International Journal of Research and Review
www.ijrrjournal.com E-ISSN: 2349-9788; P-ISSN: 2454-2237

Review Article

Modern Approaches to Cyber Attack Detection

Ikporo Stephen C.

Department of Computer Science, Ebonyi State University, Abakaliki - Nigeria.

Received: 26/06/2016 *Revised: 09/07/2016* *Accepted: 19/07/2016*

ABSTRACT

The world is quickly developing into a virtual environment known as cyberspace, where individuals can communicate with one another, or search for knowledge to broaden their horizons. However, some individuals use this cyberspace for their own devious actions, targeting unsuspecting individuals for their own enjoyment or profit. Cyber-attacks on computer and network system have continued to threaten the global information infrastructure, targeting data files, services, network or even service port. The most dangerous aspect of these attacks is how sophisticated they have become in recent times, thereby almost defiling all countermeasures always employed to detect and prevent them. Modern approach of cyber-attack detection is an advanced scientific technique deployed to prevent these sophisticated attacks on cyber networks which had become a serious threat to our network and cyberspace. There are some existing approaches used in detecting cyber-attacks on computers and networks such as signature recognition and anomaly detection and others. In this paper, a new approach to cyber-attack detection has been proposed so as to detect any type of cyber-attack. This approach uses attack-norm separation techniques for scientific discovery of data, features and characteristic of cyber signal and noise. Attack profiling and analytical discovery techniques are used to generalize the data, features and characteristics that exist in cyber-attack and norm data. Well established signal detection models are also leveraged in the physical space. It's significant to the society is that it will enables us to take the least amount of relevant data necessary to achieve detection accuracy and efficiency.

Keywords: Cyber Attack, Cyber Space, Threat, Computer Network, Security Detection.

1.0 INTRODUCTION

Cyber-attack can be seen as any type of offensive maneuver employed by individuals or group which targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts. Usually, it always has anonymous originality and either steals, alters, or destroys the target by hacking into a susceptible system. This can be termed a Cyber campaign, cyber terrorism or even cyber warfare depending on the context. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire system. [4]

The security of information and recently cyber attack has attracted much attention from many researchers in recent years that many resources have been deployed in trying to detection attacks on systems. With the increase and reduction of information processing and internet accessibility, organizations are increasingly becoming vulnerable to potential cyber threats such as network cyber attacks. Hence, there is need to secure and safeguard transactions through the use of firewalls, Cyber Attack Detection Systems (CADSs), encryption, authentication, and other hardware and software solutions. With the existence of many CADS, security managers and engineers need to identify

attack network packets primarily through the use of signature detection; i.e., the CADS recognizes attacked packets due to their well-known fingerprints or signatures as those packets cross the network's gateway threshold. According to a recent survey by CERT/CC (Computer Emergency Response Team/Coordination Center), the rate of cyber attacks has been geometrically increasing every year in recent times. Although existing security policies and mechanisms (e.g. firewalls) provide a practical protection against such cyber threats, they are not perfect and usually have inevitable vulnerabilities. In fact, report indicated that every month, assailants make thousands of unauthorized attempts to gain access to these systems, amounting to a nearly continuous assault, [9] Therefore, mechanisms for detecting cyber attacks are of great interest for national defense and security.

Homeland security includes security of system in different areas with modern technology such as; video surveillance, image detection, cyber attack detection and a new homeland security Smartphone app. The existence of the internet society has divided human life into real and virtual world. And with large number of the people spending their life in virtual world, there is much misused of the internet society. Cyber detection may be divided into static and dynamic anomaly detection. A static anomaly detector is based on the assumption that there is a portion of the system being monitored that does not change. Usually, static detectors only address the software portion of a system and are based on the assumption that the hardware need not be checked. The static portion of a system is the code for the system and the constant portion of data upon which the correct functioning of the system depends. For example, the operating systems, software and data to bootstrap a computer never change. If the static portion of the system ever deviates from its original form, an error has occurred or an intruder has altered the static portion of the system. Therefore static anomaly detectors focus on integrity checking. Dynamic anomaly detection typically operates on audit records or on monitored networked traffic data. Audit records of operating systems do not record all events; they only record events of interest. [10]

2.0 Review of Related Literature

Cyber attacks are actions that attempt to bypass security mechanisms of computer systems. Cyber attack detection has been defined as the problem of identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are abusing their privileges. It assumes that a cyber attack will always reflect some deviations from normal patterns. [14]

2.1 Types of Attacks

According to [10] there are a number of techniques been utilized in cyber-attacks and a variety of ways employed to attack individuals or establishments on a broader scale. Attacks are of two categories, Syntactic and Semantic attacks.

a. Syntactic attacks: These are straight forward; it is considered malicious software which includes viruses, worms, and Trojan horses.

Viruses: Viruses are a self-replicating program that can attach itself to another program or file in order to reproduce. The virus can hide in unlikely locations in the memory of a computer system and attach itself to whatever file it sees fit to execute its code. It can also change its digital footprint each time it reproduces making it even harder to track down in the computer.

Worms: This is a self-sustaining running program which does not need another file or program to copy itself. Worms replicate over a network using protocols. The latest incarnation of worms make use of known vulnerabilities in systems to penetrate, execute their code, and replicate to other systems such as the Code Red II worm that infected more than 259 000 systems in less than 14 hours. On a much larger scale, worms can be designed for industrial

espionage to monitor and collect server and traffic activities then transmit it back to its creator.

Trojan horses: A Trojan horse is designed to perform legitimate tasks but it also performs unknown and unwanted activity. It can be the basis of many viruses and worms installing onto the computer as keyboard loggers and backdoor software. In a commercial sense, Trojans can be imbedded in trial versions of software and can gather additional intelligence about the target without the person even knowing it happening. All three of these are likely to attack an individual and establishment through emails, web browsers, chat clients, remote software, and updates.

b. Semantic attack: Semantic attack is the modification and dissemination of correct and incorrect information. Information modification could have been done without the use of computers even though new opportunities can be found by using them. To set someone into the wrong direction or to cover your tracks, the dissemination of incorrect information can be utilized. This is seen as an attack because it can cause al alteration of the overall result of the original program.

2.2 Other types of cyber attacks according to [10] include;

Access Attacks - An attack where intruder gains access to a device in which he has no right for access. When this happens, the attacker can perpetuate his malicious acts.

Denial of Service - Intrusion into a system by disabling the network with the intent to deny service to authorized users Denial of service (DOS) is class of attack where an attacker makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate user access to a machine. A denial-of-service attack generally means attacking the network to bring it down completely with useless traffic by affecting the host device which is connected to the internet. A DOS attack targets websites or services which are hosted on the servers of banks and credit card payment gateways.

Direct-access Attack - A direct-access attack simply means gaining physical access to the computer or its part and performing various functions or installing various types of devices to compromise security. The attacker can install software loaded with worms or download important data, using portable devices.

Spoofing - Spoofing is a cyber attack where a person or a program impersonates another by creating false data in order to gain illegal access to a system. Such threats are commonly found in emails where the sender's address is spoofed.

Privilege Escalation Attack - A privilege escalation attack is a type of network intrusion which allows the user to have an elevated access to the network which was primarily not allowed. The attacker takes the advantage of the programming errors and permits an elevated access to the network.

Social Engineering Attack - An attack by a known or a malicious person is known as social engineering. They have knowledge about the programs used and the firewall security and thus it becomes easier to take advantage of trusted people and deceive them to gain passwords or other necessary information for a large social engineering attack.

3.0 Cyber Security

There are multiple interlocking issues around the field of cyber security. Disjoining the term cyber security helps to situate the discussion within both domains of "cyber" and "security" and reveals some of the legacy issues. "Cyber" is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality. [12,13] According to, [13] it evolved from the term "cybernetics", which referred to the "field of control and communication theory, whether in machine or in the animal". The term "cyberspace" was popularized by William Gibson's 1984 novel, *Neuromancer*, in which he describes his vision of a three-dimensional space of pure information, moving between computer and computer clusters where

people are generators and users of the information. What we now know as cyberspace was intended and designed as an information environment and there is an expanded appreciation of cyberspace today. For example, Public Safety, [6] defines cyberspace as "the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where people are linked together to exchange ideas, services and friendship." Cyberspace is not static; it is a dynamic, evolving, multilevel ecosystem of physical infrastructure, software, regulations, ideas, innovations, and interactions influenced by an expanding population of contributors, [5] who represent the range of human intentions.

As for the term "security", in the literature we reviewed, there appeared to be no broadly accepted concept, and the term has been notoriously hard to define in the general sense. According to, [3] discourses in security necessarily include and seek to understand who securitizes, on what issues (threats), for whom (the referent object), why, with what results, and under what conditions (the structure). Although there are more concrete forms of security (e.g., the physical properties, human properties, information system properties, or mathematical definitions for various kinds of security), the term takes on meaning based on one's perspective and what one values. It remains a contested term, but a central tenet of security is being free from danger or threat. [13] Further, although we have indicated that security is a contested topic, [1] states that one cannot use this designation as "an excuse for not formulating one's own conception of security as clearly and precisely as possible".

Cyber-attacks are the disruption in the normal functioning of computers and loss of private information in a network due to malicious network events (threats), [14] and they are becoming widespread. In the United Kingdom, organizers of the London 2012 Olympic Games believe that there is an increased danger of cyber-attacks that could seriously undermine the technical network supporting everything, from recording world records to relaying results to commentators at the Games.

Professional hackers can be employed by the government or military service or even on their own can be on the search of any computer systems with vulnerabilities lacking the appropriate security software. Once found, they can infect systems with malicious code and then remotely control the system or computer system or computer by sending commands to view content or to disrupt other computers. They need an existing system flaw within the computer such as no antivirus protection or faulty system configuration for viral code to work. Many professional hackers try to promote themselves to cyber terrorists where a new set of rules govern their action. Cyber terrorists have premeditated plans and their attacks are not born of rage. They need to develop their plans step-by-step and acquire the appropriate software to carry out an attack. Usually, they have political agendas and motivation, and hence target political structures; through this their corruption and destructions. [2]

3.1 Factors that necessitate Cyber-attack

According to, [2] there are basically three factors that contribute to why cyber-attacks are launched against a state or an individual: the fear factor, spectacular factor, and vulnerability factor.

Fear factor: The most common factor been employed by cyber terrorist is creation of fear amongst individuals, groups, or societies. The bombing of a Bali nightclub in 2002 created fear amongst the foreign tourists who frequently visited the venue. Once the bomb went off and casualties ensued, the influx of tourists to Bali significantly reduced due to fear of death.

Spectacular factor: With spectacular factors, it is the actual damage of the attack, meaning the attacks created direct losses and gained negative publicity. In 1999 a

denial of service attack rendered Amazon.com unusable. Amazon experienced losses because of suspended trading and it was publicized worldwide.

Vulnerability factor: Vulnerability factor exploits how easy an organization or government establishment is vulnerable to cyber-attacks. An organization can easily be vulnerable to a denial of service attack or a government establishment can be defaced on a web page. A computer network attack disrupts the integrity or authenticity of data, usually through malicious code that alters program logic that controls data, leading to errors in output.

4.0 Process Control Systems (PCS) Security

According to, [7] Process Control Systems (PCS) are used by the Smart Grid to monitor and control physical aspects of the electrical power grid. Traditional PCSs are designed to run in isolated environments with no outside network connection. Hence, typically do not have any security built in. Since these PCSs will be monitoring large geographical areas of the power grid, it becomes an issue for the Smart Grid as there may be many entry points to get into the network. PCSs used in the Smart Grid helps to address these security issues. There are several different kinds of PCS. The most commonly used in the electrical power grid is the Supervisory Control and Data Acquisition (SCADA) system. Since the PCSs will be controlling physical aspects of the electric power grid, the security of these systems is very important. When a computer is compromised only the data on the computer is compromised, and in extreme cases some of the hardware in the computer may be damaged. When a PCS is compromised, multi-million dollar equipment can be physically damaged in addition to data being lost. In extreme cases it can cause human injury or loss of life. The most important security objective of the PCS is availability. The electrical power system must be available at all times, so the PCS controlling the power system must also be always available. The integrity of the PCS is the next important security objective. It will not be able to make correct decisions if it is given false data as input. Confidentiality is the least important security objective. The PCS needs to run in real time, and that means the system must have minimal overhead. Implementing confidentiality may be too time-consuming to meet latency requirements. Security in PCSs has traditionally been disregarded. This has caused them to be designed with limited or no security considerations.

Over time, business requirements have led to corporate networks being connected to the PCS network. Doing this has led to security breaches resulting in physical damage and injuries. The Smart Grid is using PCSs that are connected to a large network which has many access points, and this means that PCSs must address security concerns that large networks have [7]

5.0 Mobile CPS Security

Many cyber physical system applications are implemented on computing devices using mobile ad hoc networks. Before these systems can be used in multifarious environments, the security properties of mobile cyber physical systems must be fully understood. Automotive CPS Security is a kind of safety-critical cyber physical system in which the protection against malicious design and interaction faults is paramount to guaranteeing correctness and reliable operation. Armin Wasicek, et al., introduced aspect-oriented modeling as a powerful, model-based design technique to access the security of automotive cyber-physical systems. [11]

In telecommunication cyber attack have straight forward results. Telecommunication integration is becoming common practice, systems such as voice and IP networks are merging as shown in Figure 1 below. Everything is being run through the internet because the speeds and storage capabilities are endless. Apart from Denial-of-service attacks, more complex attacks can be made on BGP routing protocols or DNS infrastructures. It is less likely that an

attack would target or compromise the traditional telephony network of SS7 switches, or an attempted attack on physical devices such as microwave stations or satellite facilities. The ability would still be there to shut down those physical facilities to disrupt telephony networks. [11]

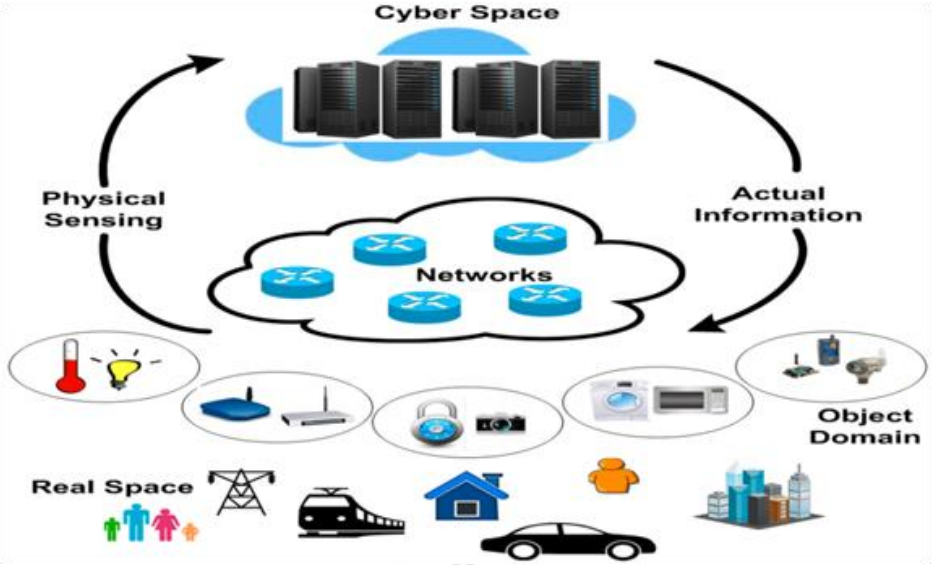

Figure 1: Mobile Physical security Image Source: http//:www.mdpi.com

6.0 Cyber Attacks Detection System Techniques

Modern cyber attack detection systems when employed will help monitor either host computers or network links to capture cyber attack data. Some modern techniques for detecting cyber attacks according to [8] are as follows:

a. Intrusion Detection Systems (IDS)

Here, the host intrusion detection is employed. The Host intrusion detection refers to the class of intrusion detection systems that reside on and monitor an individual host machine. Since these attackers use the cyber space to invade their victims, the Intrusion detectors are switched between the cyber space and the host computer as shown in Figure 2 and 3 below.

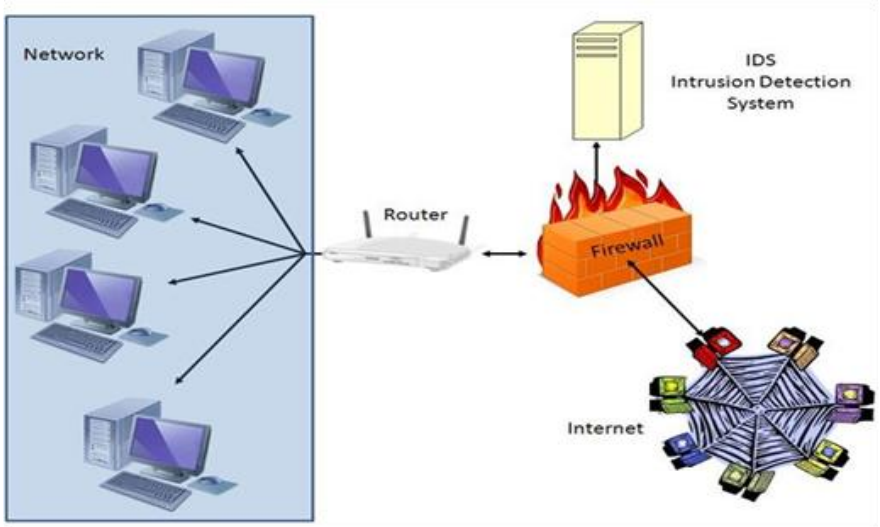

Figure 2: host on Cyber network. Source: http//:www.brighthub.com

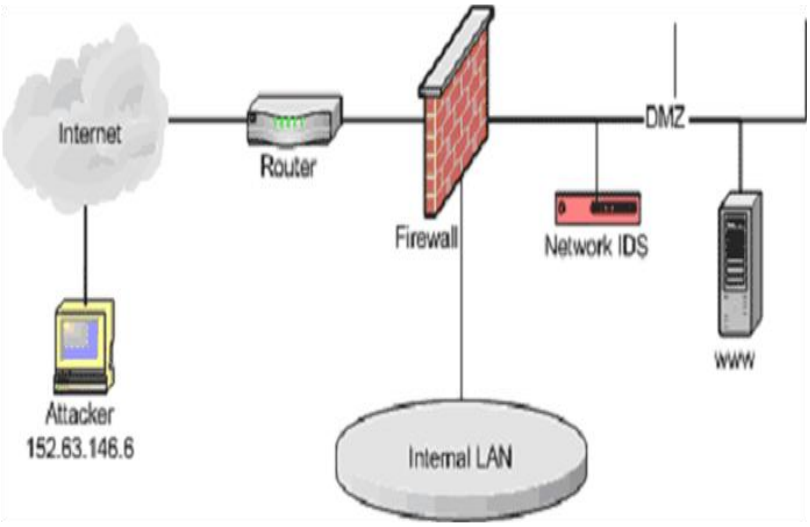

Figure 3: Intrusion detection system. Image source: http//.www.sans.org

Intrusion Detection Systems are categorized into two categories based on detection techniques they use: [9]

Misuse Detection/Misbehavior Detection

Misuse detectors analyze system activity, looking for events or sets of events that match a predefined pattern of events that describe a known attack. Misuse detection technique is the most widespread approach used in the commercial world of IDSs. The basic idea is to use the knowledge of known attack patterns and apply this knowledge to identify attacks in various sources of data being monitored. Misuse (signature) detection is based on the knowledge of system vulnerabilities and known attack patterns. It is concerned with finding intruders who are attempting to break into a system by exploiting some known vulnerability.

Therefore, misuse detection based IDSs attempt to detect only known attacks based on predefined attack characteristics.

b. Signature based Approach

Signature based approach of misuse detection works just similar to the existing anti-virus software. In this approach the semantic characteristics of an attack is analyzed and details is used to form attack signatures. The attack signatures are formed in such a way that they can be searched using information in audit data logs produced by computer systems.

c. Anomaly Detection

Anomaly detectors identify abnormal or unusual behavior on a host network. They function on the assumption that attacks are different from legitimate activity and can therefore be detected by systems that identify these differences. Using statistical method for anomaly detection is one of the oldest techniques applied in IDS research. In this approach, the normal user behavior is first defined based on what is acceptable within the system usage policies. Some statistical modeling technique, Hidden Markov Model (HMM) can be employed on system calls to detect anomalous intrusions.

CONCLUTION

The study of cyber attack detection system is a quite relative to many other areas of system research and this paper tries to x-ray some cyber attacks. Cyber attack detection system varies in the way they use to obtain data in the specific techniques they employ to analyze this data. There is high level cyber attack which demands that a modern techniques or approach such as CPS security be developed in order to beat the newly emerging cyber attacks. This is because, there are still many challenges facing designers, operators and researchers. While the threat of cyber-attacks is growing, many organizations struggle to even get the basic safeguards in place to protect their infrastructure and data. Some of these

modern approaches include Intrusion detection system, Misuse Detection /Misbehavior Detection; Signature based Approach, Anomaly Detection and so on.

REFERENCES

1. Baldwin, D. A. The Concept of Security. Review of International Studies, (1997).
2. Barbara, D. and Jajodia, S., Detecting novel network intrusion using baye estimator, "In proceedings of the first SIAM International Conference on Data Mining (SDM 2001), Chicago, USA.
3. Buzan, B., Waver, O. and De Wilde, J. Security: A New Framework for Analysis. (1998). Boulder, CO: Lynne Rienner Publishers.
4. Lewis, James, United States. Center for Strategic and International Studies. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. (2002). Washington, D.C
5. Deibert, R., and Rohozinski, R., Liberation vs. Control: The Future of Cyberspace. (2010). Journal of Democracy:
6. Canada, "Definition of Cyberspace" defines cyberspace as "the electronic world created by interconnected networks of information technology and the information on those networks, (2010).
7. Dmoroso, E., Guidelines for Smart Grid Cyber Security, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, (2011).
8. Karthikeyan K. R. and Indr. A, "Intrusion Detection Tools and Techniques A survey", International Journal of Computer Theory and Engineering, (2010).
9. Uma .M and Padmavathi M., "A Survey on Various Cyber Attacks and their Classification", International Journal of Network Security, (2013).
10. Singh .S and Silakari, S., "A Survey of Cyber Attack Detection Systems", IJCSNS International of Computer Science and Network Security, (2009).
11. Stiawan, .S and A. H. Abdullah, "Intrusion Prevention System: A Survey", Journal of Theoretical and Applied Information Technology, (2010). Retrieved (2012).
12. Oxford. "Cyber" is a prefix connoting cyberspace and refers to electronic communication networks and virtual reality, (2014).
13. Zarrabi A., "Internet Intrusion Detection System Service in a Cloud", International Journal of Computer Science Issues, vol. 9, (2011). Retrieved (2012).
14. White House, "White House Shooting Suspect's Path to Extremism", (2011). The New York Times. Archived from the original on April 22, 2012. Retrieved January 26, 2015.

How to cite this article: Stephen CI. Modern approaches to cyber attack detection. Int J Res Rev. 2016; 3(7):12-19.

****