# Exit from Hell? – Reducing the Impact of Amplification DDoS Attacks

Marc Kührer[1]
Thomas Hupperich[1]
**Christian Rossow[2]**
Thorsten Holz[1]

[1] Ruhr-University Bochum
[2] Saarland University

USENIX Security, August 2014

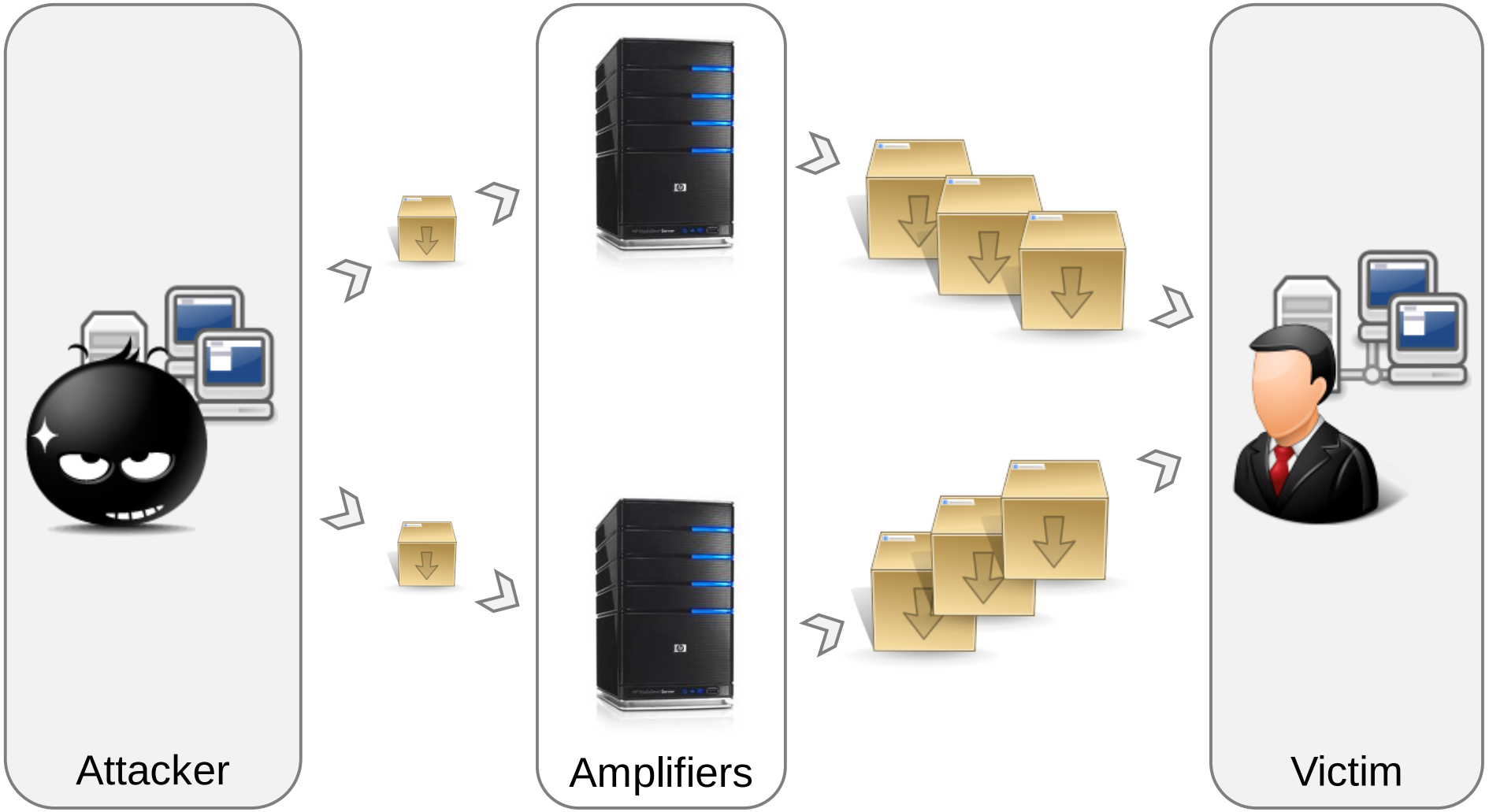
# Technical Details Behind a 400Gbps NTP Amplification DDoS Attack

*Published on February 13, 2014 01:00AM by Matthew Prince.*




On Monday we mitigated a large DDoS that targeted one of our customers. The attack peaked just shy of 400Gbps. We've seen a handful of other attacks at this scale, but this is the largest attack we've seen that uses NTP amplification. This style of attacks has grown dramatically over the last six months and poses a significant new threat to the web.

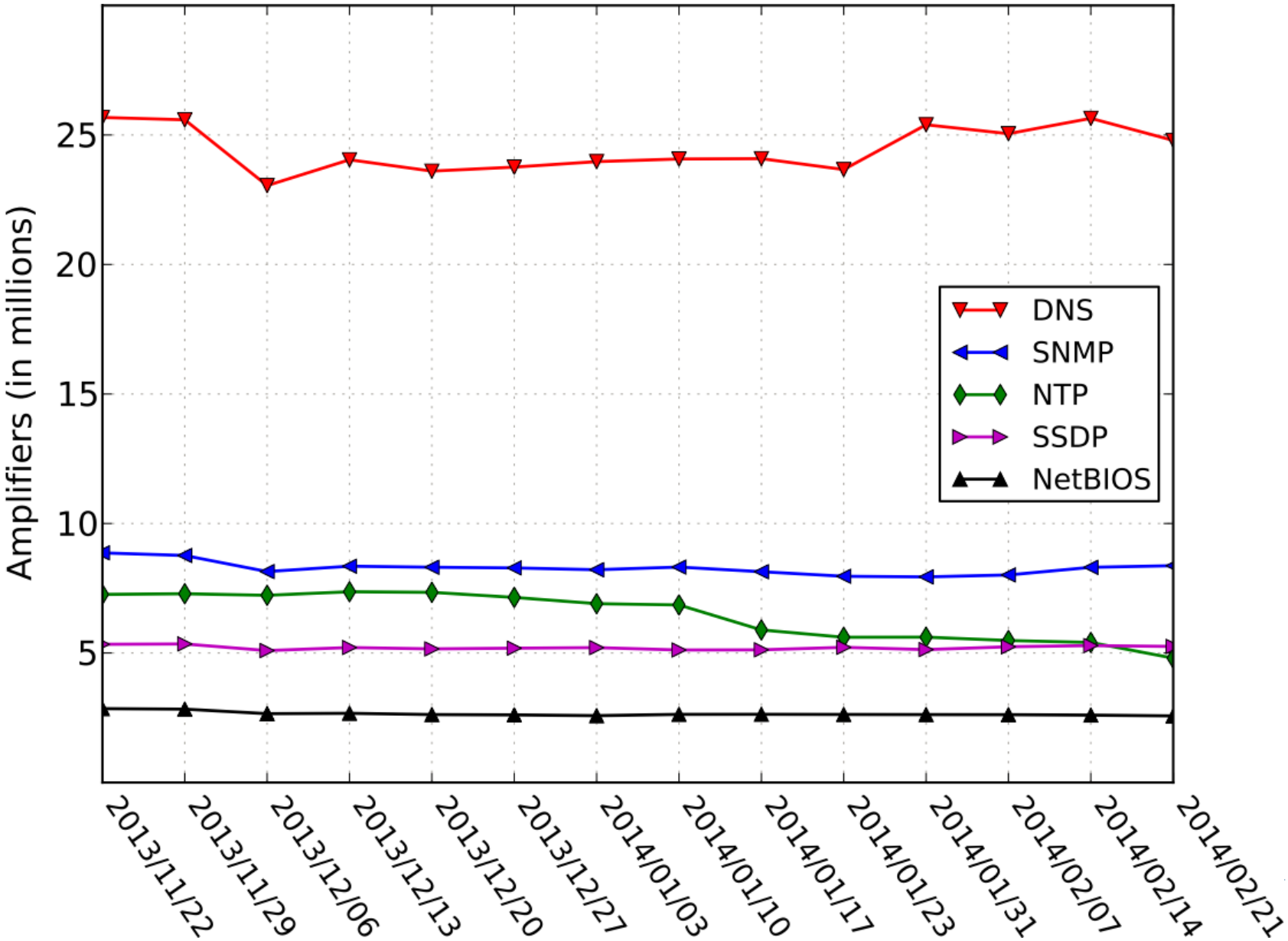
# Amplification DDoS Attacks



# Contents

- **Can we mitigate the UDP-based amplifications?**
- Are there other amplifiers than UDP?
- Can we identify spoofing-enabled networks?

# Number of Amplifiers per Protocol



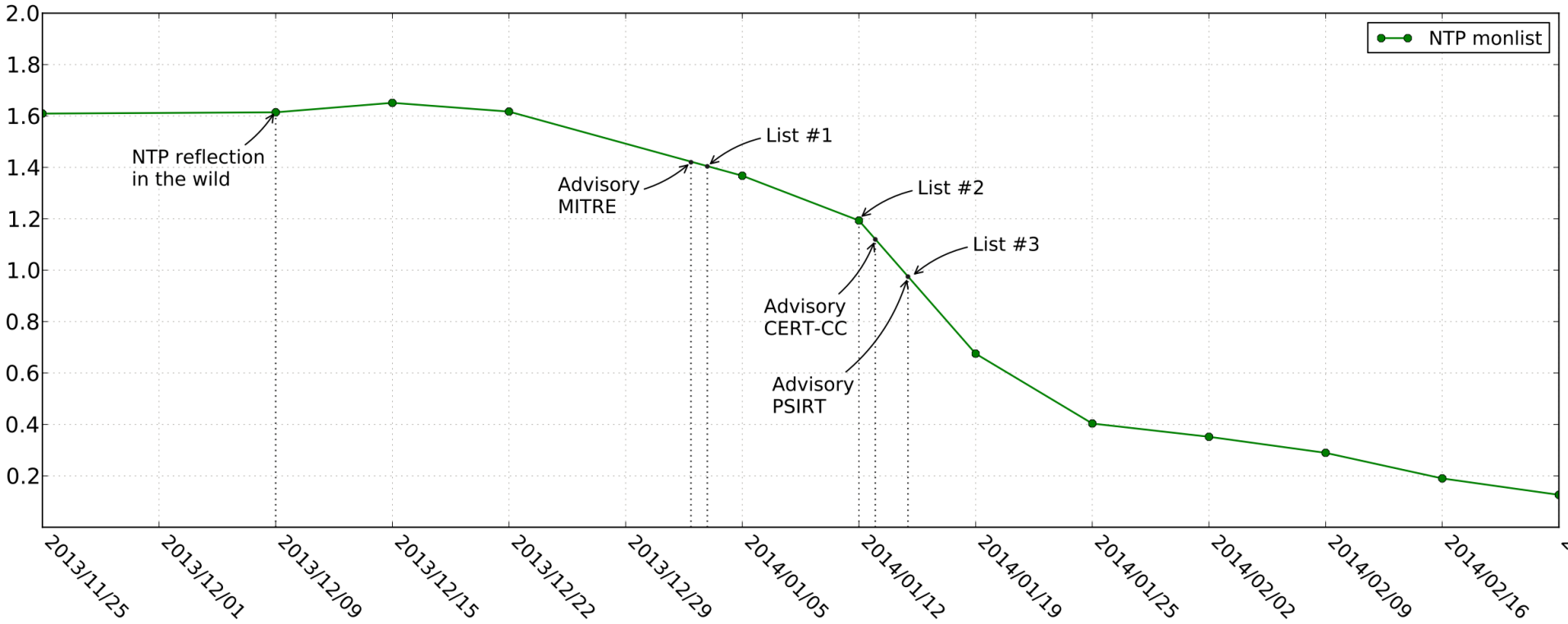
# Amplifier Classification

| | Operating System (in %) | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Protocol | *Unix* | *Linux* | *Ubuntu* | *FreeBSD* | *Windows* | *ZyNOS* | *Cisco IOS* | *Junos* | *NetOS* | *Others* | *Unknown* |
| *DNS* | 3.6 | 3.4 | 0.0 | 0.0 | 0.8 | 7.5 | 0.1 | 0.0 | 0.0 | 1.1 | 83.5 |
| *NetBIOS* | 0.4 | 0.1 | 0.0 | 0.0 | 87.3 | 0.3 | 0.0 | 0.0 | 0.0 | 0.7 | 11.2 |
| *NTP* | 18.2 | 26.8 | 0.0 | 4.7 | 0.2 | 0.0 | 40.8 | 2.9 | 0.0 | 1.7 | 4.7 |
| *SNMP* | 1.5 | 11.4 | 0.1 | 0.1 | 0.8 | 17.8 | 2.2 | 0.0 | 0.0 | 8.7 | 57.4 |
| *SSDP* | 1.8 | 36.0 | 5.5 | 0.0 | 1.3 | 0.7 | 0.0 | 0.0 | 19.3 | 1.8 | 33.6 |

# NTP Amplification Case Study

- NTP: Network Time Protocol
  - Optional `monlist` debug feature
  - 8B request and 44kB response → >1000x amplification
  - In Dec ‘13: **1.6 million amplifiers**
- Timeline of vulnerability discovery
  - Aug ‘13: Notified vendors, reserved CVE
  - Jan ‘14: Released CVE + coop with CERTs/ISPs
  - Feb ‘14: Presented vulnerabilities at NDSS

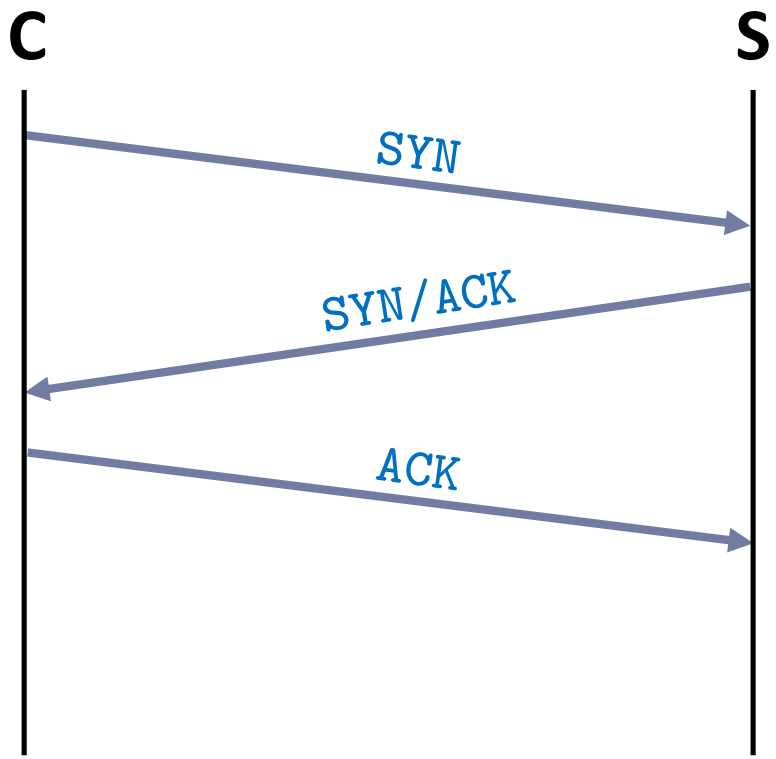
# Number of NTP `monlist` Amplifiers



# Contents

- Can we mitigate the UDP-based amplifications?
- **Are there other amplifiers than UDP?**
- Can we identify spoofing-enabled networks?

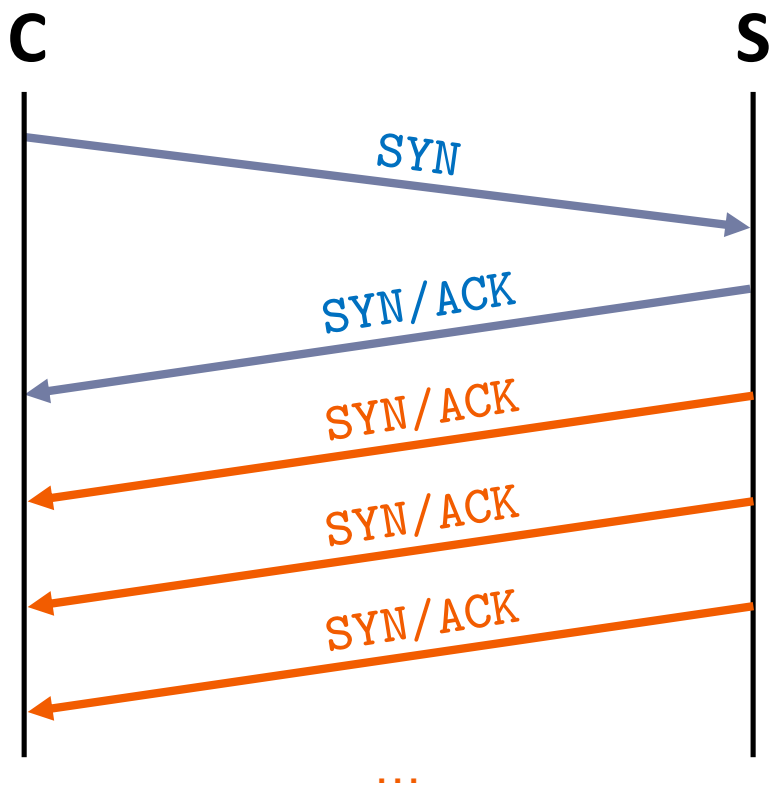
# TCP and Reflection




**TCP 3-Way Handshake**

- Reflection
- No amplification

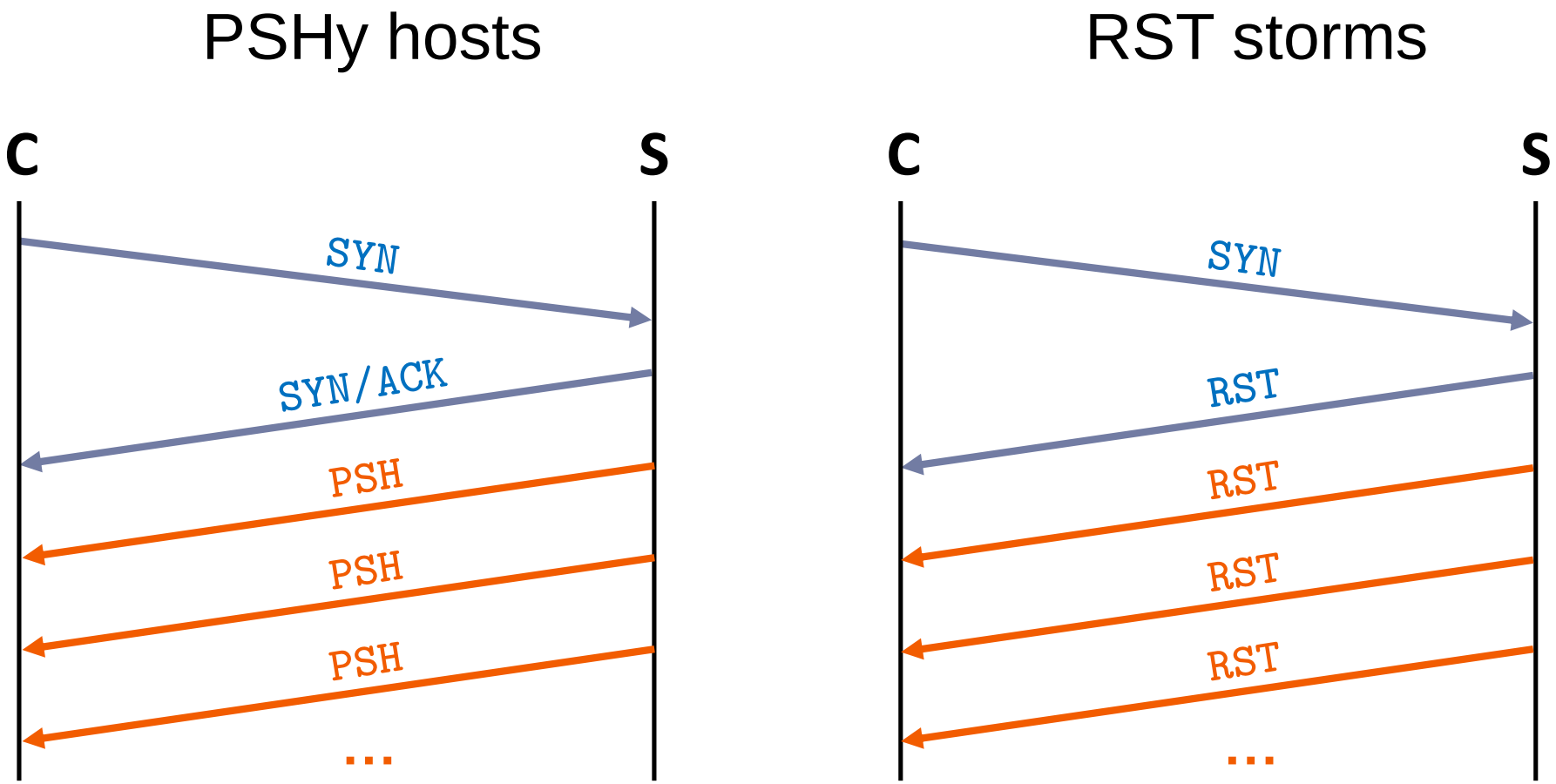
# TCP and Reflection




**SYN/ACK Amplifiers**

- Keep repeating `SYN/ACK` until `ACK`
- Default, e.g., in *nix
- Reason: packet loss

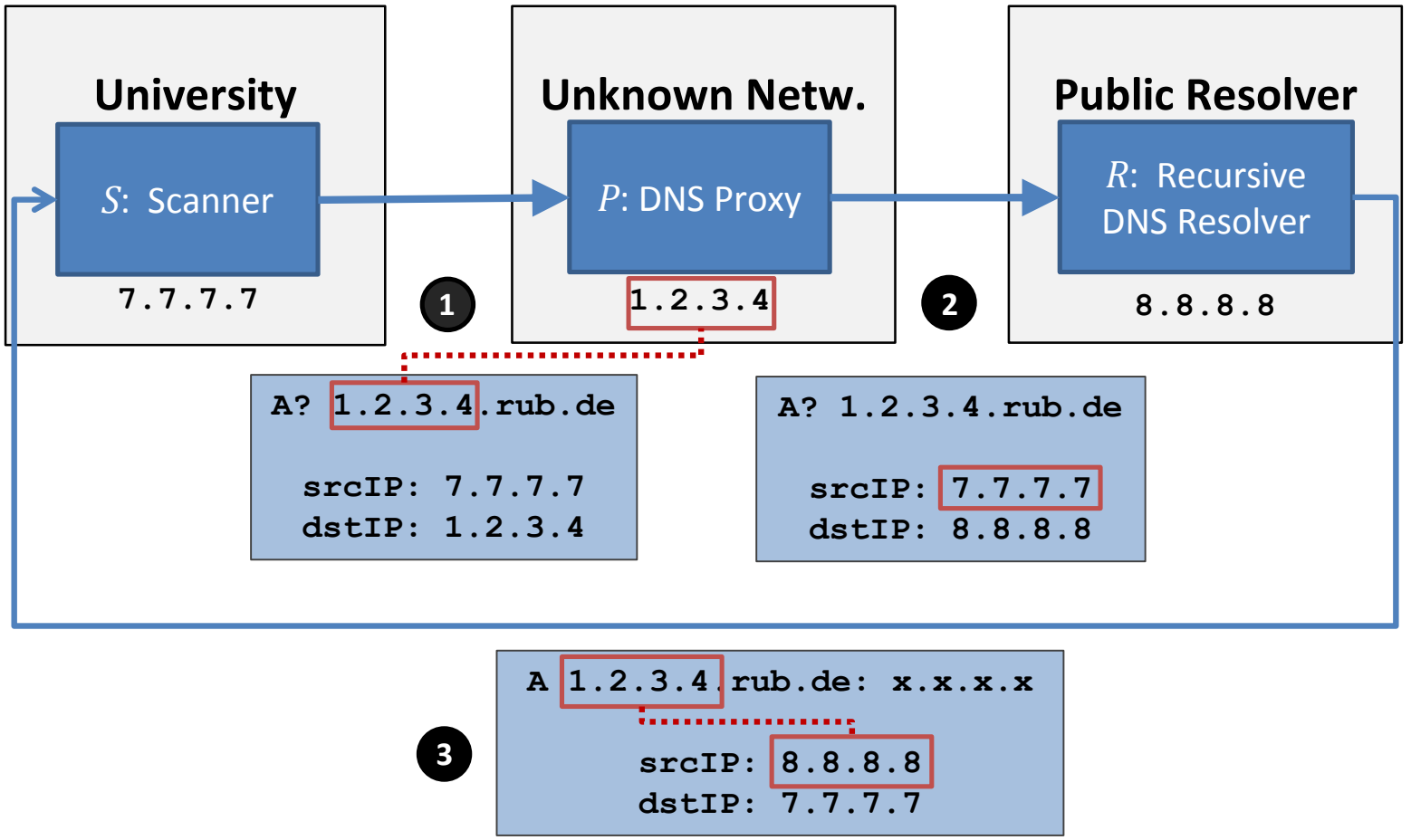
# TCP and Reflection (also see WOOT ‘14 paper)



# Contents

- Can we mitigate the UDP-based amplifications?
- Are there other amplifiers than UDP?
- **Can we identify spoofing-enabled networks?**

# Remote Spoofer Test via DNS



# Remote Spoofer Test Results

| Filter | $\#P$ | $\#AS_P$ |
|---|---|---|
| Top 4 Resolver | 42,691 | 301 |
| Top 10 Resolver | 45,072 | 352 |
| Distinct AS | 170,451 | 2,692 |

# Conclusion

- **Mitigation of NTP amplifiers** (largely) successful
- **TCP amplification** may cause issues in the future
- Remote test finds **at least 300 spoofing ASes**

# Exit from Hell? – Reducing the Impact of Amplification DDoS Attacks

Marc Kührer[1]
Thomas Hupperich[1]
**Christian Rossow[2]**
Thorsten Holz[1]

[1] Ruhr-University Bochum
[2] Saarland University

USENIX Security, August 2014