ABSTRACT

In the modern world, where most of the population is connected to the internet via smart devices, the surface for committing crimes and being attacked by hackers have been increased drastically. Number of cybercrimes keep increasing and may ramp up when IoT, M2M, 5G and other new network technologies become more popular in coming years. The electronic crimes that involve the use of computer networks are considered the most complex category. After an attack is identified on a network, there is a necessity for computer forensics to investigate and gather digital evidence to bring to justice. Network forensics is dealt with the dynamic and volatile information instead of static/stored data. Hence, highly sophisticated techniques are required for instantaneously tracing down criminals network activities. A honeypot tool can be used to trap intruders and collect essential information on the crime activities. Classification of network forensics, reviews on emerging network areas, intrusion and prevention methods, attack detection process, network forensic process, reviews on various NFATs, survey on network forensic approaches are incorporated in this paper.

KEYWORDS

Cyber Forensics, Network Forensics, Digital Security, Live Forensics Mechanisms, NFAT, Honeypot

1 INTRODUCTION

Computer forensic experts often face difficulties during data collection from a network to aid in forensic investigation. The crime scene constantly changes and as the traditional crimes reduce in number, the cyber crimes incidents are occurring more frequently. To comprehensively solve the emerging network problems through network forensics, understanding the context of forensic investigation and the general nature of emerging networks is the key issue.

Network forensics is a scientific field that deals with the collection, recovering and the examinations of network events for the purposes of establishing sources of security attacks. This phenomenon is useful in the identification of unauthorized access to computer network systems and is an investigative tool in case of such occurrences. According to Alzaabin [1], network forensics plays an investigative role at network level, the issues that take place or have occurred within an information technology system. The major components of network forensics include intrusion detection through logging and correlating with the process. Network forensics plays a primary role in the provision of sufficient evidence to allow the perpetrators of crime to be successfully persecuted. Practical application of network forensics in emerging networks could be present in areas such as email investigation, hacking, insurance companies, fraud detection, drug trafficking, software piracy, credit card cloning, electoral law, discrimination and sexual harassment [2].

This study aims at conducting a literature survey to ascertain the emerging network forensic areas and identify effective architectures for maintaining network security. The process for network attacks detection, network forensic process and the essential tools for network forensic analysis shall also be analyzed to compile the study. Questions of network security issues and attacks and the investigation mechanisms used in a network security accident will also be discussed in the study. Concerns as whether network forensic mechanisms can be used in eliminating network security issues and attacks will also be considered in the research.
2. BACKGROUND

The word computer crime was first used in 1976 by Donn Parker in a book “crime in computer” [12], [13] that it is referred as dealing with unauthorized modification or deletion of data in a computer system [14]. Nevertheless, FBI was established first actual computer analysis and response team in 1984 to conduct advanced digital forensic investigation of the crime scenes [15]. It was in 1986 the first complicated digital forensic investigation case was executed, chasing a hacker named Markus Hess [16]. Mr Hess had intruded to the LBL, the Lawrence-Berkeley-National-Laboratory. It was detected and investigated by Mr. Clifford Stoll. There wasn’t any standard digital forensic investigation framework in place at the time of the incident, so Stoll had to carry out the investigation on his own. As Stoll’s objective was discovering the identity of the intruder, he didn’t alter anything in the system and only collected the possible traces. He finally managed to discover the identity and location of the attacker by tracking the hacker for many months using alarms which send notification when the attacker was active with the cooperation of FBI and Telco Company. The case became a big issue since it was involved academic and individual bodies in U.S, Germany and military bodies [17]. Day by day improvement of digital devices makes digital crime more complicated than it was in 1986. Our augmented dependency on latest networked technologies and the prevalent inter-connectivity of systems used in our networked modern world are potentially be exploited for criminal purposes (e.g. malware, hacking, phishing, theft of trade secrets & intellectual properties etc.). There are basically two approaches for network protection. 

Defensive Mechanism is used to defend from intruders by blocking malicious communications on network. Tools like Firewall, IDS are used by this method. Firewalls control network traffic according to the rules set, but has many limitations. IDS is primarily a real time system for detecting and reporting attacks as it happens on the fly, however it has no evidence gathering capability. Preventive Mechanism will not block the network attack, but tries to prevent it by access control or authentication. Reliable and comprehensive network security and forensics architecture are essential in maintaining security of the emerging networks.

2.1 Definition

Network forensics is a science that monitors and analyzes network traffic, aiming at detecting malicious network activities and preserving the trace to produce as legal evidence at court. It deals with capturing, recording and analyzing of network traffic in order to discover the source of attack and the criminals behind it. From the existing network security products and tools, network log data are collected, analyzed for attack classification and investigated to trace through the perpetrators. This process can bring out deficiencies in security products which can be utilized to guide deployment and improvement of these security tools as well. The scope of network related incidents should be quickly determined and also be able to rewind the breach by the forensics investigator so that they can detect where to look for the potential evidence. Network forensic investigator will require the same thought process and skill set as hackers in order to detect why and what has happened and also to identify the motivation for the crime. Different networks may be spanned across multiple geographical zones and various jurisdiction, which demands the use of absolute trusted timestamps to make sure the integrity and authentication of timestamps for each portion of network evidence ensuring that all jurisdictions collaborate. The network data will be available in both real time and off line modes, the former requiring the ability to pick and analyze data on the fly. The amount of data could be massive due to the increasing size of network bandwidth and also it could involve various different protocols. A protocol could in turn involve multiple layers of signals. The current available set of forensics tools may not be able to handle the real-time and huge data volume. Various techniques are required for instantaneously tracing criminal’s network activities on computers and for mapping the networks topology.

For any cyber-attack, an evidence trajectory would be left in IDS - intrusion detection systems, firewalls, proxies, routers and within the network traffic. Hence, there is an increasing need for investigators to analyze network traffic, events,
logs, netflow and digital device log, in order to discover how an attack was carried out. Such activities could lead in reconstruction of a crime and eventually the identification of the criminal(s). Rigorous methodology and set of procedures for conducting network forensics and investigations are very much required in place. However, the increasing use of networked technologies, fast advancing networking technologies and the need to deal with volatile and dynamic live data, complicates the efforts to identify, collect and preserve evidence data in a timely fashion.

In order to keep up to the pace with the modern changing face of criminal activities and its growth, it is important for the forensic research and practitioner communities to have an in-depth understanding of the types of artefacts that are likely to remain on network and on networked devices as well as the capability to undertake data collection and acquisition in well-paced and in a forensically sound manner.

Network security is not another term for network forensics. Network forensics is an extended phase of network security. Network security protects systems against attacks whereas network forensics focuses on capturing evidences of the attacks. Network forensics is considered as an extension of computer forensics. Monitoring is a continuous process. However, network forensics involves post mortem investigation of the attack and is initiated post crime notification. It is case specific since each crime development is different and the process is time sensitive.

2.2 Classification

Network forensics can be classified into two types: “Catch-it-as-you-can” systems, whereby all the packets that are passing a specific traffic point are captured and analyzed subsequently in batch mode. This method requires lots of storage space as it captures volumes of data. Also, searching and finding required information from the stored data is a big overhead. “Stop, look and listen” is another network forensics system that analyzes information in a rudimentary manner in memory and only certain information is saved for future analysis [3]. Figure 1 depicts the classification of forensics.

It is often a long and tedious process that requires standard operational procedures for the management. In order to come up with a standard operating procedure for network forensics in emerging networks, it is recommended to have a standard investigation image for system. This image should not be of a bit stream and do not contain all the standard applications used. When an intrusion incident occurs, the vulnerability of the system should be fixed to prevent any chances of attacks. All the volatile data should be acquired through live acquisition before the system is switched off during the development of the standard procedure for network forensics [5]. Additionally, a compromised drive should be acquired and an image of it is taken. Comparison of forensic images should be done and hash values properly checked to ascertain if there are any changes in them [5].

Traditional vs Live - Live forensics (forensics on a system that cannot be switched off, as in the critical systems) and the attribution root question (linking the criminal activities to the convicts behind it) are examples of issues that requires additional research. The traditional forensics and Live forensics have common features, where both of them are looking for similar artifacts on a system. However, the differentiator with live response is that the artifacts are discovered on a live running system against an active adversary. With traditional forensics, images are taken of volatile memory and hard disks before being analyzed. Imaging alone can take many hours and then the images should get processed and indexed to allow for keyword searches. Obtaining and then processing the image could take a day or longer with large capacity disks. With live response, there won’t be any scope for imaging or processing that has to occur, everything will be real time. This would dramatically improve the response time in identifying and quantifying a
threat. The quicker the threat is identified, the quicker it can be contained and remediated.

3. LITERATURE REVIEW

3.1 Emerging Network Forensic Areas

Network forensics plays an important role in the emerging network areas such as Machine-to-machine (M2M), 5G and Internet of Things (IoT).

**M2M** - The Internet in achieving intelligent interactions between machines having different terminals uses the Machine-to-Machine networks. This emerging network is composed of equipments, back-end systems, transmission links and front-end sensors. The front end sensors helps in the collection and transmission data to the back end systems that is overhauled and the back end nodes transmits information to back end control system. When the M2M networks are attacked, the terminals it is associated with becomes affected and the network is eventually paralyzed and cannot function. The security issues of M2M are attracting many concerns as the encounter of several attacks, hence, the need for an elaborate forensic expertise arises. Network security architectures and protocols are evolving to counteract the challenges experienced by emerging networks. This evolution is key in the unauthorized access prevention leading to security improvement [18].

**5G** – Even though, the specifications of the 5G is still not finalized, but the technology is expected to be the fastest speed as high as 10Gbps. The new technology would lead to ultra-low latency applications, high volume data rate applications, network of network applications. Real time threat detection and network isolation are going to be a big challenge for 5G networks. Interoperability and diversity in networks increase attack surface and motivation of attacks. Forensics of such a superfast network would be a nightmare for the experts in coming years. [31]

**IoT** - The development and advancement of the Internet and other smart electronic systems have led to the emergence of computing prototypes such the Internet of Things (IoT). The IoT has been considered as the future of Internet works with other emerging networks such as M2M communication and Radio Frequency Identification (RFID). IoT has the primary mandate of adequately securing data exchange between real world applications and devices. The paradigm of digital forensics in line of Internet of Things is challenging and diverse and the traditional model of forensics does not adequately address the recent IoT environment [19].

3.2 Preliminaries of Network Security and Forensics.

*Intrusion detection and prevention systems* are used to monitor network traffic and activities of the network system for any malicious activities. Intrusion prevention system takes action by sending an alarm, resetting connection, dropping malicious packets or blocking traffic from any offensive IP addresses. Intrusion prevention System (IPS) is also essential in cyclic redundancy check (CRC) errors correction, eliminating extra features and network layer options as well as unnecessary packet streams [18].

*Honeypots and Forensics* - With the rise of cyber-attacks, Honeypots have been considered one of the best in network crime forensics, warm attack detection and other aspects of active defense methods. A honey pot is a trap network that is static and is effective for attackers who are reckless. When the attackers are however aware of the existence of the honey pot, their functionality becomes degraded. In order to increase the functionality and persuasiveness of the Honeypots, the behaviors of the attackers need to be collected and stored in a safe place [11]. Honeypots are copies of the real servers and are often used to simulate real service through the coordination of various modules. These modules include data acquisition module, remote storage module, detection module and implementation module. Data acquisition module captures and collects the activities of intruders or attackers. The remote storage module in the other hand backs up the network system remotely and captures data to the log servers and keeps the information without any further modification. Detection module protects the host and records the invasion process. Implementation module on the other hand is used in the simulation and
protection of the host and prevents attacks from any intruders.

**Surveillance and Vulnerability Scanning** - During a forensic event, the surveillance and vulnerability scanning systems are usually not stored through the SIEM system. Surveillance & vulnerability systems are potential parameters in attacks minimization via firewall rule adaptations or alterations. The above mentioned preliminaries of network security and forensics helps in the detection of all network anomalies and are useful in the identification of all the attackers. After the attackers have been traced by these systems network forensics then follows. This process experiences challenges such as the loss lag of network forensics and to some extent even loss of evidence. Attack detection needs to be integrated with network forensics in order to improve the timeliness of forensics after the detection of attackers.

**Attack Detection Process** - During the attack, the network defense system sends out attack alerts. Such alert information needs to be collected in order to identify the exact location. Access authority is then sought and the behaviors of the attackers analyzed according to their path and finally their operations intercepted and the information of the attackers recorded. The main attack detection process includes sending a request to the URL that has been accessed to request the collection of data information, recording the results of traffic anomalies and the actual suspicious traffic, analysis of the obtained suspicious traffic and then accessing the relevant static resources. The behaviors of the attackers are then analyzed and finally the interception and recording of the information will help in the network criminal forensics process [4].

### 3.3 Network Forensics Process

Demand for evidences collection is changeable in the process of network forensics. For one to meet such demand, composition of network forensic modules has to be designed. This can be done through network data, which records the process of network communication evidence collection and binary network data packets preservation. Content crawling network is one module that can be designed in meeting the demand of data collection. This layer helps in the preservation of documents relevant to a specific network and that, which is readable in terms of images and text data. With such a module, it is easy to extract information for network forensics.

Another module that can be designed is the data analysis layer. It analyzes network contents from the content crawling layer. It extracts and displays information that is useful and related to the attackers and finally helps in the compilation of a report of evidence. Forensics implementation layer is an additional module that is significant in the adjustment of the evidence collection stability and flexibility and it modifies the acquisition of information and filters them in order to simulate the login rules [7].

During network forensics process, after the design and compilation of the layers in the forensics analysis modules, the network forensic analysis needs to finish the collection of data, collection of information, analysis of the collected data and ultimately and most importantly the implementation of the forensics process [8]. A waterfall model which has been commonly followed in forensics has various steps – Preparation, Detection, Collection, Preservation, Examination, Analysis, Investigation, Presentation and Incident response. Feedback from steps examination, analysis and presentation can be used for improvement of network security, tools used etc. Figure 2 depicts the process of network forensics.
3.4 Network Forensics Analysis Tools (NFAT)

Network Forensic Analysis Tools (NFATs) are essential forensic tools used in the collection of data and aggregation of data from various security tools. They function in IP security provision, inside and outside network attack detection, data recovery, risk analysis, attack patterns detection, future attacks prediction and detection of anomalies in the network system. The main properties of network forensics analysis tools include collection of information [6].

Some of the network forensics analysis tools include but are not limited to NetIntercept, which collects and analyzes bundles of traffic, Iris, which collects data from the Internet, then reassembles them and reconstructs the actual text from the session. NetDetector is another NFATs that capture the attack, integrates signature anomalies and reconstructs the actual text from the session [10]. NetDetector also supports network interfaces and analyzes report on network traffic. Silent Runner is a network forensic tool that primarily focuses on inside threats and analyzes the threats in a three dimension on the network in order to monitor all the packets passing through a specific network. Other network forensic tools include NetWitness, NetworkMinor, and NetStumbler etc [9].

3.5 Literature survey evaluation on Network Forensic approaches

Evidence Graphs for Network Forensics Analysis [21], is a technique for network forensics analysis which includes manipulation, effective evidence presentation and automated reasoning. Also included is an evidence graph which facilitates the presentation and manipulation of intrusion evidence. Automated evidence analysis has an ordered hierarchical reasoning framework that includes local and global reasoning. Local reasoning aims to infer the roles of suspicious hosts from local observations. Global Reasoning aims to identify group of strongly correlated hosts in the attack and derive their relationships. Most comprehensive and sophisticated step is the analysis step. More realistic experiments and investigate methods to automate the process for hypothesizing missing evidence and validating hypotheses are needed in the model in local and global reasoning process as mentioned by the authors.

Step by step framework [22], has detailed about merging the previous frameworks to form a reasonably complete framework that groups all the existing processes into three stages - preparation, investigation and presentation. They are implemented as guidelines in network forensics. The aim of the framework is to establish guideline of what steps should be followed in a forensic process. However, it looks to be difficult in understanding how the framework addresses all phases of network forensics as it lacks clarification in many places.

Forensics Zachman (FORZA) [23] depicts a framework that focuses on the legal rules and participants in the organization rather than technical procedures. The framework tries to solve complex problems by integrating answers for the queries why (the motivation), what (the data attributes), who (the people involved), where (the location), how (the procedures) and when (the time) questions. Framework also includes eight rules namely case leader, legal advisor, system or business owner, security or system architect or auditor, digital forensic specialist, digital forensic analyst, digital forensic investigator or system administrator or operator and legal prosecutor. Framework is human dependent and requires more tools to conduct network forensic analysis in order to provide accurate results in investigation phase.

Two-dimensional evidence reliability amplification process model [24], it consists of sixteen sub-phases and they are then grouped in to five main phases namely initializing, evidence collection, evidence examination or analysis, presentation and case termination. All phases of the model are explained in detail by identifying the roles of the inspector and manager in each phase. The model aims to provide answers to common cybercrime queries, however it doesn’t focus on intention and strategic analysis (why and how questions). It has much similarity with incident response and computer forensics. Both presents a common process model for incident response and computer forensics to improve the investigation phase. The model includes steps grouped into three main phases consisting of pre
analysis (detection of incidents, initial response and formulation of response strategy), analysis (live response, data recovery, forensic duplication, harvesting, reduction and organization), and post analysis (report and resolution). Standard methods of detecting and collecting evidence doesn’t exist, which produces insignificant evidence and it affects the accuracy of the incident response as well.

Digital forensics investigation procedure model [25], it consists of ten phases with investigation preparation, classifying cybercrime & deciding investigation priority, investigating damaged (victims) digital crime scene, criminal profiling consultant and analysis, tracking suspects, investigating injurer digital crime scene, beckoning suspect, writing criminal profiling and reporting. Model presents block diagram without any technical details or process to manipulate with all these phases. Main focus was on the number and the type of the network forensics phase rather than how they works and how they conduct outcomes.

Categorization of investigation procedure was done [26] to group and merge the similar processes in five phases that provide the same outcome. The phases lists: Phase-1 (preparation), Phase-2 (collection & preservation), Phase-3 (analysis & examination), Phase-4 (presentation & reporting) and Phase-5 (publishing the case). Also proposes a mapping process of digital forensic investigation process model to eradicate the redundancy of the process involved in the model and standardize the terms used in achieving the investigation goal.

<table>
<thead>
<tr>
<th>Author</th>
<th>Proposed work</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stephenson et. al 2003</td>
<td>Forensics Zach man (FORZA)</td>
<td>The framework could solve complex problems by integrating answers for the queries why (motivation factor), what (data attributes), who (people involved), where (location), how (procedures) and when (time) questions.</td>
<td>It is human dependent. Requires many tools to conduct network forensic analysis in order to deliver accurate results in investigation phase.</td>
</tr>
<tr>
<td>Kohn et. al 2006</td>
<td>Step-by-step framework</td>
<td>It reasonably has complete framework which groups all existing processes in to three stages like preparation, investigation and presentation, which are implemented as guidelines in Network forensics.</td>
<td>Clarity of understanding how framework addresses all the phases of network forensics in main stages is a bit difficult.</td>
</tr>
<tr>
<td>Khatir et. al 2008</td>
<td>Two-dimensional evidence reliability amplification process.</td>
<td>Consists of 16 sub phases and are grouped them in to five main phases. This methodology aims to provide answers to most of cybercrime queries.</td>
<td>No standard method of detection and collection of evidence exists, it affects the accuracy of incident response.</td>
</tr>
<tr>
<td>Yong-Dal et. al 2008</td>
<td>Digital forensics investigation procedure model</td>
<td>Contains ten phases. This model shows block diagram without technical details or methods to manipulate with these phases.</td>
<td>Main focus deviated from how the phases work and how they organize the outcomes. Rather it focused on the volume and the type of network forensics phases.</td>
</tr>
<tr>
<td>Rahayu et. al 2008</td>
<td>categorization of investigation process</td>
<td>proposes a mapping process of digital forensic investigation process model to eradicate the redundancy of the process involved in the model and standardize the terms used in achieving the investigation goal.</td>
<td>Little bit of unclarity on grouping and merging the various process and arriving at 5 processes.</td>
</tr>
<tr>
<td>Wei et. al 2010</td>
<td>Evidence graphs for Network Forensics Analysis</td>
<td>It includes effective evidence presentation, automated reasoning and manipulation of intrusion evidence with a graph.</td>
<td>The model needs to be refined in both native and global reasoning process with more representative experiments.</td>
</tr>
</tbody>
</table>
4 CONCLUSION

Network forensics is the scientific process that ensures investigation of attacks that are performed in network or network devices. The significantly surfacing problem in emerging networks is the constant change of the crime scene. An increase in the advancement of technology attracts network revolution that calls for effective methods for monitoring and control of security and forensics. This paper effectively addressed how network forensic mechanisms can be used to eradicate network security attacks. The researches failed to deal with the concerns raised by the emergence of new networks such as M2M and IoT as per the advancement of improved network forensics essential in handling the situation of attacks. It is of essence to comprehensively analyze the emerging networks to help with forensic investigation. Network forensics plays a crucial role in new and developing areas of network and those related to data mining, social networking, data visualization and data imaging.

Future Work - With the empirical survey on advances of network forensics in emerging networks like IoT, 5G, it has been identified that there is a need in research to be conducted on the upcoming IoT (Internet of Things) forensics, to capture the network attacks and identify attack patterns using honeypots.

REFERENCES


31. IEEE 5G Summit Trivandrum – “IoT & Cyber security” 2017