Sicherheit im Internet Backbone

Anwendungen 1

Jan Henke

HAW Hamburg

10. November 2011

Gliederung

Gliederung

Autonome Systeme (AS)

Definition

Ein Autonomes System (*AS*) ist ein Netzwerk, welches ein internes Routingprotokoll benutzt, unter einer administrativen Verwaltung steht und über Verbindung zu mindestens zwei anderen AS verfügt.

Autonome Systeme (AS)

Definition

Ein Autonomes System (*AS*) ist ein Netzwerk, welches ein internes Routingprotokoll benutzt, unter einer administrativen Verwaltung steht und über Verbindung zu mindestens zwei anderen AS verfügt.

- weltweit eindeutige AS-Nummer (*ASN*)

Autonome Systeme (AS)

Definition

Ein Autonomes System (*AS*) ist ein Netzwerk, welches ein internes Routingprotokoll benutzt, unter einer administrativen Verwaltung steht und über Verbindung zu mindestens zwei anderen AS verfügt.

- weltweit eindeutige AS-Nummer (*ASN*)
- Internet Backbone -> alle inter-AS-Verbindungen

Autonome Systeme (AS)

Definition

Ein Autonomes System (*AS*) ist ein Netzwerk, welches ein internes Routingprotokoll benutzt, unter einer administrativen Verwaltung steht und über Verbindung zu mindestens zwei anderen AS verfügt.

- weltweit eindeutige AS-Nummer (*ASN*)
- Internet Backbone -> alle inter-AS-Verbindungen
- *Edge-Routern* -> Verbindungen zwischen ASen

Das Border Gateway Protocol(BGP)

- Das Border Gateway Protocol (*BGP*)
  - Pfadvektorprotokoll.

Das Border Gateway Protocol(BGP)

- Das Border Gateway Protocol (*BGP*)
  - Pfadvektorprotokoll.
  - Standardprotokoll für Inter-AS-Routing

Das Border Gateway Protocol(BGP)

- Das Border Gateway Protocol (*BGP*)
  - Pfadvektorprotokoll.
  - Standardprotokoll für Inter-AS-Routing
  - wird direkt zwischen zwei Edge-Routern gesprochen

Das Border Gateway Protocol(BGP)

- Das Border Gateway Protocol (*BGP*)
  - Pfadvektorprotokoll.
  - Standardprotokoll für Inter-AS-Routing
  - wird direkt zwischen zwei Edge-Routern gesprochen
  - basiert auf IP-Präfixen

Das Border Gateway Protocol(BGP)

- Das Border Gateway Protocol (*BGP*)
  - Pfadvektorprotokoll.
  - Standardprotokoll für Inter-AS-Routing
  - wird direkt zwischen zwei Edge-Routern gesprochen
  - basiert auf IP-Präfixen
- Export bester Routen an Nachbarn via *Update Nachrichten*

Update Nachrichten

- Mitteilung über neue (Announcement) oder zurückgezogene (Withdrawal) Routen

Update Nachrichten

- Mitteilung über neue (Announcement) oder zurückgezogene (Withdrawal) Routen
- Präfix und *AS-Pfad*

Update Nachrichten

- Mitteilung über neue (Announcement) oder zurückgezogene (Withdrawal) Routen
- Präfix und *AS-Pfad*
- Jeder Edge-Router fügt sein eigenes AS am Anfang des AS-Pfades ein

Update Nachrichten

- Mitteilung über neue (Announcement) oder zurückgezogene (Withdrawal) Routen
- Präfix und *AS-Pfad*
- Jeder Edge-Router fügt sein eigenes AS am Anfang des AS-Pfades ein
- Letztes AS des Pfad ist das *Origin-AS*

Update Nachrichten

- Mitteilung über neue (Announcement) oder zurückgezogene (Withdrawal) Routen
- Präfix und *AS-Pfad*
- Jeder Edge-Router fügt sein eigenes AS am Anfang des AS-Pfades ein
- Letztes AS des Pfad ist das *Origin-AS*
- Kennt ein Router mehre Routen zum selben Ziel, wird u.a. die Länge des jeweiligen AS-Pfads berücksichtigt

AS Beziehungen

- Beziehungen zwischen zwei ASen:
  - Kunde-Provider

AS Beziehungen

- Beziehungen zwischen zwei ASen:
  - Kunde-Provider
  - Peering

AS Beziehungen

- Beziehungen zwischen zwei ASen:
  - Kunde-Provider
  - Peering
  - "Geschwister"

AS Beziehungen

- Beziehungen zwischen zwei ASen:
  - Kunde-Provider
  - Peering
  - "Geschwister"
- Beziehung bestimmt Export Policy

AS Beziehungen

- Beziehungen zwischen zwei ASen:
  - Kunde-Provider
  - Peering
  - "Geschwister"
- Beziehung bestimmt Export Policy
- Policy Violation -> Routinganomalie

Routinganomalien

- Umleitung von IP-Verkehr

Routinganomalien

- Umleitung von IP-Verkehr
- Ursache:
  - Fehlkonfiguration -> *Prefix leak*

Routinganomalien

- Umleitung von IP-Verkehr
- Ursache:
  - Fehlkonfiguration -> *Prefix leak*
  - Absicht -> *Prefix hijack*

Routinganomalien

- Umleitung von IP-Verkehr
- Ursache:
  - Fehlkonfiguration -> *Prefix leak*
  - Absicht -> *Prefix hijack*
- Klassen von Routingangriffen:
  - Origin AS

Routinganomalien

- Umleitung von IP-Verkehr
- Ursache:
  - Fehlkonfiguration -> *Prefix leak*
  - Absicht -> *Prefix hijack*
- Klassen von Routingangriffen:
  - Origin AS
  - AS Path

Gliederung

Origin AS Angriff

- Ziel: Verkehr des Zielpräfixes erhalten

Origin AS Angriff

- Ziel: Verkehr des Zielpräfixes erhalten
- BGP: keine Validierung des Origin AS

Origin AS Angriff

- Ziel: Verkehr des Zielpräfixes erhalten
- BGP: keine Validierung des Origin AS
- Longest Prefix Routing -> Subnet prefix hijack erhält gesamten Verkehr

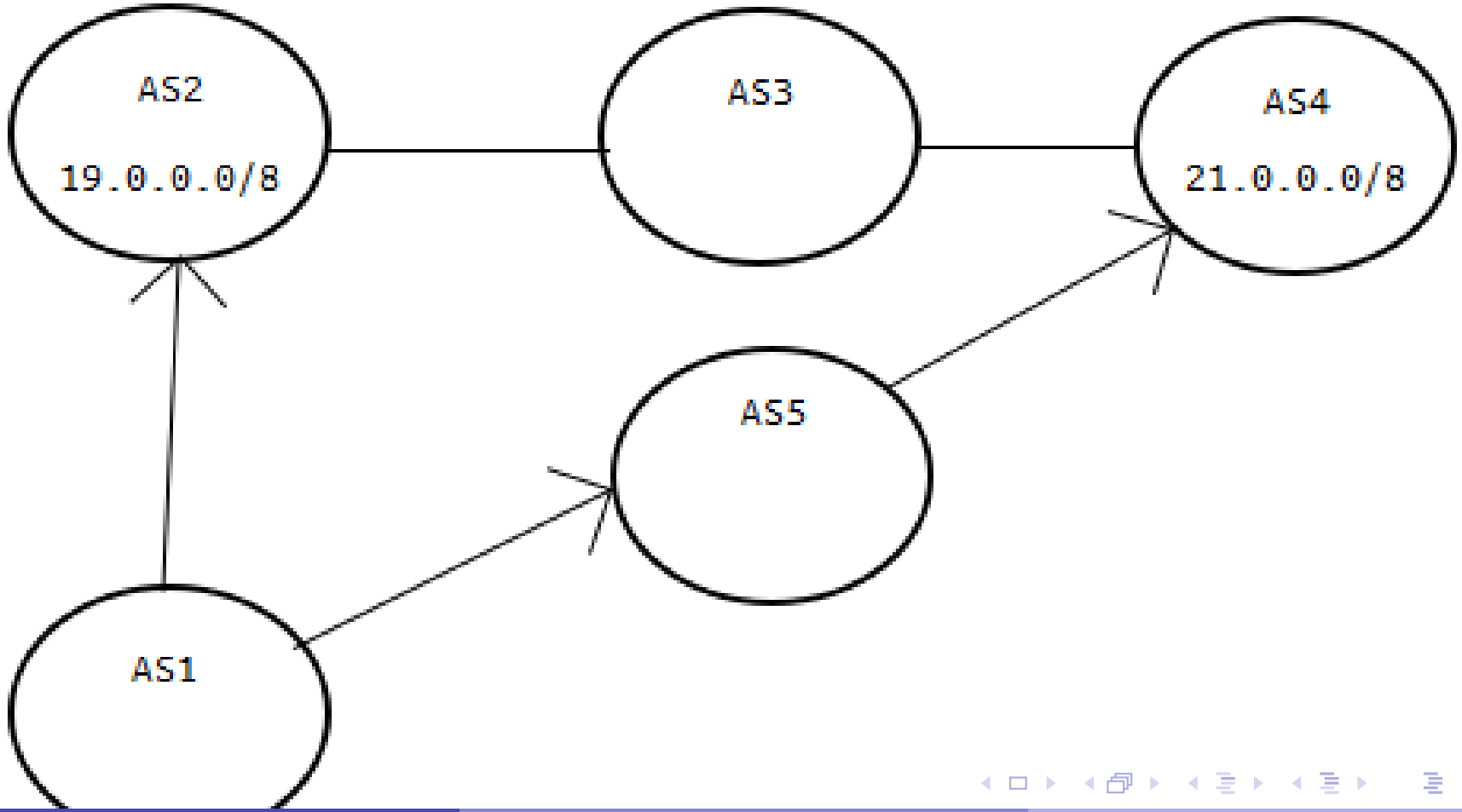
Origin AS Angriff

- Ziel: Verkehr des Zielpräfixes erhalten
- BGP: keine Validierung des Origin AS
- Longest Prefix Routing -> Subnet prefix hijack erhält gesamten Verkehr
- Unterbinden: geschickte Routenfilterung

Origin AS Angriff

- Ziel: Verkehr des Zielpräfixes erhalten
- BGP: keine Validierung des Origin AS
- Longest Prefix Routing -> Subnet prefix hijack erhält gesamten Verkehr
- Unterbinden: geschickte Routenfilterung
- -> *Beispiel*

Beispiel



Gliederung

AS Path Angriffe

- Ziel: Verkehr eines anderen ASes erhalten

AS Path Angriffe

- Ziel: Verkehr eines anderen ASes erhalten
- ungültige Pfade:
  - gefälschte Kante oder ASN

AS Path Angriffe

- Ziel: Verkehr eines anderen ASes erhalten
- ungültige Pfade:
  - gefälschte Kante oder ASN
  - Verletzung der Export Policy

AS Path Angriffe

- Ziel: Verkehr eines anderen ASes erhalten
- ungültige Pfade:
  - gefälschte Kante oder ASN
  - Verletzung der Export Policy
- Typen:
  - gefälschter kürzester Pfad

AS Path Angriffe

- Ziel: Verkehr eines anderen ASes erhalten
- ungültige Pfade:
  - gefälschte Kante oder ASN
  - Verletzung der Export Policy
- Typen:
  - gefälschter kürzester Pfad
  - gültiger kürzester Pfad

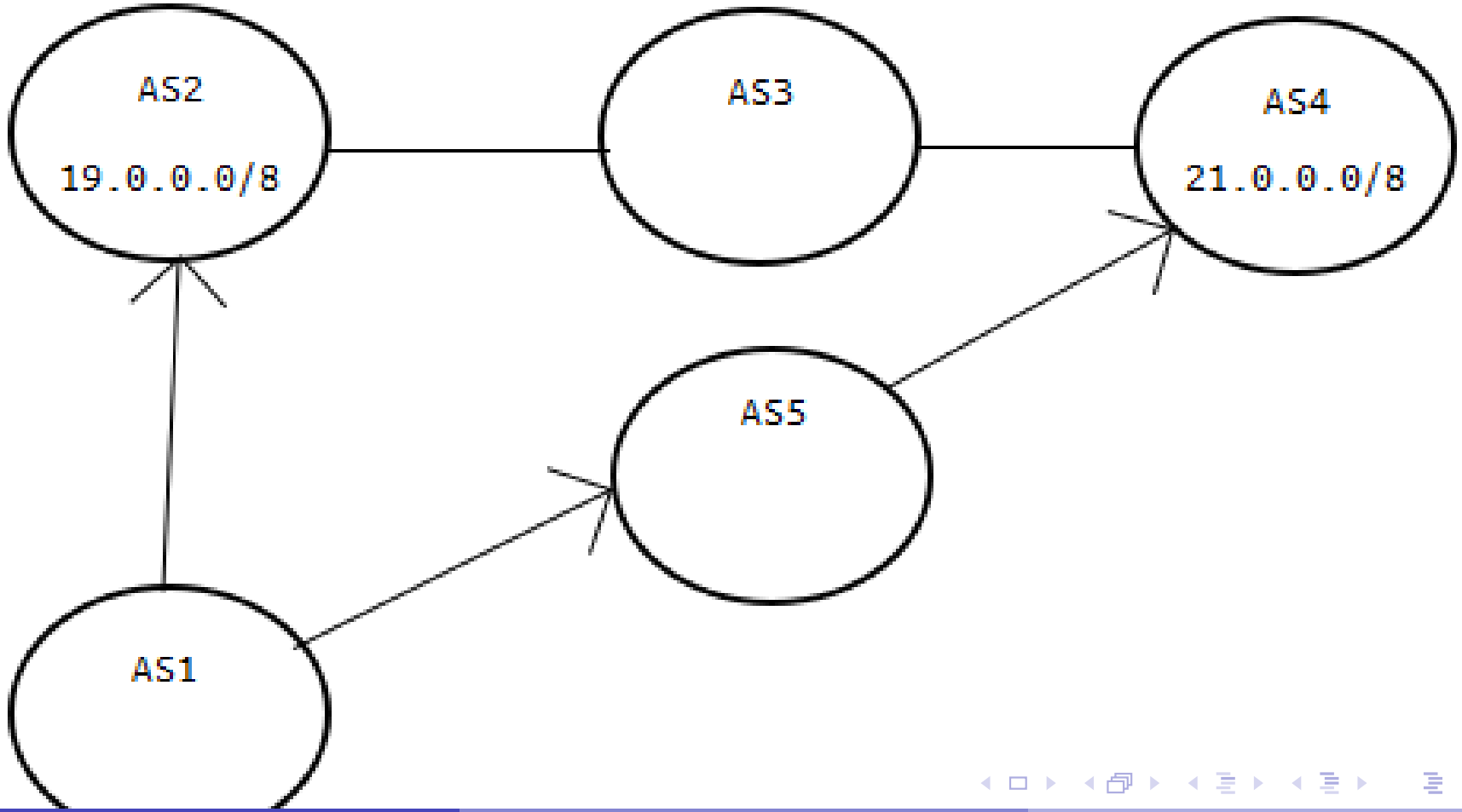
AS Path Angriffe

- Ziel: Verkehr eines anderen ASes erhalten
- ungültige Pfade:
  - gefälschte Kante oder ASN
  - Verletzung der Export Policy
- Typen:
  - gefälschter kürzester Pfad
  - gültiger kürzester Pfad
  - Weiterverteilung

AS Path Angriffe

- Ziel: Verkehr eines anderen ASes erhalten
- ungültige Pfade:
  - gefälschte Kante oder ASN
  - Verletzung der Export Policy
- Typen:
  - gefälschter kürzester Pfad
  - gültiger kürzester Pfad
  - Weiterverteilung
  - ASN Fälschung

Beispiel



Ausblick

- Feld aktueller Forschung und Diskussion

Ausblick

- Feld aktueller Forschung und Diskussion
- Vielzahl unterschiedlicher Vorschläge

Ausblick

- Feld aktueller Forschung und Diskussion
- Vielzahl unterschiedlicher Vorschläge
- Resource Public Key Infrastructure (RPKI)

Ausblick

- Feld aktueller Forschung und Diskussion
- Vielzahl unterschiedlicher Vorschläge
- Resource Public Key Infrastructure (RPKI)
  - Validierung von IP prefixen/ASN

Ausblick

- Feld aktueller Forschung und Diskussion
- Vielzahl unterschiedlicher Vorschläge
- Resource Public Key Infrastructure (RPKI)
  - Validierung von IP prefixen/ASN
  - Bibliothek in Entwicklung an der HAW

Ausblick

- Feld aktueller Forschung und Diskussion
- Vielzahl unterschiedlicher Vorschläge
- Resource Public Key Infrastructure (RPKI)
  - Validierung von IP prefixen/ASN
  - Bibliothek in Entwicklung an der HAW
  - Weitere Tätigkeiten: Validierung der Bibliothek

Fragen/Diskussion

Danke für eure Aufmerksamkeit.
Sind noch Fragen offen?

Literatur I

Barbir, A. ; Murphy, S. ; Yang, Y.:
Generic Threats to Routing Protocols.
RFC 4593 (Informational).
`http://www.ietf.org/rfc/rfc4593.txt`.
Version: Oktober 2006 (Request for Comments)

Literatur II

Butler, K. ; Farley, T.R. ; McDaniel, P. ; Rexford, J.:
A Survey of BGP Security Issues and Solutions.
In: *Proceedings of the IEEE* 98 (2010), jan., Nr. 1, S. 100 –122.
http://dx.doi.org/10.1109/JPROC.2009.2034031. –
DOI 10.1109/JPROC.2009.2034031. –
ISSN 0018–9219

Gao, Lixin:
On inferring autonomous system relationships in the Internet.
In: *Global Telecommunications Conference, 2000. GLOBECOM '00. IEEE* Bd. 1, 2000, S. 387 –396 vol.1

Literatur III

Karlin, Josh ; Forrest, Stephanie ; Rexford, Jennifer:
Autonomous security for autonomous systems.
In: *Computer Networks* 52 (2008), Nr. 15, 2908 - 2923.
http://dx.doi.org/10.1016/j.comnet.2008.06.012. –
DOI 10.1016/j.comnet.2008.06.012. –
ISSN 1389–1286. –
<ce:title>Complex Computer and Communication Networks</ce:title>

Qiu, Jian ; Gao, Lixin ; Ranjan, Supranamaya ; Nucci, Antonio:
Detecting bogus BGP route information: Going beyond prefix hijacking.
In: *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, 2007, S. 381 –390

Literatur IV


Rekhter, Y. ; Li, T. ; Hares, S.:
A Border Gateway Protocol 4 (BGP-4).
RFC 4271 (Draft Standard).
`http://www.ietf.org/rfc/rfc4271.txt`.
Version: Januar 2006 (Request for Comments). –
Updated by RFC 6286