Blocking DNS Messages is Dangerous

Florian Maury, *Mathieu Feuillet*

October 5-6, 2013

ANSSI

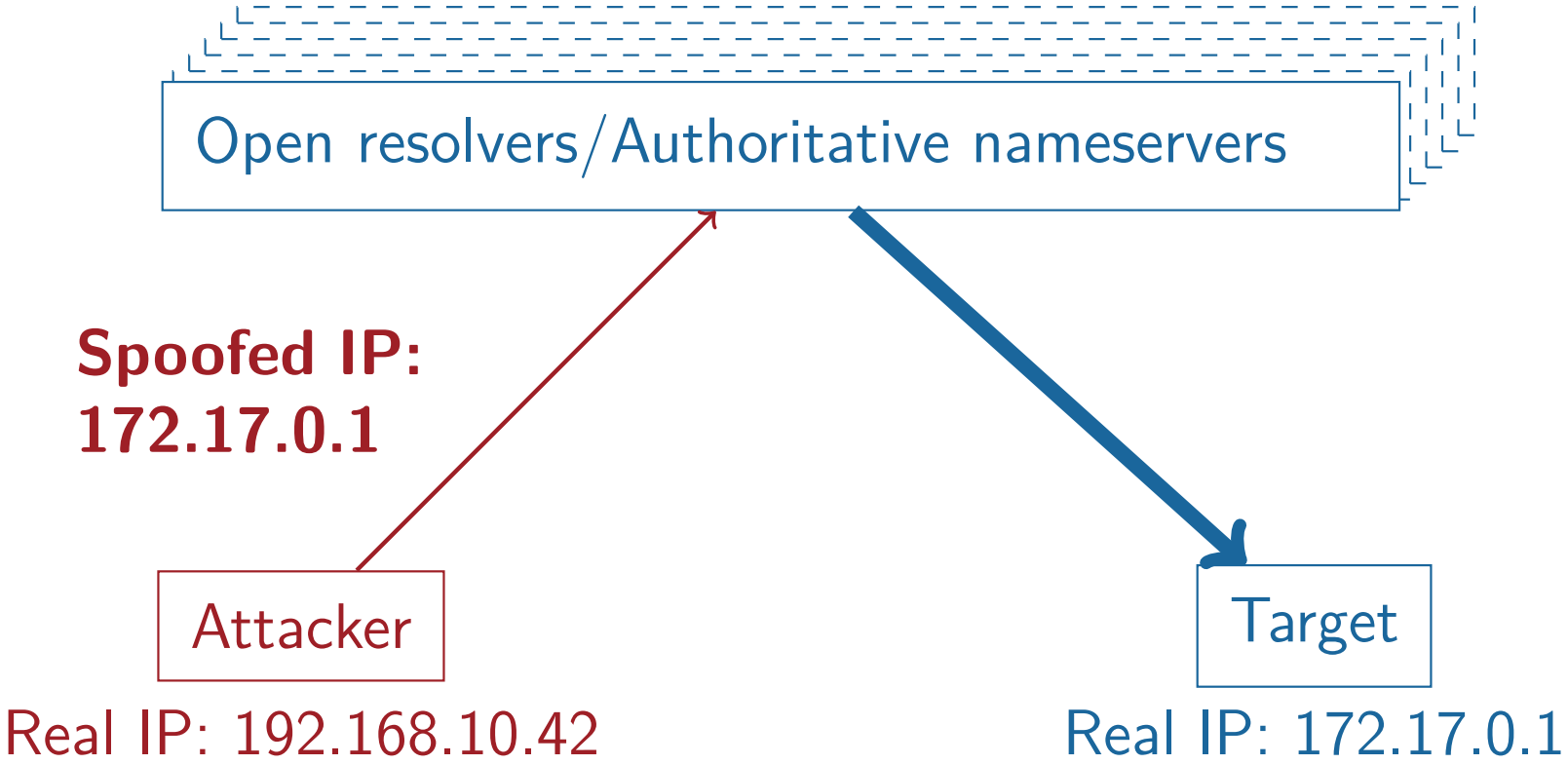
- Created in 2009, the ANSSI is the French national authority for the defense and the security of information systems
  - in French, ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information
- Under the authority of the Prime Minister
- Main missions are:
  - prevention
  - defense of French information systems
- One of its priorities is DDoS prevention and mitigation

http://www.ssi.gouv.fr/en

State of the art regarding DNS-related DDoS

DNS reflection attacks

Threat: on IP networks, sender address **can be spoofed**



DNS amplification attacks

Principle:

- Based on reflection attacks
- **Increase** the attacker **throughput** by leveraging **non-malicious nameservers**
- DNS answer IP packets are often **40-50 times** the size of the associated query IP packets
- 2 Mbps (attacker) $\Rightarrow$ 100 Mbps (target)

Amplifications attacks countermeasures

What can an operator do?

DNS messages can be filtered at different levels:

- L3 Drop packets
- L4-7 Drop DNS datagrams or queries
- L7 Response Rate Limiting (RRL):
  - Identical DNS answers detection
  - Bind, NSD, Knot
  - **Slips a truncated answer every X queries**
    - e.g. 2 Mbps (attacker) $\Rightarrow$ up to 2 Mbps (target)

Can anti-DDoS technologies

be useful for cache poisoning attacks?

Cache poisoning attacks reminder

Principle:

- Insert forged data in cache

Example:

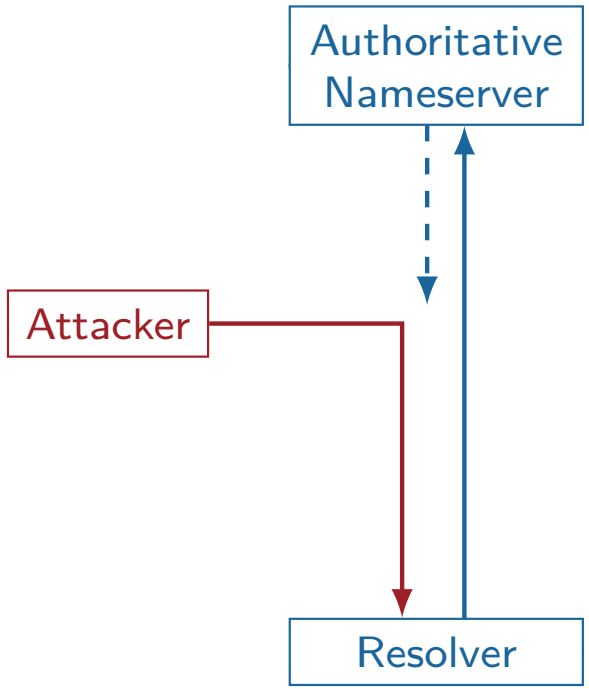
- 2008: Kaminsky attack

Current Fix:

- Source Port Randomization

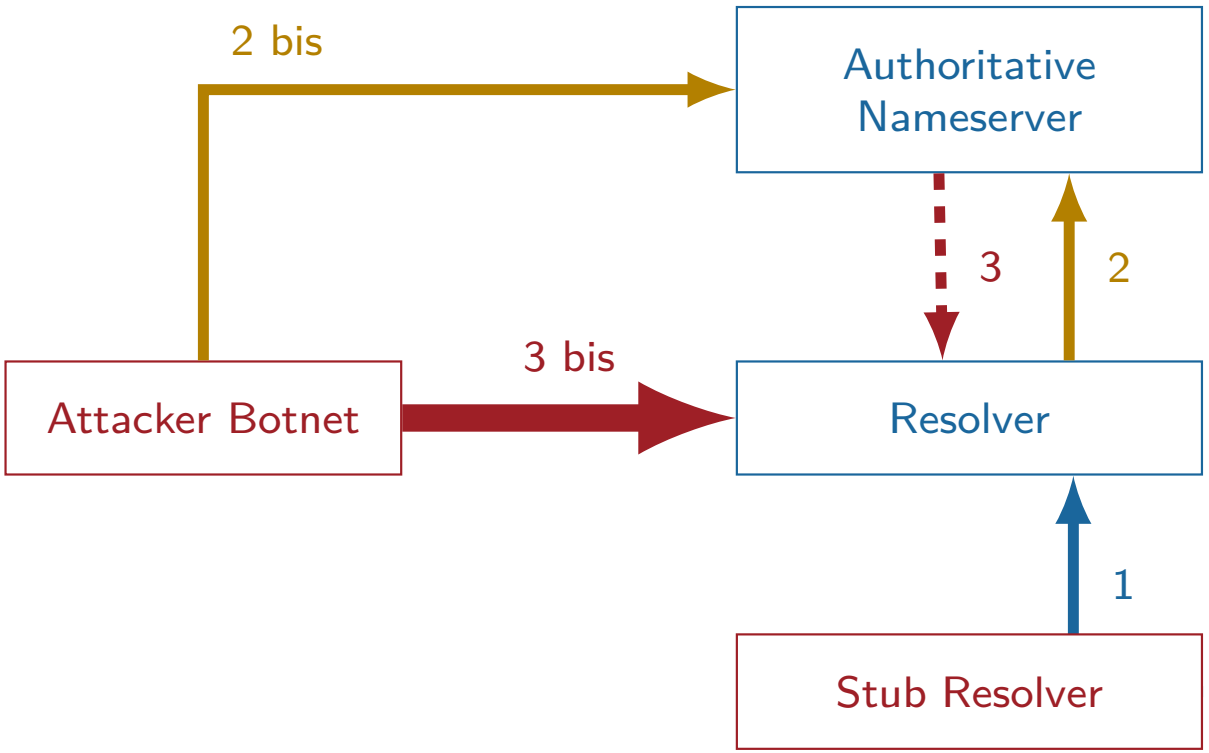
Long Term Fix:

- DNSSEC
  - Requires large adoption



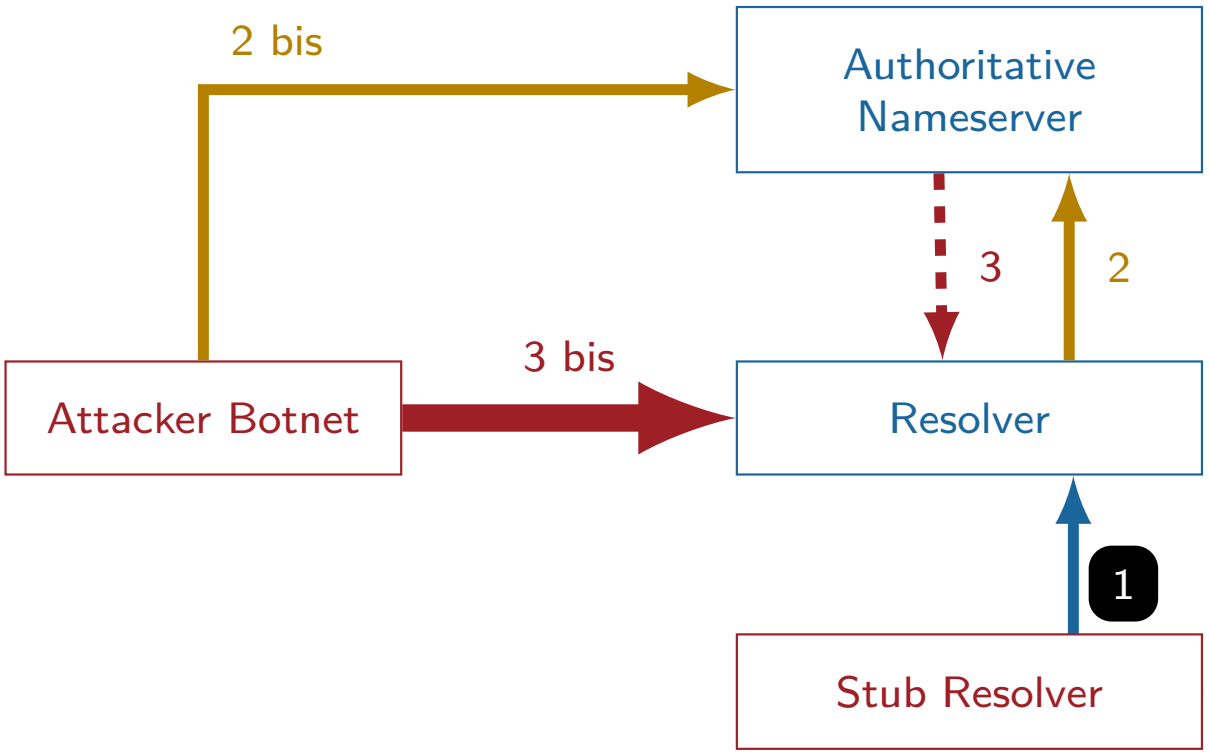
Exploiting anti-DDoS mechanisms

Our cache poisoning attack: Step by step



Exploiting anti-DDoS mechanisms

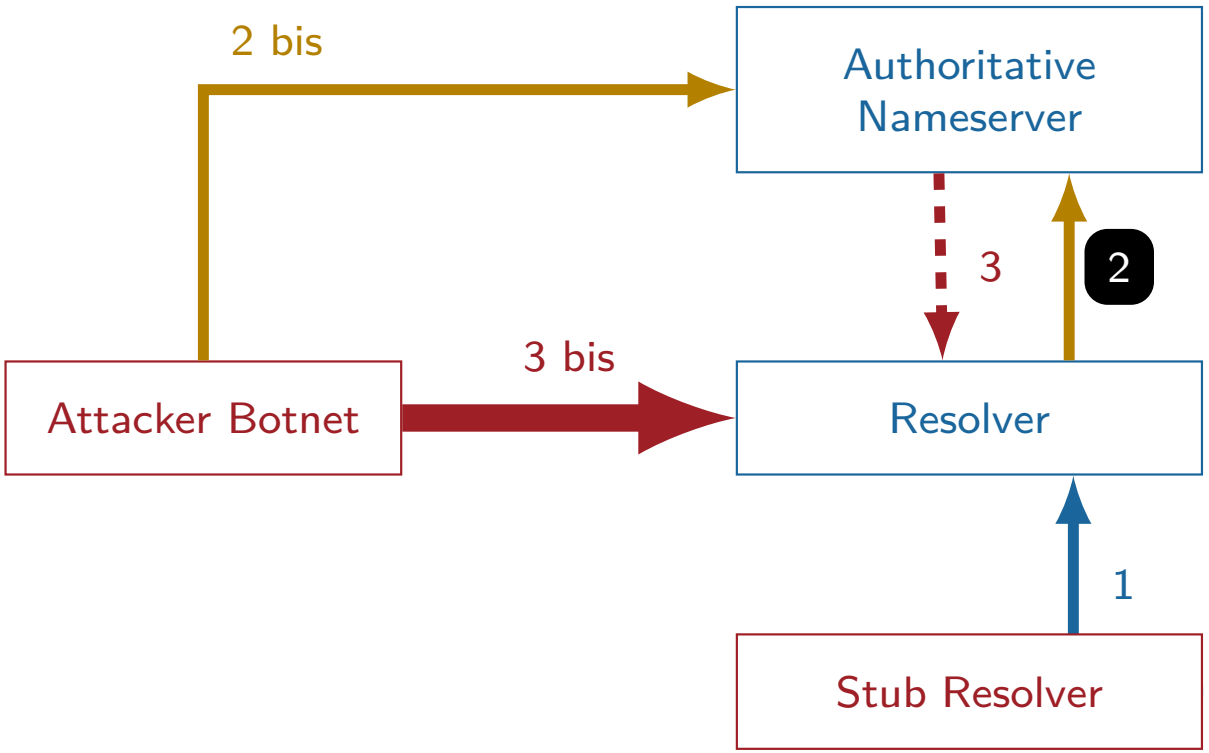
Our cache poisoning attack: Step by step



1: Send a query

Exploiting anti-DDoS mechanisms

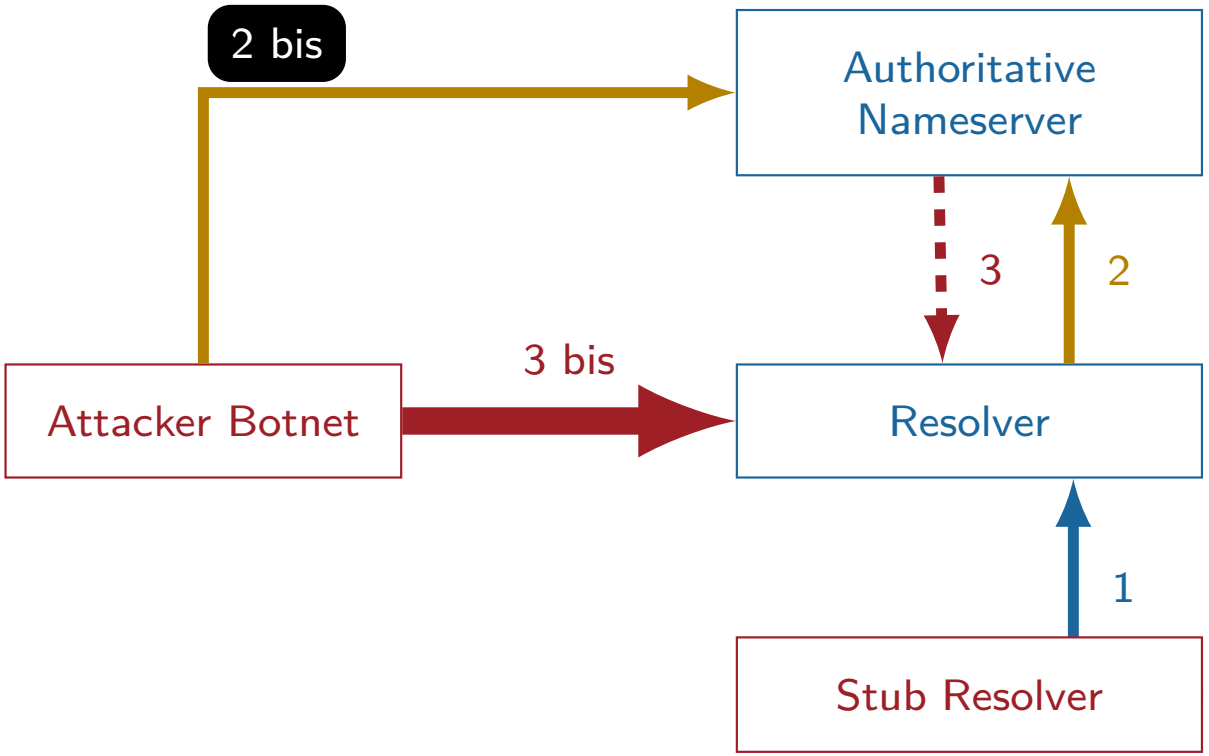
Our cache poisoning attack: Step by step



2: Perform the recursive resolution

Exploiting anti-DDoS mechanisms

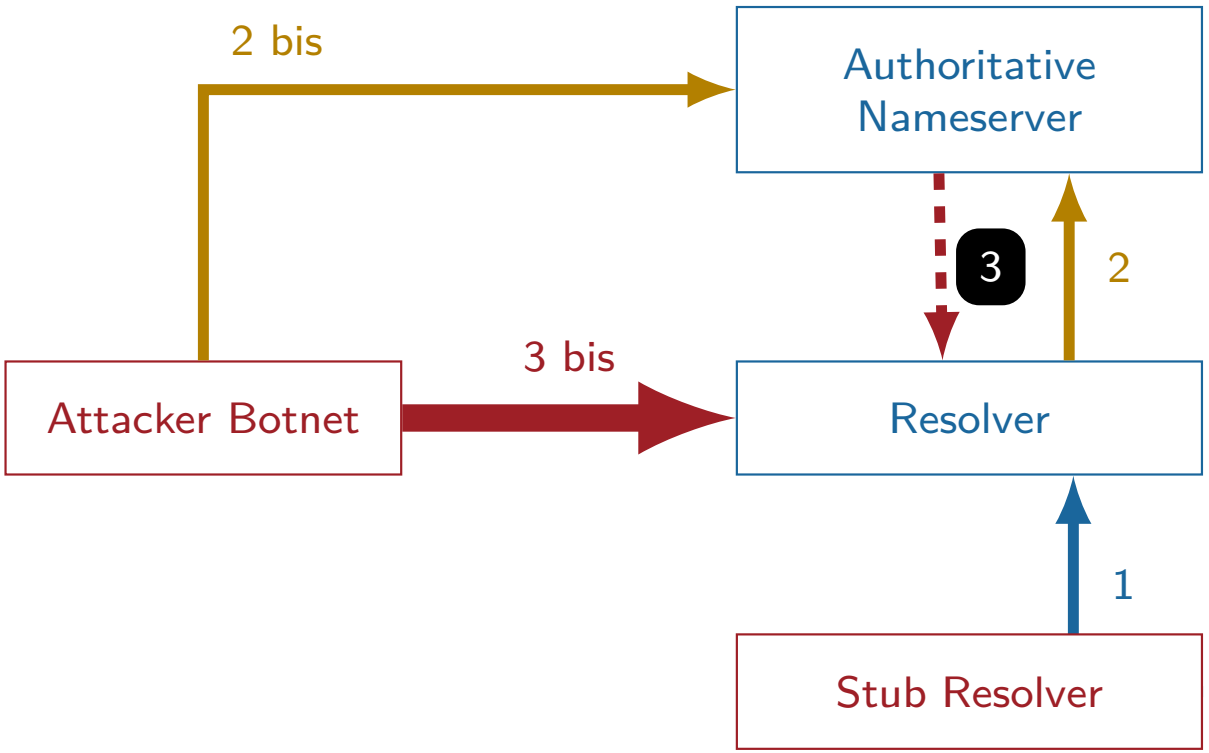
Our cache poisoning attack: Step by step



2 bis: Trigger anti-DDoS mechanism against the resolver

Exploiting anti-DDoS mechanisms

Our cache poisoning attack: Step by step

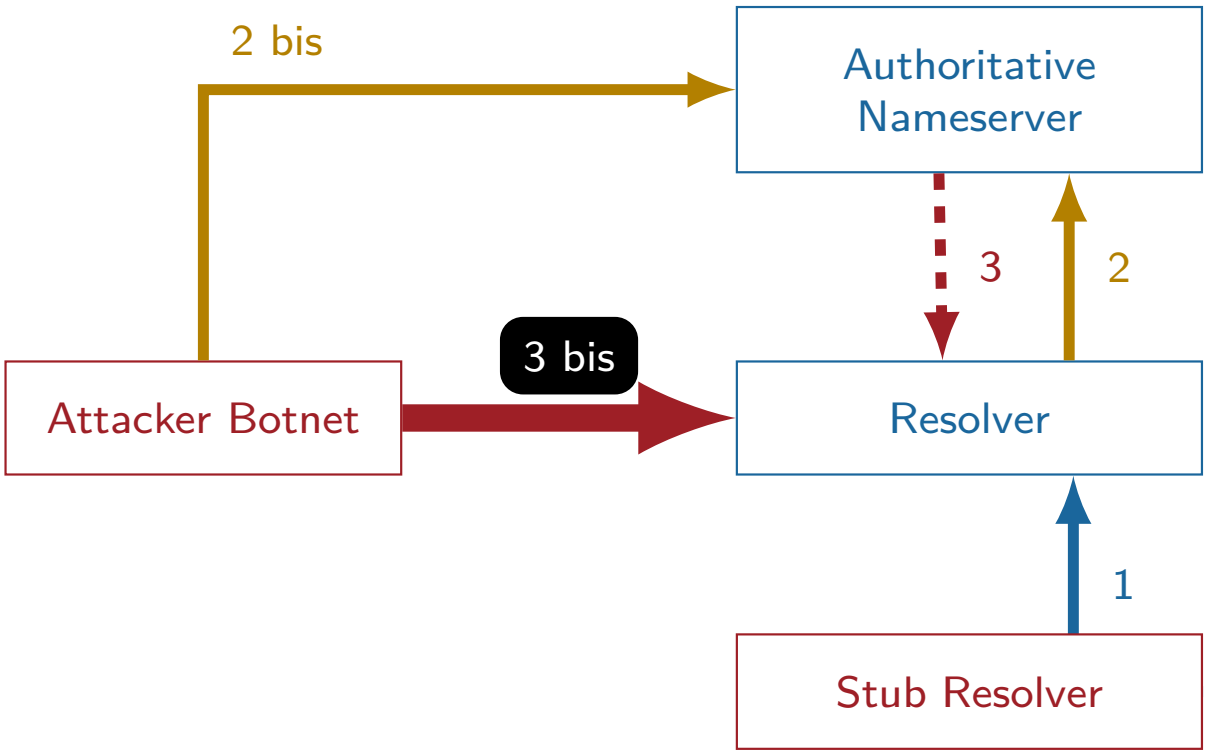


3: Either answer with a truncated answer or drop the query

Dropping answers lead to resolver timeouts and retries

Exploiting anti-DDoS mechanisms

Our cache poisoning attack: Step by step



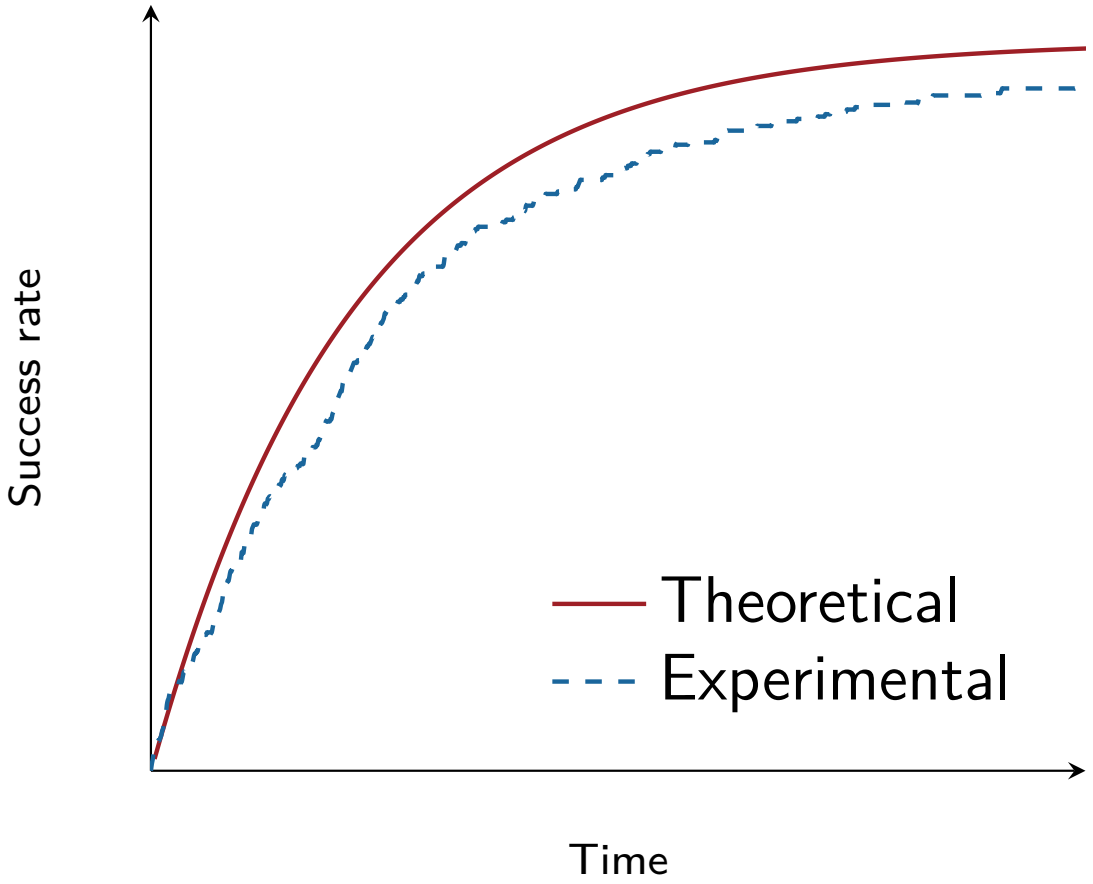
3 bis: Send lots of Kaminsky-style answers to poison the cache

Experiments & results

Attack setup

- A single authoritative nameserver
  - Realistic thanks to authoritative nameserver selection attacks (Shulman fragment attacks, SRTT tricks. . .)
- A single outbound IP on resolver
- 100 Mbps of spoofed traffic
  - would go unnoticed by most ISP
- RRL with slip=2

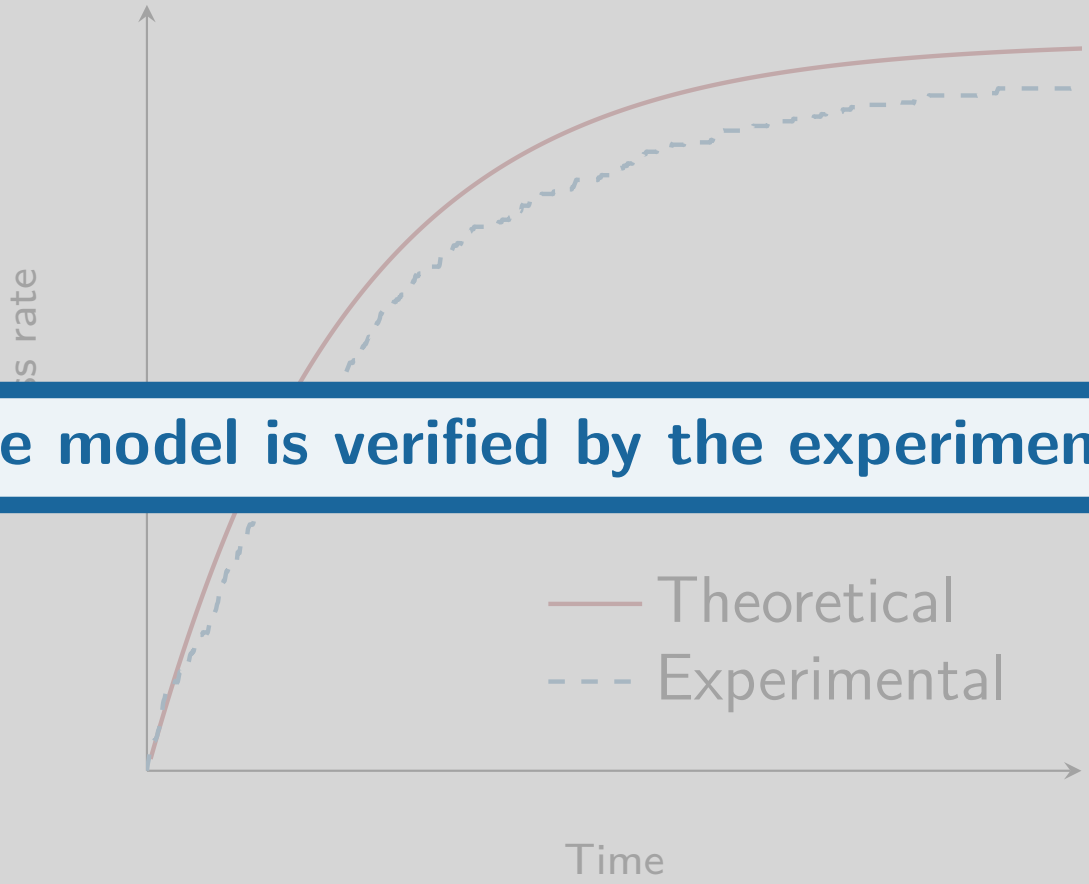
Validation of the theoretical model



We mathematically modeled the attack

Details available on demand

Validation of the theoretical model



The model is verified by the experiments

We mathematically modeled the attack

Details available on demand

Results based on the model

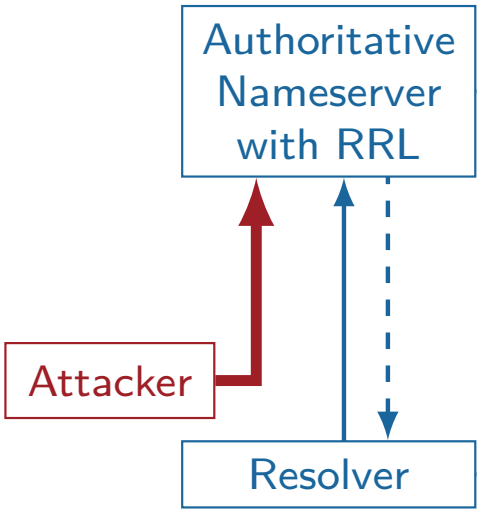
Based on the model, real-world attacks can be successful with a probability P in less than the following time estimates:

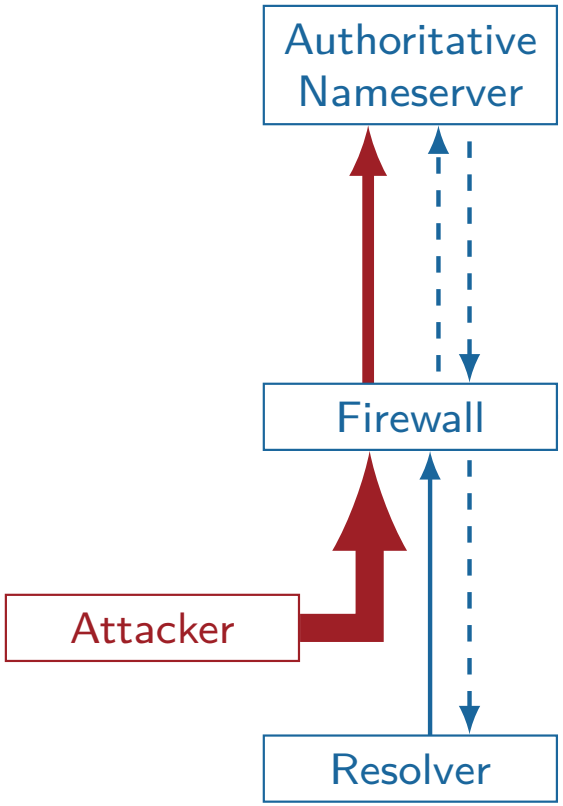
P: Probability of a successful cache poisoning attack

$P = 10\%$	$\approx$ **1h 15min**
$P = 50\%$	$\approx$ **8h**

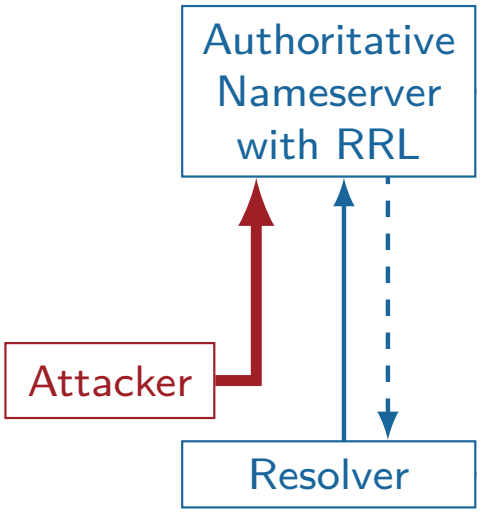
Are firewalls doing any better?

General-purpose firewalls

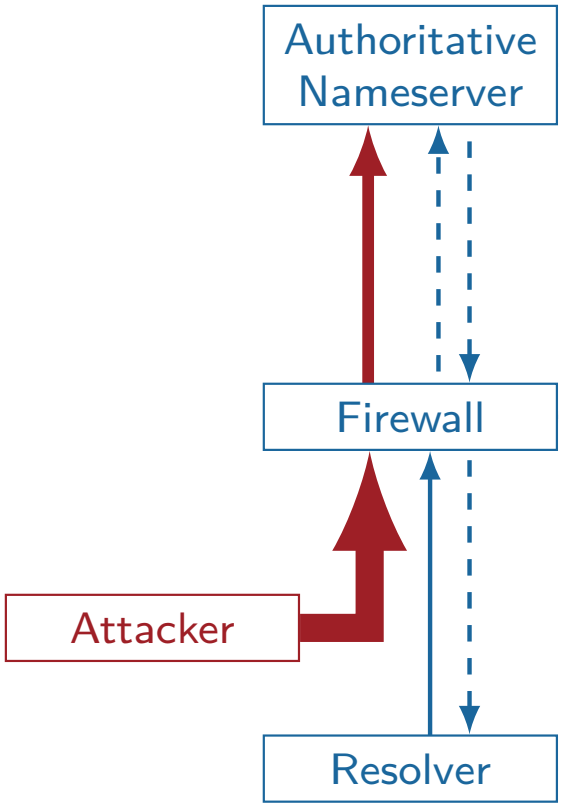




General-purpose firewalls



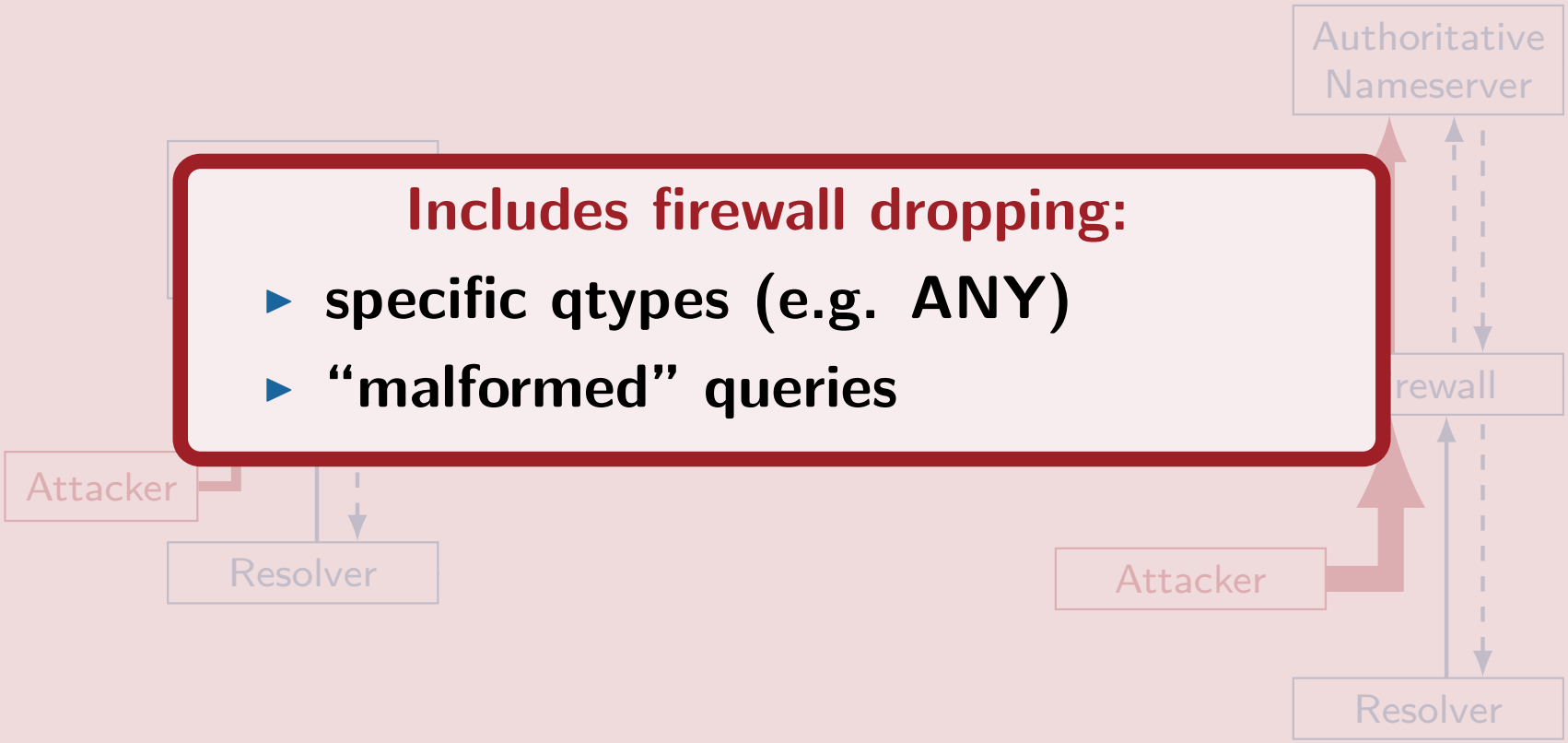
is equivalent to



General-purpose firewalls

Includes firewall dropping:

- **specific qtypes (e.g. ANY)**
- **“malformed” queries**



ANSSI recommendations

ANSSI recommendations

Always answer queries

- **Never drop DNS queries when you can't tell which are legitimate**

Slip 1 is the only RRL safe configuration against our cache poisoning attack

Disclosure timeline

Timeline and feedbacks

Disclosure timeline:

- June: DNS Software Vendors, Packagers
- August: NIC and root operators
- May-August: CERTs

Security notifications:

- CVE-2013-5661 and CVE-2013-5752
- CERTA and NCSC advisory bulletin (September 9th, 2013)

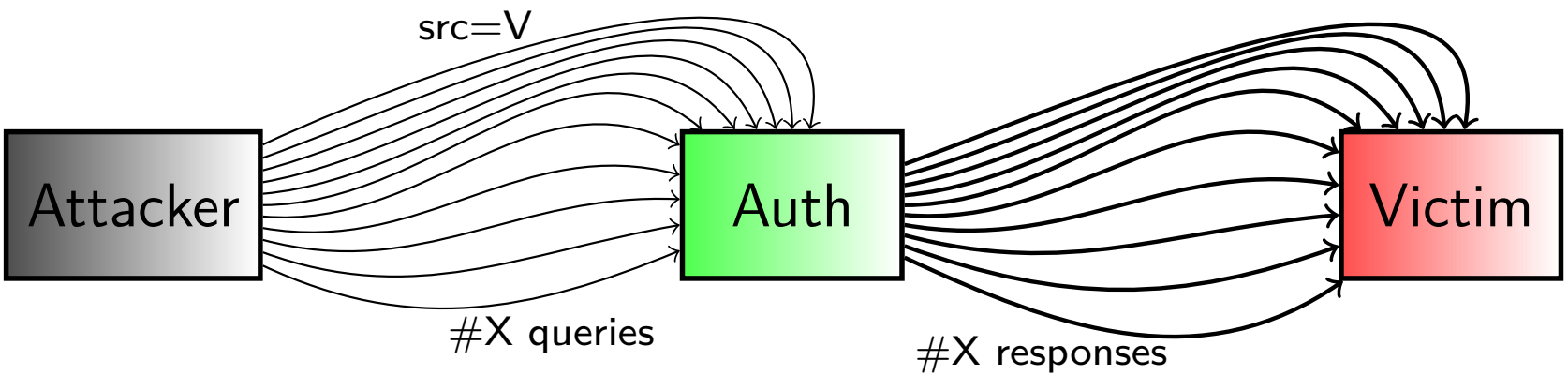
All have confirmed the vulnerability

Some raised concerns

Is slip 1 dangerous?

Is slip 1 dangerous?

Concern 1: reflection attacks

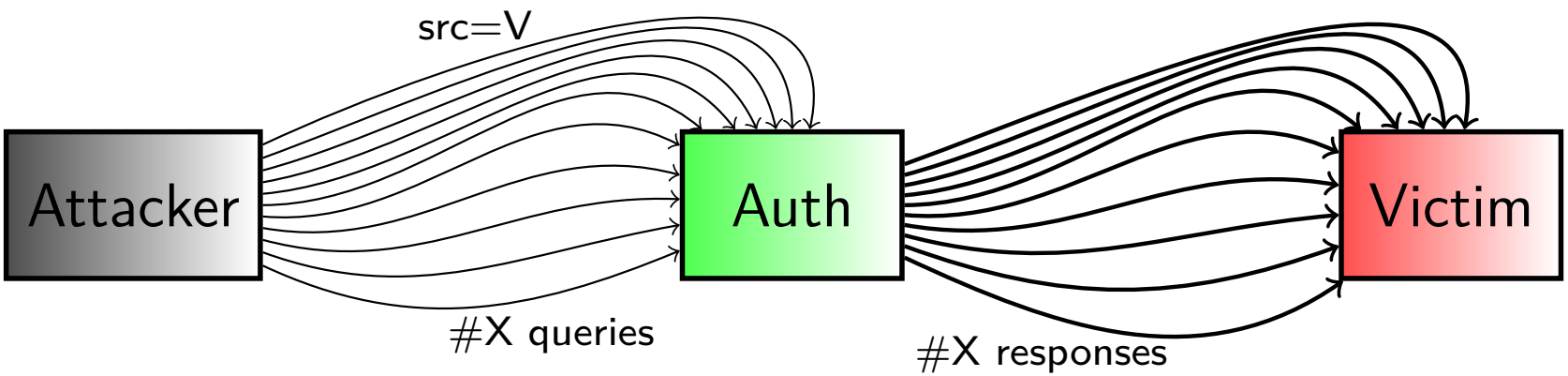


courtesy of netnod

As slip 1 grants an even payback, is this configuration dangerous for PPS attacks?

Is slip 1 dangerous?

Concern 1: reflection attacks

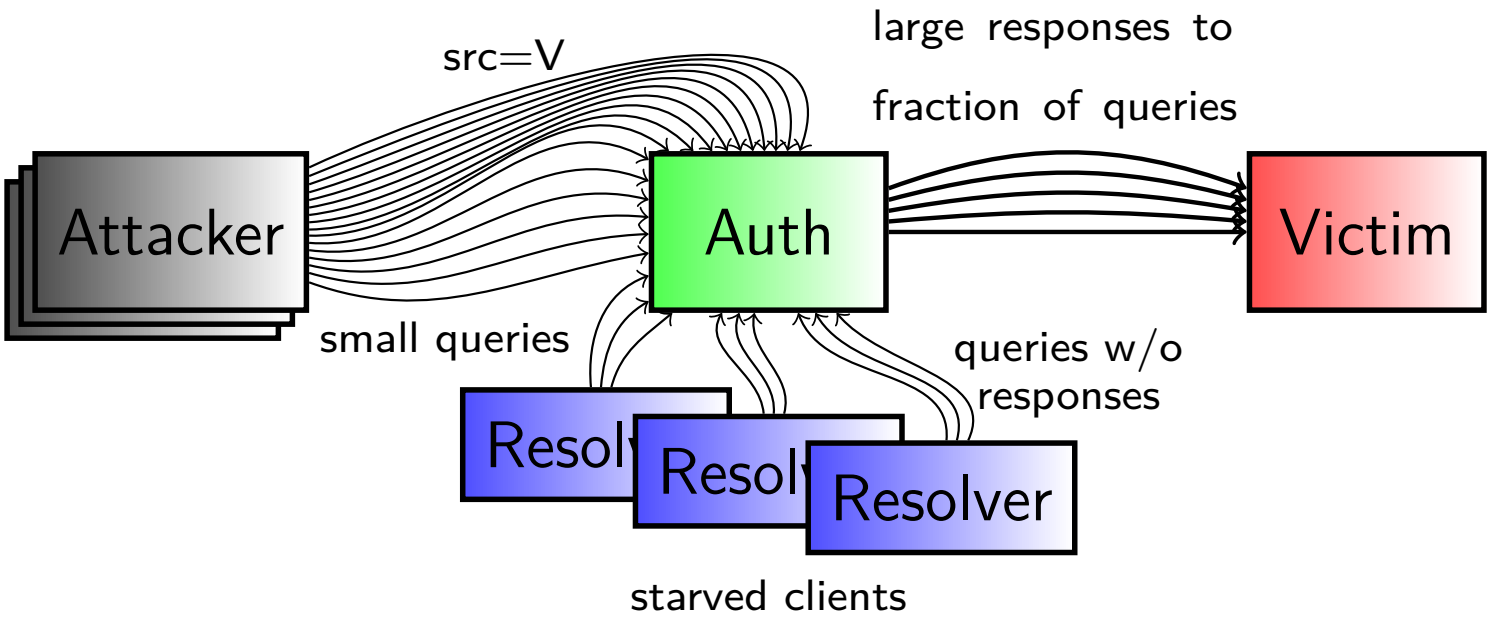


Facts:

- **Current** attacks are volumetric/bandwidth-related DDoS
- More susceptible protocols available for PPS attacks

Is slip 1 dangerous?

Concern 2: authoritative nameservers DDoS

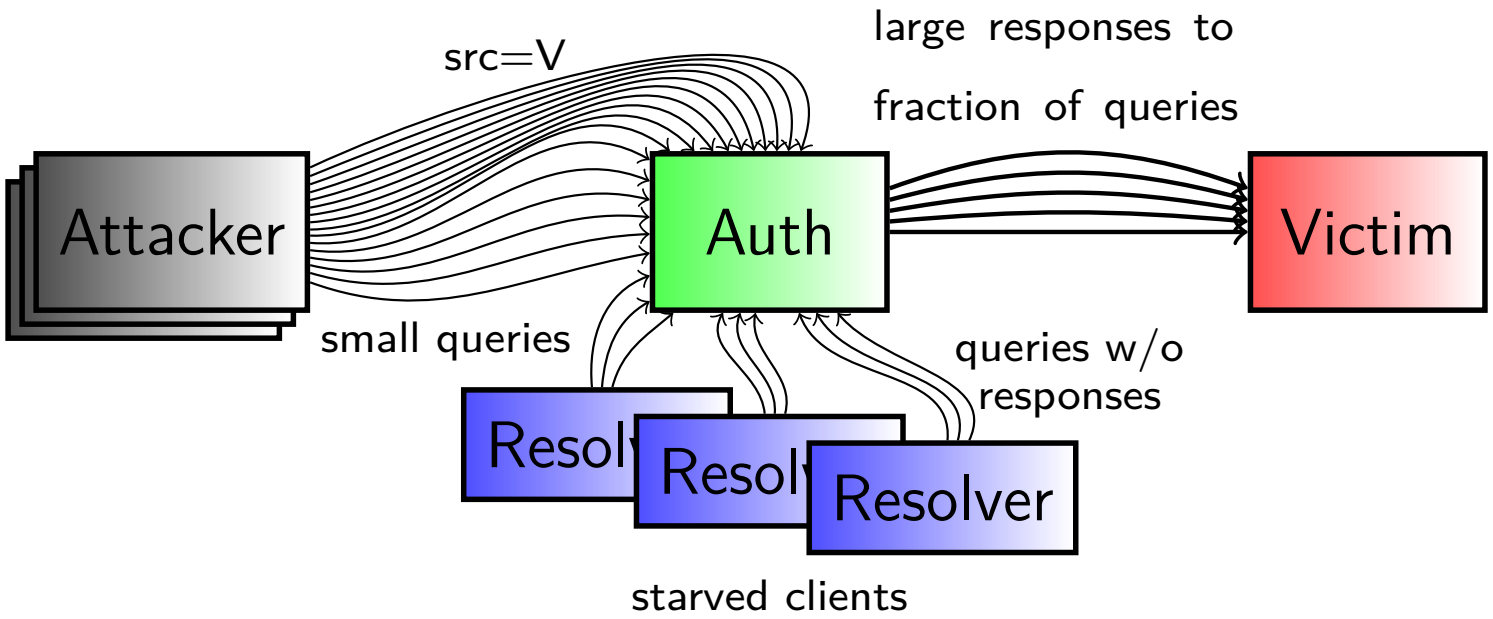


courtesy of netnod

Network DDoS on the authoritative nameservers because of slip 1?

Is slip 1 dangerous?

Concern 2: authoritative nameservers DDoS



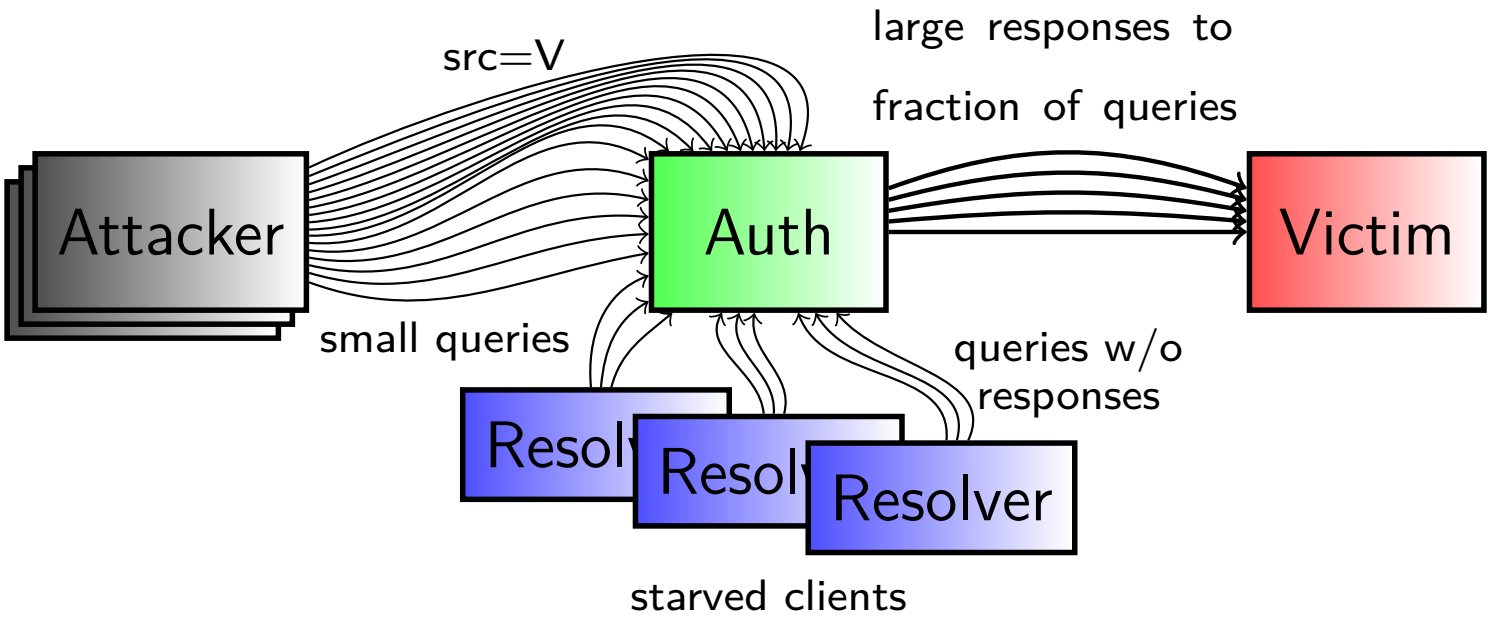
Facts:

- Amplification factor: 1:1
- Operators have symmetric bandwidth

Investigation should be led if upload capacity is reached

Is slip 1 dangerous?

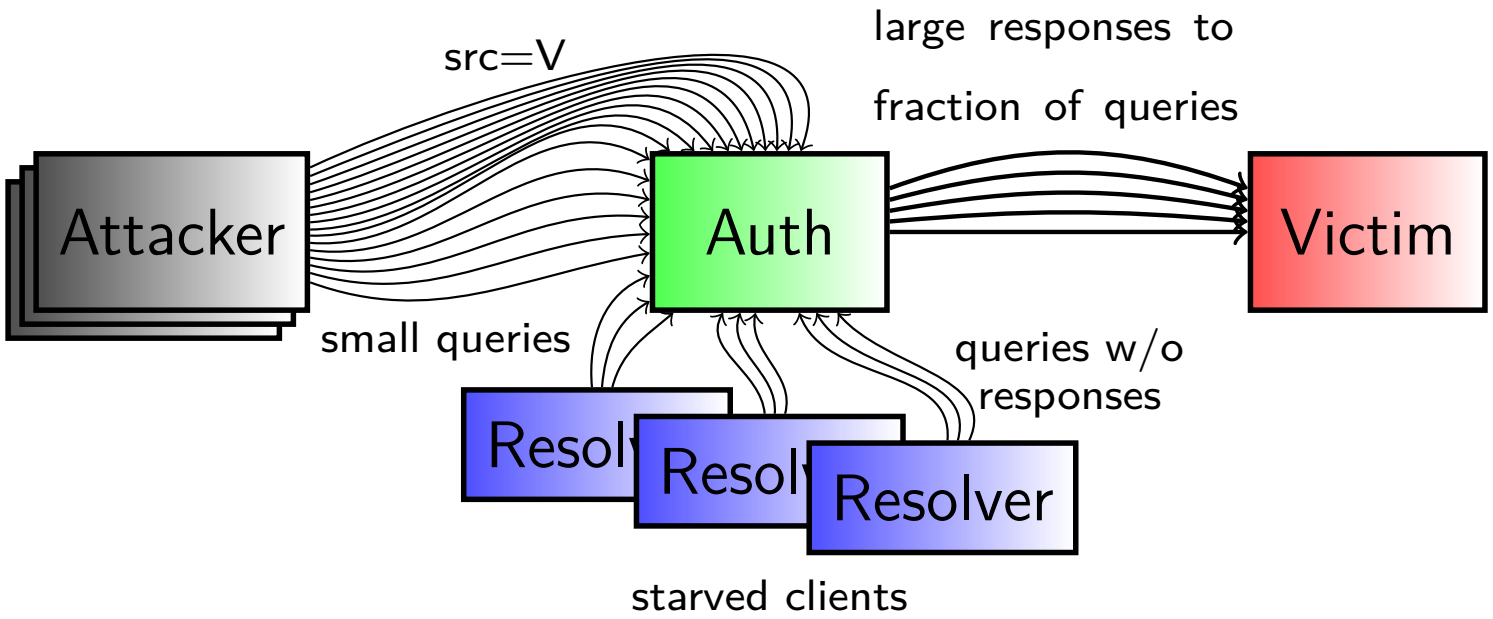
Concern 2: authoritative nameservers DDoS



Computational DDoS on the authoritative nameservers because of slip 1?

Is slip 1 dangerous?

Concern 2: authoritative nameservers DDoS



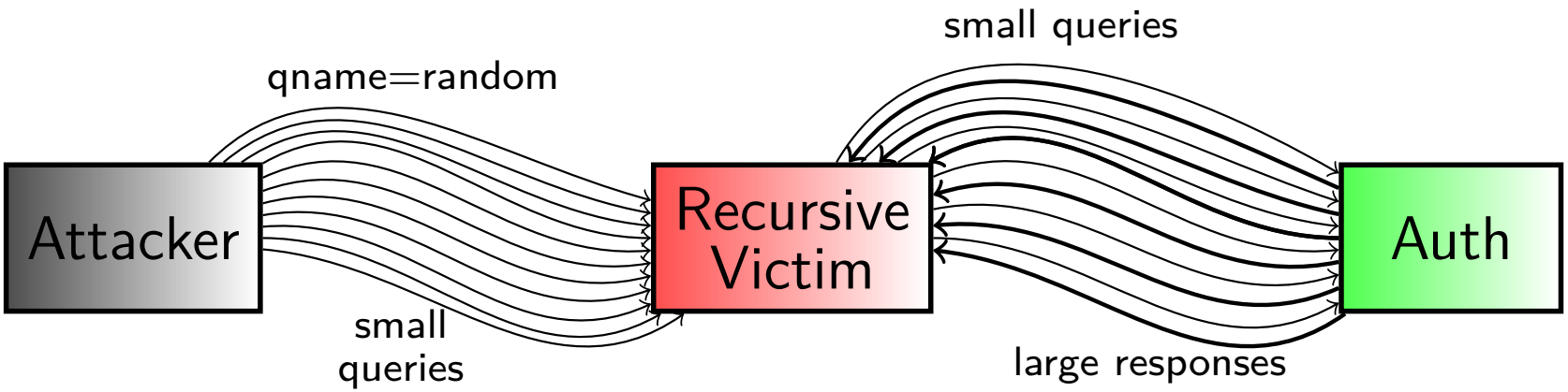
Fact[a]:

- Slip 1 **increases** CPU consumption by less than 5% depending on implementations

[a] tested on Xeon X5650 @2.67Ghz with 4000 qps

Is slip 1 dangerous?

Concern 3: recursive servers DDoS

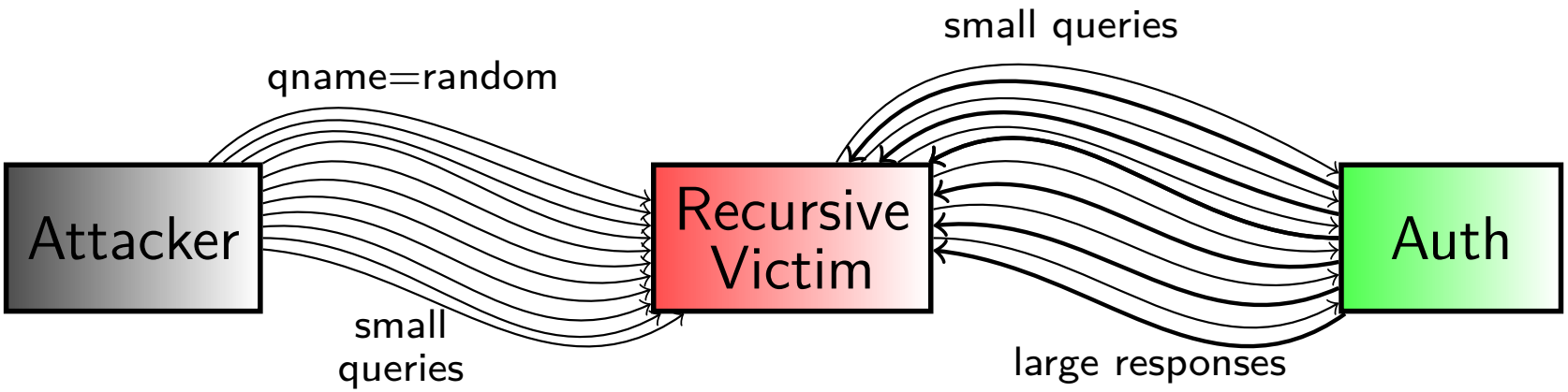


courtesy of netnod

Network DDoS on the resolver because of slip 1 on the authoritative nameserver?

Is slip 1 dangerous?

Concern 3: recursive servers DDoS

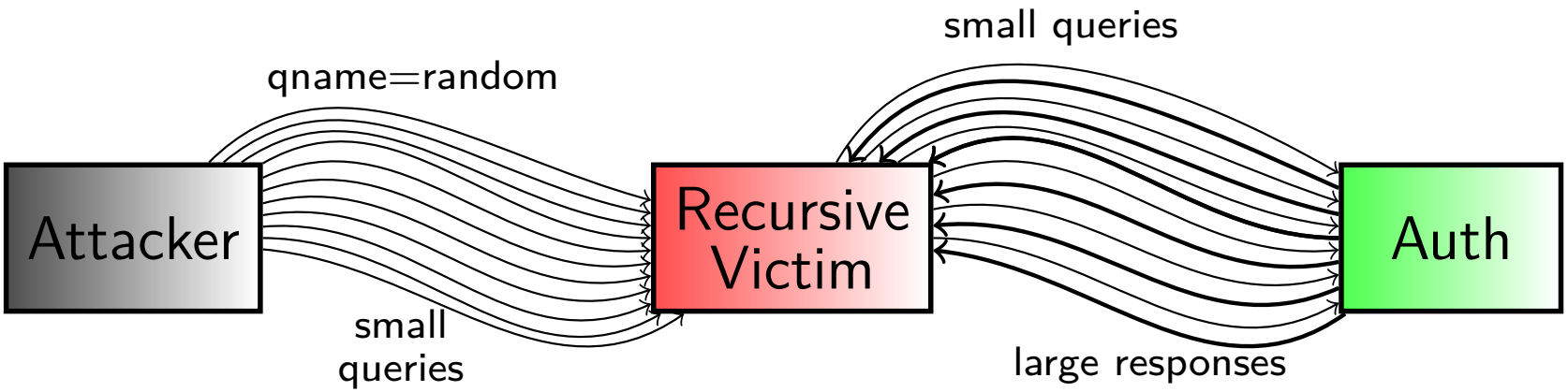


Fact:

- On average, the number of packets exchanged between a resolver and authoritative nameserver per query:
  - Slip 1: 9
  - Slip 2: 9.68

Is slip 1 dangerous?

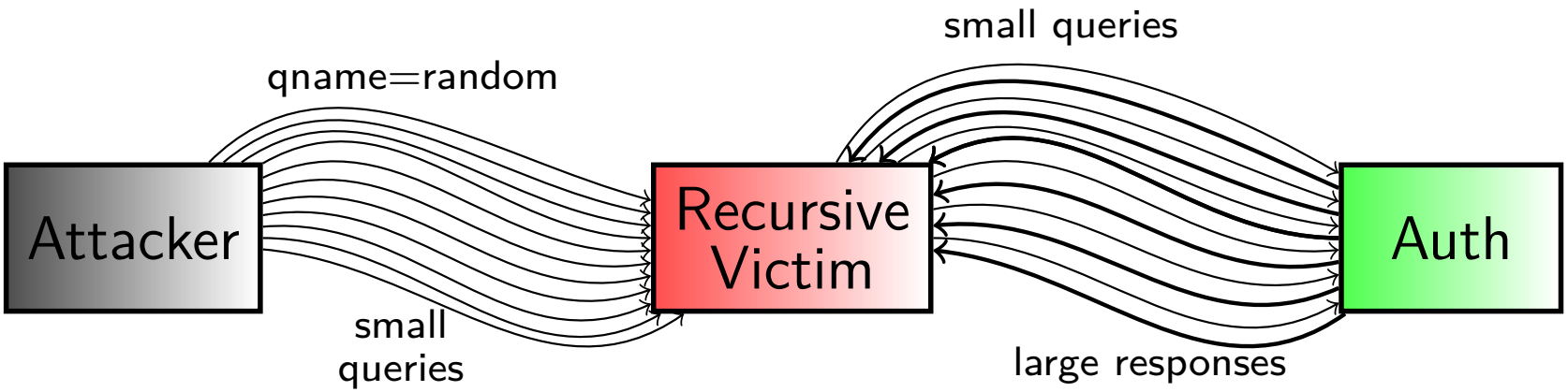
Concern 3: recursive servers DDoS



Computational DDoS on the resolver because of slip 1 on the authoritative nameserver?

Is slip 1 dangerous?

Concern 3: recursive servers DDoS



Fact[a]:

- Slip 1 **decreases** CPU consumption by up to 20%, depending on implementations

[a] tested on Xeon X5650 @2.67Ghz with 4000 qps

Is slip 1 dangerous?

RRL with Slip 1:

- Is worthless for attackers performing volumetric or PPS DDoS attacks
- is less CPU consuming for flooded resolvers
- Is a negligibly more CPU consuming for authoritative nameservers

TL;DR summary: **Slip 1 is OK**

Conclusion

- Timeouts lead to more efficient cache poisoning attacks
- Always answering queries:
  - **Thwarts** our attack
  - Offers **no benefit** for attackers
- **RRL Slip=1 mitigates DDoS**
  - RRL Slip=2 is **overkill** for current DDoS attacks and is **vulnerable** to our cache poisoning attack
- Always answering is a temporary fix:
  - DNSSEC wake-up call?

Thank you for your attention

Any questions?

Packets count for DOS of recursive servers

$$E(PC) = \sum_{i=1}^{n} \left(1 - \frac{1}{s}\right)^{i-1} \left(1 + \frac{8}{s}\right)$$

with $E(PC)$ being the mean packet count,
n being the number of retries by the resolver
and s being the slip value