Acta Scientific COMPUTER SCIENCES

Volume 3 Issue 9 Septembr 2021

Editorial

The Next-Generation Stepping-Stone Intrusion Detection Systems

Lixin Wang*

Associate Professor, TSYS School of Computer Science, Columbus State University, Columbus, Georgia, USA

***Corresponding Author:** Lixin Wang, TSYS School of Computer Science, Columbus State University, Columbus, Georgia, USA.

Received: July 24, 2021

Published: August 01, 2021

Hackers on the Internet usually send attacking packets using compromised hosts, called stepping-stones, in order to avoid being detected. With stepping-stone attacks, an attacker remotely logins to a chain of such stepping-stone hosts using programs like SSH or telnet, and then sends the attacking commands to a target host. A great number of detection approaches have been developed for stepping-stone intrusion (SSI) in the last two decades [1-11]. Most of these existing detection methods for SSI only worked effectively when session manipulation by intruders are not present.

By far, the two most popular session manipulation techniques used by intruders for evasion are time-jittering and chaff-perturbation. Time-jittering is a technique that attacker could hold a packet for a while and then release it for transmission. The goal of employing the time-jittering technique is to modify the gap between the TCP/IP packets' timestamps in a connection in order to avoid being detected by all the existing time-based detection methods for SSI. Chaff- perturbation is a different evasion approach that intruders can insert some meaningless packets into a TCP/IP connection to modify not only the gap between the packets' timestamps, but also the total number of packets existing in the network traffic in a certain time period. Chaff-perturbation technique can easily make the existing SSI approaches that were based on the amount of network traffic not work effectively.

While network security researchers have been proposing various detection approaches for SSI since 1995, intruders have also been developing new techniques to evade our detection.

Nowadays intruders tend to use session manipulation techniques to evade detection when SSI attacks are launched. Currently, all the known detection methods for SSI to handle intruders' session manipulation such as time-jittering and/or chaff-perturbation are either not feasible to implement or don't work effectively.

Some of such detection methods can only handle intruder's evasion with very limited capacity. Therefore, the next-generation SSI detection methods should be robust in resisting intruders' session manipulation so that they can be actually implemented to protect practical computer networks against SSI attacks.

Volume 3 Issue 9 September 2021