AIRSE: an approach for attack intention recognition based on similarity of evidences

Abdulghani Ali Ahmed, Noorul Ahlami Kamarul Zaman*
Faculty of Computer Systems & Software Engineering Universiti Malaysia Pahang, 26300,
Kuantan, Pahang, Malaysia
abdulghani@ump.edu.my, noorul.ahlami@gmail.com

ABSTRACT

Sensitive information can be exposed to critical risks when communicated through computer networks. The ability of attackers in hiding their attacks' intention obstructs existing protection systems to early prevent their attacks and avoid any possible sabotage in network systems. In this paper, we propose a similarity approach called Attack Intention Recognition based on Similarity of Evidences (AIRSE). In particular, the proposed approach AIRSE aims to recognize attack intention in real time. It classifies attacks according to their characteristics and uses the similar metric method to identify attacks motives and predict their intentions. In this study, attack intentions are categorized into specific and general intentions. General intentions are recognized by investigating violations against the security metrics of confidentiality, integrity, availability, and authenticity. Specific intentions are recognized by investigating the network attacks used to achieve a violation. The obtained results demonstrate that the proposed approach is capable of investigating similarity of attack signatures and recognizing the intentions of network attack.

KEYWORDS

Cyberattacks; Network forensics; Attack intention recognition; Similarity of evidences

ACKNOWLEDGMENT
RDU grant number RDU160365, Faculty of Computer System and Software Engineering, Universiti Malaysia Pahang supported this work.