Attack Intention Recognition: A Review

Abdulghani Ali Ahmed, Noorul Ahlami Kamarul Zaman

(Corresponding author: Abdulghani Ali Ahmed)

Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang
26300 Gambang, Pahang, Malaysia
(Email: abdulghani@ump.edu.my)

(Received Nov. 3, 2015; revised and accepted Apr. 6 & May 7, 2016)

Abstract

Sensitive information faces critical risks when it is transmitted through computer networks. Existing protection systems are still limited in their capacities to ensure network information has sufficient confidentiality, integrity, and availability. The rapid development in network technologies has only helped increase network attacks and hide their malicious intent. This paper analyzes attack types and classifies them according to their intent. A causal network approach is used to recognize attackers' plans and predict their intentions. Attack intention is the ultimate attack goal which the attacker attempts to achieve by executing various methods or techniques, and recognizing it will help security administrators select an appropriate protection system.

Keywords: Attack intention recognition, causal network approach, cyber security, network forensics

1 Introduction

Information security over a network has become more challenging due to the expansion of technologies for hacking and anti-forensics. Sensitive information should be treated confidentially in any system as it represents a high risk to the owners if exposed to the public. Information is at risk due to several factors, including human and technical errors, accidents and disasters, fraud, commercial espionage, and malicious damage [1, 2, 4].

Activities such as unauthorized access, damage to computer data or programs, obstruction of the functions of computer systems or networks, interception of data, and computer espionage are categorized as cybercrimes [7, 8, 10, 11, 17, 21]. Cybercrimes are broad in scope and are defined as attacks that involve the use of computers or networks to commit the crimes. According to [3, 4, 9], cyber-attacks can be categorized into unauthorized access, malicious code (malware), and interruption of services. Figure 1 shows common types of network threats.

Network forensics, as a part of network security, works with laws and guiding principles established in the judicial system to deal with cyber criminals. Network forensics has two approaches: reactive and proactive. Reactive network forensics is a traditional approach that deals with cybercrime cases a period of time after an attack. The reactive forensic approach consumes considerable time during the investigation phase. Proactive network forensics is a new, different approach that focuses on investigating concurrently with an attack [5, 14].

Figure 2 shows a framework of the generic process model in network forensics that splits the phases into two groups. The first group relies on actual time and includes five phases: preparation, detection, incident response, collection, and preservation. The second group relies on the post-investigation phases.

Authors in [16] also classify the first group as proactive and the second group as reactive. The proactive phases have advantages in saving time and money during investigation, as they work concurrently with the occurrence of the cybercrime. By contrast, reactive phases begin with the examination phase to integrate the trace data and identify the attack indicators. The indicators are then prepared for the analysis phase, which reconstructs the attack indicators either by soft computing or statistical or data mining techniques to classify and correlate the attack patterns. Attack intention is the ultimate goal the attacker is attempting to achieve by executing various methods or techniques of attack. Even for an expert, it is difficult to predict methods of attack. An attacker will work toward his goal through a sequence of tactical steps using sophisticated techniques to hide and cover his patterns. Attack Intention Recognition (AIR) is the process of using known attack scenarios to observe an attacker's behavior and infer his intention [19]. With the rapid developments in networking technology, attacks have become more dangerous than ever, deploying sophisticated mechanisms to hide malicious behavior. Understanding attackers' behavior will help security administrators recognize their intentions and better predict their activities.

In the following section, work related to this research is critically analyzed. This study discusses using proactive AIR methods to identify attack plans to predict future ac-