ROGUE IPV6 ROUTER ADVERTISEMENT ATTACK

Jozef Pivarník
Master Degree Programme (2), FIT BUT
E-mail: xpivar00@stud.fit.vutbr.cz

Supervised by: Matěj Grégr
E-mail: igregr@fit.vutbr.cz

Abstract: This paper describes first hop security issue of IPv6 Neighbor Discovery Protocol. Vulnerability of this protocol is exploited to perform a Rogue Router Advertisement attack. Currently, there are few mitigation techniques available against this type of attack, but none of them is widely used, mainly because insufficient support of vendors. One of them – RA Snooping – is presented with assessment of its applicability.

Keywords: IPv6 Neighbor Discovery, Router Advertisement, Rogue RA attack, RA Guard.

1 ÚVOD

Tento článok si kladie za cieľ otestovať obranu proti IPv6 útoku Rogue Router Advertisement s využitím súčasného hardvéru a aktuálneho softvéru. Sekundárnym cieľom je vytvorenie nástroja na realizáciu útoku a testovanie obrany voči nemu, pretože v súčasných penetračných nástrojoch toto nie je vždy komplexne riešené. Útok využíva zraniteľnosť protokolu NDP definovaného v RFC 4861. Ide o IPv6 protokol, ktorý zastrešuje funkcionalitu troch IPv4 protokolov, menovite ARP (RFC 826), ICMP Router Discovery (RFC 1256) a ICMP Redirect (RFC 792).

NDP protokol pre svoju činnosť využíva štyri druhy správ (tiež definované v RFC 4861). Pre účely tohto článku je najpodstatnejšia správa Ohlásenie Smerovača (Router Advertisement – RA). V skutočnosti je to ICMPv6 správa, ktorou smerovač ohlasuje parametre siete, ako napr. prefix siete, implicitnú bránu, používané MTU atď. Správy tohto typu vysiela smerovač jednak v pravidelných časových intervaloch, a jednak ako odpoveď na ICMPv6 správu – Výzvu Smerovača (Router Solicitation – RS).

2 VEKTOR ÚTOKU

Rogue IPv6 RA útok spočíva v tom, že útočník sa sfalšovaním RA správy vydáva za legálny smerovač, čím môže spôsobiť zmenu parametrov siete a/alebo interných datových štruktúr klientskych staníc. Dôsledkov to môže mať niekoľko. Buď zapríčiní zhoršenie výkonu siete, spôsobí stratu konektivity ostatných klientskych staníc alebo v najhoršom prípade presmeruje komunikáciu obete bez jej vedomia, často práve cez stanicu útočníka.

Internými datovými štruktúrami sú myslené zoznamy on-link prefixov, zoznamy implicitných brán a IPv6 adresy rozhraní. Popis ich funkcionality je možné nájsť v RFC 4861. Zmeny týchto štruktúr sú podmienené príjmom RA správy alebo vypršaním časovačov odpovedajúcich záznamov.

3 MOŽNOSTI OBRANY

Cieľom protiopatrení voči uvedenému útoku je správne identifikovať jednotlivé RA správy ako pravé, resp. falošné. Je treba brať do úvahy aj prípady, kedy RA správy neboli sfalšované zámerne, ale buď chybou administrátora (nesprávna konfigurácia rozhrania smerovača) alebo chybou užívateľa (napr. ak užívateľ zabudne vypnúť službu Windows Internet Connection Sharing a pripojí sa do siete).

V súčasnosti existuje niekoľko druhov protiopatrení voči tomuto útoku, ktoré sú popísané v RFC 6104. Väčšina z nich sa dokáže viac či menej úspešne vyrovnať s jedným z uvedených scénárov, prípadne s oboma za cenu striktných obmedzení a veľkej zložitosti, viď SEND (RFC 3971). Za doposiaľ najlepšie riešenie sa dá považovať RA Snooping.

V prípade uvedeného útoku sú cieľom inšpekcie RA správy, predovšetkým ich zdroj. Nutnou súčasťou konfigurácie zariadenia proti uvedenému útoku je definovanie dôveryhodných a nedôveryhodných portov. Ak prepínač identifikuje RA správu doručenú na nedôveryhodnom porte, zahodí ju, a tým prekazí útok (aj neúmyselný). Vo väčšine prípadov budú dôveryhodné porty k smerovačom a nedôveryhodné všetky ostatné. RFC 6105 uvádza popis tejto technológie, tiež známej pod názvom **RA Guard**.

4 OBÍDENIE OBRANY

Proti vyššie popísanému útoku v jeho najjednoduchšej forme (falošná ICMPv6 RA správa je jediným obsahom IPv6 paketu) je toto protiopatrenie úspešné.V súčasnosti sa však objavujú techniky obídenia tejto obrany, proti ktorým sa niektoré implementácie RA Guard javia ako neúspešné. Ide o zneužitie konceptu rozšíriteľných hlavičiek a fragmentácie IPv6 paketov.

4.1 ROZŠÍRITEĽNÉ HLAVIČKY

Niektoré implementácie RA Guard identifikujú ICMPv6 správy na základe položky *Next Header* priamo v hlavičke IPv6 paketu. Výsledkom je neúspešná identifikácia všetkých ICMPv6 paketov, ktoré obsahujú pred samotnou ICMPv6 správou jednu alebo viac rozširujúcich hlavičiek, čo na nedôveryhodnom porte znamená zlyhanie obrany. Správnym riešením je inšpekcia celého reťazca rozširujúcich hlavičiek.

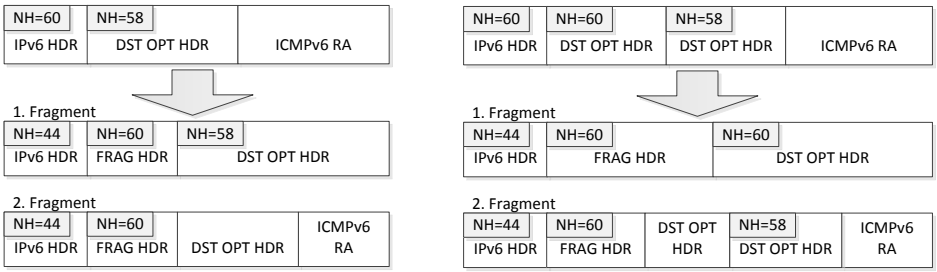
Útočník však môže vytvoriť paket s nezmyselne dlhým reťazcom hlavičiek, ktorého kontrola nemusí byť na niektorých zariadeniach realizovateľná. Inšpekcia môže byť z dôvodu zvýšenia výkonnosti implementovaná v hardvéri, ktorý má obmedzené zdroje, a teda ak sa útočníkovi podarí tieto zdroje vyčerpať, obrana zlyháva. Tento typ útoku je vo svojej podstate unikátny a doposiaľ nebol nikde popísaný.

4.2 FRAGMENTÁCIA

Prakticky všetky súčasné implementácie RA Guard sú zraniteľné voči Rogue RA útoku využívajúcemu fragmentáciu IPv6 paketov. Základnou myšlienkou je to, že v IPv6 sieti dochádza k (de)fragmentácii paketov vždy na koncových zariadeniach, preto prechodné sieťové prvky ako prepínače nemajú informáciu o úplnej podobe IPv6 paketov. Praktická realizácia uvedeného útoku teda môže vyzerať nasledovne.

Do pôvodnej RA správy vloží útočník jednu alebo viac rozširujúcich hlavičiek dostatočne veľkých na to, aby mohol byť paket rozdelený na aspoň 2 fragmenty, viď obr. 1 vľavo. Keďže dĺžka rozširujúcej hlavičky je špecifikovaná v prvom fragmente, zariadenie spracúvajúce druhý fragment nevie identifikovať začiatok ICMPv6 RA správy. Týmto spôsobom je možné zakryť obsah ICMPv6 správy pred zariadením s nakonfigurovaným RA Snoopingom.

Túto myšlienku je možné ďalej rozšíriť tak, že útočník pred L2 zariadením skryje aj ten fakt, že sa jedná o ICMPv6 správu. Toto je možné docieliť napríklad takým spôsobom, že pred samotnú ICMPv6 správu sa vložia aspoň dve ďalšie hlavičky tak, aby bol paket znova rozdelený na dva fragmenty, viď obr. 1 vpravo. Zariadenie spracúvajúce prvý fragment v tomto prípade nemá ani informáciu o tom, že sa jedná o ICMPv6 správu.



Obrázek 1: Obídenie RA Guard s využitím fragmentácie.

5 ZÁVER

Uvedený útok bol testovaný na zariadeniach so zapnutou ochranou RA Guard od firmy Cisco – Catalyst 3750-X a 2960S, s operačnými systémami IOS verzie 15.0.(2)SE1, resp. 15.0(1)SE2[1] a od firmy HP – A5800 s operačným systémom verzie 5.20.

Všetky testované zariadenia sú zraniteľné voči útoku pomocou rozšíriteľných hlavičiek. Cisco zariadenia sú schopné identifikovať len podvrhnuté RA správy, ktoré majú menej ako sedem rozširujúcich hlavičiek, HP zariadenie dokonca len menej ako tri. Testované zariadenia sú tak isto zraniteľné aj voči útoku využívajúcemu fragmentáciu paketov. Riešením tohto problému by mohlo byť zahodenie všetkých paketov, ktorých typ nemohol byť z nejakého dôvodu určený. Vzťahuje sa to predovšetkým na IPv6 pakety, ktorých kompletný reťazec hlavičiek sa nevojde do prvého fragmentu. Cisco toto riešenie implementovalo v podobe IPv6 ACL `deny ip any any undetermined-transport`, avšak na testovaných zariadeniach tento ACL zatiaľ nebol plne podporovaný. Veľkou nevýhodou tohto riešenia je fakt, že môže zahodiť aj nezvyčajné validné pakety.

Testované zariadenia sú najaktuálnejšou verziou prvkov určených pre prístupovú a distribučnú vrstvu, na ktorých nastáva problém falošných RA správ. Súčasná špecifikácia RA Guard nijak nezohľadňuje problém fragmentácie IPv6 paketov, a preto sú prakticky všetky jej implementácie zraniteľné voči tejto forme útoku. Bez ohľadu na to je dôležitým zistením fakt, že ani najnovšie prvky od firiem Cisco a HP nie sú schopné správne identifikovať falošné RA správy s veľkým množstvom rozširujúcich hlavičiek. Aj keby hardvérové prostriedky iných zariadení chrbticovej vrstvy boli dostatočné na potlačenie uvedeného útoku, tieto prvky nebudú nasadené na prístupovú, resp. distribučnú vrstvu, teda aj keby podporovali danú funkcionalitu, bude zbytočná.

Za v súčasnosti jediný univerzálny spôsob obrany voči uvedenému útoku bolo považované využitie RA Guard na prístupových prvkoch, avšak ako bolo uvedené, aj toto protiopatrenie je možné obísť, čo môže mať celkom závažné dôsledky. Útočník je bez väčšej námahy schopný znemožniť pripojenie užívateľov do siete, prípadne odchytávať ich dáta. Jediným obmedzením útočníka je, že musí mať fyzický prístup k danej sieti.

REFERENCE

[1] Ferry. Bypass Cisco ICMPv6 Router Advertisement Guard. Máj 2011. Dokument dostupný na URL http://www.ipv6security.nl/?p=763.

[2] Chown, T. and S. Venaas. Rogue IPv6 Router Advertisement Problem Statement. RFC 6104. Február 2011.

[3] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi. IPv6 Router Advertisement Guard. RFC 6105. Február 2011.

[1] http://docwiki.cisco.com/wiki/Cisco_IOS_IPv6_Feature_Mapping#IPv6_First-Hop_Security_Features