A Review of Current Research in Network Forensic Analysis

Ikuesan R. Adeyemi, Information Assurance and Security Research Group in the Department of Computer Science, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia

Shukor Abd Razak, Information Assurance and Security Research Group in the Department of Computer Science, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia

Nor Amira Nor Azhan, Information Assurance and Security Research Group in the Department of Computer Science, Universiti Teknologi Malaysia, Johor Bahru, Johor, Malaysia

ABSTRACT

Establishing facts on cyber crime is gradually gaining wider relevance in prosecuting cyber criminals. The branch of cyber policing saddled with this responsibility is the network forensic community (researchers, developer, and investigator). However, the recurring rate of advances in cybercrime poses greater challenge to the available improvements in network forensics analysis tools (NFAT) as well as to investigators, and ultimately, researchers. The need for an efficient cutting-edge research finding in curbing network crimes therefore is undeniably critical. This paper describes the distinction between network security and network forensics. In addition, the authors identify factors that militate against most network forensic techniques as well as the research challenges in network forensics. Furthermore, the paper discusses on the current research works on network forensics analysis. This research is useful to the research community of network forensics, for knowledge on existing research techniques, and direction on further research in network forensics.

Keywords: *Digital Forensic Investigation, Insider Misuse, Network Forensics, Network Security, Network-Traffic Profiling, User-Anonymity*

INTRODUCTION

Forensic science is the methodological and correct application of broad spectrum of scientific discipline to answer questions significant to legal system; an interception between technology, methodology and application (Greitzer & Frincke, 2010). Digital forensics is that branch of forensic science that deals with the nitty-gritty of 0s and 1s, otherwise known as digital values, of a computer system with the view to establishing hidden, lost or covered facts. The act of establishing a forensic paradigm in digital world involves interpreting digital processes in such a way that it explains 'what' event / action/process was carried out by/with/against a particular digital device under examination.

DOI: 10.4018/jdcf.2013010101

Network forensics has received various definitions since its inception by Marcus J. (Ranum, 2012) and its research community has greatly expanded since then. However, the generally accepted, but not encompassing definition was proposed at the 2001 DFRWS (Palmer, 2001). Palmer (2001), defines network forensics as "the 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".

Schwartz (2010) describes network forensics as the reconstruction of network event to provide definitive insight into action and behavior of users, applications as well as devices. In other words, network forensics involves the use of scientifically proven techniques to collect, identify, corroborate, examine, analyze and document digital information from live network session. However, these processes must be in conformance with forensically sound manner. Network forensics evidence source includes the capture of network traffic, and other relevant information from multiple devices, active processes, and digitally transmitting sources. Such device includes audit trails, Logs, routers, firewalls, servers, browsers, honey pot and network security device in general.

Uncovering facts related to planned intent, measurement of success of unauthorized activities, investigation of the source of an intrusion and the reasons for the success of such intrusion as well as the possible reason for such as intrusion are some of the vast needs for network forensics. Additionally, network forensics provides information to assist in response to/or recovery from an intrusion. Thus, network forensics can be termed as a proactive, as well as a retrospective approach to both law enforcement, and security hardening perspective. Network forensics can therefore be defined as the act (scientific process) of, measuring level of intrusion; investigating source of intrusion, deciphering intrusion intent and vulnerability exploited; or information provision to recover from an intrusion as well as the process of discovering planned intent of network traffic for the purpose of strengthening system security, and culpable evidence presentation. Network forensics can be classified into three classes: which are; based on purpose, process of collection, and nature of technology used. This classification forms the distinction between network forensics and network security. The rest of this paper is organized thus: The next section discusses the distinction between network forensics and network security. The following section elucidates on the research challenges on network forensics and details the premises on which network forensics challenges emanates. The various research works on network forensics are then presented. This paper also discusses the research works, challenges solved and lingering challenges still facing the research community. Conclusion is presented in the last section.

DISTINCTION BETWEEN NETWORK FORENSICS AND NETWORK SECURITY

The fact that a particular activity/event does not violate certain security protocol, does not necessarily exempt it from violating organizational policy defined under organization crime. Such scenario therefore falls outside the scope of network security expert, thus require investigation (Pilli, 2010). Network security entails securing (identifying network vulnerabilities; attacks & attack patterns; patching network & devices; just-enough system configuration; staff training and awareness; et cetera), monitoring and implementing network facilities in process consistent with organizational policy, and information security best practices[1]. Figure 1 shows a graphical description of the relationship, and distinction between network forensics and network security.