experience removing tamper-evident PSA tape seals, I had removed bumper stickers from my car using a heat gun. Based on this practical experience, I applied a heat gun to the tape seal. This softens the adhesive enough so that I can remove the seal (using a single-edge razor blade), and later re-place it, without any evidence of tampering. The letters "VOID" or "OPEN" do not appear. I found that 80 seconds application of heat was sufficient, followed by 40 seconds of carefully peeling off the tape. Thus, it took 2 minutes to remove the tape. Reinstalling the tape later is simple: one just presses it down. This takes about 2 seconds.

7.1. Evaluating Seal Regime #2

(1) Is the seal in place at times when the attacker has access to the container?
   No, for inside attackers whose job includes replacing the batteries on the mother-board.
   Yes, for outside attackers such as those in the polling place.
(2) Must one remove (or otherwise defeat) the seal to gain access to the protected item?
   Yes. The circuit-board cover cannot be removed without removing these seals.
   (No.) Roger Johnston's group found a way to replace the ROM chips without remov-ing the circuit-board cover. It is not clear whether an amateur attacker would find this method.
(3) Is it difficult for the attacker to remove and replace the (same) seal without leaving evidence of tampering?
   No. The methods I describe above allow the attacker to remove and replace these seals.
(4) Is it difficult for the attacker to remove the seal and replace it with a different one?
   Unknown. I did not attempt to determine how easy it would be to purchase seals from ACM and from Brooks with duplicate serial numbers, or to purchase seals with different serial numbers and change the numbers.
(5) Did the seal user (county election officials) implement and execute a protocol for ap-plying the seals, with organized records of which serial-numbered seal is attached to which serial-numbered container?

   No. Subsequent deposition and trial testimony by New Jersey election officials
       showed that they had not taken significant steps in seal regimes #2, #3, and #4
       to design a seal use protocol.
(6) Did the seal user inspect the seal for evidence of tampering, and compare its serial-
    number with the records?

   No. (see the item above)
(7) Are seal instructors trained (a) to understand the purpose of the inspection, (b, c)
    to understand the physical properties of the seal and modes of tampering, (d) to
    perform recordkeeping, (e) to report anomalies?

   No. Subsequent deposition and trial testimony showed no such action taken by
       election officials.
(8) If anomalies are detected and reported, is some appropriate action taken?

   Unknown.

In conclusion, seal regime #2 is ineffective on at least two critical fronts: the seals
themselves are easy for even amateurs to defeat, and there was no protocol for training
seal inspectors. The AVC Advantage voting machine is inherently insecure, and the
seals are applied as a kind of adhesive-tape placebo, that is, a band-aid, to give the
appearance of security.

8. SEAL REGIME #3, DECEMBER 2008

On December 1, 2008 Plaintiffs delivered to the Court (and to the State) an expert
report outlining the defeats of all four seals in seal regime #2. The State Defendant
informed the Court that they would abandon all four of those seals, and would adopt
new seals. I will call this seal regime #3. This seal regime was demonstrated to me at
the end of December, and samples were provided to me to examine. This seal regime
was never used in an election.

   The State proposed to use four new seals; I examined them in January 2009 and I
describe them here.

   Half-inch cup seal. This is similar in design to the $3/4$-inch cup seal used in seal regime
#2, except with a $1/2$-inch (or slightly smaller) diameter. It is also made by American
Casting and Manufacturing. Unlike the $3/4$-inch cup seal, the $1/2$-inch cup does not have
a serial number engraved, and therefore it is technically not a seal. ACM is unwilling
to sell it with engraved serial numbers. The State proposed to apply three cup "seals":
one at top left of the circuit-board cover, one at bottom right, and one at bottom center.
The bottom-right "seal" is in a deep recess under the daughterboard box. The bottom-
center "seal" attaches the circuit-board cover to a small panel that holds the on-off
knob and two other switches (Figure 14).

   Like the $3/4$-inch cup seal, the smaller one can also be defeated with a screwdriver.
But I also devised a faster and more reliable method, which required the preparation
of two special devices, which I made in my basement workshop in a few minutes using
a bench grinder (see Figure 15).

(a) An ordinary cold chisel (cost $5), ground to fit between the base and cap of the
    cup seal;
(b) A long-nose pliers (cost $10), ground to grip under the cap and pull it off.

   Using these tools, I can remove a cup "seal" in a matter of seconds, destroying the
base but leaving the cap unchanged. Since replacements are easily purchased from
AMC, the attacker can replace the base. Even if the cap had a serial number, the
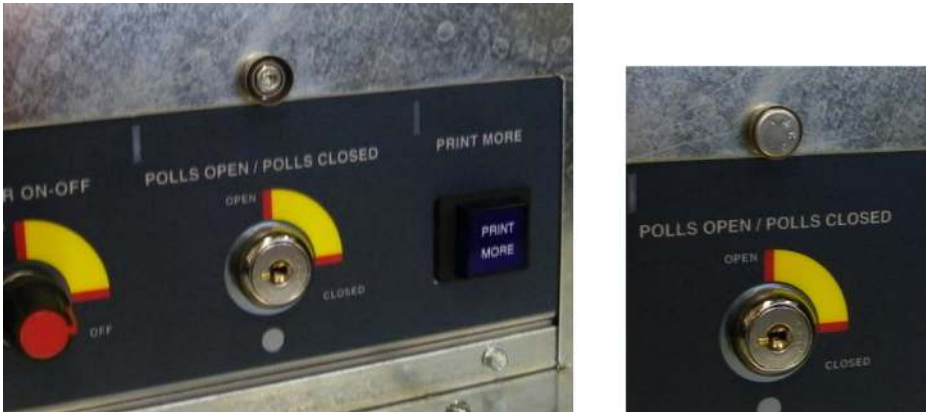attacker could replace the original cap.

Fig. 14.   Small cup "seal" installed on AVC Advantage voting machine. At left, base installed; at right, cap pressed into place.

Fig. 15.   (top) chisel ground to radius of cup; (bottom) pliers ground to grip and remove cap from base.

Fig. 16.   Small cup "seal". Top left, base; bottom left, cap; top right, base after removal; bottom right, cap after removal.

Figure 16 shows an example with slight evidence of tampering on the cap after removal. More practice remedies this; regrinding the pliers to better dig under the cap would help.

As with the ³/₄-inch cup seal, the smaller one is also vulnerable to Johnston's attack using a battery-powered drill [Opinion 2010, p. 133].

Fig. 17.   Catalog description of padlock seal [Brooks 2007].

Plastic "padlock" seal. This seal (Figure 17) is manufactured by E. J. Brooks; it has a body that is about 1.25" square and $1/4$" thick. Inside the plastic body of the padlock seal is a spring-steel grip that is supposed to permit the U-shaped steel shackle to be pushed in but not withdrawn. The shackle is to be inserted through the hole (marked DO NOT REMOVE) at the upper-right of the circuit-board cover, and through a corresponding hole in the circuit-board enclosure. This is supposed to prevent the circuit-board cover from being removed without tamper-evidence.

I have found that this seal is quickly and easily defeated. I drill two tiny holes (1/16" diameter) in the plastic housing. These holes are almost invisible. Any person who was checking these seals for tamper evidence, using a bar-code reader, would be unlikely to notice these holes unless they were specially trained to do so.

To drill the holes I use a special jig (Figure 18) that I built using a hacksaw, drill press, and bench grinder. After I clamp this onto the padlock, I drill through the two holes on the top of the jig using a Dremel tool with 1/16" drill bit. The drill penetrates the plastic, but stops short of the metal spring clip inside the padlock.

Then I remove the jig and apply the device shown in Figure 19. The two pins at the top fit into the two drilled holes, and apply pressure to the spring clip. The screw at top left (in the right-hand photo), when turned, moves the screw at left to push the padlock against the pins. This releases the spring clip, inside the padlock. Then the shackle can be pulled out. It is easy to reinstall the shackle later. The entire operation of drilling and releasing takes just a minute or two, on the actual voting machine.

The two drilled holes constitute slight evidence of tampering. However, they are almost invisible, and will not be noticed except by a trained eye paying careful attention. During my trial testimony, I gave two of these padlocks to the Court to examine. I explained that one of them had been tampered with, and the other had not. I had not yet explained the method of tampering. Judge Linda Feinberg examined the two padlocks (one of which had holes drilled in it), and said in court, "For the record, I can't see any difference." Her written opinion was, "After this was completed, the two holes were visible, albeit subtle with a little damage to the top of it." [Opinion 2010, p. 52]

The devices I constructed to defeat these seals did not require a great level of skill or expertise. I am just an amateur machinist, and I do not possess sophisticated machine tools. It took me about two days of design and shop-work to construct the devices that I have described for defeating seal regime #3 (including cup seal and padlock seal).

Johnston has other attacks on this padlock seal that produce substantially less evidence of tampering [Johnston 2010].
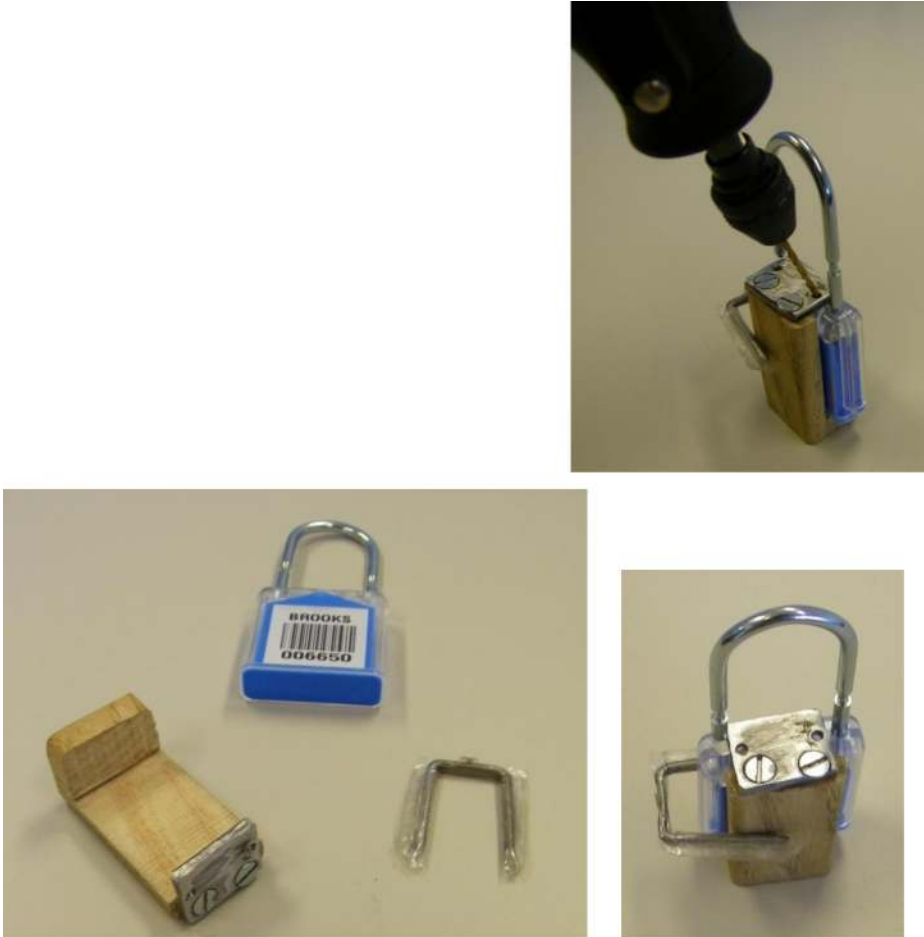
Fig. 18.   Drilling jig.

Pressure-sensitive adhesive (PSA) tape seal. The State proposed to use a different pressure-sensitive adhesive seal in place of the red tape seals used in regime #2. The seals would be applied roughly in the same position as in that regime (shown in Figure 10). The proposed seal is similar to type MRS2 in the E. J. Brooks catalog [Brooks 2008], as shown in Figure 20.

The MRS2 seal has quarter-circle incisions that are supposed to come apart if someone tries to remove the seal. Applying a heat gun to this seal causes the vinyl seal to shrink back from the incisions.

In addition, the State proposed to add an ultraviolet marking, possibly with a logo, to the MRS2 seal, visible only under ultraviolet light.

The attacker can defeat this seal by applying clear plastic packing tape over the seal. Applying the heat gun softens the adhesive of the seal, so that a razor blade can remove it from the sheet metal of the circuit-board cover. The clear plastic tape holds the white vinyl tape so that the vinyl does not shrink back from the incisions. After the circuit-board cover is replaced and the seal is pressed back down, the clear plastic tape can be removed, since the adhesive of the packing tape does not adhere very strongly to the vinyl.

Fig. 19.   Pressure device.

Fig. 20.   E. J. Brooks catalog description of MRS2 seal [Brooks 2008].

This method of removing the seal also works without the heat gun.

This defeat of the seal, with or without the heat gun, has no effect on the ultraviolet marking. The ultraviolet marking does not provide any significant additional security.

The State also proposed to place two of these Brooks seals across the ROM chips in their sockets on the motherboard. I found that the same technique—clear plastic packing tape plus razor blade—works to remove them from the ROMs, with or without the heat gun.

Johnston has other attacks on the Brooks MRS seals, which are probably comparable in effectiveness to my attacks [Johnston 2010].

Plastic strap seal. Seal regime #3 includes a different plastic strap seal used as a Results Cartridge seal. The seal is described by US Patent 6,981,725, "Pull seal with bi-directional locking arrangement", assigned to E. J. Brooks Co. (Figure 21). This is a polypropylene strap seal with an axially symmetric tail. The locking device contains a nylon insert that has two sets of teeth; depending on which way the tail is inserted through the tubular locking device, one set of teeth or the other will grip. The diameter of the locking mechanism (from point 102 to point 56 in Figure 20) is approximately one centimeter.

This seal is not as easy to defeat as the plastic strap seal used in regimes #1 and #2, but it is still not difficult. Simply poking with a jeweler's screwdriver will damage the teeth enough to permanently disengage them. Anyone who removes the seal without a specific inspection protocol will not notice the difference.

The attacker could improve the defeat by squirting an appropriate glue into the seal after reapplying it, assuming he could find an appropriate glue that adheres both
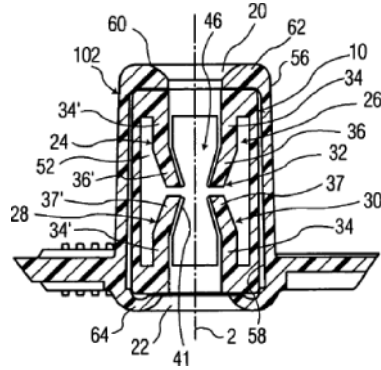
Fig. 21.   Diagram from U.S. Patent 6,981,725.

to nylon and polypropylene; or a space-filling glue that adheres just to polypropylene.
Even if the attacker can't distinguish plastics such as nylon and polypropylene by their
look and feel, the Brooks catalog [Brooks 2007] and patent (easily found with a search
engine) helpfully explain what the materials are.

It is probable that simple methods could be devised to pick this seal with less dam-
age to the nylon teeth, so that no glue would be required to reinstall the seal.

8.1. Evaluating Seal Regime #3

(1) Is the seal in place at times when the attacker has access to the container?

No, for inside attackers whose job includes replacing the batteries on the mother-
board. (However, the Brooks seals on the ROM chips themselves would be in
place in that situation.)

Yes, for outside attackers such as those in the polling place.

(2) Must one remove (or otherwise defeat) the seal to gain access to the protected item?

Yes. The circuit-board cover cannot be removed without removing these seals.

(3) Is it difficult for the attacker to remove and replace the (same) seal without leaving
evidence of tampering?

No. The methods I describe above allow the attacker to remove and replace these
seals. In the courtroom I demonstrated for the judge the complete removal and
replacement of all seals with no visible evidence of tampering; this took me less
than 45 minutes[2], including the 7 minutes that it would have taken to remove
and replace screws and ROMs if there were no seals present at all. At that time
I was relatively unpracticed on most of the seals, and entirely unpracticed at
the plastic strap seal. A practiced attacker would take substantially less time.
"To the court's untrained eye, most of the seals appeared unaltered with a few
showing minimal damage." [Opinion 2010, p. 52]

(4) Is it difficult for the attacker to remove the seal and replace it with a different one?

No. It is not particularly difficult to alter the serial numbers on the padlock and
PSA seals, so an attacker could purchase a supply of fresh seals and make the
numbers match.

---

[2]The Opinion, page 52, contains an error of fact by the judge: she writes that it took me two hours and forty
five minutes, when it fact it took less than 45 minutes. There were at least 8 people in the courtroom at the
time, including attorneys and the judge, so this error is a bit mystifying.

(5) Did the seal user (county election officials) implement and execute a protocol for applying the seals, with organized records of which serial-numbered seal is attached to which serial-numbered container?

No. Deposition and trial testimony by New Jersey election officials showed that they had not taken significant steps in seal regimes #2, #3, and #4 to design a seal use protocol.

(6) Did the seal user inspect the seal for evidence of tampering, and compare its serial-number with the records?

No. (see the item above)

(7) Are seal instructors trained (a) to understand the purpose of the inspection, (b,c) to understand the physical properties of the seal and modes of tampering, (d) to perform recordkeeping, (e) to report anomalies?

No. Deposition and trial testimony showed no such action taken by election officials. Given a complete lack of planning for training in seal inspection, the attacks described here that leave only slight evidence of tampering would likely not be detected.

(8) If anomalies are detected and reported, is some appropriate action taken?

Unknown.

In conclusion, seal regime #3 is ineffective on at least two critical fronts: the seals themselves are easy for even amateurs to defeat, and there was no protocol for training seal inspectors.

9. SEAL REGIME #4, MARCH 2009

On January 25, 2009, Plaintiffs delivered to the Court and to the State an expert report outlining the defeats of the seals in regime #3. In February 2009 the State informed the Court that they would be switching to a fourth seal regime, which they described to Plaintiffs' experts in March and April 2009.

I observed Mr. Robert F. Giles, Director of the New Jersey Division of Elections, demonstrate the application of seal regime #4 to an AVC Advantage voting machine, and I had the opportunity to examine samples of each seal in detail, and draw conclusions.

Cup seal. The half-inch AMC cup "seal" (which is not a seal because it does not have a serial number). The change from regime #3 is that superglue is squirted around the perimeter between the base and the cap.

Padlock seal. The Brooks plastic-and-steel padlock seal is used, as in regime #3, but superglue is squirted into the open hole before inserting the shackle into that hole.

Brooks sticky adhesive tape seal. A different pressure-sensitive adhesive tape seal is used. This is a clear plastic seal with most of it overprinted in solid white ink. On the reverse of the seal there is a very soft and sticky adhesive. Between the adhesive and the tape is a layer of red ink, which adheres to the adhesive at least as much as to the tape. Between the clear plastic and the red layer is a black serial number (in a box where there is no solid white ink layer). When the tape is peeled away from a sheet-metal surface, most of the adhesive remains on the sheet metal, including the serial number.

I observed Mr. Robert F. Giles, Director of the New Jersey Department of Elections, demonstrate the application of this seal. The seal comes as a large roll of tape. The adhesive is so soft and sticky, and adheres so poorly to the tape, that he ruined nine consecutive seals before finding a usable one. Even then, on both tapes that he

Fig. 22.   Sticky adhesive tape seal.

placed (one at left of the circuit-board cover, one attaching the circuit-board cover to the daughterboard) there are visible gaps in the adhesive that could be misconstrued as evidence of tampering; this could lead to false positives by a seal inspector. Also, in the process of applying the seal Mr. Giles got a visible spot of seal adhesive on the sheet metal (visible to the right of the seal in Figure 22), which could also be misconstrued as evidence of tampering.

Brooks MRS2 seal. In addition to that seal, a Brooks MRS2 vinyl tape seal (described earlier) is used on the ROM chips, as in Seal Regime #3.

Plaintiffs' expert witness Roger G. Johnston testified about these seals as the Court summarized in her opinion.

> Johnston's report outlines the type of seal, the method of attack, and the time to defeat each seal. He testified that most seal manufacturers provide free samples. Currently, the State intends to use six seals in nine locations. One seal, the Brooks padlock seal, is a device with a blue interior body that looks like a padlock; it has a shackle and is locked closed. It is a tamper-indicating seal. There is an interior serial number and barcode that provides a unique fingerprint. Johnston testified that a laser printer and some image processing is all one would need to produce a counterfeit seal and barcode.
>
> Johnston also examined the Brooks red adhesive label seal, two versions of the MRS2 adhesive label seal, a metal cup seal made by American Casting and Manufacturing, and a plastic strap seal made by Brooks. He described the MRS2 seals as: (1) sticky labels that, with careful handling, can be removed with solvents; and (2) low-tech attacks that require tools, materials and supplies that are widely available at a low cost. Anticipating that the State may add an ultraviolet mark, possibly a logo to the seal, Johnston testified that with inexpensive tools and supplies, available on the Internet, this is no different than counterfeiting a visible ink mark or logo." [Opinion 2010, p. 132]

In the courtroom during his testimony, Johnston demonstrated defeats of all of these seals for the Court.

The Brooks MRS2 seal is described in the Brooks catalog. It is a white vinyl seal with cutouts that are supposed to break if the seal is removed. I demonstrated for the Court one way of defeating this seal; Johnston demonstrated a different method.

The "Brooks red adhesive label seal" in Regime #4 is not the same seal as the red tape in Seal Regime #2. "While the seal has a remarkably good adhesive, it is very

difficult to apply the seal without damaging it, and Johnston noted that the serial number stays behind when the seal is removed. According to Johnston, when every single tape removed has visible damage, the inspection of the seal is compromised. Johnston devised an attack and demonstrated it in court." [Opinion 2010, p. 132]

The adhesive is so soft and sticky that it makes the seal impractical to use in any realistic seal use protocol. This seal must be removed and replaced whenever the circuit board cover is removed (such as for battery replacement). Once the tape is pulled off (by a voting-machine maintenance worker), the sticky adhesive remains on the sheet metal. If the residue is not removed, then when the machine is then resealed, the residue would mask evidence of tampering. But to remove the residue takes generous amounts of hazardous solvents. Johnston demonstrated the use of these solvents in the courtroom, and the judge's clerk suffered so much from the fumes that she had to be excused from the courtroom. Any facility in which these seals would have to be routinely removed and replaced would have to stock drums of hazardous chemicals, install ventilation systems, and train staff in safety procedures. Johnston testified that this would make the use of these seals impractical.

The Court's summary of Johnston's testimony about Seal Regime #4 is as follows.

> New Jersey is proposing to add six different kinds of seals in nine different locations to the voting machines. Johnston testified he has never witnessed this many seals applied to a system. At most, Johnston has seen three seals applied to high-level security applications such as nuclear safeguards. According to Johnston, there is recognition among security professionals that the effective use of a seal requires an extensive use protocol. Thus, it becomes impractical to have a large number of seals installed and inspected. He testified that the use of a large number of seals substantially decreases security, because attention cannot be focused for a very long time on any one of the seals, and it requires a great deal more complexity for these seal-use protocols and for training. [Opinion 2010, p. 138]

9.1. Evaluating Seal Regime #4

(1) Is the seal in place at times when the attacker has access to the container?
   Yes or No, similar to Regime #3.
(2) Must one remove (or otherwise defeat) the seal to gain access to the protected item?
   Yes.
(3) Is it difficult for the attacker to remove and replace the (same) seal without leaving evidence of tampering?
   No. Seal regime #4 increases the time needed, but does not markedly increase the difficulty.
(4) Is it difficult for the attacker to remove the seal and replace it with a different one? *No.* Johnston's testimony includes several different ways of altering serial numbers on new seals to make the match the old ones.
(5) Did the seal user (county election officials) implement and execute a protocol for applying the seals, with organized records of which serial-numbered seal is attached to which serial-numbered container?
   No. There is still no seal use protocol.
(6) Did the seal user inspect the seal for evidence of tampering, and compare its serial-number with the records?
   No. (see the previous item).

(7) Are seal instructors trained (a) to understand the purpose of the inspection, (b, c) to understand the physical properties of the seal and modes of tampering, (d) to perform recordkeeping, (e) to report anomalies?

No. (see the previous item).

(8) If anomalies are detected and reported, is some appropriate action taken?

Unknown.

10. SEAL REGIME #5, AUGUST 2009

Testimony of all witnesses concluded in May 2009. Three months after the conclusion of all witnesses' testimony, the State informed the press that they were switching to a fifth seal regime.

A press release dated August 11, 2009 begins as follows.

> FARMINGDALE, N.J., Aug. 11 /PRNewswire-FirstCall/ – Allied Security Innovations, Inc. (ASI) (OTCBulletinBoard: ADSV), reports that their tamper evident security products, manufactured and distributed by its wholly owned subsidiary, CGM-Applied Security Technologies, Inc. (CGM-AST) have been selected by Mr. Robert F. Giles, Director of the Department of Elections, to secure voting machines throughout the State of New Jersey [Prnewswire 2008].

However, as it became clear a year later that the State had not actually selected any seals, it's not at all clear that regime #5 actually existed.

11. SEAL REGIME #6, 2010

Judge Feinberg's lengthy opinion made it clear that she paid close attention to Roger Johnston's testimony about the importance of a rigorous seal use protocol. In her decision of February 1, 2010, she ordered the following.

> SEALS AND SEAL-USE PROTOCOLS (REQUIRED)
>
> For a system of tamper-evident seals to provide effective protection seals must be consistently installed, they must be truly tamper-evident, and they must be consistently inspected. While the new seals proposed by the State will provide enhanced security and protection against intruders, it is critical for the State to develop a seal protocol, in writing, and to provide appropriate training for individuals charged with seal inspection. Without a seal-use protocol, use of tamper-evident seals significantly reduces their effectiveness.
>
> The Court directs the State to develop a seal-use protocol. This shall include a training curriculum and standardized procedures for the recording of serial numbers and maintenance of appropriate serial number records [Opinion 2010, p. 190].

The Court imposed a deadline of July 6, 2010, for the State to have in place a seal use protocol. The State missed that deadline. The plaintiffs filed a motion to the Court, and on July 29 the State submitted a certification by the Director of Elections (Mr. Giles) that outlined a plan for choosing a vendor to train county workers in seal procedures. The state's submission did not include a seal use protocol, though it included what might be characterized as a "draft table of contents" of such a protocol. No particular seals were identified in that submission, and it appears that specific seals had not yet been chosen.

In a letter to the Court, the Plaintiffs pointed out that the State was still not in compliance with the court's order, and the State submitted another protocol on September

14th. By this time the State had chosen a vendor for training and advice on seals, but had not yet chosen any specific seals. In a hearing on September 23, 2010, the Court recognized that this was not a seal use protocol because the seals themselves had not been selected and identified, and gave the State ten days to submit a seal use protocol in compliance with the order.

The Court recognized that seals are ineffective without an effective seal-use protocol. But unfortunately, even the best possible seal use protocol cannot really protect elections on the Sequoia AVC Advantage voting machine. In some applications, seals can be effective: when they have to protect a container that was designed to be sealed, for a limited time, against attackers who have limited access, where there are adequate institutional incentives to report anomalies. None of these favorable conditions apply to the AVC Advantage. The seals are supposed to protect against access to ROM chips for a period of years, against insiders and outsiders, while the voting machines are in warehouses, in transit on commercial delivery services to polling places, and in storage at polling places. One breach of protection permits replacement of voting-machine ROMs with fraudulent firmware that can cheat in many elections. While the Court recognized that New Jersey's existing seal protocols are inadequate, I believe the Court is too optimistic about the ability of a better protocol to provide effective protection.

12. BYPASSING ALL THE SEALS

The analyses in Sections 6–9 have assumed that one must replace the ROM chips to make the AVC Advantage voting machine cheat in elections. This is not actually the case. Other authors have described and demonstrated attacks that bypass all the seals described above.

Voter-panel hack [Argonne Vulnerability Assessment Team 2009]. A segment of the front-side voter panel can be replaced with a fraudulently altered section. The alteration causes the button for candidate A to send a signal corresponding to a different button, e.g. the button for candidate B. The alteration also switches the corresponding LEDs that give feedback to the voter about which button has been pressed. The alteration is activated by a radio-control remote similar to a remote garage-door opener button; this activation can be done only after the polls open on election day, so that no anomalous behavior is noticed during preelection or postelection testing.

The front-side voter panel is not even in the main cabinet of the AVC Advantage, so it is completely unprotected by any of the seals discussed in this paper. Not one of the State's seal regimes would even begin to address this vulnerability.

Return-oriented programming [Checkoway et al. 2009]. The AVC Advantage can be made to run arbitrary algorithms by a software-based attack through the Auxiliary Cartridge port, which is unprotected by seals in any seal regime I have ever seen used or even proposed for this machine.

13. ON THE USE OF SEALS IN PROTECTING OPTICAL-SCAN BALLOTS

The informed consensus among most of those computer scientists who have studied the security issues with electronic voting machines is that it is impossible to be certain what software is loaded inside a voting machine, or what computer processor is actually interpreting that software. Thus, it is impossible to defend against software-based fraud simply by trying to secure the installation of software within a voting machine by physical means.

This is in part because of the danger of insider threats all the way back to the manufacturer of the voting machine. Even if it were possible to secure the software against any possible replacement or alteration after manufacture, there remains the

question of determining whether the authorized software was correctly installed in the first place (a separate issue from whether the authorized software itself contains flawed or fraudulent design). There is no good way of asking a computer (mediated by its software) to report on what software is loaded, as the reporting software itself may be fraudulent. One can try to replace the reporting software with reporting hardware, but then the same attacks are available on the reporting hardware.

There are some techniques using advanced cryptography that may, in the future, permit voting protocols that allow each individual voter to verify that his or her vote has been included in the final count, in such a way that the voter cannot reveal to others how he or she voted. However, such techniques have not yet been refined to the point where they are usable in national elections, or where their principles can be understood by most voters.

At the opposite extreme, some countries (such as France, Ireland, and Canada) vote entirely (or almost entirely) using paper ballots counted by hand. Furthermore, if this counting is done at the polling place immediately at the close of the polls, then no seals need be relied upon to secure the ballots between the polling place and the counting place. This may work well in political systems where there is only one contest on the ballot in each election, so that counting the ballots is simple enough to do reliably and accurately by hand. However, counting paper ballots by hand would not work well in most of the United States, where there are many contests on the ballot in a typical election.

Therefore most computer scientists recommend methods of voting that allow computers to count the vote, with random audits to verify that (with high statistical probability) the computers are not cheating. For this to work, there must be a record of each ballot that is not mediated by a computer that could possibly cheat in creating this record. One method that satisfies these criteria is to let the ballots be paper optical-scan forms: the voter blackens bubbles corresponding to her choice of candidates in a voting booth, and then feeds the paper ballot into a scanner/computer at the polling place. The voting machine retains the paper ballot in a ballot box. Immediately at the close of the polls, the computer can report the candidate totals for that precinct, and in addition there are paper ballots that can be audited in a hand count of randomly selected precincts.

This method of voting, known as "Precinct-Count Optical Scan" (PCOS) is used in the majority of the states in the United States.

There remains a security problem to solve: how is the integrity of the ballot box to be maintained between the close of the polls and the time of the audit? One method would be to perform the audit immediately, in the presence of the same witnesses (from both political parties and from the state) that have been (presumably) watching the ballot box all day. This might be the best approach, but it has disadvantages: those witnesses may have been working for 14 hours already running the election, and it requires the random selection of precincts to audit to be made by the time the polls close.

Therefore it is usually presumed that some combination of security seals with chain-of-custody arrangements will provide for the integrity of the paper ballots. Therefore, the considerations discussed elsewhere in this paper—regarding security seals and their associated protocols—are very relevant to optical-scan balloting.

14. ON THE USE OF SEALS IN ELECTIONS IN GENERAL

A seal use protocol can allow the seal user to gain some assurance that the sealed material has not been tampered with. But who is the seal user that needs this assurance? It is not just election officials: it is the citizenry.

Democratic elections present a uniquely difficult set of problems to be solved by a security protocol. In particular, the ballot box or voting machine contains votes that may

throw the government out of office. Therefore, it is not just the government—election officials—that need evidence that no tampering has occurred, it's the public and the candidates. The election officials (representing the government) have a conflict of interest; corrupt election officials may hire corrupt seal inspectors, or deliberately hire incompetent inspectors, or deliberately fail to train them. Even if the public officials who run the elections are not at all corrupt, the democratic process requires sufficient transparency that the public (and the losing candidates) can be convinced that the process was fair.

In the late 19th century, after widespread, pervasive, and long-lasting fraud by election officials, democracies such as Australia and the United States implemented election protocols in an attempt to solve this problem. The struggle to achieve fair elections lasted for decades and was hard-fought.

A typical 1890s protocol works as follows: At the beginning of election day, in the polling place, the ballot box is opened so that representatives of all political parties can see for themselves that it is empty (and does not contain hidden compartments). Then the ballot box is closed and sealed. The witnesses from all parties remain near the ballot box all day, so they can see that no one opens it and no one stuffs it. The box has a mechanism that rings a bell whenever a ballot is inserted, to alert the witnesses. At the close of the polls, the ballot box is opened, and the ballots are counted in the presence of witnesses.

In principle, then, there is no single person or entity that needs to be trusted: the parties watch each other.

Democratic elections pose difficult problems not just for security protocols in general, but for seal use protocols in particular. Consider the use of tamper-evident security seals in an election where a ballot box is to be protected by seals while it is transported and stored by election officials out of the sight of witnesses. A good protocol for the use of seals requires that seals be chosen with care and deliberation, and that inspectors have substantial and lengthy training on each kind of seal they are supposed to inspect. Without such training, it is all too easy for an attacker to remove and replace the seal without likelihood of detection.

Consider an audit or recount of a ballot box, days or weeks after an election. It reappears to the presence of witnesses from the political parties from its custody in the hands of election officials. The tamper evident seals are inspected and removed—but by whom?

If elections are to be conducted by the same principles of transparency established over a century ago, the rationale for the selection of particular security seals must be made transparent to the public, to the candidates, and to the political parties. Witnesses from the parties and from the public must be able to receive training on detection of tampering of those particular seals. There must be (the possibility) of public debate and discussion over the effectiveness of these physical security protocols.

It is not clear that this is practical. To my knowledge, such transparency has never been attempted. In examining any election system, whether based on DREs, optical-scan ballots, or hand-counted paper ballots, one should avoid the temptation to pretend that physical seals accomplish more than they actually do.

15. CONCLUSION

The state of New Jersey's protocols for applying tamper-evident seals in an attempt to secure its DRE voting machines have been completely ineffective. The primary reasons are that (1) as a matter of computer science, DRE voting machines cannot effectively be secured by physical seals; (2) the seals chosen by state election officials can be defeated even by amateurs, as can most physical seals in general; (3) state election officials had given no thought at all to protocols for applying seals, inspecting seals, and training

inspectors. Finally, the complex trust relationships in democratic elections pose very difficult problems for seal use protocols, for which no good solutions are yet known.

ACKNOWLEDGMENTS

REFERENCES

APPEL, A. W., GINSBURG, M., HURSTI, H., KERNIGHAN, B. W., RICHARDS, C. D., AND TAN, G. 2008. Insecurities and inaccuracies of the Sequoia AVC Advantage 9.00H DRE voting machine. http://citp.princeton.edu/voting/advantage.

APPEL, A. W., GINSBURG, M., HURSTI, H., KERNIGHAN, B. W., RICHARDS, C. D., TAN, G., AND VENETIS, P. 2009. The New Jersey voting-machine lawsuit and the AVC Advantage DRE voting machine. In *Proceedings of the Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE'09)*. USENIX Association.

ARGONNE VULNERABILITY ASSESSMENT TEAM. 2009. Electronic vote tampering. Video rep. APT #64451. Argonne National Laboratory.

BROOKS. 2007. Strap & Plastic Security Seals, E. J. Brooks Co. http://www.brooksseals.com/images/product/pdfs/Plastic_Strap_Seal_Brochure_04202007.pdf.

BROOKS. 2008. Tamper Indicative Labels, Tapes, and Anti-Counterfeit Products, E. J. Brooks Co. http://www.brooksseals.com/images/product/pdfs/Tapes_and_Labels_Brochure.pdf.

CHECKOWAY, S., FELDMAN, A. J., KANTOR, B., HALDERMAN, J. A., AND FELTEN, E. W. 2009. Can DREs provide long-lasting security? The case of return-oriented programming and the AVC Advantage. In *Proceedings of the Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE'09)*. USENIX Association.

JOHNSTON, R. G. 1997. The real deal on seals. *Security Manag. 41*, 93–100.

JOHNSTON, R. G. 2006. Some comments on choosing seals & on PSA label seals, slide presentation. In *Proceedings of the 7th Security Seals Symposium*. http://pearl1.lanl.gov/seals/images/choosing_seals.pdf.

JOHNSTON, R. G. 2010. Insecurity of New Jersey's seal protocols for voting machines. http://www.cs.princeton.edu/~appel/voting/Johnston-AnalysisOfNJSeals.pdf.

JOHNSTON, R. G. AND GARCIA, A. R. E. 1997. Vulnerability assessment of security seals. *J. Sec. Admin. 20*, 15–27.

FELTEN, E. W. 2006. Unattended voting machines already showing up. Freedom to Tinker. http://freedom-to-tinker.com/blog/felten/unattended-voting-machines-already-showing.

FELTEN, E. W. 2008a. Unattended voting machines, as usual. Freedom to Tinker. http://freedom-to-tinker.com/blog/felten/unattended-voting-machines-usual.

FELTEN, E. W. 2008b. NJ election day voting machine status. Freedom to Tinker. http://freedom-to-tinker.com/blog/felten/nj-election-day-voting-machine-status.

FELTEN, E. W. 2009. Trial testimony in Gusciora v. Corzine, 2/09.

OPINION. 2010. Superior Court of New Jersey, Opinion in Gusciora v. Corzine, Docket No. MER-L-2691-04, Decided by Linda Feinberg, A.J.S.C., 2/10. http://www.cs.princeton.edu/~appel/voting/election_case100201.pdf.

PRNEWSWIRE. 2009. New Jersey Division of Elections selects Allied Security Innovations products to secure voting machines, PR Newswire, 8/11. http://sev.prnewswire.com/homeland-security/20090811/NE5891011082009-1.html.

SEQUOIA. 2008. Response from Sequoia Voting Systems to the report of Andrew W. Appel, http://www.sequoiavote.com/documents/SVS_Response_to_Appel_report_NJ.pdf.