Bezpečnost síťových technologií – Remotely-Triggered Black Hole

Ing. Josef Kaderka, Ph.D.

Remotely-Triggered Black Hole

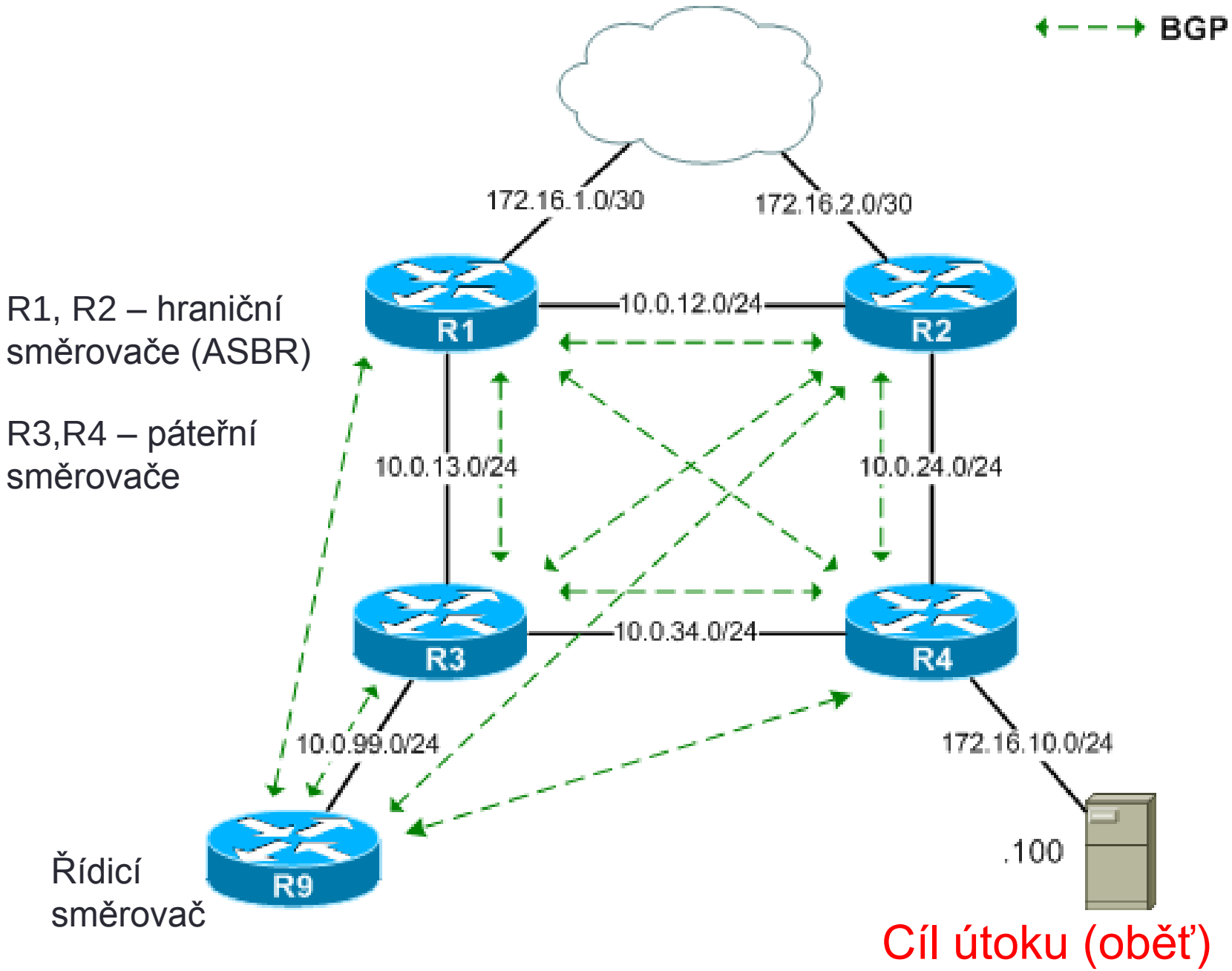
- Obranný mechanismus zmírňující následky útoků typu DDoS
  - Masivní útok proti jednomu nebo několika konkrétním serverům
  - Tyto servery v první fázi obrany obětujeme, abychom uchránili infrastrukturu
  - RFC 5635 – Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)

Remotely-Triggered Black Hole

- Aplikace směrovacího protokolu BGP4
  - Primárně externí protokol, tj. určen pro směrování mezi autonomními systémy, avšak lze jej provozovat i jako interní
  - Princip činnosti: „Path Vector“ – varianta vektoru vzdálenosti
  - Používá protokol TCP (port 179)
  - Manuální konfigurace všech vztahů sousedství („peers“, směrovač sám je označován jako „BGP speaker“)

Základní myšlenka

- Předem počítáme se obětováním cíle útoku
  - Zachráníme zbytek sítě, zejména infrastrukturu
- Předběžná příprava obrany - východiska
  - Konfigurace směrovačů
  - Prostřednictvím protokolu BGP4 lze distribuovat statické cesty včetně uvedení parametru `tag`
- Aktivace obrany v případě útoku
  - Zjištěna IP adresa oběti útoku
  - Je manuálně vytvořen statický směrovací záznam (cesta), odvádějící provoz místo k cíli do prázdného zařízení (`Null0`)
  - Tato cesta je prostřednictvím protokolu BGP4 okamžitě distribuována (injektována) všem [hraničním] směrovačům



http://packetlife.net/blog/2009/jul/6/remotely-triggered-black-hole-rtbh-routing/

Krok 1 - budování obrany

- Příprava černé díry (Null route)
  - Je vhodné provést před útokem
- Vytvořením statické cesty ve všech hraničních směrovačích (zde R1, R2)
  - `R1(config)# ip route 192.0.2.1 255.255.255.255 Null0`
  - Data zasílaná na adresu 192.0.2.1/32 budou předávána do zařízení `Null0`, tj. ihned zahazována
  - Konkrétní adresa není důležitá, viz dále (zde zvolen rozsah určený pro Test-Net, viz RFC 3330)

Krok 2a – budování obrany

- Vytvoření mapy cest (Route-map) na R9 pro redistribuci označkované statické cesty s modifikovanou hodnotou adresy dalšího skoku.
  - `R9(config)# route-map RTBH`

    Jméno mapy
  - `R9(config-route-map)# match tag 666`

    pokud je přišedší prefix doplněn tagem 666
  - `R9(config-route-map)# set ip next-hop 192.0.2.1`

    nastav pro něj další skok na uvedenou IP adresu
  - `R9(config-route-map)# set origin igp`

    informace o něm pochází z interního směrovacího protokolu
  - `R9(config-route-map)# set community no-export`

    nikdy nešiř tuto informaci do jiných AS (tj. šiř jen v rámci IBGP)

Krok 2b – budování obrany

- Předchozí mapa cesty představuje klíčový faktor RTBH
  - každá cesta propagovaná na hraniční směrovač s dalším skokem `192.0.2.1` bude rekursivně přesměrována na dříve vytvořenou statickou cestu vedoucí na `Null0`
  - příslušný provoz bude tudíž zahozen.

Krok 2c – budování obrany

- Povolení redistribuce statické cesty do protokolu BGP4 s využitím mapy cesty
  - `R9(config)# router bgp 65100`
  - `R9(config-router)# redistribute static route-map RTBH`

Krok 3 – nastal útok – obrana!

- Jako cíl útoku / oběť identifikována IP adresa 172.16.10.100

- Vytvoření cesty k oběti na řídicím směrovači
  - `R9(config)# ip route 172.16.10.100 255.255.255.255 Null0 tag 666`
- Tuto cestu nelze kvůli formálně nekorektní adrese dalšího skoku `Null0` přímo propagovat do hraničních směrovačů. Proto byla přidána značka (tag) `666`, aby se zajistilo, že mapa cesty bude tuto cestu redistribuovat s modifikovanou adresou dalšího skoku.

Ověření funkce

- Hraniční routery zahazují provoz směřující k oběti

```
R1# show ip route 172.16.10.100
Routing entry for 172.16.10.100/32
  Known via "bgp 65100", distance 200, metric 0, type internal
  Last update from 192.0.2.1 00:06:14 ago
  Routing Descriptor Blocks:
  * 192.0.2.1, from 10.0.99.9, 00:06:14 ago
  Route metric is 0, traffic share count is 1
  AS Hops 0

R1# show ip route 192.0.2.1
Routing entry for 192.0.2.1/32
  Known via "static", distance 1, metric 0 (connected)
  Routing Descriptor Blocks:
  * directly connected, via Null0
  Route metric is 0, traffic share count is 1
```

Závěr

- Oběť je nyní bohužel nedostupná
  - Lze jí přidělit jinou IP adresu a tuto zavést do DNS
    - Doba platnosti starého údaje v DNS může být značná
    - Útočník může změnu odhalit a zaútočit znovu na novou adresu
- Infrastruktura je ochráněna proti přetížení.

Děkuji za pozornost