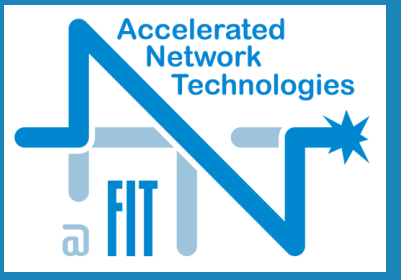
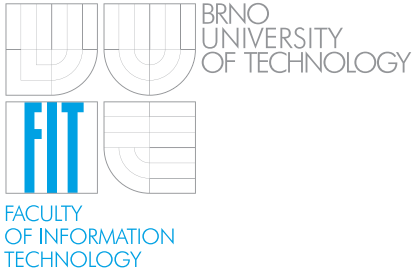
Inter-Domain Routing and Addressing



Jiří Novotňák

Brno University of Technology, Faculty of Information Technology
Božetěchova 2, 612 00 Brno, CZ
www.fit.vutbr.cz/~inovotnak



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Obsah

Tři články

- Internet Inter-Domain Traffic
- How Secure are Secure Interdomain Routing Protocols
- Understanding Block-level Address Usage in the Visible Internet

Internet Inter-Domain Traffic

Data o provozu mezi doménami

- Provoz mezi doménami (AS)
- Vývoj objemu a typu provozu
- Změna struktury Internetu

Cíle

- Sledování dlouhodobého vývoje internetového provozu
- Odhad růstu Internetu
- Analýza změn v požadavcích Internetového provozu

Způsob měření

- 110 Providerů
- 3000 hraničních routerů 100 000 rozhranní
- Komunikace mezi AS
- Chybějící informace o vnitřní struktuře AS
- Založeno na NetFlow JFlow atd.

Rozložení providerů v měření

Segment	zastoupení(%)
Regionální / T2	34
Globální /T1	16
Neklasifikované	16
Koncové (DSL, ...)	11
Hosting	11
Výzkum / vzdělávání	9
CDN	3

Poměr regionů v měření

Region	zastoupení(%)
Severní Amerika	48
Evropa	18
Neklasifikované	15
Asie	9
Jižní Amerika	8
Střední východ	1
Afrika	1

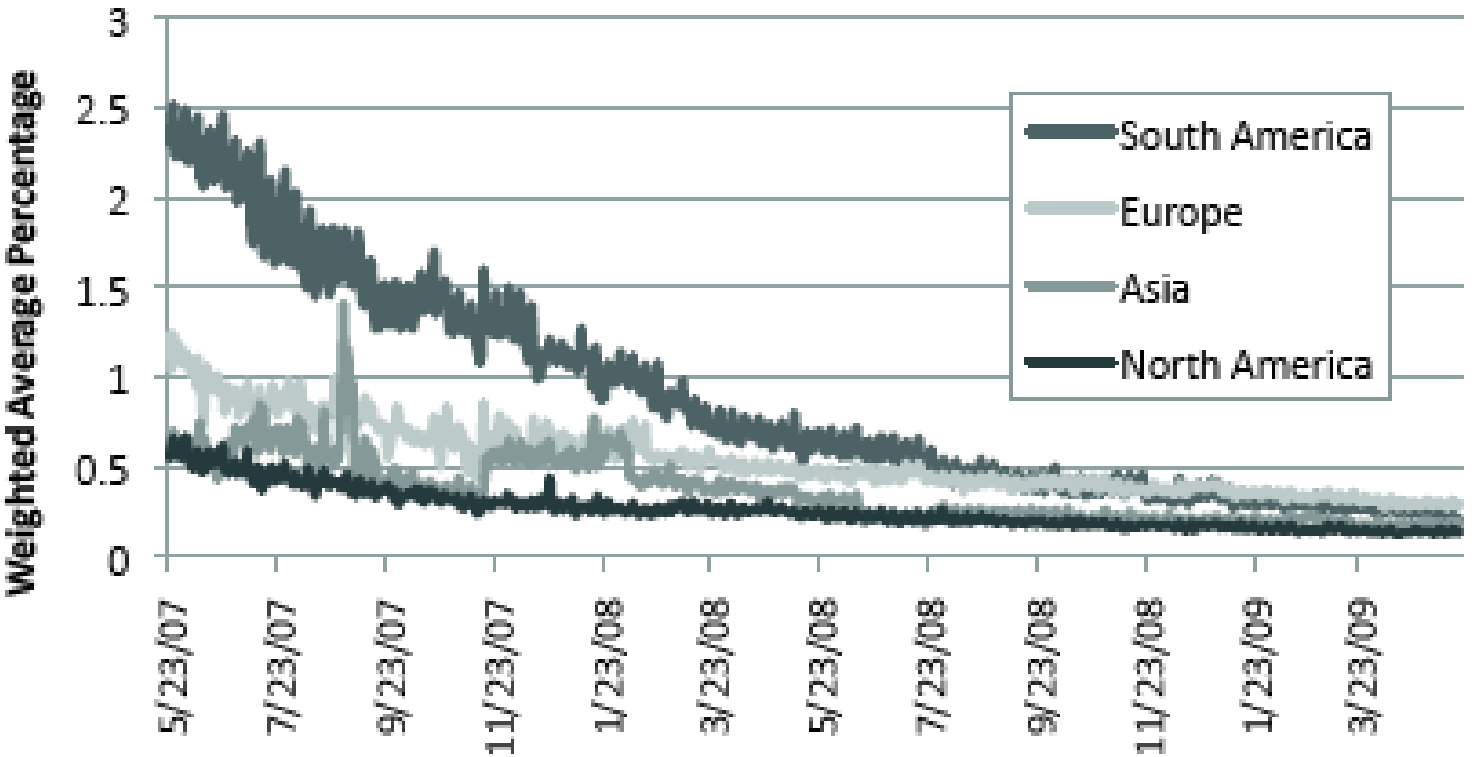
Poměr zastoupení jednotlivých služeb dle TCP/UDP portů

Pořadí	Služba	2007	2009	Změna
1	Web	41.68	52.00	+10.31
2	Video	1.58	2.64	+1.05
3	VPN	1.04	1.41	+0.38
4	Email	1.41	1.38	-0.03
5	News	1.75	0.97	-0.78
6	P2P	2.96	0.85	-2.11
7	Games	0.38	0.49	+0.12
8	SSH	0.19	0.28	-0.08
9	DNS	0.20	0.17	-0.04
10	FTP	0.21	0.14	-0.07
	jiné	2.56	2.67	+0.11
	nerozpoznané	46.03	37.00	-9.03

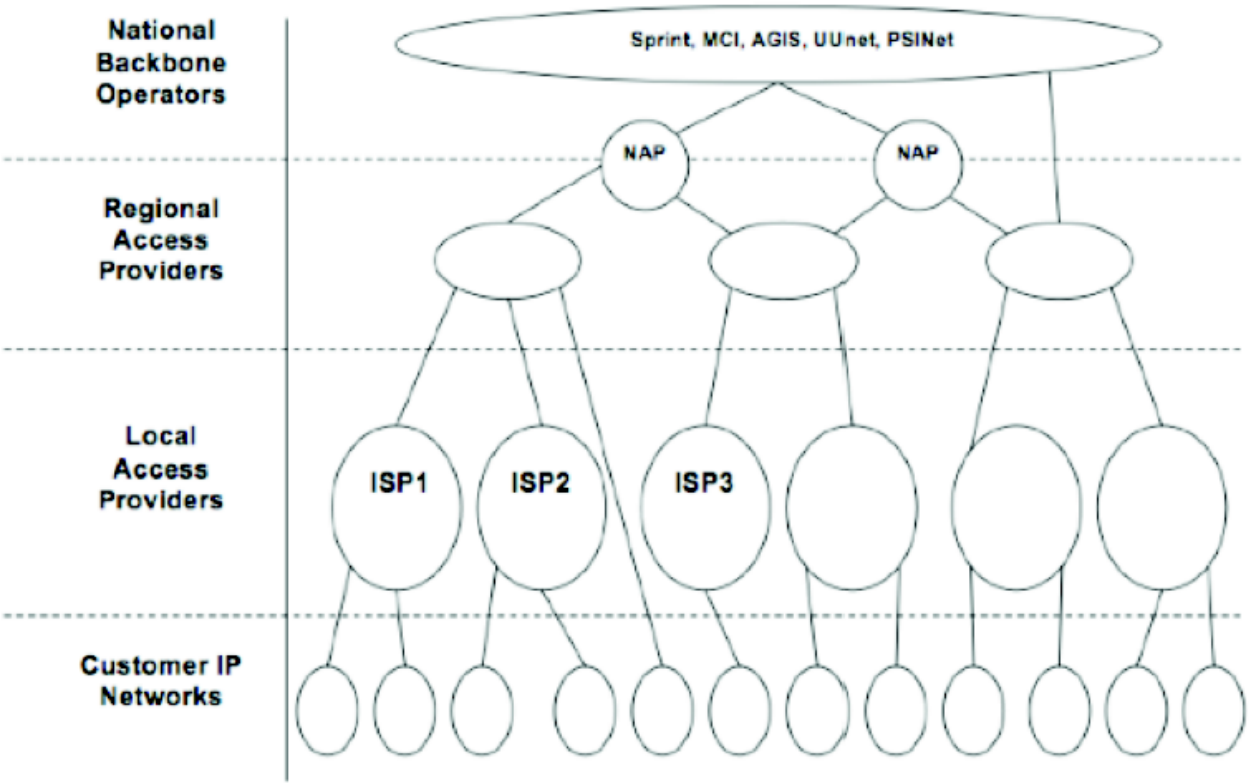
Poměr zastoupení jednotlivých služeb dle obsahu

Služba	Procento
Web	52.12
Video	0.98
Email	1.54
VPN	0.24
News	0.07
P2P	18.32
Games	0.52
SSH	N/A
DNS	N/A
FTP	0.16
jiné	20.54
nerozpoznané	5.51

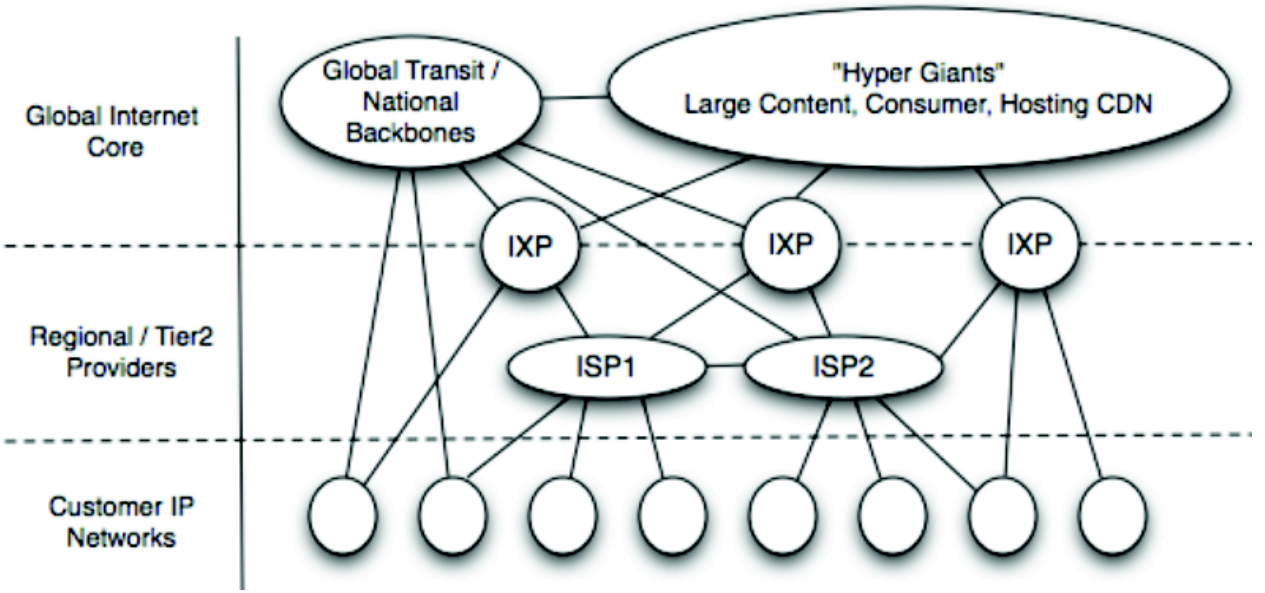
Pokles zastoupení p2p komunikace



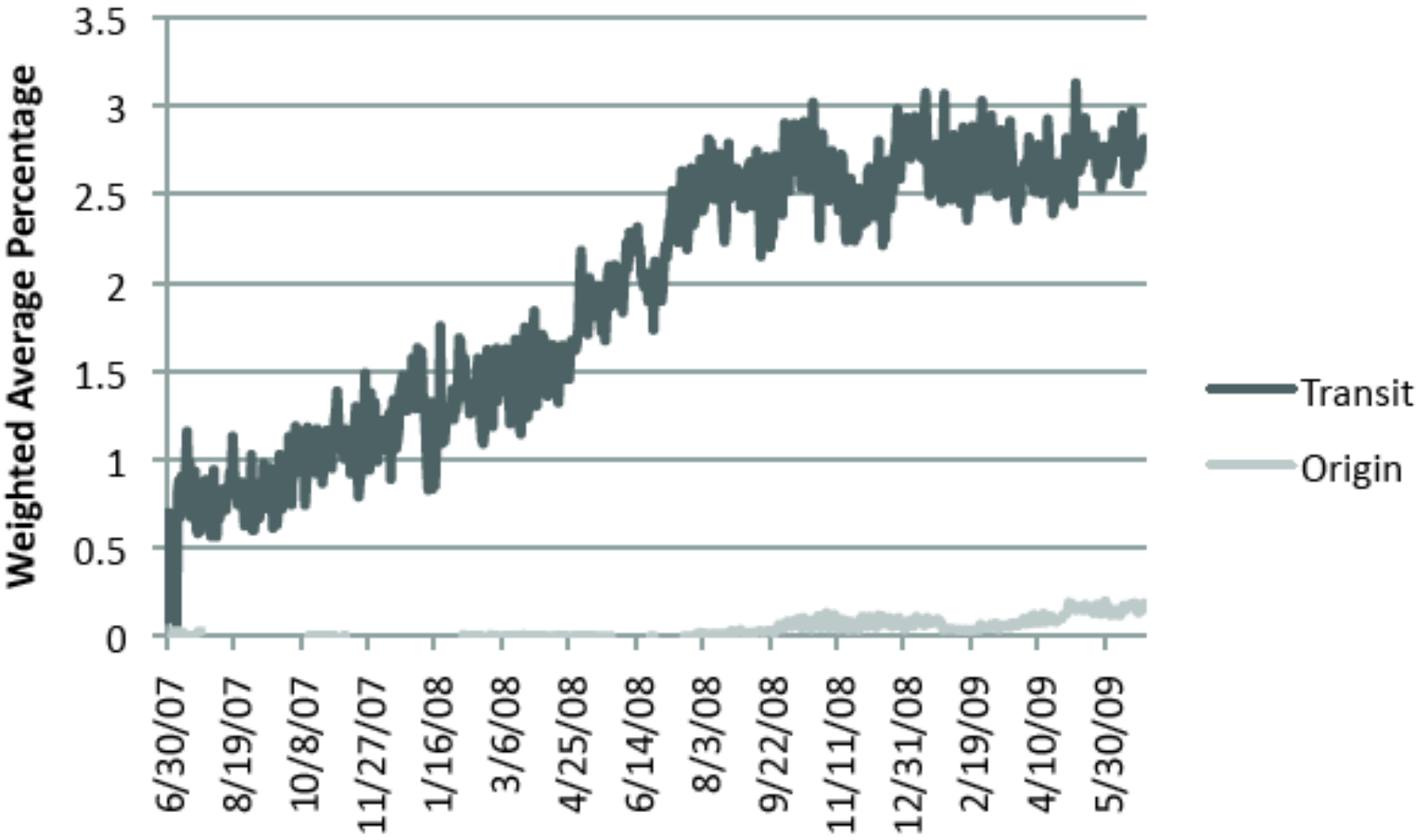
Tradiční model Internetu



Dnešní model Internetu



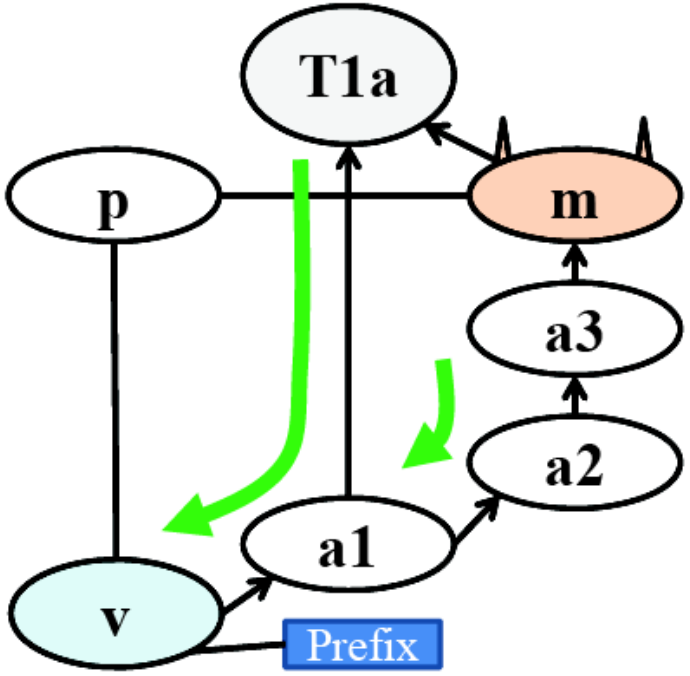
Nárůst objemu tranzitních dat

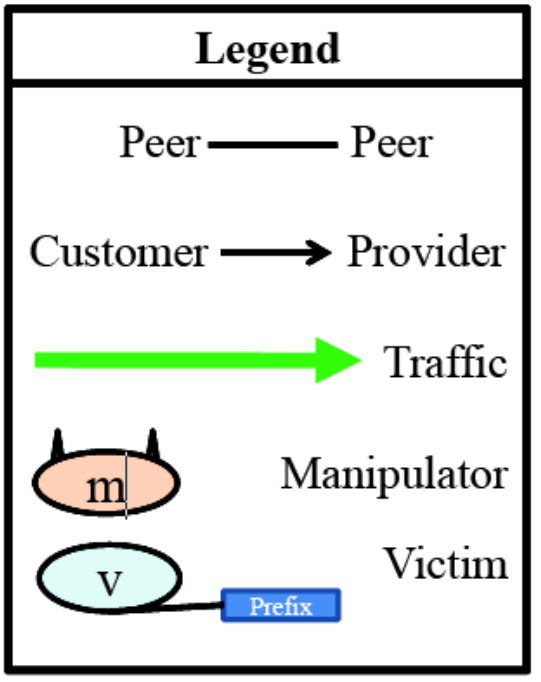


Cíl článku

- Seznámení s možnými útoky na routovací protokoly
- Rozbor hrozeb takových útoků
- Odolnost jednotlivých zabezpečovacích mechanismů

Útok na BGP


T1a
p
m
a3
a2
a1
v
Prefix


Legend
Peer
Peer
Customer
Provider
Traffic
m
Manipulator
v
Victim
Prefix

Podstata útoku

- Útočník napadne routery providera
- Útočník se pokusí přesvědčit ostatní providery, že jedině přes něj vedou ty jediné, správné a rychlé cesty
- Při úspěšném přesměrování provozu se snaží nějakým způsobem naložit s datovými přenosy konkrétní oběti

Metody zabezpečení protokolu BGP

Origin Authentication

- Hraniční router má důvěryhodnou databázi AS společně s prefixy jejich zákazníků
- Lze obejít nabídnutím alternativní cesty (i neexistující), která ale skutečně vede k cíli

Secure Origin BGP (soBGP)

- Databáze hraničního routeru je rozšířena fyzické cesty
- Hraniční router je schopen ověřit, že nabízená cesta skutečně existuje
- Lze obejít nabídnutím cesty, která skutečně existuje, ale není aktuálně dostupná (legitimní router ji nemůže nabídnout)

S-BGP

- Nabídka cesty musí být digitálně podepsána
- Router je schopen nabídnout cestu pouze pokud s cílem sousedí, jinak je třeba podpisů dalších routerů na cestě.
- Útočník musí nabídnout cestu, která skutečně existuje a je ověřitelná, může se však snažit, aby se cesta zdála výhodná

Metody zabezpečení protokolu BGP

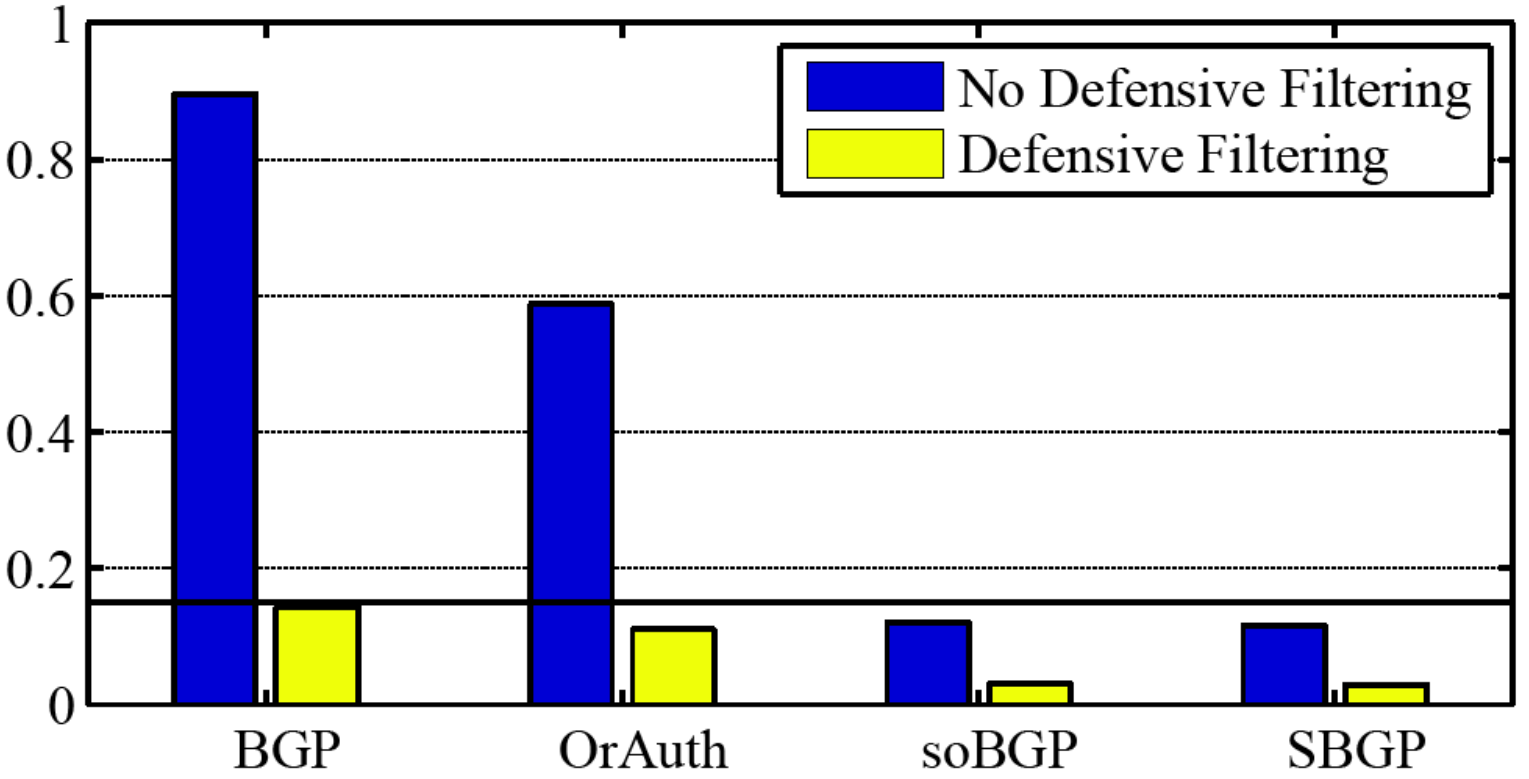
Data-plane verification

- Hraniční router si ověřuje, zda router, který nabízí cestu sám nepřeposílá opačně směrovaná data jinudy.
- Útočník musí přesvědčit hraniční routery na obou stranách a sám tuto cestu využívat

Defensive Filtering

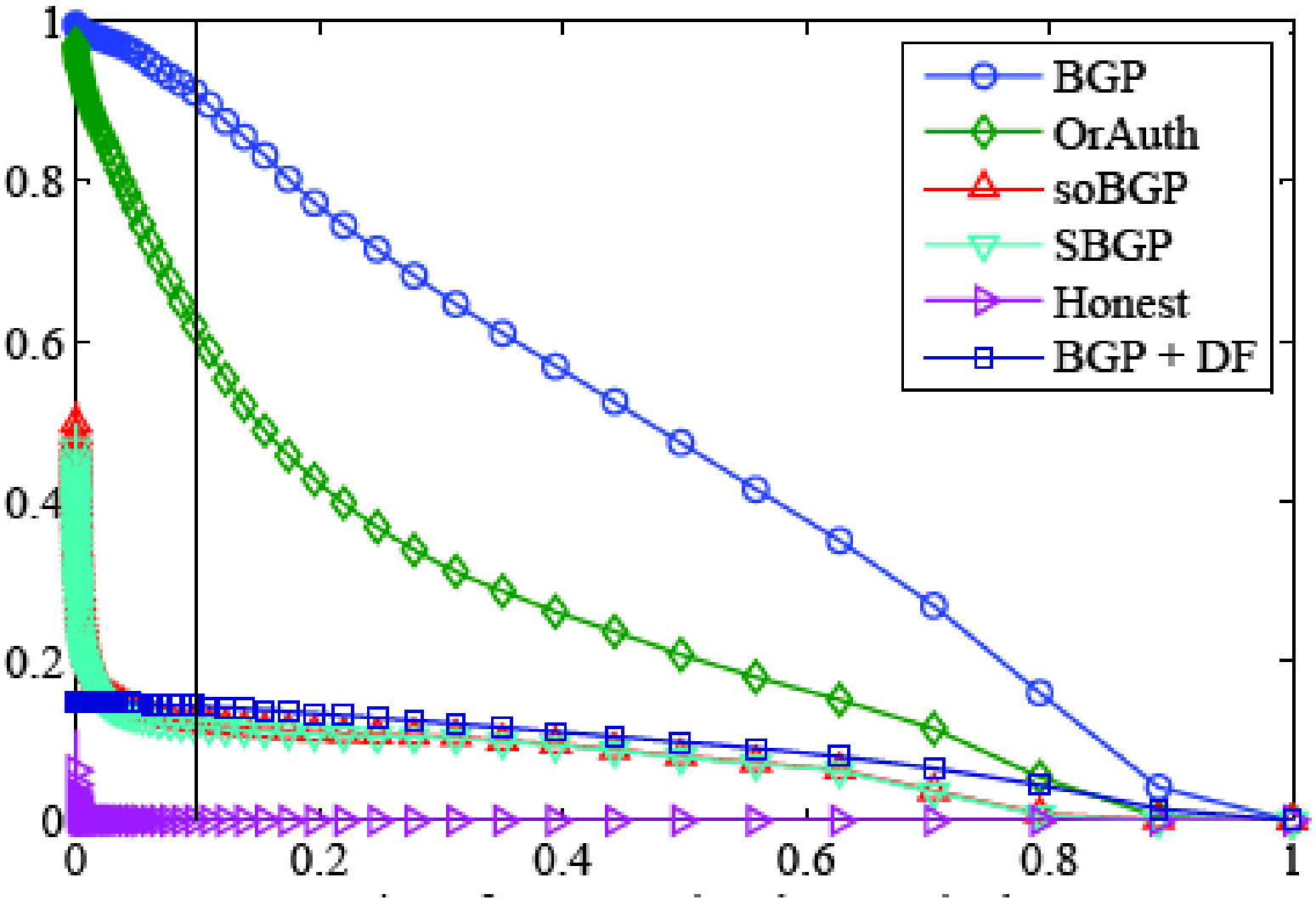
- Hraniční router má informaci, jaké prefixy patří zákazníkům daného AS
- Útočník nemůže nabídnout cestu k prefixu, který nevlastní
- Tato metoda zaměřena zejména na providery, kteří nemají vlastní koncové zákazníky
- Metoda je obecně velmi účinná a je schopna pokrýt i zabezpočovací schopnost oBGP, soBGP a S-BGP

Defensive Filtering



Obrázek: Schopnost útočníka oklamat alespoň 10% AS

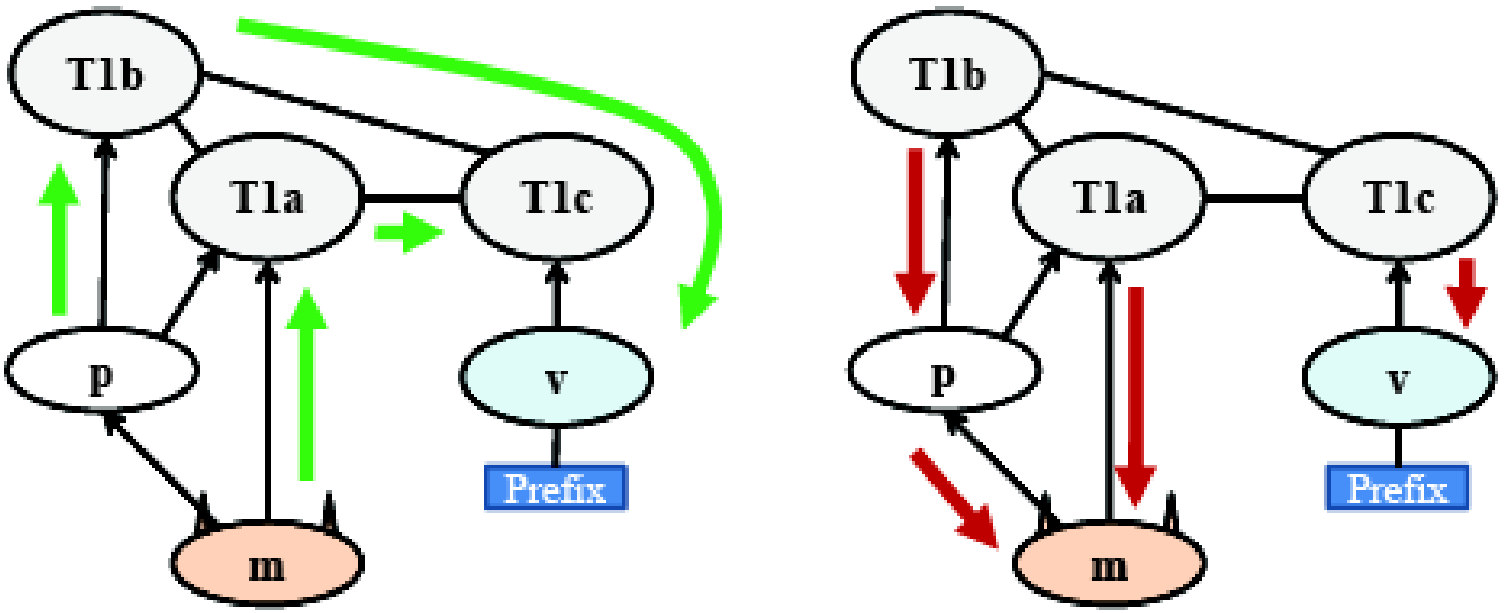
Srovnání zranitelnosti



Obrázek: Poměrná část AS směrujících přes útočníka

Problém vzniku černé díry

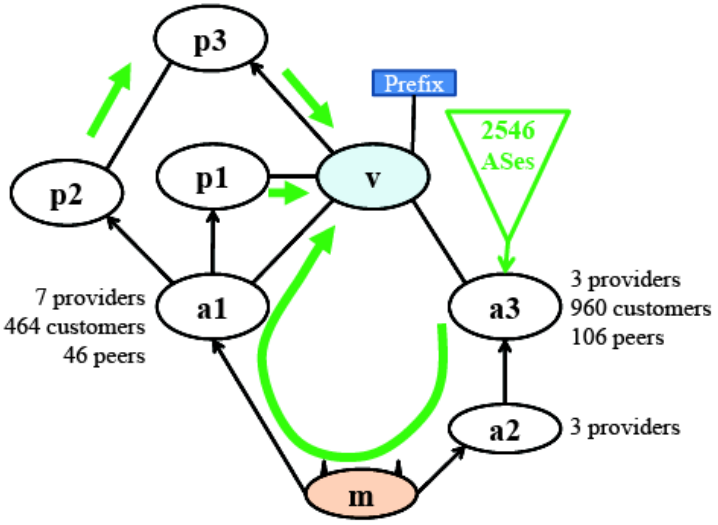
Pokud si útočník neověří, zda po změně směrování bude mít volnou cestu k oběti, začne pohlcovat veškerý provoz k oběti a vytvoří tak "černou díru".

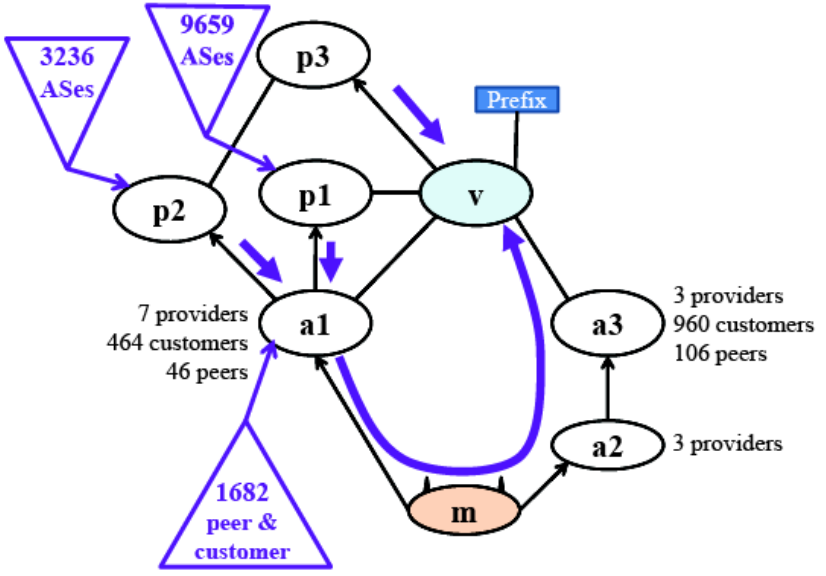


Obrázek: Vytvoření černé díry po přesměrování provozu

Neefektivita nejkratší cesty

- Vnutit okolním routerům nejkratší cestu nemusí být optimální
- Pro optimální strategii je třeba dobře znát topologii sítě
- Jedná se o NP-těžký problém





Cíl článku je analyzovat

- Využití adresního prostoru
- Stabilitu jednotlivých adresních blocků
- Detekovat jak velké bloky jsou přidělovány

Metodika detekce bloků

- Testovány jsou bloky /24 a menší
- Vždy je vybrána náhodná část bloku, není testován celý blok
- Po otestování bloku je spuštěna detekce podbloků

Metodika detekce bloků

- Testovány jsou bloky /24 a menší
- Vždy je vybrána náhodná část bloku, není testován celý blok
- Test je proveden pomocí ICMP a následně analyzována dostupnost, RTT atd.
- Po otestování bloku je spuštěna detekce podbloků
- Testováno 24 000 bloků /24

Prefix	vždy stabilní	občas stabilní	přerušované	zřídka využité
/24	1,603 (18 %)	2,517 (29 %)	2,673 (30 %)	1,994 (23 %)
/25	323 (23 %)	523 (38 %)	295 (21 %)	237 (17 %)
/26	346 (21 %)	617 (38 %)	378 (23 %)	274 (17 %)
/27	432 (20 %)	855 (40 %)	506 (23 %)	361 (16 %)
/28	759 (20 %)	1,301 (34 %)	993 (46 %)	734 (19 %)
/29	2,077 (21 %)	3,190 (32 %)	2,355 (24 %)	2,227 (23 %)
/30	3,312 (19 %)	5,656 (33 %)	4,679 (27 %)	3,707 (21 %)
/31	4,195 (16 %)	9,867 (37 %)	7,864 (30 %)	4,566 (17 %)
/32	52,646 (3 0 %)	42,847 (24 %)	43,266 (25 %)	36,707 (21 %)

Nestabilně přidělené zřídka využité adresy

- Jedná se o dynamicky přidělované bloky.
- Největší zastoupení v Číně (80 %) takových bloků
- Ukazuje na nedostatek volných adres a snahu přidělit adresu právě aktivnímu zařízení
- Největší množství "řídce" využívaných blocků bývá zároveň s pomalým připojením

Reference

- Craig Labovitz, Scott Iekel-Johnson, Danny McPherson, Jon Oberheide, Farnam Jahanian: Internet Inter-Domain Traffic. SIGCOMM. 2010
- Sharon Goldberg, Michael Schapira, Peter Hummon, Jennifer Rexford: How Secure are Secure Interdomain Routing Protocols?. SIGCOMM. 2010
- Xue Cai, John Heidemann: Understanding Block-level Address Usage in the Visible Internet. SIGCOMM. 2010

Děkuji za pozornost.