Anti-Spoofing and your network: BCP38, SAVI, and what to look for

Mike Hughes, Ethernorth Consultancy

IX Leeds 3 Open Meeting - June 2013

March 2013: Spamhaus attacked


CLOUDFLARE

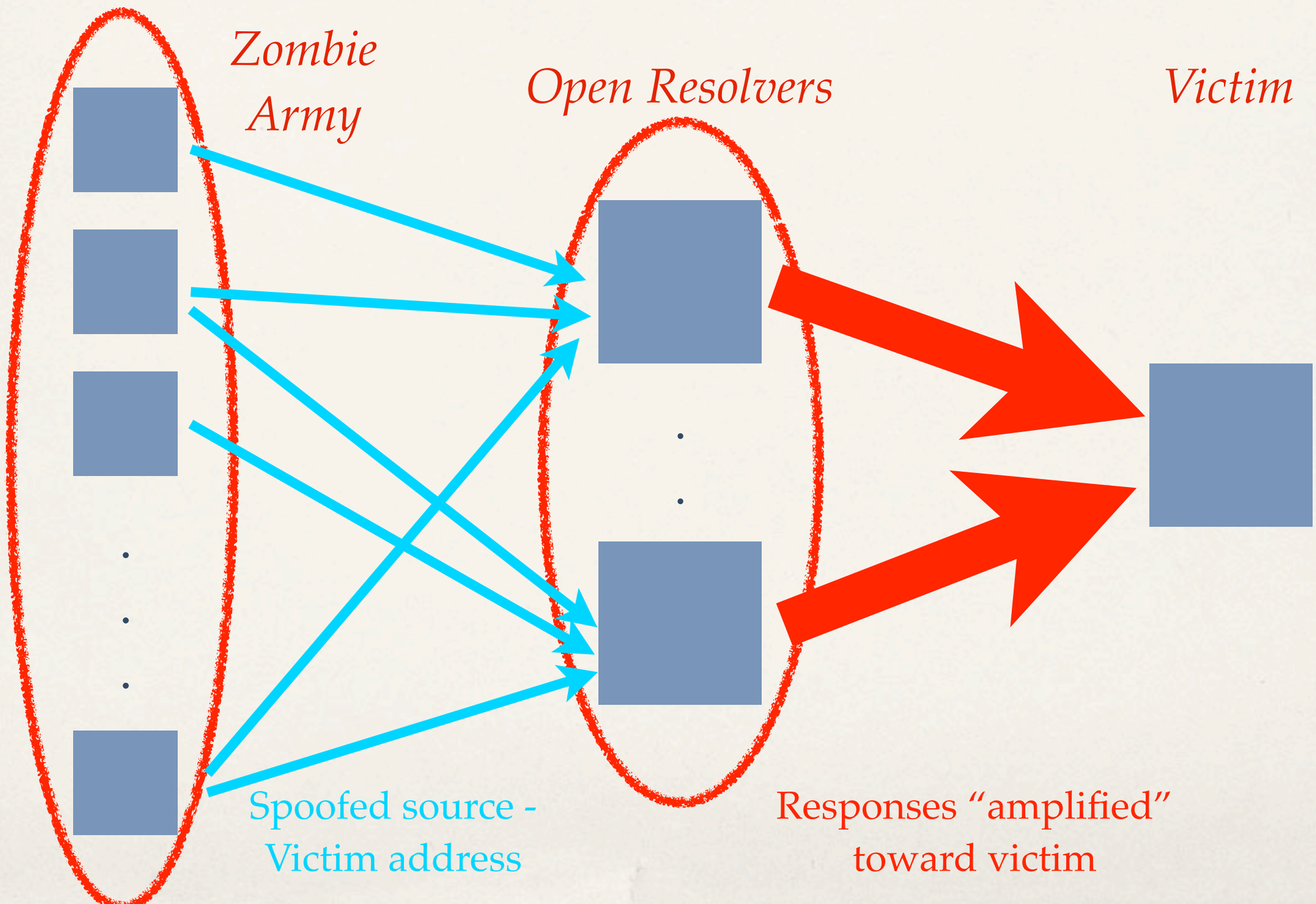
Blog home

The DDoS That Almost Broke the Internet

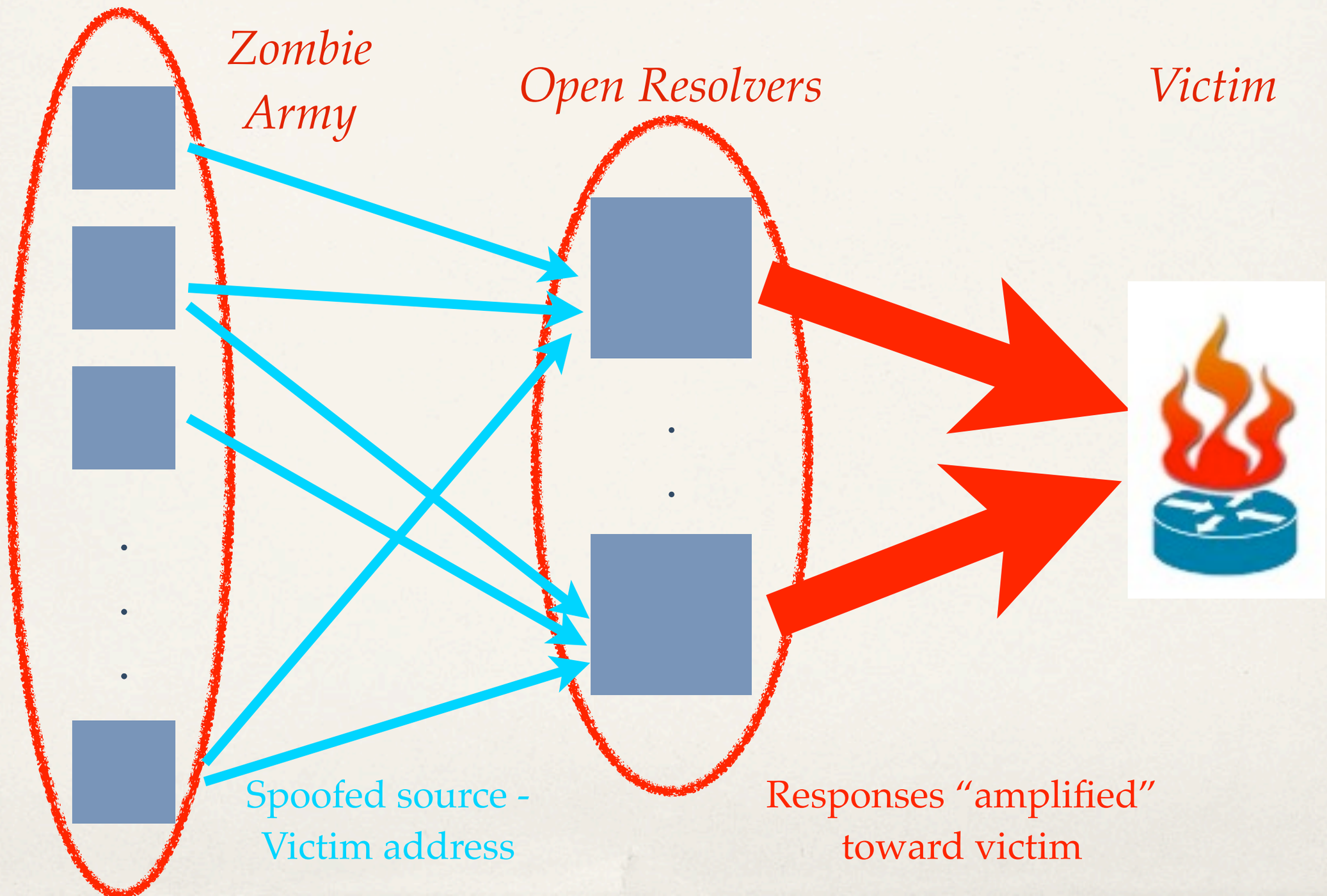
Published on March 27, 2013 04:35PM by Matthew Prince.

- Dubbed by some as “biggest attack seen so far” - but debatable
- Basically a huge “backscatter” attack - reported >300Gb/sec

Anatomy of a Backscatter Attack

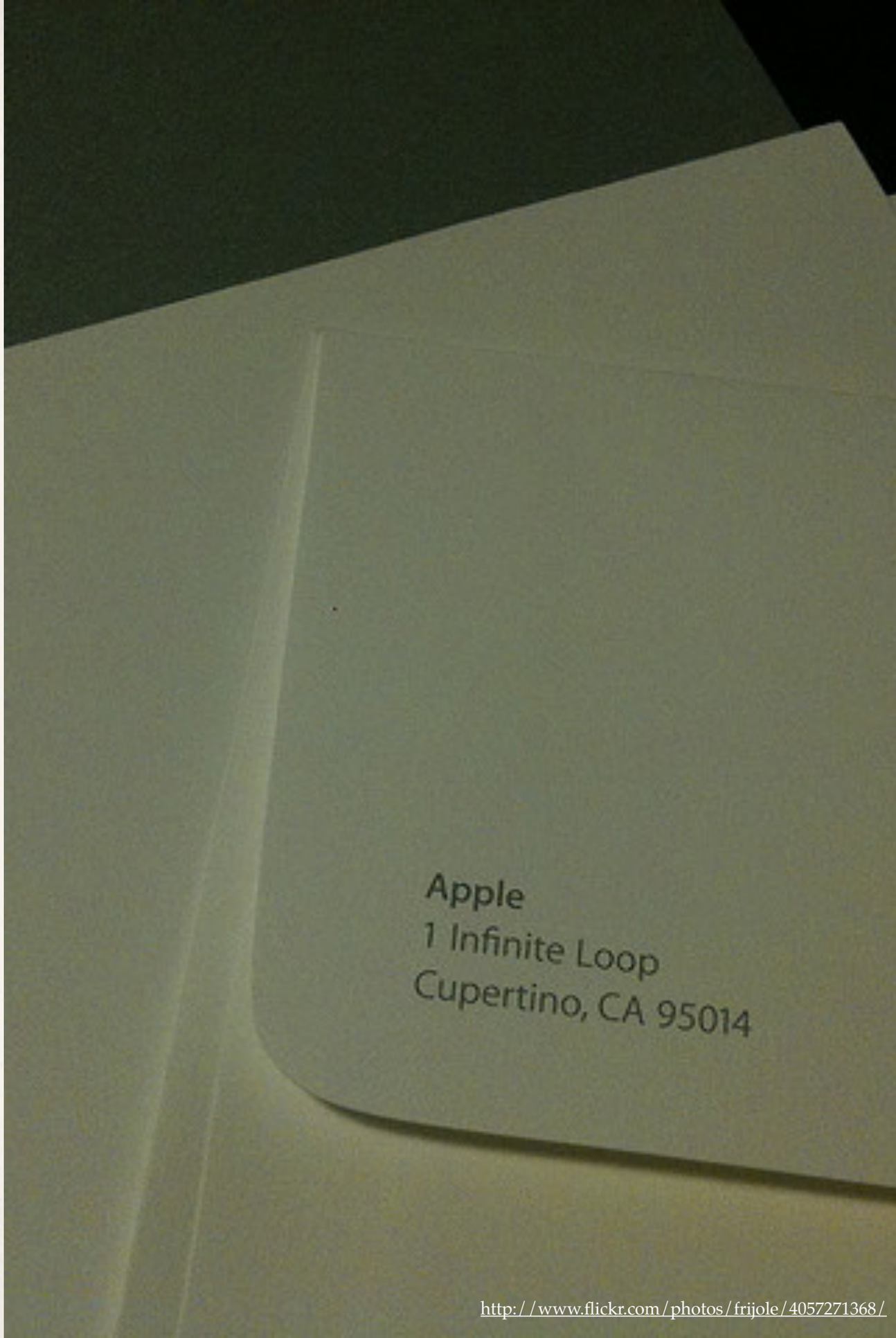


Anatomy of a Backscatter Attack



Spoofed Source Address

Easy as writing it on the back of an envelope if you know how (or with the right malware)...



http://www.flickr.com/photos/frijole/4057271368/

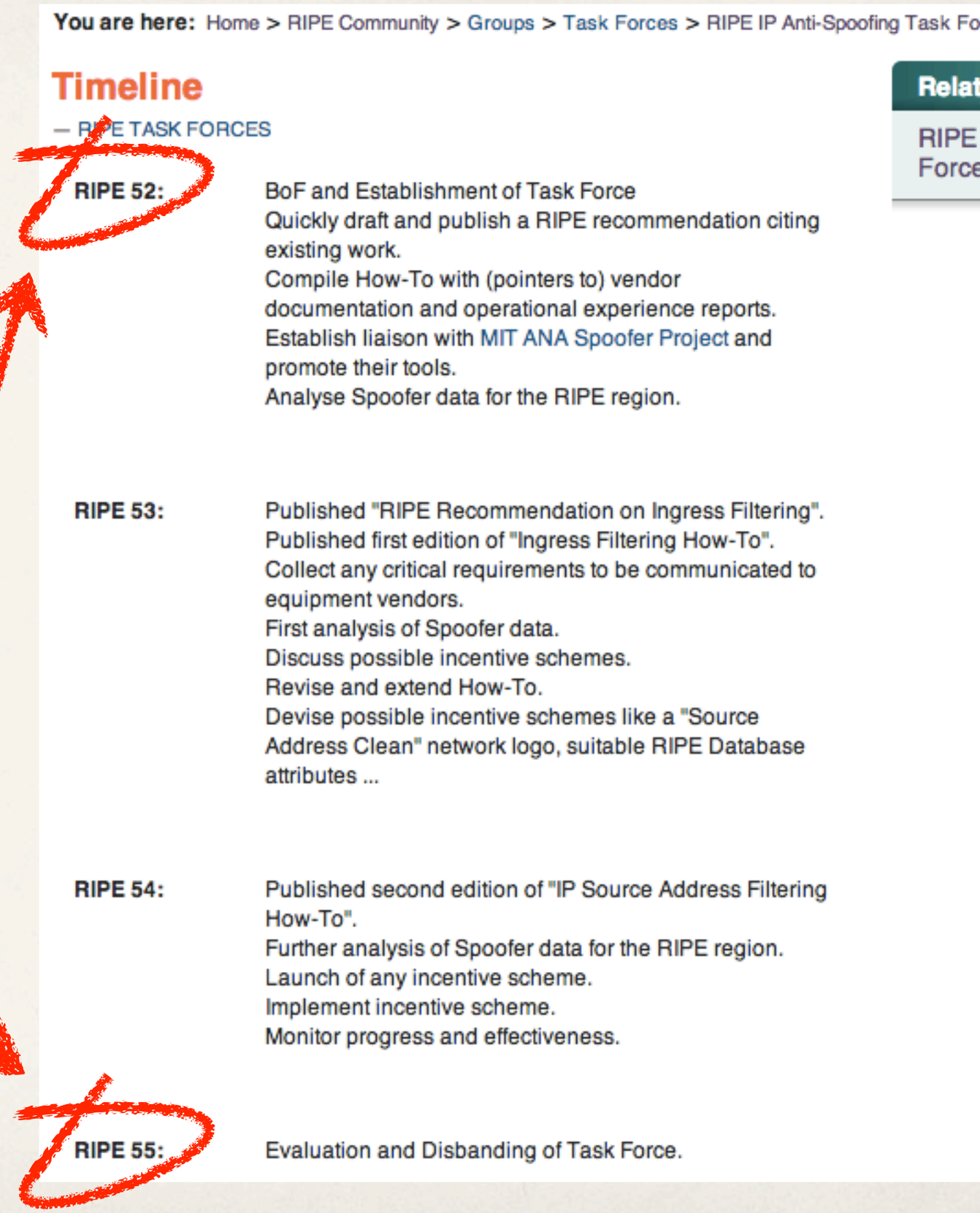
Anti-Spoofing Measures: BCP38

- Search “IETF BCP38” for the document
- Describes current “best practice”
- Even if seems that it’s not widely followed?

http://www.flickr.com/photos/8212496@N06/2380082505

Does anybody care?

- Industry tries on occasion to raise awareness
- RIPE Task-Force started in 2006 to raise awareness
- Disbanded late 2007
- 5 years on, still banging on about this... really?



You are here: Home > RIPE Community > Groups > Task Forces > RIPE IP Anti-Spoofing Task Fo

Timeline

— RIPE TASK FORCES

RIPE 52: BoF and Establishment of Task Force
Quickly draft and publish a RIPE recommendation citing existing work.
Compile How-To with (pointers to) vendor documentation and operational experience reports.
Establish liaison with MIT ANA Spoofer Project and promote their tools.
Analyse Spoofer data for the RIPE region.

RIPE 53: Published "RIPE Recommendation on Ingress Filtering".
Published first edition of "Ingress Filtering How-To".
Collect any critical requirements to be communicated to equipment vendors.
First analysis of Spoofer data.
Discuss possible incentive schemes.
Revise and extend How-To.
Devise possible incentive schemes like a "Source Address Clean" network logo, suitable RIPE Database attributes ...

RIPE 54: Published second edition of "IP Source Address Filtering How-To".
Further analysis of Spoofer data for the RIPE region.
Launch of any incentive scheme.
Implement incentive scheme.
Monitor progress and effectiveness.

RIPE 55: Evaluation and Disbanding of Task Force.

Why should you care?

- What's it got to do with me?
- Running a clean network
- Doing the "right thing"
- You pay for your bandwidth, right?
- Costs of response and cleanup

http://www.flickr.com/photos/auntiep/3083645776/

Applying Anti-Spoofing

- Easier toward the edge
- More complex toward the core
- Common approaches are...
  - Access list based filtering
  - uRPF - Unicast Reverse Path Forwarding

Why isn't it deployed?

- Management of config
- Cost & time considerations?
- Because "no-one is demanding it"
- Perception that it's "difficult"

IETF “SAVI” effort

- Search for “IETF SAVI” for more info & working group
- Currently an informational RFC (6959) as a “problem statement”
- To make anti-spoofing and source address validation more applicable
- Thought is that you sanity check at the “downstream” edges
- Tie anti-spoofing to what is already known about topology

What should you do?

- BCP38 filter own single-homed downstream customers, hosting networks, etc.
- Filter your own estate
- Ask your suppliers to use anti-spoofing measures if they don't already

http://www.flickr.com/photos/thinkofacolour/5248664776/

Ta-Dah!

Questions? Comments? Brickbats?

Mike@ethernorth.net