Detection of SIP Scans and Bruteforce Attacks

Tomas Jansky, Tomas Cejka, Vaclav Bartos
CESNET, a.l.e
Zikova 4, 160 00 Prague 6, Czech Republic

jansktol@fit.cvut.cz, cejkat@cesnet.cz, bartos@cesnet.cz

Keywords. SIP, VoIP, netflow, attack detection.

Abstract

Extended flow records with application layer (L7) information allow for detection of various types of malicious traffic. Voice over IP (VoIP) is an example of technology that works on L7 and many attacks against it cannot be reliably detected using just basic flow information. Session Initiation Protocol (SIP), which is commonly used for VoIP signalling, is a frequent target of many types of attacks. This paper proposes and evaluates a novel algorithm for near real time detection of username scanning and password guessing attacks on SIP servers. The detection is based on analysis of L7 extended flow records.

Paper origin

This paper has been accepted and presented at the conference Autonomous Infrastructure, Management and Security (AIMS) 2017.

Acknowledgment

This work was supported by the CTU grant No. SGS17/212/OHK3/3T/18 funded by Ministry of Education, Youth and Sports of the Czech Republic.