IPv6 Mýty a skutečnost, díl VI. - Bezpečnostní mechanizmy

17. 3. 2011 6:25 Tomáš Podermański, Matěj Grégr

Seriál Pohněme s IPv6

- IPv6 Mýty a skutečnost, díl V. - Zjednodušené hlavičky
- IPv6 Mýty a skutečnost, díl VI. - Bezpečnostní mechanizmy
- IPv6 Mýty a skutečnost, díl VII. - Podpora Multicast a anycast provozu
- IPv6 Mýty a skutečnost, díl VIII. - Přechodové mechanizmy
- IPv6 Mýty a skutečnost, díl IX. - Quo Vadis, IPv6?

Všechny díly seriálu

Bezpečnost počítačových sítí, společně s jejích rostoucí důležitostí, jistě nenechává nikoho chladným. Přináší protokol budoucího Internetu nějaká bezpečnostní vylepšení oproti IPv4, anebo je se potřeba obávat nových bezpečnostních rizik? Odpověď se pokusíme najít v dnešním dílu věnovanému problematice bezpečnostních mechanizmů protokolu IPv6.

IPv6 poskytuje mnohem lepší zabezpečení pro aplikace a sítě. Vysoké úrovně zabezpečení je dosaženo využitím protokolu IPSec, který zajišťuje autentizaci a šifrování přenášených dat s využitím kryptografických metod. Podpora mechanizmu IPSec je povinně požadována jako součást základní implementace IPv6. Další bezpečnostní prvek IPv6 je dán velkým adresovým prostorem, nad kterým není možné provádět sekvenční scanning a vyhledávat zařízení zapojená v IPv6 síti. IPv6 poskytuje lepší úroveň zabezpečení, než jaká byla možná v sítích na bázi IPv4.

Tímto krátkým odstavcem, jak vytaženým z reklamní brožurky, by mohl náš dnešní díl skončit. V různých diskusních skupinách a mnohých dokumentech zabývajících se otázkami bezpečnosti IPv6 je toto téma řešeno (nabízelo by se slovo odbyto) přesně tímto způsobem. Jak už je v našem seriálu zvykem, nenecháme se uchlácholit lacinými reklamními slogany a podíváme se na otázku bezpečnosti IPv6 trošku detailněji.

Technologickým garantem seriálu Pohněme s IPv6 je CZ.NIC .

Horizontální skenování

Skenování představuje základní prostředek útočníka k odhalení případných bezpečnostních nedostatků. Výstupem skenování bývá množina adres zařízení, která jsou v síti aktivní a tedy vhodná k vedení potenciálních útoků. Skenování tedy představuje první útočníkův krok a je vstupní bránou pro vykonávání

dalších záškodnických akcí. Ze strany správců je vyvíjeno poměrně velké úsilí k eliminaci těchto aktivit. V případě IPv4 se skenování provádělo poměrně snadno. Útočník si vybral potenciálně zajímavou síť a postupně otestoval jednu adresu za druhou. Vzhledem k omezenému množství adres se nejednalo o časově nijak náročnou operaci.

V případě IPv6 je situace odlišná. V dřívějších dílech jsme si řekli, že pro koncové sítě je vyhrazený adresový prostor v délce 64 bitů. Taková kombinace nám dává 1.8×10^{19} adres. Prostými propočty zjistíme, že pokud bychom chtěli provést skenování na takové síti hrubou silou (*Brute Force*), trvalo by 28 let, než bychom nalezli první aktivní IPv6 adresu. Skenování by navíc muselo být vedeno s intenzitou 1 milion testů za sekundu, což by vyžadovalo datové pásmo o šířce 400Mb/s. S klidem tedy můžeme říci, že tato varianta je mimo hru.

Je nereálné, že by se různé záškodnické a hackerské skupiny spokojily s takovýmto závěrem, a skenování sítí zkrátka přestaly provádět. Vzniknou tedy snahy, jak poměrně velký adresový prostor zúžit a zaměřit se na ty adresy, u nichž je větší pravděpodobnost výskytu. Jaká možná zjednodušení se dají použít:

- **Služby poskytující informace o adresách:** DNS, Dynamické DNS, Whois, NetFlow záznamy, logy serverů, NI Query (RFC 4620) atd.
- **Odhadování na základě předpokládaného výskytu adres:** EUI 64, sekvenčně přidělované adresy, tzv. *well-known MAC adresy*.
- **Odhalování na základě existujících IPv4 adres:** v různých tunelovacích systémech, na serverech atd. IPv6 adresy serverů bývají dnes často konfigurovány tak, že se současná IPv4 adresa serveru zapíše hexadecimálně do spodních 32 bitů IPv6 adresy.

Názorná ukázka provedení takového skenování byla prezentována na konferenci 27th Chaos Communication Congress . Výsledek provedených optimalizací je poměrně zajímavý. Nalezeno bylo cca 2000 aktivních IPv6 adres v průběhu 20 vteřin.

Výše uvedené komplikace platily pouze v případě snahy identifikovat aktivní IPv6 adresy ze vzdálených sítí. Pokud se ale útočník dostane na úroveň lokální sítě, je v naprosto odlišné situaci. Zde není problém odposlouchávat informace signalizačního protokolu ICMPv6 v multicastové skupině *FF02::1*, a z této komunikace sestavit přehled o všech aktivních IPv6 uzlech v lokální síti. Není potřeba dokonce žádného sofistikovaného nástroje. Pro začátek můžete vyzkoušet příkaz `ping6 FF02::1`, a poté prohlédnout cache sousedů (*Neigbor Cache*). Bezpečně v ní najdete *Link-Local* adresy všech zařízení v lokální síti.

Vzdálené skenování sítě je v IPv6 prostředí o něco náročnější a vyžaduje kombinování informací z více zdrojů. Lze tedy říci, že oproti IPv4 zde dochází k jisté komplikaci, nicméně vhodným postupem lze dosáhnout velice dobrých výsledků. Skenování na úrovni lokálních sítí je naopak operace velice jednoduchá a proveditelná jakýmkoliv uzlem připojeným v příslušné lokální síti.

Bezpečný IPSec

Rozšíření protokolu v podobě IPSec umožňuje volitelně autentizovat a zabezpečovat provoz pomocí rozšiřujících hlaviček AH (*Authentication Header*) a ESP (*Encapsulation Security Payload*), kde se hlavička AH používá k autentizaci a pro kontrolu síťové adresy a ESP pro šifrování obsahu. Hlavičky mohou být použity současně, pokud požadujeme autentizaci i šifrování, nebo zvlášť. Povinně implementovaná musí byt pouze hlavička ESP . Do budoucna se plánuje vypuštění hlavičky AH a implementace IPSec budou používat pouze hlavičky ESP. Hlavička ESP šifruje obsah datagramu, takže účinně zabraňuje odposlechu, nicméně informace z hlaviček IP datagramů (například zdrojová a cílová IP adresa) mohou být útočníkem bez problému odposlouchávány.

IPSec může obecně pracovat ve dvou režimech. První varianta řeší zabezpečení komunikace mezi koncovými uzly. Další varianta použití IPSec-u je tunelovací režim. Tento je použitelný zejména pro propojování celých sítí. Data vstupující do zařízení realizujících tunelovací režim jsou obalena vnější zabezpečenou vrstvou a předána protější straně tunelu, která zajistí opačný proces.

Samotný proces šifrování a autentizace vyžaduje další podpůrné mechanizmy. Jedná se zejména o správu

bezpečnostních asociací, pravidelnou výměnu klíčů, správu certifikačních cest. Případné zájemce lze odkázat na publikaci PAVLA SATRAPY IPv6 , kde je problematika IPSecu popsána velice precizně.

IPSec a aplikace

IPSec, jak už to s novinkami bývá, nepřináší pouze výhody v podobě možnosti bezpečného transportu dat, ale také jisté komplikace. První riziko pramení z faktu, že samotná data jsou šifrována. Tímto se veškerá zařízení v podobě firewallu, IDS, IPS, monitorovacích sond stávají prakticky slepá. Obsah IP datagramu je šifrovaný a výše uvedené systémy se nedostanou dál než na úroveň IPv6 hlavičky. Zcela jim zůstanou utajeny informace o protokolu vyšší vrstvy – nedokáží identifikovat, zda v šifrovaném obsahu je přenášena webová TCP relace, UDP datagramy útočící na DNS server, záškodnická ICMPv6 zpráva anebo další rozšiřující hlavičky. Lze namítnout, že úplně stejnému typu problému jsme vystaveni při jakékoliv šifrované komunikaci (např. https, ssh, imaps). To je do jisté míry pravda, ani tam nedokážeme provádět detailní inspekci obsahu, nicméně máme k dispozici informace o provozované službě a směru komunikace. V rámci firemní bezpečnostní politiky dokážeme například definovat, že služba https (443) na serveru s adresou a.b.c.d (či spíše *a:b::c:d*) je v pořádku, zatímco provoz služby na portu 445 (*Microsoft-DS*) již nikoliv. V případě IPSec tuto rozlišovací schopnost ztrácíme.

Ochrana před IPSec-em

Z výše uvedeného plyne doporučení, které se na první pohled mnohým může jevit poněkud zvláštně. **Provoz protokolu IPSec by měl být blokován na úrovni korporátního firewallu.** Obecně lze problém přirovnat k letištnímu provozu, kdy vstupní kontrola zcela jistě nedovolí nikomu vstoupit do letadla s nedobytným, olověným bezpečnostním kufříkem, aniž by znala jeho obsah. Případné výjimky pro provoz IPSec-em by měly vznikat jen pro ta zařízení, o kterých je bezpečně známo, že jsou sama o sobě dostatečně zabezpečena a nemohou tak posloužit jako útočníkova přestupní stanice do vnitřní sítě. IPSec je realizován jako jedna z rozšiřujících hlaviček a tedy pro filtraci je možné použít prostředky, které jsme si popsali v předchozím dílu . V některých implementacích firewallu je možno specifikovat i další parametry, jako například Index asociace (SPI), a tímto omezit provoz jen na správcem schválené IPSec asociace.

Další spornou výhodou IPSecu je, že pro aplikace pracuje zcela transparentně. To přináší velkou výhodu tvůrci aplikace, který využívá běžná volání systému pro práci se sítí, a zabezpečením se nemusí nijak zabývat. To, co je výhodou, je současně obrovským nedostatkem. Aplikace tímto ztrácí možnost ověřit, zda komunikuje zabezpečeně a s důvěryhodnou protistranou. Dotazovací dialog na ověření certifikátu, který vám nabízí například webový prohlížeč při vstupu do internetového bankovnictví, je najednou skryt před očima aplikace. Nemůžete si být jistí, zda vám nějaký útočník nepodstrčil prostřednictvím DNS jinou IP adresu, kde není bezpečnostní politika prostřednictvím IPSec definována, a vy tedy komunikujete s útočníkem nezabezpečeně.

IPSec naživo

Zbývající problémy IPSec-u jsou ryze praktického rázu. Po detailnějším seznámení s architekturou IPSec-u zjistíte, že se jedná o poměrně složitý systém. Pokud jste se někdy pokoušeli zprovoznit IPSec v reálné síti (nikoliv ve školní laboratoři), jistě mi dáte za pravdu, že se nejedná o zcela jednoduchý proces – správa certifikátů, asociací, definice politik atd. Jednotlivé implementace ne vždy fungují zcela spolehlivě. Diagnostické nástroje jsou velmi omezené, což je zvláště nepříjemné, pokud nemáte kontrolu nad oběma konci spojení a případné problémy musíte řešit s využitím česko-německé angličtiny. I přesto, že byl mechanizmus IPSec-u jako volitelné rozšíření integrován i do protokolu IPv4, je jeho využívání spíše omezené. Příkladem může být snaha použití IPSec protokolu pro zabezpečení komunikace mezi radius servery v projektu Eduroam . I přes nemalé úsilí vysoce kvalifikovaných správců je nakonec upřednostňována varianta aplikačního SSL/TLS zabezpečení protokolem RadSec . Nejčastěji můžeme nalézt využití IPSec v tunelovacím režimu, kdy jsou jeho prostřednictvím vytvářeny virtuální privátní sítě (VPN), například pro propojení firemních poboček. Nicméně i v těchto případech je mnohdy voleno jiné řešení – například prostřednictvím OpenVPN nebo komerčními produkty (paradoxně mnohdy využívajícího IPSec-u, ale v poněkud stravitelnější podobě).

IPSec rozhodně nepatří mezi zavrženíhodné technologie a v IP sítích si postupně nachází své místo. Díky tomu, že byl integrován jako volitelná nadstavba do protokolu IPv4, existují již praktické zkušenosti, které

mohou být využity ke zlepšení standardů a zdokonalení stávajících implementací. Oproti původní představě rozhodně nelze IPSec považovat za komplexní řešení bezpečnostních problémů budoucího Internetu, ale pouze jako prostředek ke zvýšení úrovně zabezpečení mezi komunikujícími uzly, tam, kde je to požadováno.

Ale žádné další problémy už nejsou, je to tak?

Jak jistě víme, síť není ohrožena pouze na úrovni transportní cesty. Téměř každá operace, počínaje detekcí směrovače, objevováním sousedních uzlů, zjišťováním adres rekurzivních DNS serverů, přihlašováním do multicastové skupiny, překládáním adres atd. je potenciálním zdrojem problémů a vnáší do sítě příslušná rizika. Popis jednotlivých rizik a problémů s nimi spojených by nepochybně vydal na samostatný seriál. Shrňme v rychlosti jen ty nejznámější a v současné době nejpalčivější bezpečnostní problémy IPv6. Vzhledem k tomu, že souvisejícími bezpečnostními problémy se snažíme zabývat vždy v příslušných dílech, bude u mnohých případů uveden odkaz, kde jsme problematiku již řešili, anebo řešit budeme.

Podvržení záznamů v cache sousedů (Neighbor Cache)

Jednotlivé uzly v síti si udržují vyrovnávací paměť obsahující vazbu IPv4 (arp tabulka), IPv6 (*Neigbour Cache*) a MAC adresa. Doba uchovávání záznamů se liší u různých operačních systémů a zařízení. Většinou je ale doba uchovávání záznamů u IPv6 delší než u záznamů IPv4. Pokud tedy bude podvrhnut záznam, bude ve vyrovnávací paměti uchován po delší dobu. Z hlediska způsobu podvržení záznamů nabízí IPv6 obdobné možnosti jako IPv4 (*ARP spoofing* , NC spoofing).

DoS – pomocí detekce duplicity/dosažitelnosti

Pro detekci duplicity adres vytvořených mechanizmem autokonfigurace se používá standardní nebo optimistický algoritmus Duplicate Address Detection (DAD). K získání informací o duplicitě používá kombinaci zpráv *Neighbor Solicitation* a *Neighbor Advertisement*. Ty jsou zasílány na skupinovou adresu, kterou může útočník odposlouchávat a následně na každý výskyt nové adresy v síti reagovat zprávou informující o tom, že adresa je již používána. Tímto znemožní uzlu nakonfigurovat si IPv6 adresu, čímž zamezí přístupu do sítě.

Podvržení oznámení směrovače zpráv, šíření falešných oznámení směrovače

Jak jsme si již dříve popsali, integrální součástí IPv6 je mechanizmus autokonfigurace uzlů (SLAAC). Autokonfigurace je zajišťována dvojicí ICMPv6 zpráv – prostřednictvím výzvy směrovači (RS – Router Solicitation) a oznámení směrovače (*RA – Router Advertisment*). Tyto zprávy je možno podvrhnout, anebo v síti, kde není konfigurován IPv6 směrovač, cíleně šířit falešné zprávy. Tímto je možno přesměrovat data z klientů na jiný uzel v lokální síti. Problematiku jsme probírali v díle o autokonfiguraci .

DHCPv6 – podvržení odpovědi, chybějící konfigurační parametry

Podobně jako v IPv4 i v IPv6 může být odpověď od DHCPv6 serveru podvržena útočníkem, který na síti provozuje vlastní server. V IPv4 tento mechanismus efektivně řešil DHCP Snooping, tedy aktivní filtrování DHCP zpráv na L2 prvcích. V IPv6 zatím takovéto řešení není masově implementováno v zařízeních. Podpora pro DHCPv6 Snooping v praxi na L2 prvcích je velice omezená, a tedy v současné době je podvrhnutí DHCPv6 zprávy podstatně jednodušší než v sítích IPv4.

Zneužití skupinových adres

Uzly standardně musí naslouchat na několika skupinových (multicast) adresách. Na adrese pro všechny uzly v rámci rozhraní, linky a vyzývaného uzlu. Adresa vyzývaného uzlu je určena pro *Neighbor Solicitation* (NS) zprávy a spodních 6 bajtů je tvořeno z identifikátoru rozhraní. Pokud má uzel více adres na rozhraní, musí naslouchat na více skupinových adresách. Filtrovat příjem paketů ze skupinového vysílání je obecně problém, a díky velkému množství adres se ještě zesložiťuje. Uzly tak mohou být vytíženy vysíláním, které nepotřebují přijímat. Pokud se navíc některá standardní skupina omylem namapuje stejně jako skupina sloužící pro šíření video přenosu, dojde k dalšímu vytížení uzlu.

Přeplnění tabulky sousedů (Neigbour Cache)

Skutečnost, že typicky hostitelská část IPv6 adresy poskytuje 2^{64} možných kombinací, otevírá možnost vedení útoku za účelem zaplnění tabulky sousedů směrovače. V tomto případě prostřednictvím Neigbour Discovery protokolu vytvoříme směrovači iluzi velkého množství uzlů v síti, a tím dojde k přeplnění příslušných tabulek směrovače. Výsledkem mohou být komplikace na straně směrovače, anebo alespoň znemožnění vytváření záznamů pro nově připojená zařízení.

Fragmentace a obcházení bezpečnostních pravidel

Rozdělení přenášených dat na jednotlivé fragmenty komplikuje práci bezpečnostním zařízením. Touto problematikou jsme se zabývali v předchozím dílu .

IPv6 hlavičky, problémy se zřetězením a pořadím hlaviček

Protokol IPv6 zavádí zcela nový koncept rozšířených hlaviček umožňující přidávání nových vlastností do protokolu. Problematiku jsme rovněž probírali v předchozím dílu .

Tranzitní mechanizmy – obcházení bezpečnostních pravidel

Tranzitní, tunelovací mechanismy jsou legitimní techniky sloužící k přenosu IPv6 dat přes IPv4 síť. Použití těchto mechanizmů může vést k obcházení bezpečnostních politik, vytváření směrovacích smyček a DoS útokům. Podrobněji se touto problematikou budeme zabývat v samostatném dílu věnovaném přechodovým mechanizmům.

Vedení DoS a DDoS útoků

Možnosti vedení DoS a DDoS útoků jsou shodné s možnostmi, které nabízí IPv4. Teoreticky by měly být lépe dohledatelné zdroje takových útoků díky přehlednější hierarchii síti. Nadále však zůstává možnost podvrhávání zdrojové IPv6 adresy a případná kontrola správnosti zdrojové IPv6 adresy je, tak jak doposud, pouze záležitostí konfigurace hraničních směrovačů.

THC IPv6 toolkit

Jak vidíte, bezpečnostních problémů je v IPv6 více než dost. Řada problémů, ačkoliv již byla před dávnou dobou řešena v IPv4, se přesto v protokolu IPv6 objevuje znova. Poměrně nízká atraktivita protokolu IPv6 současně vede k tomu, že o tuto problematiku bezpečnosti IPv6 prakticky není zájem. Abychom závažnosti problému dali nějaký rozměr, ukážeme si, že provádět útoky není nijak složité. Jedna z mála skupin zabývajících se problematikou bezpečnosti IPv6 je *The Hacker's Choice* (THC). Z webu si můžete stáhnout sadu nástrojů pod názvem *IPv6 Attack Toolkit* umožňující provádění mnoha z výše popsaných útoků. Stačí stáhnout, přeložit a začít experimentovat.

Zcela záměrně zde nebudeme poskytovat praktické návody na likvidaci sítě. Snad jen jeden příklad za všechny pro demonstraci snadnosti provedení. Jedná se o již publikovaný typ útoku . Z balíku THC použijete jeden z příkazů:

```
flood_router6 eth0
```

Ten způsobí, že všechny systémy z produkce Microsoftu (a nejen tyto) se stanou zcela nepoužitelné. Zatížení CPU stoupne na 100% a se systémy se nedá pracovat. I po ukončení útoku systémy zůstanou ve stavu, kdy se s nimi nedá pracovat a nutně musí následovat reboot. Firewally ani jiné ochranné prostředky vám nepomůžou. Problémy způsobíte prakticky řádově desítkami až stovkami *Router Advertisment* zpráv za vteřinu. Pro představu: zdrojový soubor *flood_router6* má 119 řádků. Zkrátka ideální prostředek pro páteční odpoledne, pokud si ve firmě chcete zkrátit pracovní dobu a vašemu ajťákovi připravit skutečně zajímavý víkend. Vrátíme se zpět ke grafům z prvního dílu . Pro tento typ útoku absolutně nezáleží na tom, zda aktivně zavádíte IPv6 ve vaší síti. Stačí, že příslušné zařízení pouze podporuje IPv6, a je tímto typem útoku zranitelné.

SEND – všelék druhé generace

Pozornému čtenáři jistě neuniklo, že poměrně výrazná skupina problémů IPv6 je spojena se signalizací na úrovni lokální sítě. Tento mechanizmus je naprostým základem pro chod IPv6 sítě, nicméně je velice obtížné jej zabezpečit prostřednictvím firewallu či nějakými jinými metodami. Ve snaze o komplexní řešení

byl firmou Cisco vyvinut prostředek, který by měl řešit většinu problémů spojených právě se signalizací na úrovni lokálních sítí. Řešení bylo pojmenované *SEcure Network Discovery* (SEND), tedy česky bezpečné objevování sousedů. Rozšíření SEND je velice dobře popsáno jak v knize PAVLA SATRAPY IPv6 , tak v článku na lupě. Zde poukážeme na některé principiální problémy, které jsou s použitím SEND spojené:

- Vzhledem k tomu, že SEND využívá kryptografických metod pro zabezpečení, je s jeho aplikací spojená poměrně komplikována správa klíčů a certifikátů, a tedy i související infrastruktury veřejného klíče.
- Použitá IPv6 adresa je výsledkem kryptografické operace. SEND tedy není možno použít pro zabezpečení komunikace na obecných adresách, EUI 64 ad adresaách vytvořených podle Privacy Extensions.
- Zatím se příliš neřeší otázka možných útoků na SEND, ale i zde je poměrně velký prostor pro nové typy. I přes silné optimalizace, operace v SEND-u vyžadují jistý početní výkon. Pro představu můžete otestovat nástroj `sendpees6` z již dříve zmíněného balíku ipv6-thc generující velké množství zpráv, které musí SEND klient ověřovat.

SEND se v současné době dostává do stejné pozice, jakou kdysi zaujímal protokol IPSec. Sotva je poukázáno na nějaký bezpečnostní problém, je vše odbyto tvrzením, vždyť je tady přece SEND. Poměrně masivní podpora ze strany CISCO zanechává obecný dojem, že SEND je něco, co stačí začít jen používat. Skutečnost je ovšem taková, že v dnešní době jsou k dispozici pouze silně experimentální implementace klientů a velice malá podpora na straně směrovačů. Jisté je, že v existujících produktech Microsoftu SEND podporován nebude a maximálně je zvažována podpora pouze do některé z příštích verzí viz. článek na Microsoft TechNetu. O SEND-u lze uvažovat pouze jako o potenciálním prostředku pro sítě nové generace a zcela jistě bude potřeba ještě dlouhého času a nemalých praktických zkušeností, než jej bude možné použít v praxi. Zatím také není vůbec vyloučeno, že SEND skončí v propadlišti dějin.

Závěr

Protokol IPv6 v současné době nedisponuje jediným prakticky použitelným prvkem, který by výrazně zvyšoval úroveň zabezpečení sítí. Časté upínání se k technologii IPSec-u zanechává ve stínu mnohem závažnější bezpečnostní problémy protokolu IPv6. Tato skutečnost je do značné míry způsobena faktem, že bezpečnostní problémy IPv6 byly zatím řešeny velice okrajově. Většina bezpečnostních rizik známa z protokolu IPv4 je současně i v IPv6, navíc doplněna o zcela nové možnosti. Díky stavu implementace IPv6 v jednotlivých systémech nepředstavuje hledaní bezpečnostních hrozeb IPv6 žádné výrazné intelektuální úsilí, a řada útoků je proveditelná skutečně triviálními prostředky.

Tento nepříjemný stav je dán zejména dosavadním obecným nezájmem o protokol IPv6. Jeho postupná penetrace a nasazování v sítích si bezpochyby velice rychle vynutí urychlené řešení těchto problémů. Ačkoliv to zní paradoxně, tím největším pomocníkem v tomto směru může být protokol IPv4. Díky velké podobnosti obou protokolů může být řada mechanizmů odhalených pro IPv4 převzata do IPv6. Současně však ale bude nutno na tomto poli věnovat nemálo výzkumné a implementační práce, aby protokol IPv6 v rovině zabezpečení dosahoval alespoň parametrů současného IPv4.

Tomáš Podermański

Autor pracuje jako správce metropolitní sítě VUT v Brně. Podílí se na řešení projektů zaměřenýchna bezpečnost a monitoring sítí. Je aktivním členem evropského projektu GÉAN3 v aktivitě Campus Best Practice.

Matěj Grégr

Studuje na Fakultě informačních technologií VUT v Brně. Snaží se porozumět počítačovým sítím a teoretické znalosti pak

(ne)úspěšně uplatňovat v praxi jako správce kolejní sítě VUT.

Seriál Pohněme s IPv6

- IPv6 Mýty a skutečnost, díl V. - Zjednodušené hlavičky
- IPv6 Mýty a skutečnost, díl VI. - Bezpečnostní mechanizmy
- IPv6 Mýty a skutečnost, díl VII. - Podpora Multicast a anycast provozu
- IPv6 Mýty a skutečnost, díl VIII. - Přechodové mechanizmy
- IPv6 Mýty a skutečnost, díl IX. - Quo Vadis, IPv6?

Všechny díly seriálu