Survey Report on Cyber Security related issues on Nuclear Stations, Vehicles and Wireless Networks

Sarvesh Joshi
Department of Information Technology
Mukesh Patel School of Technology Management and Engineering, NMIMS Deemed-to-be University
Mumbai, India.

Abstract *— Lately, the world has turned into a technological world. So, security was and will also be a concern as well as a priority with the adaptive technology. The domain selected was Cyber Security and the Sub – Domain which was targeted was the DOS attack.*

The first paper gave measures to solve issues related to DOS attack on Nuclear Stations. The second paper gave measures to solve issues related to DOS attack on Vehicles. The third paper gave measures to solve issues related to DOS attack on Wireless Networks. The authors of each paper gave their individual solutions to the problems they had faced and the solution to it using few techniques and models.

Keywords — *Cyber Security, Nuclear Security, Vehicular Security, Wireless Network Security*

I. INTRODUCTION

In this technological world, security is a concern as well as a want considering the confidentiality and the integrity of people's data. Every person not only an IT expert understands the importance of security of electronic devices and also understand what can lack of security do that can cause numerous problems to your system as well as your network. When a computer system becomes vulnerable to threats, any attacker can monitor, modify, steal or even delete data from the system or the network. The developers and the IT Security experts have to continuously patch these vulnerabilities. These updates or patches help counter the upcoming attacks that may occur at any instance of time. The security goals of confidentiality, integrity and availability must be achieved. There are multiple attacks that an attacker can make. The DOS attack is one of them. What the DOS attack does is? That it makes a system crash and go offline for a certain instance of time. The attacker floods the targeted system with heavy traffic which the system and cannot handle and it ultimately crashes.

The first paper consisted of threats to Nuclear Power Stations. Nowadays automation and technology is being used in every field of work. Every electronic product has its own vulnerabilities which need to assessed and corrected time to time. Nuclear Engineering also uses digital equipments and digital systems which can lead to serious hazards. These equipments use software's which can be bypassed by any anonymous cyber security expert and can cause threat to the nation as well. In order to avoid such incidents, agencies around the world have announced guidelines for cyber security related issues. A cyber security risk evaluation model has been proposed to control such incidents using two control systems which are Bayesian Network (BN) and Event Trees (ET). BN would be a model which would collect analytical data for assessment and ET which would implement safety assessment methods. The proposed method will provide insight into safety and cyber security risks. [1]

The second paper consisted of threats to Vehicular Security. The vehicles in the current time are also connected to the web continuously and have adapted to automation. The entertainment systems in the vehicles are connected to the internet continuously.Technologies such as anti-lock brake systems, steering assist, and in some cases autonomous driving, manufactures nearly eliminated the dangers of driving. But it is also increased the level of cyber-threat as everything is computed and connected to servers where all the data about the automation system will be stored. Unfortunately, when dealing with vehicular technologies, cyber security experts and automotive manufactures cannot treat automotive networks and its digital resources as they would with computing networks. The author gave solutions to the problems related to vehicular security by the use of Distributed Firewalls and Firewall Like Program(FLP). [2]

The third paper consisted of threats to Wireless Networks. Wireless Networks are very vulnerable as it is open medium. Wireless Networks are vulnerable to Rogue Access Points(RAP). It is an unauthorized access point which can be installed by any user without the knowledge of the network administrator.

Whenever the rogue device is connected to the internet, it can be used as a weapon to breach the security of any system. The author introduced a technique called as HoneyPot Intrusion Detection System (HoneyPot IDS). It is introduced for the detection and prevention of attacks on wireless networks via Rogue Access Point. It is the combination of Honeypot and Intrusion Detection System. It diminishes the false alarm rate caused by the IDS. Wireshark is used to detect the flow of packets. The malicious user can also use an authorized IP address to make an DOS attack. The Wireshark tool detects the DOS attack, but at some instances if the attacks is being made by an authorized IP address then the HoneyPot IDS fails to track and block the attack. [3]

To address all the security challenges the authors have presented with few solutions to which may help overcome these issues.

II. RELATED WORK

To handle, monitor and patch cyber-attacks on systems, cyber security experts have come up with various solutions apart from the ones that are mentioned in the papers. The use of Demilitarized Zone(DMZ) is another solution provided by some practitioners to solve the problems. The problems related to DOS attack have also be solved by making the attack less effective by the use of Load Balancer.

A. Cyber Security Risk Evaluation of a Nuclear I&C

a). Model Architecture

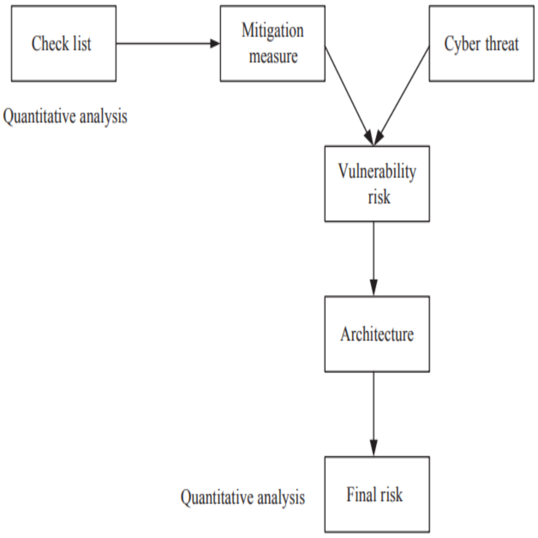

Fig. (1) Flow Chart of BN

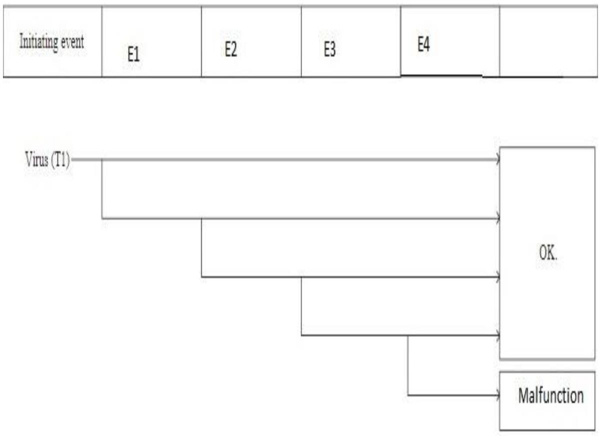

Fig (2) Flow of Event Tree

A risk evaluation program was proposed by the author which consisted of the use of two models, Bayesian Network (BN) and Event Tree(ET).BN would be a model which would collect analytical data for assessment and ET which would implement safety assessment methods. As an alternative, the paper proposes the use of a cyber-security risk evaluation method using a Bayesian network (BN) model. Fig (1). shows us the flow of Bayesian Network. Fig (2). shows us the flow of Event Tree. [1]

b). Performance and Evaluation

In this paper, the author gave solutions to safeguard networks of a Nuclear station. SQL Slammer worm a type of DOS attack was had affected many nuclear systems around the world. SQL Slammer Worm is an attack which finds the system, copies the worm program and then remotely executes it. The author in this report indicated that they encountered difficulties in obtaining data through penetration testing. Nuclear facilities have a SCADA system that is separated from outside systems, and used to control and monitor measurement data from the I&C (instrumentation and control) system. Although the SCADA (supervisory control and data acquisition) system is separated from the outside, cyber-attacks occur in nuclear facilities such as nuclear power plants and centrifugation facilities that enrich uranium. [1]

The author proposed a RPS (Reactor Protection System) which defined six type of threats, each threat defines a cyber-attack method for the system, and each mitigation measure is a method of preventing cyber-attacks. [1]

B. Cyber Security related to Vehicles

a) . Model Architecture

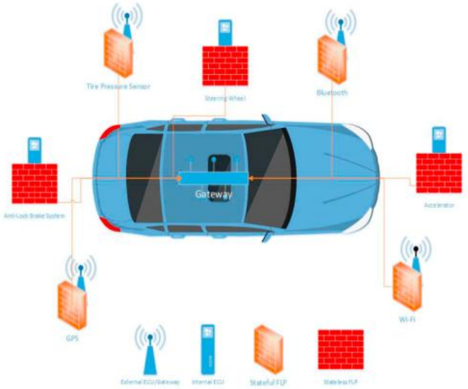

Fig (3). Firewall Setup for Vehicular Security

The suggested model was that a stateful firewall will be connected to every electronic device in a vehicle. Each firewall will act individually so it can focus on each element properly and the ratio of correctness increases. This firewall is a Firewall Like Program (FLP). Technologies such as anti-lock brake systems, steering assist, and in some cases autonomous driving are the technologies which are considered as vulnerable to cyber-attacks. So each entity of technology is attached a separate firewall. [2]

b). Performance and Analysis

Passive Key Entry and Start System (PKES) is a technology which is used by some car models. It is basically the connection generated between the car key and the car to open or close the car. The attackers spoof the PKES by mimicking the signal between the car key and the car. This is called as the Replay attack. The mimicked signal automatically authenticates the end user to access the car. It is a type of sniffing. It makes the original receiving end i.e. the car to think that the mimicked signal is the original signal. This Replay attack is also called as the stepping stone to car hacks. This enables the attacker to access the cars Car Area Network (CAN). There were multiple solutions provided to stop the Replay attack such as removing the battery from the car remote, shielding the key remote physically so that it cannot be sniffed. But these all solutions would only work when the car driver is in particular nearby distance. The main threat caused by this attack is that the anonymous attacker can start the car as well using the key.

A DOS attack can be made to the entertainment systems in a vehicle. Most of the entertainment systems are continuously connected to a network over the internet. A DOS Attack on the Electronic Throttle Control System (ETC) could lead to malfunction in the throttle of the car. The safety of the people in the car as well to the people around the car could be in danger. Some DOS attacks may also affect the Controller Area Network (CAN) bus which control critical parts of the car. These critical parts include the brakes, throttle and steering of the car. These parts could be disabled by an overload on their processor.

The use of Distributed Firewall and Firewall Like Programs (FLP) have not abandoned the threats but have definitely reduced them. [2]

C. Cyber Security related to Wireless networks

a). Model Architecture

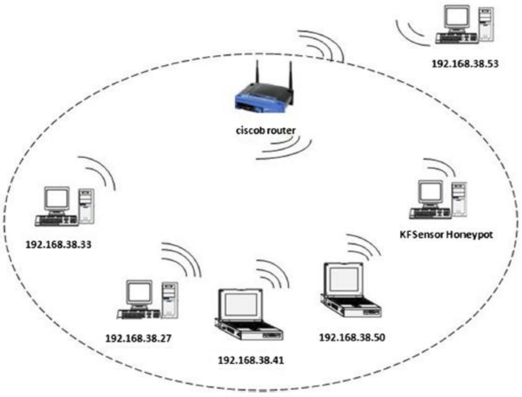

Fig (4). Experimental Setup for Honeypot IDS

The suggested model includes the use of Honeypot Intrusion Detection System (IDS). Honeypot IDS is used for reducing the false alarm rate generated. This even helps in the detection of Rogue Access Point (RAP) in a wireless network. The detection of RAP in a wireless network is very important as it brings various security threats with it. [3]

b). Performance and Analysis

The most common threats detected on wireless networks were DOS attacks, DNS Spoofing attack, etc. A Honeypot IDS is setup in a network to lure the attacker to attack the system so that with help of Wireshark tool they can track the incoming packets and detect as well as monitor the attacker as well the attack which is being made. Measures are taken once the attack type is known to the cyber security expert. Detection of Rogue Access Point (RAP) is a must. It can cause a lot of threat if the RAP is breached by an attacker. MAC Spoofing is also very easy when it comes to wireless networks.
The proposed algorithm helps us monitor incoming threats and act upon it as soon as possible to avoid any major loss. [3]

III. COMPARATIVE ANALYSIS

Evaluation Parameters	Paper 1	Paper 2	Paper 3
Key Features	-Bayesian Network (BN) -Event Tree (ET) -Reactor Protection System (RPS)	-Distributed Firewall -Passive Key Entry and Start Systems (PKES)	-Uses Honeypot IDS to reduce false alarm rate generated by existing IDS. -Sustains the overall workload of honeypot. -Analyses the traffic directed towards the protected network.
Pros	-DOS attack is prevented. -SQL Slammer Worm is eliminated.	-DOS attack is stopped. -Replay attacks are avoided.	-Detects Rogue Access Points(RAP) Prevents the installation of RAP. -Minimizes False alarm rate. -It is capable of deceiving the attackers to a greater extent. -DOS attack is tracked and stopped.
Cons	Man in Middle attack is neglected by the author and it could be an even threat to the system as any external entity could make changes to the actual signals transmitted from one processor to the other processor and send corrupt or malicious data. Dumpster Diving is a technique which may not exactly come under cyber security but can be a threat to the nuclear systems in every way as it may contain technical as well as non-technical data about the systems through which vulnerabilities can easily be triggered.	Trojan can act as a major disadvantage to Distributed firewalls as most of the firewalls fail to detect a Trojan which could act as a major threat. Car Area Network is extremely vulnerable.	The Honeypot Intrusion Detection System method is time-consuming and expensive. It will fail to detect a spoofed MAC address. An attacker can easily turn off the AP during scanning and fails to detect MAC spoofing.
Key Assumption	-Ransom ware may affect the system. -There is an existence of worm. -DOS attack is possible.	-Vulnerabilities are found in stateless firewalls. -The Compromised Firewall Like Program would not be able to mitigate any attack. -The distributed firewall can work on every car model.	-Some malicious user will spoof the -MAC address. The proposed work will work on large wireless networks. -The same architectural design will work on cloud as well.
Quantitative Analysis	The author found out that vulnerabilities can be penetrated in the Reactor Protection System (RPS) through Bistable Processor (BP) which receives signals regarding the status of the nuclear plant. BN and ET algorithms were used to assess and eliminate these vulnerabilities. These algorithms helped in eliminating the SQL Slammer Worm which was a big threat to the nuclear system and its presence could have caused lot of data loss as well would have enabled data transparency.	The author made corrections regarding vehicular security using Distributed Firewalls to avoid DOS attacks and stopped Replay attacks on PKES in the automated systems in a car which would mimic the signal of a car remote through which doors of the car could be opened.	The calculated false alarm rate was 15% compared to the 38% which was predicted. False Positive Rate without Honeypot is 0.67% False Positive Rate with Honeypot is 0.28%.
Analysis	The author has found out measures to eliminate SQL Slammer Worm using BN and ET algorithms but has neglected the threats which could be caused by Man in Middle Attack or even Dumpster Diving technique. The author tried to prevent cyber security attacks on few things but also missed out on a few which could cause a threat to the nuclear stations in one way or the other.	The author found out measures of correction for vehicular cyber security by using Distributed Firewalls which will try to stop DOS Attacks and Replay Attacks. But these are done under the Car Area Network (CAN) which is extremely vulnerable. In CAN basically an attacker can exploit parking sensors which will allow the attacker to open the car without any remote.	The solution provided to reduce false alarm rate using Honeypot IDS is a very good solution provided by the author but it is a work which is implemented on small wireless networks and we don't know whether the same technique might work on large networks or not.

IV. RESEARCH GAPS

a) It is a work which is implemented on small network and we don't know whether thesame technique might work on large networks or not.

b) DOS attack can be attacked virtually or even through a physical medium (pen drive,dvd, etc.). The author has just given solutions and provided modules regarding thevirtual DOS attacks which are made by the attackers remotely through a network. Nosolutions were given regarding DOS attacks which can be made through physicalmediums.

c) Social Engineering could be a main cause for any attack to DOS a system. Amalicious attacker can grab all the information regarding the system from the systemadministrator and use that confidential information to DOS the system or even deleteor modify the existing data.

V. FUTURE WORK

a) The proposed solution to it would basically be the use of Demilitarized Zone(DMZ)to extremely integrated systems if the cost is not an issue. DMZ will not only avoidthe DOS attack but also reduce the chances of any other attack which could cause a threat.

b) The use of Load Balancer could reduce the damage caused by a DOS attack as it can handle more data and requests compared to normal servers.

c) A Network Performance Tool can be installed to every system which can continuously monitor and track incoming and outgoing traffic.

d) The solutions must be tried and tested on larger platforms with larger networks as well for the understanding of its better functioning.

ESTIMATE OF TIMELINE

There is can no such timeline be set in terms of the security of any system i.e. it will take 1 year or 2-year s or 3 years. Monitoring threats and providing solutions to those threats is a continuous process. Every day, every second there is a new type of virus generated which no one is aware about. Finding solution to those threats is a redundant and daily process. The systems need to be updated with solutions to these new attacks and viruses on day to day basis. The timeline of the solutions exists till the system exists.

Timeline can be set for a particular set of viruses. For e.g. if a new virus is found out, then a timeline of 1 to 2 months per virus can be set to patch it. The same way, if a virus or a ransomware is of the similar type of any previous patched viruses then patching it would be much quicker job. A batch of virus can take any amount of time ranging from 1 year to 2 years as well. The SQL Slammer Worm was a type of DOS attack which took almost 3 to 4 years to be patched as experts could not track and know about its existence in the system. If a similar type of virus comes into existence, then it is a tough job for the experts to patch it. SO the time in in such cases can vary between 2 years to 3 years.

VI. CONCLUSION

In this technological world, security of electronic devices has become a concern due to its extensive use. Every electronic device has its own flaws which can be bypassed easily by any hacker. The devices which are continuously connected to the internet are continuously in threat of being hacked as they are more open to the real world. Vulnerabilities in electronic devices becomes a source of hack for malicious hackers to bank on. Safety is and should always be the first priority. With the progress in technology on daily basis, there is a rise of threats.

Whether it is the security in cars or nuclear plants or wireless networks, the concern of security has the same importance in every field of work. To avoid security breaches in computer systems, security experts work day in and day out to patch the bugs and provide utmost integrity to public data.

The researchers have come up with solutions for the safeguarding of computer devices which may affect humans. Few methodologies and modules are provided by the researchers for their respective fields. The proposed methods are expected to provide safety and security to human kind.

REFERENCES

[1] Jinsoo Shin, Hanseong Son, Gyunyoung Heo, Cyber Security Risk Evaluation of a Nuclear I&C Using BN and ET, Department of Nuclear Engineering, Kyung Hee University,Republic Of Korea, 2016.

[2] Syed Rizvi, Jonathan Willet, Donte Perino, Seth Marasco, Chandler Condo, A Threat to Vehicular Cyber Security and the Urgenct for Correction, Department of Information Science and Technology, Penn State University, Altoona, USA, 2017.

[3] Neha Agrawal, Shashikala Tapaswi, The Performance Analysis of Honeypot Based Intrusion Detection System for Wireless Network, Int J Wireless Inf Networks, New York, USA, 2015.

[4] R.V. Deshmukh, K.K. Devadkar, ―Understanding DDoS Attack & Its Effect In Cloud Environment‖, Procedia Computer Science 49 (2015) 202 – 210, 4th International Conference on Advances in Computing, Communication and Control (ICAC3'15).

[5] A.K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition, IEEE Transactions on Circuits and Systems for Video Technology 14 (1) (2004).

[6] Abdulkader A. Alfantookh "DoS Attacks Intelligent Detection using Neural Networks" J. King Saud University, Vol. 18, Computer & Information Science.

[7] Stephen M. Specht, Ruby B. Lee, "Distributed Denial of Service:Taxonomies of Attacks, Tools and Countermeasures," Electrical Engineering, Princeton University Princeton, NJ 08544.