available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

Network forensic frameworks: Survey and research challenges

*Emmanuel S. Pilli**, *R.C. Joshi*, *Rajdeep Niyogi*

Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, Roorkee, Uttarakhand 247667, India

ARTICLE INFO

Article history:
Received 22 December 2009
Received in revised form
13 February 2010
Accepted 16 February 2010

Keywords:
Network forensics
NFATs
Distributed systems
Soft computing
Honeypots
Data fusion
Attribution
Traceback
Incident response

ABSTRACT

Network forensics is the science that deals with capture, recording, and analysis of network traffic for detecting intrusions and investigating them. This paper makes an exhaustive survey of various network forensic frameworks proposed till date. A generic process model for network forensics is proposed which is built on various existing models of digital forensics. Definition, categorization and motivation for network forensics are clearly stated. The functionality of various Network Forensic Analysis Tools (NFATs) and network security monitoring tools, available for forensics examiners is discussed. The specific research gaps existing in implementation frameworks, process models and analysis tools are identified and major challenges are highlighted. The significance of this work is that it presents an overview on network forensics covering tools, process models and framework implementations, which will be very much useful for security practitioners and researchers in exploring this upcoming and young discipline.

1. Introduction

On August 6, 2009, social networking sites like Twitter, Facebook and Google blogger were knocked down by distributed denial of service (DDoS) attacks. Facebook and Google could recover within a day while Twitter staff team worked round the clock in the weekend to deal with the attack as reported in Computer World. Los Angeles Times speculated that perpetrators of the DDoS attack may have been bored teenagers or Russian and Georgian political operatives involved in cyberspace fighting. The newspaper quoted security experts that fingerprints of a sophisticated operation involving botnets were observed and Twitter website had limited capacity to handle incoming traffic. The obvious reason for the success of this attack was that Twitter's network did not have the defenses in place to mitigate a massive DDoS attack. Most traditional security products aren't equipped to handle massive bombardment of packets that happens in a DDoS attack. The lack of solid contingency plan and pro-active security mechanism created a fragile platform vulnerable to attack as reported in ChannelWeb.

Rosenberg referring to the attack on Twitter, wrote that having appropriate tools in place and following correct procedures help to eliminate or mitigate the effects of an attack. A network analysis tool can be used to capture all packets in a common data format for analysis. It can also raise alerts when thresholds are exceeded. Network forensic tools can be used to reconstruct the sequence of events that occur at the time of

* *Corresponding author*. Tel.: +91 1332 285650/5896; fax: +91 1332 273560.
E-mail addresses: emshudec@iitr.ernet.in, emmshub@gmail.com (E.S. Pilli), rcjosfec@iitr.ernet.in (R.C. Joshi), rajdpfec@iitr.ernet.in (R. Niyogi).
1742-2876/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2010.02.003

attack. Crucial information is gained to prevent a similar attack in future even if the present attack could not be prevented.

Habib in his detailed analysis explained that network forensics can be used to analyze how the attack occurred, who was involved in that attack, duration of the exploit, and the methodology used in the attack. It also helps in characterizing zero-day attacks. In addition, network forensics can be used as a tool for monitoring user activity, business transaction analysis and pinpointing the source of intermittent performance issues.

Network forensics is not another term for network security. It is an extended phase of network security as the data for forensic analysis are collected from security products like firewalls and intrusion detection systems. The results of this data analysis are utilized for investigating the attacks. However, there may be certain crimes which do not breach network security policies but may be legally prosecutable. These crimes can be handled only by network forensics (Broucek and Turner, 2001).

Network security protects system against attack while network forensics focuses on recording evidence of the attack. Network security products are generalized and look for possible harmful behaviors. This monitoring is a continuous process and is performed all through the day. But, network forensics involves post mortem investigation of the attack and is initiated *notitia criminis* (after crime notification). It is case specific as each crime scenario is different and the process is time bound.

Network forensics is the science that deals with capture, recording, and analysis of network traffic. The network log data are collected from existing network security products, analyzed for attack characterization and investigated to traceback the perpetuators. This process can bring out deficiencies in security products which can be utilized to guide deployment and improvement of these tools.

Network forensics is a natural extension of computer forensics. Computer forensics was introduced by law enforcement and has many guiding principles from the investigative methodology of judicial system. 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.

In computer forensics, investigator and the hacker being investigated are at two different levels with investigator at an advantage. In network forensics, network investigator and the attacker are at the same skill level. The hacker uses a set of tools to launch the attack and the network forensic specialist uses similar tools to investigate the attack (Berghel, 2003). Network forensic investigator is further at disadvantage as investigation is one of the many jobs he is involved. The hacker has all the time at his disposal and will regularly enhance his skills, motivated by the millions of dollars in stake. The seriousness of what is involved makes network forensics an important research field.

The aim of this work is to provide a detailed overview of network forensics. The paper is organized as follows: definition, categorization and motivation are clearly stated in Section 2. The various tools available for network forensic analysis and security tools which can also be used for specific phases are described in Section 3. Section 4 surveys the existing network forensic models. We use the term 'model' to imply a theoretical representation of phases involved in network forensics. This model may or may not have been implemented. We propose a generic process model for network forensics, considering only the phases applicable to networked environments, based on the existing models.

Section 5 surveys many implementation frameworks of these models. They are discussed under various categories like distributed systems, soft computing, honeypots and aggregation systems. We use the term 'framework' to mean practical implementation. The specific research gaps existing in these framework implementations and major challenges are presented in Section 6. Conclusions and future work are given in Section 7.

2. Background

Network forensics is being researched for a decade but it still seems a very young science and many issues are still not very clear and are ambiguous. The definition, categorization and motivation for this upcoming field are given below.

2.1. *Definition*

The concept of network forensics deals with data found across a network connection mostly ingress and egress traffic from one host to another. Network forensics tries to analyze traffic data logged through firewalls or intrusion detection systems or at network devices like routers and switches.

Network forensics is defined in Palmer (2001) as ''use of scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources for the purpose of uncovering facts related to the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to assist in response to or recovery from these activities.''

Ranum is credited with defining network forensics as ''capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents.''

Network forensics involves monitoring network traffic and determining if there is an anomaly in the traffic and ascertaining whether it indicates an attack. If an attack is detected, then the nature of the attack is also determined. Network forensic techniques enable investigators to track back the attackers. The ultimate goal is to provide sufficient evidence to allow the perpetrator to be prosecuted (Yasinsac and Manzano, 2001).

2.2. *Classification of Network Forensics Systems*

Network forensic systems are classified into two types each based on various characteristics like purpose, collection and nature:

- Purpose: 'General Network Forensics' to enhance network security and 'Strict Network Forensics' to get evidence