How do we address the problem of IP spoofing?
And is it a problem worth solving?

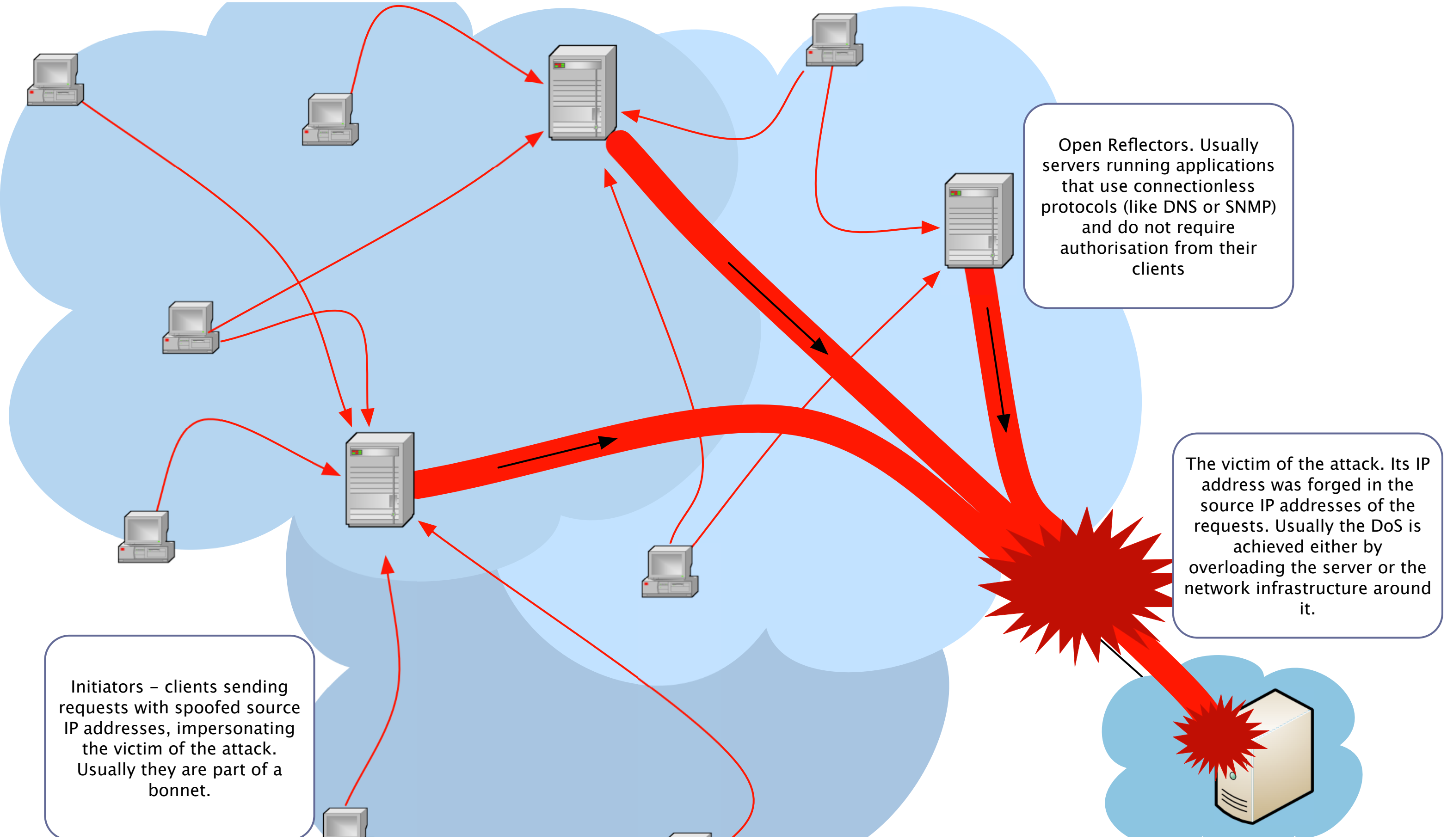
Benno Overeinder <benno@NLnetLabs.nl>

Andrei Robachevsky <robachevsky@isoc.org>

Outline/Agenda

- What is the problem (in a bigger sense)?
- State of Play
- Areas of impact
- Critical elements
- Way forward (discussion)
    - Are we solving the problem?
    - Are we solving it in a right way?
    - Are we solving the right problem?

Anatomy of a reflection attack

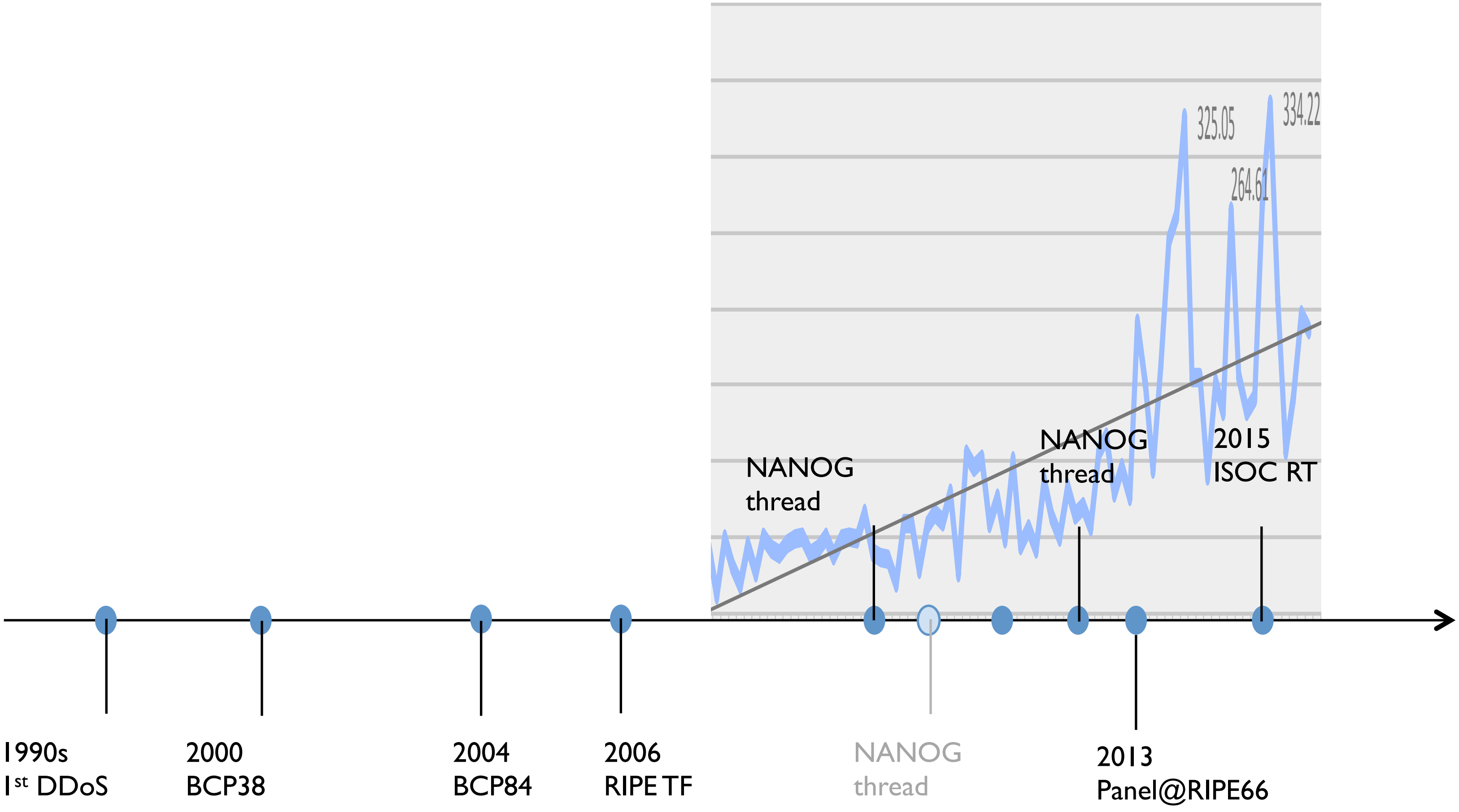


Open Reflectors. Usually servers running applications that use connectionless protocols (like DNS or SNMP) and do not require authorisation from their clients

The victim of the attack. Its IP address was forged in the source IP addresses of the requests. Usually the DoS is achieved either by overloading the server or the network infrastructure around it.

Initiators – clients sending requests with spoofed source IP addresses, impersonating the victim of the attack. Usually they are part of a bonnet.

A brief history of anti-spoofing



1990s
1st DDoS

2000
BCP38

2004
BCP84

2006
RIPE TF

NANOG
thread

NANOG
thread

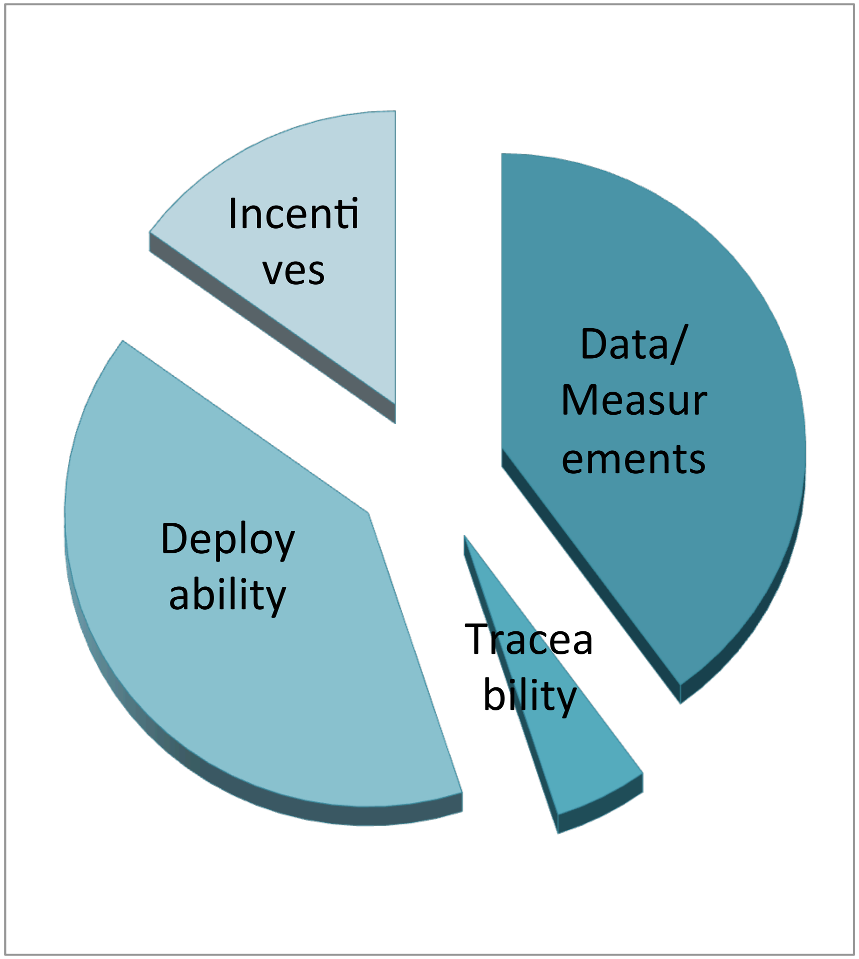
NANOG
thread

2013
Panel@RIPE66

2015
ISOC RT

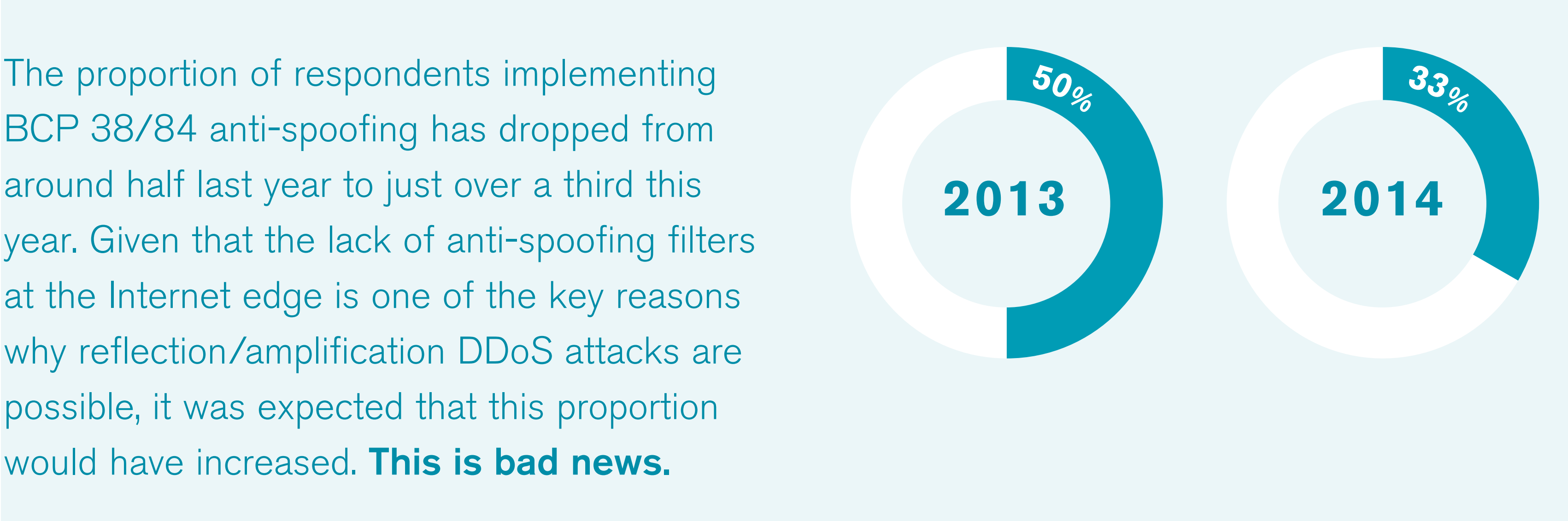
Data: ATLAS Q2 2015 Update

Areas of impact



Measurements

- Measurement techniques
- What do we measure?
- Can we do this better (discussion)?



The proportion of respondents implementing BCP 38/84 anti-spoofing has dropped from around half last year to just over a third this year. Given that the lack of anti-spoofing filters at the Internet edge is one of the key reasons why reflection/amplification DDoS attacks are possible, it was expected that this proportion would have increased. **This is bad news.**

Traceability

- Important, but unfeasible

Deployability

- Device capability
- Anti-spoofing by default
- Tailored operational guidance

Incentives

- Mobile networks
- Broadband access
- Enterprises
- Datacenters and hosting providers

Way forward (discussion)

- Are we solving the right problem?
  - Back to the anatomy of the attack
- Are we solving the problem?
  - How do we know?
- Are we solving it in a right way?
  - How can we maximize impact and scale up?