Současný stav bezpečnosti protokolu IPv6

Nejeden síťový administrátor doufal, že při návrhu IPv6 se zvažoval současný stav (ne)bezpečnosti Internetu a že protokol přinese značná zlepšení. Je tomu opravdu tak? A jak je bezpečný současný IPv6 svět?

Atraktivním tématem bezpečnosti protokolu IPv6 se zabývalo již několik článků. Následující text si klade za cíl navázat na ty již publikované v DSM (1/2011), dostat se hlouběji do problematiky, podrobněji rozebrat explicitní bezpečnostní prvky (IPsec, SeND) i ty s implicitním dopadem (rozšiřující záhlaví, rozsáhlý adresní prostor) a pokrýt současný vývoj.

Od IPv6 se v oblasti bezpečnosti očekávalo možná až příliš, protože předchůdce IPv4 mnoho bezpečnostních prvků ve svém návrhu neobsahoval. Ve skutečnosti však byla největším opravdovým přínosem protokolu v oblasti bezpečnosti původně povinná [1] implementace podpory IPSec (Internet Protocol Security), šifrovaného přenosu mezi koncovými uzly, na každém zařízení podporujícím IPv6. Tato povinnost byla později zmírněna na doporučení [2] vzhledem ke konceptu Internet of Things, tedy připojení téměř čehokoli do Internetu. Např. lednička, hodinky nebo senzory nebudou mít procesor dostatečně silný na to, aby byl neúměrně zatěžovaný kryptografickými operacemi a všestranný natolik, aby podporoval protokoly pro výměnu klíčů. Na druhou stranu nové směrovací protokoly RIPng, EIGRPv6 a OSPFv3 v oblasti bezpečnosti spoléhají pouze na IPSec.

Na kryptografii spoléhá také další explicitně bezpečnostní mechanismus protokolu. Slabé místo lokálních sítí – nezabezpečený protokol ARP (Address Resolution Protocol), který fungoval na pomezí druhé a třetí vrstvy ISO/OSI modelu, byl nahrazen specifickými zprávami protokolu ICMPv6 (Internet Control Message Protocol version 6). Tyto zprávy tvoří protokol Neighbor Discovery Protocol (NDP), tedy výhradně třetí vrstvy (viz Box 1). NDP sám o sobě také není odolný vůči různým formám podvrhů nebo falšování zpráv, které mohou vést např. k útokům typu Man-in-the-Middle nebo Denial-of-Service [3]. Za účelem prokázání původu a věrohodnosti zpráv vznikl mechanismus CGA (Cryptographicaly Generated Addresses) a s ním i protokol SeND (Secure Neighbor Discovery), bezpečná varianta protokolu NDP. I tak zůstává bezpečnost prvního skoku na lokálních sítích citlivou oblastí, které je potřeba věnovat zvláštní pozornost v prostředích s protokolem IPv6. Rozhodně už není možné úplně odfiltrovat IMCPv6 zprávy, protože se staly nedílnou součástí protokolu IPv6, který bez nich nemůže fungovat.

Rozšiřující záhlaví

Protokol IPv6 postihlo samozřejmě také mnoho různých změn, které se netýkají bezpečnosti explicitně, ale mají nemalý vliv. Jednou takovou změnou je zjednodušení záhlaví protokolu (viz Box 2). Původní záhlaví IPv4 padlo za oběť rychlosti, vše se zjednodušilo a některé možnosti protokolu se spolu s těmi novými přestěhovaly do tzv. rozšiřujících záhlaví (Extension Headers).

Asi nejdiskutovanější je v současnosti fragmentační záhlaví a potažmo fragmentace jako taková. V prostředí protokolu IPv6 je možné fragmentovat data pouze na zdroji, na mezilehlých bodech nikoli. Potenciální útočník tak má úplnou kontrolu nad tím, jak budou datové proudy vypadat. Snadno pak může zneužít nedokonalosti v implementacích IPv6 překrývajícími se fragmenty nebo pakety, jejichž konečná velikost je větší než avizovaná. Zranitelnosti typu buffer overflow v nových implementacích IPv6 skutečně existují [4]. Objevují se ale i techniky obcházení systémů prevence nebo detekce průniku [5] s využitím řízené fragmentace, což je asi nejživější oblast protokolu. Přístup ke zpracování

atomického fragmentu (paketu, který obsahuje fragmentační záhlaví, ale ve skutečnosti fragmentován není) byl standardizován teprve v květnu 2013 [6]. Nyní se diskutuje o úplném odstranění fragmentace [7].

Prostor, který si tvůrci protokolu ponechali v jednotlivých záhlavích pro další případný vývoj, může být také zneužit k nelegitimním účelům. Do polí možností, která nejsou nikterak omezena právě z důvodu rozšiřitelnosti, je možné vložit libovolná data. Vzniká tak elegantní skrytý kanál, který odhalí pouze systém prevence úniku dat s implementovanou hloubkovou inspekcí paketů protokolu IPv6.

Průzkum sítě

Implicitní vylepšení bezpečnosti se očekávalo i od největší změny, kterou IPv6 přináší. Velký adresní prostor jistým způsobem stíží např. šíření internetových červů nebo průzkum sítě potenciálním útočníkem. Uvažujme o podsíti s prefixem /64 a v ní 100 rovnoměrně rozmístěných aktivních hostů. Při rychlosti 1 000 000 paketů za sekundu by trvalo více než 2 800 let, než bychom odhalili adresu prvního aktivního hosta [8]. To ovšem platí pouze za předpokladu použití hrubé síly. Byly publikovány metody selektivního skenování [9], které mohou za určitých podmínek časovou náročnost značně zmírnit. Ve skutečnosti totiž většina IPv6 adres není náhodná [10], a tím se zmenšuje adresní prostor, který je nutné skenovat. V adresách se objevují tyto vzory:

- *Autokonfigurace* – IPv6 adresy založené na MAC adresách, kde je ve skutečnosti neznámých jen 24 oproti 64 bitům. Je snaha tyto adresy z konceptu IPv6 odstranit [11] také kvůli ztrátě soukromí majitele.
- *IPv4* – Často použité ve dvouzásobníkovém prostředí, např. adresa 2001:db8::192:168:1:1. V tomto případě je velikost adresního prostoru stejná jako v prostředí protokolu IPv4.
- *Nízké bajty* – Pouze spodní bajt či dva jsou použity k adresaci hostů. Adresní prostor je tak pouze 28 nebo 216.
- *Slovní adresy* – Adresy jako 2001:db8::b00b:babe nebo 2001:db8::dead:beef se dobře pamatují, ale také se dají lehce uhádnout, např. použitím slovníku takovýchto hexadecimálních slov.
- *Port služby* – Používají se na strojích dedikovaných pro určitý typ služby. Adresa webového serveru by pak byla 2001:db8::80 a adresní prostor opět pouze 28.

I přes tato vylepšení skenovacích technik je pravděpodobné, že se potenciální útočníci zaměří na službu DNS. Pokud administrátor používá naprosto náhodné adresy na své síti, bude pravděpodobně používat, vzhledem k formátu IPv6 adres, také dynamické DNS. DNS server se tak může stát častějším terčem útoků. Zvykem administrátorů bývá pojmenovat servery podle vzorů, např. řečtí bohové nebo hlavní města států. I v tomto případě si útočník může ulehčit práci použitím slovníku.

Bezpečnost současného IPv6 světa

Rozhodně se nedá říci, zda je protokol IPv6 bezpečnější než IPv4. Každý má svá specifika, o kterých je třeba vědět a počítat s nimi. Pověsti protokolu určitě

Neighbor Discovery Protocol (NDP) BOX 1

NDP je tvořen podmnožinou zpráv protokolu IMCPv6. Mezi jeho funkce patří objevování směrovačů, mechanismus autokonfigurace, překlad IPv6 adres na MAC adresy, přesměrování, detekce duplicitních adres a dostupnosti uzlů.

Secure NDP (SeND) je zabezpečená varianta protokolu NDP. Zajišťuje prokázání původce zprávy a její integritu. Nejčastější použití je pak pro autorizaci směrovače těmito podepsanými zprávami.

Cryptographically Generated Addresses (CGA) je prostředek, kterým se zajišťuje bezpečnost protokolu SeND. Bezpečná adresa hosta je vypočtena jednosměrnou hash funkcí z jeho původní adresy a veřejného klíče. Každou zprávu pak podepisuje svým soukromým klíčem. Stinnou stránkou je možnost útočníka vytvářet své vlastní CGA a těmi zahlcovat cíl, který spotřebuje velkou část svého výpočetního času ověřováním nesmyslných podpisů. Nemůže si však přivlastnit už existující adresu a vydávat se za někoho jiného.

Záhlaví protokolu IPv6 a rozšiřující záhlaví BOX 2

Záhlaví protokolu IPv6 byla z výkonnostních důvodů zjednodušena. Obsahují pouze informace o verzi protokolu, třídě přenosu a návěští toku (důležité pro Quality of Services), délce přenášených dat, následujícím záhlaví, maximálním počtu skoků, zdrojové a cílové adrese.

Verze, 4 bity	Třída přenosu, 8 bitů	Návěstí toku, 20 bitů
Celková délka dat, 16 bitů	Násl. hlavička, 8 bitů	Max. počet skoků, 8 bitů
Zdrojová adresa, 128 bitů		
Cílová adresa, 128 bitů		

Ostatní možnosti se, včetně několika nových, přestěhovaly do rozšiřujících záhlaví. RFC 2460 [12] definuje celkem 6 typů záhlaví (Hop-by-Hop Options, Destination Options, Routing Header, Fragment Header, AuthenTication Header, Encapsulating Security Payload). Pořadí jejich výskytu v paketu, počet a způsob zpracování není detailně definován a existující zásady jsou pouze doporučeními. Tato flexibilita protokolu má zásadní bezpečnostní dopady. Vhodným řetězením záhlaví je možné obcházet např. firewally nebo se vyhnout hloubkové inspekci paketů. V současných implementacích zásobníku protokolu IPv6 je přístup k rozšiřujícím záhlavím nekonzistentní a nezřídka k jejich zpracování nedochází korektně. Není divu. Pokud totiž zařízení podrobně analyzuje všechna záhlaví, není těžké ho zahltit a způsobit tak jednoduchý, ale účinný útok typu Denial-of-Service.

nepřidá skutečnost, že implementace zásobníku jsou v komerčně dostupných zařízeních na různých úrovních.

Některá zařízení ho nepodporují otevřeně, jiní výrobci věří, že stačí správně zpracovat nové záhlaví a vše je vyřešeno. Jsou však i tací, u nichž je podpora na velmi vysoké úrovni. Doporučuji si u výrobce ověřit, které RFC požadavky zařízení splňují, IPv6 funkčnosti neopomíjet a každé zařízení předem otestovat. Nedávno jsem se setkal se systémem prevence průniků s integrovaným firewallem. Ten dokázal spolehlivě identifikovat pokusy o obcházení firewallu. Při vypnutí této funkčnosti ale vyšlo najevo, že integrovaný firewall je těmi samými technikami zranitelný.

V roce 2012 bylo oficiálně registrováno 23 zranitelností (Common Vulnerabilities and Exposures – CVE) souvisejících přímo s protokolem IPv6, v roce 2013 pak 31 [13]. Je to v porovnání s rozšířením využití těchto funkčností v reálném prostředí málo nebo moc? A kolik jich bude v roce 2014?

Je zřejmé, že nasazení protokolu se nevyhne žádná organizace závislá na Internetových službách. I pokud má v současnosti dostatek IPv4 adres, pro partnery, současné nebo budoucí zákazníky už to pravda být nemusí. IPv6 není dokonalý, vylepšení však přináší a stále se vyvíjí. Při jeho nasazení je nutné brát bezpečnostní specifika v potaz, zařízení testovat a platí, že čím dříve se začne, tím lépe. Čekání na další verzi protokolu by připomínalo Čekání na Godota.

Ve většině organizací, kde jsem měl možnost o tématu IPv6 diskutovat, si je IT oddělení tohoto problému vědomo a snaží se nakupovat nová zařízení s podporou IPv6. Nedaří se získat podporu vedení, které uvádí především dva argumenty: nevidí obchodní důvod k nasazení protokolu a mylně se domnívá, že až to bude nutné, postačí přepnout pomyslný IP přepínač z polohy '4' do polohy '6'.

K prvému bych dodal už jen pár čísel, ze kterých vyplývá jasný trend. Celosvětově přistupovalo ke službám Internetového giganta Google k 1. lednu 2013 1,07 % uživatelů, o rok později už to bylo 2,80 % [14] – nárůst o více než 160 %. Podobný vývoj se očekává i v roce 2014, kdy se v druhé polovině února prolomila hranice 3 % [14]. Optimistické odhady očekávají dvouciferné číslo koncem letošního roku. V České republice se aktuálně jedná o 2,44 % uživatelů [14]. Pokud je Internetová přítomnost a klientský online přístup ke službám stěžejní pro vaši organizaci, nečekejte. Podle mého názoru nasazení protokolu IPv6 úzce souvisí se zachováním kontinuity podnikání a navíc tím můžete získat konkurenční výhodu.

K druhé námitce bych chtěl zdůraznit komplexnost, která vzniká zavedením další verze IP protokolu do sítě. I když začne organizace používat IPv6 pouze směrem do Internetu, je důležité si uvědomit, že přechod na IPv6 je běh na dlouhou trať a období koexistence s IPv4 bude trvat řádově roky. Po celou dobu je nutné stejnoměrně konfigurovat, udržovat a zabezpečovat dva poměrně odlišné protokoly. Bude nutné přizpůsobit také procedury, procesy a politiky společnosti. Překladový mechanismus IPv4 adres na IPv6 a opačně na perimetru bude, společně s překladem veřejných a privátních IPv4 adres (NAT, PAT), velice pravděpodobně tvořit úzké hrdlo sítě. Nasazení protokolu i směrem dovnitř společnosti bude nahrávat jednodušší údržba a koncept IPv6, který podporuje přímou komunikaci mezi koncovými zařízeními. Tomu se musí přizpůsobit celková síťová, komunikační a bezpečnostní architektura organizace. Novému protokolu je nutné kromě hardwarového vybavení přizpůsobit také software. Přepsání nebo upgradu se nevyhnou nejen některé obchodní aplikace, ale i aplikace používané na půdě IT oddělení. Žádný IP přepínač opravdu neexistuje.

Petr Fojtů
petr.fojtu@cz.ey.com

Ing. Petr Fojtů

Je absolventem Fakulty aplikovaných věd Západočeské univerzity v Plzni. V současnosti pracuje jako konzultant informační bezpečnosti ve společnosti EY.

POUŽITÉ ZDROJE

[1] LOUGHNEY, J. RFC 4294, *IPv6 Node Requirements*. Duben 2006.
[2] JANKIEWICZ, E., LOUGHNEY, J., NARTEN, T. RFC 6434, *IPv6 Node Requirements*. Prosinec 2011.
[3] NIKANDER, P., KEMPF, J., NORDMARK, E. RFC 3756, *IPv6 Neighbor Discovery (ND) Trust Models and Threats*. Květen 2004.
[4] HEUSE, M. *IPv6 Insecurity Revolutions*. Hack in the Box, 8.–11. října 2012. Kuala Lumpur, Malajsie.
[5] ATLASIS, A. *Attacking IPv6 Implementation Using Fragmentation*. Black Hat Europe, 14.–15. května 2012. Amsterdam, Nizozemsko.
[6] GONT, F. RFC 6946, *Processing of IPv6 "Atomic" Fragments*. Květen 2013.
[7] BONICA, R., KUMARI, W., BUSH, R., PFEIFER, H. draft-bonica-6man-frag-deprecate-02, *IPv6 Fragment Header Deprecated*. Červenec 2013.
[8] CONVERY, S. and MILLER, D. *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0)*. Cisco Systems Technical Report, 2004.
[9] GONT, F., CHOWN, T. draft-ietf-opsec-ipv6-host-scanning-03, *Network Reconnaissance in IPv6 Networks*. Leden 2014.
[10] GONT, F. a HEUSE, M. *Security Assessment of IPv6 Networks and Firewalls*. IPv6 Kongress 2013, 6.–7. červenec 2013. Frankfurt, Německo.
[11] GONT, F., COOPER, A., THALER, D., LIU, W. draft-gont-6man-deprecate-eui64-based-addresses-00, *Deprecating EUI-64 Based IPv6 Addresses*. Říjen 2013.
[12] DEERING, S., HINDER, R. RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*. Prosinec 1998.
[13] Internetové stránky organizace MITRE Corporation - CVE-Common Vulnerabilities and Exposures, http://cve.mitre.org/, přistupováno v únoru 2014.