Útok na DNS pomocí IP fragmentů

Původní článek Amira Herzberga & Hayi Shulmanové

Tomáš Hlaváček • tomas.hlavacek@nic.cz •
IT13.2, 30.11.2013

Fragmentační útok na IP protokol

- Článek Amir Herzberg & Haya Shulman: Fragmentation Considered Poisonous
- Existují dva PoC:
  - Tomáš Hlaváček & Ondřej Mikle, CZ.NIC Labs
  - Brian Dickson, VeriSign Labs
- Relativně nízká technická složitost, ale hodně podmínek a detailů

Nový vektor útoku: Fragmenty

- Útok na UDP
- Zneužití IP fragmentace & skládání fragmentů
- Změna a nebo zahození packetů bez přístupu k přenosovému kanálu
- Záleží na 16-bit IP ID čísle v IP hlavičkách
- IP ID je generované čítačem
- Problém jsou limity IP reassembly cache

Útok přes IP fragmentaci na DNS

- Otrávení cache (cache poisoning)
- Redukce entropie z 32 bitů (source port + DNS ID) na 16 bitů (jen IP ID)
- … funguje to, protože UDP hlavička a začátek DNS dat zůstane v prvním fragmentu
- Útočník modifikuje druhý fragment (authority a additional sekce)

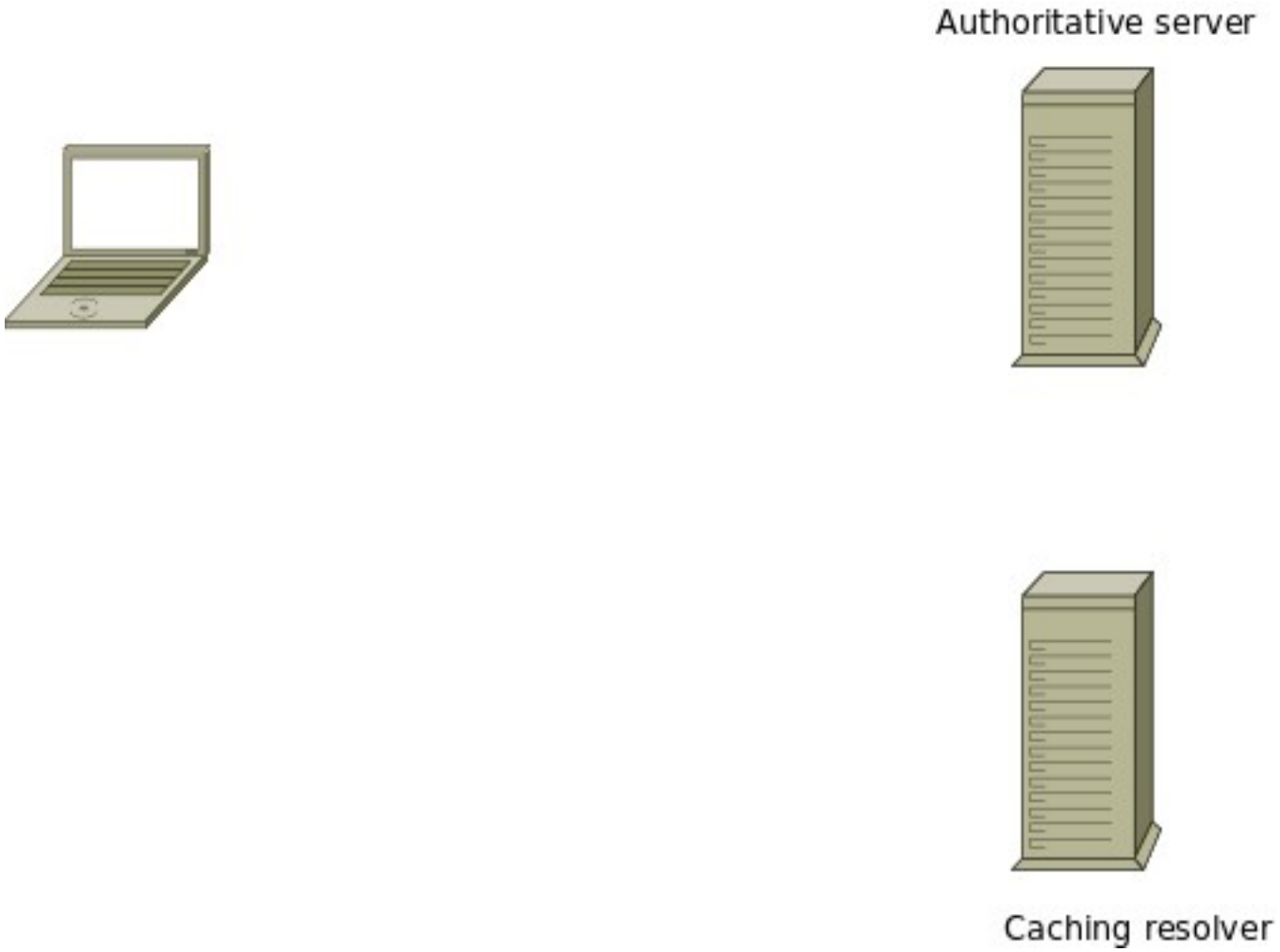
Typy fragmentačních útoků na DNS

- Zatím jsou známé dva typy:
  - 1) Donucení autoritativního serveru, aby fragmentoval odpovědi pro reálnou doménu pomocí podvržených ICMP packetů
  - 2) Registrováním speciálně zformátované zóny, která generuje odpovědi přes 1500 B

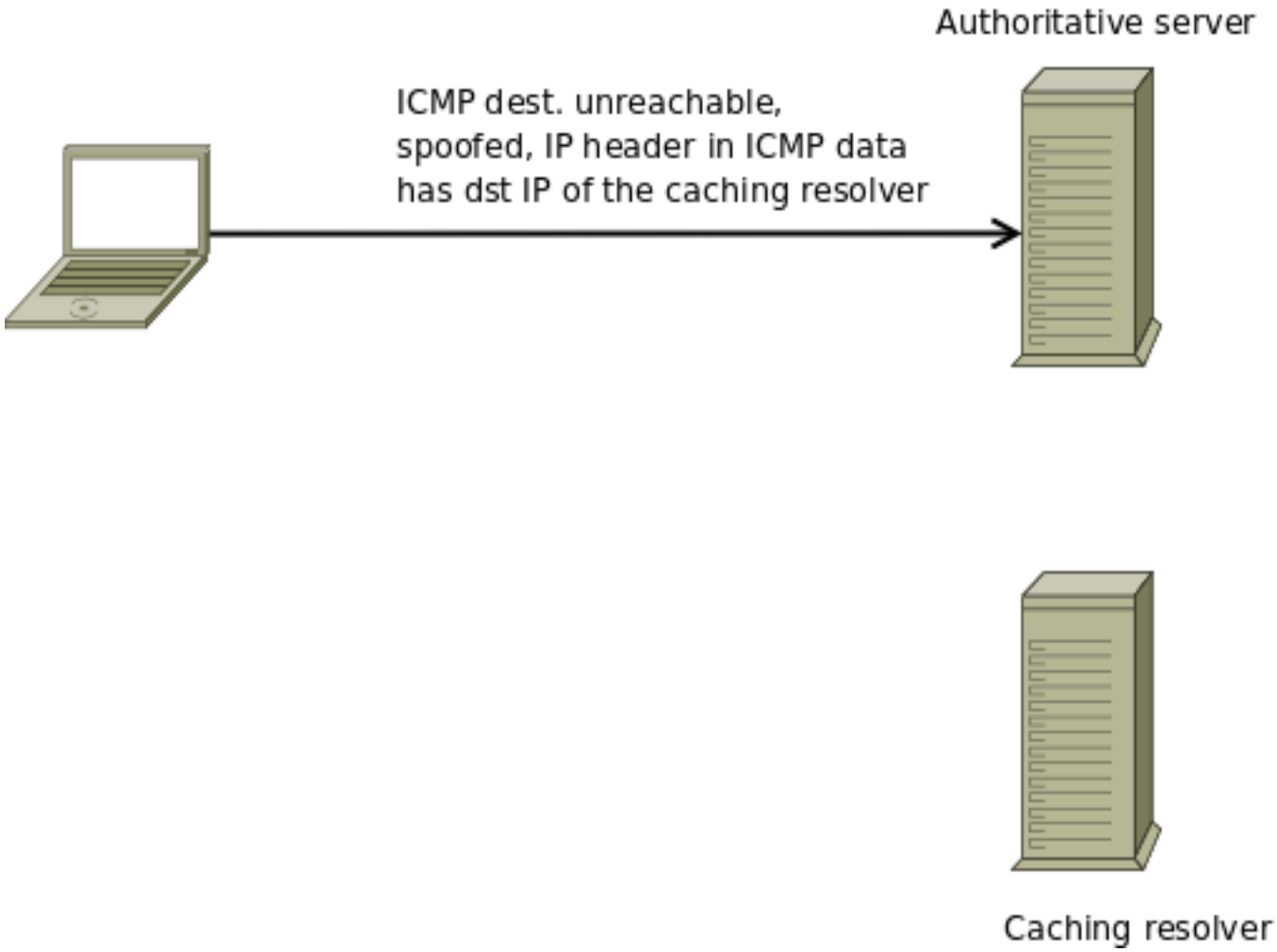
První typ – přinucení k fragmentaci

- ICMP destination unreachable, frag. needed but DF bit set (type=3, code=4)
- Podvržení ICMP (BCP38 není problém, firewally mohou být problém)
- Linux akceptuje signalizované MTU do routing cache na 10 minut
- Linux má minimální MTU = 552 B

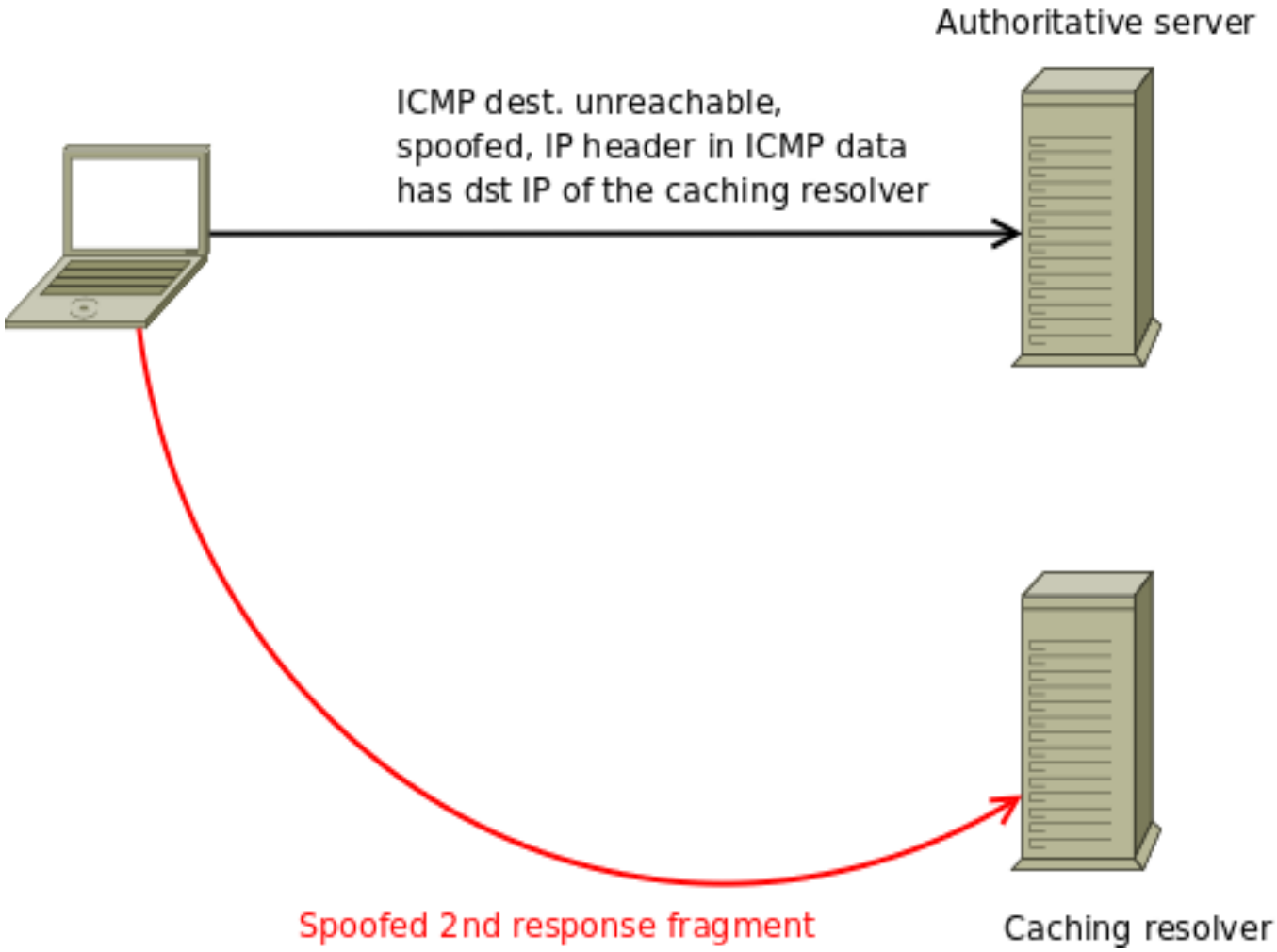
Znázornění prvního typu útoku



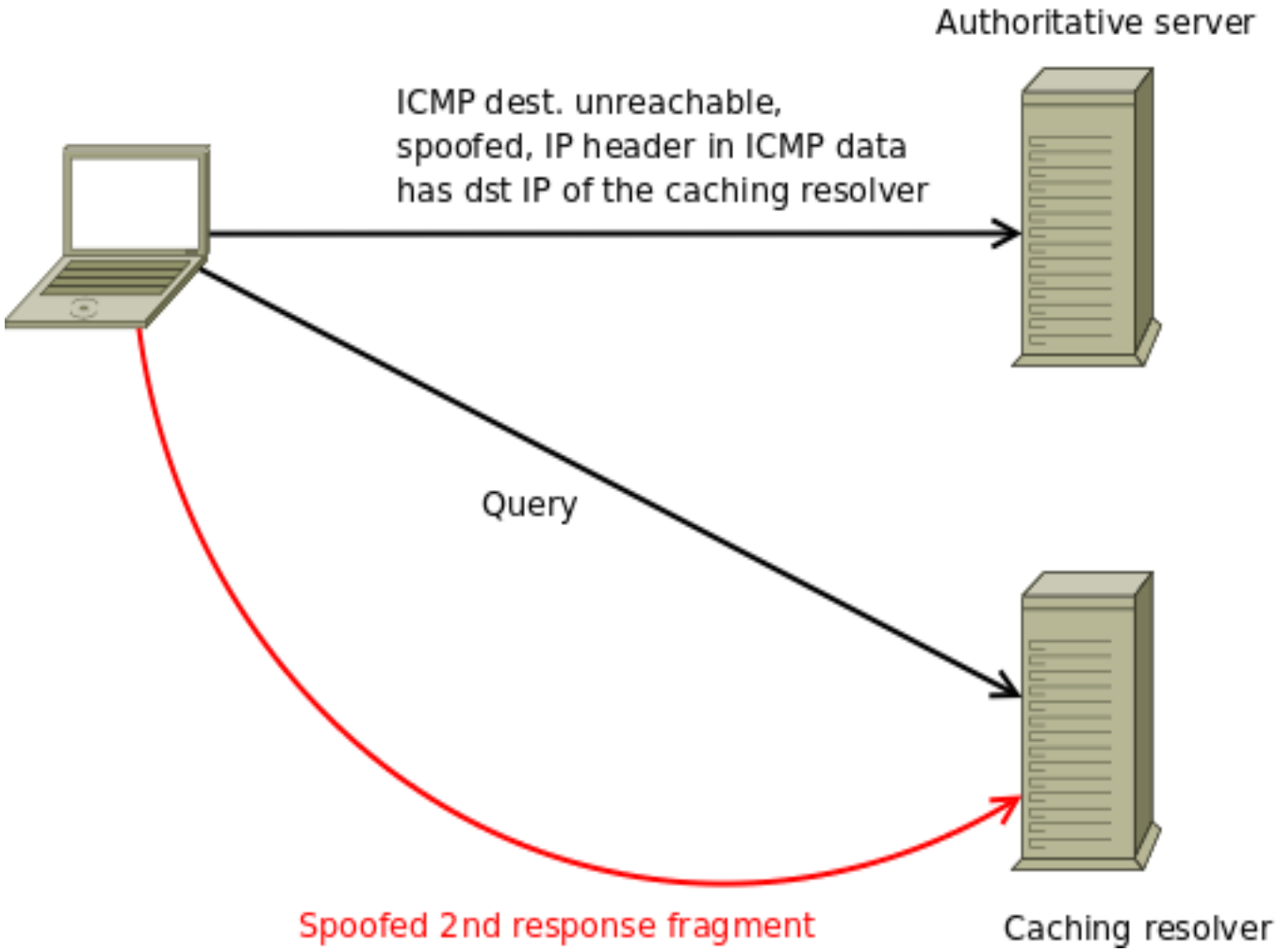
Znázornění prvního typu útoku



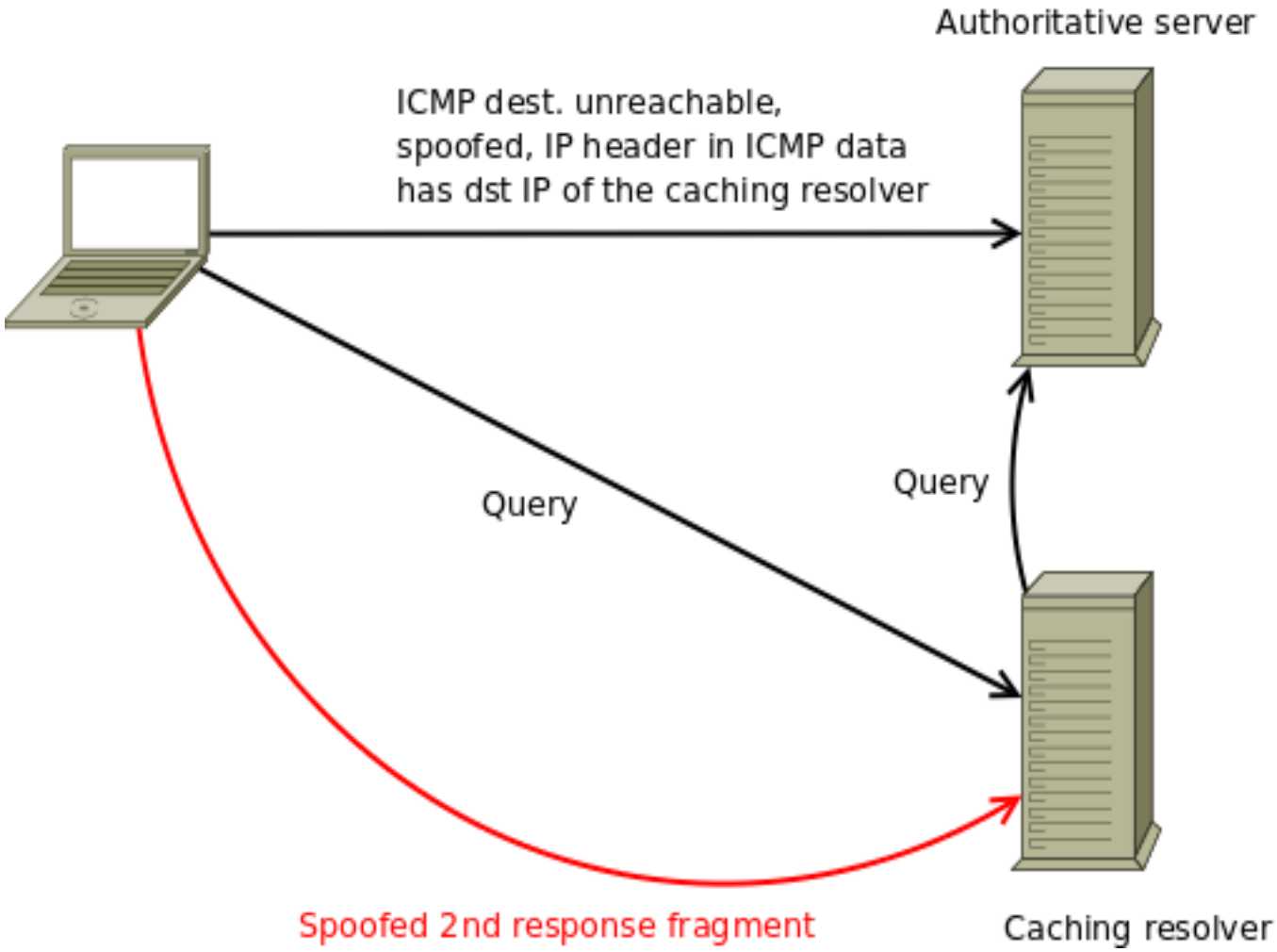
Znázornění prvního typu útoku



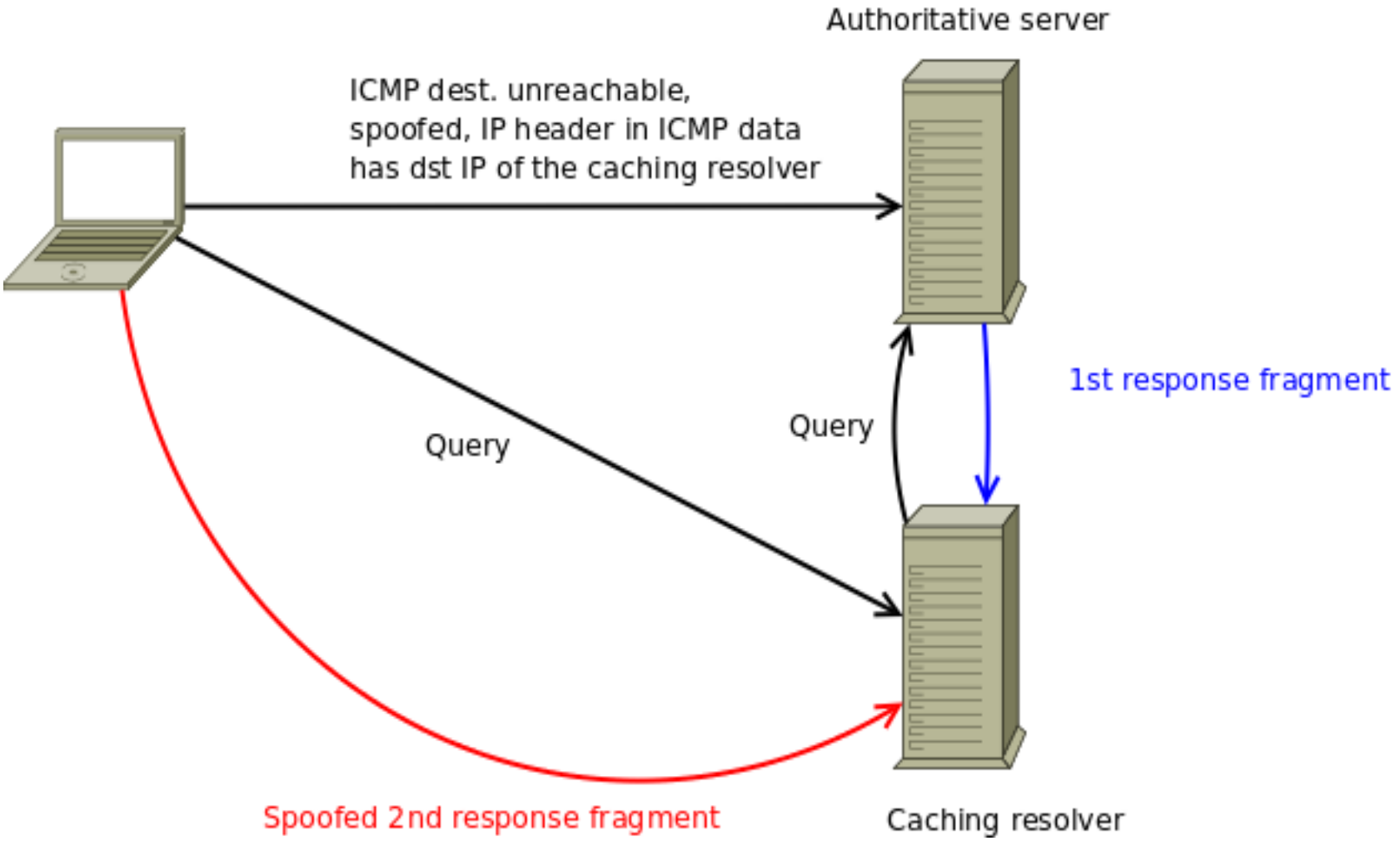
Znázornění prvního typu útoku



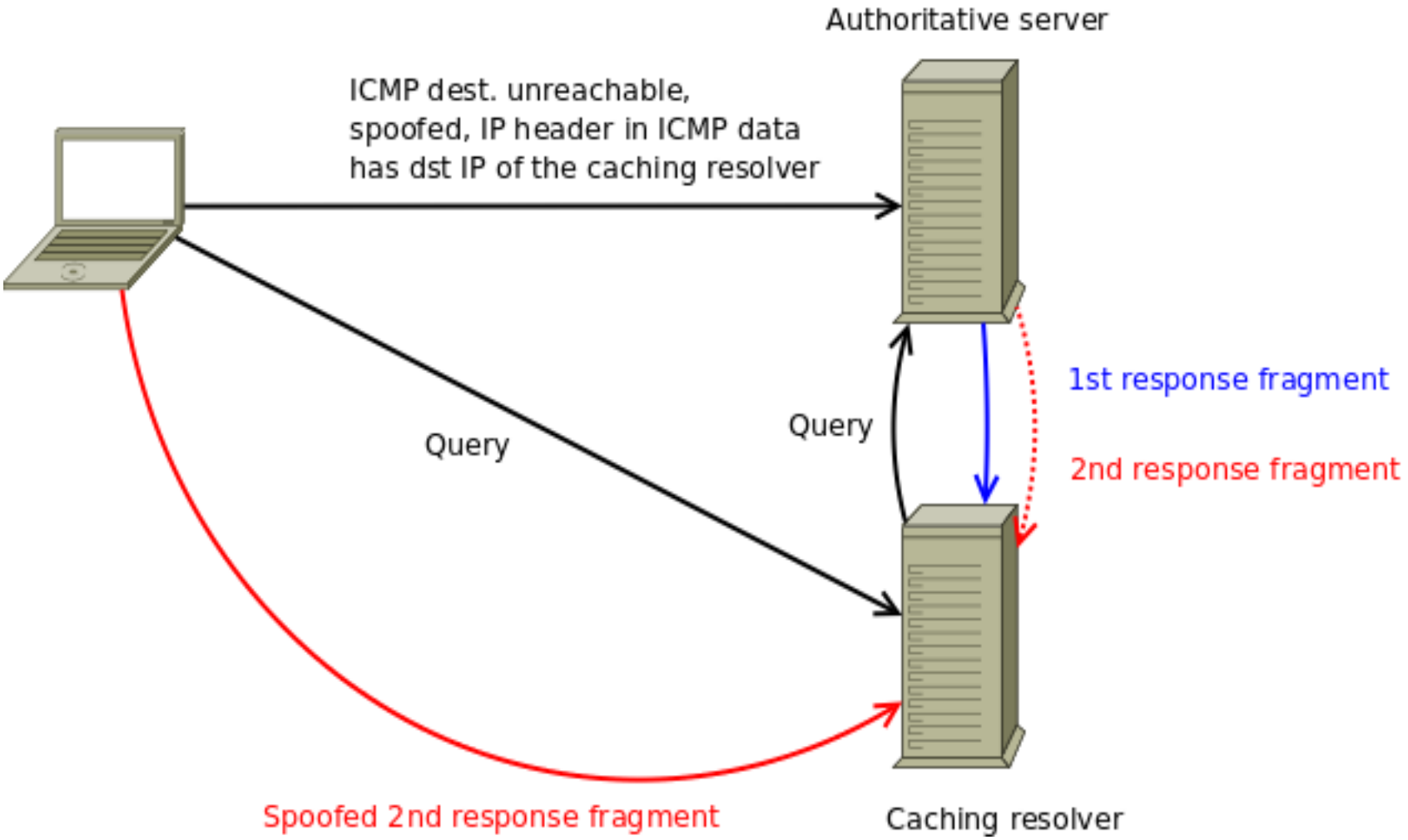
Znázornění prvního typu útoku



Znázornění prvního typu útoku



Znázornění prvního typu útoku



Effekt podvrženého ICMP packetu

root@authoritative_server:/# ip route show cache

...

77.243.16.81 from 195.226.217.5 via 217.31.48.17 dev eth0

cache ipid 0xe8a1

62.109.128.22 from 195.226.217.5 via 217.31.48.17 dev eth0

cache expires 576sec **ipid 0x6ef3 mtu 552** rtt 4ms rttvar 4ms cwnd 10

63.249.32.21 from 195.226.217.5 via 217.31.48.17 dev eth0

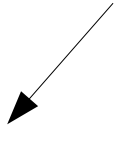
cache ipid 0xa256

Odpověď autoritativního serveru

```
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.aaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaa.aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.aaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.aaaaaaaaaaaaaaaaaaaaaaa.aaaaaaaaaaaa
aa.ad.example.cz. IN A

;; AUTHORITY SECTION:
ad.example.cz.          360     IN      NS      ad-ns1.example.cz.
ad.example.cz.          360     IN      NS      ad-ns2.example.cz.
ad.example.cz.          360     IN      NSEC    ad-ns1.example.cz. NS ...

;; ADDITIONAL SECTION:
ad-ns1.example.cz.      360     IN      A       217.31.49.71
ad-ns1.example.cz.      360     IN      RRSIG   A 5 3 360 ...
ad-ns2.example.cz.      360     IN      A       217.31.49.70
ad-ns2.example.cz.      360     IN      RRSIG   A 5 3 360 ...
```



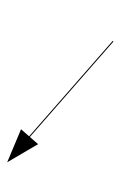
Hranice mezi prvním a druhým fragmentem

Odpověď přijatá resolverem

```
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.aaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaa.aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.aaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.aaaaaaaaaaaaaaaaaaaaaaa.aaaaaaaaaaaa
aa.ad.example.cz. IN A

;; AUTHORITY SECTION:
ad.example.cz.          360    IN    NS     ad-ns1.example.cz.
ad.example.cz.          360    IN    NS     ad-ns2.example.cz.
ad.example.cz.          360    IN    NSEC   ad-ns1.example.cz. NS ...

;; ADDITIONAL SECTION:
ad-ns1.example.cz.      360    IN    A      217.31.49.71
ad-ns1.example.cz.      360    IN    RRSIG  A 5 3 360 …
ad-ns2.example.cz.      360    IN    A      62.109.128.20
ad-ns2.example.cz.      360    IN    RRSIG  A 5 3 360 ...
```



Hranice mezi prvním a druhým fragmentem

Oprava UDP checksumu

Technické výzvy v PoC

- Formátování ICMP packetů (snadné)
- Výběr napadnutelných zón (střední)
- Formátování fragmentů, dopočítání UDP checksumu (těžké)
- Přehrání podvržených packetů do sítě (záleží na administrátorech sítí)
- IP reassembly queue size = 64 @ Linux (další výzkum)
- Randomizace pořadí RR-setů (drobnost)
- Komprese labelů (nevadí)
- Změna pořadí příchodu fragmentů (potenciálně znemožňuje útok)

Akceptace podvrženého packetu

- Bailiwick rules
- Malá důvěra v RR z additional sekce
- Postupné zesilování pravidel v BINDu od roku ~2003
- Neznáme pravidla Unboundu (ale asi budou stejně přísná)

PoC & triky

- Tento útok (prvního typu) funguje v labu!
- Trik: Útočník zná IP ID
- Bez firewallů, bez conntracku
- Průměrně 1 ze 3 pokusů uspěje (kvůli RR-set randomizaci a časování)

Útok druhého typu

- Vytvoření zóny ze specifickými NS RR:
  - Připojíme NS (a jeho glue) serveru, co chceme napadnout
  - Vytvoříme zónu, co způsobuje dlouhé referral odpovědi (N x ~250 B NS RR)
- Zaregistrujeme zónu na nejnižším možném levelu (2nd level zone)

Podvodná zóna v ccTLD

;**poisonovacizona.cz.** IN NS

;; AUTHORITY SECTION:

poisonovacizona.cz. 18000 IN NS eaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

kaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

qaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

waaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

poisonovacizona.cz.

...

poisonovacizona.cz. 18000 IN NS **ns2.ignum.cz.**

;; ADDITIONAL SECTION:

ns2.ignum.cz. 18000 IN A **217.31.48.201**

eaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

kaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

qaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

waaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.

poisonovacizona.cz. 18000 IN A 217.31.48.1

...

;; **MSG SIZE rcvd: 1949**

Útok pomocí podvodné zóny

- Zóna způsobuje sama fragmentaci odpovědí
- Zóna je zcela validní
- … přestože je na první pohled “divná”
- Obshauje NS pro důležitý DNS server, jehož glue chceme napadnout
- Glue pro cílový server bude v druhém fragmentu

Obrana

- Nasaďte DNSSEC!

- Dočasná opatření
  - První typ: Ignorovat ICMP type=3, code=4
  - Druhý typ: omezit velikost odpovědi a nastavit EDNS0 buffer size na stejnou hodnotu, jako MTU (na obou stranách – autoritativní i rekurzivní)

Děkuji za pozornost!

Tomáš Hlaváček • tomas.hlavacek@nic.cz •
IT13.2, 30.11.2013