18. Februar 2013

Fraunhofer
FKIE

Visibility of Routing Anomalies for End Users

Matthias Wübbeling

Fraunhofer FKIE
D-53113 Bonn

wueb@cs.uni-bonn.de

Organisation und Struktur des Internet

© CyberDefense Research Group, Fraunhofer FKIE

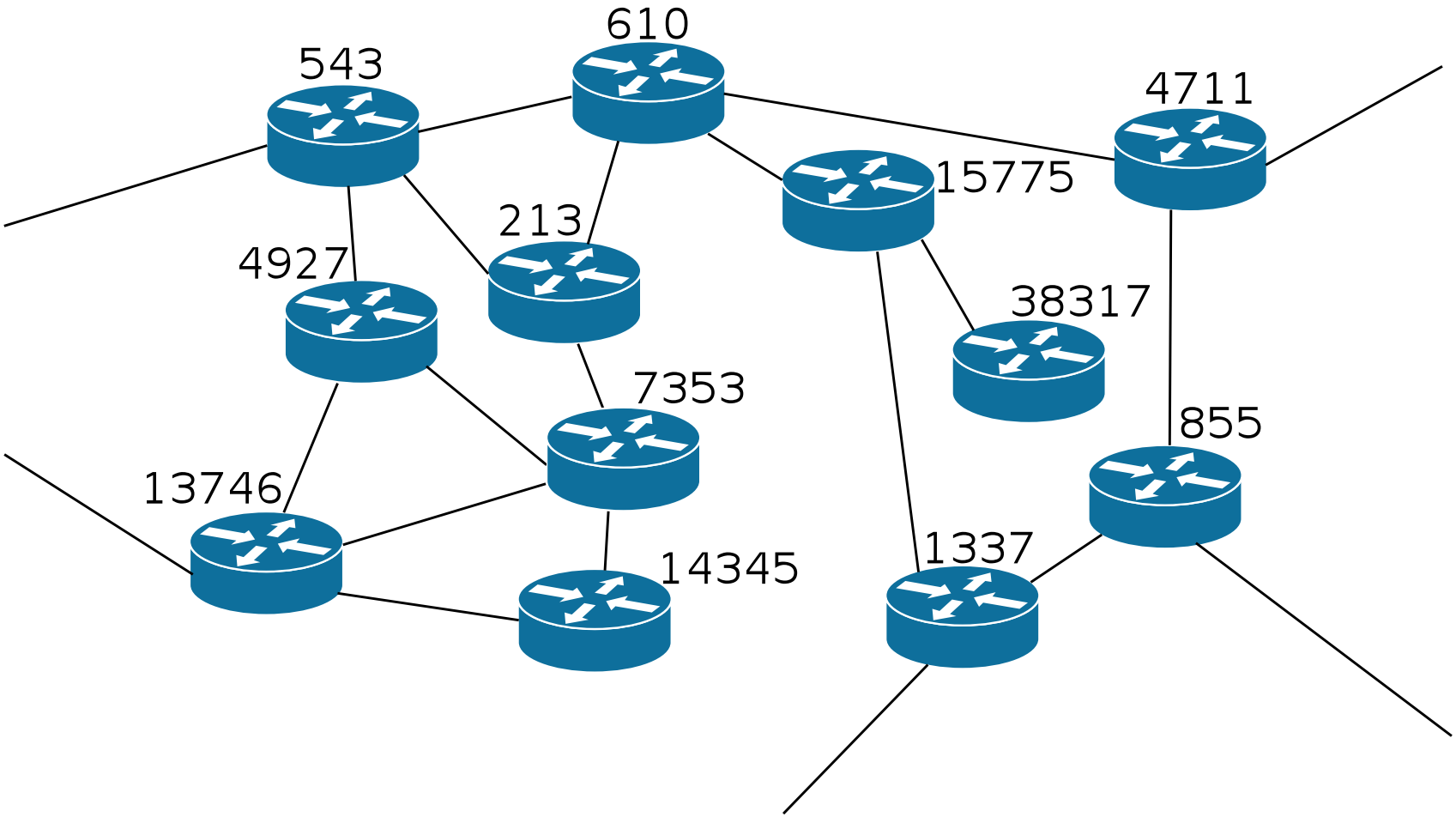
Fraunhofer FKIE

Organisation und Struktur des Internet

© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE

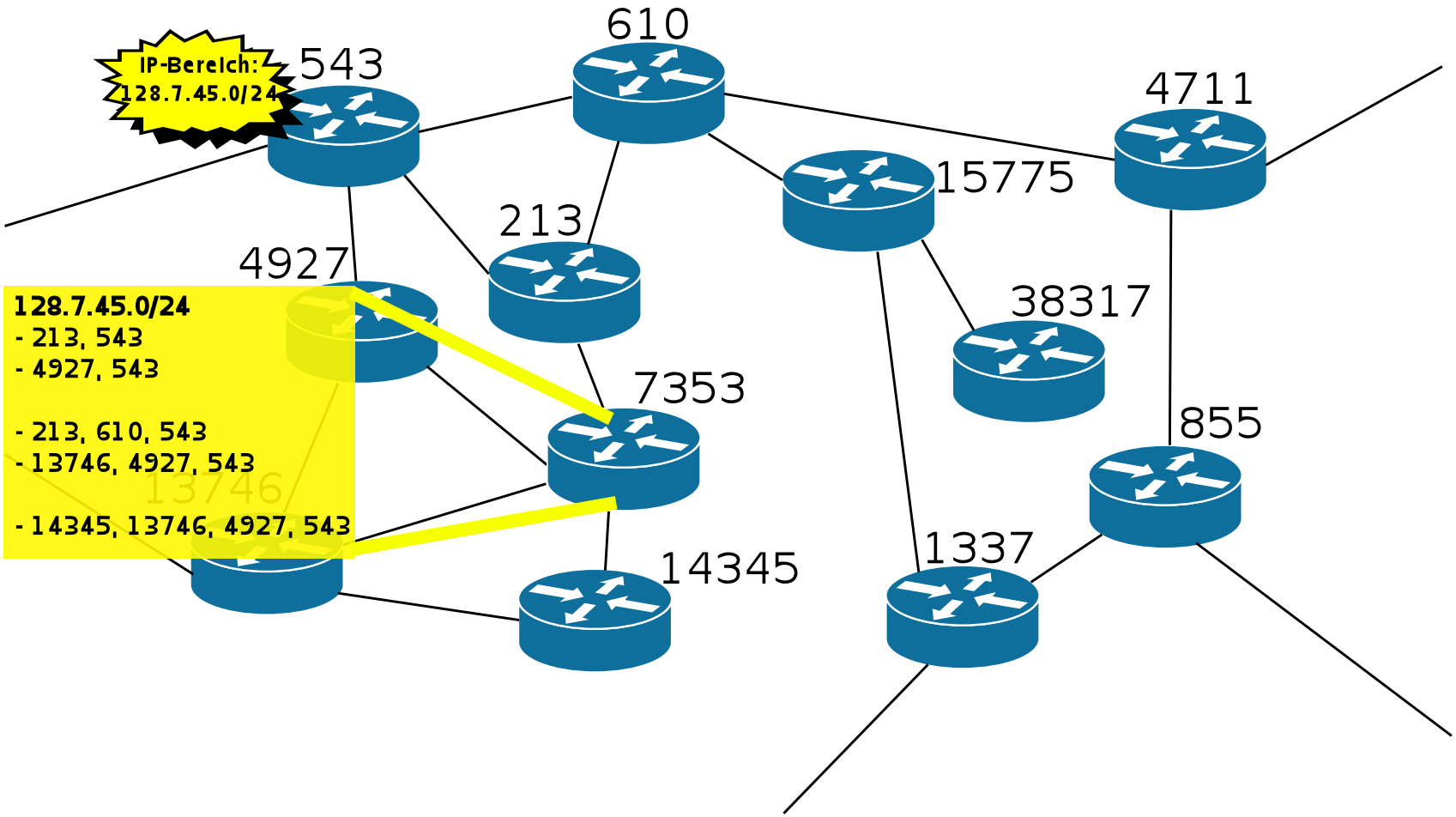
Organisation und Struktur des Internet



© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE

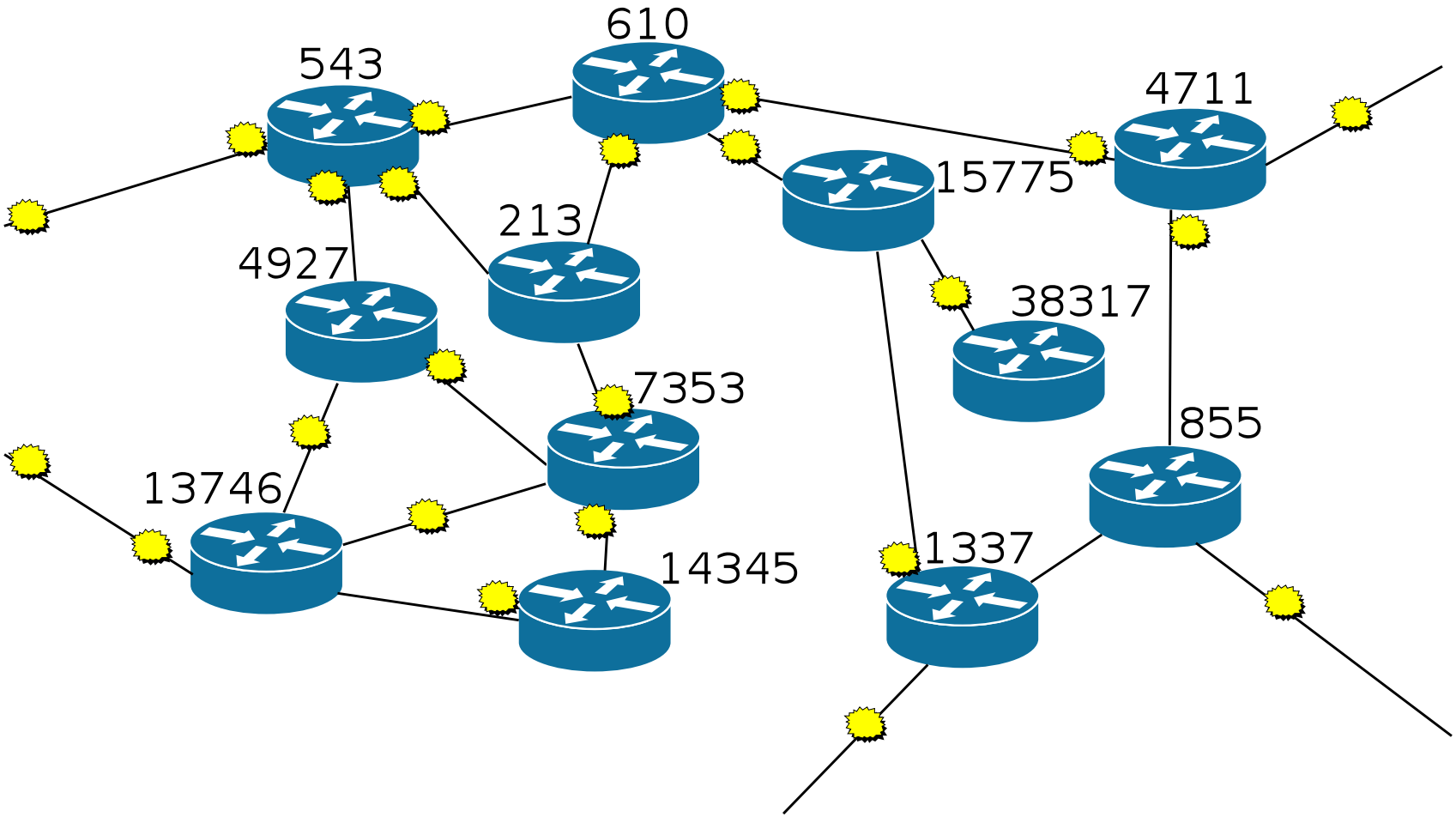
Inter-AS-Routing



© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE

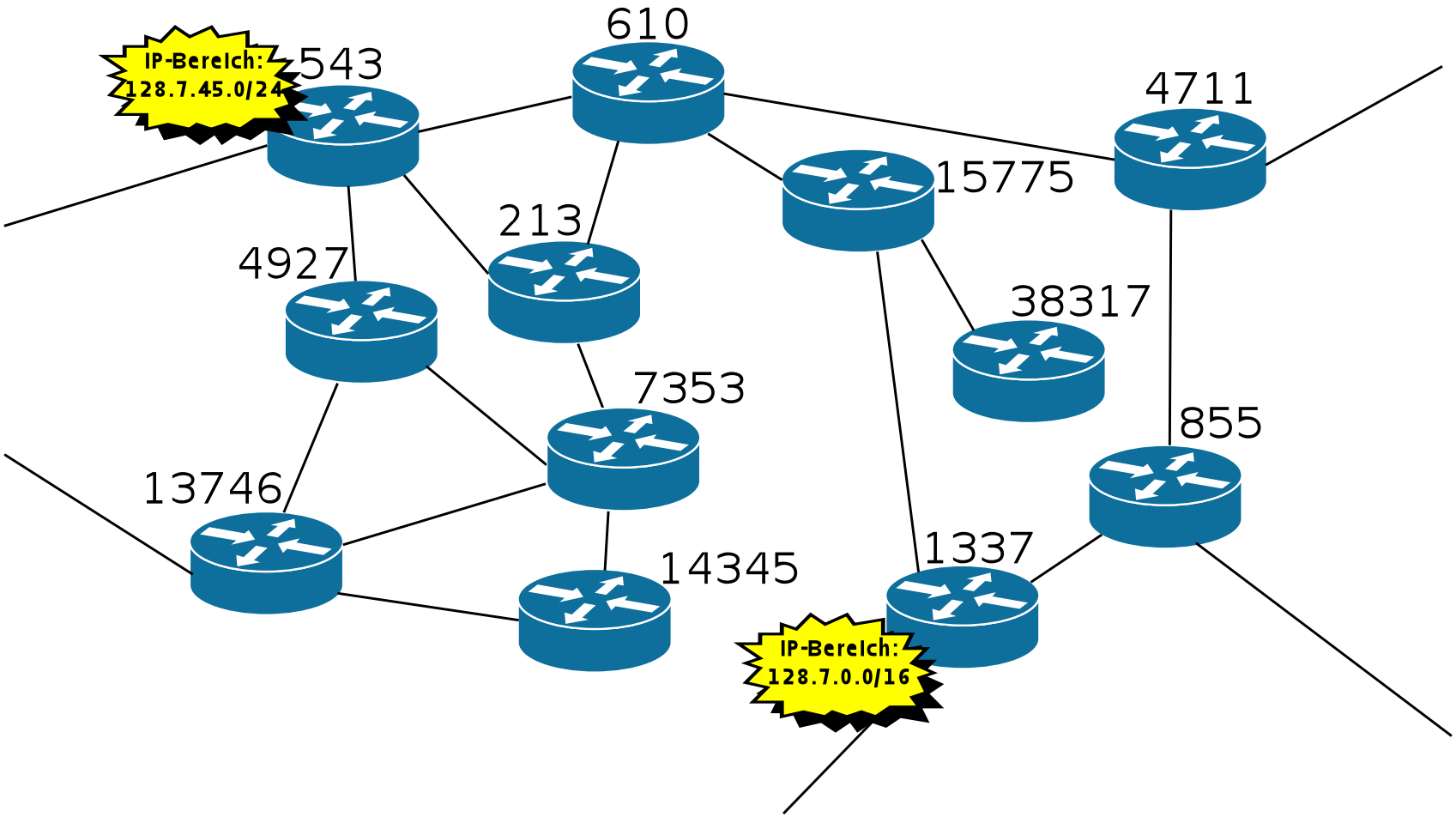
Inter-AS-Routing



© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE

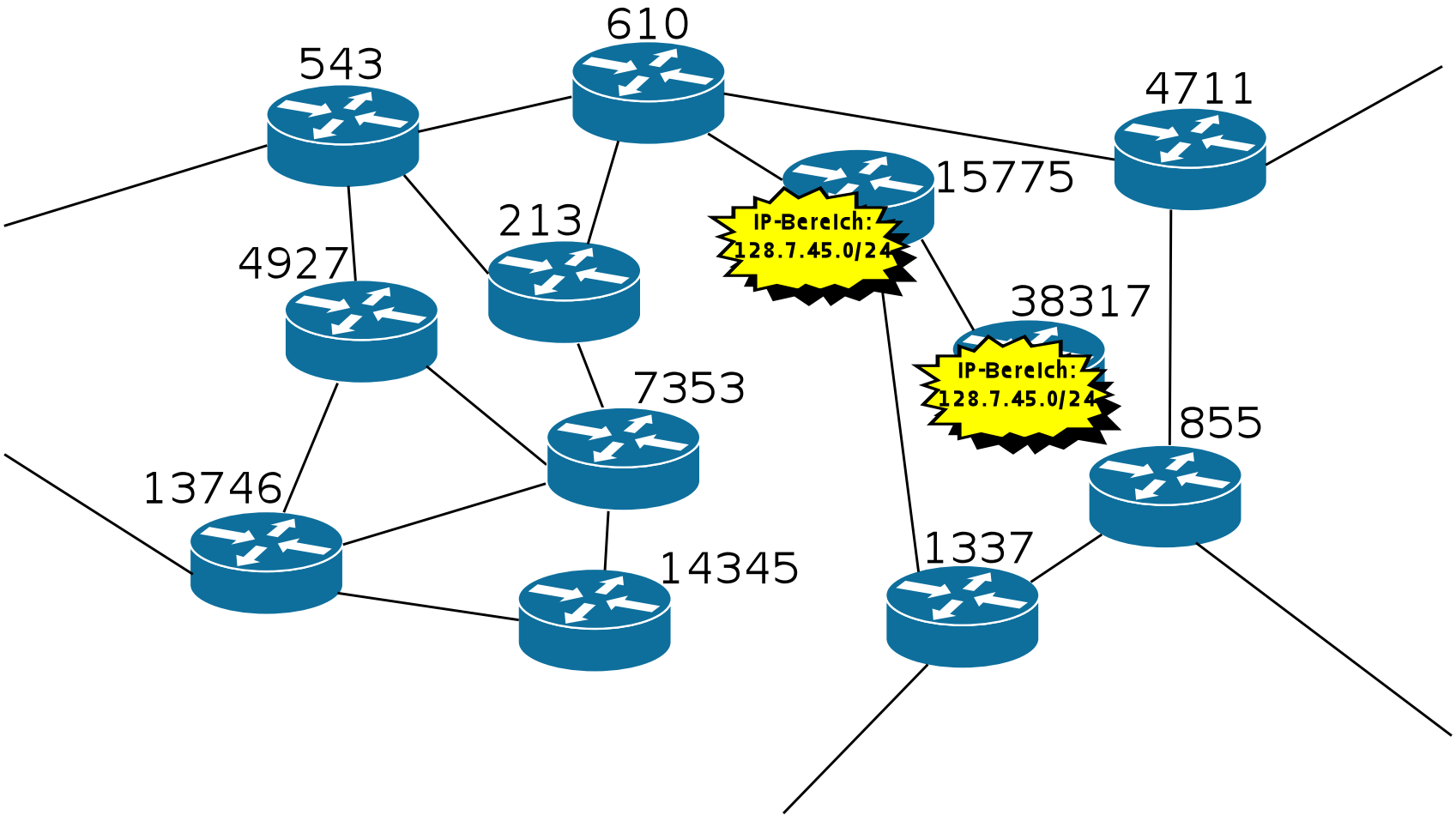
Routing-Anomalie



© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE

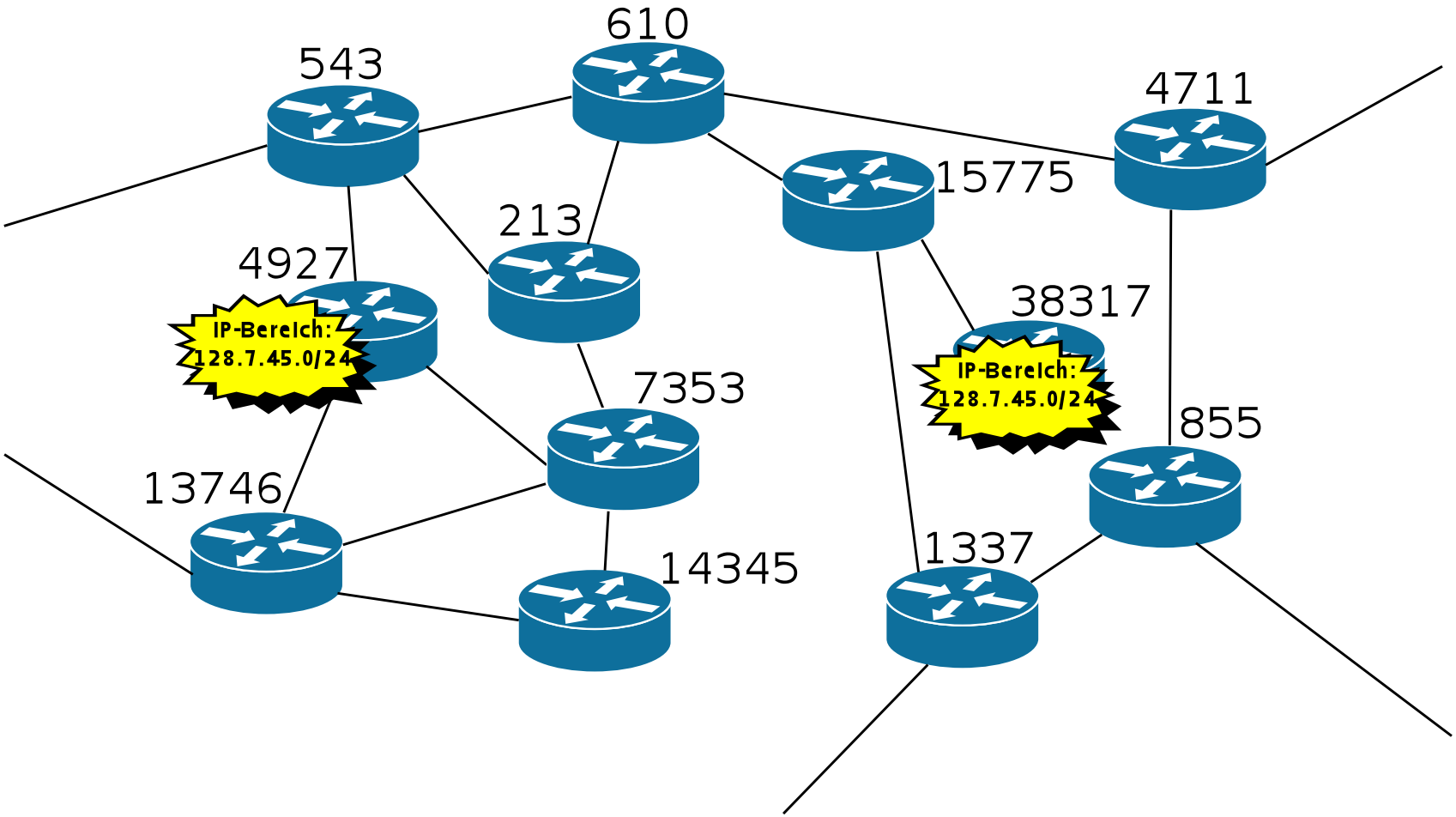
Routing-Anomalie: MOAS-Konflikt



© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE

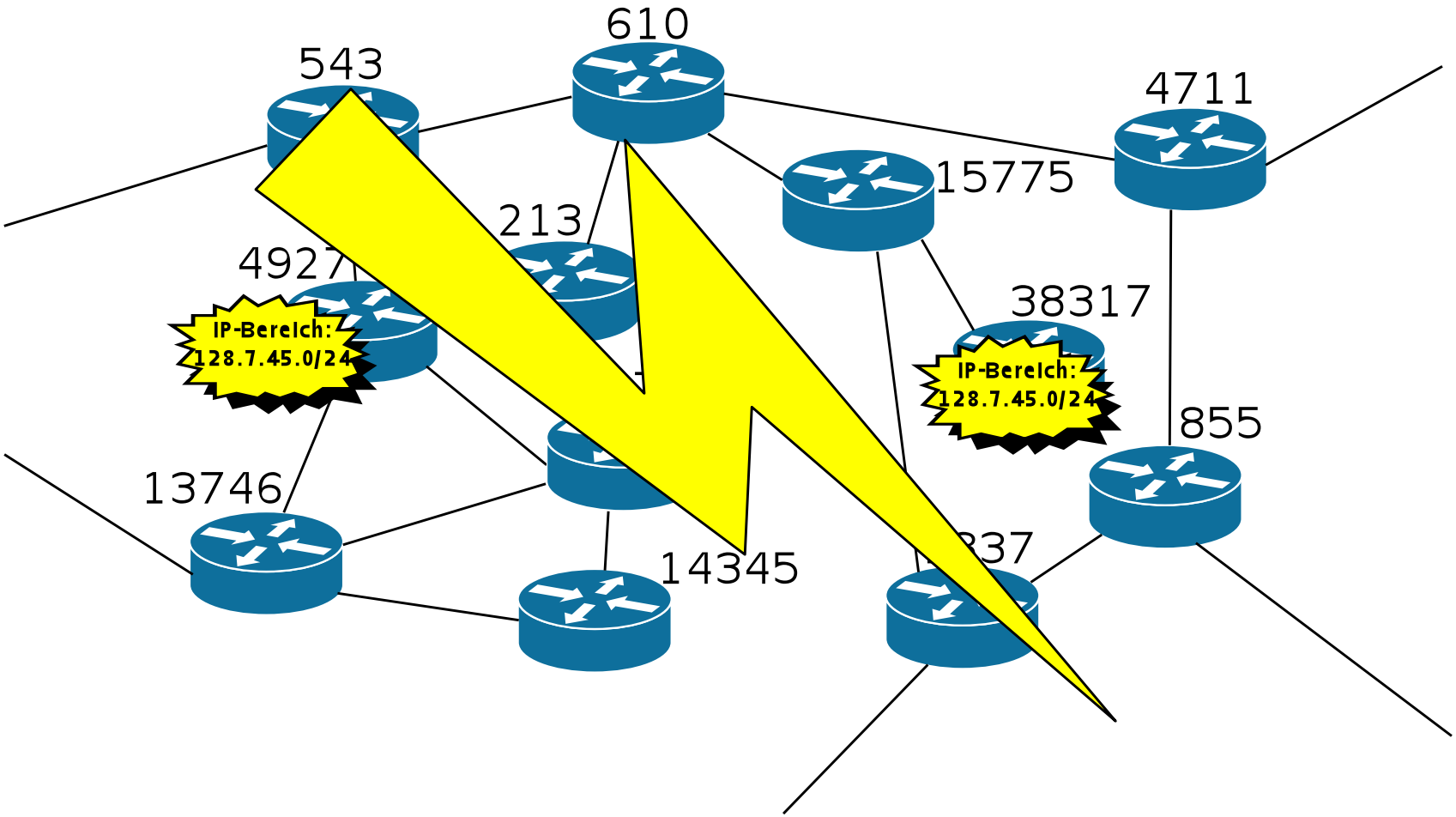
Routing-Anomalie: MOAS-Konflikt



© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE

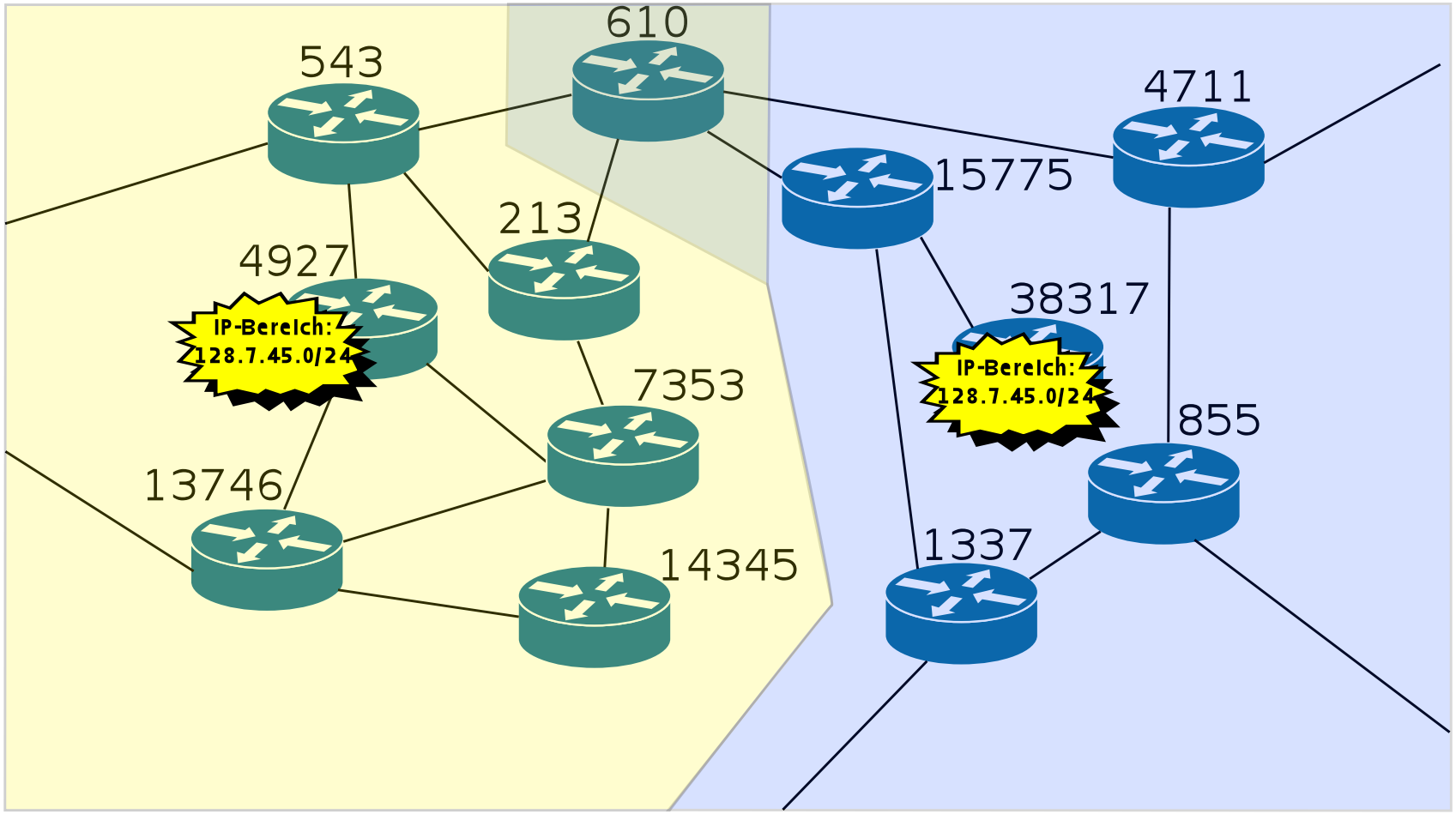
Routing-Anomalie: MOAS-Konflikt



© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE

Routing-Anomalie: Partitionierung



© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE

Routing-Anomalien

- MOAS-Konflikte

© CyberDefense Research Group, Fraunhofer FKIE

Routing-Anomalien

- MOAS-Konflikte

  Allgemeine Konflikte

  Mehr als ein AS annonciert dasselbe IP-Präfix.

© CyberDefense Research Group, Fraunhofer FKIE

Routing-Anomalien

- MOAS-Konflikte

  Allgemeine Konflikte
  : Mehr als ein AS annonciert dasselbe IP-Präfix.

  Sub-MOAS-Konflikte
  : Ein AS annonciert einen Bereich, der das IP-Präfix eines anderen beinhaltet.

© CyberDefense Research Group, Fraunhofer FKIE

Routing-Anomalien

- MOAS-Konflikte

  Allgemeine Konflikte
  Mehr als ein AS annonciert dasselbe IP-Präfix.

  Sub-MOAS-Konflikte
  Ein AS annonciert einen Bereich, der das IP-Präfix eines anderen beinhaltet.

  Provider und Multi-Home-Customer
  Ein Provider annonciert selbst ein IP-Präfix, welches dem Kunden zugewiesen wurde, der Multi-Homing über unterschiedliche Provider realisiert.

© CyberDefense Research Group, Fraunhofer FKIE

Routing-Anomalien

- MOAS-Konflikte

  Allgemeine Konflikte
  Mehr als ein AS annonciert dasselbe IP-Präfix.

  Sub-MOAS-Konflikte
  Ein AS annonciert einen Bereich, der das IP-Präfix eines anderen beinhaltet.

  Provider und Multi-Home-Customer
  Ein Provider annonciert selbst ein IP-Präfix, welches dem Kunden zugewiesen wurde, der Multi-Homing über unterschiedliche Provider realisiert.

  Diese Konflikte lassen sich jeweils in “legitime” und “illegitime” Konflikte unterteilen.

© CyberDefense Research Group, Fraunhofer FKIE

Routing-Anomalien (forts.)

- Topologie-Konflikte

© CyberDefense Research Group, Fraunhofer FKIE

Routing-Anomalien (forts.)

- Topologie-Konflikte

  Erfundene Pfade

  Ein Announcement enthält einen AS-Pfad ohne physikalisches Äquivalent.

© CyberDefense Research Group, Fraunhofer FKIE

Routing-Anomalien (forts.)

- Topologie-Konflikte

  Erfundene Pfade

  Ein Announcement enthält einen AS-Pfad ohne physikalisches Äquivalent.

  Pfadkürzung

  Ein annoncierter AS-Pfad wurde gekürzt.

© CyberDefense Research Group, Fraunhofer FKIE

Routing-Anomalien (forts.)

- Topologie-Konflikte

  Erfundene Pfade
  : Ein Announcement enthält einen AS-Pfad ohne physikalisches Äquivalent.

  Pfadkürzung
  : Ein annoncierter AS-Pfad wurde gekürzt.

  Pfadverlängerung
  : Ein annoncierter AS-Pfad wurde verlängert.

© CyberDefense Research Group, Fraunhofer FKIE

Anomalie-Erkennung und Gegenmaßnahmen

BGPmon.net

Erkennt MOAS-Konflikte im Auftrag von AS-Betreibern und Präfix-Besitzern und informiert diese im Anomaliefall.

PHAS

Das “Prefix Hijack Alert System” nutzt die öffentlichen Daten von RIPE RIS und alamiert bei Anomalien für einzelne Prefix nach einer Registrierung.

© CyberDefense Research Group, Fraunhofer FKIE

Weitere Gegenmaßnahmen

- Mögliche Gegenmaßnahmen sind meist sehr theoretisch:

  S-BGP nutzt asymmetrische Kryptografie zur Absicherung von Announcements. Der Rechenaufwand ist viel zu groß für industriell eingesetzte Routinghardware.

  psBGP im Grunde eine Erweiterung von S-BGP, hat sich aber ebenfalls nicht durchsetzen können.

- Eine praktisch (beschränkt) funktionierende Maßnahme wäre ein Announcement mit einem längeren IP-Präfix (nur bis /24 möglich, führt jedoch zu einer dramatisch hohen Anzahl an Routen).

© CyberDefense Research Group, Fraunhofer FKIE

Problemstellung meiner Betrachtungen:

- Es werden IP-Präfix-Besitzer adressiert und über Anomalien informiert. Deren Möglichkeiten zur Gegenmaßnahme sind dabei eher gering.

© CyberDefense Research Group, Fraunhofer FKIE

Problemstellung meiner Betrachtungen:

- Es werden IP-Präfix-Besitzer adressiert und über Anomalien informiert. Deren Möglichkeiten zur Gegenmaßnahme sind dabei eher gering.
- Keine Information über Anomalien an Endnutzer (es sei denn, diese haben den BGPmon-RSS-Feed abonniert), diese könnten aber die Kommunikation noch beeinflussen.

© CyberDefense Research Group, Fraunhofer FKIE

Gafahr für Endnutzer durch Routing-Anomalien

- Endnutzer erfahren gar nicht oder nur selten von Routing-Anomalien
- Warum ist die Information von Endnutzern so wichtig?

© CyberDefense Research Group, Fraunhofer FKIE

Gafahr für Endnutzer durch Routing-Anomalien

- Endnutzer erfahren gar nicht oder nur selten von Routing-Anomalien
- Warum ist die Information von Endnutzern so wichtig?
  - SSL-Zertifkate authentifizieren zwar die Gegenstelle, aber sind die CAs sicher? (Comodo, TürkTrust, DigiNotar, . . .).

© CyberDefense Research Group, Fraunhofer FKIE

Gafahr für Endnutzer durch Routing-Anomalien

- Endnutzer erfahren gar nicht oder nur selten von Routing-Anomalien
- Warum ist die Information von Endnutzern so wichtig?
  - SSL-Zertifkate authentifizieren zwar die Gegenstelle, aber sind die CAs sicher? (Comodo, TürkTrust, DigiNotar, ...).
  - Sehr abstrakte Vorstellung des "Internet" und keine Möglichkeit zur eigenständigen Prüfung.

© CyberDefense Research Group, Fraunhofer FKIE

Gafahr für Endnutzer durch Routing-Anomalien

- Endnutzer erfahren gar nicht oder nur selten von Routing-Anomalien
- Warum ist die Information von Endnutzern so wichtig?
  - SSL-Zertifkate authentifizieren zwar die Gegenstelle, aber sind die CAs sicher? (Comodo, TürkTrust, DigiNotar, . . .).
  - Sehr abstrakte Vorstellung des “Internet” und keine Möglichkeit zur eigenständigen Prüfung.
  - Kriminelle und “Internet-Schurkenstaaten” haben durchaus Interesse an gezielten Routenmanipulationen (z.B. Pakistan-Telecom, China-Telecom, . . .).

© CyberDefense Research Group, Fraunhofer FKIE

Erkennen von Anomalien

- Whois-Datenbanken von Internet-Registraren oft alt und schlecht gepflegt.
- Keine eindeutige Zuordnung von IP-Präfix zu AS möglich.

© CyberDefense Research Group, Fraunhofer FKIE

Erkennen von Anomalien

- Whois-Datenbanken von Internet-Registraren oft alt und schlecht gepflegt.
- Keine eindeutige Zuordnung von IP-Präfix zu AS möglich.
  - Nutzung öffentlicher Daten (z.B. RouteViews, RIPE RIS und BGPmon).

© CyberDefense Research Group, Fraunhofer FKIE

Erkennen von Anomalien

- Whois-Datenbanken von Internet-Registraren oft alt und schlecht gepflegt.
- Keine eindeutige Zuordnung von IP-Präfix zu AS möglich.
  - Nutzung öffentlicher Daten (z.B. RouteViews, RIPE RIS und BGPmon).
  - Sammlung von Paket-Traces durch Teilnehmer.

© CyberDefense Research Group, Fraunhofer FKIE

Erkennen von Anomalien

- Whois-Datenbanken von Internet-Registraren oft alt und schlecht gepflegt.
- Keine eindeutige Zuordnung von IP-Präfix zu AS möglich.
  - Nutzung öffentlicher Daten (z.B. RouteViews, RIPE RIS und BGPmon).
  - Sammlung von Paket-Traces durch Teilnehmer.
  - Routen und Traces von teilnehmenden AS-Betreibern.

© CyberDefense Research Group, Fraunhofer FKIE

Erkennen von Anomalien

- Whois-Datenbanken von Internet-Registraren oft alt und schlecht gepflegt.
- Keine eindeutige Zuordnung von IP-Präfix zu AS möglich.
  - Nutzung öffentlicher Daten (z.B. RouteViews, RIPE RIS und BGPmon).
  - Sammlung von Paket-Traces durch Teilnehmer.
  - Routen und Traces von teilnehmenden AS-Betreibern.
  - Statische Informationen (z.B. bekannte legitime MOAS-Konflikte, Customer-Provider-Informationen).

© CyberDefense Research Group, Fraunhofer FKIE

Erkennen und Informieren von Betroffenen

- Simulation von Routing-Algorithmen und Verbreitung von Announcements zur Bestimmung des Ausmaßes.

© CyberDefense Research Group, Fraunhofer FKIE

Erkennen und Informieren von Betroffenen

- Simulation von Routing-Algorithmen und Verbreitung von Announcements zur Bestimmung des Ausmaßes.
- Endnutzer kommunizieren regelmäßig mit unterschiedlichen Servern um genutzte Routen abzugleichen $\Rightarrow$ Identifikation von Betroffenen.

© CyberDefense Research Group, Fraunhofer FKIE

Erkennen und Informieren von Betroffenen

- Simulation von Routing-Algorithmen und Verbreitung von Announcements zur Bestimmung des Ausmaßes.
- Endnutzer kommunizieren regelmäßig mit unterschiedlichen Servern um genutzte Routen abzugleichen $\Rightarrow$ Identifikation von Betroffenen.
- Browser-Plugin informiert Endnutzer, wenn es für den IP-Bereich einer besuchten Webseite keine Anomaliefreiheit gibt:
  - Wahl des Benutzers, ob die Seite trotzdem aufgerufen werden soll und
  - Information des Benutzers, falls die Anomalie nicht mehr vorhanden ist.

© CyberDefense Research Group, Fraunhofer FKIE

Work in Progress

- Bisher (und in naher Zukunft): Umsetzung in einem Projekt vor dem Hintergrund verteilten und kooperativen Monitorings.
- Derzeit: Abschluß der Konzeptionsphase und erste prototypische Entwicklung von Klassifikationen zur Anomalieerkennung.
- Später: Auch Nutzung von öffentlich zugänglicher Infrastruktur (z.B. RIPE Atlas), um die Datendichte weiter zu erhöhen und noch präzisere Aussagen treffen zu können.

© CyberDefense Research Group, Fraunhofer FKIE

Literatur

- S. Kent, C. Lynn, and K. Seo: Secure Border Gateway Protocol (S-BGP) in IEEE Journal on Selected Areas in Communications Vol. 18, No. 4, 2000.
- van Oorschot, P. C., Wan, T. und Kranakis, E.: On Interdomain Routing Security and Pretty Secure BGP (psBGP) in ACM Transactions on Information and System Security Vol. 10, No. 3, 2007.
- Labovitz, C., Malan, G. R. und Jahanian, F.: Internet routing instability in IEEE/ACM Trans. Netw. Vol. 6, No. 5, 1998.
- Lad, M., Massey, D., Pei, D., Wu, Y., Zhang, B. und Zhang, L.: PHAS: a prefix hijack alert system in Proceedings of the 15th conference on USENIX Security Symposium - Volume 15, USENIX Association, 2006.

© CyberDefense Research Group, Fraunhofer FKIE

Literatur (forts.)

- X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S.F. Wu, L. Zhang: Detection of Invalid Routing Announcement in the Internet. In: Proceedings of International Conference on Dependable Systems and Networks (DSN) (2002), Juni 2002
- C. McArthur, M. Guirguis,: Stealthy IP prefix hijacking: don't bite off more than you can chew. In: Proceedings of the 28th IEEE conference on Global telecommunications. Piscataway, NJ, USA : IEEE Press, 2009 (GLOBECOM'09), S. 2480–2485
- C. Krügel, D. Mutz, W. Robertson, F. Valeur: Topology-Based Detection of Anomalous BGP Messages. In: RAID, 2003, S. 17–35

© CyberDefense Research Group, Fraunhofer FKIE

Literatur - Belletristik

- BGP-Routing-Anomalien
  - Chinese ISP hijacks the Internet
    `http://www.bgpmon.net/chinese-isp-hijacked-10-of-the-internet/`
  - YouTube Hijacking: A RIPE NCC RIS case study
    `http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study`
- Sicherheit von SSL-CAs
  - Fatale Panne bei Zertifikatsherausgeber Türktrust
    `http://heise.de/-1776879`
  - Falsches Google-Zertifikat ist Folge eines Hacks
    `http://heise.de/-1333588`
  - Another Comodo SSL registrar hacked
    `http://www.h-online.com/security/news/item/Another-Comodo-SSL-registrar-hacked-1250283.html`

© CyberDefense Research Group, Fraunhofer FKIE

Ende.

- Fragen oder Anregungen?

© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE

Ende.

- Fragen oder Anregungen?
- Matthias Wübbeling <wueb@cs.uni-bonn.de>

© CyberDefense Research Group, Fraunhofer FKIE

Fraunhofer FKIE