World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 1, No. 7, 297-301, 2011

A Survey of Remote Internet Voting Vulnerabilities

Okediran O. O.
Department of Computer Science & Engineering,
Ladoke Akintola University of Technology,
P.M. B. 4000, Ogbomoso, Nigeria

Omidiora E. O.
Department of Computer Science & Engineering,
Ladoke Akintola University of Technology,
P.M. B. 4000, Ogbomoso, Nigeria

Olabiyisi S. O.
Department of Computer Science & Engineering,
Ladoke Akintola University of Technology,
P.M. B. 4000, Ogbomoso, Nigeria

Ganiyu R. A.
Department of Computer Science & Engineering
Ladoke Akintola University of Technology,
P. M. B. 4000, Ogbomoso. Nigeria

Abstract- Majority of the conventional voting techniques have been employed over the years in elections. Each of these techniques had attendant short comings. The existing conventional voting systems have been subjected to gross abuse and irregularities. Electronic voting which is emerging as an alternative to these conventional voting systems, though highly promising is not free of flaws; remote internet voting systems still suffer from many security problems which rely on the clients, the servers, and the network connections. Denial-of service attacks and viruses still belong to the most challenging security issues. In this paper we discuss the security issues associated with remote internet voting. In particular, we examine the feasibility of running national elections over the Internet. The focus of this paper is on the limitations of the current deployed infrastructure in terms of the security of the hosts and the Internet itself. We conclude that without appropriate security measures, internet based elections can be a challenge.

Keywords- Internet voting; Electronic voting; Penetration attacks; Denial of service; Digital divides.

I. INTRODUCTION

Elections and voting are fundamental to any consensus-based society. They are one of the most critical functions of democracy. Not only do they provide for the orderly transfer of power, but they also cement citizens' trust and confidence in government when they operate as expected. Naturally, the integrity of the election process is fundamental to the integrity of democracy itself. The election system must be sufficiently robust to withstand a variety of fraudulent behaviors and must be sufficiently transparent and comprehensible that voters and candidates can accept the results of an election [3].

In times past, different voting systems that were based on traditional paper ballots, mechanical devices, or electronic ballots were developed for elections [5, 6]. However, these voting systems have littered history with example of elections being manipulated in order to influence their outcome. Allegations of violence, intimidation, ballot stuffing, under-age and multiple voting, counting error, complicity of the security agencies and the absence or late arrival of election materials etc often trail elections conducted using these systems of voting [6].

As the computing, communicating, and cryptographic techniques progress rapidly, increasing emphasis has been placed on developing voting schemes that uses information and communications technology resources for providing more efficient voting services than conventional paper-based voting methods. Furthermore, the explosion of the Internet culture worldwide has caused many to question why we should not be able to cast our ballots in the same manner as we order books on the web-from home or from work. Voters see themselves as customers and expect government to make the business of voting more convenient. These and many other issues facilitated the interest and attention on internet voting (i-voting) in the last few years.

Internet voting (i-voting) is a specific case of remote electronic voting, whereby the vote takes place over the Internet such as via a web site or voting applet [1, 4]. Sometimes also used synonymously with Remote Electronic Voting. That usage is however deprecated and it will be used instead as a strict subset of remote electronic voting. The term internet voting encompasses a variety of concepts. Variants of i-voting include [2, 4]:

i. Poll Site Internet Voting: This refers to the casting of ballots at public sites where election officials control the voting platform (i.e., the hardware and software

used to vote and the physical environment of the voting place). In these kinds of systems, clients are intended to be accessed only at the poll site under the observation of election officials.

ii. Remote Internet voting refers to the casting of ballots at private sites (e.g., home, school, office) where the voter or a third party controls the voting client. Ideally, this type of open network system would enable voting from virtually anywhere at anytime; however, the concomitant risks are significant.

iii. Kiosk voting, offers an intermediate step between poll site and remote voting. In this model, voting terminals would be tamper-resistant and located in convenient places like malls, post offices, or schools, but remain under the control of election officials. Kiosk voting could be monitored by election officials, observers, or even cameras to address security and privacy concerns, and prevent coercion or other forms of intervention. The challenges and risks associated with kiosk voting are considerable, but more approachable than those associated with remote voting.

The main focus of this paper is remote internet voting.

II. PRIMARY INTERNET VOTING SYSTEM VULNERABILITIES

Internet-based voting systems are vulnerable to attack at three major points:

- the server
- the client, and
- the communications infrastructure.

Penetration attacks target the client or server directly whereas denial of service (DOS) attacks target and interrupt the communications link between the two. Each target and attack are discussed explicitly in the following subsections.

A. The Client and Server (Voting Platform)

Penetration attacks involve the use of a delivery mechanism to transport a malicious payload to the target host in the form of a Trojan horse or remote control program. Once executed, it can spy on ballots, prevent voters from casting ballots, or, even worse, modify the ballot according to its instructions. What makes the latter threat particularly insidious is that it can be accomplished without detection, and such security mechanisms as encryption and authentication (e.g., secure socket layer (SSL) and secure hypertext transport protocol (https)) are impotent against this kind of attack in that its target is below the level of abstraction at which those security protocols operate (e.g., the operating system or browser). Virus and intrusion detection software is also likely to be powerless against this threat because detection mechanisms generally look for known signatures of malicious programs or other signs of unauthorized activity. These stealth attacks generally emanate from unknown or modified programs, and alter system files to effectively "authorize" the changes made (after which they might disable further virus protection). The attacks could originate from anywhere in the world.

These malicious payloads can be delivered either through some input medium (e.g., floppy or CD-ROM drive), download, or e-mail; or by exploiting existing bugs and security flaws in such programs as Internet browsers. Activation need not be intentional (e.g., double clicking an icon), but can also occur by executing compromised code that users intentionally download from the Internet (e.g., device drivers, browser plug-ins, and applications) or unknowingly download (e.g., ActiveX controls associated with Web pages they visit). Even the simple viewing of a message in the preview screen of an e-mail client has, in some cases, proved sufficient to trigger execution of its attachment.

A Trojan horse, once delivered to its host and executed, might be activated at any time, either by remote control, by a timer mechanism, or through detecting certain events on the host (or a combination of all three). If such a program were to be widely distributed and then triggered on or about Election Day, many voters could be disenfranchised or have their votes modified. Attacks do not have to be confined to individual or random voters, but can be targeted on a particular demographic group. Remote control software introduces a similar concern in that the secrecy and integrity of the ballot may be compromised by those monitoring the host's activity.

In principle, poll site voting is much less susceptible than remote voting to such attacks.
The software on voting machines would be controlled and supervised by elections officials, and would be configured so as to prevent communication with any Internet host except the proper election servers. Election officials and vendors could configure voting clients so that voters and poll workers would be unable to reboot the machines or introduce any software other than the voting application. Careful monitoring of the system could reduce the risks even further. Opportunities for attack and insider fraud, however, would still exist, especially since voting jurisdictions may have difficulty getting the reliable technical support they need to administer their system properly.

B. The Communications Path

The communications path refers to the path between the voting client (the devices where the voter votes) and the server (where votes are tallied). For remote voting, this path must be "trusted" (secure) throughout the period during which votes are transmitted. This requires both an authenticated communications link between client and server, as well as the encryption of the data being transported to preserve confidentiality. In general, current cryptographic technologies, such as public key infrastructure, are sufficient for this latter purpose, assuming the standards required to run such

technologies are met. Maintaining an authenticated communications linkage, however, cannot be guaranteed.

Perhaps the most significant threat in this regard is a denial of service (DOS) attack, which involves the use of one or more computers to interrupt communications between a client and a server by flooding the target with more requests that it can handle. This action effectively prevents the target machine from communicating until such time as the attack stops. A refinement of this technique is referred to as distributed denial of service (DDOS) in which software programs called *daemons* are installed on many computers without the knowledge or consent of their owners (through the use of any of the delivery mechanisms referenced above), and used to perpetrate an attack. In this manner, an attacker can access the bandwidth of many computers to flood and overwhelm the intended target.

Currently, there is no way to prevent a determined DOS attack, or to stop one in progress without shutting down unrelated and legitimate communications-and even then it may take several hours of diagnosis and network administration time. While research is currently being conducted to find ways of limiting this threat, no solution has yet been identified. For poll site voting, these threats can be avoided by designing the voting clients with the capability to function even if communication between the precinct and the server is lost without warning and never re-established. Accordingly, these systems must, in effect, include the functionality of a DRE (direct recording electronic) system and be able to revert to DRE mode without losing a single vote. If the voting clients act as DRE machines, and use the Internet to transmit votes when it is available, then poll site voting systems are not vulnerable to denial of service attacks. Even if the path is totally corrupted, because the votes have been accumulated correctly in the vote clients, one can still recover after the fact from any communication problem. The philosophy is not to rely on the reliability or "security" of the communications link.

This approach is not feasible for remote voting systems because it is not practical or desirable for PCs to emulate all the characteristics of DRE systems. One does not want to store votes on remote PCs because of the possibilities it would create for vote selling or coercion. It is simply not reasonable to expect voters who were unable to connect to the server due to a DOS attack to physically carry their votes to the election office for tallying. Remote voting systems will also have to contend with an attack known as spoofing-luring unwitting voters to connect to an imposter site instead of the actual election server.

While technologies such as secure socket layer (SSL) and digital certificates are capable of distinguishing legitimate servers from malicious ones, it is infeasible to assume that all voters will have these protections functioning properly on their home or work computers, and, in any event, they cannot fully defend against all such attacks. Successful spoofing can result in the undetected loss of a vote should the user send his ballot to a fake voting site. Even worse, the imposter site can act as a "man-in-the-middle" between a voter and the real site, and change the vote. In short, this type of attack poses the same risk as a Trojan horse infiltration, and is much easier to carry out.

III SECONDARY INTERNET VOTING VULNERABILITIES

Secondary internet voting vulnerabilities are mainly through:

- Social engineering
- Digital divide

A Social Engineering

In respect of election and voting, social engineering is the term used to describe attacks that involve deceiving voters into compromising their security [7]. Literature survey in social sciences and humanities shows that many voters do not follow simple directions. It is surprising to learn that, for example, when instructed to circle a candidate's name, voters will often underline it. While computers would seem to offer the opportunity to provide an interface that is tightly controlled and thus less subject to error, this is counter to the typical experience most users have with computers. For non-computer scientists, computers are often intimidating and unfamiliar. User interfaces are often poor and create confusion, rather than simplifying processes [7].

A remote voting scheme will have some interface. The actual design of that interface is not the subject of this paper, but it is clear that there will be some interface. For the system to be secure, there must be some way for voters to know that they are communicating with the election server. The infrastructure does exist right now for computer security specialists, who are suspicious that they could be communicating with an imposter, to verify that their browser is communicating with a valid election server [7]. The SSL protocol and server side certificates can be used for this. While this process has its own risks and pitfalls, even if it is assumed to be flawless, it is unreasonable to assume that average internet users who want to vote on their computers can be expected to understand the concept of a server certificate, to verify the authenticity of the certificate, and to check the active cipher suites to ensure that strong encryption is used. In fact, most users would probably not distinguish between a page from an SSL connection to the legitimate server and a non-SSL page from a malicious server that had the exact same look as the real page.

There are several ways that an attacker could spoof the legitimate voting site. One way would be to send an e-mail message to a user telling that user to click on a link, which would then bring up the fake voting site. The adversary could then collect the user's credentials and in a sense, steal the vote. An attacker could also set up a connection to the legitimate

server and feed the user a fake web page, and act as a man in the middle, transferring information between the user and the web server, with all of the traffic under the attacker's control. This is probably enough to change a user's vote, regardless of how the application is implemented.

A more serious attack is possible by targeting the Internet's Domain Name Service (DNS). The DNS is used to maintain a mapping from IP addresses, which computers use to reference each other to domain names, which people use to reference computers. The DNS is known to be vulnerable to attacks, such as cache poisoning, which change the information available to hosts about the IP addresses of computers. The reason that this is serious is that a DNS cache poisoning attack, along with many other known attacks against DNS, could be used to direct a user to the wrong web server when the user types in the name of the election server in the browser. Thus, a user could follow the instructions for voting, and yet receive a page that looked exactly like what it is supposed to look like, but actually is entirely controlled by the adversary. Detailed instructions about checking certificate validity are not likely to be understood nor followed by a substantial number of users.

Another problem along these lines is that any computer under the control of an adversary can be made to simulate a valid connection to an election server, without actually connecting to anything. So, for example, a malicious librarian or cyber café operator could set up public computers that appear to accept votes, but actually do nothing with the votes. This could even work if the computers were not connected to the Internet, since no messages need to be sent or received to fool a user into believing that their vote was cast. Setting up such machines in districts known to vote a certain way could influence the outcome of an election.

B Digital Divides

Remote Internet voting brings along the potential for a "digital divide", which can occur in two ways. There is a digital divide between those who have home computers with Internet connections and those who do not. Second, there may be a digital divide between those who have faster access and those who have slower connections and hence lower quality access. People with higher incomes are more likely to be able to afford access. Furthermore, access is often less expensive and of higher quality in urban areas. Those with lower incomes and who live in rural areas are at a disadvantage. In the western world where tamper-resistant devices, such as smart cards are used for authentication, cryptographic keys can be generated and stored on these devices, and they can perform computations, such that proper credentials can be exchanged between a client and a voting server. However, there are some limitations to the utility of such devices. The first is that there is not a deployed base of smart card readers on peoples' personal computers. Any system that involves financial investment on the part of individuals in order to vote is unacceptable. Some people are more limited in their ability to spend, and it is unfair to decrease the likelihood that such people vote. It would, in effect, be a poll tax. This issue is also referred to as digital divide.

Even if everybody did have smart card readers on their computers, there are security concerns. The smart card does not interact directly with the election server. The communication goes through the computer. Malicious code installed on the computer could misuse the smart card. At the very least, the code could prevent the vote from actually being cast, while deceiving the user into believing that it was. At worst, it could change the vote. Other specialized devices, such as a cell phone with no general-purpose processor, equipped with a smart card, offer more promise of solving the technical security problems. However, they introduce even greater digital divide issues. In addition, the user interface issues, which are fundamental to a fair election, are much more difficult. This is due to the more limited displays and input devices. Finally, while computers offer some hope of improving the accessibility of voting for the disabled, specialized devices are even more limiting in that respect.

Therefore, the extension of Internet voting has the potential to create divides with respect to many socio-economic variables, namely income, education, gender, geography and race and ethnicity. These potential divides could be problematic for participation and representation.

IV CONCLUSION

The motivation for i-voting is multi-fold; accuracy and speed of results, substantially reduced overall cost and minimization of population transfers are some of the most profound benefits. So far, due to security, technological concerns and limitations, as well as due to the digital divides, i-voting have been proposed only as an alternative solution to traditional election process. Many internet-based approaches have often been criticized for reasonable and sometimes proven security concerns due to the fact that an open inter-network is always vulnerable to hacker attacks. For example in the USA, the Secure Electronic Registration and Voting Experiment (SERVE), designed by Accenture on a USD22 million contract for expatriates participation in the US presidential elections of November 2004, was shelved by the Department of Defense of the US because of "justified security concerns". Therefore, without appropriate security measures, electronic based elections can be a challenge. In contrary to internet base voting methods, we suggest that solutions based on Virtual Private Networks (VPNs) and reinforced with strong security layers pose as more viable approaches to implement reliable and strongly secure e-elections.

REFERENCES

[1] Buchsbaum T. M., (2004), "E-voting: International Developments and Lessons Learnt". Proceedings of Workshop on Electronic Voting in Europe –Technology, Law, Politics and Society, Austria, at www.subs.emis.de/LNI/Proceedings/Proceedings47/ Proceeding.GI.47-4.pdf.

[2] Boniface M., (2008), "A Secure Internet-Based Voting System for Low ICT Resourced Countries". Master of Information Technology Thesis, Department of Information Technology, Makerere University, Uganda.

[3] Kohno T., Stubblefield A., Rubin A. and Wallach D. S., (2003),"Analysis of an Electronic Voting System" Johns Hopkins University Information Security Institute Technical Report TR-2003-19.

[4] Magi T., (2007)," Practical Security Analysis of E-Voting Systems", Master of Information Technology Thesis, Department of Informatics, Tallinn, University of Technology, Estonia.

[5] Malkawi M., Khasawneh M. and Al-Jarrah O., (2009), "Modeling and Simulation of a Robust E-voting System", Communications of the IBIMA, Volume 8, 2009. ISSN: 1943-7765.

[6] Okediran O. O., Omidiora E. O., Olabiyisi S. O., Ganiyu R. A. and Alo O. O., (2011), " A Framework for a Multifaceted Electronic Voting System". International Journal of Applied Science, Philadelphia, USA, vol. 1 No .4 pp 135-142.

[7] Rubin A., "Security Considerations for Remote Electronic Voting over the Internet" Available at http://avirubin.com/e-voting.security.html

AUTHORS PROFILE

Okediran O. O. is a lecturer in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He graduated with B.Tech. Computer Engineering and M. Tech. Computer Science from Ladoke Akintola University of Technology, Ogbomoso, Nigeria, in 2002 and 2008 respectively. He has almost finished his Ph.D Computer Science in the same Institution. He has published in reputable journals. His research interests include: Computational optimization, e-commerce, biometrics-based algorithms and their applications to e-voting systems. He belongs to the following professional bodies: Full member, Computer Professionals (Registration) Council of Nigeria (MCPN); Registered Engineer, Council for the Regulation of Engineering in Nigeria (COREN).

Omidiora E. O. is currently a lecturer in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He graduated with B.Sc. Computer Engineering (1991) from Obafemi Awolowo University, Ile-Ife, Nigeria. He bagged M.Sc. Computer Science from University of Lagos, Nigeria (1998) and Ph.D Computer Science from Ladoke Akintola University of Technology (2006). He has published in reputable journals and learned conferences. His research interests include: The study of Biometric Systems, Computational Complexity measures and Soft Computing. He belongs to the following professional bodies: Full Member, Computer Professionals (Registration) Council of Nigeria; Corporate Member, Nigeria Society of Engineers; Register Engineer, COREN etc.

Olabiyisi S. O. received B. Tech., M. Tech and Ph.D degrees in Mathematics from Ladoke Akintola University of Technology, Ogbomoso, Nigeria, in 1999, 2002 and 2006 respectively. He also received M.Sc. degree in Computer Science from University of Ibadan, Ibadan, Nigeria in 2003. He is a lecturer in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He has published in reputable journals and learned conferences. Dr Olabiyisi is a member of Computer Professional (Registration) Council of Nigeria (CPN). His research interests are in Computational Mathematics, Computational Complexity, Theoretical Computer Science, Simulation and Performance Evaluation.

Ganiyu R. A. is a lecturer in the Department of Computer Science and Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He graduated with B.Tech. Computer Engineering and M. Tech. Computer Science from Ladoke Akintola University of Technology, Ogbomoso, Nigeria, in 2002 and 2008 respectively. He has almost finished his Ph.D Computer Science in the same Institution. He has published in reputable journals. His research interests include: Dynamic Programming and their Applications; Theoretical Computer Science; Modelling and Simulation of Concurrent Systems Using Petri Nets (Low level and High level). He belongs to the following professional bodies: Full member, Computer Professionals (Registration) Council of Nigeria (MCPN); Registered Engineer, Council for the Regulation of Engineering in Nigeria (COREN).