Comparative Risk Analysis: Using Technology to Make Military Members First Class Voters

Alec Yasinsac
School of Computer and Information Sciences
University or South Alabama
Mobile, Alabama 36688-0002

Abstract

In 2004, the Department of Defense cancelled a legislatively mandated Secure Electronic Registration and Voting Experiment (SERVE). Six years later, the SERVE Report continues to dominate Internet Voting security discussions. While little has changed regarding the SERVE Report's main theme, substantial progress is evident in voting system risk analysis, where threat likelihood and prospective impact offer comparative rigorous voting system risk analysis capability. In this paper, we present a risk-based comparison between the present voting paradigm for military voters (Vote By Mail or VBM) and Internet Voting. We describe and illustrate the threats to them head-to-head and then consider the prospective impact of replacing VBM with kiosk-based Internet Voting for the military community.

Keywords: UOCAVA, VBM, Military Voting

1. Introduction.

In an effort to extend E-Government into the elections realm, in 2003, the Department of Defense initiated the legislatively mandated Secure Electronic Registration and Voting Experiment (SERVE). After security concerns were expressed and widely trumpeted in the media, DoD cancelled SERVE. Six years later, the SERVE Report [1, 2] continues to dominate Internet Voting security discussions, while military members and their families (hereinafter referred to as military voters) continue to face daunting voting procedures [3], high voting error rates, and disproportionate disenfranchisement [4] relative even to other remote voters. These shortcomings are nothing new and have gone on for decades, either being accepted as "the best we can do" or with occasional, near-trivial improvements over the years [see, e.g. 5, 6].

While little has changed regarding the SERVE Report's main theme, substantial progress is evident in voting system risk analysis, where threat likelihood and potential impact offer rigorous voting system risk analysis capability [7, 8]. It is this development that offers a prospect for a near term solution to elevating military members and their families to "first class voter" status.

This paper presents three views of the plight of military voters. First, we identify the properties that signify the "first class voter" status that is sought for military voters. We then discuss the prospective, comparative impact that increasing effective participation and changing risk for military voters can have on electoral outcomes. Finally, we identify comparative factors between Vote By Mail[1] (VBM) and Internet Voting systems as they relate to support of Military Voters. We conclude with a summary and final thoughts.

2. First Class Voters

Military voters rarely complain about the hardships that they face, particularly those that are in harm's way. Many believe that military members should have their votes counted first and that the lack of a "squeak" is little justification for relegating them to ineffective voting support. The following principle drives this paper:

> It is imperative that every military voter be able to vote with comparable confidence and effort as any other voter in their jurisdiction.

In support of our troops, we cannot accept anything less than parity with those voters that they are protecting.

2.1. Introducing a First Class Status. Voting systems come in many shapes and sizes. The Precinct Count Optical Scan (PCOS) voting system paradigm is widely employed in U. S. elections. While other voting system paradigms may offer specialized advantages, the overall properties of PCOS are widely accepted as effectively meeting the needs of the voting public for speed, accuracy, and security. The following properties form a foundation for military "First Class Voters" status and are approximated in PCOS systems in local polling places:

1. Ballots cast & counted on election day
2. There is no delay between marking the ballot and casting the ballot
3. The voting system provides error checking to the voter
4. Voters can attain one or more replacement ballots without delay
5. Voters verify that their ballot was cast
6. Where state law allows, the voter may register and vote on election day

Collectively, these tenets identify first class voter status. Military voters should have the same electoral rights and privileges as any other voter in their voting district. To date, it has not been possible to provide first class status to military voters. Nonetheless, nothing less than first class status is satisfactory.

[1] While some suggest using registered or commercial carriers to deliver VBM ballots, no reasonable access or cost model has been offered to date. Thus, our analysis is based on first class mail delivery.

3. Risk Factors for Military Voters

In many senses, the U.S. military is a microcosm of American society that brings together young men and women from across the United States. Unfortunately, one place where there is little similarity between military and resident citizens is how they cast their ballot. We identify several unique challenges that military voters face in the following subsections.

Because military voters generally cannot vote in person, there is an inherent delay in their ability to acquire the proper blank ballot and confidently cast their marked ballot. For paper ballots Voted By Mail (VBM), the delay is determined by the postal service. Military mail takes between 12 and 18 days for a single envelop to travel in one direction [3]. For states that require that VBM ballots arrive on or before election day, military voters that use the military postal system must cast their ballot approximately three weeks before the election. For those that cast their ballot just two weeks out, they run a substantial risk that their ballot will not be counted because it will arrive at the LEO too late.

The vast majority of military voters are unable to go to their designated polling place on election day. VBM's pivotal security property is that marked ballots are out of the control of both the voter and elections officials once they enter the postal system. VBM systems do not support the fundamental voting system requirements of coercion resistance, vote-sale resistance, verifiable privacy, nor do they provide suitable artifacts that meet a reasonable standard for audit. In many cases, VBM voters are not able to detect that their VBM ballot was (or was not) delivered, and if they do discover that their ballot did not arrive, they are unable to attain and send a replacement ballot in time for it to be counted.

Additionally, remote voting procedures dictate that administrative procedures be rigorously followed to reduce the likelihood of voter fraud. While these procedures are necessary and clear to elections officials, they are often unknown or unintuitive to voters. A simple mistake such as including ballots from both a service member and their spouse in the same return envelope could invalidate both ballots. The most common such risk is signature problems [3].

We describe the administrative error risk in greater detail below.

Military members move frequently and often with little notice. Notifying elections officials of the new address is not a high priority and, due to frequent reassignments, the forwarding address may become invalid quickly. Mail forwarding service cannot satisfactorily meet military members' electoral needs.

Providing timely, accurate mail delivery within a single mail system is very difficult. Depending on interfaces between multiple, otherwise independent postal services substantially increases complexity. Elections officials have no control over the United States Postal Service or over mail systems run separately by the military services. None of these services routinely guarantee delivery or integrity and failure in any one of them, or in the interfaces between them, can cause service denial and disenfranchisement or loss of integrity.

An often overlooked remote voting challenge is that the voting experience for military voters is much less rich than for their polling place counterparts. For example, depending on the state from which they hail and other details of the situation, military and overseas voters may not be able to:

- Change their mind
- Employ routine voting error checks
- Fix mistakes
- Reliably track their ballot
- Stop in to vote on their way to work
- Register on election day
- Change residence close to election day

Think of the simplest of restrictions: e.g. if while marking their ballot a military voter errantly selects a candidate, the only means to make a correction may be to request a replacement ballot. In most cases, it is unlikely that a replacement ballot could arrive in time to complete the process.

Additionally, if after they mail their ballot they gain additional information about the candidates, e.g. by watching a televised debate, they are unlikely to be able to change their mind because of the inherent delivery delays.

A Note on Remote Voting Terminology

Terminology surrounding military voting is often vague or ambiguous because the voting method is sometimes used interchangeably with the reason for using that technique. Vote By Mail (VBM) is a remote voting method that relies on postal delivery of voted ballots. Remote voting (aka absentee voting), on the other hand, reflects the property of voters that are not physically present in their local polling place to cast their ballot.

VBM was introduced to support voters that had legitimate reasons for being unavailable to vote in their local precinct on election day. Military voters met that standard and military member voting support drove some VBM efforts.

Another confusing factor is that several states permissively allow voters to elect to cast their ballots via VBM without cause. This paradigm is alternatively termed permissive VBM, permissive absentee voting, no excuse VBM, on demand VBM, etc. These voters voluntarily cast their ballots using a remote voting system.

To further complicate terminology, Vote by Phone voting can be used as a remote voting system or within a local polling place to facilitate disabled voter access.

Finally, the state of Oregon's official voting approach for all voters is VBM, though there are many local ballot collection points that distinguish the Oregon VBM system from VBM used for remote voting.

4. Potential Attack Magnitude

A pivotal consideration in estimating the risk of attacks on voting applications is the size of the prospective target population. It is unlikely that an attacker would risk committing felony voting fraud in order to change a few votes with little likelihood of controlling a contest result. Moreover, if an attacker should choose to undertake a low-impact attack, the impact of a successful attack in that scenario is, by definition, low.

Conversely, as the opportunity for success rises in terms of the size of the potential population, the cost or risk to the prospective attacker is more easy to justify, of course depending on the value of the particular office in question, or of the opportunity to have a minimal, but potentially decisive, impact on a large number of contests. The latter is an interesting scenario that directly applies to the military voter population. That is, military voters do not dominate any voting districts, but they impact many, many different voting districts and the contests in those districts.

By this standard, the general risk level for voting applications for military & overseas voters is of low magnitude. If there are one million prospective military voters spread over more than 3,000 voting jurisdictions (and many more precincts), the opportunity for meaningful mischief is minimal.

The risk situation is even stronger for pilot projects with controlled, limited participation and exaggerated security procedures. The safest, most effective way to exercise and examine solutions for military & overseas voters is through government sponsored pilot projects.

5. Comparing Vote By Mail (VBM) and Electronic Voted Ballot Return (EVBR)

We now present and compare various scenarios and properties that reflect on the risk status of VBM and EVBR for military voters.

5.1. Denial of Service (DoS). One way to disrupt an election or to influence its outcome is to prevent targeted voters from being able to cast their ballots. The denial can target a voting constituency with predictable voting patterns to reduce an opponents vote count or the attacker can attempt to deny a large number of voters in an attempt to discredit the election or a particular contest.

Since denial of service occurs during the voting period, an attacker that is trying to influence a contest's outcome does not know how many votes they need to change. They only know that the more votes they influence, the greater their chance of success.

Vote By Mail inherently denies service to a substantial percentage of voters through lost mail, voter errors, and election official errors as we discuss below as non-malicious lost ballots. Targeted denial of service is less a problem than is lost VBM ballots.

Most VBM DoS attacks occur as Man in The Middle attacks, which we describe. Flooding is not generally a VBM DoS risk, since elections officials can add resources and extend deadlines to ensure that their ability to process many VBM ballots is not overwhelmed.

The most common, and most insidious DoS, is a Distributed Denial of Service attack that employs a large number of malware-infected hosts (called zombies) to conducted a synchronized flooding attack on a target host or network. The "flood" of messages is intended to overwhelm the target system and prevent them from accomplishing their intended purpose.

The risk to EVBR systems is that a malicious adversary may be able to prevent transmitted electronic ballots from arriving at the local elections office undamaged and in time to be counted.

For example, attackers could target either a dedicated voting station or the voting server in any Internet voting architecture.

DDoS attacks are becoming rare on the Internet today and some experts believe that DDoS is a solved problem where reasonable resources are applied to the network architecture. Nonetheless, if successfully employed, DDoS attacks could stifle voters trying to cast their ballot over the target network.

5.2. Vote Flipping

If a cast vote is somehow changed from its intended selection to a different selection, the vote is termed to have been flipped. Vote flipping is a particularly sinister form of vote fraud because one vote flipping instance causes twice the damage of one ballot stuffing incident.

For a variety of reasons, there is very little risk of vote flipping attacks with VBM ballots, the primary one being the difficulty of accessing original ballots, and doing so without detection. Most VBM ballots are mailed inside two sealed envelopes. Overcoming time and detection obstacles ensures that such an attack would demand significant planning and resources.

It is generally accepted that the greatest threat to any electronic voting system is the possibility of vote flipping caused by malicious software, or malware. Malware on a voting terminal or server may be able to alter votes without detection.

5.3. Lost Ballots (non-malicious). Optimally, every eligible voter that attempts to cast their ballot deserves to have their votes count. While registration errors, natural disasters, and other issues can cause ballots to not be counted, below we address risks that involve delivery of the blank ballot from the LOE to the voter or delivery of the voted ballot from the voter to the LOE.

5.3.1. Vote By Mail. While most understand the risk that VBM voters take of loosing a ballot in the mail. What is not as well understood is that a significant number of VBM ballots are lost or invalidated due to administrative error.

The mail system is designed to deliver a large volume of mail in a short time. It is not generally designed to track each item, so, as many of us have experienced ourselves, mailed items are routinely lost.

Because of its design that does not establish a rigorous chain of custody, any approach that employs regular mail for marked ballot delivery is not auditable. Mail can be lost with no ability to find lost items, or in some cases, even to detect their loss.

VBM ballots must make at least two passes across the postal system. This doubles the likelihood that VBM voters ballot will be lost in transit.

VBM procedures are inherently complex and error prone. We found little broadly applicable historical data on this topic, but in the 2008 election in Minnesota approximately 4.2% of all VBM ballots were rejected (approximately 12,000 of 288,000) due to procedural errors by voters. Common errors include failure to sign, signing in the wrong place, and improper packaging (e.g. husband and wife bundling two absentee ballots in the same envelope).

This 4.2% vote loss percentage does not include ballot marking errors that may have been prevented or corrected at the polling place, so the overall vote loss/error rate is likely substantially higher than 4.2%, while in-precinct ballot rejection is near zero, because voters can correct errors on the spot.

VBM denial of service is further exacerbated for military voters, where a study by the Pew Foundation found that a huge contrast between the percentage of requested absentee ballots returned among the general voting population (86%) and those from overseas/military voters (27%) [3].

Inherently complex VBM procedures are also difficult for temporary elections officials, even those who routinely process VBM ballots, to understand and follow. In Minnesota, at least 13% of the rejected absentee ballots were rejected in error. The actual percentage of erroneously rejected ballots may be higher, because there may still be erroneously rejected ballots that have not been detected. In one Minnesota county, after the senate contest was certified and reviewed, another, further review revealed that 20% (30 of 150) of the thrice-reviewed rejected ballots had been erroneously rejected by local elections officials "...who misunderstood state law or mishandled ballot applications".

Administering VBM ballots is an inherently complex process and significant errors are certain to occur.

5.3.2. Lost Electronically Voted Ballots. Electronic cast vote records, i.e. electronic records that reflect candidate selections per ballot, are the subject of much debate, particularly when there is no corresponding paper record. Electronic voting antagonists point out that the electronic records cannot be directly verified and subtle software errors, or software malice, can be very difficult to detect. Moreover, many electronic voting machines do not keep an electronic ballot, per se. Rather, they simply add the votes to the candidate totals when the ballots are cast. In either case, votes can be lost or altered, either accidently or intentionally, when they are counted, stored, or reported.

While there have been reports of lost electronic ballots [9], those numbers are dwarfed by the number of lost paper ballots that occur in every election. The greater risk posed by electronic voting systems is the potential for difficult to detect error malice, which is well documented [10, 11, 12, 13, 14, 15, et al.].

5.4. Vote Attribution. Voter privacy is commonly seen as the voters' ability to cast their ballot without anyone being able to know their selections, that is no one should be able to confidently attribute any specific vote to any specific voter. Beyond issues of personal privacy, vote attribution can allow a malicious party to coerce a voter into voting a certain way or can allow a voter to sell their vote.

All forms of unsupervised voting schemes are susceptible to vote attribution attacks.

VBM is inherently susceptible to violations of this minimal privacy interpretation since each VBM ballot must be bound to the voter's identity (i.e. each ballot must be attributed to the voter that cast that ballot) in order to ensure one-person, one-vote. Elections officials institute procedures to protect voter privacy, but the inherent vulnerability still exists for every VBM ballot. VBM does not protect against vote attribution and is susceptible to widespread fraud.

Electronic voting systems based on supervised voting kiosks can provide strong protection against voter attribution, because the electronic ballot and voter never need be bound together after the ballot is cast. On the other hand, any voting system that allows unsupervised voting (including voting from a private computer) is susceptible to vote attribution attacks. This is true for EVBR systems and they are all susceptible to widespread coercion and vote buying.

5.5. Man in the Middle (MitM) Attacks. MitM attacks involve a malicious party that is able to insert itself between two communicating parties without either principal being able to detect the MitM. While MitM can occur in any public communication, the most dangerous attacks occur at some common relay or aggregation point in the network, where the attacker can accomplish maximum access. Both VBM and EVBR are susceptible to MitM attacks.

A simple example of MitM attack against VBM ballots is a mailbox replacement attack, where an attacker that has detected that a VBM voter has placed their VBM ballot in the mailbox, replaces the VBM ballot with a different ballot that was previously prepared. More insidious attacks occur within the postal service, where many more ballots are accessible. There, ballots can be modified or destroyed by a malicious postal employee.

For military voters, another aggregation point is the relay through Army or Fleet Post Offices that handle all official mail for overseas military members. Malicious APO/FPO workers could destroy blank or voted ballots, could alter the ballots addresses for mis-delivery, or could open the envelope and alter targeted ballots.

Finally, VBM processing is often accomplished by temporary employees in LEO offices. These employees may have unfettered access to VBM ballots that cold allow them to destroy or alter the ballots.

A Man in the Middle (MitM) attack in an electronic network is a simple attack structure where a malicious or compromised computer acts like a customer to a service host and as a service host to a customer at the same time. It is a very effective attack approach and many MitM attacks are widespread on the Internet today.

Many MitM attack types exist that are relevant to EVBR systems. One straightforward MitM attack against EVBR systems would leverage phishing techniques to attract voters to connect to a false voting site. The server hosting the false voting site would act as the MitM. By using information harvested directly from the voter, the false voting server may be able to establish a session with the official site, and then replace the voter's choices with its own selections.

5.6. Post-Election Attacks. The canonical method of resolving close contests in U. S. elections is to conduct a recount [16]. Recently, some states have begun to require post-election audits to ensure widespread electoral confidence[2]. While post election processes can improve accuracy and integrity, they also introduce electoral risk. An election whose result is wrongly decided during the voting period is no worse than a result that is wrongly decided through a post election audit or recount process.

Some conjecture that it is easier and there is a greater likelihood of fraudulently influencing an electoral outcome after the voting period has ended, as is reflected in the following quote.

> Given access to the jurisdiction's voting records and knowing how many votes must be switched, an attacker could change the results of a close election by "retail" fraud. Essentially this means that knowing how many votes must be switched and the interval of time during which they can be switched, enhances the opportunity of attackers to compromise the election with a greater likelihood of success and a lesser likelihood of detection [16]..

The canonical scenario for vote fraud during an audit or recount is one where a large population of paper ballots are found or lost. Unfortunately, paper ballots are inherently difficult to manage/track. In the best case, they are single sheets with no identifying information on them. They are maintained in a place where there are invalid marked ballots, scores of unmarked ballots, and are managed by temporary employees that have had minimal training. VBM ballot arguments and contention have been central in virtually every contested election in recent memory.

While wholesale attacks pose a significant threat to large-scale electronic voting systems, changing electronic results after the results have been reported does not display similar risks. The challenge is that, even if malware is installed on the electronic devices, the possible result scenarios vary greatly and there is no channel for the software to receive instruction from a human coordinator.

---

[2] http://www.leginfo.ca.gov/cgi-bin/caasm/postquery?bill_number=ab_2023&sess=CUR&House=B

6. Auditability

There are three dominant voting system architectural approaches to achieving auditability:

1. Physical cast vote record audit
2. Process audit
3. Cryptographic algorithms

Paper ballot proponents objections to electronic voting systems that do not maintain a physical cast vote record as the ballot of record are founded on the fact that there is an absolute, theoretical upper bound on the possibility of systematically detecting malware. This is well known [17], is universally accepted in computer science, and much has been written about it.

However, that upper bound does not mean that systematic malware detection is impossible; to the contrary, we know that systematic malware detection is possible. There are many research results that confirm this [18, 19, 20, 21, et al.] and companies such as Norton, McAfee, and many others successfully conduct for-profit systematic malware detection.

The limit imposed by Thompson's theoretical upper bound is that we know that no systematic detection approach can be *guaranteed* to detect *all* malware. Moreover, we know by experience that even the best systematic detection approaches sometimes miss very important malware.

The real problem for voting systems is that the theoretical limit leaves the question of whether any detection system in an electronic ballot delivery scheme would detect malware that attacks an election as an open question. It goes without saying, this is a very bad thing.

On the other hand, VBM harbors precisely the same upper bound; that is, there is no systematic way to ensure end-to-end auditability for VBM.

As example, there is no viable approach to systematically determine that in any state where VBM comprises a significant % of the vote (Oregon, California, Florida, etc.), that no group (Political Action Committee, foreign entity, crime syndicate, etc.) that controls, say, 10% of the VBM vote by coercion and/or vote buying.

Additionally, because VBM ballots are not under signed custody control through their transmission from the time the voter marks the ballot until it is validated and cast by elections officials, there is no systematic guarantee of their end-to-end safety in transmission, even from administrative error, let alone from attack.

7. Conclusion

In this paper, we present comparative risk factors for two voting alternatives for military voters: Vote By Mail and Electronic Voted Ballot Return. We identify several elections scenarios and properties that are critical to effective electoral processes and compare the prospective process against one another.

The greatest risks to VBM for military voters are the time delay in ballot transmission (both directions) and in the risk of failed or errant administrative procedures by the VBM voter.

Conversely, the greatest risk for EVBR is the threat of wholesale attack accomplished via malware injection.

It is our opinion that the risks of VBM generally outweigh those of EVBR for military members. This is borne out by the documented impact of disenfranchisement of this voting constituency over the years and by consideration of the comparatively limited military voter population.

8. Acknowledgments

This work was supported in part through the U. S. Elections Assistance Commission under contract USEAC08C001. This acknowledgment does not constitute endorsement by the EAC.

9. Bibliography

[1] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)," January 20, 2004, http://www.servesecurityreport.org/

[2] David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, "Analyzing Internet Voting Security," Communications of the ACM, October 2004, Vol. 47, No. 10, pp. 59-64

[3] Pew Trusts, “No Time to Vote”, January 6, 2009, http://www.pewtrusts.org/news_room_detail.aspx?id=47924

[4] R. Michael Alvarez and Thad E. Hall, "Whose Absentee Votes are Counted?", Caltech/MIT Voting Technology Project, VTP WORKING PAPER #6, April 2004

[5] GAO 01-1026, "ELECTIONS: Voting Assistance to Military and Overseas Citizens Should Be Improved", September 2001

[6] GAO-06-1134T, "ELECTIONS: DOD Expands Voting Assistance to Military Absentee Voters, but Challenges Remain," Statement of Derek B. Stewart, Director, Defense Capabilities and Management, Thursday, September 28, 2006

[7] J. Harold Pardue and Alec Yasinsac, "Voting System Risk Assessment Using Threat Trees," accepted to the 2010 Conference on Information Systems Applied Research, October 28-31, 2010

[8] J. Harold Pardue, Alec Yasinsac, and Jeffrey P. Landry, "Towards Internet Voting Security: A Threat Tree for Risk Assessment," accepted to the International Conference on Risks and Security of Internet and Systems 2010, October 10-13, 2010

[9] Thadeus Greenson, "Software glitch yields inaccurate election results", The Times-Standard, 12/05/2008, http://www.times-standard.com/localnews/ci_11145349

[10] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, “Analysis of an Electronic Voting System”, IEEE Symposium on Security and Privacy, May 9-12, 2004, pp. 27-40.

[11] The Black Box Report, SECURITY ALERT: Critical Security Issues with Diebold Optical Scan Design, July 4, 2005.

[12] A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, “Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware, Final Report”, Security and Assurance in Information Technology Laboratory, Florida State University, February 23, 2007, http://election.dos.state.fl.us/pdf/FinalAudRepSAIT.pdf.

[13] “Software Review and Security Analysis for ES&S iVotronic Voting Machine Firmware.”, Florida State University Statement of Work, December 15, 2006, available on the web at http://election.dos.state.fl.us/pdf/FSUstatementWork.pdf

[14] Ryan Gardner, Alec Yasinsac, Matt Bishop, Tadayoshi, Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke, “Software Review and Security Analysis of the Diebold Voting

Machine Software", Final Report For the Florida Department of State, July 27, 2007, http://election.dos.state.fl.us/pdf/SAITreport.pdf

[15] California Secretary of State, UC Final Reports for the Top-to-Bottom Review (July-Aug. 2007); available at http://www.sos.ca.gov/elections/elections_vsr.htm.

[16] Alec Yasinsac and Matt Bishop, "The Dynamics of Counting and Recounting Votes", IEEE Security and Privacy Magazine, May-June 2008, Volume: 6, Issue: 3, pp. 22-29

[17] Ken Thompson. "Reflections On Trusting Trust" Communications of the ACM, 27(8):761–763, Aug. 1984. Also appears in ACM Turing Award Lectures: The First Twenty Years 1965-1985, Copyright 1987 by the ACM Press and Computers Under Attack: Intruders, Worms, and Viruses Copyright, Copyright 1990 by the ACM Press. http://www.acm.org/classics/sep95/

[18] Dorothy E. Denning, "An Intrusion-Detection Model", From 1986 IEEE Computer Society Symposium on Research in Security and Privacy, pp 118-31

[19] S. Hofmeyr, S. Forrest, and A. Somayaji, "Intrusion Detection using Sequences of System Calls", Journal of Computer Security, 6:151-180, 1998

[20] George C. Necula and Peter Lee, "Research on Proof-Carrying Code for Untrusted-Code Security," In Proceedings of the 1997 IEEE Symposium on Security and Privacy, Oakland, 1997

[21] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla. Pioneer: Verifying code integrity and enforcing untampered code execution on legacy systems. In SOSP '05: ACM Symposium on Operating Systems Principles, 2005.