A SURVEY OF CYBER ATTACK DETECTION STRATEGIES

Hari prakash Mishra, Sreelakshmi Nair

Abstract—Home security field deals with vibrant subjects, audio processing, image detection, geolocation purpose, and cyber attack detection. Audio processing and video surveillance area are significant for the security of public places and land border area. However, the massive threat for Office of independent agency is cyber attacks. Cyber terror attacks and cyber crime attacks may give practical networks and strength get every home. Nowadays, we consider the Office of independent agency field however we set the cyber attack detection area the most effective priority in our research. This document introduces the summary of the state of the skill in cyber attack detection strategies

Keywords: cyber attack strategy, homeland security

1 INTRODUCTION

The main task of independent agency is to secure the state from the numerous threats. independent agency includes different areas, video surveillance, image detection [1], cyber attack detection and a replacement independent agency smartphone app. This paper considers the cyber attack detection area. Since exist of the net society the human life is split in globe and virtual world. sizable amount of the people spends their life in virtual world. many of us have misused the net society. Cyber attacks crime and cyber attacks terror increase exponentially. to avoid wasting innocent people life we recommend to line ethical rules for virtual world per reality. Furthermore new security actions are required to shield private life in virtual world. This paper shows a survey of cyber attack detection. Cyber attacks are the actions that try to divert the security procedures of computer systems. Cyber attack detection has been defined as the problem of identifying attackers who are employing a system in an unauthorized way and people who have legitimate access to the system but are abusing their privileges. We augment this definition the identification of at-tempts to use a system without authorization or to abuse existing privileges. The paper is organized as follow. 2nd section shows the review of cyber attacks types and attacks detection strategies. 3rd section shows cyber attacks detection source in real-time.

2 CYBER ATTACK TYPES:

2.1 Denial of service attack

Denial of service (DOS) is a type of attack where an attacker makes a computing or memory resource very busy or full to handle legitimate requests, thus denying legitimate user access to a machine.

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

A remote to local (R2L) attack could be a class of attacks where an attacker sends packets to a machine over network, then utilizes the machine's vulnerability to illegally accquire local access to a machine. It occurs when an attacker who has the pliability to send packets to a machine over a network but who doesn't have an account on it machine exploits some vulnerability to realize local access as a user of that machine.

2. User to Root Attacks (U2R)

User to root (U2R) attacks could be a class of attacks where an attacker starts with access to a

normal user account on the system and is ready to use vulnerability to realize root access to the system during which the attacker starts out with access to a traditional user ac-count on the system (perhaps gained by sniffing passwords, a dictionary attack, or social engineering) and is ready to use some vulnerability to realize root access to the system.

3. Probing

- *Hariprakash Mishra is currently pursuing masters degree program in Information Technology in Mumbai University, India, PH-8169575206. E-mail: hariprakashm15@gmail.com*
- *Sreelakshmi Nair is currently a lecturer in Mumbai University, India, PH-8169119781. E-mail:*

Probing is class of attacks where an attacker scans a network to collect infor-mation or find known vulnerabilities. An at-tacker with map of machine and services that are available on anetwork can use the knowledge to note for exploit.

2.2 Attack Detection Straregy

Current cyber attack detection systems monitor host computers or network links to capture cyber attack data.

1. Intrusion detection System.
2. Misuse Detection/Misbehaviour Detection
3. Signature based Approach
4. Anomaly detection

2.3 Analysis Approach

Presently there are three approaches to cyber attack detection. The CADS utilizes its analysis engine to operate this data in order to recognize cyber attacks. Modern systems essentially use three approaches to perform this analysis.

1. Misuse/Misbehaviour
2. Artificial Immune System

a. A cell has been classified asa pathogen

b. This cell could cause some damage to the human organism

3. Anomaly

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 sensibly organized methods leads them to get more well-organized results.

1. Reconnaissance Attack: Type of attack which involves unauthorized detection system mapping and services to steal data
2. Access Attacks: An attack where intruder gains access to a device to which he has no right for access.
3. 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 grip lawful requests, thus denying legitimate user access to a machine.
4. Cyber Crime: The use of computers and the internet to exploit users for materialistic gain
5. Cyber esplonage: The act of using the internet to spy on others for gaining benefit
6. Cyber Terrorism: The use of cyber space for creating large scale disruption and destruction of life and property.
7. Cyber War: The act of a nation with the intention of disruption of another nations network to gain tactical and military.
8. Active Attacks: An attack with data transmission to all parties thereby acting as a liaison enabling severe compromise
9. Passive Attacks: An attack which is primarily eaves dropping without meddling with the database.
10. Mallicious Attacks: An attack with a deliberate intent to cause harm resulting in large scale disruption.
11. NonMallicious Attacks: Accidental attack due to mishandling or operational mistakes with minor loss of data
12. Attacks in MANET: Attacks which aims to slow or stop the flow of information between the nodes
13. Attacks on WSN: An attack which prevent the sensor from detecting and transmitting information through the network.

2.5 Offered solution

1. Embeded Programming Approach:
2. Agent Based Approach
3. Software Engineering Approach
4. Artificial Intelligence Approach
5. Cyber Attacks Detection in Cloud
6. Cloud Intrusion Detection Service Requirements

3 DETECTING A CYBER-ATTACK SOURCE IN REAL-TIME

Conventional cyber attacks detection which involves cyber defense has limitations. The main limitation of fraud detection based IDSs is that they can only 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 needs human security experts to manually examine attack related data and formulate attack specifications. Attack requirement can be generated automatically by applying different automated techniques.

Most of the misuse detection systems has a deficiency in this capability. Most of the systems focal point on data produced by single source. preferred features for the cyber attack detection system depend on both the methodology and the modeling move toward used in building the cyber attack detection system.

3.1. System Model.

This kernel is not based on Linux, also it is not traditional monolithic kernel. It's based upon microkernel which provides

1. Home agent for monitoring:
2. Social agent for Suspect object detection:
3. 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.

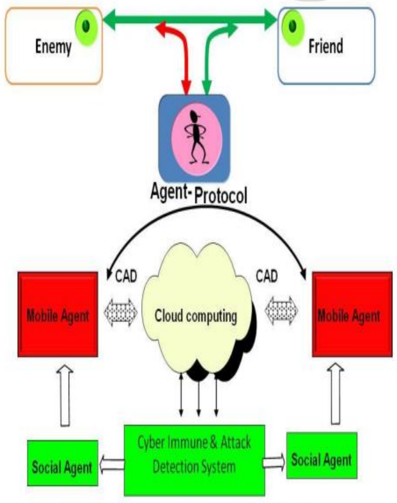

Figure 1. CAD&CIS Infra Structures

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.

3.2. Methodology.

Today many several 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 highest concern. during this paper we use the IP address to track exact geographic location of users.

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

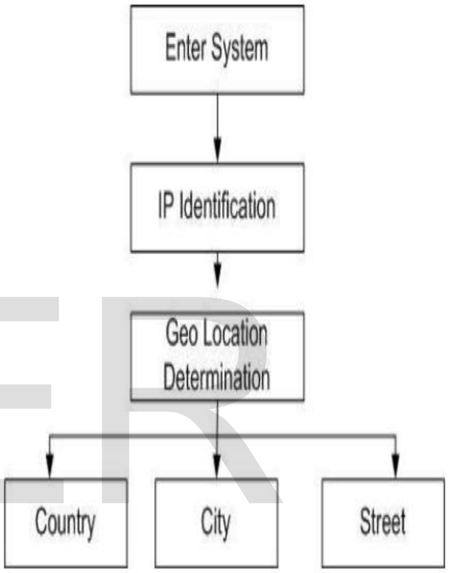

Figure 2. IP tracking Process

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

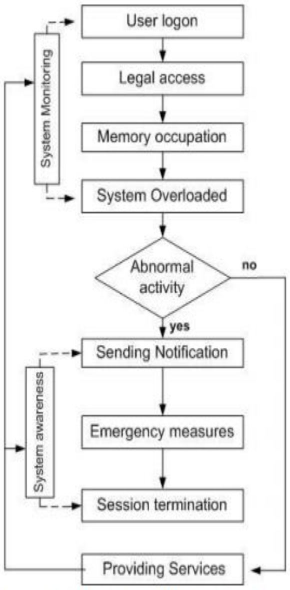

Figure 3. User's Activity Tracking

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

4 CONCLUSION:

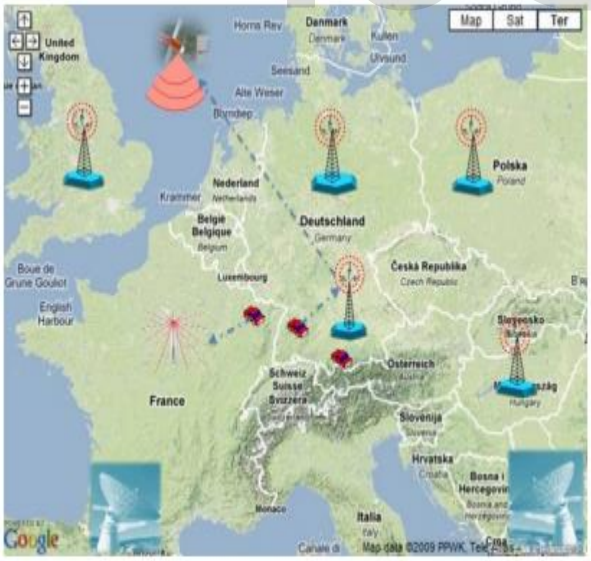

Figure 4. Roaming Process

This paper discusses 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 requires intelligence techniques to characterize the cyber attackers. It appears that conventional cyber attacks detection schemes may avert cyber attackers temporary and partial. To overcome the lack of conventional cyber attacks detection schemes we present new scheme for real-time and short-term response to actual attacks.

5 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.