Wirkungsanalyse von Routing-Angriffen im Internet

Anwendungen 2

Jan Henke

HAW Hamburg

26. April 2012

Outline

Erkenntnisse aus AW1

- Interdomain-Verkehr im Internet wird mittels BGP[1] gerouted
- BGP arbeitet auf Autonomenen Systemen(AS) als Hierarchisierung der Internet-Topologie
- Jeder Router hat eine unterschiedliche (lokale) Sicht auf die AS-Topologie
- BGP ist anfällig für verschiedene Arten von Angriffen
- Durch die Wichtigkeit des Internets wird diese Anfälligkeit zu einem immer größeren Problem

Arten von Angriffen

- Longest common Prefix
- Invalid Origin
- Invalid Next Hop

RPKI kann die ersten beiden Angriffsarten unterbinden.[2]

Arten von Angriffen

- Longest common Prefix
- Invalid Origin
- Invalid Next Hop

RPKI kann die ersten beiden Angriffsarten unterbinden.[2]

Auswirkung von Routing-Angriffen

- Der Erfolg eines Angriffs ist abhängig von der relativen Position von Angreifer und Opfer zueinander innerhalb der Routing-Topologie
- Die gefälschte Route soll von möglichst vielen AS genutzt werden
- Eine theoretische Abschätzung hilft daher bei:
  - der Einschätzung möglicher Angriffspunkte
  - der Analyse laufender oder zurückliegender Angriffe
  - der Durchführung eines Angriffes

Studie von Francis et. al.[3] I

- Analysiert Verbreitungswege von gefälschten BGP-Updates in der Routing-Topologie
- Aus dem Jahre 2007, basiert auf dem Topologie-Modell von Lixin Gao aus dem Jahre 2001
- Unterscheidet zwischen *Hijacking* und *Intercepting*

Studie von Francis et. al.[3] II

- Hijacking:
  - Einfacher zu realisieren
  - Daten werden einfach verworfen
  - Aber: Opfer kann den Angriff relativ leicht entdecken
- Intercepting:
  - Benötigt intakte Route vom Angreifer zum Opfer
  - Daten werden zum eigentlichen Ziel weitergeleitet
  - Dadurch wesentlich schwerer zu entdecken

Studie von Francis et. al.[3] III

- Grundlage für das weitere Vorgehen
- Aber, die Ergebnisse sind teilweise überholt, durch Evolution der Routing-Topologie
- Untersucht keine verteilte Attacken

Topologiemodell nach Gao[4] I

- Ein Topologie-Modell erstellt durch Analyse empirischer Daten
- Analysiert die Verbindung zwischen der wirtschaftlichen Beziehung zweier AS und deren Beziehung auf Routing-Ebene
- Alle Beziehungen lassen sich in eine dieser vier Klassen einordnen:
  - Kunde-Provider
  - Provider-Kunde
  - Peering
  - „Geschwister“-AS

Topologiemodell nach Gao[4] II

- Die Beziehung bestimmt wie sich BGP-Updates in der Topologie verteilen
- Datenbasis von 2001 $\rightarrow$ Bildet die Entwicklung der letzten Jahre nicht ab

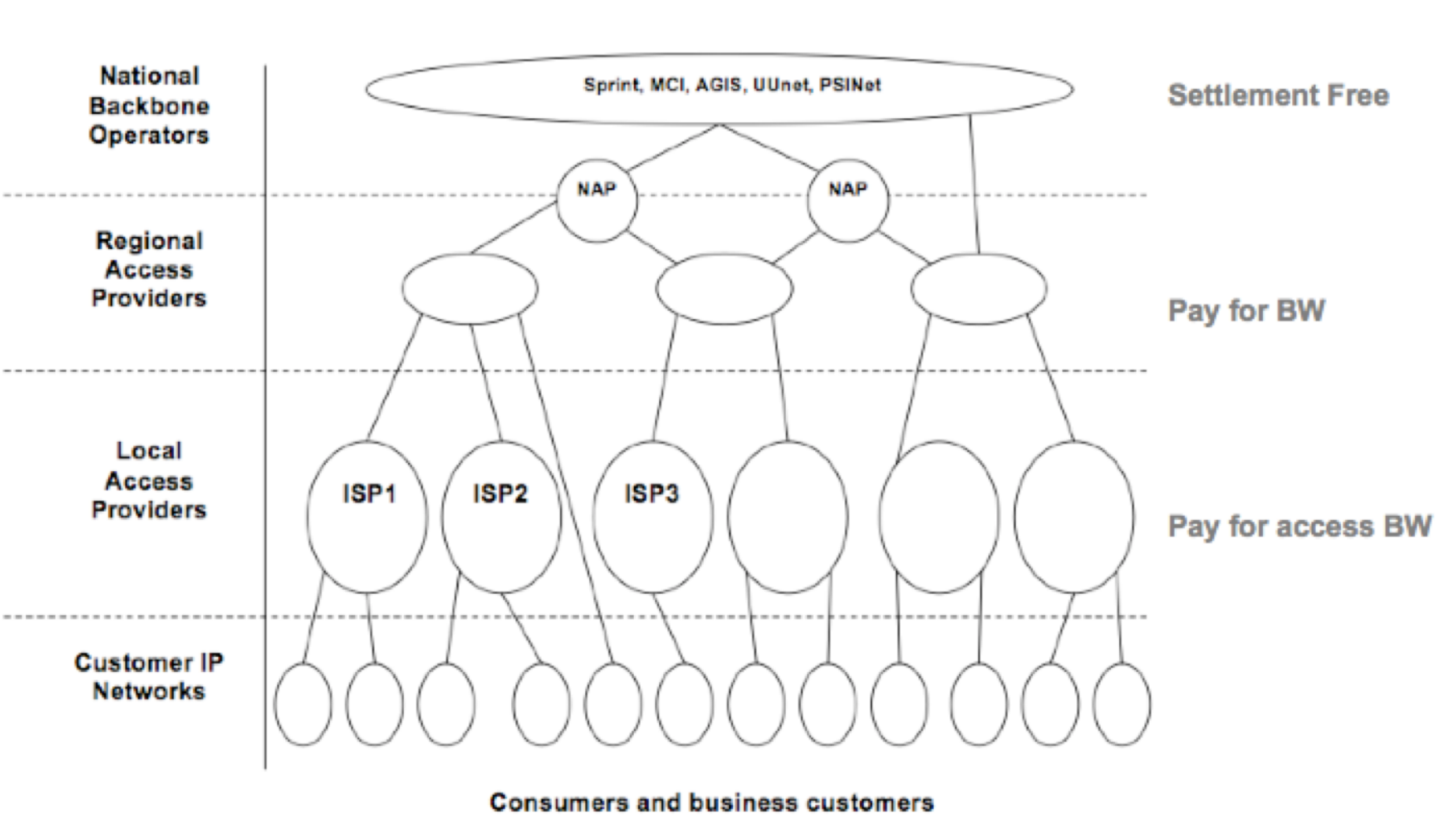

Abbildung: Klassische Routing-Topologie, Quelle: [5]

Aktuelle Einflüsse auf die Routing-Topologie

Zwei Einflüsse haben die Routing-Topologie in den letzten Jahren stark verändert:

- Die zunehmende Bedeutung von IXPs
- Große Content-Provider suchen direkten Anschluss an die Consumer-Netzwerke

Der Aufstieg der Internet-Exchange-Points (IXPs) I

- IXPs gibt es schon seit längerer Zeit
- Ihre Bedeutung ist in den letzten Jahren stark gewachsen
- Immer mehr Firmen bevorzugen die Anbindung an (mehrere) IXPs gegenüber eines direkten Peerings

Der Aufstieg der Internet-Exchange-Points (IXPs) II

- Vorteile:
  - Geringere Kosten
  - Einfacherer Zugang zu neuen Peering-Vereinbarungen
- Konsequenzen:
  - Peering wird auch für kleine ISPs ermöglicht
  - Es gibt wesentlich mehr „Querverbindungen“, welche die Tier-1 oder Tier-2 ISPs umgehen

Konzentration der Datenströme

- Spezialisierte Contentprovider (z.B. Google, Facebook, CDNs) wachsen überproportional und verursachen einen steigenden Anteil am weltweiten inter-domain Datenvolumen
- Über eigene Netze und die IXPs suchen die Contentprovider das direkte Peering mit den Consumer-Netzwerken

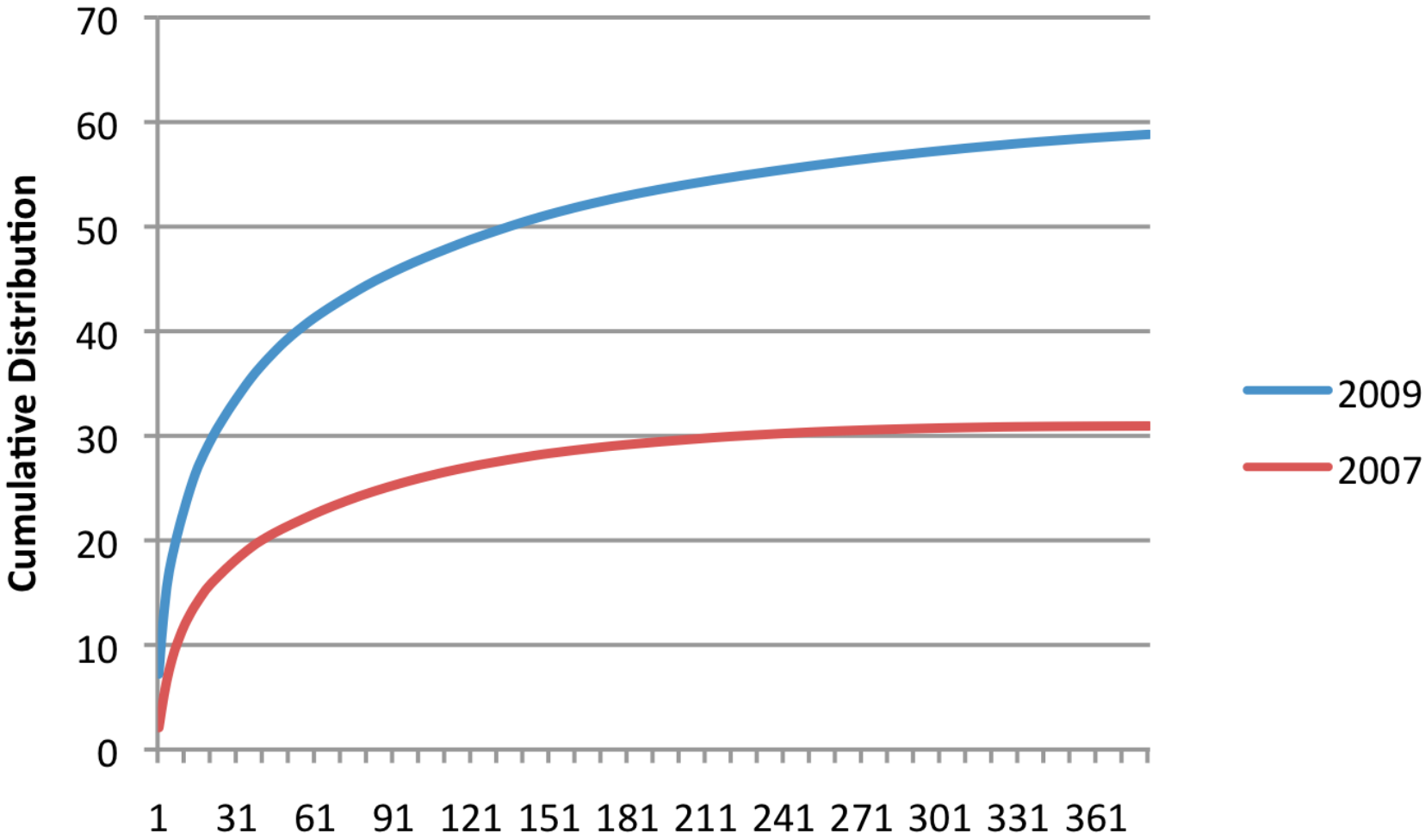

Abbildung: Anzahl ASN vs. Anteil am globalen inter-domain Verkehr, Quelle: [5]

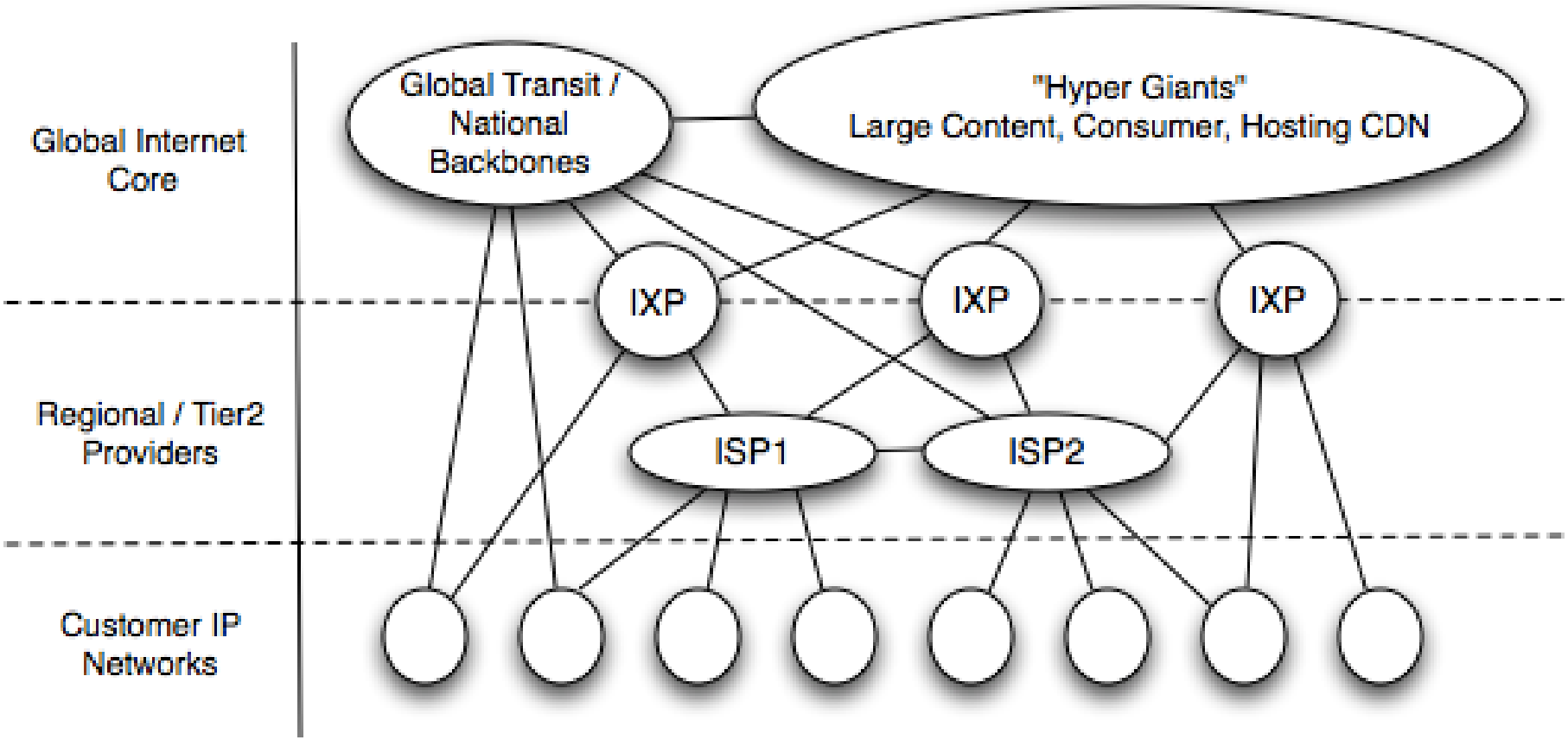

Abbildung: Aktuelle Routing-Topologie, Quelle: [5]

Fazit

- In Anbetracht der Anfälligkeit von BGP ist es wichtig die Auswirkungen von Angriffe zu verstehen und vorhersagen zu können
- Es gibt bestehende Arbeiten zu dem Thema, diesen fehlt jedoch:
  - Die Berücksichtigung der Veränderungen in der Routing-Topologie der letzten Jahre
  - Eine Untersuchung verteilter Angriffe, alle bisherigen Arbeiten gehen von einem einzelnen Angreifer aus

Literatur


Y. Rekhter, T. Li, and S. Hares, "A Border Gateway Protocol 4 (BGP-4)," IETF, RFC 4271, January 2006.


M. Lepinski and S. Kent, "An Infrastructure to Support Secure Internet Routing," IETF, RFC 6480, February 2012.


H. Ballani, P. Francis, and X. Zhang, "A Study of Prefix Hijacking and Interception in the Internet," in *Proc. of SIGCOMM '07*. New York, NY, USA: ACM, 2007, pp. 265–276.


L. Gao, "On Inferring Autonomous System Relationships in the Internet," *IEEE/ACM Trans. Netw.*, vol. 9, no. 6, pp. 733–745, 2001.


C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, "Internet Inter-domain Traffic," in *Proc. of the ACM SIGCOMM '10*. New York, NY, USA: ACM, 2010, pp. 75–86.

Danke für die Aufmerksamkeit. Sind noch Fragen offen?