Seven Years of Anti-Spoofing

Introduction to RIPE 66 panel on anti-spoofing

Moderators: Andrei Robachevsky (ISOC)
Benno Overeinder (NLnet Labs)

Brief Historic Perspective

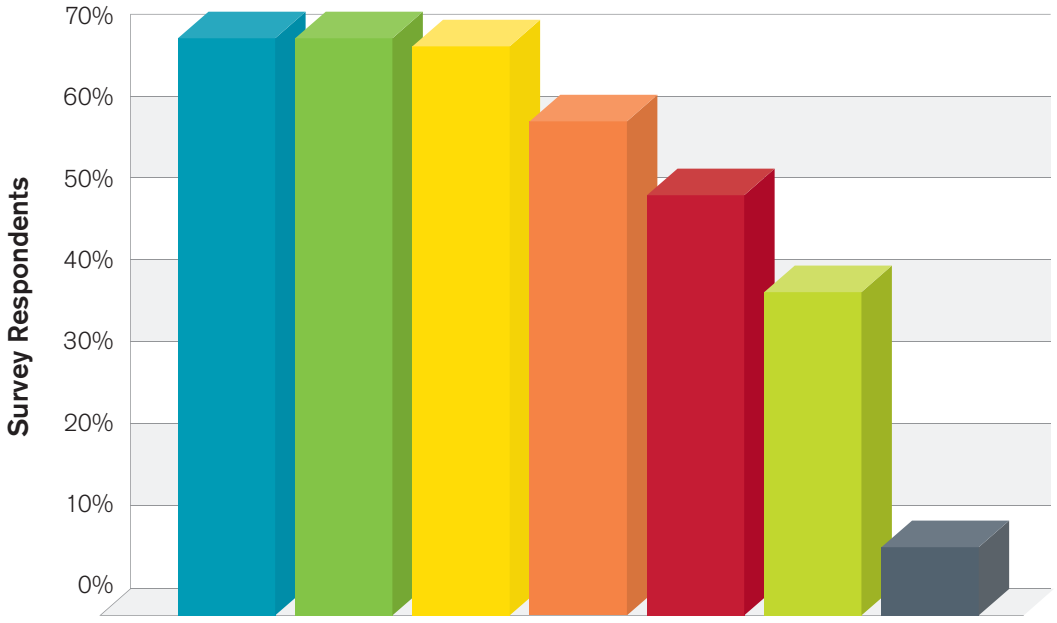
- In 2006–2008 RIPE Anti-Spoofing Task Force
  - RIPE 431, RIPE Anti-Spoofing Task Force HOW-TO
  - RIPE 432, Network Hygiene Pays Off – The Business Case for IP Source Address Verification
- In 2012–2013 fresh examples of long-term trend
  - large DDoS attacks (ab)using authoritative name server and spoofed packets

Why This Panel?

- Spoofed traffic is still a problem
  - Spamhaus attack of order 300 Gb/s
- Has the landscape changed?
  - attack vectors in 2006 and in 2013
  - severity
  - availability of solution
- What concrete actions we—as individual networks and as the community—can undertake?

DDoS Statistic

- Arbor Networks Worldwide Infrastructure Security Report
  - DDoS mentioned on 61 of 96 pages

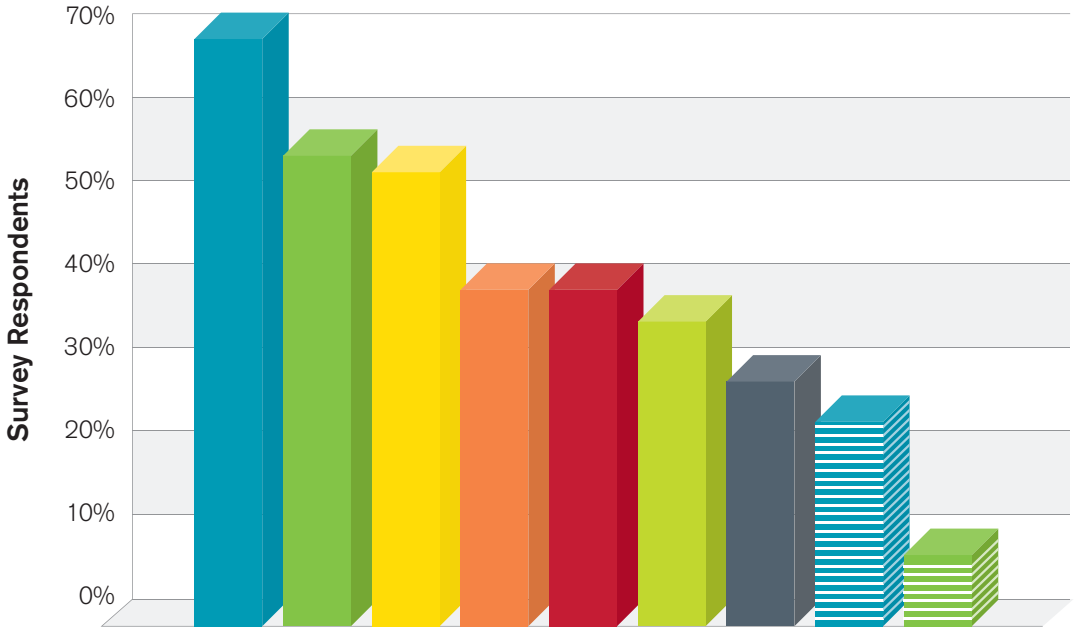


- **67%** Authentication for BGP, IGPs (MD5, SHA-1)
- **67%** iACLs at Network Edges
- **66%** Separate Out-of-Band (OOB) Management Network, Also Known As a Data Communication Network (DCN)
- **57%** BCP38/BCP84 Anti-Spoofing at Network Edges
- **48%** IRR Route Registration of Customer Prefixes
- **36%** Generalized TTL Security Mechanism (GTSM) for eBGP Peers
- **5%** Other

Network infrastructure security practices
Source: Arbor Networks

DDoS Statistic

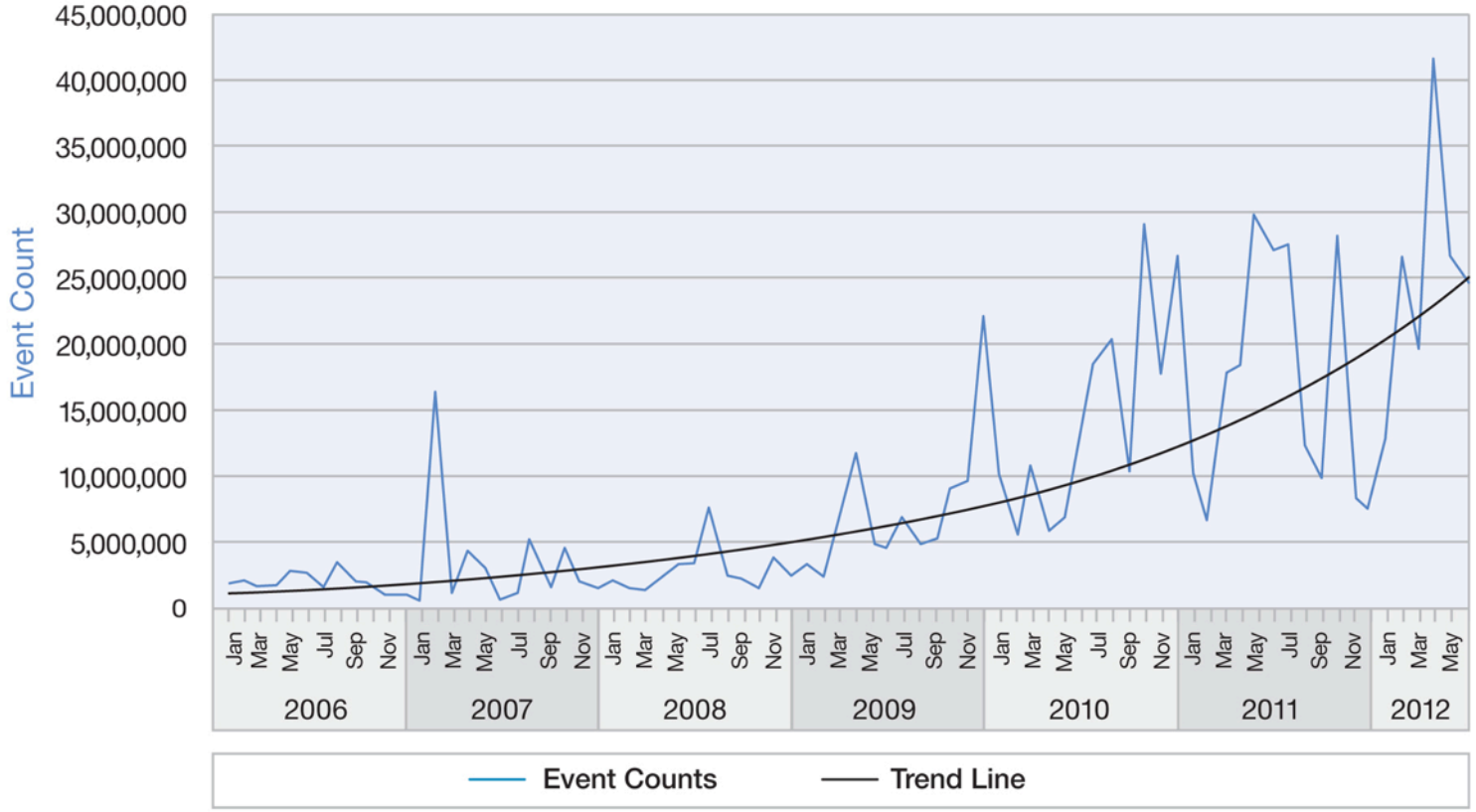
- Arbor Networks Worldwide Infrastructure Security Report
  - DDoS mentioned on 61 of 96 pages



- **67%** Interface ACLs (iACLs) on Network Edge
- **53%** Intelligent DDoS Mitigation Systems (IDMS) Such As Peakflow SP Threat Management System (TMS)
- **51%** Firewalls
- **37%** Source-Based Remote Triggered Blackhole (S/RTBH)
- **37%** Unicast Reverse-Path Forwarding (uRPF) and/or Other Anti-Spoofing Mechanisms
- **33%** Separate Production and Out-of-Band (OOB) Management Networks
- **26%** Destination-Based Remote Triggered Blackhole (D/RTBH)
- **21%** IPS/IDS
- **5%** FlowSpec on Gateway or Access Routers

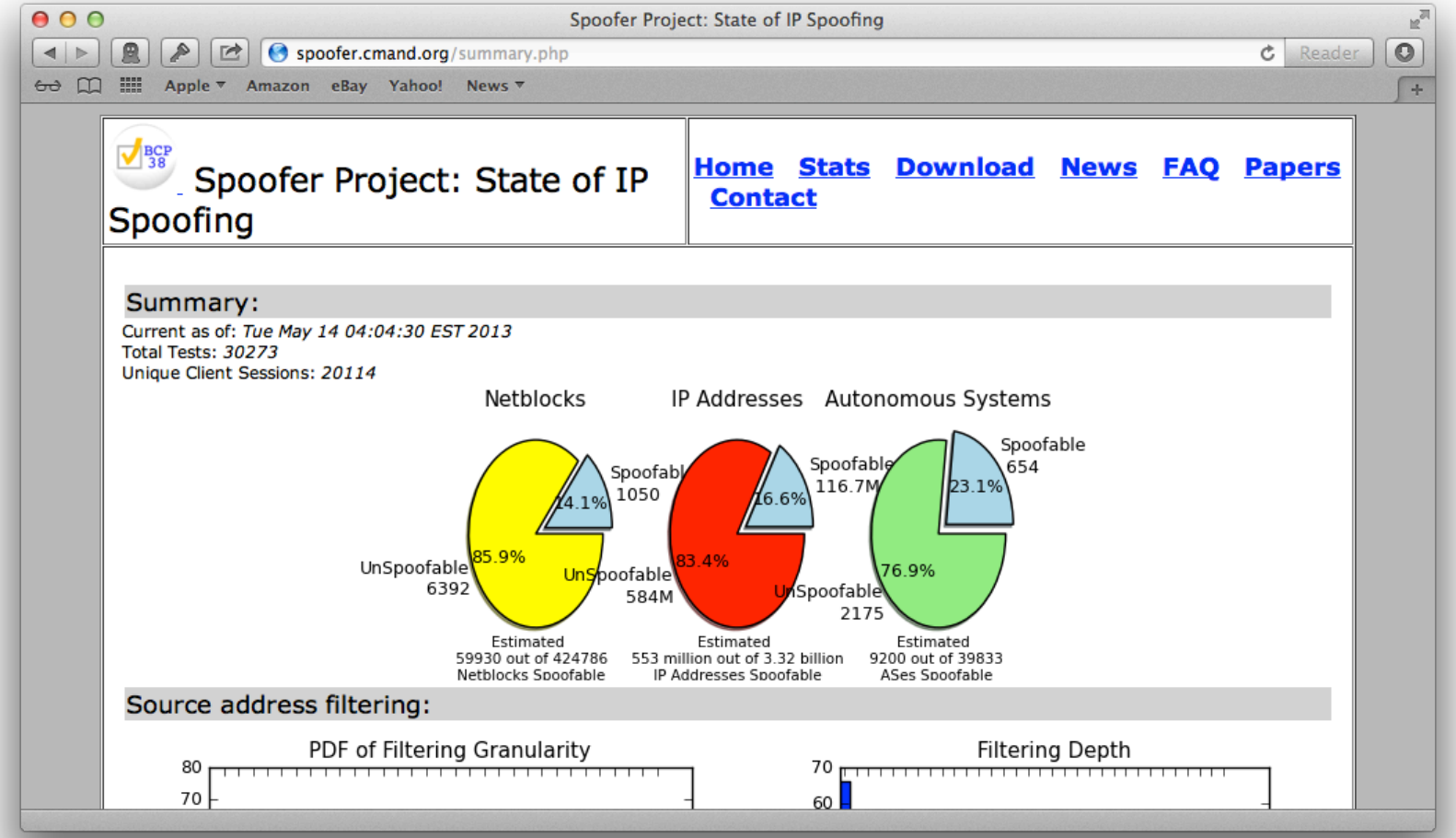
DNS security measures
Source: Arbor Networks

DDoS Statics (cont'd)



Backscatter trend as side effect of spoofed DDoS attacks. Data from a darknet with aperture of 25,600 addresses. Source: IBM X-Force R&D.

Spoofer Project



Panellists

- Merike Kaeo (IID)
- David Freedman (Claranet)
- Eric Osterweil (Verisign)
- Hessel Schut (NL High Tech Crime Unit)
- Marek Moskal (Cisco)
- Nick Hilliard (INEX)

Key Message of Co-chair RIPE Anti-Spoofing Task Force

- Daniel Karrenberg
  - Let's not be naive and not just repeat the earlier effort that was not all that successful. It is important to convince operators, especially eyeball networks, that it is in their business interest to address this problem before someone addresses it by regulation.