1 Border Gateway Protocol (BGP)

1.1 Grundlagen des Routings: LAN vs. Internet

Bevor BGP behandelt wird, ist es wichtig, den Unterschied zwischen lokalem Switching und globalem Routing zu verstehen.

1.2 Lokale Netzwerke (LAN)

In lokalen Netzen (Layer 2) erfolgt die Weiterleitung durch **Switches** basierend auf MAC-Adressen.

- **Funktionsweise:** Switches führen eine *Address Table* (MAC-Adresstabelle), die MAC-Adressen physischen Ports zuordnet.
- **Lernphase:** Ist die Ziel-MAC unbekannt, wird das Paket an *alle* Ports gesendet (*Flooding*). Antwortet der Empfänger, speichert der Switch die Port-Zuordnung.

1.3 Internet Routing

Das Internet basiert auf IP-Adressen (Layer 3). Hier übernehmen **Router** die Weiterleitung.

- **Routingtabelle:** Ordnet IP-Adressbereiche (**Prefixes**) bestimmten Ausgänge (Interfaces/Ports) zu.
- **Problemstellung:** Während Switches lokal lernen können, benötigt das Internet ein Protokoll, um Routingtabellen global auszutauschen. Hier kommt BGP ins Spiel.

1.4 Border Gateway Protocol (BGP)

Autonomes System (AS)

Ein **Autonomes System (AS)** ist ein Verbund von IP-Netzwerken, der unter der Kontrolle einer einzigen administrativen Instanz steht und eine einheitliche Routing-Policy verfolgt. Jedes AS wird durch eine eindeutige Nummer identifiziert, die **ASN** (Autonomous System Number).

Beispiele für AS sind ISPs (Deutsche Telekom), Content Provider (Google) oder große Institutionen (TU Darmstadt). Das Internet ist ein Verbund zehntausender solcher AS.

1.5 Funktionsweise von BGP

BGP organisiert die Kommunikation *zwischen* diesen Autonomen Systemen.

- **Protokoll-Typ:** BGP ist ein **Path-Vector-Protokoll**. Es speichert nicht nur die Kosten, sondern den gesamten Pfad (Liste der ASNs) zum Ziel, um Schleifen zu vermeiden.
- **Transport:** BGP nutzt **TCP Port 179** für eine zuverlässige Übertragung.
- **Peering:** Zwei Router bauen eine direkte Nachbarschaft auf („Peers“), um Routeninformationen auszutauschen.
- **NLRI:** Ausgetauscht werden *Network Layer Reachability Information* (Erreichbarkeitsinformationen für IP-Präfixe).

1.6 BGP Varianten

1. **External BGP (EBGP):** Verbindet Router in *unterschiedlichen* AS.
   - *Sicherheitsregel:* Die TTL (Time to Live) ist standardmäßig auf 1 gesetzt. Das erzwingt eine physische Direktverbindung.

2. **Internal BGP (IBGP):** Verbindet Router *innerhalb desselben* AS.
    - Dient dazu, extern gelernte Routen im eigenen Netz zu verteilen.
    - Erfordert oft ein Full-Mesh (jeder mit jedem) oder Route Reflectors.

1.7 Routing-Entscheidungen

BGP-Router müssen entscheiden, welchen Weg sie für ein Paket wählen, wenn mehrere Routen zum gleichen Ziel existieren. Die Hierarchie der Entscheidungskriterien ist für das Verständnis von Angriffen essenziell (Reihenfolge ist wichtig):

1. **Longest Prefix Match (Spezifität)**: Das spezifischere Präfix gewinnt *immer*.
    - *Beispiel:* AS2 kennt Route A zu 1.1.0.0/16 und Route B zu 1.1.1.0/24.
    - Obwohl 1.1.1.0 Teil von 1.1.0.0 ist, wird für eine IP wie 1.1.1.5 die Route B gewählt, da /24 spezifischer (länger) ist als /16.
    - **Wichtig:** Diese Regel schlägt alle anderen Metriken, sogar die Pfadlänge! Dies ist die Grundlage für *Sub-Prefix Hijacking*.
2. **Shortest AS Path**: Bei gleicher Präfix-Länge gewinnt die Route, die über weniger Autonome Systeme führt.

1.8 Angriffe gegen BGP

BGP wurde ursprünglich ohne Sicherheitsmechanismen entwickelt („Vertrauensbasis“). Dies ermöglicht verschiedene Angriffe.

1.9 BGP Hijacking

Ein Angreifer (ein feindliches AS) kündigt IP-Präfixe an, die ihm nicht gehören.

Hijacking Varianten

- **Same-prefix Hijack**: Der Angreifer kündigt exakt das gleiche Präfix an wie das Opfer (z.B. Opfer: 10.10.0.0/24, Angreifer: 10.10.0.0/24).
    - *Effekt:* Das Internet teilt sich auf. Nur Router, die "näher" (kürzerer AS-Pfad) am Angreifer sind, leiten den Verkehr falsch um.
- **Sub-prefix Hijack**: Der Angreifer kündigt ein *spezifischeres* Teilnetz an (z.B. Opfer: 10.10.0.0/24, Angreifer: 10.10.0.0/25).
    - *Effekt:* Aufgrund der *Longest Prefix Match*-Regel gewinnt der Angreifer global den gesamten Verkehr für dieses Subnetz, unabhängig von der Pfadlänge. Dies ist der mächtigere Angriff.

1.10 Weitere Angriffsvektoren

- **AS_PATH Fälschung:** Der Angreifer manipuliert den AS-Pfad in seinem Announcement, um legitim zu erscheinen (fügt z.B. das Opfer-AS in den Pfad ein), oder um Pfade künstlich attraktiv zu machen.
- **Route Leaks:** Ein AS verbreitet Routen, die es gelernt hat, versehentlich weiter (oft Konfigurationsfehler). Dies kann dazu führen, dass globaler Verkehr durch ein kleines, überlastetes Netz geleitet wird.

1.11 Ziele der Angriffe

- **Blackholing (DoS):** Verkehr wird angezogen und verworfen.
- **Redirection / Man-in-the-Middle:** Verkehr wird durch den Angreifer geleitet, analysiert/manipuliert und dann zum Ziel weitergeleitet (schwer zu entdecken).
- **Subversion:** Umgehen von Zensur oder Geolokalisierung.

1.12 Reale Angriffsbeispiele

Die Vorlesung nennt drei prominente Beispiele, die die theoretischen Konzepte verdeutlichen:

1. **KLAYswap (2022) - Redirection & Diebstahl:**
   - *Ziel:* Krypto-Dienst KLAYswap.
   - *Methode:* Angreifer hijackten den IP-Bereich einer Drittanbieter-Bibliothek (KakaoTalk Messenger), die von KLAYswap geladen wurde.
   - *Folge:* Der Angreifer lieferte schadhaften Code aus, da er durch den Hijack gültige SSL-Zertifikate ausstellen konnte. Nutzer überwiesen Krypto-Währung an den Angreifer.
2. **China Telecom (2015-2017) - Route Leak / Subversion:**
   - *Vorfall:* China Telecom kündigte sich fälschlicherweise als Transit-Provider für US-Netze (Verizon) an.
   - *Folge:* Inneramerikanischer Verkehr (USA → USA) wurde über China umgeleitet. Ermöglichte Spionage/-Analyse. Dauerte ca. 2,5 Jahre.
3. **Cloudflare / Eletronet (2024) - Blackholing:**
   - *Vorfall:* Ein kleiner brasilianischer ISP kündigte versehentlich (Route Leak) das spezifische Präfix 1.1.1.1/32 an.
   - *Mechanismus:* Cloudflare kündigt normalerweise 1.1.1.0/24 an. Da /32 spezifischer ist als /24, zog der brasilianische ISP den globalen DNS-Verkehr an.
   - *Ergebnis:* Globaler Ausfall des DNS-Dienstes 1.1.1.1.

1.13 Gegenmaßnahmen

Es gibt keinen eingebauten Schutz in BGP. Sicherheit muss "aufgesetzt" werden.

1.14 Organisatorische Basis

- **RIR (Regional Internet Registries):** Organisationen wie RIPE (Europa) verwalten IP-Adressen und ASNs.
- IP-Adressen sind Eigentum. Wer sie "besitzt", darf sie announcen.

1.15 Internet Routing Registry (IRR)

Ein Netzwerk verteilter Datenbanken, in denen Betreiber dokumentieren, welche Routen ihnen gehören.

- **Problem:** Rein manuell gepflegt, oft veraltet, ungenau. Dient nur als sekundäre Informationsquelle.

1.16 Resource Public Key Infrastructure (RPKI)

Der aktuelle Standard zur Absicherung des *Ursprungs* (Origin) einer Route. Nutzt Kryptographie.

1. **ROA (Route Origin Authorization):** Ein kryptografisch signiertes Objekt in der RPKI-Datenbank. Es legt fest:
   - Welches **AS** darf das Präfix announcen? (Origin ASN)
   - Welches **Präfix** (z.B. 10.20.0.0/16)?
   - **Max Length:** Die maximal erlaubte Präfixlänge (z.B. /24). Verhindert Sub-Prefix Hijacking.
2. **ROV (Route Origin Validation):** Der Router lädt ROAs herunter und prüft eingehende BGP-Announcements.
   - **Valid**: Announcement stimmt mit ROA überein. → Route wird akzeptiert.
   - **Invalid**: AS stimmt nicht oder Präfix ist spezifischer als *Max Length* erlaubt. → Route wird verworfen ("Do Not Route").

- **Not Found**: Keine ROA vorhanden. → Route wird meist akzeptiert (da RPKI noch nicht flächendeckend ist).

Grenzen von RPKI

RPKI schützt nur den **Origin** (Wer darf announcen?). Es schützt **nicht** den Pfad (**AS_PATH**).

- Ein Angreifer kann immer noch den Pfad manipulieren, solange er den korrekten Ursprung im Announcement lässt (Path-Manipulation ist weiterhin möglich).
- Implementierungsfehler in Routern können RPKI wirkungslos machen.

1.17 BGPSec

Eine Erweiterung, um auch den Pfad zu schützen.

- **Konzept:** Jedes AS signiert kryptografisch das Announcement an das nächste AS. Es entsteht eine lückenlose Signaturkette.
- **Vorteil:** Schützt vor Pfad-Manipulationen und AS-Spoofing.
- **Nachteile (Warum es kaum genutzt wird):**
  - Sehr hoher Rechenaufwand auf den Routern.
  - Erfordert lückenlose Unterstützung: Wenn ein Router im Pfad kein BGPSec spricht, bricht die Kette ("Chain of Trust").