Contribution ID: **21** Type: **not specified**

SECURITY ARCHITECTURE FOR PREVENTING MALICIOUS ATTACKS IN SOFTWARE DEFINED NETWORK (SDN)

Despite the successful record of Internet it short comings in the area of network configuration, response to fault(s), load and change(s) led to concept of software defined network (SDN) that separates combined network's control (brains) from forwarding (muscle) planes for easier optimization, network programmability and control logic centralization capabilities, this introduced new fault and attack planes, that open doors for new threats that where not existing or harder to exploit, SDN OpenFlow (OF) paradigm embraces third party development efforts, and therefore suffers from potential trust issue on OF applications (apps), an attacker can inject malicious programs into network packets and forward them into the network. This study prevents SDN from malicious attacks and guarantees a secured SDN paradigm from malicious attacks.

An algorithm was designed using white/black list source identification combined with content based packet filtering as a security measure to prevent malicious attack. When a packet arrived at the port, algorithm check through the openflow flowtable for status of previous transaction from that particular source if legitimate (Whitelist), the newly arrived packet granted secured and delivered as a secured packet, if otherwise (Blacklist) newly arrived packet disqualified and dropped. But if transaction from the source is taken place for the first time algorithm then apply the content based packet filtering using word hashing combined with Bayes' theorem to calculate the spamicity chances of newly arrived packet, if spamicity result gotten is greater than or equal to (>=) particular set threshold the packet concluded malicious and dropped, if otherwise legitimate packet delivered and flowTable updated for subsequent transaction(s).

Results from the study indicate that initiated transactions where previously existing transaction from same source on the flowTable was grouped/classified to be Blacklist where dropped as a malicious packet, while those with previously existing transaction on the flowTable grouped/classified to be Whitelist where forwarded to their destination as a legitimate packet. In case of newly initiated transaction(s) where there is no previous transaction from transaction initiated source on the flowTable, content based filtering method was initiated and malicious packet where grouped/classified to be malicious and legitimate where grouped/classified to be legitimate.

It indicated from findings that algorithm combined source identification/authentication (using white/blacklist) and content filtering (using word hashing and Bayes'theorem) methods of malicious identification/authentication and packet grouping, provides effective solution to legitimate/malicious mail grouping/identification and as such prevents malicious attack from accessing their targeted host in Software Defined Network. And therefore recommends combined methods of source identification/authentication as a preventive measure for malicious attack in Software Defined Network (SDN) due to its efficiency and effectiveness.

Summary

Keywords: Security, OpenFlow, Flow table, network communications

Primary author: Dr OSUNADE, Oluwaseyi (University of Ibadan)

Co-author: Mr OKUNADE, Oluwasogo (National Open University of Nigeria, Abuja)

Presenter: Dr OSUNADE, Oluwaseyi (University of Ibadan)

Track Classification: Trust, Identity and Security