Comparative Analysis: Network Forensic Systems

Vishvendu M. Bhatt[1] Prof. R. K. Somani[2] Prof. Pankaj Singh Parihar[3]
[1, 2, 3] Department of Computer Science & Engineering
[1, 2, 3]Institute of Technology & Management, Bhilwara (RTU), Rajasthan, India,

Abstract—Network Forensics is scientifically proven technique to accumulate, perceive, identify, examine, associate, analyse and document digital evidence from multiple systems for the purpose of uncovering the fact of attacks and other problem incident as well as performing the action to recover from the attack. Many systems are proposed for designing the network forensic systems. In this paper we have prepared comparative analysis of various models based on different techniques.

I. INTRODUCTION

The firewall and IDS are used to handle the network attacks, but they acquire many limitations like they can't protect systems against attacks that bypass them, they can't protect the systems against internal threats, and they are not capable of perceiving new attacks. The a) Analysis b) Examination and c) Reconstruction of an attack cannot be based on the firewall logs and IDS alerts.

The preventing mechanism performs investigation and also traces back the source of attack and prosecutes the skilful attackers. Such preventing mechanism is provided by Network forensic.

Network forensics is the science that requires the network setup i.e. network with security mechanisms and policies that deals with perceiving, accumulating, storage and analysis of network traffic, if there is an anomaly in the traffic and if the anomaly can be an attack, if it is an attack, then rule information and investigation is performed. At the end action is performed to implement the rule and restrict the future attacks.

Network forensics is not another term for network security [1]. It is an extended phase of network security as the data for forensic analysis are accumulated from security products like firewalls and IDS. The outcomes of this data analysis are utilized for the further investigation of attacks.
Network security protects system against attack while network forensic focuses on recording evidences of the attacks. Network security products are generalized and look for possible harmful behaviours. This monitoring is a continuous process and is performed all through the day. But, network forensics involves post-mortem investigation of the attack.

Network forensics is a natural extension of computer forensics [2]. Computer forensics involves preservation, identification, extraction, documentation, and interpretation of computer data. Network forensics evolved as a response to the hacker community and involves capture, recording, and analysis of network events in order to discover the source of attacks.

II. BACKGROUND

A. Network protection approaches

Networked computers are playing very important roles in our daily life as well as in our business. As nodes of the vast network, the networked computers are more vulnerable than ever before. Network protection approaches are required to protect the networked computer. These approaches can be classified in two categories: Defensive Mechanism and Preventive Mechanism.

1) Defensive Mechanism

Defensive mechanisms are used to prevent the network from attacks. These types of approaches typically find out network vulnerabilities and then block any malicious communication from outside.

Current solutions for defensive approach include Firewall and Intrusion Detection System (IDS); former is used for protection and the later for recognition. Firewalls control traffic that enters a network and leaves a network based on source and destination address and port numbers. It filters malicious network traffic according to the firewall rules. But, it is difficult to find update the signatures of all vulnerabilities as new vulnerabilities will always keep occurring. Firewalls are also limited on the amount of state available and their knowledge of the hosts receiving the content. The other shortcomings of firewalls are:

1) It cannot protect against attacks that bypass it, such as a dial–in capability.
2) It is at the network interface and does not protect against internal threats.
3) It cannot protect against the transfer of virus–laden files and programs.

Intrusion Detection System (IDS) [3] are primarily for learning, perceiving and reporting attacks as they happen in real time and have no evidence gathering feature. IDSs are of two types – signature based (misuse) recognition and statistical based (anomaly) recognition. Pattern matching is done in signature based IDS to perceive intrusion signatures. It cannot perceive new attacks but has a low false positive rate. Anomaly based IDS does activity monitoring and is able to perceive new attacks but has higher false positive rate. The other shortcomings of IDS are:

1) They increase the complexity of network security management.
2) They must know a priori the signature or anomaly pattern.

B. Preventive Mechanism

As the defensive approaches have limitations, the other approach of network protection becomes more important [4]. This approach does not block the network crimes but accumulate enough evidence of these crimes. Network criminals will be punished for their illegal actions thereby

providing a deterrent to online crime. These methods are called network forensics.

C. Network forensics

Network forensics deals with the capture and analysis of the trace and log data of network intrusions from the current network security products and provides information to characterize intrusion or misbehaviour features. The power of various network forensic analysis tools available as open source can be integrated so that the investigator can have an edge over the attacker. The storage to handle large volumes of data and computing power to analyse the same is now available at cheaper rate. An effective network forensic system will increase the cost of the network crimes for the attacker and thus reduce network crime rates.

As it was concerned before, there are two major purposes for network forensics: one is to enhance network security; the other is to get evidence for legal issues. Therefore, there are two types of network forensics. In some circumstances, the focus of network forensics is only for security enhancement. The analysis of data is to discover some characters of the network attacking and to utilize them guiding the strategies and managements of firewall or intrusion detection system. Thus, they can be captured and obtained in the process without rigid legal principles. We call it GNF - General Network Forensics. The other is SNF– Strict Network Forensics, which is the intersection between the computer science and forensics science [5]. It has strict forensics purpose and its result can be used as evidence. It has more rigid criteria in the requirement of the legal validation than the GNF. In SNF processes include many steps that must satisfy the legal principles. For ensuring these legal requirements in the process, some computer and network techniques need be utilized.

We describe the conceptual model of NF as a set of processes, that is:

NF {Pi [Tj, Lk] | i, j, k 1, 2}

NF: Network Forensics;

Pi: Processes;

Tj: Techniques/Method/Approaches/Systems/Tools;

Lk: Legal principles

This model means network forensics is not a single product, system, or tool set, but a process involving many products, systems and tools. The more rigid legal principles satisfied, the more rigid evidence obtained. Different purpose of network forensics needs different requirement of legal principles. If there are more satisfactions of the legal principles, the GNF will become to SNF. SNF always need the tools and manual behaviour with the authority, which are provided by the official authority originations. In current conditions, with no general agreements in the cyber law and the delay of the respective rules, the GNF may maintain a long time, not only in law enforcement communities but also in the civil or enterprise communities.

In other words, GNF may have more non-law enforcement applications than SNF, especially if the attackers are from the different countries or in the conditions that there is no law to punish the attacker even if you get the evidence. In this circumstance, perusing the rigid evidence seems to be wasteful, and then perusing security intelligence or knowledge from the attacking data seems to be more useful.

There are two ways of developing a network forensic process. One way is to reactively use traditional security products like firewalls & intrusion detection systems, analyse the data and investigate. The other way is to proactively lure the attacker by means of honeynets [6] or greynets [7] to observe the attack patterns and create behavioural profiles of attackers and their exploitation mechanisms.

Honeynet is a highly controlled network of computers, designed in such a way that they will be attacked and all activity is captured.

A variant of a network, consisting of a region of IP address space that is sparsely populated with 'dark net' addresses interspersed with active (or 'lit') IP addresses.

D. Network forensics systems can be of two kinds [8]:

1) "Catch-it-as-you-can" systems, in which all packets passing through certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage.
2) "Stop, look and listen" systems, in which each packet is analysed in a rudimentary way in memory and only certain information saved for future analysis. This approach requires a faster processor to keep up with incoming traffic.

E. Network forensic analysis tools

Network Forensic Analysis Tools (NFATs) [9] allow administrators to monitor the networks, gather all information about anomalous traffic, and help in network forensics. NFATs synergizes with IDSs and firewalls making preserving long term record of network traffic possible and allowing quick analysis of trouble spots identified by IDSs and firewalls.

A few functions of an NFAT

- Network traffic recording and analysis
- Network performance evaluation
- Data aggregation from multiple sources
- Anomaly recognition
- Determination of network protocols in use
- Recognition of employee misuse of resources
- Security investigations and incident response
- Intellectual property protection

1) The commercial NFATs available in the market are – Net Intercept, NetPerceiveor, Net Flow, Silent Runner, EnCase, and Visual Route.
2) The open source / freeware NFATs are – TCPDump / Libpcap / WinDump, Wireshark , Snort , Nmap , P0f , Tcpstat , Tcptrace, Tcpflow
3) The following commands are inbuilt in many modern operating systems and are useful for Network Forensics – Nslookup, Traceroute, Netstat, Nbtstat, Whois, Ping, Wget, Dig.

III. NETWORK FORENSICS SYSTEM

Generic Network forensic System includes the following steps [10]:

1) Identification
2) Preservation
3) Accumulation

4) Examination
5) Analysis
6) Presentation
7) Incident Response.

A. Identification

Recognizing an incident from indicators and determining its type. This is not explicitly within the field of forensics, but significant because it impacts other steps [11].

Preservation – isolate, secure and preserve the state of physical and digital evidence. This includes preventing people from using the digital device or allowing other electromagnetic devices to be used within an affected radius. Accumulation – record the physical scene and duplicate digital evidence using standardized and accepted procedures.

B. Examination

In-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating evidence which can be potential, possibly within locations which are unconventional. Construct detailed documentation for analysis.

C. Analysis

Determine significance, reconstruct fragments of data and draw conclusions based on evidence found. It may take several iterations of examination and analysis to support a crime theory. The distinction of analysis is that it may not require high technical skills to perform and thus more people can work on this case.

D. Presentation

Summarize and provide explanation of conclusions. This should be written in a layperson's terms using abstracted terminology. All abstracted terminology should reference the specific details.

Incident Response – The response to crime or intrusion perceived is initiated based on the information gathered to validate and assess the incident.

This work analyses a process model for Network Forensic that meets the following requirements:

1) The model must be based on existing theory for physical crime investigations.
2) The model must be practical and follow the same steps that an actual investigation would take.
3) The model must be general with respect to technology and not be constrained to current products and procedures.
4) The model must be specific enough that general technology requirements for each phase can be developed.
5) The model has to be abstract that can apply to law enforcement investigations, corporate investigations, and incident response.

A. Distributed systems based Network Forensic System

Internet and LANs are distributed in nature and networks attack events are logged in clients at various locations. There is a need to these logs, fuse them and analyse on a central server. A general scheme for the frameworks is shown in Figure 1 [5].

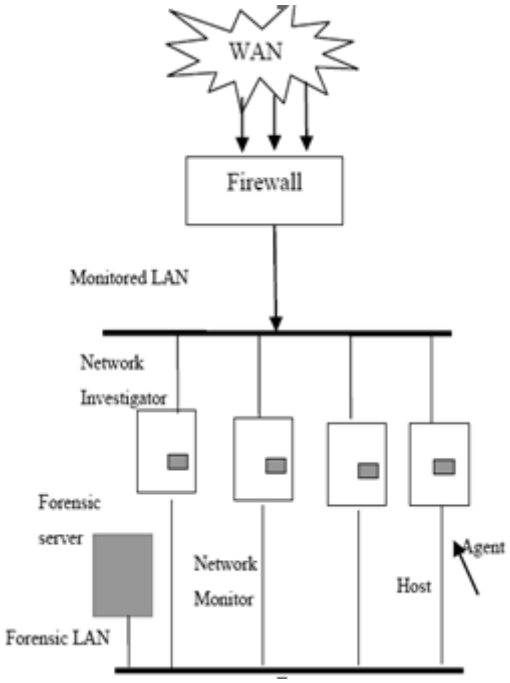

Fig. 1: A general schema for Distributed Network Forensic Systems [5]

B. Soft computing based Network forensic System

The soft computing implementations are used to analyse captured data and classify the attack data. Neural network and Fuzzy tools are used for validation of attack occurrence. A general scheme for the fuzzy logic based system is shown in Figure 2[4].

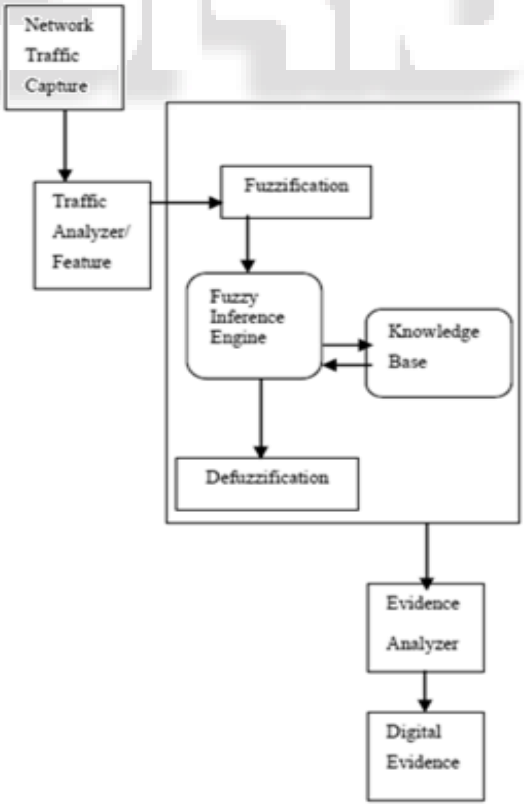

Fig. 2: A general scheme for soft computing based network forensics system [4]

C. Honeypot based Network forensic system

Honeypot based system is used to attract the attackers so that their process methodology can be observed and analysed to improve defence mechanisms.

IV. COMPARATIVE ANALYSIS

In distributed model the capturing of packet is on multiple hosts while in Soft computing model it is on the single host. Distributed model decision making is based on statistical data while in it is based on non-statistical data. Time and cost involve in forensic analysis is less in soft computing model compare to distributed model. In soft computing model, if the rules are such that we can differentiate between an attack and legitimate traffic then we get desirable results. In distributed model it is very hard to differentiate between an attack and legitimate traffic, so desirable results are not possible every time. All network traffic is captured in distributed model; while in soft computing approach some data may be lost due to centralize capturing system. Incident response can be easily handled in soft computing model compare to distributed model.

Honeypot based model is generally used to improve the defensive mechanisms because they attract the attackers so that the process methodology can be observed and analysed. While distributed model and soft computing based model are mainly used for the preventive mechanisms.

Honeypot based model cannot be used for investigation purpose, while distributed based model and soft computing model can be used for investigation because the evidence gathering facility is available in these models.

V. CONCLUSION

Network forensics ensures investigation of the attacks by tracing the attack back to the source and attributing the crime to a person, host or a network. It has the ability to predict future attacks by constructing attack patterns from existing traces of intrusion data. The incident response to an attack is much faster. The preparation of authentic evidence can be admissible into a legal system is going to be facilitated.

We have analysed and compared different approaches used for network forensic system. We found that no one covers all characteristic of network forensic system. Distributed model is efficient in capturing the complete network traffic. Soft computing model is efficient in differentiating the attack and legitimate traffic. Honey pot model is helpful in improving the defensive mechanism.

REFERENCES

[1] V. Broucek and P. Turner, “Forensic computing: Developing a conceptual approach for an emerging academic discipline,” 5th Australian Security Research Symposium, July, 2001.
[2] H. Berghel, “The discipline of Internet forensics,” Communications of the ACM, vol. 46, no. 8, Aug., 2003, pp. 15–20.
[3] S. Axelsson, “Intrusion Detection Systems: A Survey and Taxonomy,” Dept. of Computer Engineering, Chalmers University of Technology, Mar., 2000.
[4] Z. Liu and D. Feng, “Incremental Fuzzy Decision Tree-Based Network Forensic System,” Proc. Int’l Conf. Computational Intelligence and Security (CIS 2005), LNAI 3802, Springer, 2005, pp. 995-1002.
[5] W. Ren and H. Jin, “Distributed Agent-based Real Time Network Intrusion Forensics System Architecture Design,” Proc. IEEE 19th Int’l. Conf. Advanced Information Networking Applications (AINA 2005), pp. 177–182.
[6] L. Spitzner, “Honeypots: Definitions and Value of Honeypots”, http://www.trackinghackers.com/papers/ honeypots.html
[7] L. Spitzner, “Know Your Enemy: Defining Virtual Honeynets”, http://www.honeynet.org
[8] S. Garfinkel, “Network Forensics: Tapping the Internet” http://www.oreillynet.com/pub/a/network/ 2002/04/26/ nettap.html
[9] V. Broucek and P. Turner, “Forensic computing: Developing a conceptual approach for an emerging academic disciple Australian Security Research Symposium, July, 2001.
[10] Emmanuel S. Pilli “Network forensic frameworks: Survey and research challenges” Journal of Elsevier Ltd. 2010.
[11] Bura.brunel.ac.uk/bitstream/2438/7651/1/Full text Thesis.pdf by K Shanmugam - 2011

