Detecting End-Point (EP) Man-In-The-Middle (MITM) Attack based on ARP Analysis: A Machine Learning Approach

Jerry Kponyo[1], Justice Agyemang[1], and Griffith Selorm Klogo[2]

[1]Affiliation not available
[2]Kwame Nkrumah University of Science and Technology

May 13, 2020

Abstract

End-Point (EP) Man-In-The-Middle (MITM) attack is a well-known threat in computer security. It targets the data flow between endpoints, and the confidentiality and integrity of the data itself. Several techniques have been developed to address this kind of attack. With the current emergence of machine learning (ML) models, we explore the possibility of applying ML in EP MITM detection. Our detection technique is based on address resolution protocol (ARP) analysis. The technique combines signal processing and machine learning in detecting EP MITM attack. We evaluated the accuracy of the proposed technique using linear-based ML classification models. The technique proved itself to be efficient by producing a detection accuracy of 99.72%.

Hosted file

`MC-manuscript.pdf` available at https://authorea.com/users/303547/articles/450795-detecting-end-point-ep-man-in-the-middle-mitm-attack-based-on-arp-analysis-a-machine-learning-approach

Posted on Authorea 13 May 2020 — CC-BY 4.0 — https://doi.org/10.22541/au.158938565.57807215 — This a preprint and has not been peer reviewed. Data may be preliminary.