MOKSLAS – LIETUVOS ATEITIS
SCIENCE – FUTURE OF LITHUANIA
ISSN 2029-2341 / eISSN 2029-2252
http://www.mla.vgtu.lt

ELEKTRONIKA IR ELEKTROTECHNIKA
ELECTRONICS AND ELECTRICAL ENGINEERING

2016 8(3): 273–277

http://dx.doi.org/10.3846/mla.2016.930

ICMPV6 PROTOKOLO RA ŽINUČIŲ ATSISAKYMO APTARNAUTI ATAKOS TYRIMAS

Linas Juozas JOČYS

Vilniaus Gedimino technikos universitetas, Vilnius, Lietuva
El. paštas linas-juozas.jocys@stud.vgtu.lt

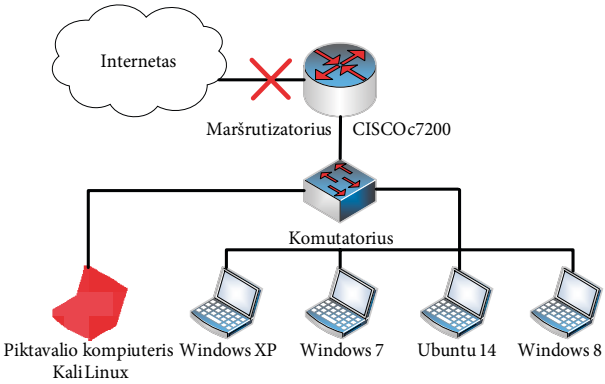
Santrauka. ICMPv6 yra naujausios versijos interneto kontrolės žinučių protokolas, kurio pagrindinis tikslas pranešti apie paketų apdorojimo klaidas IPv6 tinklo mazgams. Analizuojant ICMPv6 protokolą nustatyta, jog šis protokolas yra technologiškai pažeidžiamas. Vienas iš pažeidžiamumų yra ICMPv6 maršrutizatoriaus skelbimo žinučių (RA) atsisakymo aptarnauti pažeidžiamumas, kuris leidžia sulėtinti arba visiškai sutrikdyti operacinių sistemų darbą kompiuteriuose, esančiuose vietiniame tinkle. Straipsnyje aprašomas Windows (XP, 7, 8.1) ir Linux Ubuntu tipų operacinių sistemų atsparumo ICMPv6 protokolo RA žinučių atsisakymo aptarnauti atakai tyrimas. Tyrimo metu nustatytas pasirinktų operacinių sistemų atsparumas RA žinučių atsisakymo aptarnauti atakai, esant skirtingiems techninės įrangos resursams. Straipsnyje taip pat pateiktos prevencinės priemonės ICMPv6 RA žinučių atsisakymo aptarnauti pažeidžiamumui šalinti arba minimizuoti.

Reikšminiai žodžiai: ICMPv6 RA atsisakymas aptarnauti ataka, IPv6 pažeidžiamumai, ICMPv6 pažeidžiamumas.

Įvadas

Interneto protokolo versija 6 (IPv6) yra naujausia interneto protokolo versija, pasaulyje oficialiai išleista naudoti 2012 metų liepos 6-tą dieną. Pagrindinis IPv6 protokolo kūrimo tikslas buvo pakeisti šiuo metu vis dar plačiai naudojamą IPv4 interneto protokolą dėl išsekusio globaliai unikalių interneto adresų skaičiaus. Didėjantis IPv6 protokolo naudojimas, kuris šiuo metu siekia beveik 6 % interneto tinklo srauto, priverčia susirūpinti ir saugumo problemomis. Viena iš tokių saugumo problemų yra glaudžiai su IPv6 protokolu susijusio interneto kontrolės žinučių protokolo ICMPv6 (angl. *Internet Control Message Protocol*) maršrutizatoriaus skelbimo žinučių (toliau – RA) atsisakymo aptarnauti pažeidžiamumas. Šis pažeidžiamumas leidžia sulėtinti arba visiškai sutrikdyti operacinių sistemų darbą kompiuteriuose, esančiuose vietiniame tinkle. Tyrimo tikslas – nustatyti pasirinktų operacinių sistemų atsparumą RA žinučių atsisakymo aptarnauti atakai, esant skirtingiems techninės įrangos resursams.

Kiekvienas technologinis pažeidžiamumas yra sąlygojimas tam tikros blogos charakteristikos. Dėl šios priežasties siekiant išsiaiškinti pažeidžiamumo kilmę pirmiausia reikia suprasti nagrinėjamo technologinio funkcionalumo veikimo principą. Interneto kontrolės žinučių protokolas ICMPv6 yra neatskiriama IPv6 protokolo dalis, todėl siekiant įgyvendinti pilną IPv6 protokolo funkcionalumą ICMPv6 turi būti pilnai įgyvendintas kiekviename vietinio tinklo mazge. ICMPv6 protokolas naudojamas visuose vietinio IPv6 tinklo mazguose, pranešant apie įvykusias klaidas apdorojant paketus arba atliekant tinklo diagnostikos procedūras (*RFC 4443* 2006). Dar vienas, nuo IPv6 ir ICMPv6 neatskiriamas protokolas yra kaimyno aptikimo protokolas NDP (angl. *Neighbor Discovery Protocol*). NDP užtikrina gretimų IPv6 tinklo mazgų aptikimą, gretimų tinklo mazgų kanalo lygmens adresų nustatymą, aktyvių maršrutizatorių paiešką, IPv6 mazgų pasiekiamumo palaikymą ir informacijos apie kelius iki aktyvių kaimyno palaikymą ir atnaujinimą (*RFC 4861*, 2007). IPv6 tinkle maršrutizatorius siunčia RA žinutes periodiškai, apibrėžtu laiko intervalu. Kiekvienas tinklo mazgas, nepriklausomai nuo apibrėžto periodinio laiko intervalo, gali inicijuoti naują RA žinučių gavimą išsiunčiant maršrutizatoriaus prašymo žinutę (toliau – RS) maršrutizatoriui (Hagen 2006). Skelbimo ir prašymo žinučių siuntimo ir gavimo tikslas yra nuolatos atnaujinti tinklo mazgų maršrutizavimo lentelių informaciją ir pranešti apie naujus prie tinklo prisijungusius maršrutizatorius. Toliau straipsnyje yra aprašomas tyrimo aplinkos ir pačio tyrimo modeliavimas, RA atsisakymo aptarnauti atakos įgyvendinimas, tyrimo rezultatai ir analizė bei pažeidžiamumo prievencinės priemonės.



1 pav. IPv6 pažeidžiamumų aptikimo tinklo diagrama
Fig. 1. IPv6 vulnerability assessment network diagram

Tyrimo aplinka

IPv6 pažeidžiamumų tyrimui buvo sudaryta tinklo diagrama, kuri buvo realizuota virtualioje GNS3 kompiuterinių tinklų modeliavimo aplinkoje. Atsparumo ICMPv6 RA žinučių atsisakymo aptarnauti atakos tyrimui pasirinktos keturios operacinės sistemos: Windows XP; Windows 7; Windows 8.1 ir Ubuntu 14. Atsisakymo aptarnauti atakos inicijavimui panaudota Kali Linux operacinė sistema, kurioje yra integruoti tinklo paketų generavimo įrankis *Scapy* bei *THC-IPv6* IPv6 tinklo pažeidžiamumų testavimo įrankis. Panaudojus *Python 2.7* programavimo kalbą, buvo sudarytas programinis paketų siuntimo ciklas. Visos operacinės sistemos, įskaitant ir piktavalio kompiuterį (1 pav.), tyrimo metu veikė naudojant *VMware Player* virtualizijos platformą, kuri buvo sujungta su GNS3 modeliavimo aplinka. IPv6 tinklo funkcionalumui realizuoti panaudotas CISCO iOS c7200 virtualus maršrutizatoriaus atvaizdas (angl. *Image*).

RA žinučių atsisakymo aptarnauti atakos aprašymas

ICMPv6 RA žinučių „užtvindymo“ atakos įgyvendinimas susideda iš dviejų etapų:

1. Numatytojo maršrutizatoriaus suklastojimas;
2. Atsisakymo aptarnauti atakos įgyvendinimas.

Pirmajame etape vykdomas naujo numatytojo maršrutizatoriaus suklastojimas. Piktavalis (šiuo atveju Kali Linux operacinė sistema) siunčia suklastotą RA paketą. Šis pažeidžiamumas gali būti išnaudotas todėl, kad IPv6 protokolas leidžia bet kokiam į tinklą patekusiam įrenginiui identifikuoti save kaip maršrutizatorių. Toliau suklastotas įrenginys yra pridedamas į maršrutizatorių grupinio transliavimo grupę, o tinklo mazgai, gavę naujas RA žinutes, pakeičia savo numatytojo šliuzo (angl. *default gateway*) adresą į suklastoto maršrutizatoriaus adresą. Pirmajame etape atlikti veiksmai sąlygoja dar vieną ataką, t. y. dalinę tarpininko ataką. Ši ataka yra grėsminga, nes visi tinklo mazgų generuojami ir į internetą siunčiami tinklo duomenys keliaus per suklastotą maršrutizatorių bei potencialiai galės būti perskaityti arba iššifruoti.

Antrajame etape įgyvendinama atsisakymo aptarnauti ataka. Šios atakos esmę sudaro falsifikuotų ir atsitiktinių RA žinučių siuntimas visiems tinklo mazgams, taip priverčiant tinklo mazgus, kuriuose veikia operacinės sistemos, nuolatos atnaujinti maršrutizacijos lentelių įrašus ir išnaudoti turimus informacijos apdorojimo resursus.

Tyrimo rezultatai ir analizė

ICMPv6 protokolo RA žinučių atsisakymo aptarnauti tyrimas buvo suskirstytas į šešis mažesnius tyrimus. Šie tyrimai atlikti taikant skirtingus techninės įrangos resursus bei interpretuojant ir kompiliuojant programinius kodus (1 lentelė).

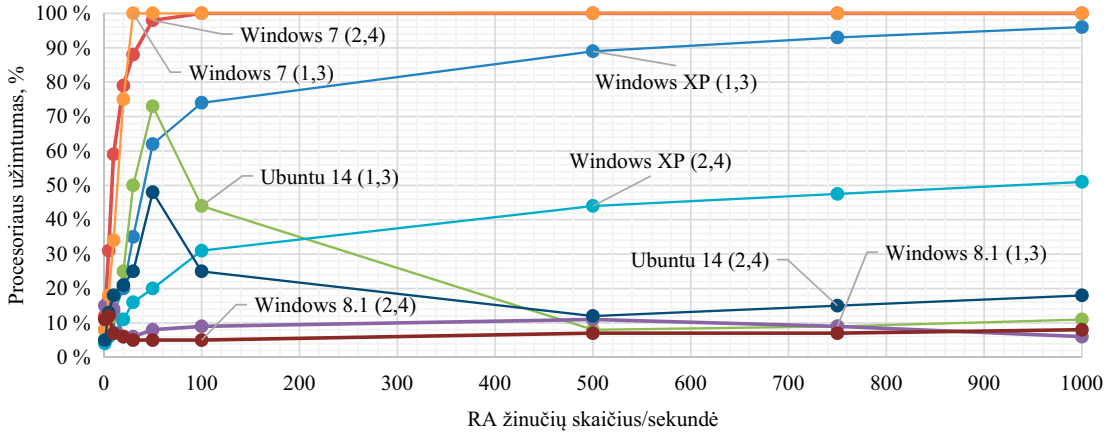
1 lentelė. Tyrimų techninės charakteristikos
Table 1. Study's technical characteristics.

Tyrimo Nr.	Naudotos techninės charakteristikos
1.	Dviejų branduolių IntelCore i7@2,2 GHz procesorius su 1 GB operatyviąja atmintimi.
2.	Keturių branduolių IntelCore i7@2,2 GHz procesorius su 1 GB operatyviąja atmintimi.
3, 5.	Dviejų branduolių IntelCore i7@2,2 GHz procesorius su 2 GB operatyviąja atmintimi.
4, 6.	Keturių branduolių IntelCore i7@2,2 GHz procesorius su 2 GB operatyviąja atmintimi.

Pabrėžtina tai, kad vienu metu buvo testuojama tik viena operacinė sistema. Visų tyrimų etapai vykdyti 45 s, t. y. per laikotarpį, kurio metu sistemos buvo laikomos tam tikroje RA žinučių siuntimo apkrovoje. Tyrimams Nr. 1–4 atlikti sudarytas ir panaudotas interpretuojamas programinis ciklas, kurio tikslas siųsti nurodytą kiekį RA žinučių su vienos sekundės delsos laiku.

Siekiant generuoti kaip įmanoma didesnę RA žinučių apkrovą, tyrimams Nr. 5 ir Nr. 6 atlikti panaudotas sukompiliuotas programinis kodas. Kompiliuoto programinio kodo naudojimo tikslas – generuoti ir siųsti kaip įmanoma daugiau RA žinučių, išnaudojant spartesnį sukompiliuoto kodo vykdymą taip sudarant maksimalią RA žinučių apkrovą. Testų metu buvo stebimos šios charakteristikos: procesoriaus užimtumas, tinklo apkrova, operatyviosios atminties užimtumas.

2 pav., šalia operacinių sistemų pavadinimų, pateiktuose skliausteliuose įrašyti tyrimų numeriai. Atliekant tyrimus Nr. 1–4 nustatyta, jog, didinant operatyviosios



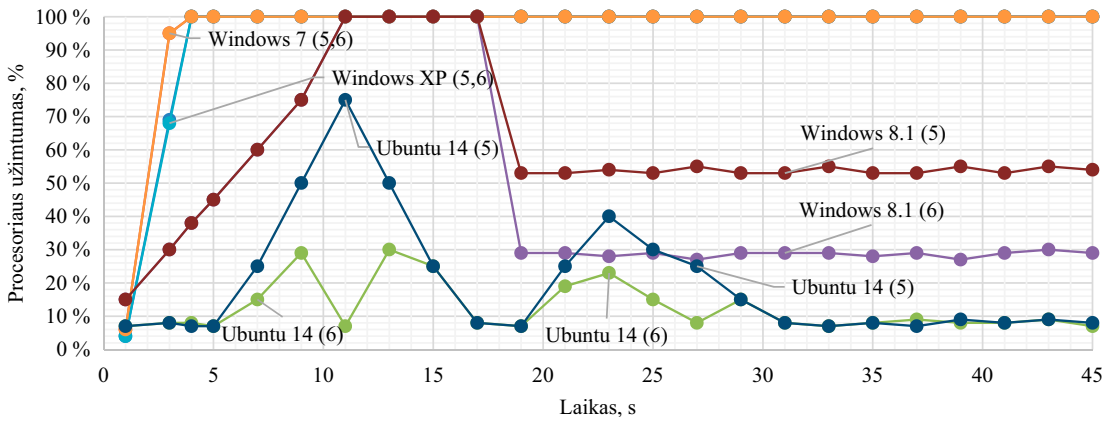
2 pav. Tyrimų Nr.1–4 procesoriaus užimtumo priklausomybės nuo RA žinučių apkrovos grafiniai rezultatai
Fig. 2. Studies' No. 1–4 processor usage dependency of RA messages load graphical results

atminties kiekį tyrimų rezultatai praktiškai nesikeitė ir skyrėsi tik keliais procentais. Dėl šios priežasties tyrimų Nr. 1 ir 3 bei Nr. 2 ir 4 rezultatai buvo sujungti. Iš tyrimo Nr. 1 ir 3 (2 pav.) rezultatų matyti, kad RA žinučių siuntimo atakai mažiausiai atsparios yra Windows XP ir Windows 7 sistemos. Abiejų minėtų operacinių sistemų darbas smarkiai sulėtėjo esant 50–100 RA žinučių per sekundę siuntimo apkrovai, sistemų darbas pasidarė nestabilus, atsirado dažnų strigčių. Viršijus 100 RA žin./s apkrovą Windows 7 operacinė sistema tiesiog užstrigo. Windows XP operacinė sistema užstrigo peržengus 500 RA žin./s apkrovos ribą. Ubuntu 14 operacinės sistemos atveju procesoriaus užimtumo pikas (73 %) buvo pasiektas esant 50 RA žin./s apkrovai, tačiau sistema nestrigo. Viršijus minėtą RA žinučių apkrovą, procesoriaus užimtumas galiausiai sumažėjo ir grįžo į normalų režimą. Iš tirtų operacinių sistemų RA žinučių apkrovai atspariausia buvo Windows 8.1 operacinė sistema. Windows 8.1 atveju procesoriaus darbo suaktyvėjimas matomas tik esant 1–10 RA žin./s apkrovai ir svyruoja nuo 14–17 %. Toliau didinant apkrovą, Windows 8.1 operacinės sistemos darbas praktiškai nesikeitė ir svyravo ties 6–7 % procesoriaus užimtumo. Iš tyrimo Nr. 2 ir 4 rezultatų matyti, kad RA žinučių siuntimo atakai mažiausiai atspari sistema yra Windows 7. Pasiekus 30–50 RA žin./s apkrovą procesoriaus užimtumas siekė 100 %, tačiau Windows 7 sistemos veiksena strigo nežymiai. Toliau padidinus RA žinučių apkrovą iki 100 RA žin./s ir daugiau, procesoriaus užimtumas išliko toks pats (100 %), bet darbas su Windows 7 sistema nebebuvo įmanomas, sistema užstrigo, o jos normalios veiksenos atstatymas buvo galimas tik perkrovus kompiuterį.

Įdomu tai, kad, nors ir būdama technologiškai senesnė, Windows XP sistema su šia ataka susidorojo geriau. Pasiekus 500 RA žin./s apkrovos ribą, sistema strigdavo tik kartais ir nežymiai. Pasiekus 1000 RA žin./s apkrovos ribą Windows XP sistemos procesoriaus užimtumas siekė 51 %, tačiau darbas su Windows XP sistema nebuvo įmanomas, sistemos veiksena pradėjo iš esmės strigti. Ubuntu 14 operacinės sistemos atveju procesoriaus užimtumo pikas (48 %) buvo pasiektas esant 50 RA žin./s apkrovai (pasikartojimo modelis identiškas Tyrimo Nr. 1 atvejui), tačiau sistema nestrigo. Viršijus minėta apkrovą, procesoriaus užimtumas pradėjo mažėti, kol grįžo į normalų režimą. Kaip ir Tyrimo Nr. 1 atveju, iš tirtų operacinių sistemų RA žinučių apkrovai atspariausia buvo Windows 8.1 operacinė sistema. Windows 8.1 atveju procesoriaus darbo suaktyvėjimas matomas tik esant 1–10 RA žin./s apkrovai ir svyruoja nuo 11–12 %. Toliau didinant apkrovą Windows 8.1 operacinės sistemos darbas praktiškai nesikeitė ir svyravo ties 5–7 % procesoriaus užimtumo.

3 pav. šalia operacinių sistemų pavadinimų esančiuose skliausteliuose įrašyti tyrimų numeriai. Atliekant tyrimus Nr. 5–6 nustatyta, jog Windows XP ir Windows 7 operacinių sistemų atveju didinant loginių branduolių skaičių rezultatai praktiškai nesikeitė. Dėl šios priežasties tyrimų Nr. 5–6 rezultatai Windows XP ir Windows 7 sistemų atveju buvo sujungti.

Iš tyrimų Nr. 5 ir 6 rezultatų (3 pav.) matyti, kad RA žinučių atsisakymo aptarnauti atakų labiausiai pažeidžiamos yra Windows 7 ir Windows XP operacinės sistemos. Windows 7 atveju procesoriaus užimtumas pasiekė 100 % apie trečiąją sekundę po atakos pradžios ir išliko toks pats visą atakos laiką. Windows XP atveju procesoriaus užimtumas pasiekė 100 % ribą 5-ąją sekundę po atakos pradžios. Abi sistemos užstrigo, o jų veikseną atstatyti galima buvo tik perkrovus kompiuterį. Naudojant dviejų



3 pav. Tyrimų Nr. 5–6 procesoriaus užimtumo priklausomybės nuo maksimalios RA žinučių apkrovos grafiniai rezultatai
Fig. 3. Study No. 5–6 processor usage dependency of maximum RA messages load graphical results

branduolių procesorių Windows 8.1 (5) operacinės sistemos atveju procesoriaus užimtumas pasiekė 100 % ribą 11-ąją atakos sekundę, tačiau šioje riboje išsilaikė tik 6 s. 19-ąją sekundę nuo atakos pradžios Windows 8.1 operacinės sistemos darbas stabilizavosi ties 53–54 % procesoriaus užimtumo ir išliko pastovus visą likusią tyrimo dalį. Ubuntu 14 operacinės sistemos atveju dviejų branduolių procesoriaus užimtumo pikai buvo pasiekti 11-ąją (75 %) ir 23-iąją (40 %) sekundę nuo tyrimo pradžios. Po to sistemos procesoriaus darbas stabilizavosi apie 7–9 % ir išliko pastovus likusį tyrimo laiką. Padidinus loginių branduolių skaičių iki keturių Windows 7 ir Windows XP operacinių sistemų tyrimo rezultatai nepasikeitė. Windows 8.1 operacinės sistemos atveju pradėjus tyrimą procesoriaus užimtumas didėjo nuosekliai ir apie vienuoliktą sekundę pasiekė 100 % ribą. Maksimalioje apkrovoje procesoriaus darbas išbuvo tik apie 5 s. Po to Windows 8.1 procesoriaus užimtumas pradėjo mažėti ir nusistovėjo ties 27–29 % užimtumo. Lyginant Windows 8.1 operacinės sistemos tyrimų Nr. 5 ir Nr. 6 rezultatus pastebimas ženklus, nusistovėjusio procesoriaus darbo apkrovos sumažėjimas nuo 55 % iki 29 % procesoriaus užimtumo. Dėl šios priežasties galima daryti išvadą, kad Windows 8.1 sistemos atveju didinant loginių branduolių skaičių, atsparumas RA atsisakymo aptarnauti atakai didėja. Naudojant 4 loginius branduolius Ubuntu 14 sistemos procesoriaus užimtumo pikai buvo mažesni nei tyrimo Nr. 5 atveju ir maksimaliai siekė 30 % procesoriaus užimtumo. Lyginant Nr. 5 ir Nr. 6 rezultatus matyti, kad nepriklausomai nuo loginių branduolių skaičiaus Ubuntu 14 operacinės sistemos darbas abiem atvejais pradėjo stabilizuotis ties 30-ąja sekunde po tyrimo pradžios ir po to išliko stabilus. Iš 3 pav. matyti, kad nusistovėjus procesoriaus darbui RA atsisakymo aptarnauti ataka įtakos Ubuntu 14 sistemos darbui praktiškai neturėjo.

Pažeidžiamumo prevencinės priemonės

Siekiant apsaugoti operacines sistemas nuo RA žinučių atsisakymo aptarnauti atakos, galima naudoti kelias apsaugos priemones. Nors dauguma apsaugos priemonių ir užkerta kelią RA žinučių atsisakymo aptarnauti atakos įgyvendinimui, tačiau tuo pačiu mažina arba net panaikina kaimyno aptikimo NDP protokolo funkcionalumą. Žemiau pateikiamos kelios šiai dienai žinomos apsaugos priemonės ir apibendrinami jų privalumai bei trūkumai.

Maršrutizatoriaus aptikimo funkcijos blokavimas. Šis apsaugos priemonės sprendimas yra bene pats paprasčiausias, tačiau panaikina IPv6 automatinės adresų konfigūracijos galimybę. Toks sprendimas būtų tinkamas tarnybinėms stotims, tačiau ne klientų sistemoms.

Tarpsegmentinio ekrano / ugniasienės naudojimas. Kliento pusėje panaudojus ugniasienę galima blokuoti RA žinutes iš pasirinktojo šaltinio. Ši apsaugos priemonė leidžia išlaikyti IPv6 automatinės adresų konfigūracijos galimybes ir blokuoti suklastotas RA žinutes. Nepaisant išvardintų privalumų, ugniasienės apsauga gali būti apeita suklastojant šaltinio adresą.

Prieigos kontrolės sąrašų naudojimas (Small 2013). Ši apsaugos priemonė leidžia maršrutizatoriuose ir komutatoriuose nustatyti maršrutizavimo taisykles, kurios draudžia persiųsti RA žinutes tinklo mazgams iš bet kokių tinklo įrenginių. Nors ši apsaugos priemonė ir užkerta kelią RA žinučių atsisakymo aptarnauti atakai, tačiau gali būti apeita fragmentuojant paketus. Taip pat ne visi maršrutizatoriai/komutatoriai turi prieigos kontrolės sąrašų funkciją.

Komutatoriaus su RA Guard funkcija naudojimas (Small 2013). Ši apsaugos priemonė taikoma specialiuose tarpiniuose tinklo įrenginiuose, dažniausiai tinklo komutatoriuose. *RA Guard* funkcija yra tikrinti kiekvieną į komutatorių patekusį RA paketą/žinutę ir remiantis nustatytomis

taisyklėmis minėtą žinutę praleisti arba atmesti. Pagrindinis *RA Guard* funkcijos privalumas yra tas, kad kiekvienas į komutatorių RA patekęs paketas išanalizuojamas, tačiau ne visi komutatoriai arba maršrutizatoriai turi *RA Guard* funkciją ir be to analizuoti kiekvienai RA žinutei ši funkcija naudoja papildomus procesoriaus resursus. *RA Guard* apsaugos priemonė taip pat gali būti apeita naudojant paketų fragmentaciją.

Atsižvelgiant į šiai dienai žinomų apsaugos priemonių privalumus ir trūkumus galima teigti, kad bene geriausias būdas apsisaugoti nuo RA žinučių atsisakymo aptarnauti atakos yra atlikti tam tikrus pakeitimus pačiame NDP protokole:

1. RA žinutė turėtų būti siunčiama tiesiai prašančiajam mazgui, o visos kitos žinutės, siunčiamos grupinio transliavimo adresu, t. y. tinklo mazgų grupei, turi būti atmestos. Šis pakeitimas leistų apsisaugoti nuo falsifikuotų RA žinučių.
2. Maršrutizatoriai neturėtų siųsti RA žinučių tinklo mazgams prieš tai negavę maršrutizatoriaus prašymo RS žinutės. Tai užkirstų kelią piktavaliams siųsti nelegalias RA žinutes.

Išvados

1. Tyrimo metu nustatyta, kad visos pasirinktos operacinės sistemos (Windows 7, XP, 8.1 ir Ubuntu 14) yra pažeidžiamos.
2. Išanalizavus tyrimo duomenis nustatyta, kad RA žinučių apkrova neturi praktinės įtakos kompiuterio operatyviajai RAM atminčiai. Taip atsitinka todėl, kad paketų buferiui dar nespėjus užsipildyti, procesoriaus užimtumas pasiekia maksimumą dėl falsifikuotų IPv6 adresų apdorojimo.
3. RA žinučių atsisakymo aptarnauti ataka neturi praktinės įtakos operacinės sistemos tinklo pralaidai, kadangi vienas kompiuteris nesugeba generuoti tokio skaičiaus paketų, kuris turėtų pastebimų pasekmių tinklo pralaidai.
4. Nustatyta, kad didinant loginių branduolių skaičių atsparumas RA žinučių atsisakymo aptarnauti atakai didėja, išskyrus Windows 7 operacinės sistemos atvejį.
5. RA žinučių apkrovos testui naudojant delsos laiką atspariausia buvo Windows 8.1 operacinė sistema. Generuojant maksimalią RA žinučių apkrovą, apkrovos testui atspariausia sistema buvo Ubuntu 14.
6. Kadangi praktiškai visos, šiai dienai žinomos apsaugos priemonės yra apeinamos arba riboja IPv6 protokolo funkcionalumą, bene geriausia RA žinučių pažeidžiamumo apsaugos priemonė būtų pačio NDP protokolo modifikavimas saugumo atžvilgiu.

Literatūra

RFC 4443. 2006. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification [interaktyvus]. The Internet Society [žiūrėta 2015 m. balandžio 24 d.]. Prieiga per internetą: https://tools.ietf.org/html/rfc4443

RFC 4861. 2007. Neighbor Discovery for IP version 6 (IPv6) [interaktyvus]. The IETF Trust [žiūrėta 2015 m. balandžio 24 d.]. Prieiga per internetą: https://tools.ietf.org/html/rfc4861

Hagen, S. 2006. *IPv6 essentials*. 2nd Ed. 1005 Gravenstein Highway North, Sebastopol, CA 95472. ISBN: 0-596-10058-2.

Small, J. 2013. *IPv6 attacks and countermeasures* [interaktyvus]. CDW Advanced Technology Services [žiūrėta 2015 m. balandžio 23 d.]. Prieiga per internetą: http://www.rmv6tf.org/wp-content/uploads/2013/04/5-IPv6-Attacks-and-Countermeasures-v1.2.pdf

ICMPV6 RA FLOODING VULNERABILITY RESEARCH

L. J. Jočys

Abstract

ICMPv6 is the newest version of internet control message protocol, whose main purpose is to send error message indicating packet processing failure. It is know that ICMPv6 is technologically vulnerable. One of those vulnerabilities is the ICMPv6 RA flooding vulnerability, which can lead to systems in Local Area Network slow down or full stop. This paper will discuss Windows (XP, 7, 8.1) and Linux Ubuntu 14 operating systems resistance to RA flooding attack research and countermeasures to minimize this vulnerability.

Keywords: IPv6, ICMPv6 RA flooding, IPv6 vulnerabilities.