Reflections on Amplifications

(Protocols as Weapons)

Jaap Akkerhuis

NLnet Labs

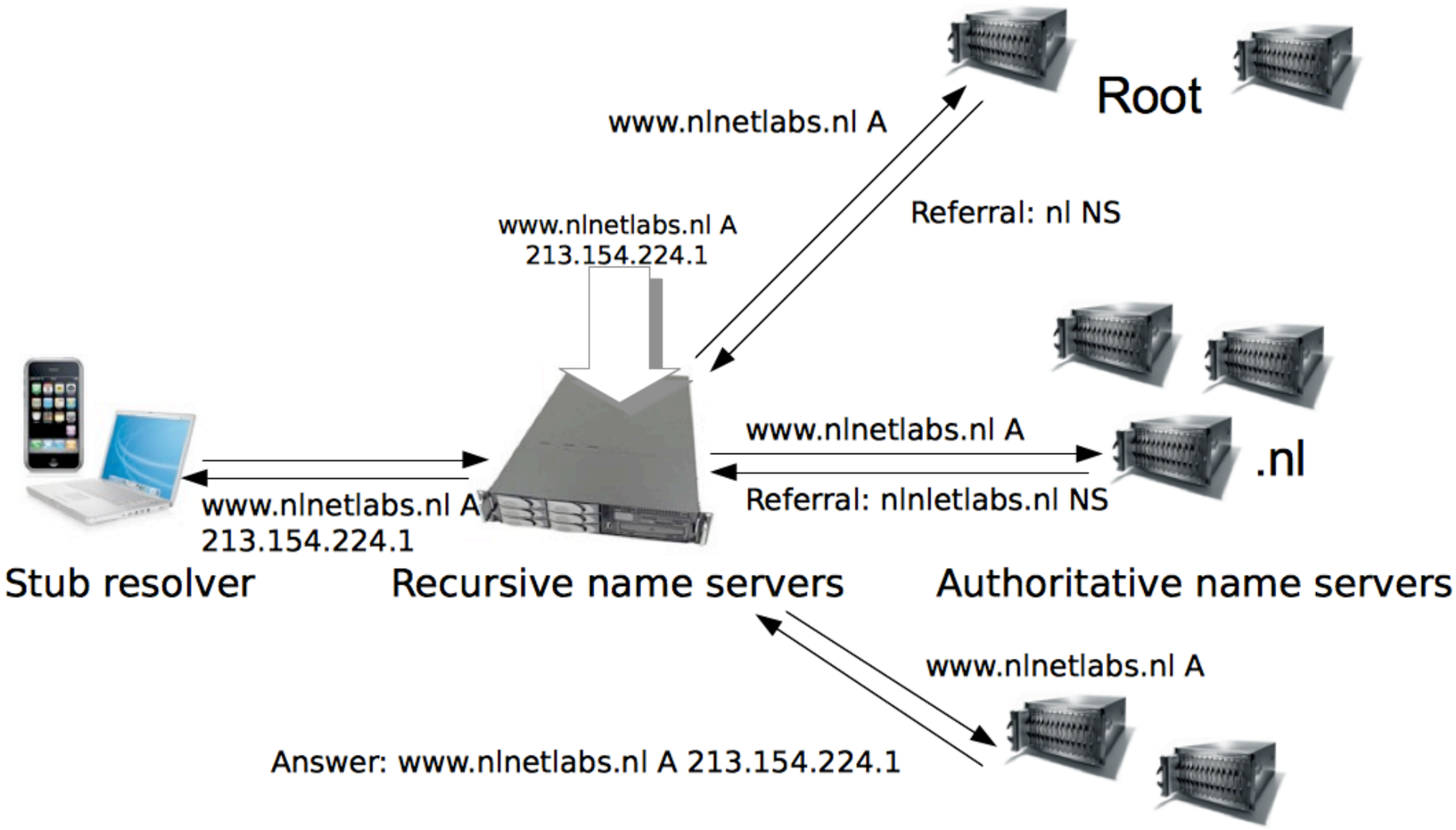
who m i

- Old Timer
- NLnet Labs guy
- Ripe DNS-WG co-chair
- IETF participant
- SSAC member
- Gray Beard is missing...

Overview

- Amplification
- Reflection
- Spoofing
- Mitigation of Attacks
- Some conclusions

DNS Overview



Amplification

- A small question can cause big answers
- UDP has no authentication model
- "Makes DNS a hot Target"

Amplification rates

- ANY Queries
  - Up to 80 times
- NXDomain + DNSSEC
  - NXDOMAIN, NSEC: 18x
  - NXDomain, NSEC3: 25x

Reflection & Spoofing

- Make answer go somewhere else
- Lie about origination of the question
- Replace with victims address

"Source address spoofing"

NLnet Labs

Mitigation, the Easy part

- Answer only to who you know
  - Close Open Resolvers
    - 21 Million of them
    - Don't forget the nasty NAT boxes (CPEs)
    - Saves bandwidth, reputation, headaches
- RFC 5358

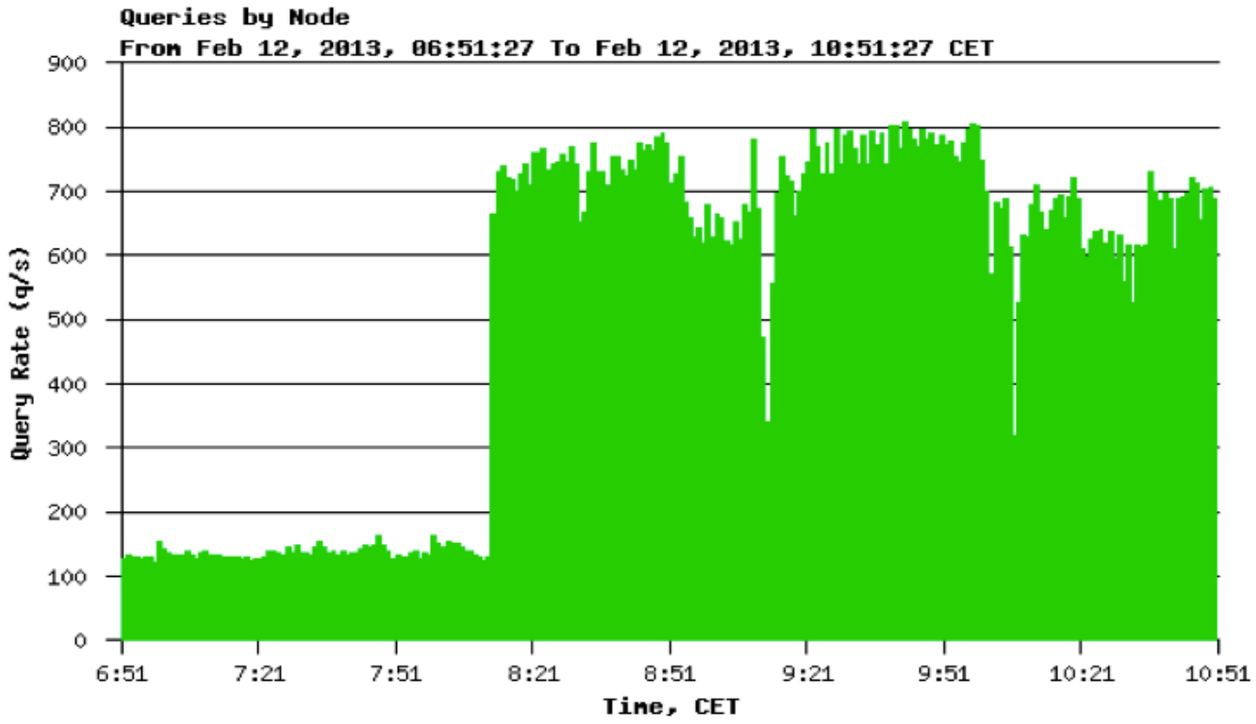
Abusing the Authoritative

Service to many recursive name servers

Wide Audience, RFC 5358 not applicable

NLnet Labs

Impact of Attack



Mitigation Principle

- Don't help the attacker
  - Keep answering some queries to well behaving clients
- No Service degrading
  - (victims or others)

Mitigation Proposals

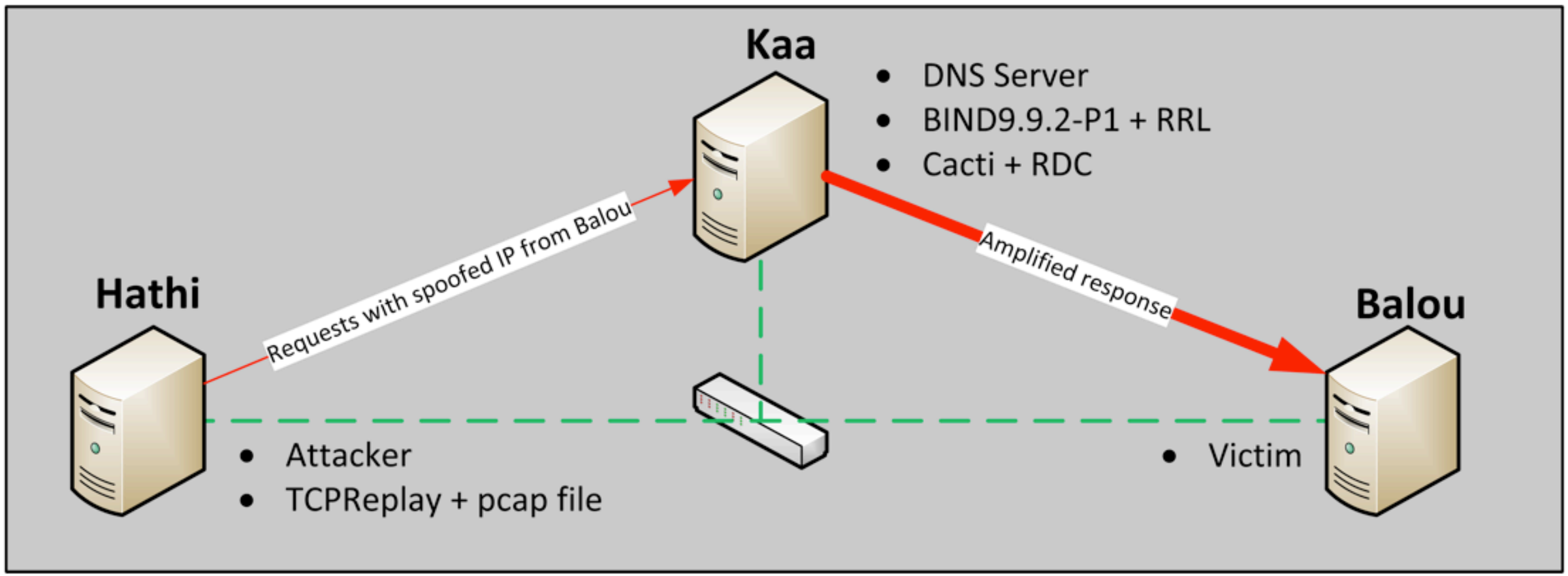
- Query limiting
  - DNS Firewalls
    - Suppress ANY Queries
- DNS Dampening
- Response Rate Limiting (RRL)

RRL

- Drop answers that exceed limits
- False positive mitigation
  - TCP fallback
    - allows victim to contact server over TCP
- Performs reasonably well

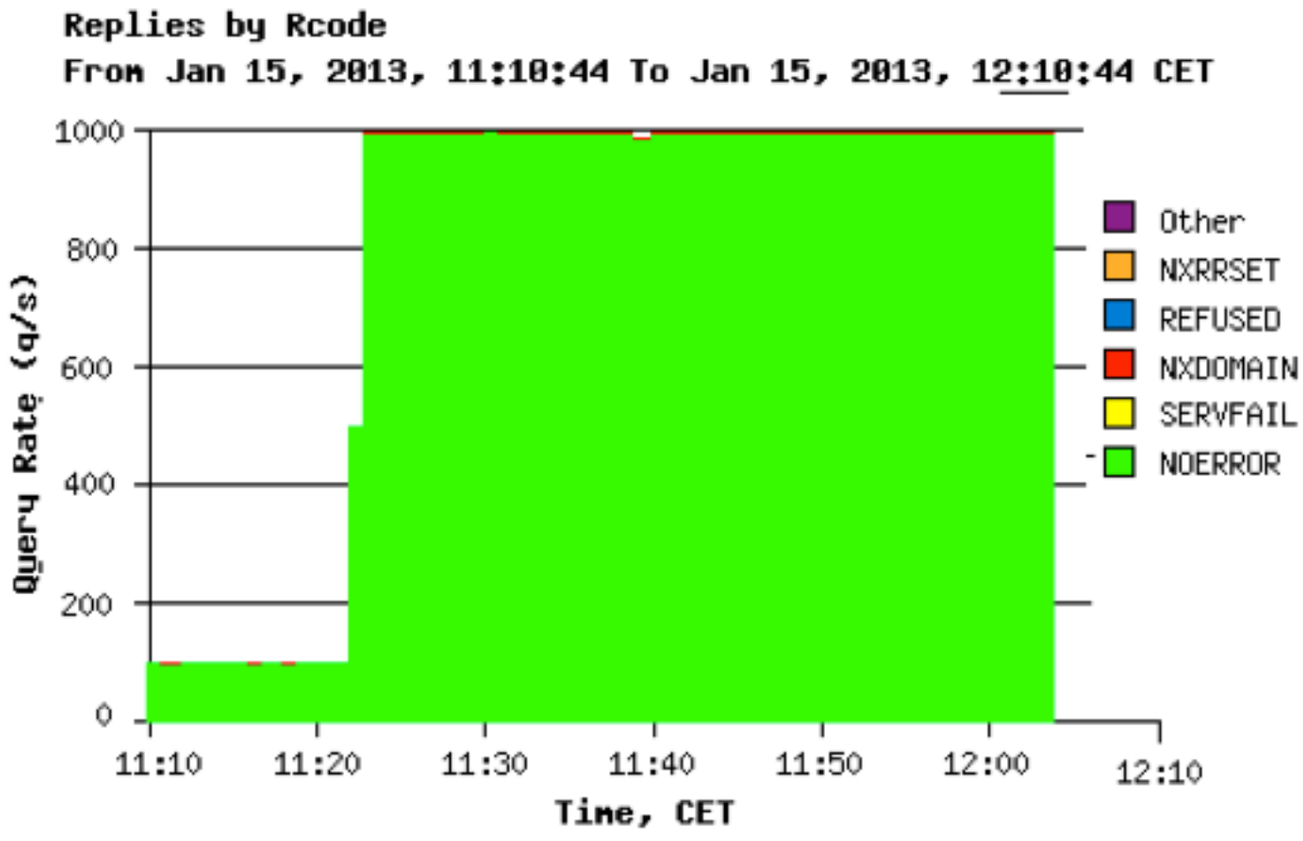
RRL Measurements

- Set up



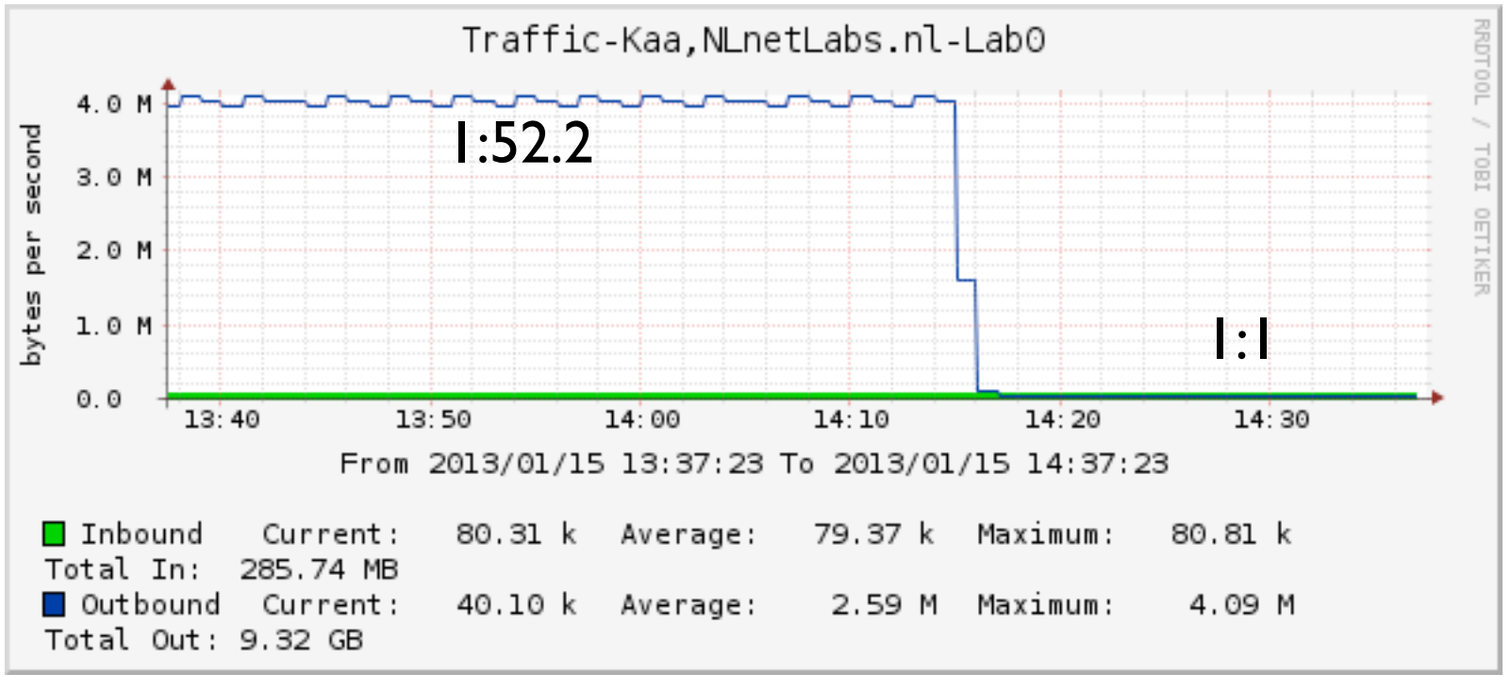
RRL Measurements

- ANY attack at 11:20



RRL Measurements

- ANY attack at 11:20, RLL enabled at 14:15

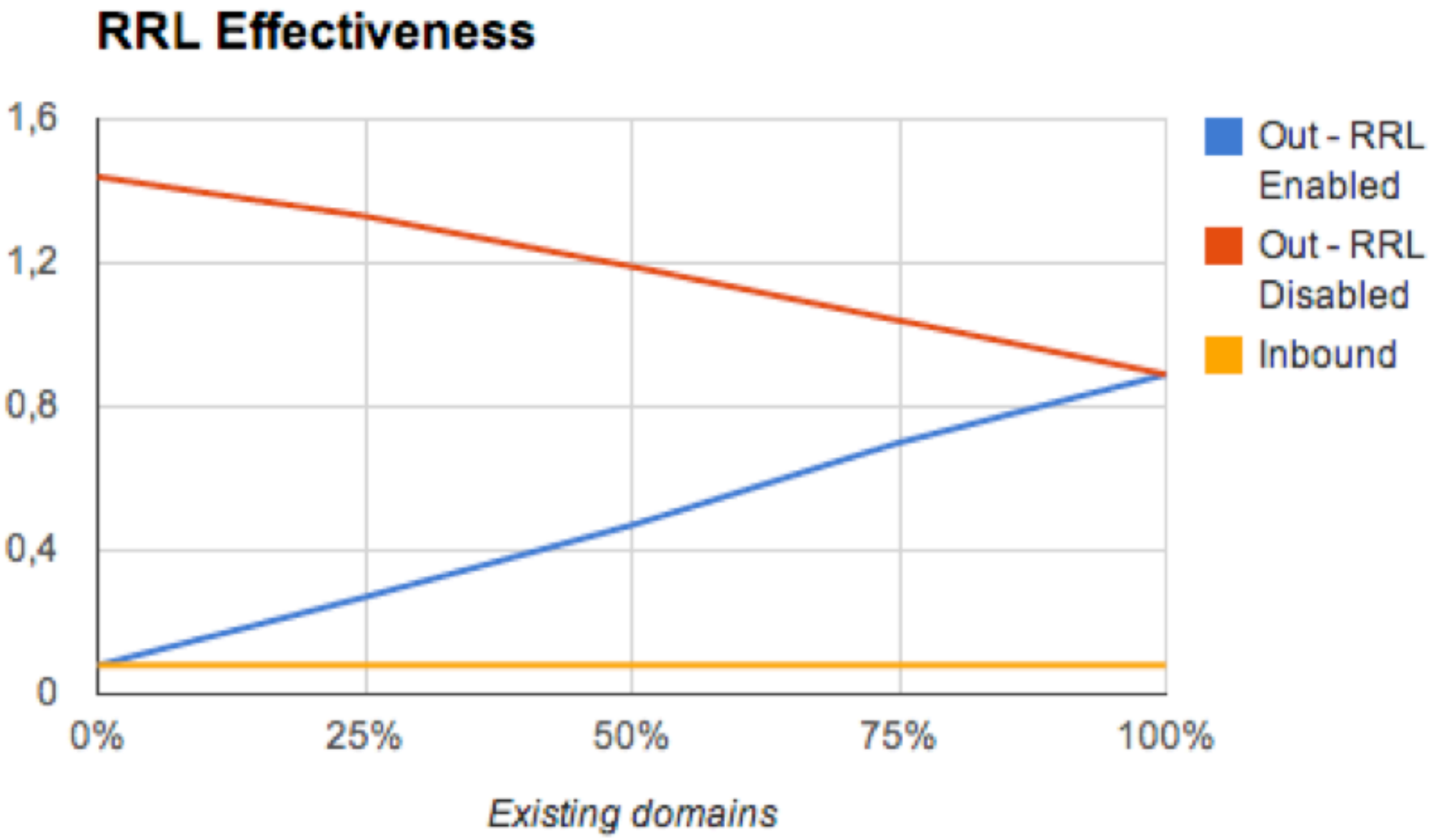


RRL Measurements

SLIP	In	Out	Amp. Ratio	False positives*	TCP responses
1	80 KB/s	81 KB/s	≈1:1	0%	100 %
2	79 KB/s	39 KB/s	≈1:0.5	50%	87.5 %
3	79 KB/s	26 KB/s	≈1:0.3	66.6%	66 %
5	80 KB/s	16 KB/s	≈1:0.2	80%	49 %
10	80 KB/s	8 KB/s	≈1:0.1	90%	27 %

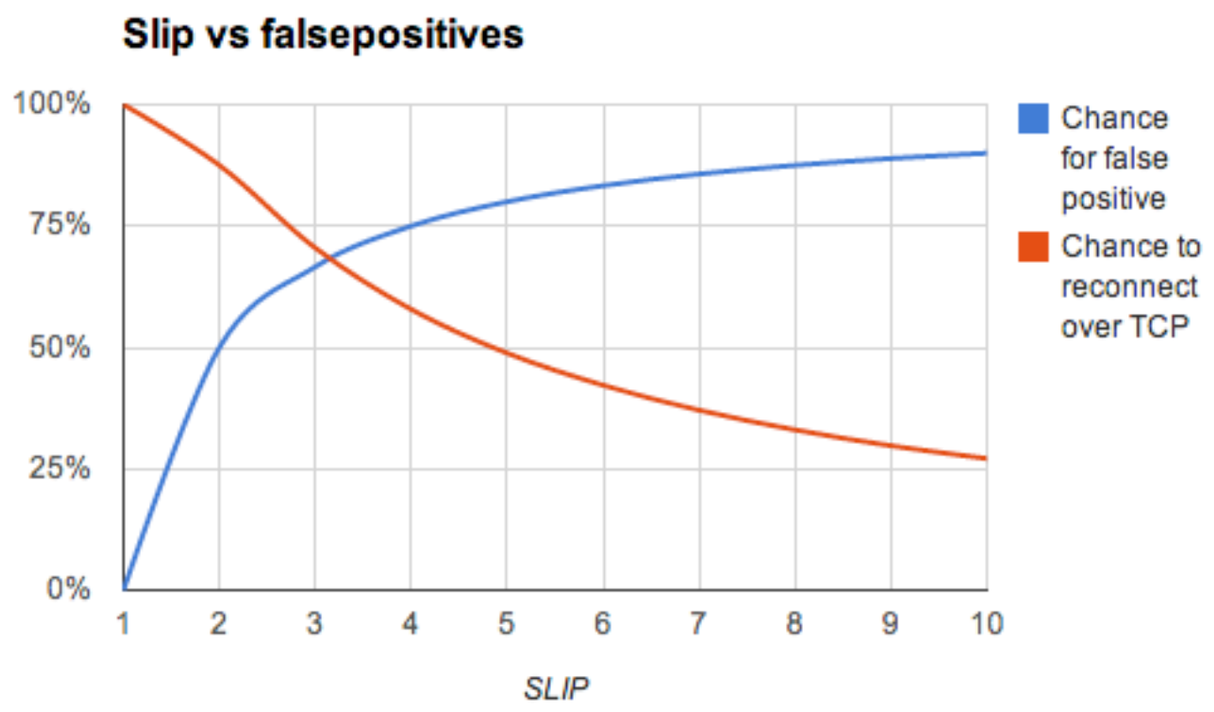
* Possible fps, assuming 3 tries

RRL Measurements



RRL Measurements

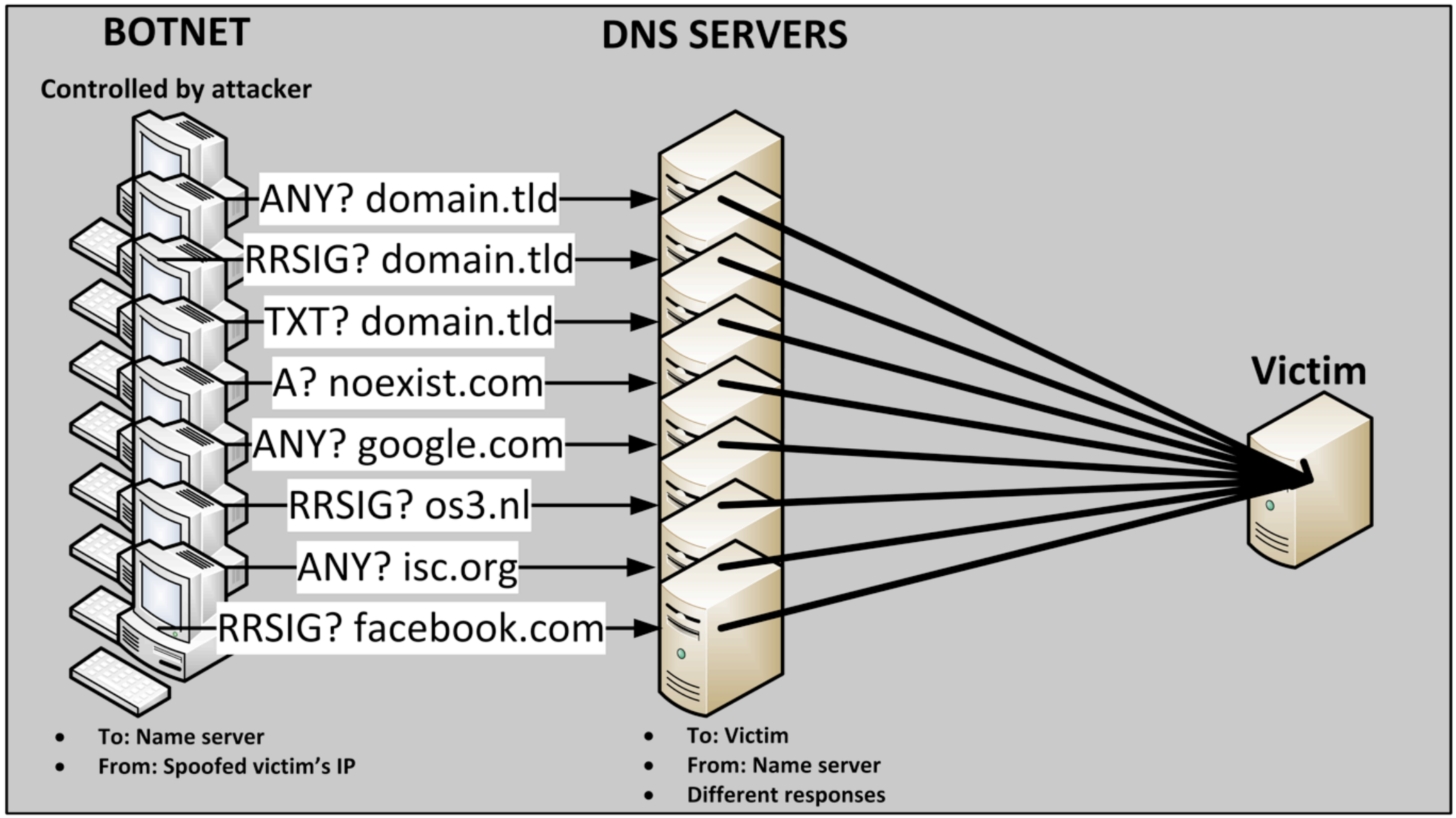
- Slip
  - Trade off between #false positives and# TCP sessions
- Default 2



Whac-A-Mole

NLnet Labs

Getting sophisticated



Other Protocols

- Most UDP have similar attributes
  - NTP
  - SNMP
    - 100 Gb/s
- DNS is the low hanging fruit of the day

Breaking News RLL is broken?

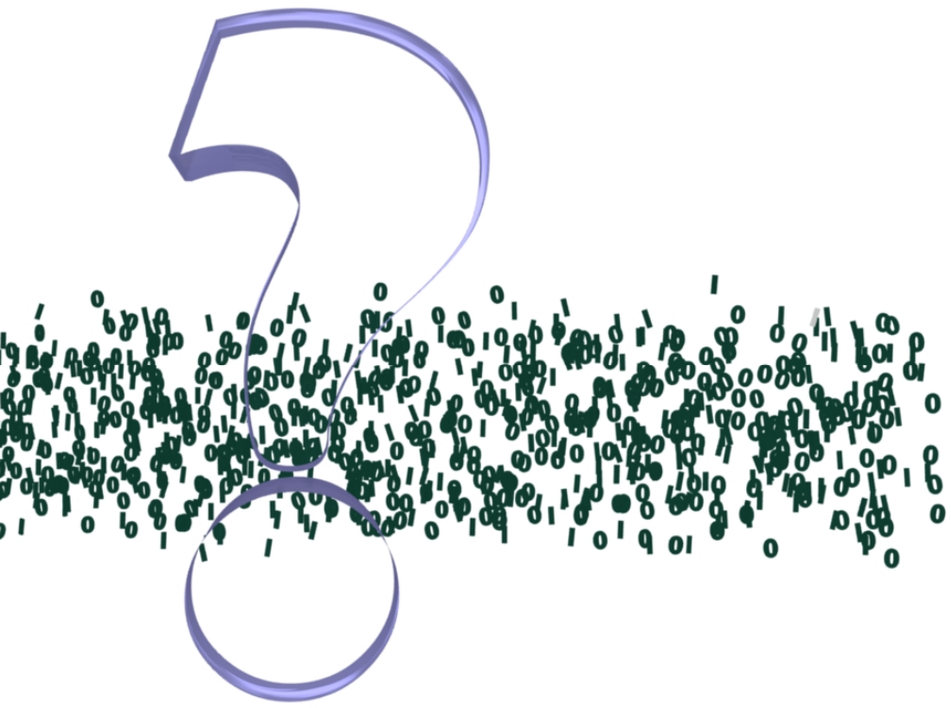
- CERTA-2013-AVI-506
  - Aids Kaminsky style attacks
  - http://www.certa.ssi.gouv.fr/site/CERTA-2013-AVI-506/index.html
  - https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2013-0597+1.00+Rate+limiting+van+DNS+responses+veroorzaakt+kwetsbaarheid.html

Prevent Spoofing

- Implement source validation
  - Don't let fake packets leave your network
- SAC 004, 008, BCP 38, 84 and more
  - For the good of the internet
  - For the good your reputation

Further reading

- DNS Firewall rules: http://www.bortzmeyer.org/files/generate-netfilter-u32-dns-rule.py
- Dampening: http://lutz.donnerhacke.de/eng/Blog/DNS-Dampening
- Rate limiting
  - Proposal by Paul Vixie and Vernon Schryver: http://www.redbarn.org/dns/ratelimits
    - NSD Rate limiting: https://www.nlnetlabs.nl/blog/2012/10/11/nsd-ratelimit/
    - Knot Rate limiting: https://www.knot-dns.cz
- DNS Rate Limiting, A Hard Lesson: http://conference.apnic.net/__data/assets/pdf_file/0011/58880/130226.apops-dns-rate-limit_1361839670.pdf
- RLL Measurements: http://www.nlnetlabs.nl/downloads/publications/report-rrl-dekoning-rozekrans.pdf
- Website: http://www.bcp38.info/



Questions

(If you like our work, please consider sponsoring us)

NLnet Labs

NLnet Labs