Leibniz-Rechenzentrum
der Bayerischen Akademie der Wissenschaften

Detektion und Prävention von Denial-of-Service Amplification Attacken – Schutz des Netzes aus Sicht eines Amplifiers

Timm Böttger, Lothar Braun, Oliver Gasser, Helmut Reiser, Felix von Eye

DoS Amplification Attacken

- Ein alter Hut?

DoS Amplification Attacken

- Ein alter Hut?
- Meldung von 2006:

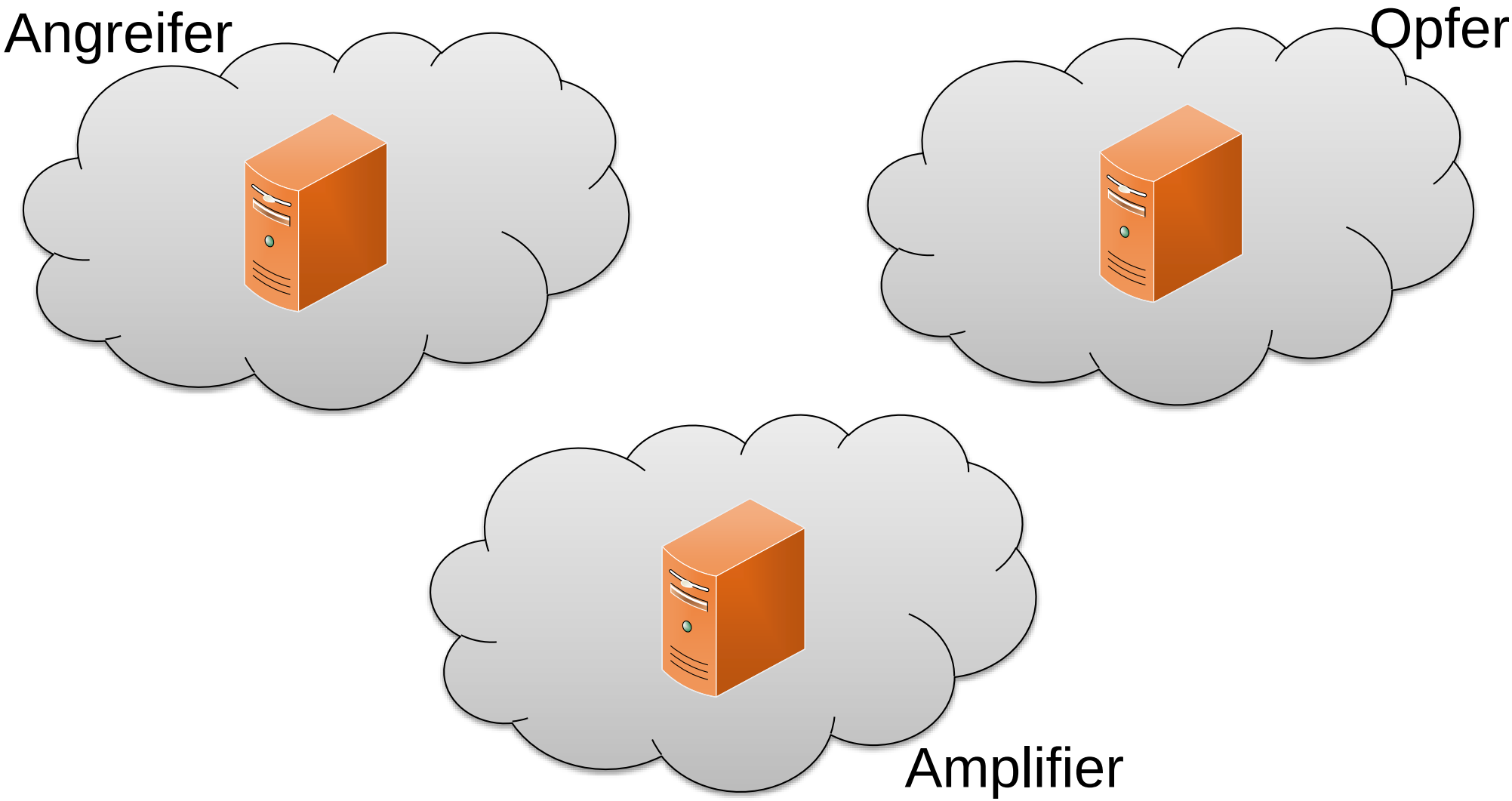
“In early February 2006, name servers hosting Top Level Domain zones were the repeated recipients of extraordinary heavy traffic loads. Analysis of traffic by TLD name server operators and security experts at large confirmed that DNS packets comprising the attack traffic exhibited characteristics associated with previously attempted DDoS attacks collectively known as amplification attacks.”

ICANN SSAC, SSAC Advisory SAC008 DNS Distributed Denial of Service (DDoS) Attacks. Internet: http://www.icann.org/committees/security/dns-ddos-advisory-31mar06.pdf

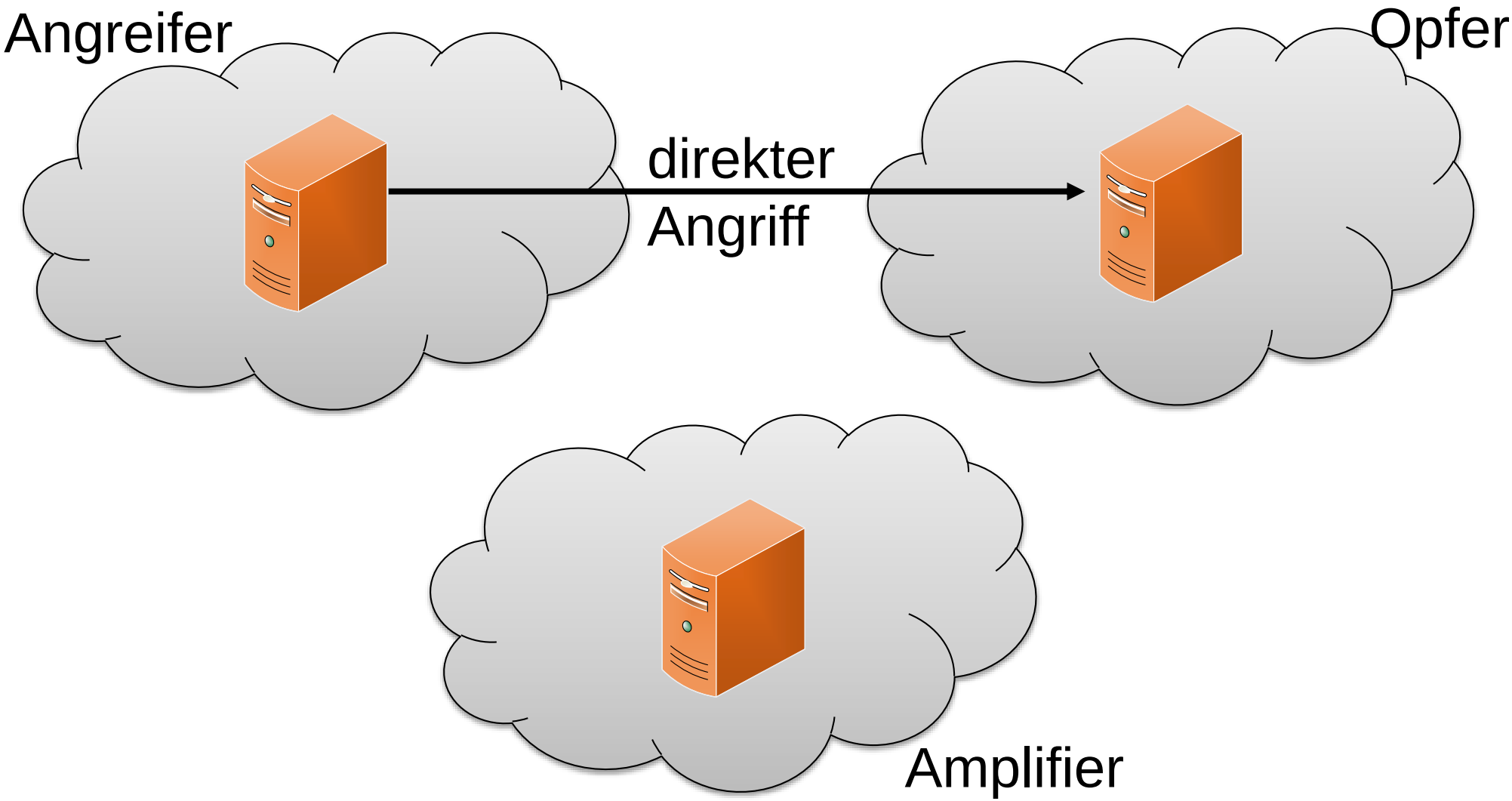
DoS Amplification Attacken

- Ein alter Hut?
- NEIN! Es werden immer noch (fast täglich) neue verwundbare Server gefunden!
- Erkennung/Meldung durch:
  - Open Resolver Scanning Project
  - BSI
  - DFN-CERT

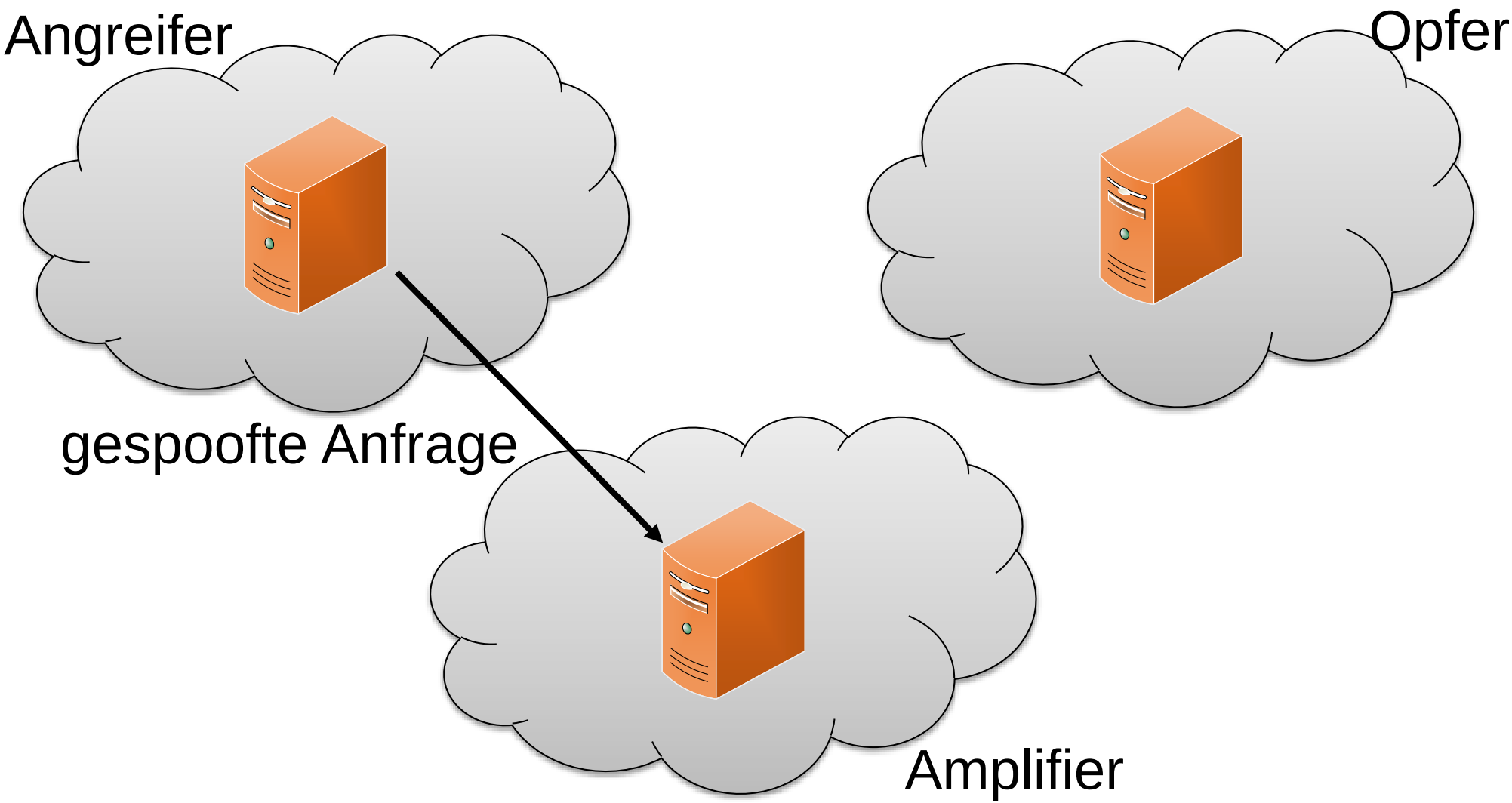
Ablauf einer Amplification Attacke



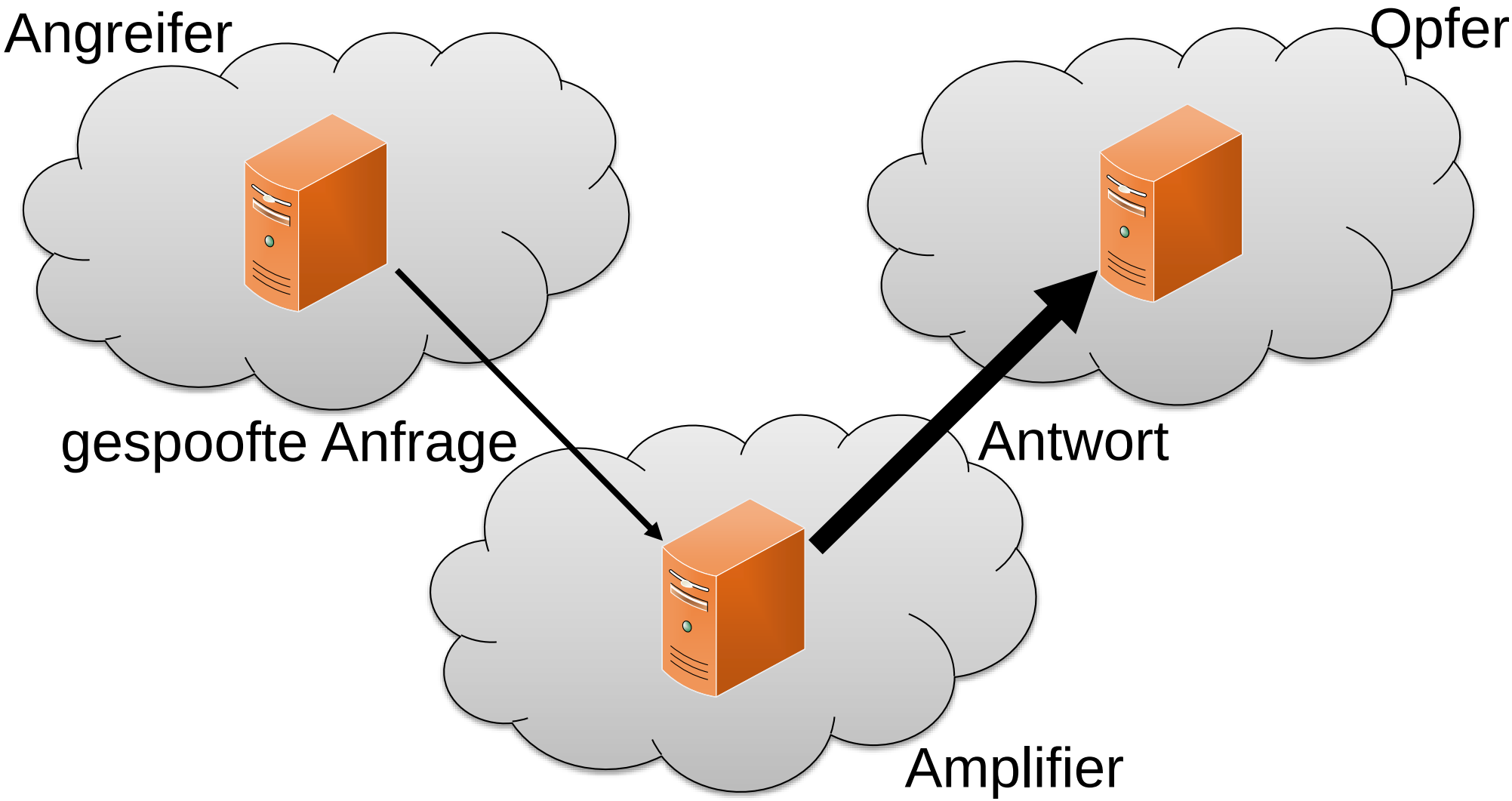
Ablauf einer Amplification Attacke



Ablauf einer Amplification Attacke



Ablauf einer Amplification Attacke



Mögliche Dienste

- SNMPv2
- NTP
- DNS
- NetBios
- SSDP

Christian Rossow. "Amplification Hell: Revisiting Network Protocols for DDoS Abuse". *2014 Network and Distributed System Security Symposium*, NDSS 2014, San Diego, CA, USA.

Mögliche Dienste

- SNMPv2
- NTP
- DNS
- NetBios
- SSDP
- Quake 3

Christian Rossow. "Amplification Hell: Revisiting Network Protocols for DDoS Abuse". *2014 Network and Distributed System Security Symposium*, NDSS 2014, San Diego, CA, USA.

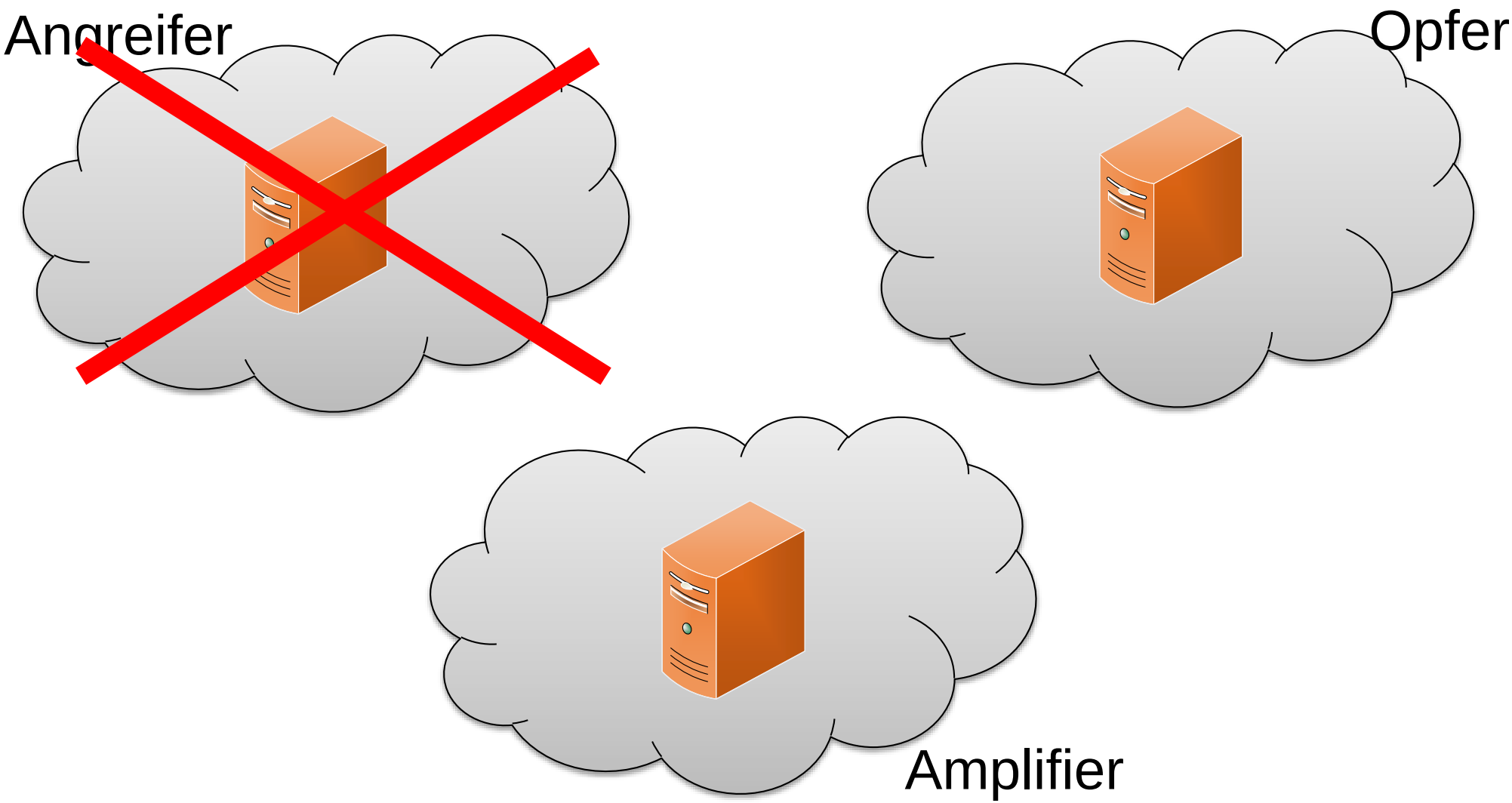
Mögliche Dienste

- SNMPv2
- NTP
- DNS
- NetBios
- SSDP
- Quake 3
- Gameover-Bot

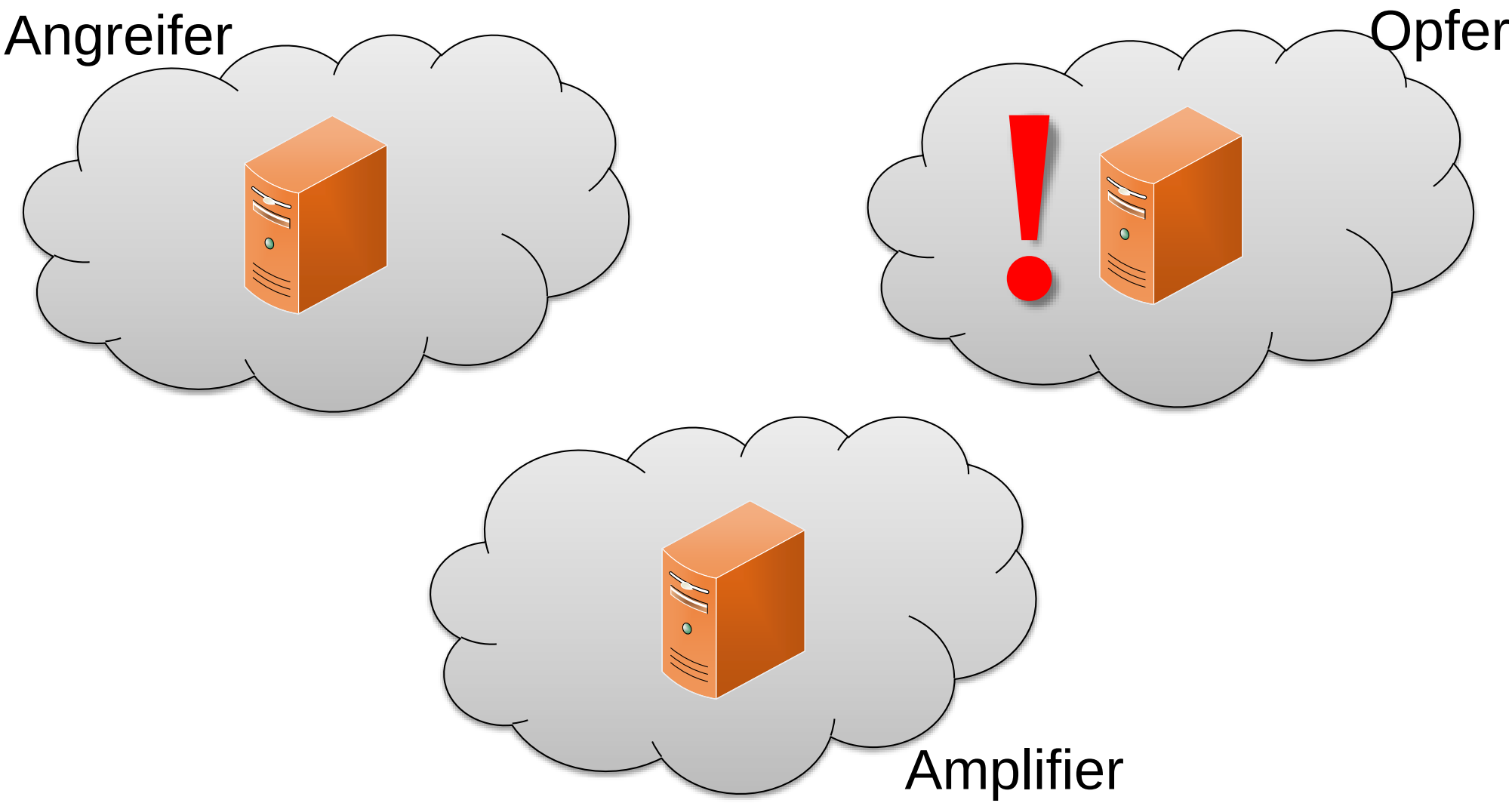
Und viele mehr!

Christian Rossow. "Amplification Hell: Revisiting Network Protocols for DDoS Abuse". *2014 Network and Distributed System Security Symposium*, NDSS 2014, San Diego, CA, USA.

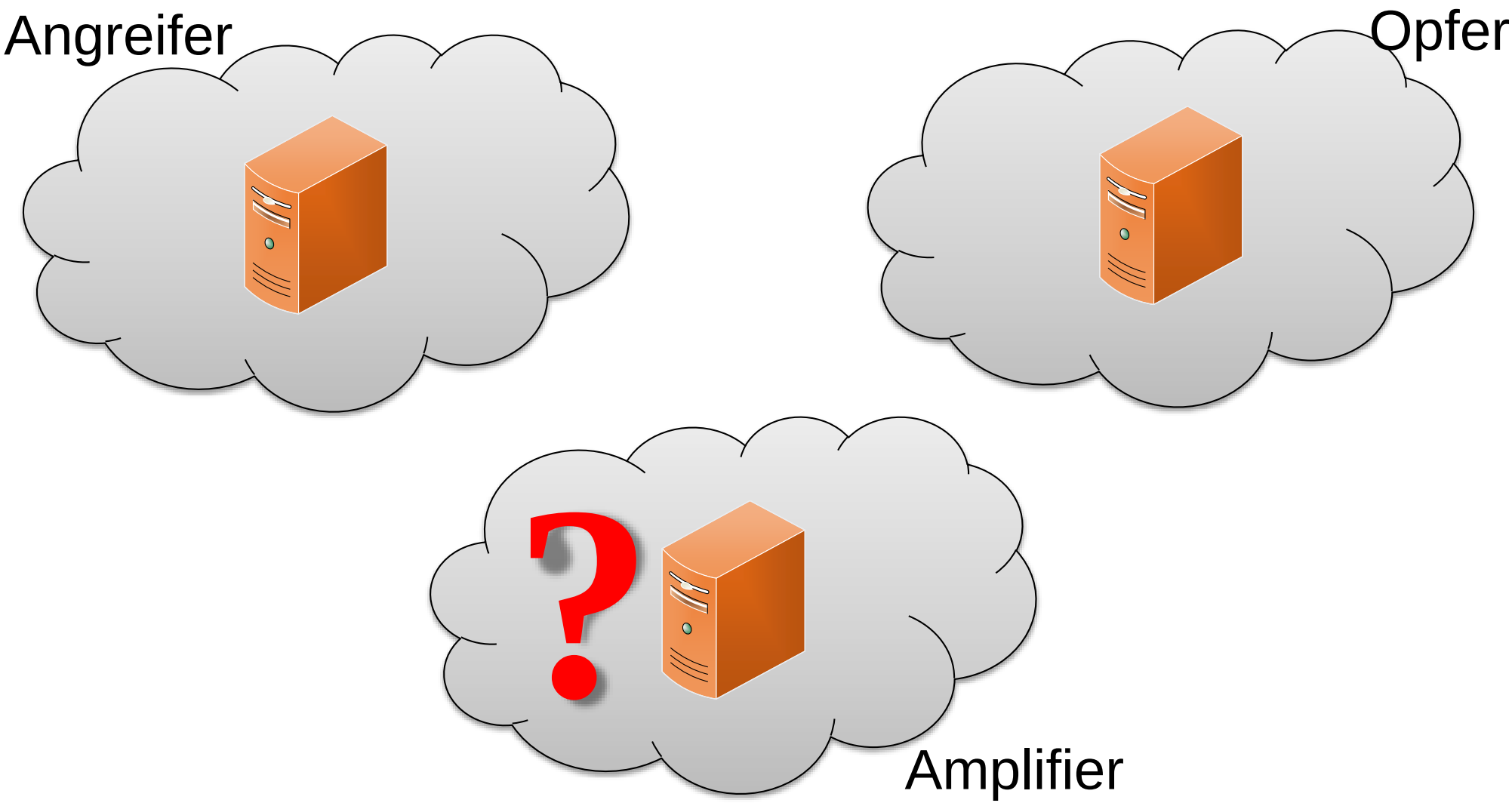
Gegenmaßnahmen?



Gegenmaßnahmen?



Gegenmaßnahmen?



Gegenmaßnahmen?

- Firewalls

Gegenmaßnahmen?

- Firewalls
- Drosselung des ausgehenden Verkehrs

Gegenmaßnahmen?

- Firewalls
- Drosselung des ausgehenden Verkehrs
- Drosselung des eingehenden Verkehrs

Gegenmaßnahmen?

- Firewalls
- Drosselung des ausgehenden Verkehrs
- Drosselung des eingehenden Verkehrs
- Patchen!

Ziel

(Generische) Erkennung von Amplification Angriffen

Bandwidth Amplification Factor

- BAF = *Ausgehender UDP-Payload* geteilt durch *Eingehender UDP-Payload*

Bandwidth Amplification Factor

- BAF = *Ausgehender UDP-Payload* geteilt durch *Eingehender UDP-Payload*

- Zusätzliche Bedingungen:
  - gesendeter Payload > 10 MB
  - gemessene Kommunikation > 10 kBits/s

Bandwidth Amplification Factor

- BAF = *Ausgehender UDP-Payload* geteilt durch *Eingehender UDP-Payload*

- Zusätzliche Bedingungen:
  - gesendeter Payload > 10 MB
  - gemessene Kommunikation > 10 kBits/s

- BAF > 5

Erkennen von Amplification Attacken – Kriterien

- IP-Spoofing

Erkennen von Amplification Attacken – Kriterien

- IP-Spoofing
- Delays

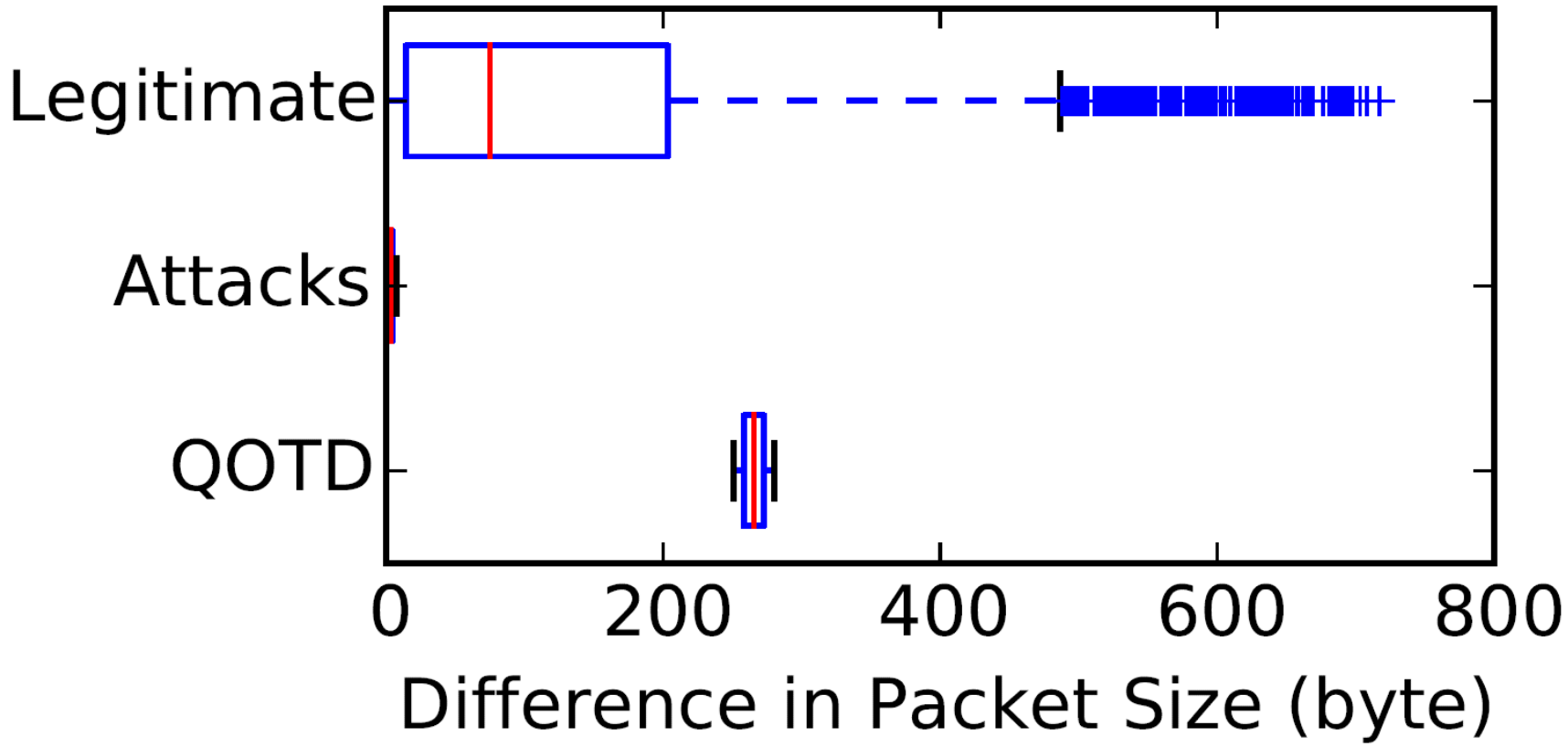
Erkennen von Amplification Attacken – Kriterien

- IP-Spoofing
- Delays
- Ähnlichkeit in
  - Paketgröße der Anfragen und Antworten
  - Inhalt des Payloads der Anfragen und Antworten

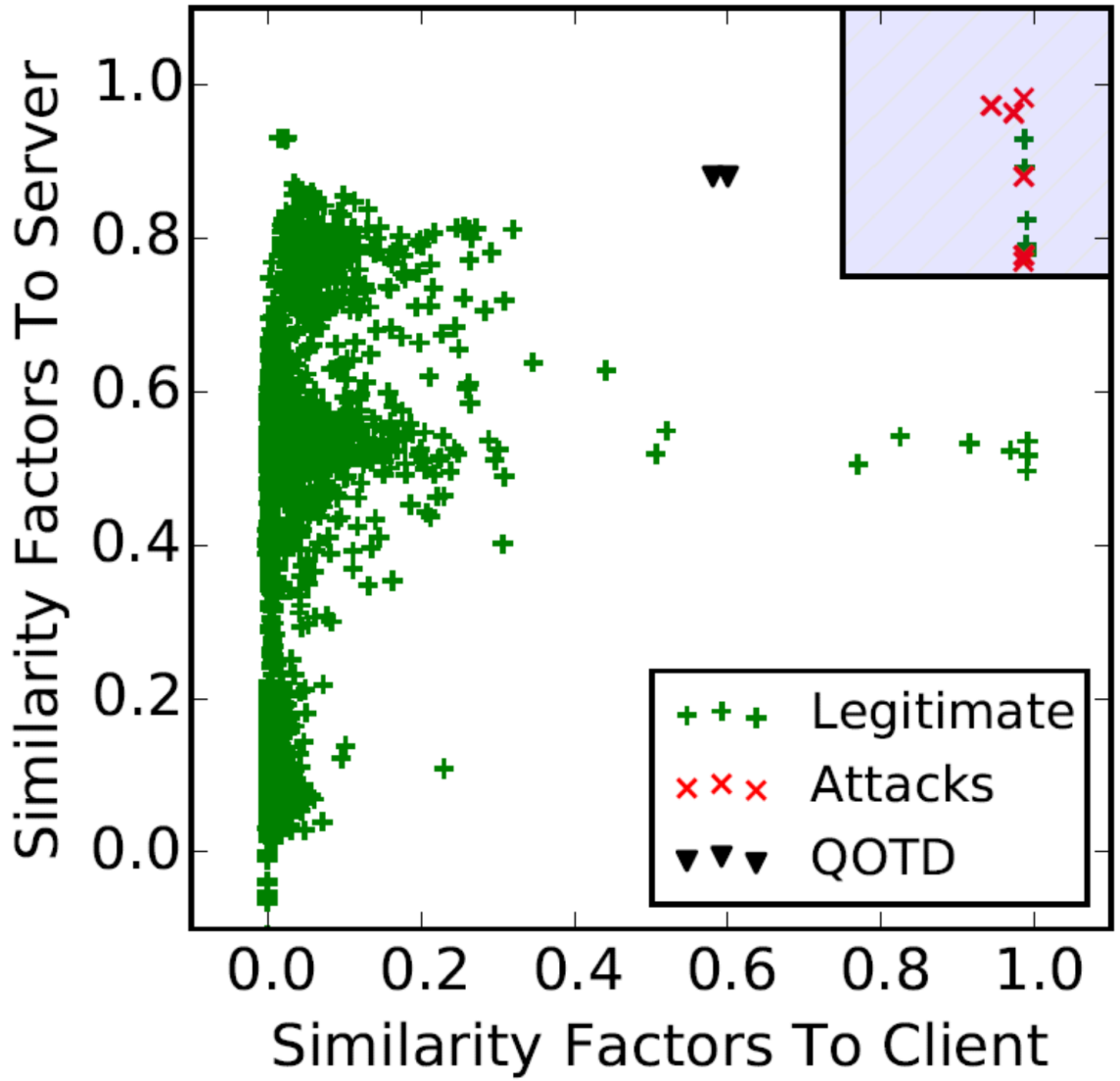
Erkennen von Amplification Attacken – Kriterien

- IP-Spoofing
- Delays
- Ähnlichkeit in
  - Paketgröße der Anfragen und Antworten
  - Inhalt des Payloads der Anfragen und Antworten
- „ICMP unreachable“-Antworten

Ähnlichkeit in der Paketgröße (Antworten)



Ähnlichkeit im Inhalt



Fazit

- Definition von Amplification Angriffen

Fazit

- Definition von Amplification Angriffen
- Mögliche Gegenmaßnahmen

Fazit

- Definition von Amplification Angriffen
- Mögliche Gegenmaßnahmen
- Erkennung von (generischen) Amplification Angriffen

Fazit

- Definition von Amplification Angriffen
- Mögliche Gegenmaßnahmen
- Erkennung von (generischen) Amplification Angriffen
- Definition verschiedener Schwellenwerte
  → Hier muss wohl noch mehr geforscht werden…

Vielen Dank für die Aufmerksamkeit

Fragen?

Kontakt:

Felix von Eye
voneye@lrz.de