INTISARI

PERANCANGAN DAN PENGIMPLEMENTASIAN METODE KOLABORASI ADAPTIF PADA *HOST* DAN *ROUTER* UNTUK PERLINDUNGAN KOMPREHENSIF DARI MITM-ARP *SPOOFING*

Oleh

STANDY OEI
22/499523/SPA/00848

Permasalahan pada fasilitas Internet publik adalah keterbukaan akses. Hal ini membuat fasilitas tersebut rentan terhadap serangan. Saat terhubung ke Internet, *network host* mengandalkan *router* sebagai *gateway* ke jaringan lainnya atau Internet. Komunikasi antara *network host* dan *router* dapat menjadi target serangan karena dapat berisikan lalu lintas data penting, seperti kredensial. Sebagian besar fasilitas Internet publik masih menggunakan Internet Protocol versi 4 (IPv4) dalam pengalamatan IP-nya. Oleh karena itu, kelemahan Address Resolution Protocol (ARP) dapat digunakan sebagai peluang oleh penyerang. Serangan MitM-ARP *spoofing* dapat diluncurkan untuk mengendus kredensial dalam komunikasi *network host* dan *router*.

Penelitian ini bertujuan untuk menghasilkan metode kolaborasi adaptif pada *network host* dan *router*, yang secara komprehensif memberikan perlindungan dari MitM-ARP *spoofing*. Metode yang diusulkan berisi 2 bagian solusi yang diterapkan secara terpisah di *network host* dan *router*. Di *network host*, penelitian ini memperkenalkan kombinasi anomali *ping* RTT, fungsi SendARP, dan entri statis untuk mendeteksi dan mengatasi serangan. Algoritma solusi *network host* bekerja dalam bentuk perangkat lunak portabel berukuran kecil yang dapat disalin dan dijalankan secara fleksibel ke *network host*. Di *router*, penelitian ini memperkenalkan kombinasi DHCP *leases* sebagai sumber entri ARP *router* dan mode ARP antarmuka *router* "*reply-only*" untuk melindungi ARP *cache router* dari serangan. Algoritma solusi *router* ini ringan dan dapat dengan mudah diterapkan di lingkungan jaringan yang ada.

Hasil penelitian ini menunjukkan bahwa serangan MitM-ARP *spoofing* mengakibatkan anomali (kenaikan) *ping* RTT, perubahan rute dari *data traffic* yang dipaksakan melalui penyerang, dan kredensial yang dapat diendus (*sniffed*). Kenaikan *ping* RTT didapati berhubungan dengan perubahan rute yang dilakukan oleh penyerang. Pada solusi *network host*, anomali *ping* RTT dan fungsi SendARP berhasil mendeteksi serangan dengan akurat dan dengan *delay time* yang minim di bawah 1.000 ms

atau 1 detik. Entri statis berhasil menimpa entri dinamis beracun yang dimasukkan penyerang dan mengembalikan rute ke rute asli/sah. Dengan begitu, nilai *ping* RTT dikembalikan ke nilai normal, dan kredensial tidak dapat diendus. Pada solusi *router*, DHCP *leases* sebagai sumber entri ARP *router* dan mode ARP antarmuka *router* "*reply-only*" berhasil menutup celah kemungkinan serangan yang memanfaatkan pesan ARP.

Kata-kata kunci: masalah keamanan IPv4, MitM-ARP *spoofing*, *network host*, *router*.

ABSTRACT

DESIGN AND IMPLEMENTATION OF ADAPTIVE COLLABORATIVE METHOD ON HOST AND ROUTER FOR COMPREHENSIVE PROTECTION AGAINST MITM-ARP SPOOFING

By

STANDY OEI
22/499523/SPA/00848

The problem with public Internet facilities is the openness of access. It makes them prone to attacks. When connecting to the Internet, network hosts rely on a router as the gateway to the other network or the Internet. Communication between a *network host* and a *router* can be a target for attacks because it can contain important data traffic, such as credentials. The majority of these public Internet facilities still use Internet Protocol version 4 (IPv4) in their IP addressing. Therefore, the Address Resolution Protocol (ARP) weakness can be exploited by attackers. MitM-ARP spoofing attack can be launched to sniff credentials in the network host and router communication.

This research aims to develop an adaptive collaborative method for network hosts and routers, which comprehensively protects from MitM-ARP spoofing. The proposed method contains 2 solution parts that are separately applied in the network host and the router. In the network host, this research introduces a combination of ping RTT anomaly, SendARP function, and static entry to detect and overcome attacks. The network host solution algorithm works as a small portable software that can be flexibly copied and run on network hosts. In the router, this research introduces a combination of DHCP leases as the router's ARP entry source and the router interface's ARP mode "reply-only" to protect the router's ARP cache from attacks. The router solution algorithm is light and can be easily applied in the existing network environment.

The results of this research show that the MitM-ARP spoofing attack results in an anomalous (increase) in the ping RTT, a forced rerouting of data traffic through the attacker, and sniffed credentials. The increase in the ping RTT is found to be related to the rerouting performed by the attacker. In the network host solution, the ping RTT anomaly and the SendARP function successfully detect the attack accurately and with a minimal delay time of under 1,000 ms or 1 second. The static entry successfully overrides the attacker's poisoned dynamic entry and reroutes the origi-

nal/legitimate route. This restores the ping RTT value to normal, and the credentials cannot be sniffed. In the router solution, DHCP leases as the source of the router ARP entries, and the router interface ARP mode “reply-only” successfully closes the gap for possible attacks that exploit ARP messages.

Keywords: IPv4 security issue, MitM-ARP spoofing, network host, router.