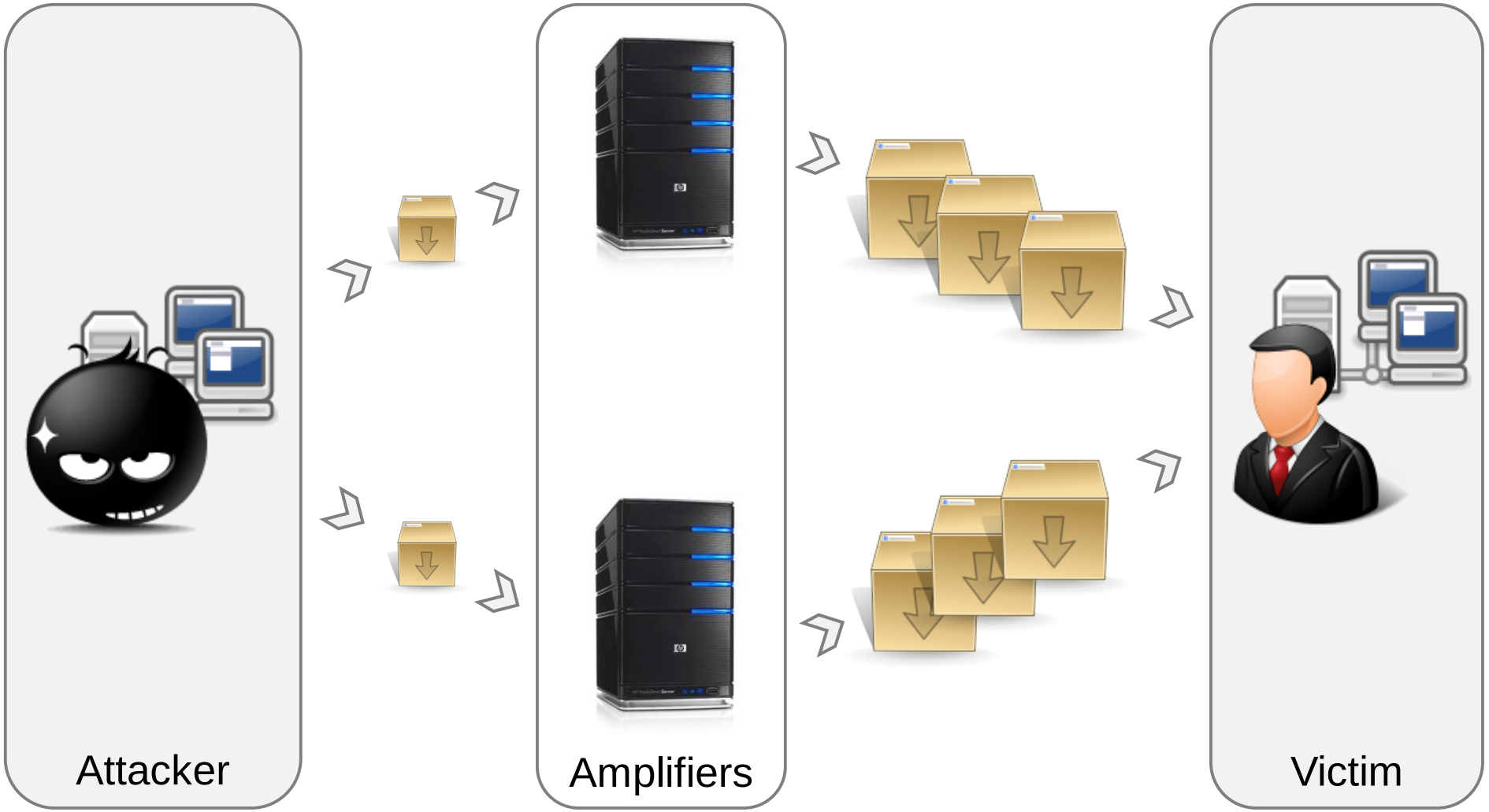
Hell of a Handshake – Abusing TCP for Amplification DDoS

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

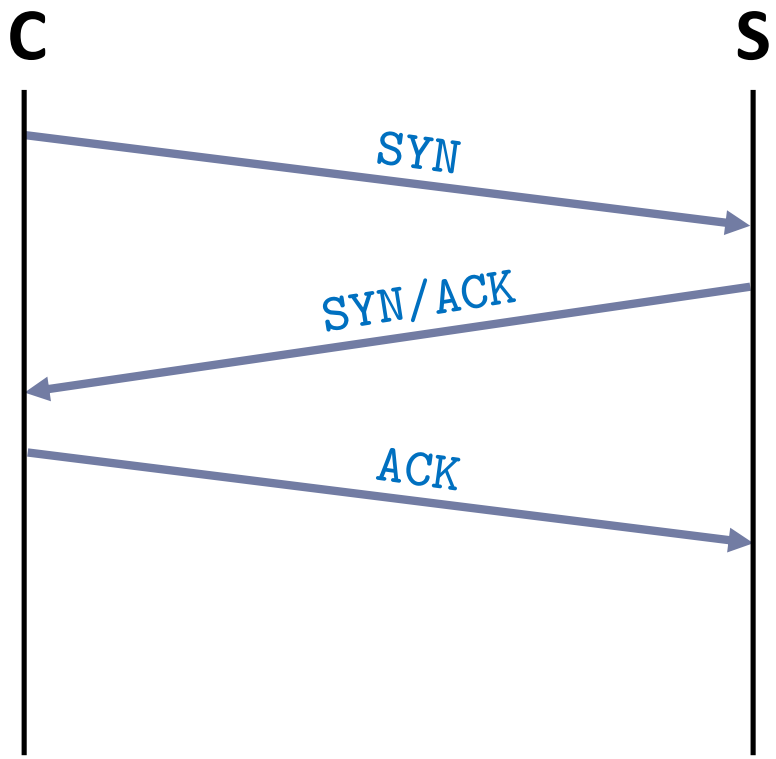
[1] Ruhr-University Bochum
[2] Saarland University

USENIX WOOT, August 2014

Amplification DDoS Attacks



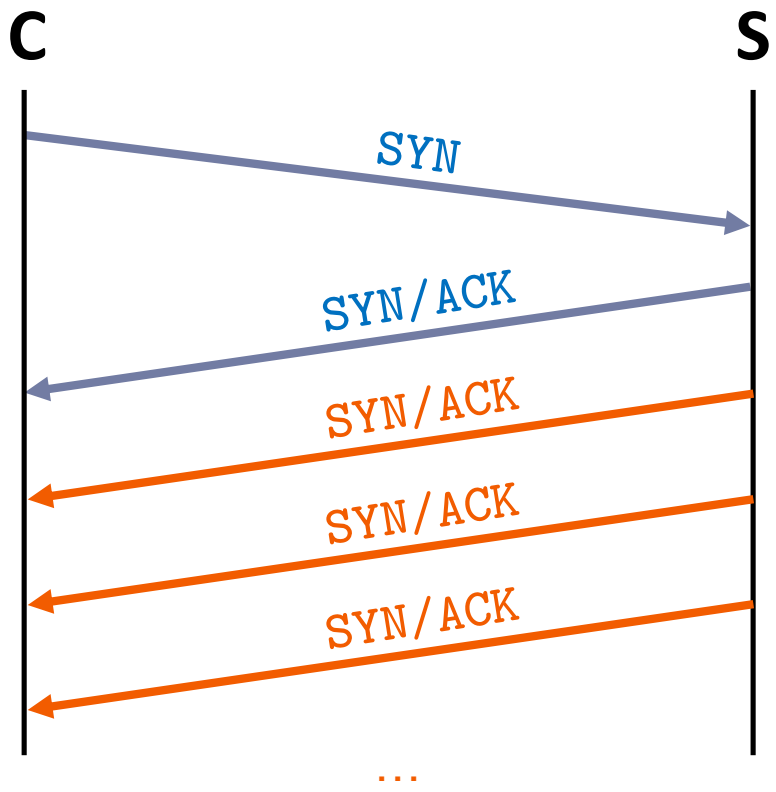
TCP and Reflection



TCP 3-Way Handshake

- Reflection
- No amplification

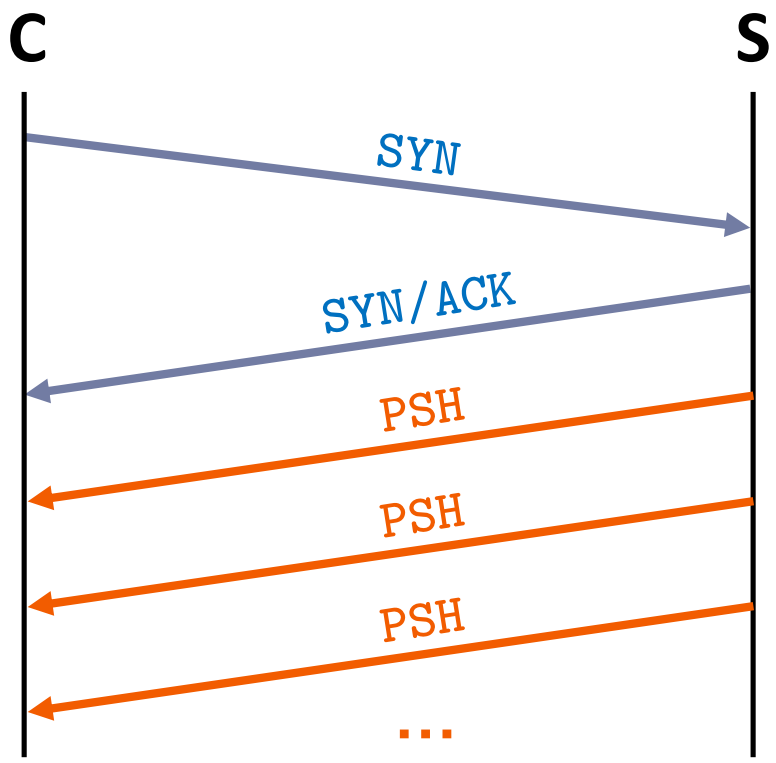
TCP and Reflection



SYN/ACK Amplifiers

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

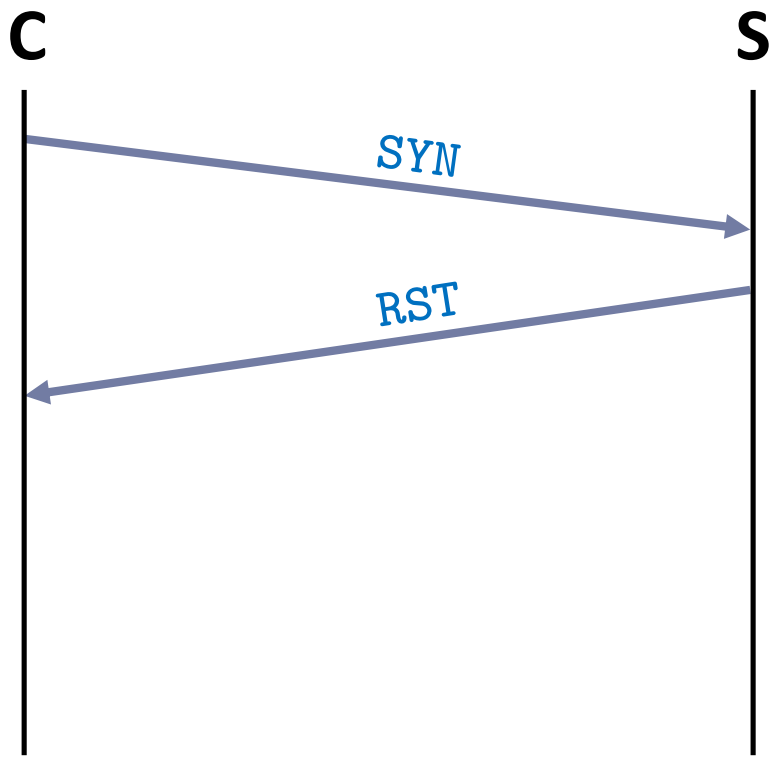
TCP and Reflection



PSH Amplifiers

- Send data *before* handshake finishes
- e.g., FTP server banner info

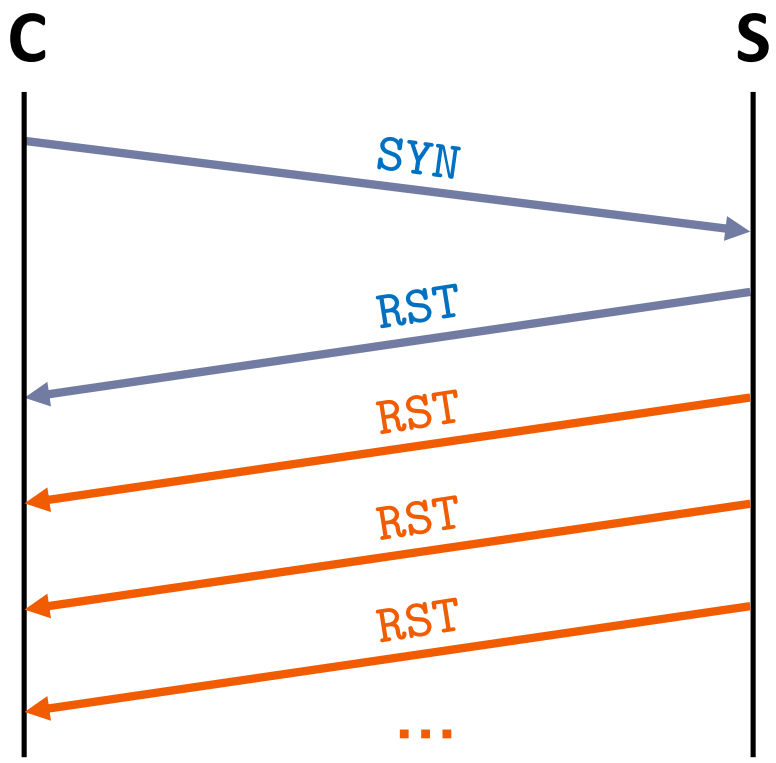
TCP and Reflection



TCP Closed Port

- Reflection
- No amplification

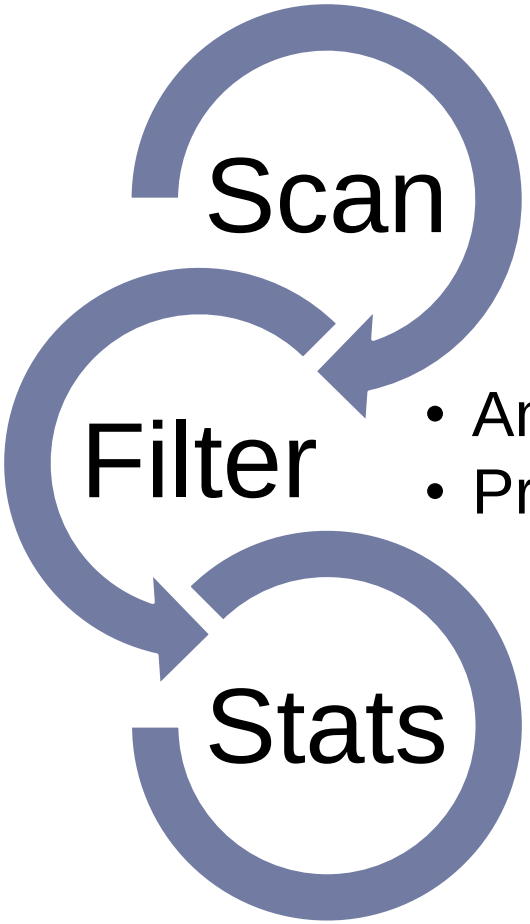
TCP and Reflection



RST Amplification

- Hosts persist sending RST
- No rationale?

Methodology



- IPv4 Address Range
- TCP `SYN` Packets

- Amplification >20
- Prevalent Protocols

- Amplifier Classification
- Evaluate Countermeasures

Amplification Statistics

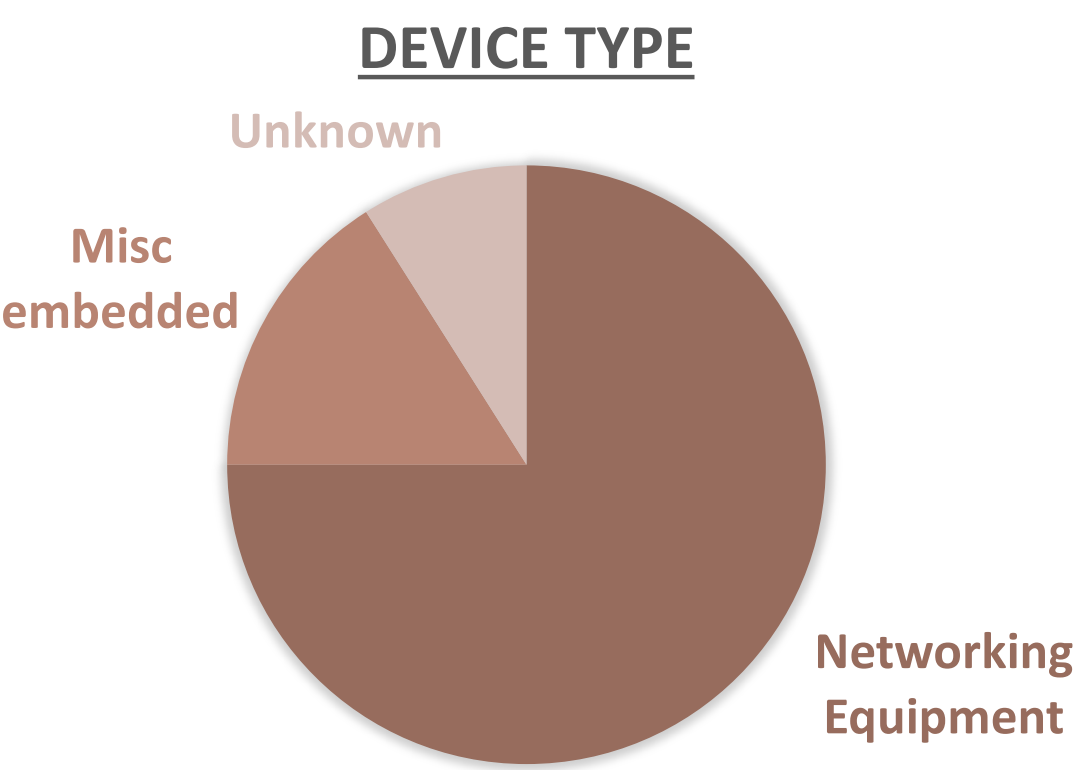
	SYN/ACK	
Protocol	# Ampl.	AF
FTP	2,907,279	22x
HTTP	421,487	60x
NetBIOS	8,863	54x
SIP	16,496	1,596x
SSH	81,256	80x
Telnet	2,112,706	28x

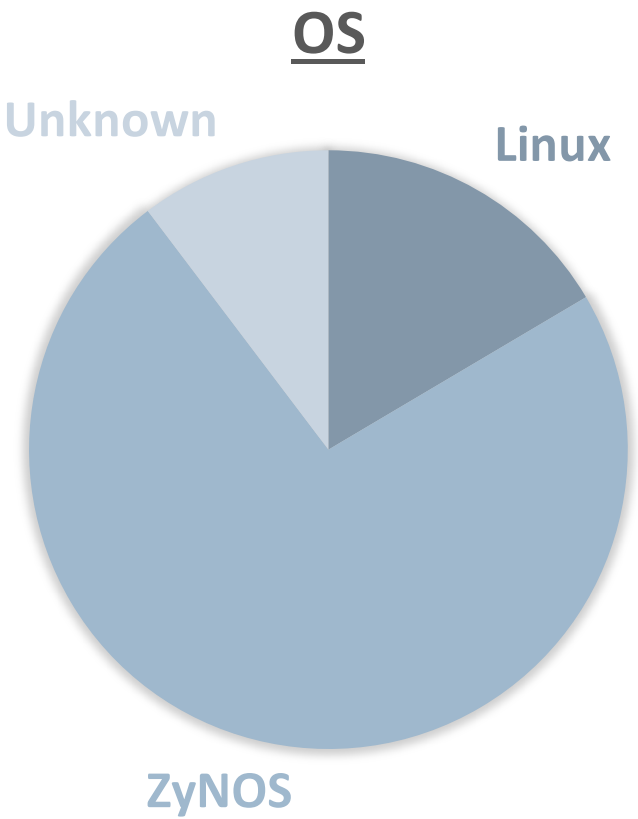
Attack Frequency

- Response packets per X seconds

	SYN/ACK			PSH			RST		
Protocol	< 10	< 30	< 60	< 10	< 30	< 60	< 10	< 30	< 60
FTP	2	5	10	5	10	14	561	1,584	3,055
HTTP	2	6	11	5	10	16	140	224	264
NetBIOS	8	17	22	5	6	8	976	2,748	5,291
SIP	2	6	12	1	1	1	562	1,360	2,497
SSH	3	6	11	6	9	10	595	1,394	2,523
Telnet	2	5	10	52	154	277	996	2,345	4,254

Amplifier Classification





Active Defense

- SYN/ACK storms: send RST segments
  - Stops about 99.9% of the SYN/ACK streams
- RST storm: send ICMP port unreachable messages
  - Stops about 80% of the RST streams

Conclusion

- Also TCP suffers from amplification vulnerabilities
  - RST, PSH and SYN/ACK storms
- We notified vendors, but fixes will take time
- Use active countermeasures to mitigate attacks

Hell of a Handshake – Abusing TCP for Amplification DDoS

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

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

USENIX WOOT, August 2014