International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Self-Defending Approach of a Network

Anshuman Kumar[1], Abhilash Kamtam[2], Prof. U. C. Patkar[3] (Guide)

[1]*Bharati Vidyapeeth's College of Engineering Lavale, Pune-412115, India*
[2]*Bharati Vidyapeeth's College of Engineering Lavale, Pune-412115, India*
[3] *HOD Computer Engineering, Bharati Vidyapeeth's College of Engineering Lavale, Pune-412115, India*

Abstract - *As nature of threat is evolving day by day on networks so it is important that defense method should also evolve. Earlier threats from both internal and external sources were slow in movement and can be easily tracked and destroyed. But now internet worms are spread all across the globe so it is important for security systems and network itself to react to threats instantaneously. The Foundation to Self-Defending Network is important to counter threats on the network. Every device present in network plays an important role in securing the network. This ensures the Data Security and protects the network against internal and external threats. It identifies threats and reacts accordingly to it, Isolates the Infected Servers and systems and then reconfigures the network in response to an attack.*

Key Words: Self Defending Network (SDN), Artificial Intelligence, End-Point Protection, Network Security, Incidence Response.

1.INTRODUCTION

As number of Computer Network is increasing day by day so it is also important to make a network more secure and reliable. As more and more data is flowing through the network, so it increases the security issues as a result more complex and secure protection is required for the network [1]. So it is very important to provide security to both software and hardware components in the network. To make a network more secure a proper analysis should be carried out of all types of threats that can occur in the network. After the analysis is made a proper network design should be made. This Paper introduces the need of Artificial Intelligence in the network Security thus making the Network Intelligent. This paper also introduces a next generation Intelligent Network, a Self-Defending Network (SDN), a network which analyze all known as well as unknown threats which may occur in a network. This Self Defending Network also provide security not only from External threats but also from Internal Threats. A Network that is able to handle large data and information very quickly thus minimizing the threat on the data.

2. ARTIFICIAL INTELLIGENCE

Artificial Intelligence is academic field of study which studies how to create computers and computer software that are capable of intelligent behavior. With the aim of helping or reducing human efforts, it is to execute intelligent activities of mankind with the help of computers, Artificial Intelligence(AI) was developed. Artificial Intelligence is the power of computers to take act intelligently in any situation and respond quickly to any operation or task given to it. Artificial Intelligence also provide the ability to computers to make decisions on its own. However, artificial intelligence academically covers a very wide range of scope involving scores of subjects and nearly any fields of theory and application in which people are engaged [2]. Without artificial intelligence the efficiency of any computer will reduce, also it will increase the human work load. Therefore, any field in technology requires artificial intelligence. The technology developing in the time with rapid change day by day and alteration [2].

3. ANALYZING RISKS

The first step towards building a secure network is to carefully analyze and identify each attack and evaluate the risk introduced on a network. Risk analysis helps in knowing what type of damage may cause on the network by the attacker. It also provides various methodology to prevent the attack before it take place on the network. A proper Risk analysis include:

- Assets identification.
- Identifying the threats.
- Identifying the vulnerabilities.
- Analyzing the Existing Control.

Fig-1: Security Design Steps [1]

To protect assets, all the asset identification is done first. It contains assets like hardware component and software

components. Risk analysis includes the protection of assets and providing the level of protection to the assets. Next step is identifying the threats that may occur on the network. So it very important that proper identification of threat should be done even before the network architecture is built. Identifying the weak links and backdoors is nothing but the identifying the network vulnerabilities. This include security systems, design issues, or the internal control which can be targeted by the attacker which may lead to network breach or violation pf security policies. The final stage in risk analysis is identifying or analyzing the existing control. That means analyzing all the security policies, existing procedures, and backdoors.

4. SELF-DEFENDING NETWORK

Self-Defending Network is an Adaptive Network which remains active all the time thus minimizing the threats and attack on the network. Self-Defending Network helps in creating an autonomous system that quickly responds to any network breech or attack. Every node or system act as a point of defense in the network and all the elements work in synchronization to provide a secure and adaptive system. It is very important to design a very strong security policy to make a network secure. It includes informing all the systems about the security policy and protecting all the network assets from intruders or attackers. Diving the users connected to a network between network administrators and normal end user will help in protecting the network and will also help in providing the level of access to each user in the network. Providing login id and password for user will also help in effectively protecting the unwanted access to the data. Firewall act as security guard of the network which controls the entry points by checking every incoming and outgoing packets, a set of rules should be predefined to properly configure the firewall [1]. Three standard characteristics of Self-Defending Network [3]:

- **Integrated Standard:** Every element in the network act as point of defense and all elements work in synchronization to provide a secure and adaptive network.

- **Collaborative standard:** Different components work together in the network and provide a different level of security to the network. This involves the coordination and communication between components like end-points, Network Admission Control(NAC), security policies, and all other network elements.

- **Adaptive Standard:** Adaptive Security means a behavioral method in which network recognizes new types of threats as they occur and adapts itself accordingly to it so that the same threat does not arise again. This includes machine learning technique which will be discussed in later part of this paper. There is continuous communication between the network intelligence and security systems which increases the effective security of the network and better response to new types threats.

The main components of Self-Defending Networks are as follows:

4.1 End-Point Protection

Protecting the end-point in any network is very important. Any non-sanitized end user connected to a network can become harmful threat to the network. This non-sanitized end user then becomes the weakest link in the network and can easily by targeted by an attacker. For this Cisco has introduced Cisco Security Agent software which is considered as Intrusion prevention tool. Working for the end-points like end users and servers, it is designed to correlate appropriate and suspicious behaviour and prevent new attacks, even before a security patch or "signature" can update the network's antivirus or other security software [3]. Configuring the operating system and the network firewall in a new way can protect the end user's information and data. The security agent detects any kind of malware or worms on the end user systems and protects them by providing security patches and antivirus update. Security agent also provide a secure and efficient data transmission over the network thus minimizing the threat on the end user's system.

4.2 Admission Control

Any user when initially joins the network is provided various security policies and level of access is granted to each user in the network. All these work is done by the Network Admission Control. Network Admission Control assists in determining the level of access which is need to be granted to each user. It also divides the end user between network administrator and end user thus providing the access levels to each user according to its type and priorities. NAC also controls the access by interrogating devices when connected to determine whether they comply security policies or not. NAC uses this information to determine appropriate network admission policy enforcement for every endpoint based on the security state of the OS and associated applications rather than simply on who is requesting access. Besides detecting, analysing, and acting on network behaviour, Cisco Security Agent can track which applications are installed on a single computer or workgroup; which applications use the network; the identity of all remote IP addresses with whom a server or desktop computer communicates; and the state of all applications on remote systems, including user-specific installation information and whether undesired applications are attempting to run [3].

4.3 Infection Containment

It's the ability of SDN to identify unauthorized systems or network attacks as they occur and thus reacting appropriately and minimizing the impact of the breech on the network. It mainly follows these three steps:

4.3.1 Identify Infected Systems

Identifying the infected system in the network is the first step in the containment. Since threats are evolving exponentially it becomes very difficult to identify the infected system due to the dynamic nature of the threat. Self-Defending Network also creates autonomous systems which quickly responds to the systems whenever they get infected.

4.3.2 Contains the Outbreak

Whenever any outbreak or infected system is found in the network it performs following operations to minimize the impact of the outbreak and to contain the outbreak in the network:

- Uses the Automated tool.
- Disables the connectivity.
- Disables the services
- Removes the vulnerability.

4.3.3 Keep Record of every Action taken

It becomes very important to keep record of all the actions that are taken by the network during outbreak so that the network can resume its services from where it had left. Some containment also requires temporary modification or configuration which needs to be removed after the incident. For all these it becomes very important to keep a solid record of each and every actions that are taken.

4.4 Incident Response

It's the services that the Self-Defending Network provides whenever any incident take place in the network. Whenever it finds any incidents in the network, it quickly responds to it provides the appropriate services and takes all the necessary steps that needs to be taken immediately. All the actions are taken by appropriate nodes and these actions are taken in real time. All the nodes work in integration to provide security solution to incident and making the network stronger. It takes the knowledge of the network infrastructure and services, overlaying it with emergency plans, and installing tools and scripts that takes immediate actions whenever any incident takes place.

5. ARTIFICIAL INTELLIGENCE IN SDN

Various methodologies have been introduced or developed in the field of Artificial Intelligence which requires the intelligence of human perspective. It would be impossible to try to give more or less complete survey of all practically useful of Artificial Intelligence methods in a brief survey [4]. Here we have divided different methods and architectures in some categories: constrain solving, machine learning, neural nets, intelligent agents, expert systems. All these fields of Artificial Intelligence are used in cyber defense. These fields also make the Self-Defending Network more reliable towards any attack.

5.1 Intelligent Agents

Intelligent Agents are software component that possess intelligence and quick reaction which make these Intelligent Agent special in Artificial Intelligence: quick reactivity (ability to take quick decisions on its own), adaptiveness (quickly adapts to any changes and works according to it), communication between other Intelligent agents in the network and works with them in integrity. They may have planning ability, mobility, and reflection ability [4]. Using intelligent agents in a Self-Defending Network will effectively defend any attack cooperatively.

5.2 Machine Learning

Learning means improving the knowledge of all known as well as unknown things by extending or rearranging the knowledge base of a system. Machine learning comprises computational methods for acquiring new knowledge, new skills and new ways to organize existing knowledge [4]. There are various problems in machine learning varying by their complexity from simple parametric learning which means learnings values of parameter to complicated symbolic learning like learning symbols, grammar, functions, sometime even learning the behaviour some systems [4, 5]. Machine Learning is very important part in designing a Self-Defending Network as it requires a system which will learn from pervious activities and accordingly predict any harmful activity in the network from all the known as well as unknown sources, thus reducing the human intervention and work load and making a network more secure and reliable.

5.3 Neural Nets

Neural Nets have a very fast speed of operation and a very fast problem solving technique. An artificial neuron is an important part of neural nets. Neural Net are combination of large number of artificial neurons. Thus Neural Nets are fast in parallel learning and makes any decision quickly. They are good in recognizing patterns and also provide various method selection for responding to any attack. Neural Nets can be implemented in hardware as well as software.

Neural Nets are widely used for intrusion detection and prevention. They are also used for DoS detection [6], Computer worm detection [7], spam detection [8] zombie detection, malware classification, and in forensic investigation.

So keeping in mind all the features of neural nets they will be used in Self-Defending Network thus these neural nets will not only detect any kind of intrusion or network breach but will also take all the necessary actions and will also prevent intrusions.

6. PROPOSED WORK

So while planning for future research in network security and cyber defense we will make use of Artificial Intelligence in network security and accordingly will design a network which will be able to defend on itself without any human intervention. The network will take all necessary steps and will make decisions on its own whenever any intrusion, network breach or outbreak is found in the network. This Self-Defending Network will work on existing infrastructure by adding only few more components to make network an intelligent network which will look for every aspects of network attack and will react accordingly.

7. CONCLUSION AND FUTURE SCOPE

So, as the nature of threat is evolving day by day on the network so, it is important that the defense mechanism should also evolve accordingly. The proposed Self-Defending Network will lead to a good, reliable and secure connectivity over a network. This network will also be able to handle any kind of network breach, intrusion or outbreak in the network on its own without any human intervention. This network will be active all the time and will work unobtrusively. This will also make the network more secure and reliable and the availability of the network will also increase. Due to the end-point protection and admission control the end user will be secure thus the Self-Defending Network will remove the exposure of the backdoor to the attacker and will also secure the backdoor. On implementation of this Self-Defending Network, there will be eventually no human intervention in controlling the network traffic. What our vision is that, this Self-Defending Network will not only be able to handle the attack that has taken palace in the network but will also be able to handle the attack that may take place in near future. With the implementation of Self-Defending Network

REFERENCES

[1] Kalaivani Chellappan, Ahmed Shamil Mustafa, Mohammed Jabbar Mohammed, Aqeel Mezher Thajeel, "Layered Defense Approach: Towards Total Network Security", from International Journal of Computer Science and Business Information(IJCSBI), Vol. 15, No. 1. JANUARY 2015.

[2] Yaoxiaoyang, "Study on Development of Information Security and Artificial Intelligence", from 2011 Fourth International Conference on Intelligent Computation Technology and Automation.

[3] Cisco Self-Defending Network
http://www.cisco.com/go/selfdefend

[4] Enn Tyugu, "Artificial Intelligence in Cyber Defense", 2011 3rd International Conference on Cyber Conflict C. Czosseck, E. Tyugu, T. Wingfield (Eds.) Tallinn, Estonia, 2011 © CCD COE Publications.

[5] AK. Ghosh, C. Michael, M. Schatz. A Real-Time Intrusion Detection System Based on learning Program Behavior. Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection, 2000, pp.93-109.

[6] B. Iftikhar, A. S. Alghamdi, "Application of artificial neural network in detection of dos attacks," in SIN '09: Proceedings of the 2nd international conference on Security of information and networks. New York, NY, USA: ACM, 2009, pp. 229-234.

[7] D. Stopel, Z. Boger, R. Moskovitch, Y. Shahar, and Y. Elovici, "Application of artificial neural networks techniques to computer worm detection," in International Joint Conference on Neural Networks (IJCNN), 2006, pp. 2362-2369.

[8] C.-H. Wu, "Behavior-based spam detection using a hybrid method of rule-based techniques and neural networks," Expert Systems with Applications, vol. 36, no. 3, Part 1, 2009, pp. 4321-4330.

BIOGRAPHIES

Anshuman Kumar is pursuing his B.E Degree from Bharati Vidyapeeth's College of Engineering, Lavale, Pune, India. He is being affiliated to Savitribai Phule Pune Unviversity, Pune, India. He is currently pursuing his B.E Degree in Computer Science and Engineering. His current research interest includes Operating Systems, Network Security and Networking.

Abhilash R Kamtam is pursuing his B.E Degree from Bharati Vidyapeeth's College of Engineering, Lavale, Pune, India. He is being affiliated to Savitribai Phule Pune Unviversity, Pune, India. He is currently pursuing his B.E Degree in Computer Science and Engineering. His current research interest includes Artificial Intelligence, Network Security, and Algorithm Design.

Prof. U. C. Patkar has completed his B.E. Degree in Computer Engineering from SSBT College of Engineering, Jalgaon, Maharshtra, India and pursued his degree from North Maharashtra University. He later completed his M. Tech Degree in the field if Information Technology from Bharati Vidyapeeth College of Engineering, Pune, Maharshtra, India and pursued his degree from Bharati Vidyapeeth Deemed University, Pune, India. He then completed his Post Graduation Diploma in Business Management from IBMR College, Pune and was affiliated to Pune University, India. He is currently working as Head of Department (HOD) for Computer Engineering Department in Bharati Vidyapeeth's College of Engineering, Lavale, Pune, India.