Imperial Journal of Interdisciplinary Research (IJIR)
Vol-3, Issue-2, 2017
ISSN: 2454-1362, http://www.onlinejournal.in

Comparative Analysis of Electronic Voting and Internet Voting Framework

Abubakar Idris Usman[1] & Dr.Sundresan Perumal [2]
[1] Limkokwing University of Creative technology Malaysia
[2] Senior Lecturer Universiti Sains Islam Malaysia,.

Abstract*: India and Estonia are the countries that widely adopt the transformation of voting using technologies. And today more than 90% of its populace cast their ballot in a digital way. In this paper, we will analyze some key requirement of Indian e-voting system and Estonian Internet voting system from polling security, confidentiality, verification, sincerity, and integrity and ballot secrecy. The voting machines are also vulnerable to threats which will impact the outcome of the national election — including Credential Theft, malwares, Botnets, insider attack, Denial of service attack, state-sponsored attacks and Remote Intrusion —We have found that the design of the machines or systems have loopholes, limitations and procedures on the architecture that might endanger the integrity of the elections. We demonstrate how such an attacker can the target server's election or voting client that damage the legitimacy of the system. Our research shows that, from experience to practical obstacles in today's world of the Internet and electronic voting, lessons learned from Estonia and India, the adaptation of E and I voting in other countries will be re-consider of using such systems, as they are vulnerable to security threats.. .*

1. Introduction

As the world we live metamorphose from old age to digital age, we witness transformation and advance in technology on how to conduct election in a transparent manner. Elections allow the people to choose whom will represent them and express their opinion on how they will be governed [1]. E-voting and I-voting is something wonderful to be enable to use computers to cast and count vote securely, to be enable to vote over the internet with all the convinces the technology brings perhaps we could reduce cost and increase participation. At the same time e-voting raise one of the most difficult challenges in the field of computer security and is a motivating problems for advances of all kind of cryptography, system construction and usability. E-voting and I-voting is a core security problem because of its usual requirements. We need two things in securing e-voting and I-voting systems above all and one of them is integrity and by integrity means the outcome of the election match the voters intend, and the election votes are counted as cast, Secondly Ballot Secrecy which mean no body can figure out how you voted. The design of the voting framework must adopt the protocol that will protects the integrity, generality, equality, freedom, secrecy and fairness of the election process to become feasible [2].

The reason why these are more complicated than other problems that we routinely solve are banking online, making purchases in electronic commerce. We also have this requirement for ballot secrecy, that the secret ballot is one of the most important technological advances in the history of election technology. The secret ballot is the thing that protects you for been coercive to voting a certain way and to protect you from selling your ballot, the secret ballot says no one can figure out how you voted and even if you try to prove it to them how you voted. This is what we want to protect people of been coercive and prevent them from selling their ballot.

The reason e-voting and I-voting has been a difficult problem, it's largely of these two properties integrity and ballot secrecy. Things we do to increase integrity as we do in e-commerce, to send people a receipt or a bank statement or to do accounting where money goes in / out and is total. These things are very much difficult or impossible to implement when we want to maintain a secret ballot and a strong framework at the same time, we want to preserve integrity so we need very different mechanism's to achieve e-voting and I-voting system that provides these critical properties and these does not stop people and countries from building electronic voting or internet voting systems.4.

2. Related works

In this section we briefly describe related work dealing with e-voting and I-voting. Other countries have largely adopted e-voting such as India which has the world's biggest trial in electronic voting to date which more than 800 million participated in the last general elections and Estonia moves not just traditional voting but move from e-voting to internet voting. We will analyze some key requirement from polling security, confidentiality, verification,

sincerity, integrity and ballot secrecy in India and Estonia electoral system.

2.1 India E-voting Elections

India is the world largest democracy in the last parliamentary elections, almost 800 million vote casted. The scale of the challenges official faced in implementation of an election system is just emends. Those official are election commission of India, the highest election authority in the country. The election authority conduct e-voting in a period of 30 years and have some vulnerabilities. In India, the electronic voting machine use an embedded system design, special purpose, and no removable storage devices. The electronic voting used in India differ from e-voting design and architecture in Europe and America. All those machine are vulnerable but in different ways. There are 1.4 million machine used to count the votes and they have some few constraints which are the cost of the machines, with so many machines in used. E.g. the cost of the voting machines in Europe and America cost thousands of dollars while in India its cost 200 dollars per each, the second constraint is power supply which means most of the rural places are not connected to the power grid or have power shortages and the votes are counted in place which do not have electricity and there environmental conditions which are very hash in parts of India which this machines are used. There are extreme in temperature from freeze cold in the Himalayas to very hot tropics. But to build reliable systems which are to be used year after year. These are concern among the threats of electronic voting machines i.e. these machine are store on non-climate control warehouses, they have to be transported for miles and miles over unpaved roads, some of them have to be taken by boats into places in the jungle that are only accessible in the river. It's a challenge the election authority faced

Election commission of India implement tamper proof e-voting machine in their elections and to ensure it's free and fair. The description of E-voting process:

- Each machine has the names and symbols of the candidates Structure of Government in a constituency.
- One Electronic Voting Machine (EVM) can accommodate maximum of 16 candidates. But if the number exceeds 16, then more than one EVM may be used.
- If the number of candidates is very large, ballot papers may be used.
- The voter has to press the appropriate button to vote for the candidate of his/her choice. As soon as the button is pressed, the machine is automatically switched off. Then comes the turn of the next voter.

The machine is easy to operate, and with this the use of ballot paper and ballot boxes is done away with. When the machine is used, the counting of votes becomes more convenient and faster.

2.2 Estonia I-voting Elections

Internet voting, or 'I-voting', is a system that allows voters to cast their ballots from remote location such as offices, homes, cafes or locals residing abroad to cast their ballot using internet-based connection, anywhere in the world [13].

I-voting was first introduced during the October 2005, 2009 and 2013 local government election, In March 2007, 2011 and 2015 the parliamentary elections and In June 2009 and 2014 the European Parliament elections, when more than 9 thousand to 176 329 thousand voters from 2005 to 2015 election vote using their home computers via the Internet (it makes 2 % from 2005 to 31 % in 2015 election). Today, I-voting with has been utilized in 8 consecutive elections in Estonia which makes it a pride among European nations [14]. Perhaps electronic voting framework has been used in the America, Asian and Europe, much concern has been rise due to costs, unforeseen problems and time consuming, Estonian type of voting framework solution is secure , elegant and simple [13]. Although the Estonia internet voting committee maintain that the system is reliable and secure as voting in a traditional way but its security has been question and criticized within the country and abroad and has not been subjected to security analysis [12]. I-voting description process that take place [14]:

- A secure computer with an internet connection and either ID card or mobile ID
- Once online, make sure you have reliable anti-virus installed and the latest digital signature software
- Download the voter's application from the website valimised.ee
- Start it, and identify yourself using ID card or mobile ID.
- Then choose the candidate you want to vote for and confirm your vote by using digital signature.
- The application will prompt you with detailed instruction on how to do that.
- The votes that have been cast electronically are encrypted and move through the internet to the central server, immediately after voting each voter can check whether the vote has reach the server in the form it was cast using a smart device application.
- The encrypted votes can be opened only with the security key of the national electoral committee which has been divided between the committee members.
- The whole committee must come together for the opening of the votes.
- Internet voting takes place under the constant watchful eye of the observer who monitors that everything is secure

- The encrypted votes are opened and counted only after all personal data have been separated from the votes.

3. Observation

3.1 Security Threat in internet-voting system

Internet voting is even more header than voting on a standalone machine in a polling station. Internet voting have a problem that a voter is using his own machine outside a protective environment and there might be vulnerable to be coerce, to having there username and password stolen, to imposter claiming to be real voting system, to malware on the machines and to Botnet that have already affected large number of machines compromising the outcome of the election and it's not only that, the server too, has not be able to resist Denial of Service, election take place for a fix period and you can stay our systems or servers are down, we postpone the elections until next month, then you have to worried about insider attack on the server about remote intrusion and even about more advance attack like state-sponsored attack. At the same time internet voting system are more difficult to study.

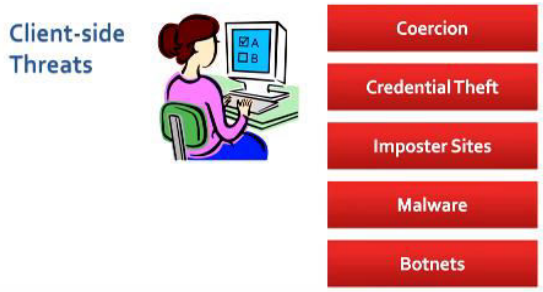

Figure 1: Client-side attack

The client side voting software is a standalone application or web browsers that enable communication with the voting server. [10]

Coercion: when a voter is been force by another party to act in a dubious way by the use of force, threats, intimidation or some form of pressure that violate the free will of the voter to induce a voter to vote in desired way.

Credential Theft: when an unauthorized individual (man in the middle attacker) obtains and uses valid voter's credentials for unauthorized access to a voter's computer. The attacker obtains credentials which violate the voter privacy by using keystroke logging.

Imposter Sites: when a voter uses a fraudulent websites similar to the legitimate electoral websites to cast his ballot. With fraudulent websites, they will use recognisable company names but the name of their website probably won't cite the well-known company mentioned in their web address.

Malicious Software: is used to destroy the computer operation, gather sensitive information, access to a dedicated computer system , or display ads do not require any software. Malware can be hidden under the plan to steal computer users' information without their knowledge or spyware extended period , such as the Swiss crystal , or it may be designed to cause harm , often as damage (for example , seismic network) , or extortion payment (crypto Locker). "Malware" is used to refer to various hostile or intrusive form of software in general , [4] including computer viruses, worms , Trojans , ransom ware , spyware , adware , scareware and other malicious programs. It can take executable code, scripts, active content, and other forms of software. [5] Malware is often disguised as or embedded, non-malicious files. As the threat of malicious software in 2011 most of the activities of a worm or Trojan horse, not a virus. .

Botnets: Botnets are infected without the user's knowledge of malware and cybercriminals control computer interconnection network. They are usually used to send spam, spread viruses and other actors engaged in cyber crime

Figure 2: Server-side attack

Server-side attack: The count of voters vote depends on the integrity of the server, which is the only correct operation that has the ability to decrypt the vote cast. And the secrecy of the ballot count depends on non- disclosure of data between the encryption and decryption of the votes on the server. Malwares can sent to infect the count server, an attacker can disrupt these critical security attributes. [12]

Denial of service: a denial of service (DoS) attacks or computer resources so users can not use it to target users temporarily or permanently interrupt or suspend service to connect to hosts on the Internet

Insider attacks: access to insider attacks is a person engaged in malicious attacks on the network or computer system through the authorized system who have legitimate access to people and network resources within an organization and has the ability leak information. Internal threats are difficult to resist than the external attack because insider has had legitimate access to the organization.

Remote Intrusion: Classification attacks, a common method of attack or invasion is an indication that they are remotely via the Internet or by cracking system privileges by the user. Note that a

remote attacker can at any time be logged without the permission of the users.

State-Sponsored Attack: it's a cyber-ware where individuals with significant knowledge of how voting architecture or infrastructures works and take control of the entire or part of the system or can be taken down. Web sites and hard drives of the election authority and governments are infiltrate, affecting it with viruses, denial-of-service attacks and worms.

3.2 Security Threats in e-voting system

Indian voting machines have a critical security flaws and constraints than other electronic voting systems used in other part of the world. The analysis conducted from our research show that the Indian EVM machine are still more vulnerable to weakness. The challenges faced by the EVM are:

- Cost: The cost of the EVMs in used in the India differ from the system used in Europe and America. It cost $200 for one set of units while United State and Europe cost several thousand dollars which make it inexpensive for programmers to do reserve engineering process to study the system.
- Power: Most polling areas are located in rural areas with shortages or lack of electricity supply. The EVMs used battery to power the machines, rather than merely using a battery as a backup.
- Replacing the ROM chips or swapping the Z80 processor with a dishonest look-alike.
- Replacing memory chips that store election software.
- Hardware-based attack that would change the signals from the machine's candidate buttons before they were recorded by the CPU.
- Reverse-engineered the hardware and software.
- Upgradeable firmware as well as external memories for ballot programming and vote tabulation.
- Built hardware devices to interface with the machine's proprietary memory cartridges and created vote-stealing software that employed return-oriented programming to bypass the machine's memory protection hardware.

4. Recommendations

Although we spend most of this report discussing the vulnerabilities and security threats, we cannot dismiss the great effort put on by the voting system developers, security managers and officials whom puts on great amount of time and resources to ensure electoral voting systems and internet voting systems becomes a success. Here are some key recommendations to ensure the safeguard of votes.

1. The Estonian system, AFAIK, uses their gov-issued cryptographic smartcards, and still does central tabulation, which is vulnerable, no e-voting system or internet voting with central tabulation can be called secure.
2. Never advocate using any electronic voting system or internet voting that is not totally open source and totally open to free inspection at all point in the system's operation.
3. Even as a developer you can still look at the source code, but you cannot be sure that it's the same source code implemented on each of the voting machines, or that some of them may have been hacked or intercepted the outcome.
4. The entire voting hardware and software are outsource to private companies whom can eventually leak the information or data to outsiders.
5. Ensure vote are protected using end-end encryption.

5. Conclusion

For over years, enthusiasm for the field of electronic voting and internet voting has been developing, as nations all inclusive are investigating strategies for utilizing ICT to build election exactness, speed and transparency, while opening democratic based procedures to a more extensive audience. Various nations have explored different avenues regarding electronic voting arrangements and have closed to relinquish its execution, until further improvements in the field are made, while others have succeeded in actualizing completely electronic vote casting frameworks without disappointments. Methodologies and conclusions appear to vary broadly, while the Netherlands have chosen to return to customary voting, forsaking voting machines, France has approved the last subsequent to 2003 however is declining to actualize e-voting in regions other than expert election, which is likewise the case in Portugal; Austria effectively directed its first e-voting legitimately restricting decision in 2009, Switzerland has revised its lawful controls to empower remote e-voting, Estonia has held two sequential legitimately restricting remote e-voting election**.**

6. References

[1] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," IEEE Symp. Secur. Privacy, 2004. Proceedings. 2004, pp. 27–40, 2004.

[2] C. Lambrinoudakis, S. Kokolakis, M. Karyda, V. Tsoumas, D. Gritzalis, and S. Katsikas, "Electronic voting systems: security implications of the administrative workflow," Database Expert Syst. Appl. 2003. Proceedings. 14th Int. Work., pp. 467–471, 2003.

[3] M. M. Olembo, P. Schmidt, and M. Volkamer, "Introducing verifiability in the POLYAS remote

electronic voting system," Proc. 2011 6th Int. Conf. Availability, Reliab. Secur. ARES 2011, pp. 127–134, 2011.

[4] S. Thammawaja and M. Lertwatechakul, "Design a secure electronic voting system for Thailand's election," 2008 Int. Symp. Commun. Inf. Technol. Isc. 2008, pp. 40–45, 2008.

[5] G. S. Matharu, A. Mishra, and P. Chhikara, "CIEVS: A cloud-based framework to modernize the Indian election voting system," 2014 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2014, 2015.

[6] M. Huarte, I. Goirizelaia, J. J. Unzilla, J. Matías, and J. J. Igarza, "A new fully auditable proposal for an internet voting system with secure individual verification and complaining capabilities," ICETE 2013 - 10th Int. Jt. Conf. E-bus. Telecommun. SECRYPT 2013 - 10th Int. Conf. Secur. Cryptogr. Proc., pp. 395–402, 2013.

[7] B. Zwattendorfer, C. Hillebold, and P. Teufl, "Secure and privacy-preserving proxy voting system," Proc. - 2013 IEEE 10th Int. Conf. E-bus. Eng. ICEBE 2013, pp. 472–477, 2013.

[8] G. Dini, "Increasing security and availability of an Internet voting system," Proc. - IEEE Symp. Comput. Commun., pp. 347–354, 2002.

[9] A. F. N. Al-Shammari, A. Villafiorita, and K. Weldemariam, "Towards an open standard vote verification framework in electronic voting systems," Proc. - 2012 7th Int. Conf. Availability, Reliab. Secur. ARES 2012, pp. 437–444, 2012.

[10] Melanie Volkamer (2009) Evaluation of electronic voting: requirements and evaluation procedures to support responsible election authorities, New York: Springer. (10)

[12] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System," Proc. 21st ACM Conf. Comput. Commun. Secur., no. May, p. 12, 2014.

[13] Estonian ICT Export Cluster (2016) I-Voting, Available at: https://e-estonia.com/component/i-voting/ (Accessed: 2nd July 2016). (13)