Investigation Approach for Network Attack Intention Recognition

Abdulghani Ali Ahmed, Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang, Gambang, Malaysia

ABSTRACT

Sensitive information has critical risks when transmitted through computer networks. Existing protection systems still have limitations with treating network information with sufficient confidentiality, integrity, and availability. The rapid development of network technologies helps increase network attacks and hides their malicious intentions. Attack intention is the ultimate attack goal that the attacker attempts to achieve by executing various intrusion methods or techniques. Recognizing attack intentions helps security administrator develop effective protection systems that can detect network attacks that have similar intentions. This paper analyses attack types and classifies them according to their malicious intent. An investigation approach based on similarity metric is proposed to recognize attacker plans and predict their intentions. The obtained results demonstrate that the proposed approach is capable of investigating similarity of attack signatures and recognizing the intentions of Network attack.

KEYWORDS

Information Security, Intention Recognition, Network Attack, Network Forensics, Similarity of Evidences

1. INTRODUCTION

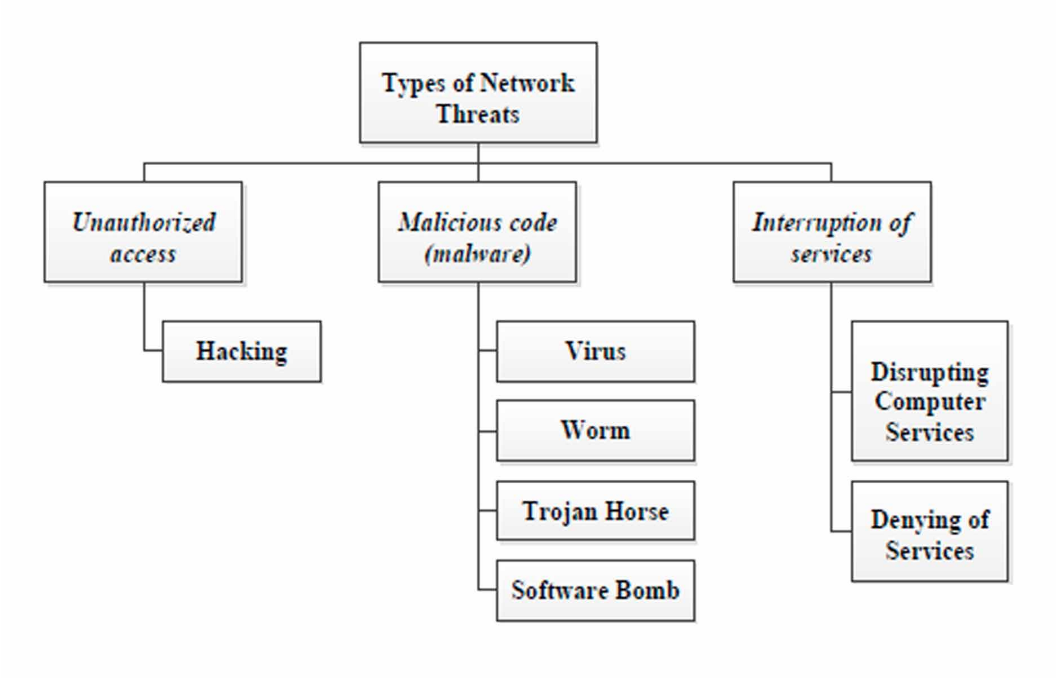
Information security over networks has become more challenging due to the new hacking and anti-forensics techniques. Sensitive information should be treated confidentially in any system as it represents high risk to its owners if exposed to the public. This information is risky for several reasons, such as human and technical errors, accidents and disasters, fraud, commercial espionage, and malicious damage.

According to Yunos, Ahmad, & Sahib (2015), unauthorized access damages computer data or programs, obstructs the functioning of computer systems or networks, and intercepts data. Acts of computer espionage are categorized as network attacks. They are broad in scope and are defined as attacks that involve a computer or network used to commit crimes. It is essential to inspect all network activity, both incoming and outgoing, and detect suspicious patterns which might be evidence of a network or system attack. Network attacks are categorized into unauthorized access, malicious code (malware), and service interruptions. Figure 1 shows common types of network threats.

As stated by Lahre, Diwan, Kashyap, & Agrawal (2013), intrusions are classified into attempted break-ins, masquerade attacks, penetration of security control systems, leakage, denial of service, and malicious use. Fortunately, there are techniques to detect intrusions, anomaly detection and misuse detection. Anomaly detection assumes that all intrusive activities are necessarily anomalous and finds patterns in data that do not comply with expected behaviour (Chandola, Banerjee, & Kumar, 2009; Ahmed & Zaman, 2017). Misuse detection embodies attacks in the form of a pattern or a signature so that variations of the same attack are detected.

DOI: 10.4018/IJDCF.2017010102

Figure 1. Common types of network threats



Network forensics is a part of network security that works with the laws and guiding principles prescribed by the judicial system to deal with cyber criminals. There are two approaches in network forensics, reactive and proactive. Reactive network forensics is a traditional approach that deals with network attacks cases after a period of time. Reactive forensic approach consumes a considerable amount of time during the investigation phase. Proactive network forensics is different from the reactive approach. Proactive forensic is a new approach in network forensics that deals with a live investigation during an attack (Rasmi & Al-Qerem, 2015).

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

Rasmi, Jantan, & Al-Mimi (2013) classify the first group as proactive and the second group as reactive. The proactive phase saves time and money during the investigation process as they work throughout the occurrence of an attack. In contrast, reactive phases begin with the examination phase to integrate trace data and identify attack indicators. The indicators are prepared for the analysis phase, which reconstructs the attack indicators using soft computing or statistical or data mining techniques to classify and correlate attack patterns.

Attack intention is the ultimate attack goal that the attacker attempts to achieve by executing various attack methods or techniques. It is difficult for an expert human to predict attack methods. An attacker achieves his goal through a sequence of tactical steps, using sophisticated techniques to hide and cover his activities.

Attack Intention Recognition (AIR) is the process of inferring an attacker's intention from observed attack behaviours, which is based on attack scenarios (Ahmed, Sadiq, & Zolkipli, 2016; Qin & Lee, 2004). With the rapid development of networking technology, attacks have become more dangerous than ever and sophisticated mechanisms are deployed to hide malicious behaviours. Recognizing attacker intentions helps security administrators to understand attack behaviour and