DDOS ANGRIFFE UND MITIGATION

Ein kurzer Überblick

Dr. Carsten Löhn | Frankfurt | 2020-12-02

Xantaro SERVICE INTEGRATION

ZU MEINER PERSON

- Dr. Carsten Löhn
- Project Consultant
  - IT Security
  - Schwerpunkte Firewalling und DDoS
- 13y ExperTeach GmbH, davon 9y Security
- 8y Xantaro – Professional Services

ABLAUF

- DDoS im Überblick
- Mitigationstechniken im Überblick
- Kurze Vorführung im Lab

DDOS IM ÜBERBLICK

Was ist DDoS?

Klassifikation von DDoS?

Typische Angriffe

DENIAL OF SERVICE - ÜBERBLICK

- Wie kann ein System “Out of Service” gesetzt werden?
  - Überfluten mit IP Paketen
    - System selbst ist überfordert
    - Geräte „auf dem Weg“ sind überfordert
    - Leitung zu 100% ausgelastet
  - Belegen von Systemressourcen
    - Anzahl paralleler Verbindungen (Session Table)
    - Rechenintensive Anfragen (Verschlüsselung, Datenbankabfragen, etc)
    - Langsame Kommunikation („Slow-and-Low“)
  - Systemabsturz provozieren
- Warum will ich ein System „Out of Service“ setzen?
- Kollateralschäden

VOM DOS ZUM DDOS

- DDoS = Distributed Denial of Service
- Je mehr Angreifer, desto größer das Volumen
- Je mehr Angreifer, desto schwerer sind sie zu identifizieren

- Botnetze können aus mehreren hunderttausend Systemen bestehen.
- IoT ist eine der führenden Technologien zum Ausbau von Botnetzen

KLASSIFIZIERUNG

- Klassifizierung von DDoS-Angriffen:
  - Volumetrische Angriffe
  - TCP State-Exhaustion
  - Applikations-basierte Angriffe

- Hilfsmittel:
  - IP Spoofing
  - Verstärkung (Reflection/Amplification)
  - Fehlerhafte Protokollimplementierungen

IP SPOOFING

- Fälschen der Absender-Adresse
- Typisch für Angriffe, die keine bidirektionale Kommunikation erfordern
  - UDP Flood
  - ICMP Flood
  - SYN Flood
- Grundideen:
  - Verschleiern der eigenen Identität
  - Angriffe können nicht anhand der Absender-IP-Adresse geblockt werden.
  - Antworten sollen eigenes System nicht überlasten
  - Gefälschte Absender-IP ist eigentliches Opfer

AMPLIFICATION ATTACKS

- Kleine Anfrage => Große Antwort
- Oftmals Drittsysteme als Verstärker

- Beispiele:
  - DNS Amplification
  - NTP Amplification
  - Memcached Amplification

- DDoS-Rekorde:
  - März 2018: Memcached 1,7 Tbit/s
  - Feb 2020: CLDAP 2,3 Tbit/s

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]
CLDAP [7]	56 to 70	—
TFTP [23]	60	—
Memcached [25]	10,000 to 51,000	—
WS-Discovery	10 to 500	—

https://us-cert.cisa.gov/ncas/alerts/TA14-017A

TYPISCHE DDOS-ANGRIFFE IM ÜBERBLICK (1)

- ICMP Flood, UDP Flood
  - Überlasten des Netzwerks oder Servers durch Masse an Paketen. Typischerweise keine Korrelation zwischen Paketen. IP Spoofing als Hilfsmittel.
- ACK Flood
  - Überlasten des Netzwerks oder Servers durch Masse an Paketen. Überlastung von Session-basiert arbeitenden Systemen wie Firewall oder Server durch zusätzlichen Session Lookup. Keine Korrelation zwischen Paketen. IP Spoofing als Hilfsmittel.
- RST/FIN Flood
  - Wie ACK Flood. Zusätzliche Chance bestehende reguläre Verbindungen zu beenden.
- Null Flood, XMAS Flood, etc.
  - Senden irregulärer TCP-Flag-Kombinationen
  - Wie andere TCP-Floods, aber zusätzliche Chance auf Systemabsturz.

TYPISCHE DDOS-ANGRIFFE IM ÜBERBLICK (2)

- SYN Flood
  - 3-Way-Handshake: SYN – SYN/ACK – ACK
  - Finales ACK-Paket wird nicht gesendet
  - Überlastung von Firewall State Tables und Backlog Queues
  - Was macht Server, wenn SYN/ACK nicht beantwortet wird?
  - Typischerweise in Verbindung mit IP Spoofing

TYPISCHE DDOS-ANGRIFFE IM ÜBERBLICK (3)

- DNS Flood
  - Überflutung eines DNS-Servers mit Anfragen. Oftmals Abfrage nicht existierender Hosts. Spezielle Form der UDP-Flood. IP Spoofing als Hilfsmittel.
- DNS Amplification Attack
  - Fluten von offenen Recursive-DNS-Servern (Resolver) mit Anfragen. Absender-IP ist die des Opfers. Antworten zumeist deutlich länger als Anfragen. Häufig Einsatz von Extended DNS.
- NTP Amplification Attack
  - Ausnutzen des „monlist“ Features. Abfrage der letzten (600) Queries. Absender-IP ist die des Opfers.
- MemCached Amplification Attack
  - OpenSource Caching Dienst. Abfragen großer Mengen an Daten mit gefälschter Absender-IP über TCP oder UDP. UDP in neuester Version deaktiviert.

TYPISCHE DDOS-ANGRIFFE IM ÜBERBLICK (4)

- HTTP GET Flood
  - Senden einer Vielzahl an GET-Requests innerhalb einer einzelnen HTTP-Sitzung. Typischerweise werden dabei Datenbankabfragen an Backend-Systeme provoziert. Typischerweise „NoCache“-Anweisungen.
- Slow-and-Low Attacks
  - Verschiedene Varianten
    - Verzögern von ACK-Paketen
    - Extreme Fragmentierung des HTTP-Headers
    - HTTP Post mit angekündigter hoher Datenmenge, die nie gesendet wird.

KOMBINATION VON ANGRIFFSVEKTOREN

- Das Kombinieren oder Wechseln verschiedener Angriffsverfahren erschwert die Abwehr.
- Eigentlicher Angriff kann unter einem DDoS-Angriff verschleiert werden.
- Nach einem abgewehrten Angriff ist ein Wechseln des Angriffsvektors wahrscheinlich.

MITIGATIONSKONZEPTE

Erkennen von DDoS

Typische Maßnahmen

ABWEHR VON DDOS-ANGRIFFEN

- Abwehr von DDoS-Angriffen ist ein zweistufiges Konzept.

1. Erkennen der Angriffe (Detection)
   - Flow Monitoring (typischerweise Flows von den Border Routern)
   - Anruf vom Kunden
2. Ergreifen von Maßnahmen
   - Remote Triggered Blackholing
   - BGP Flowspec
   - Mitigation

DETECTION

- Überwachung fest definierter oder gelernter (Profiling) Grenzwerte
  - pro Host
  - pro Netzwerk
  - pro Router
- Alarm, wenn Raten überschritten werden
  - Byte/s vs. Paket/s
  - Wie lange muss eine Rate überschritten sein?
- Einschränkungen
  - Flow Monitoring üblicherweise mit Raten 1 zu 1000
  - Flows basierend auf 5-Tupel
  - Inline Monitoring bedeutend genauer aber kostspielig

REMOTE TRIGGERED BLACKHOLING

- Remote Triggered Blackholing (RTBH) als drastische Maßnahme
  - BGP-Update: Ziel-IP -> Discard
  - Angriffsziel ist in allen Fällen „out of service“, aber andere Systeme hinter derselben Leitung sind geschützt.

- Einsatz:
  - Bei Fehlen eines Mitigation Devices
  - Mitigation Device kann Angriff nicht abwehren
  - Mitigation Device kann Datenstrom nicht abhandeln

- BGP Flowspec als mögliche Alternative

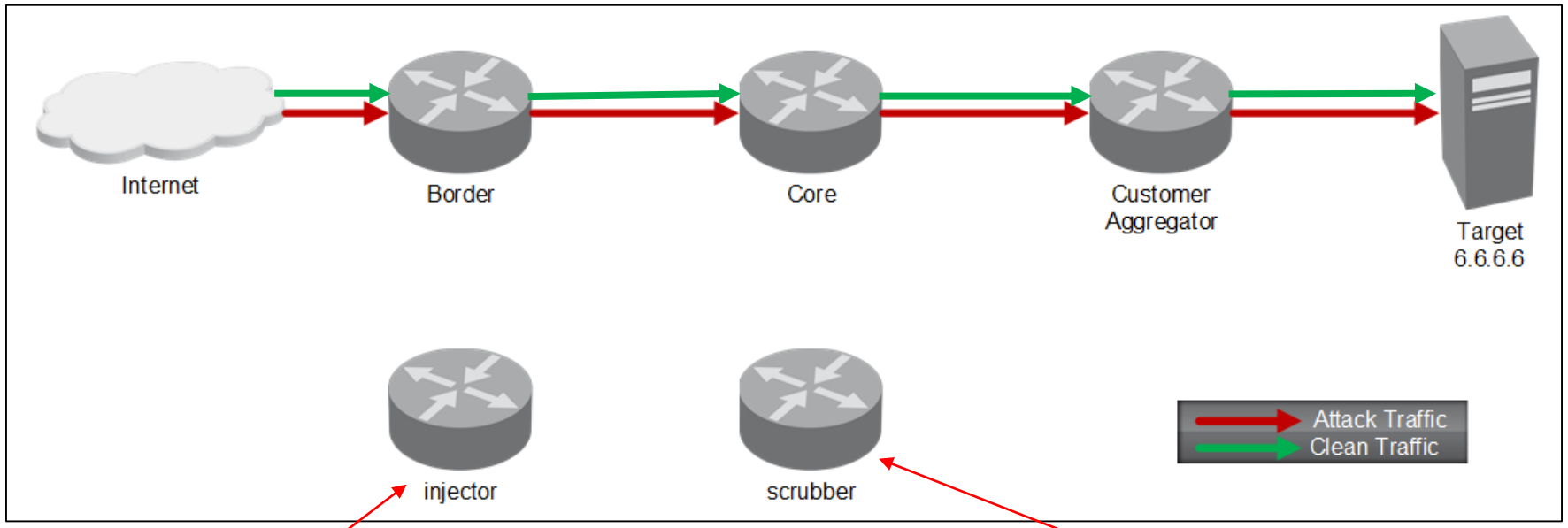
BGP FLOWSPEC

- RFC 5575
- Signalisieren von Daten zu Traffic Flows in Network Layer Reachability Information (NLRI) in MP-BGP
- Actions:
  - **Traffic-Rate Community (0=drop)**
  - Traffic-Action Community (sampling)
  - Redirect Community
  - Traffic-Marking Community (DSCP)

Type	Information
1	Destination Prefix
2	Source Prefix
3	IP Protocol
4	Source or Destination Port
5	Destination Port
6	Source Port
7	ICMP Type
8	ICMP Code
9	TCP flags
10	Packet length
11	DSCP
12	Fragment Encoding

MITIGATION - GENERELLES KONZEPT (1)

- In einem klassischen 3-stufigen Routing-Konzept befinden sich Border Router, Core Router und Customer Aggregator
- Diese klare Trennung ist in der Praxis oft nicht vorhanden, erleichtert aber das Mitigationskonzept.

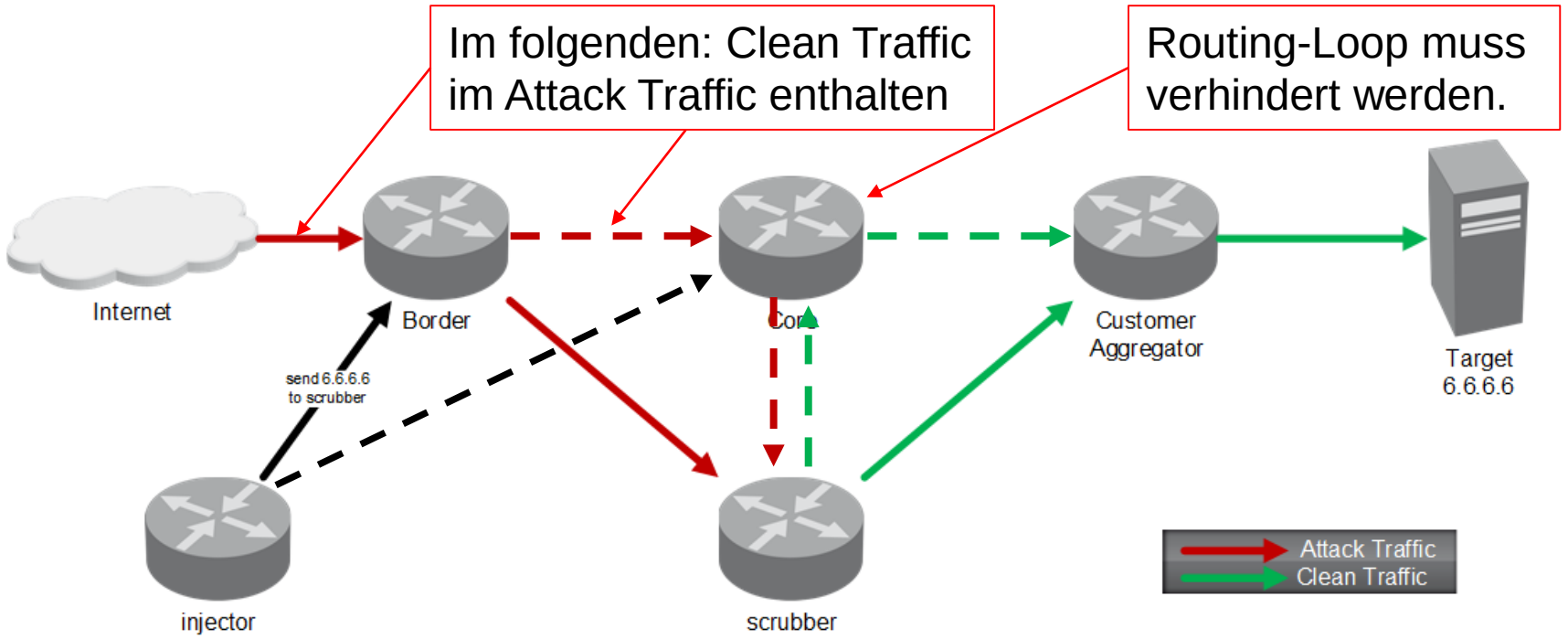


Injector steuert das Umleiten der Verkehrsströme zum Scrubber

Scrubber soll Angriffs-Traffic blocken und regulären durchlassen

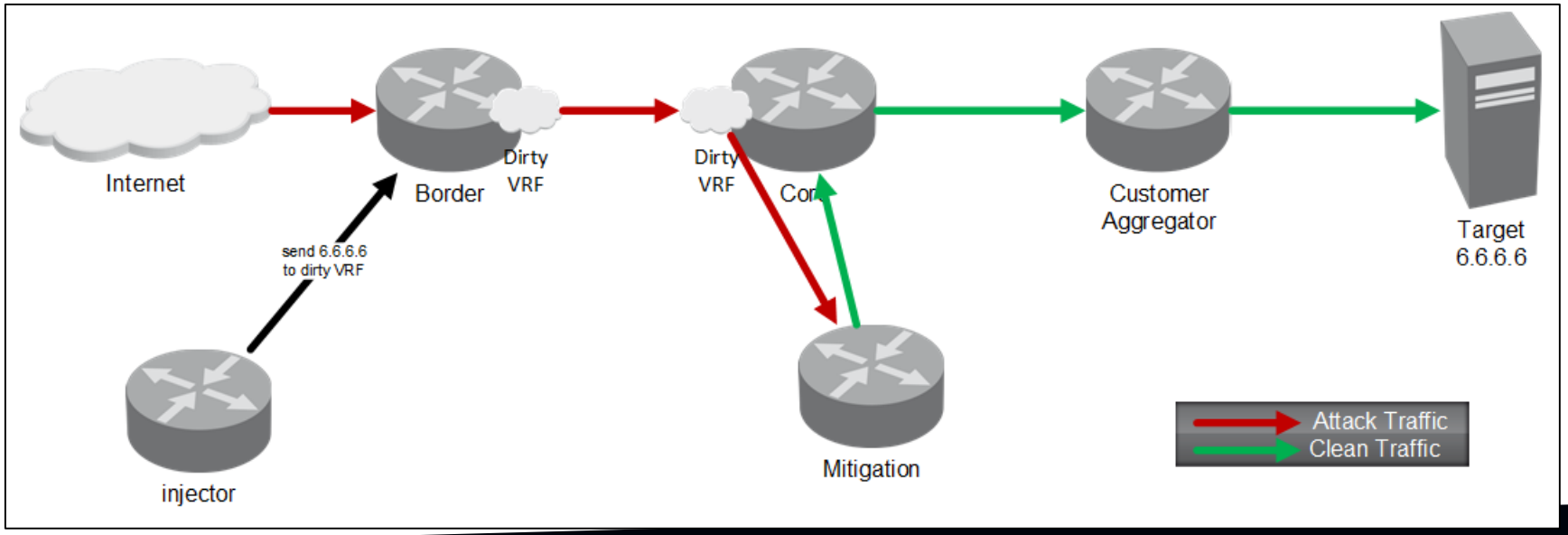
MITIGATION - GENERELLES KONZEPT (2)

- Datenströme zum Zielsystem müssen zum Scrubber umgeleitet werden.
- Umleitung geschieht am besten am Border (durchgezogene Linien). Optional auch am Core (gestrichelte Linien) möglich.
- Probleme:
  - Skalierung (GRE?)
  - Routing Loops



MITIGATION – DIRTY VRF

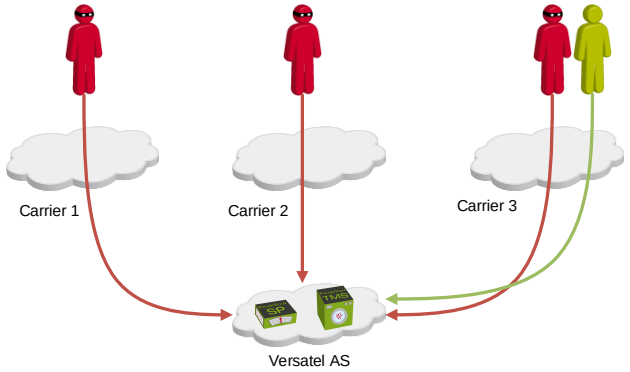
- „Dirty VRF“ als eleganteste Variante (von vielen)
  - Regulärer Weg: Border – Core – Customer Aggregator – Target
  - Dirty VRF hat Scrubber als Default Gateway
  - Im Falle eines Angriffs wird das Dirty VRF per BGP Injection zum Next-Hop für die angegriffene Ziel-IP
  - Traffic, der vom Scrubber zurückkommt, unterliegt dem regulären Routing
  - Antwort-Pakete laufen NICHT über den Scrubber!

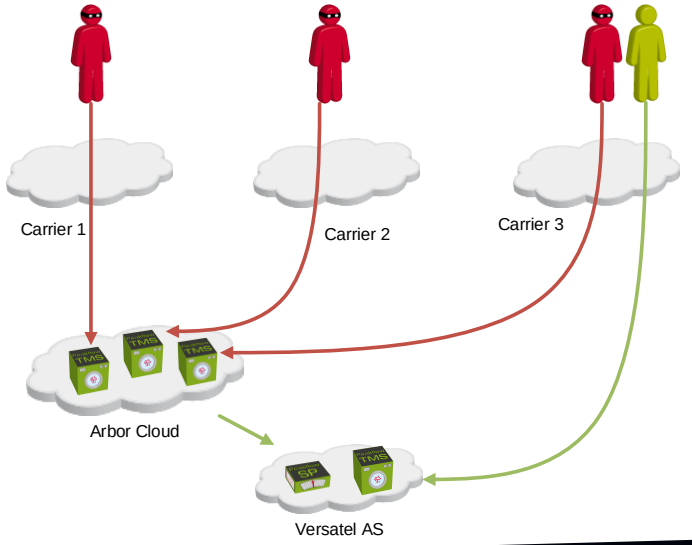


CLOUD-BASED MITIGATION

- Externe Unterstützung
  - Remote Triggered Blackholing zum Upstream/Carrier
  - BGP Flowspec zum Upstream/Carrier
  - „Cloud-based Mitigation“ (nur für >= /24)

  - Weg von der Cloud bis zum Kunden
    - Direktes Peering
    - GRE





ARBOR KOMPONENTEN

- Arbor Networks langjähriger Technologieführer im Bereich DDoS
- Mittlerweile Sparte von NETSCOUT
- Arbor TMS (Threat Mitigation System)
  - Abwehr der Angriffe
  - Trennen von validem Verkehr und Angriffen
- Arbor Sightline (bzw. Arbor SP bzw. Peakflow SP)
  - Data Collection
  - Network Visibilty
  - Reporting
  - Management
- Arbor Edge Defense (AED)
  - Vor Ort beim Kunden
  - Mitigation bis Leitungsgeschwindigkeit
- Arbor Cloud

ARBOR TMS

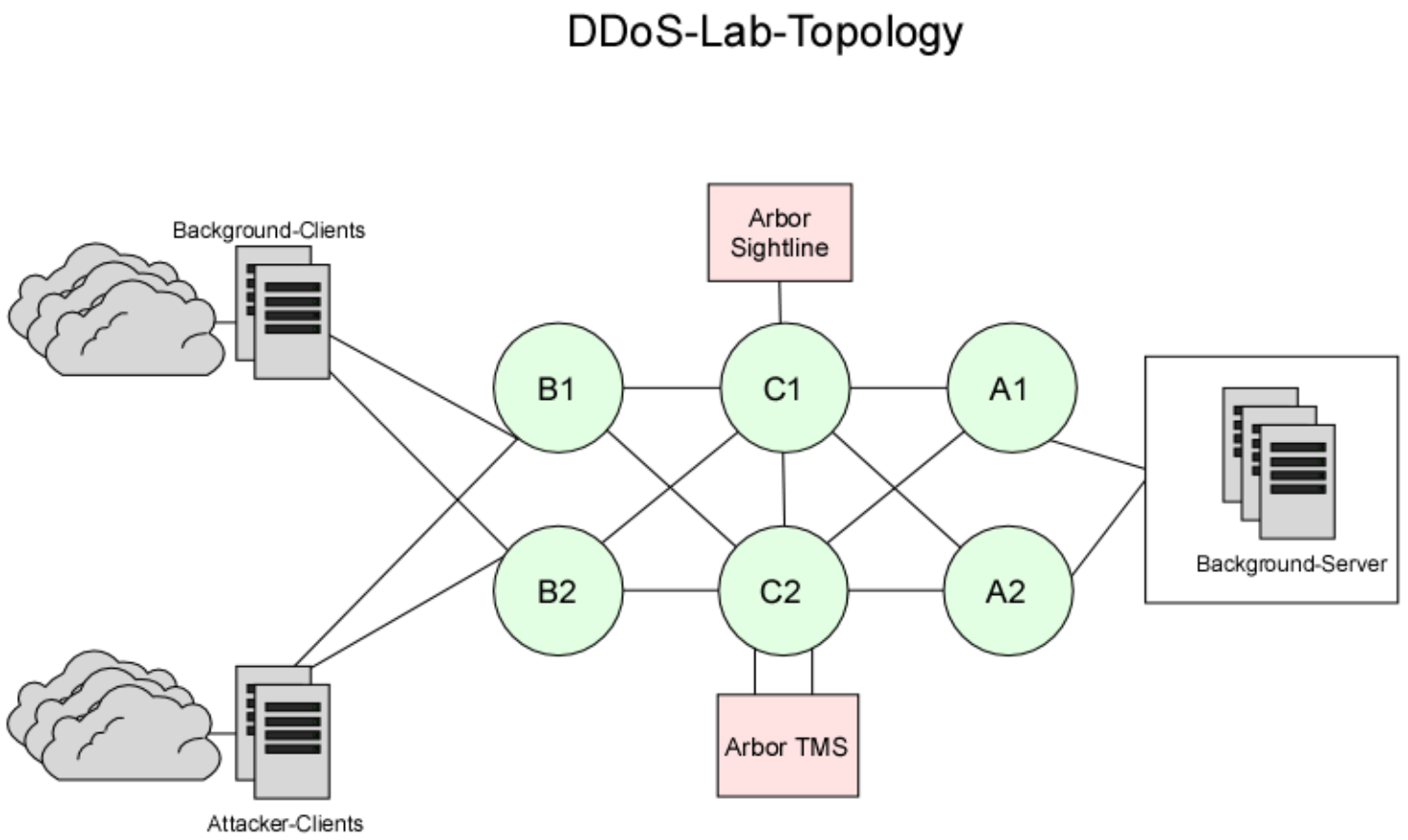
- Threat Mitigation System
- Vielzahl von Countermeasures
  - Komplexe Paketfilter
  - Spezielle Countermeasure für HTTP, DNS und SIP
  - SSL Protection
  - Botnet Signatures
- Minimales State Tracking
- Black- und Whitelisting
  - Abhängig von gewählter Countermeasure
  - Whitelisting dauerhaft während Angriff
  - Blacklisting für 5 Minuten; Optional Export per BGP Flowspec

DDOS IM LAB

Labaufbau

Präsentation: SYN-Flood

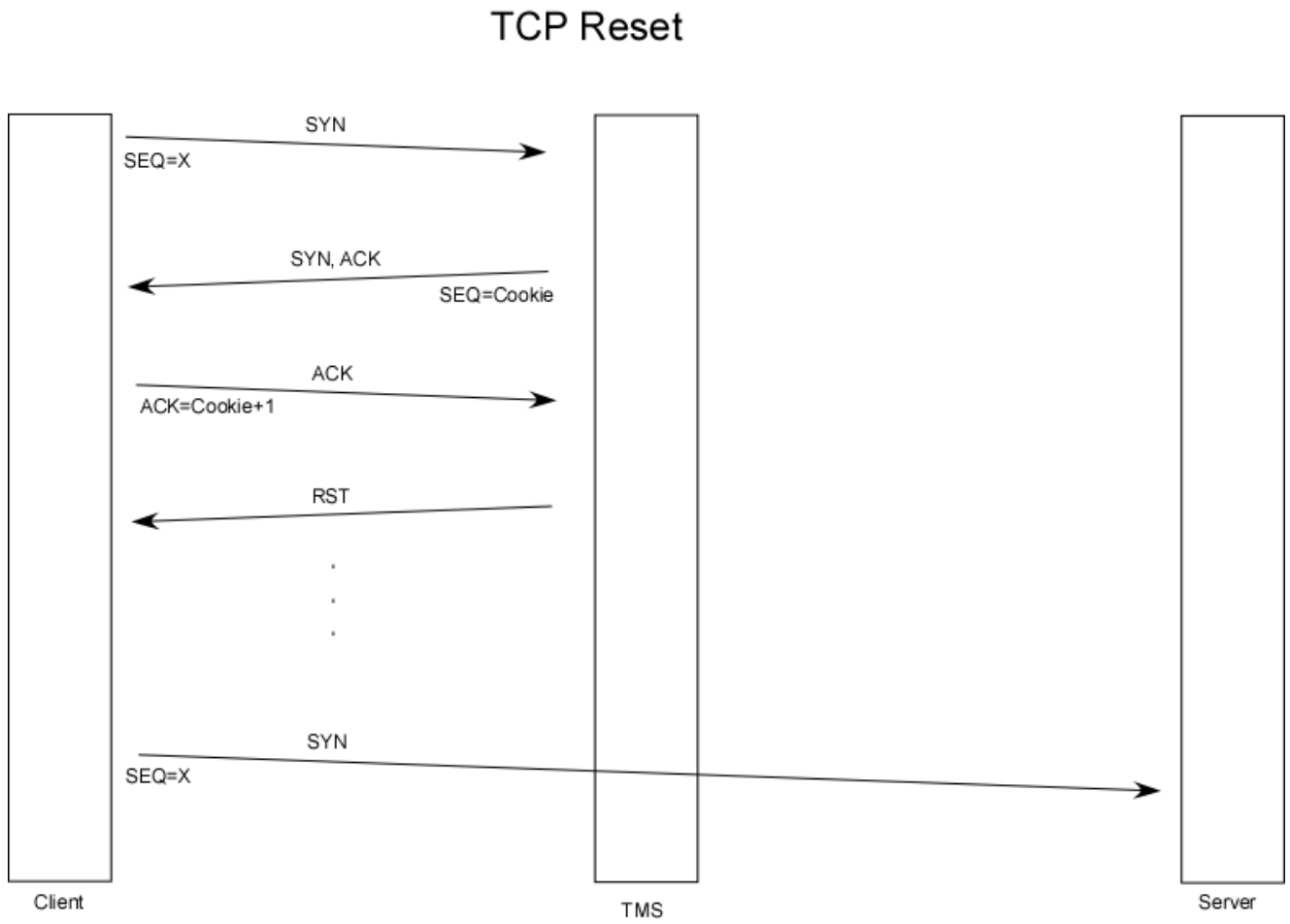
LABAUFBAU


DDoS-Lab-Topology
Background-Clients
Arbor Sightline
B1
C1
A1
B2
C2
A2
Background-Server
Arbor TMS
Attacker-Clients

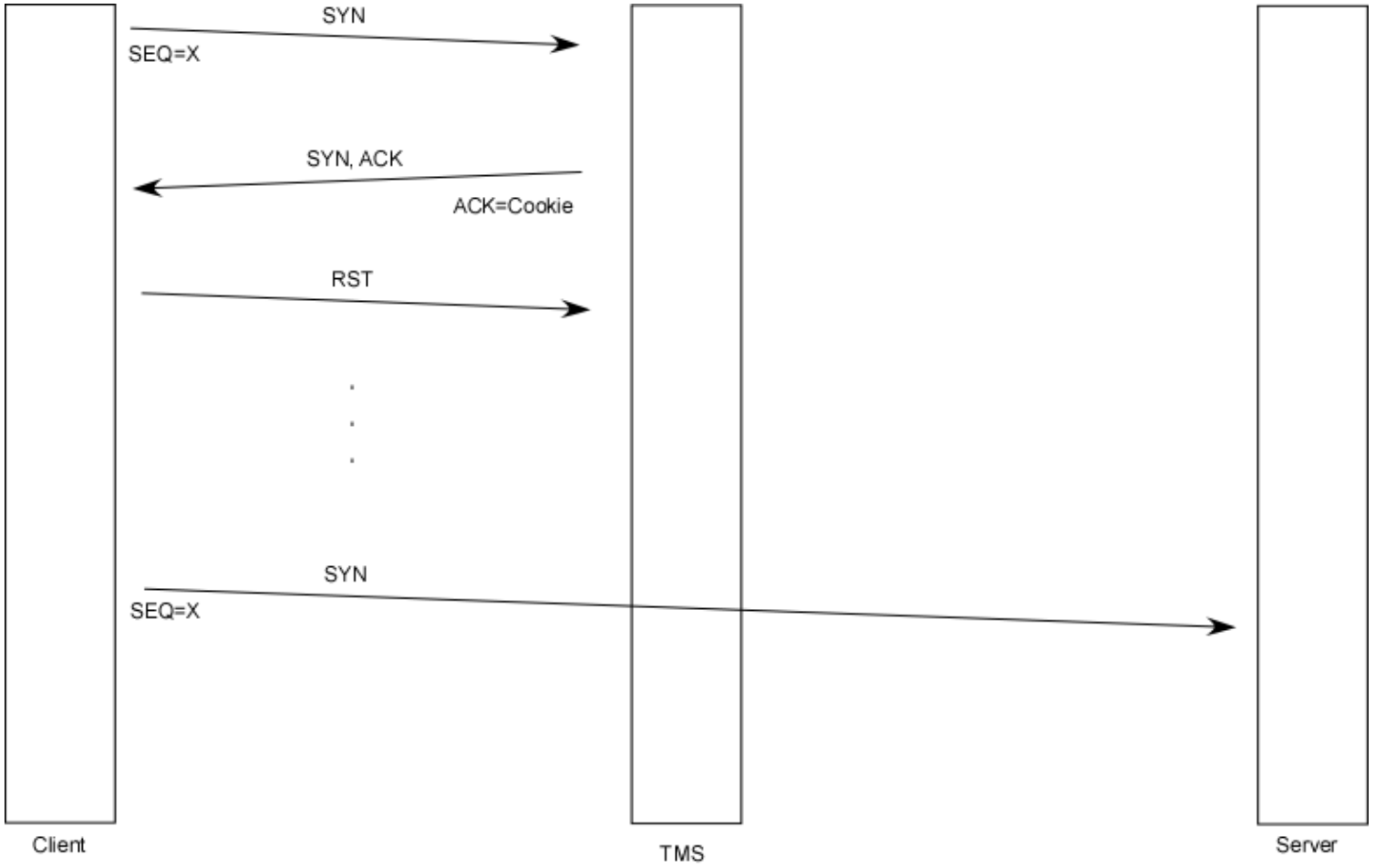
BEISPIEL: TCP SYN AUTHENTICATION

- Primär gegen SYN Flooding mit IP Spoofing
- SYN-Pakete werden nur weitergereicht, wenn der Absender valide ist
  - Reguläre Clients kommen auf eine Whitelist
- Mehrere Varianten:
  - TCP Reset
  - Out-of-Sequence Authentication
  - HTTP Authentication (nur für HTTP)
  - und weitere
- In allen Fällen wird eine Verbindung zwischen Absender und TMS aufgebaut. Die Varianten unterscheiden sich, wann und wie die TMS die Verbindung freigibt und den Client auf die Whitelist setzt.

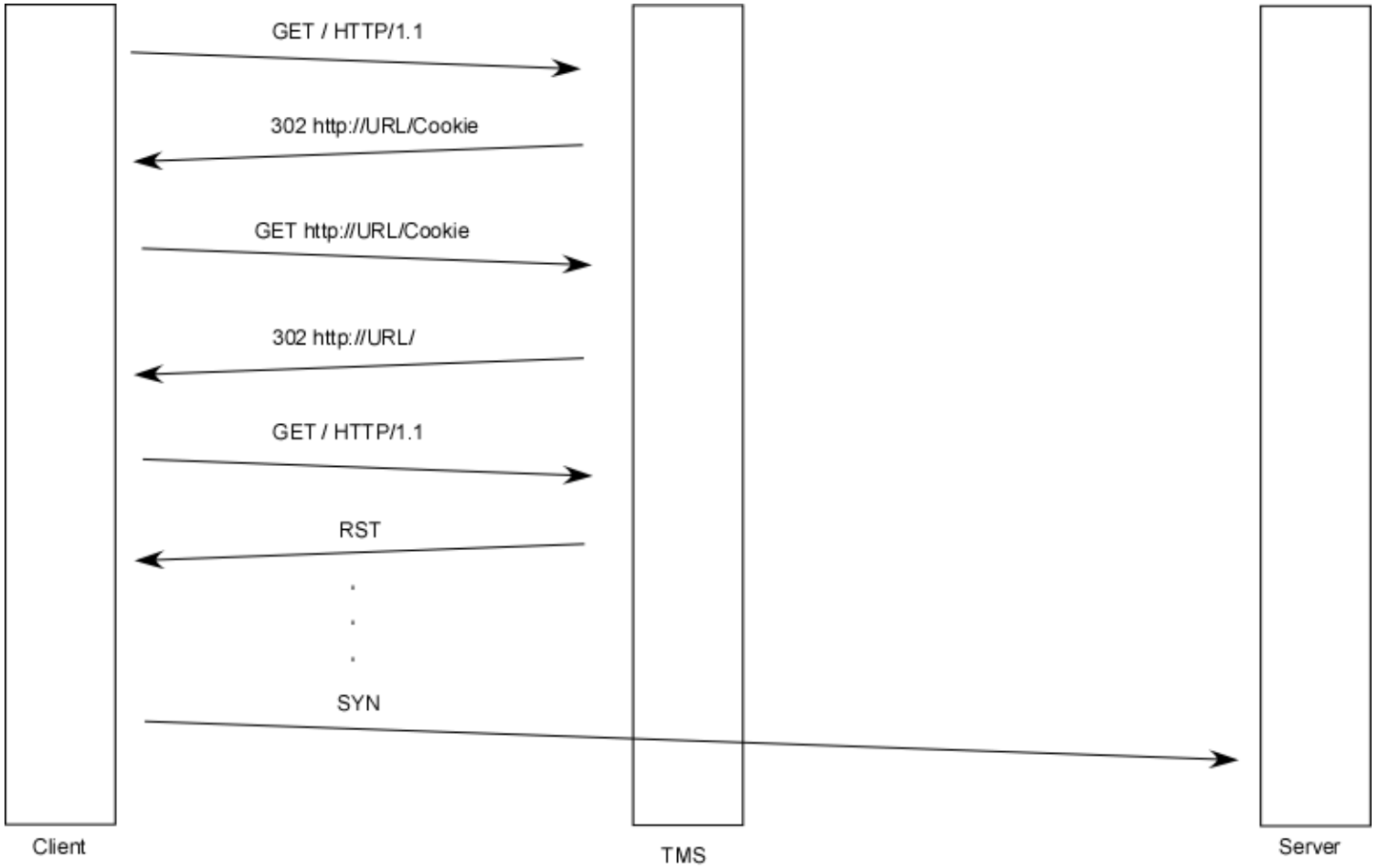
METHODE 1: TCP RESET



METHODE 2: OUT-OF-SEQUENCE AUTHENTICATION



METHODE 3: HTTP AUTHENTICATION



VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Dr. Carsten Löhn

Xantaro Deutschland GmbH | Hahnstraße 31-35 | 60528 Frankfurt a.M.

cloehn@xantaro.net