International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.247-256
http://dx.doi.org/10.14257/ijsia.2014.8.1.23

A survey of Cyber Attack Detection Strategies

Jamal Raiyn

Computer Science Department
Al-Qasemi, Academic College of Education
Baqa Alqarbiah, Israel
raiyn@qsm.ac.il

Abstract

Homeland security field deals with diverse subjects, audio processing, video surveillance, image detection, geolocation determination, and cyber attack detection. Audio processing and video surveillance area are significant for public places safety and land border area. However the big threat for homeland security is cyber attacks. Cyber terror attacks and cyber crime attacks may move over virtual networks and can get every home. Nowadays, we consider the homeland security field however we set the cyber attack detection area the highest priority in our research. This paper introduces the overview of the state of the art in cyber attack detection strategies.

Keywords: *homeland security, cyber attack*

1. Introduction

The main task of homeland security is to secure the nation from the many threats. Homeland security includes different areas, video surveillance, image detection [1], cyber attack detection and a new homeland security smartphone app. This paper considers the cyber attack detection area. Since exist of the internet society the human life is divided in real world and virtual world. Large number of the people spends their life in virtual world. Many people have misused the internet society. Cyber attacks crime and cyber attacks terror increase exponentially. To save innocent people life we suggest to set ethical rules for virtual world according to real life. Furthermore new security actions are required to protect private life in virtual world. This paper introduces a survey of cyber attacks detection. 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. We add to this definition the identification of attempts to use a computer system without authorization or to abuse existing privileges. The paper is organized as follow. Section 2 introduces the review of cyber attacks types and attacks detection strategies. Section 3 introduces cyber attacks detection source in real-time. Section 4 concludes the paper.

2. Cyber Attack Types

2.1. Denial of Service Attacks:

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.

ISSN: 1738-9976 IJSIA

2.1.1. Remote to Local (User) Attacks (R2L)

A remote to local (R2L) attack is a class of attacks where an attacker sends packets to a machine over network, then exploits the machine's vulnerability to illegally gain local access to a machine. It occurs when an attacker who has the ability to send packets to a machine over a network but who does not have an account on that machine exploits some vulnerability to gain local access as a user of that machine.

2.1.2. User to Root Attacks (U2R)

User to root (U2R) attacks is a class of attacks where an attacker starts with access to a normal user account on the system and is able to exploit vulnerability to gain root access to the system in which the attacker starts out with access to a normal user account on the system (perhaps gained by sniffing passwords, a dictionary attack, or social engineering) and is able to exploit some vulnerability to gain root access to the system.

2.1.3. Probing

Probing is class of attacks where an attacker scans a network to gather information or find known vulnerabilities. An attacker with map of machine and services that are available on a network can use the information to notice for exploit.

2.2. Attacks Detection Strategies

Modern cyber attack detection systems monitor either host computers or network links to capture cyber attack data [6].

2.2.1. Intrusion Detection Systems (IDS)

Host intrusion detection [15] refers to the class of intrusion detection systems that reside on and monitor an individual host machine. Intrusion Detection Systems are categorized into two categories based on detection techniques they use:

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

2.2.3. 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.

2.2.4. Anomaly Detection

Anomaly detectors identify abnormal unusual behavior on a host or network [7]. 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.

[16] applied a statistical modeling technique, a Hidden Markov Model (HMM), on system calls to detect anomalous intrusions. To determine various state transitions that a special UNIX based process goes through from the start to the end, they collected all the system calls specific to that process and applied these system calls to a HMM. Using these state transition sequences, they built database of normal sequences and then monitored system call sequences against this database to detect anomaly.

2.3. Analysis Approach

Currently there are three basic approaches to cyber attack detection. The CADS uses its analysis engine to process this data in order to identify cyber attacks. Modern systems primarily employ three approaches to perform this analysis:

Misuse/misbehavior:

Misuse (signature) detection is based on the knowledge of system vulnerabilities and known attack patterns. Misuse detection is concerned with finding intruders who are attempting to break into a system by exploiting some known vulnerability. Ideally, a system security administrator should be aware of all the known vulnerabilities and eliminate them.

Artificial Immune System

The Biological immune system (BIS) [11] can quickly recognize and detect the presence of foreign microorganisms in the human body. It is remarkably efficient, most of the time, in correctly detecting and eliminating pathogens such as viruses, bacteria, parasites, and in choosing the correct immune response .When confronted with a pathogen, the BIS relies on the coordinated response from both of its two vital parts: the innate system: the innate immune system is able to recognize the presence of a pathogen or tissue injury, and is able to signal this to the adaptive immune system. The adaptive system: the adaptive immune system can develop during the lifetime of its host a specific set of immune responses. For an immune reaction to occur, it is necessary that

i) a cell has been classified as a pathogen and

ii) this cell could cause some damage to the human organism.

This means that the BIS is only reactive with infectious cells, *i.e.*, with pathogens that can indeed cause harm. This demonstrates that a two-way communication, hereafter referred to as co-stimulation, between the innate and adaptive immune systems is common [10, 12]. In the subsequent sections we will introduce and evaluate an approach inspired by the interplay between the innate and adaptive immune system. The goal of this approach is to help suppress false positives and at the same time achieve energy efficiency. The early work in adapting the "Biological Immune System" to networking has been done by Stephanie Forrest [13]. In one of the first BIS inspired works, Hofmeyr and Forrest [13] described an AIS able to detect anomalies in a wired TCP/IP network. Sarafijanovi´c and Le Boudec [8] introduced an AIS for misbehavior detection in mobile ad hoc wireless networks. They used four different features based on the network layer of the OSI protocol stack. They were able to achieve a detection rate of about 55%; they only considered simple packet dropping with different rates as misbehavior. An AIS for sensor networks was proposed by Drozda *et al.*, in [13]. The implemented misbehavior was packet dropping; the detection rate was about 70%.

Anomaly

It assumes that a cyber attack will always reflect some deviations from normal patterns. Anomaly detection may be divided into static and dynamic anomaly detection [8]. 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.

2.4. Classification of Cyber Attacks

The attacker will expect the process to be harmonized in order to infect the system. Synchronization of the steps involved to steal the information leads them to achieve what they expect. The hackers will get their result in time, in step and in their line. An organized form of the methods will be used by the attacker or hacker lead to infect the system very easily. The usage of logically organized methods leads them to get more efficient results. The attacks are regimented with perfect sequence and in such a way that the resulting damage is severe enough to compromise the working of the organization [3-4].

- **Reconnaissance Attacks** Type of attack which involves unauthorized detection system mapping and services to steal data
- **Access Attacks** An attack where intruder gains access to a device to which he has no right for access.
- **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.
- **Cyber crime** The use of computers and the internet to exploit users for materialistic gain
- **Cyber espionage** The act of using the internet to spy on others for gaining benefit.
- **Cyber terrorism** The use of cyber space for creating large scale disruption and destruction of life and property.
- **Cyber war** The act of a nation with the intention of disruption of another nations network to gain tactical and military.
- **Active Attacks** An attack with data transmission to all parties thereby acting as a liaison enabling severe compromise.
- **Passive Attacks** An attack which is primarily eaves dropping without meddling with the database
- **Malicious Attacks** An attack with a deliberate intent to cause harm resulting in large scale disruption.
- **Non Malicious Attacks** Accidental attack due to mis-handling or operational mistakes with minor loss of data.
- **Attacks in MANET** Attacks which aims to slow or stop the flow of information between the nodes
- **Attacks on WSN** An attack which prevents the sensors from detecting and transmitting information through the network.

2.5. Offered Solutions

2.5.1. Embedded Programming Approach

In this method some parts of the processing is performed prior to the CADS. This preprocess will significantly reduce the processing load on the CADS and consequently the main CPU. [4] has reported a similar work by programming the Network Interface Card (NIC). This approach can have many properties including lower computational traffic and higher performance for the main processor. Implementing this approach will make it easier to detect variety of attacks such as Denial of Service (DoS) attack. This is because the NIC is performing the major part of the processing while the main processor only monitors the NIC operation.

2.5.2. Agent based Approach

In this approach, servers can communicate with one another and can alarm each other. In order to respond to an attack, sometimes it can be sufficient enough to disconnect a subnet. In this type of system in order to contain a threat, the distributed CADS can order severs, routers or network switches to disconnect a host or a subnet. There are two approaches in implementing an agent based technology. In the first approach, autonomous distributed agents are used to both monitor the system and communicate with other agents in the network. A Multi- agent based system will enjoy a better perception of the world surrounding it. Zhang et al. [9] report implementing a multi-agent based CADS where they have considered four types of agents: Basic agent, Coordination agent, Global Coordination agent and Interface agents. Each one of these agents performs a different task and has its own subcategories.

2.5.3. Software Engineering Approach

The programming language with its special components will improve the programming standard for the CADS code. CADS developers can enjoy the benefits of a new language dedicated to the CADS development. Such a language will improve both the programming speed and the quality of the final code [10].

2.5.4. Artificial Intelligence Approach

Researchers have proposed application of the fuzzy logic concept into the cyber attack detection problem area. Some researchers even used a multi disciplinary approach, for example, Gomez *et al.*, [16] have combined fuzzy logic, genetic algorithm and association rule techniques in their work. [4] Reports a work where fuzzy logic and Hidden Markov Model (HMM) have been deployed together to detect cyber attacks.

2.5.5. Cyber Attack Detection in Cloud

Developing cyber attack detection strategy in cloud computing service environment should serve the cloud user and cloud providers [5, 9, 14] have introduced a “Cloud Intrusion Detection System Service” to save the client from cyber attacks. The “Cloud Intrusion Detection System Service” is divided into three components: Intrusion Detection Service Agent: Intrusion Detection Service Agent: The agent is integrated inside the user network to collect necessary information. According to the location of the agent, the CIDSS could protect a segment of the network or the whole network. Cloud Computer Service Component, collects messages from agents. It formats all messages and send them to the IDSC according to grouping constrains defined for messages. A secure connection path should be established by CCSC to absorb information gathered by agents. Intrusion Detection Service Component

(IDSC) is responsible for intrusion detection. There are four sub components playing major rule in IDSC.

2.5.6. Cloud Intrusion Detection Service Requirements

There are a number of challenges that must be considered when implementing CIDSS. Some of these challenges are inherent in what an IDS does and others are simply part of the way that a network is configured.

3. Detecting a Cyber-attack Source in Real-Time

Traditional cyber attacks detection involving cyber defense has limitations. The main limitation of misuse detection based IDSs is that they only can detect known attacks accurately. They are unable to detect previously unseen attacks or novel attacks. Moreover, predefine attack specification has to be provided to the IDS for misuse detection, which requires human security experts to manually analyze attack related data and formulate attack specifications. Attack specification can be generated automatically by applying various automated techniques. Most of the misuse detection systems lack this capability. Most of the systems focus on data produced by single source. Desired features for the cyber attack detection system depend on both the methodology and the modeling approach used in building the cyber attack detection system.

3.1. System Model

System model infrastructure is divided into cyber attack detection and cyber immune system as illustrates Figure 1. The proposed cyber attack detection is based on adaptive agent. The cyber immune system is based on behavior analysis. The Cyber Attack Detection and Cyber Immune System (CAD&CIS) is divided into four main layers:

i. Home agent for monitoring:

ii. Social agent for suspect objects detection:

iii. Mobile Agent for tracking of suspect objects:

The Home Agent aims to monitor and control the CAD&IS units. The CAD&IS units include the CAD&IS components and the offered cloud computing services. Home agent is responsible for legal access users.

Social Agent senses the dynamic traffic in the environment. Based on the traffic behavior analysis, the social agent detects the cyber attacks. Social agent makes his decision based on historical information and based on current information.

The Mobile Agent has two tasks: The first task is to search suspects object and to update the CAD&CIS. The second task is to track the suspect objects.

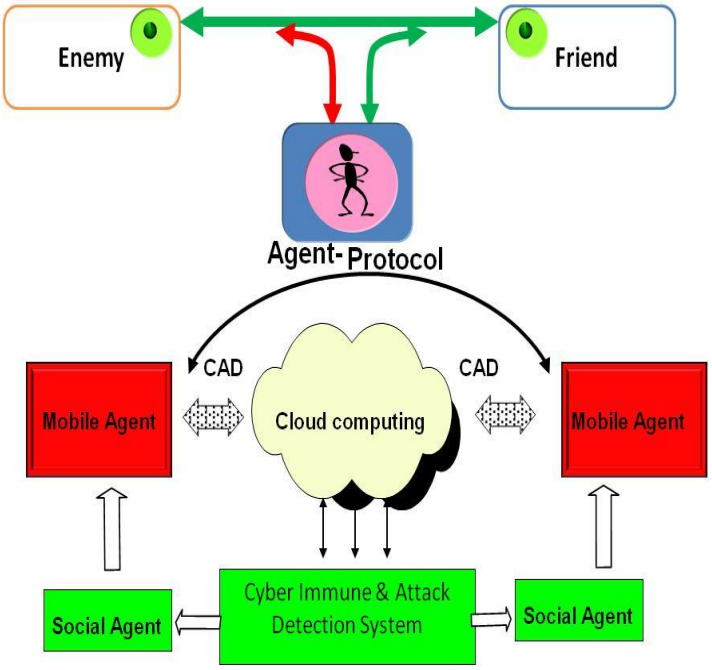

Figure 1. CAD&CIS Infra Structures

3.2. Methodology

Today hundreds of millions of cell phones use GPS and/or WiFi-based technology to support fine-grained location. Tracking exact location (coordinates from GPS or Wi-Fi tracking, postal addresses) is found to be the top concern. In this paper we use the IP address to track exact geographic location of users.

Figures 2 and 3 illustrate the CAD & CIS methodology. Figure 2 describes the home agent task. Home agent task is summarized in identification and tracking of our websites visitors.

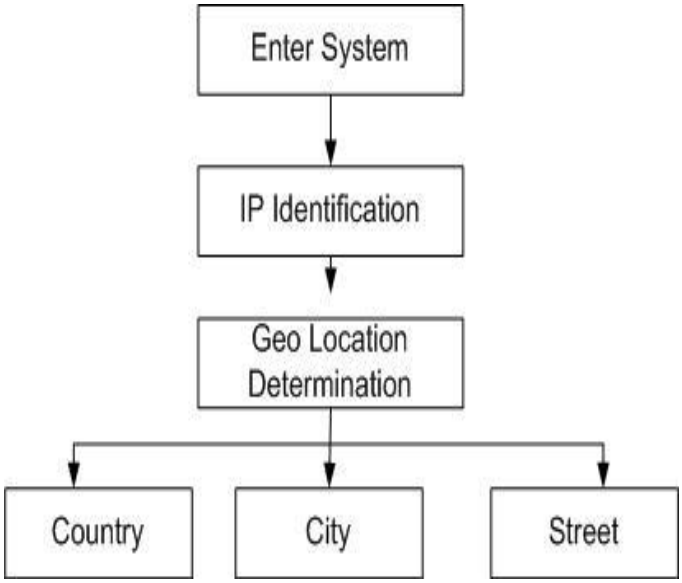

Figure 2. IP tracking Process

Figure 3 illustrates social agent task. Social agent monitors the new users activities.

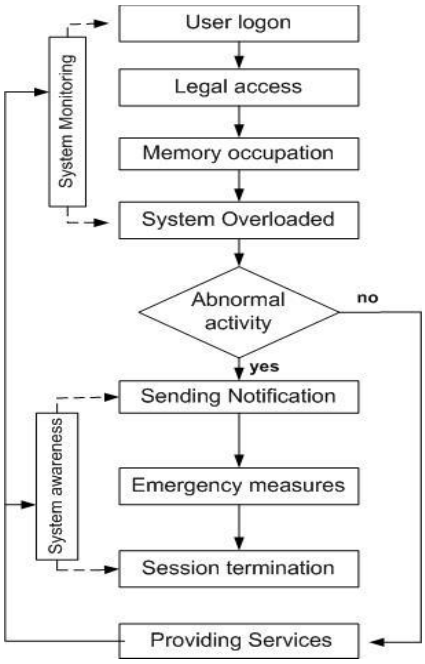

Figure 3. User's Activity Tracking

Mobile agent aims to follow suspect targets over the internet network. Mobile agent uses multiple strategies to carry out the tracking process as shown in Figure 4. For the CAD & CIS it is necessary to collect information security tools.

Figure 4. Roaming Process

4. Conclusion

This paper introduced and discussed different cyber attack detection strategies. We have carried out comparison and analysis between different cyber attacks strategies. Cyber attack techniques have been improved dramatically over time, especially in the past few years. Developing new cyber attack detection schemes is necessary because cyber attackers develop their strategies continuously too. Information fusion from multiple sources required intelligence techniques to characteristic the cyber attackers. It seems that traditional cyber attacks detection schemes may prevent cyber attackers temporary and partial. To overcome the lack of traditional cyber attacks detection schemes we propose new scheme for real-time and short-term response to actual attacks.

References

[1] D. H. Ballard and C. M. Brown, "Computer Vision", Prentice-Hall, Englewood Cliffs, NJ, **(1982)**.
[2] A. C. Bovik, T. S. Huang and D. C. Munson, Jr, "The effect of median filtering on edge estimation and detection". IEEE Trans. Pattern Anal. Mach. Intell., PAMI-9, **(1987)**, pp. 181-194.
[3] M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and their Classification", International Journal of Network Security, vol. 15, no. 6, **(2013)**, pp. 391-397.
[4] S. Singh and S. Silakari, "A Survey of Cyber Attack Detection Systems", IJCSNS International of Computer Science and Network Security, vol. 9, no. 5, **(2009)** May, pp. 1-10.
[5] A. Zarrabi and A. Zarrabi, "Internet Intrusion Detection System Service in a Cloud", International Journal of Computer Science Issues, vol. 9, is. 5, no. 2, **(2013)**, pp. 308-315.
[6] K. R. Karthikeyan and A. Indr, "Intrusion Detection Tools and Techniques A survey", International Journal of Computer Theory and Engineering, vol. 2, no. 6, **(2010)**, pp. 901-906.
[7] A. C. Kim, W. H. Park and D. H. Lee, "A Study on the Live Forensic Techniques for Anomaly Detection in User Terminals", International Journal of Network Security, vol. 7, no. 1, **(2013)**, pp. 181-188.
[8] K. Lee, "Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications, vol. 6, no. 4, **(2012)**, pp. 25-32.
[9] A. Zarrabi and A. Zarrabi, "Internet Intrusion Detection System Service in a Cloud", International Journal of Computer Science Issues, vol. 9, is. 5, no. 2, **(2012)**, pp. 308-3015.
[10] M. E. Kuhl, J. Kistner, K. Costantini and M. Sudit, "Cyber Attack Modeling And Simulation For Network Security Analysis", Proceedings of the 2007 Winter Simulation Conference, pp. 1180-1188.
[11] A. Fuchsberger, "Intrusion Detection Systems and Intrusion Prevention Systems", Information Security Technical Report, ELSEVIER, **(2005)**, pp. 134-139.
[12] C. S. Dangi, R. Gupta and G. S. Chandel, "Cyber Security Approach in Web Application using SVM", International Journal of Computer Application, vol. 57, no. 20, **(2012)**, pp. 30-34.
[13] S. Schaust and H. Szczerbicka, "Artificial Immune Systems in Context of Misbehaviour Detection", International Journal of Cybernetics and Systems: Special Issue on Smart Future of Knowledge Management, Taylor and Francis, vol. 39, no. 2, **(2008)**, pp. 136-154.
[14] J. H. Eom and M. W. Park, "Design of Internal Traffic Checkpoint of Security Checkpoint Model in the Cloud Computing", International Journal of Security and Its Applications, vol. 7, no. 1, **(2013)**, pp. 119-128.
[15] D. Stiawan, A. I. Shakhatreh, M. Y. Idris, K. A. Bakar and A. H. Abdullah, "Intrusion Prevention System: A Survey", Journal of Theoretical and Applied Information Technology, vol. 40, no. 1, **(2012)**, pp. 44-54.
[16] J. Gomez and D. Dasgupta, "Evolving Fuzzy Classifiers for Intrusion Detection", Proceeding of the IEEE Workshop on Information Assurance, United States Military Academy, **(2001)** June.

Author

Jamal Raiyn received the MS degree in mathematics and computer science from Hannover University in Germany, in 2000 and he finished the PhD study at Leiniz university of Hannover in Germany. In June 2010 he finished his Postdoctoral at the Technion in Israel. Since September 2002 till now, he is Assistant Professor in computer science department at the Al-Qasemi Academy in Israel. Since 2010 he is the head of computer science department at Alqasemi College in Israel. Since 2013 is member of EU ICT COST Action IC1304.