Cyber Risks Analysis and Mitigation: Digital Election Voting System

Dr. Shruti Mantri
Kirti M. Doongursee College, University of India.

Abstract-*When we cast our vote, we are not just marking a ballot for the candidate of our choice, but are also signifying our belief in the system. Voting system is made up of multiple different interconnected sub-system. The current trend of cyber-attacks, being directed on critical infrastructures, with election voting system being one of the important critical infrastructures. There is thus a need to identify the cyber threat vectors and attacks for election system. In the current study, the researcher has identified cyber risks threat vectors for election system and proposes a solution for countering cyber threat vectors.*

Keywords-Electronic voting system, critical infrastructure, threat vectors, risk analysis

I. INTRODUCTION

According to (Johnson 2017), the increasingly digital and connected world has been reshaping our life for more than 20 years. It has streamlined everyday tasks and changed the way we communicate with each-other. Though the constantly evolving digital age has improved our quality of life, it has also introduced an array of cyber threats and implications. Twenty years ago, the cyber-attacks were fragmented, easy to combat. The attackers attacked on servers and machines. Threats were made up of single step exploits. The recent cyber-attacks in cyber space have highlighted that the threats these days are of more holistic nature and are adaptive. They include humans and machines and are more targeted on critical infrastructure. The attacks are also multi-step exploits and are made up of covert tactics. Therefore a universal approach to cyber security is needed that covers all aspects of cyber space such as threats actors, advance telemetry of networks and a defensive strategy that continuously adapts to the adversarial capabilities and threat landscape.

A vote is an act of conscience and will. It's also an act of trust. When we cast our vote we are not just marking a ballot for the candidate of our choice, but are also signifying our belief in the system. Every vote mark counts and indicates our voice is being heard. The electoral process is not exactly a single, hack-able system. Systems for voter registration, signing-in, voting and tallying the vote vary, state to state, county to county and from district to district. Even at state level, electronic voting systems may not be directly connected to the internet or, generally, even with each other. But they are sub-systems within system. Vulnerability and risk in one system can lead to compromise in another sub-system or system as a whole. The 2017, American elections process witnessed hackers aiming to attack election system; for example, Russian government hack of the Democratic National Convention email servers, embarrassing emails leaked by WikiLeaks and Arizona and Illinois voter database being hacked. According to Lance Ulanoff 2016, along with direct attacks, the election process is also subject to indirect attacks such as sending text messages to voters on the day of the election about warning of violence at polling booths (even when there is no problem) to keep voters away from the polls for hours or even completely. The voters turn out plays a crucial fear in an election process. Spreading fear and confusion among the voters is a matter of concern. According to Joseph Lorenzo Hall, chief technologist for the Center for Democracy and Technology, there's also the potential chance that someone could hack the systems that manage the voter rolls especially when traditional computers are being used. "If the computer systems, laptops may crash or don't boot up and there's no paper backup (for the voter rolls), that will definitely lead to shut down of voting for a number of hours," said Hall. The election process is thus subject to risks and vulnerabilities. It is thus very important to treat election process as infrastructure that can have serious impact on the nation's future and economy. Every nation defines infrastructure crucial to it as critical infrastructure. This varies from nation to nation. According to Cherdantsevaa et al. 2016, critical infrastructure are those physical and information technology assets for example, data, systems, and networks, which when disrupted, damaged or destroyed, will have serious impact on the health, safety, security, economic wellbeing of citizens and the effective functioning of Governments (Cherdantsevaa et al. 2016). According to (Innovation and Paper, no date) Telecommunication Industry Association, cyberspace has become essential to every individual, business and government. Since the wide availability of internet in 1994, cyberspace has rapidly grown and evolved. Cyber space generates far-reaching benefits from our largest critical infrastructures to each individual citizen, with the integration of cyber space with critical infrastructure. Any intelligent system of the critical infrastructure is made up of multiple systems working together. As stated earlier, each of these sub-system is a critical infrastructure in itself. As

mentioned by (Abouzakhar, 2015), "Critical infrastructure represents a system or a number of systems that perform computational functions and operations." Such systems are acute when they impact other critical processes and/or devices, or provide a pathway/channel to other systems, or used to protect other systems (Knapp 2011). According to (Abouzakhar, 2015), most of the current infrastructure rely heavily on communication between multiple devices via a wireless medium to achieve specific objective (Abouzakhar, 2015).

In the current study, the researchers reviews the cyber risks and threats to election system and the future impact on society and nation's security to define election system as a critical infrasctrure.

II.RISK ANALYSIS OF ELECTION SYSTEM

Elections allow population to choose their representatives. It's a way in which people express their opinion and preferences for how they will be governed. Thus the integrity of election process and the system used in election process plays a major role in achieving the goal of election process. The election system must be robust to withstand traditional and modern risk and vulnerabilities. According to (Kohno et al., 2004), voting system must be transparent and tamper-resistant to stop a wide range of attacks for example, cyber-attacks or incorrect tallying by insiders. Risks and vulnerabilities in any one sub-system of the voting process can lead to uncertainty in all the other interconnected and interdependent systems and thus result in incorrect outcome. The election system is made up life-cycle of six stages (Wolchok, Wustrow and Halderman, 2010): (i) manufacture and safe-guard of machines to be used to cast the vote, (ii) voters registration, (iii) verification of voters on election-day, (iv) casting of vote on the day of the election, (v) the tabulation mechanisms for determining the winner and (vi) dissemination of election result. Each of these six stages are vulnerable to cyber risk and threats. Each of these six stages are prone to cyber risks and threats. The risk and vulnerabilities for the six stages are grouped into three levels (Miller 2016):

1. Manufacture level

The election system is made up of computer systems, servers, routers, wireless-network, voting machines, ballot boxes etc. Each of these devices are manufactured and purchased from a vendor or company. The vulnerability introduced at the manufacture level will be carried ahead, through the entire cycle of hardware and software. The vulnerability introduces uncertainty and risks through the entire life cycle of the election process. The attacker can decapsulate the chip and examine it, modify the software before it is built into the CPU, introduce a back door in the software before burning it into the chips. The chips are manufactured at the factory and are shipped to assembly units. The attackers can exploit this link and substitute look-alike CPU's containing the software that counts the votes wrongly.

Also some of the voting machines used to cast the vote were designed and developed almost 15 years ago. These machines in those days were not designed to counter cyber risk and threats. The machines still use DOS (1999-2000 OS) running operating system. Also the voting technology and programme code is proprietary (black box) and embedded into these devices. Hence it is difficult to analyze from forensics aspects. It is therefore very easy for an attacker to inject payload or poison the update to extract data at the manufacture level and carry it till tabulation stage. An attacker can also inject port sniffer and additional access points in the machines at the manufacture level. The greatest threat to every election is the dependence on the black-box proprietary voting systems because voters and officials do not actually know what code is running and what vulnerability exists in the systems. The dependence on private vendors to manufacture voting machines in itself introduces risk as these vendors are not government organisations or agencies. Upon, that the election officials are not qualified to identify and treat cyber threats, hence it is very difficult for them to identify any discrepancy in the voting machines introduced at the manufacture level.

2. Local level

The election officials generally believe that election systems are secure because the systems are isolated from networked systems via an air gap; they are thus under an illusion that the voting machines and the network is not prone to risks and threats. But there are varied attacks that can be executed on the voting systems such as: on the day of the election the attackers can execute cyber-attacks on memory cards, reset the switch on the voting machines, corrupt data and stuffs at the ballot boxes. They can also carry out denial of service attack, remove flash card from memory by executing social engineering attack on election employees (insiders attack), physical corruption of devices, and introduce software bugs and exceptionable open ports. The election officials have no formal training to deal with social engineering attack they thus are weak-links in the election process. There exists no standard procedures or standards for security audits of electronic voting machines and systems pre and post the elections.

3. State Level

We the voters register our-self within the state we are domicile resident of and are also allowed to vote only in the area of our resident jurisdiction. Thus election process is decentralized at the state level. Even at the state level the different components of election systems are prone to different types of cyber risks and threats. In the current study the researcher has categorized the cyber risks and vulnerabilities at state level into five different categories: (i) Exploiting website vulnerabilities (ii) breaching and exploiting state servers (iii) affecting state computer systems (iv) compromising state tabulators (v) spread of malware in network and poisoned the systems (Miller 2016):

(i) Exploiting website vulnerabilities

The voters register online through the registration websites. Post the registration process every voter receives his/her voting card. An attacker can manipulate the registration website, carry out a brute force attack on it and gain access to the sensitive information of every voter. The attacker can also carry out SQL injection attacks to tamper the database by deleting entries from the database just prior to the election thus making it difficult for voters to cast their vote on the voting day. By gaining covert access the attackers can also hamper the dissemination channel through which the results are published on websites and local platforms.

(ii) Breaching and exploiting state servers

The voters to register needs access to the state servers that acts as access point for the website.

These servers hosting sensitive information needs layered and demilitarized security. The attackers can gain access to state servers as they lack the necessary security measures, there by trying to compromise the database. The servers also lack behavioral analytics mechanism hence attackers can log into the system with higher privileges that of an administrator and carry out an attack. Attackers can also identify the election officials who are going to manage elections as there are few chosen election officials and send phishing mails to them and gain access, for example use of LinkedIn to send phishing mails. The election officials are users of the system but not trained security professionals. They thus act as one of weakest link in any system. The attackers can exploit human behavior and psychological pattern to carry out planned or unplanned insider attack either pre, during or post the election process.

(iii) Affecting state computer systems

The election systems such as PCs, servers, routers need mainatinece on regular basis. The mainatinece is usually outsourced to a maintenance company or agency. The attacker fabricating as maintenance vendor can get illegal access to the system, install malicious payloads, sniff and intercept the data packets network, inject social media malicious code capability, malicious code to infect USB ports, introduce additional droppers, screen jobbers, camera and microphone capture. The tools to design and execute the attacks are easily available on the dark web. The support for design and execution of attacks is also available on the dark web. Using the guidance and support from the dark web, the attacker can also plan and execute DDOS or DOS attack and knock off the database in the middle of election system.

(iv) Spread of malware and poison the state election systems

The network either wired or wireless is a good medium to spread malicious codes. Through the network an attacker can spread malware to state election systems and servers that can compromise the systems, database, leak sensitive, tamper the data about the voters and the voting result. He/she can poison the update at manufacture level and get access to server and database. The attacker can also add ransom-ware feature for voter registration database or vote count database on the day of the election and weaponing of encryption. The existing devices which are being used were manufactured almost 20 years prior. The device manuals for these devices is also easily available on the vendors or departmental websites, there by exposing the risk of threats. There is thus a need to define security standards for elections system.

(v) Compromising state tabulators

Windows as an operating systems is widely been used for almost 20 years and the vulnerabilities in operating system are also widely known. It is thus very easy for the attackers to exploit the vulnerabilities and carry out an attack and also replicate the attack. Post the voting process the data needs to be moved from one system to another using multiple devices which also is a compromising link in the system.

III. IMPLICATION: ELECTION AS CRITICAL INFRASTRUCTURE

Twenty years back, cyber-attacks were more aimed in compromising towards individual devices and network. The current trends of cyber threats, indicates the nature and type of attacks are more humanoid, social and enterprise directed. The aim is to crash the perilous infrasctrure and the economy of

the nation. With the recent trends of cyber risks and threats there is a need for policy makers to define new critical infrastructure. Voting is a fundamental right and the soul of democracy. The core of election process is based on integrity and confidentiality that defines that each vote is recorded and counted with accuracy and non-biased. But the election process has also been exposed to different types of attacks since 1994. Attacks on voting machines dates back to 1994 with the compromise of South African election system. A hack on Ukraine voting system in 2014 removed important files from the database just before the election. The election officials had to rely completely on backup. The cyber-attack to compromise 2016 US election system indicated foreign electoral interferences. According to Professor J.Alex Halderman(Shackelford et al., 2017), University of Michigan, by concealing a microprocessor and Bluetooth radio in the machine, the duplicate display board intercepts the total vote that the machine is trying to display and replaces them with modified votes.

There is thus need to take necessary steps such as: review and analyze new technology to be implemented that can counter cyber threats. The modern equipment needs to be designed and manufactured. The existing voting machines do not store the votes in encrypted format. There is thus need to design and implement cryptographic framework to store the information within the electronic voting machine in an encrypted format (Wolchok, Wustrow and Halderman, 2010), every voter also needs to be identified one unique one time password, digital signature and biometric mechanism in addition to voter card. Humans being the weakest link and the biggest risk in cyber-attack there is also a need to study aspect of human behavior and human dimension to prevent insiders attack. There is also a need to introduce: (i) voter-verified paper audit trail to cross-verify the results, (ii) security audits and vulnerability scans of all machines and registration systems pre-election process, (iii) forensics of source code embedded inside the electronic voting machine, (iv) post-election risk audit to identify irregularities in election process (v) design and define strategies and policies to counter cyber-attacks at local level, state level and manufacture level, (vi) protection of physical systems from physical compromising, (vii) design manuals stating the dos and don'ts for the election officials needs to be prepared.

IV. CONCLUSION

Attackers will be here for some more time and develop advanced sophisticated vectors. There is thus a need to design, develop, implement and test: (i) cyber risk assessment and management system, (ii) incident response plan; to counter cyber risks and threats at all the three levels: (a) manufacture, (b) local and (c) state level (iii) governance at national and international level, (iv) define and design international agreements (v) define rules and regulations to protect critical infrastructure from foreign enemies Every nation needs to carefully consider the cyber risks and threats for their election systems and how they can achieve a secure and transparent voting system that is suitable to its national values and requirements.

REFERENCES

[1] Abouzakhar, N. (2015) 'Critical Infrastructure Cybersecurity: A Review of Recent Threats and Violations', 1, p. 11. doi: 10.1017/CBO9781107415324.004.

[2] Innovation, T. I. A. and Paper, W. (no date) 'Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain | Telecommunications Industry Association'. Available at: http://www.tiaonline.org/policy/securing-network-cybersecurity-recommendations-critical-infrastructure-and-global-supply%0Ahttp://tiaonline.org/policy/securing-network-cybersecurity-recommendations-critical-infrastructure-and-global-supply#i.

[3] Kohno, T. et al. (2004) 'Analysis of an Electronic Voting System', IEEE Computer Society Press, (May), p. 23. doi: 10.1109/SECPRI.2004.1301313.

[4] Shackelford, S. et al. (2017) 'Making Democracy Harder to Hack: Should Elections Be Classified as "Critical Infrastructure?"', University of Michigan Journal of Law Reform, (forthcoming), pp. 1–40. Available at: https://ssrn.com/abstract=2852461.

[5] Wolchok, S., Wustrow, E. and Halderman, J. A. (2010) 'Security Analysis of India ' s Electronic Voting Machines', Human Factors, pp. 1–14. doi: 10.1145/1866307.1866309.

[6] Johnson J. (2017), 'Statement by Secretary Jeh Johnson on the designation of election infrastructure as a critical infrastructure subsector' Available at: https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical (Accessed: 20th July 2017)

[7] Cherdantsevaa Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H. and Stoddart K. (2016) 'A Review of Cyber Security Risk Assessment Methods for SCADA Systems', Computers and Security, Vol. 56, pp. 1-27. Available at http://socialdatalab.net/publications. (Accessed: 7th July 2017)

[8] Knapp E. D. (2011), 'Industrial Network Security', Syngress. (Accessed: 6th July 2017)

[9] Miller J. (2016), 'ICT and Cylance Discuss Election Hacking Risks' Available at: https://www.cylance.com/icit-and-cylance-discuss-election-hacking-risks (Accessed: 23rd July 2017)
[10] Ulanoff L. (2016), 'In ballots we trust: E-voting, hacking and the 2016 elections'Available at: http://mashable.com/2016/09/26/election-voting-system-analysis/#FkliE3kz0Sq0(Accessed: 23rd July 2017)