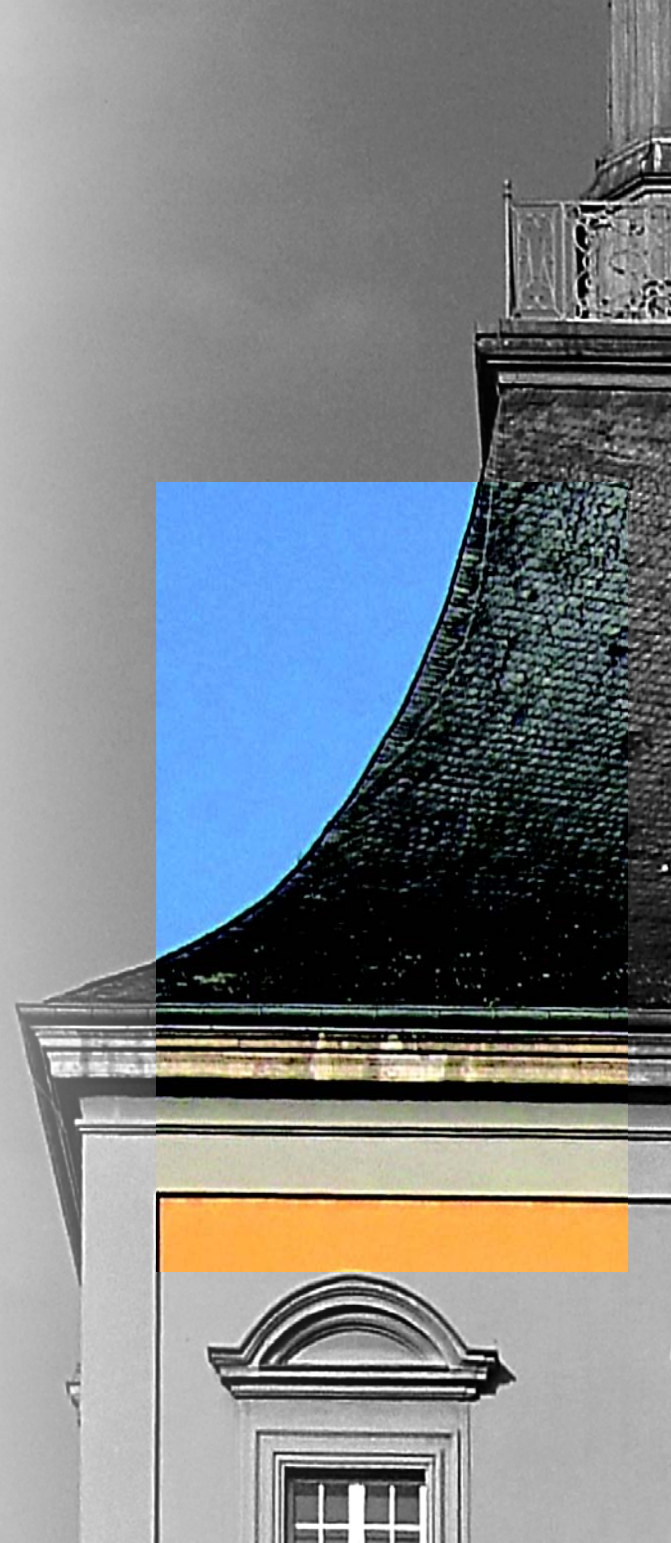
UNIVERSITÄT BONN

VORLESUNG

NETZWERKSICHERHEIT

SOMMERSEMESTER 2020

MO. 10-12 UHR



UNIVERSITÄT BONN

KAPITEL 4

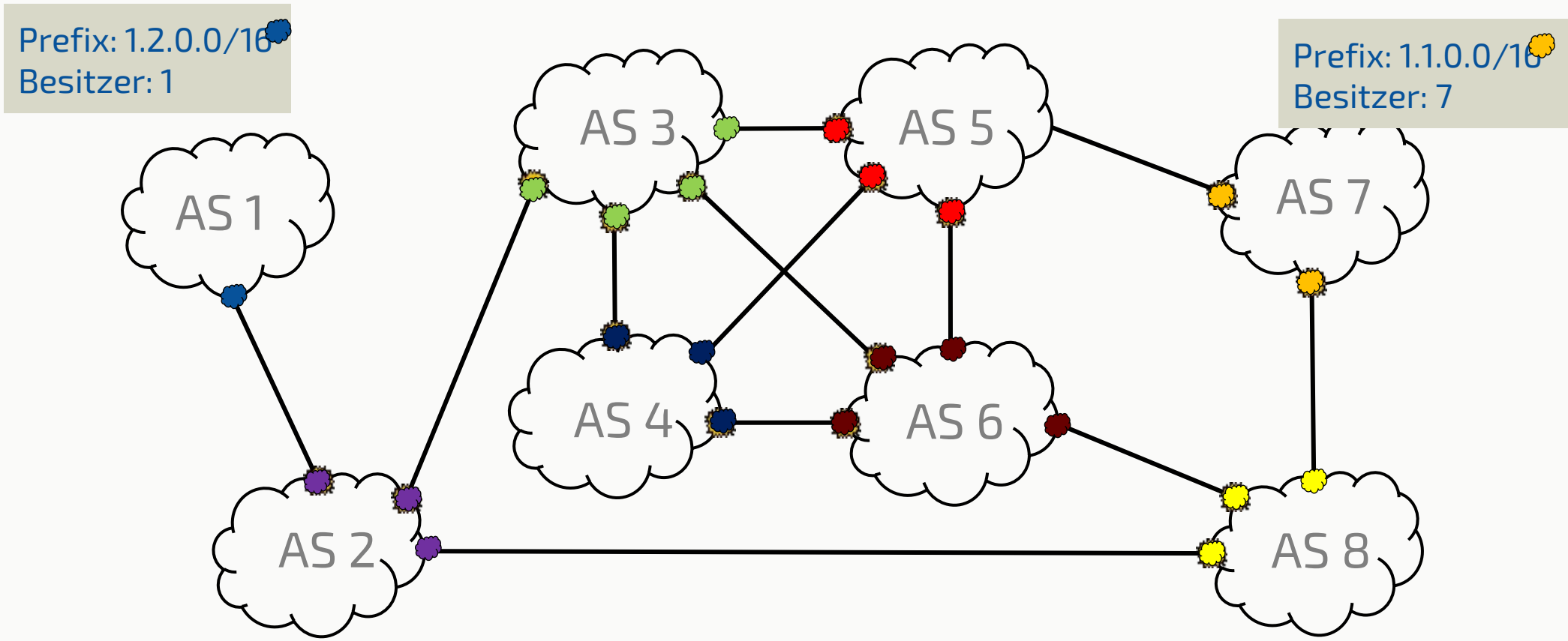
INTERNET ROUTING (ANOMALIEERKENNUNG)

UNIVERSITÄT BONN

INHALTE

- Border Gateway Protocol
- Routinganomalien, Angriffsvektoren & Angreifermodel
- Topological Disorder
  - Angriffszenario “Quantuminsert”
- **Prefix-Hijacking**
- Analyse von Routinganomalien

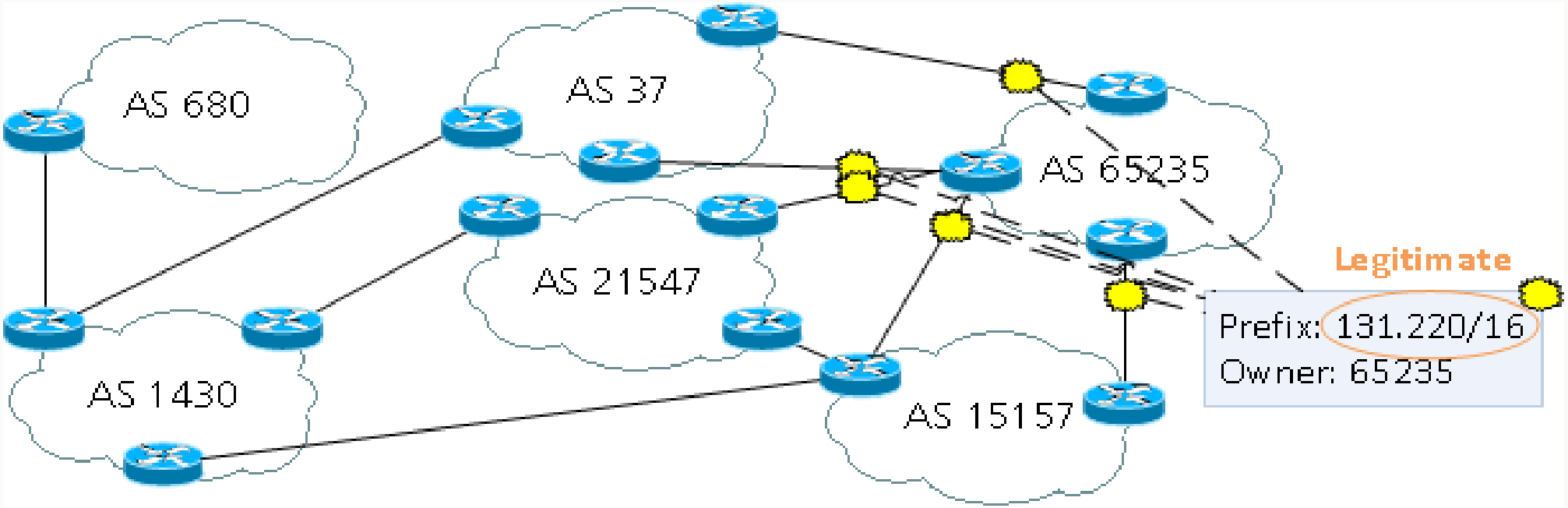
INTERNETROUTING



ROUTINGANOMALIEN – PREFIX HIJACKING

Annahme: AS 680 ist Angreifer (und möchte Datenverkehr abgreifen)

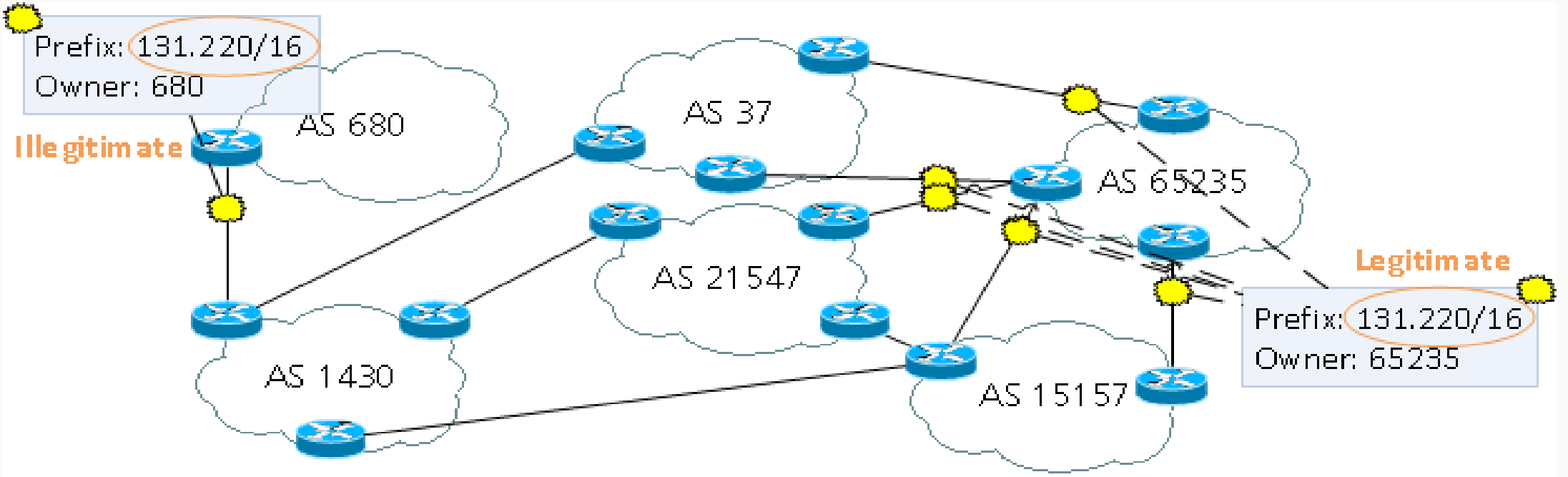
- Ziel: Datenverkehr, der eigentlich für AS 65235 gedacht ist



ROUTINGANOMALIEN – PREFIX HIJACKING

Annahme: AS 680 ist Angreifer (und möchte Datenverkehr abgreifen)

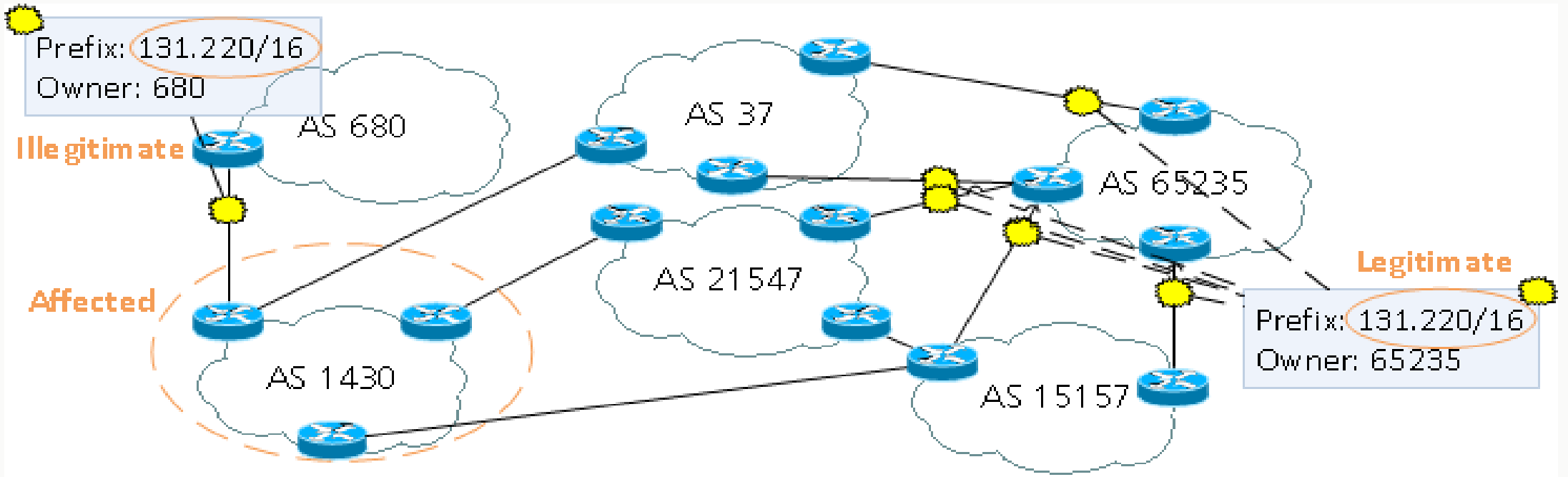
- Was kann passieren?
- Welches AS ist betroffen?



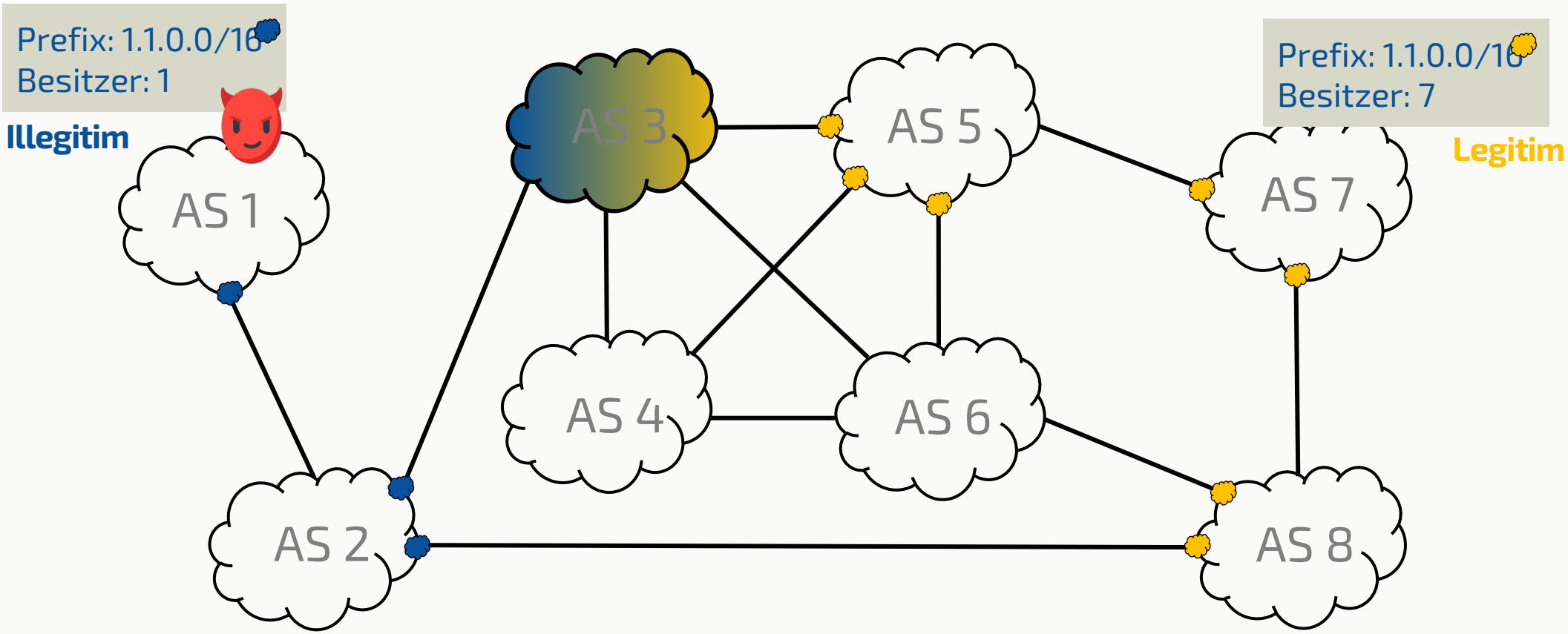
ROUTINGANOMALIEN – PREFIX HIJACKING

Annahme: AS 680 ist Angreifer (und möchte Datenverkehr abgreifen)

- Ist dies ein realistisches Szenario (= eine echte Bedrohung)?



PREFIX-HIJACKING



ROUTING ANOMALIES – PREFIX HIJACKING

- Annahme: AS 680 ist Angreifer (und möchte Datenverkehr abgreifen)
  - Ist dies ein realistisches Szenario (= eine echte Bedrohung)?

How Pakistan knocked YouTube offline (and how to make sure it never happens again)

YouTube becoming unreachable isn't the first time that Internet addresses were hijacked. But if it spurs interest in better security, it may be the last.

by Declan McCullagh @declanm / February 25, 2008 2:30 PM PST / Updated: February 25, 2008 4:28 PM PST

This graph that network-monitoring firm Keynote Systems provided to us shows the worldwide availability of YouTube.com dropping dramatically from 100 percent to 0 percent for over an hour. It didn't recover completely until two hours had elapsed.

Keynote Systems

A high-profile incident this weekend in which Pakistan's state-owned telecommunications company managed to cut YouTube off the global Web highlights a long-standing security weakness in the way the Internet is managed.

THIS WEEK'S MUST READS /

1 How Pakistan knocked YouTube offline (and how to make sure it never happens again)
Tech Culture

2 Google's Android Wear software will let you leave your phone at home (if there's Wi-Fi)
Mobile

3 Twitter makes it easier for strangers to send direct messages
Internet

4 This is what a 'Game of Thrones' spring break looks like
Tech Culture

5 With Fizz, Google hopes to bring new power to mobile Web
Software

ars technica

MAIN MENU · MY STORIES: 25 · FORUMS · SUBSCRIBE · JOBS · ARS CONSORTIUM

RISK ASSESSMENT / SECURITY & HACKTIVISM

How China swallowed 15% of 'Net traffic for 18 minutes

In April 2010, 15 percent of all Internet traffic was suddenly diverted …

by **Nate Anderson** - Nov 17, 2010 8:45pm CET

Share Tweet 54

In a 300+ page report (PDF) today, the US-China Economic and Security Review Commission provided the US Congress with a detailed overview of what's been happening in China—including a curious incident in which 15 percent of the world's Internet traffic suddenly passed through Chinese servers on the way to its destination.

Here's how the Commission describes the incident, which took place earlier this year:

> For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed US and other foreign Internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's destinations through servers located in China. This incident affected traffic to and from US government (".gov") and military (".mil") sites, including those for the Senate, the army, the navy, the marine corps, the air force, the office of secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others. Certain commercial websites were also affected, such as those for Dell, Yahoo!, Microsoft, and IBM.

The culprit here was "IP hijacking," a well-known routing problem in a worldwide system based largely on trust. Routers rely on the Border Gateway Protocol (BGP) to puzzle out the best route between two IP addresses; when one party advertises incorrect routing information, routers across the globe can be convinced to send traffic on geographically absurd paths.

This happened famously in 2008, when Pakistan blocked YouTube. The block was meant only for internal use, and it relied on new routing information that would send YouTube requests not to the company's servers but into a "black hole."

As we described the situation at the time, "this routing information escaped from Pakistan Telecom to its ISP PCCW in Hong Kong, which propagated the route to the rest of the world. So any packets for YouTube would end up in Pakistan Telecom's black hole instead." The mistake broke YouTube access from across much of the Internet.

The China situation appears to have a similar cause. The mistaken routing information came from IDC China Telecommunications, and it was then picked up by the huge China Telecom. As other routers around the world accepted the new information, they began funneling huge amounts of US traffic through Chinese servers, for 18 minutes.

As with many things involving cyberattacks and Internet security, it's hard to know if anything bad

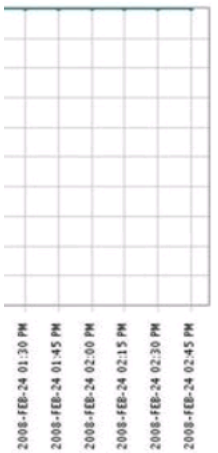
Connect with us

Video · How To · Games · Download · Log In / Join · US E

…ouTube offline (and
…r happens again)

…t addresses were hijacked. But if it spurs interest in

…08 4:28 PM PST



…s the worldwide
…or over an hour. It

THIS WEEK'S MUST READS /

1. How Pakistan knocked YouTube offline (and how to make sure it never happens again) — Tech Culture
2. Google's Android Wear software will let you leave your phone at home (if there's Wi-Fi) — Mobile
3. Twitter makes it easier for strangers to send direct messages — Internet
4. This is what a 'Game of Thrones' spring break looks like — Tech Culture
5. With Fizz, Google hopes to bring new power to mobile Web — Software

A high-profile incident this weekend in which Pakistan's state-owned telecommunications company managed to cut YouTube off the global Web highlights a long-standing security weakness in the way the Internet is managed.

How the Internet in Australia went down under

Posted by Andree Toonk - February 27, 2012 - BCP instability - 2 Comments

This Wednesday for about 30 minutes many Australians found themselves without Internet access. All these users were relying either directly of indirectly on the Telstra network, which at that point was isolated from the Internet. This story quickly hit the local headlines, in this blog we'll look at the technical details of this event and what the cause of this outage likely was.

Telstra is one of Australia's major Internet providers. It normally originates approximately 500 Ipv4 prefixes and 3 Ipv6 prefixes. Telstra also provides Transit for many ISP's and enterprises such as for example AS38285 'Dodo' an Australian ISP and AS10235 'National Australia Bank'. So how could such a large provider go down, surely it has lots of redundant hardware and multiple connections in and out of the country?

As it turns out Wednesday's outage was caused by a routing error many network engineers have first hand experience with, a simple routing leak. A routing leak can happen when small ISP X buys transit from ISP A and also from ISP B. ISP X receives a full bgp routing table from A and because of incorrect filtering relays these messages to ISP B. As a result ISP B now learns all Internet routes via ISP X to ISP B and ISP X (the customers) now became an upstream provider for ISP B.

The above is likely what happened last Wednesday between Telstra en Dodo (AS38285). Dodo a Telstra customer, re-announced all Internet routes to Telstra, which because it prefers customer routes now thinks the best way to the Internet is through Dodo. This post on the Ausnog mailings list shows how Telstra was using Dodo (a customer) as transit to reach a network in India.

This is not a new zero day attack scenario or anything like it. Instead it's probably the number one mistake when configuring BGP routing. I remember when I was just learning about BGP my mentor always used to tell me.. Filter, Filter, Filter, filter!! Which is exactly what didn't happen here. Because it is so easy to accidentally leak routes in BGP you have to explicitly define filters that prevent this. In this case Dodo should have had filters to make sure they would only announce their prefixes and Telstra should have had these filters as well to prevent hijacks but more importantly to protect its own infrastructure. In this case these filters did not seem to be in place, which allowed this leak to happen.

However, this alone should not have brought down all of Telstra's International connections. So what happened? It's likely that Telstra now tagged all routes learned from Dodo (all 400,000 of them) as customer routes and faithfully announced this to all of its peers and upstream providers.

As keeping large filters up to date can be tedious we often see large providers use a mechanism known as max prefix limits. Instead of explicitly defining which prefixes to allow the number of prefixes expected plus some extra is set as the maximum number of prefixes allowed. This is useful to prevent a sudden spike in announcements, often caused by leaks. In case the limit is reached the BGP session is brought down to prevent the leak from spreading

BGPMON

HOME BLOG ABOUT US PRODUCTS A

How the Internet in Australia

Posted by Andree Toonk - February 27, 2012 - BGP ins

This Wednesday for about 30 minutes man
All these users were relying either directly o
was isolated from the Internet. This story qu
technical details of this event and what the

Telstra is one of Australia's major Internet p
prefixes and 3 Ipv6 prefixes. Telstra also pr
for example AS38285 'Dodo' an Australian
such a large provider go down, surely it has
and out of the country?

As it turns out Wednesday's outage was ca
first hand experience with, a simple routing
transit from ISP A and also from ISP B. ISP X r
incorrect filtering relays these messages to
ISP X to ISP B and ISP X (the customers) now

The above is likely what happened last We
Telstra customer, re-announced all Internet
routes now thinks the best way to the Inter
list shows how Telstra was using Dodo (a c

This is not a new zero day attack scenario
mistake when configuring BGP routing. I rem
always used to tell me.. Filter, Filter, Filter, fil
Because it is so easy to accidentally leak ro
prevent this. In this case Dodo should have
prefixes and Telstra should have had these
protect its own infrastructure. In this case th
this leak to happen.

However, this alone should not have broug
what happened? It's likely that Telstra now
them) as customer routes and faithfully ann

As keeping large filters up to date can be te
known as max prefix limits. Instead of explic
prefixes expected plus some extra is set as
to prevent a sudden spike in announcemen
BGP session is brought down to prevent the

СТРОГО СЕКРЕТНО
STROGO SEKRETNO

Hijacked? UK's Nuclear Weapons Data Re-Routes and Travels via Ukraine

Sensitive internet data from British company Royal Mail and the UK Atomic Weapons Establishment (AWE) has passed through Russia and Ukraine via insecure connections, according to internet performance and analysis company Dyn.

An article published in technewstoday.com, suggests "web traffic originating from Texas, intended for certain addresses in the UK has been taking an unconventional route to its destination, through Ukraine and Russia".

According to research carried out by Dyn, Ukrainian telecom provider Vega "began announcing 14 British Telecom (BT) routes, resulting in the redirection of Internet traffic through Ukraine for a handful of BT customers". This includes the UK's Atomic Weapons Establishment.

AWE is 'responsible for the design, manufacture and support of warheads for the United Kingdom's nuclear deterrent'.

WIRED

HACKER REDIRECTS TRAFFIC FROM 19 INTERNET PROVIDERS TO STEAL BITCOINS

Adam Voorhes Gail Anderson + Joe Newton

1 K

20. April 2020

AMONG ALL THE scams and thievery in the bitcoin economy, one recent hack sets a new bar for brazenness: Stealing an entire chunk of raw internet traffic from more than a dozen internet service

Nuclear Weapons Data Re-Routes and ine

om British company Royal Mail and the UK Atomic Weapons s passed through Russia and Ukraine via insecure connections, formance and analysis company Dyn.

nnewstoday.com, suggests "web traffic originating from Texas, sses in the UK has been taking an unconventional route to its ine and Russia".

ied out by Dyn, Ukrainian telecom provider Vega "began announcing utes, resulting in the redirection of Internet traffic through Ukraine ers". This includes the UK's Atomic Weapons Establishment.

e design, manufacture and support of warheads for the United nt'.

WIRED

HACKER FROM 19 TO STEA

Adam Voorhes Gail

1 K

AMON
econo
braze
traffi

20. April 2020

ars technica

MAIN MENU · MY STORIES: 25 · FORUMS · SUBSCRIBE · JOBS · ARS CONSORTIUM

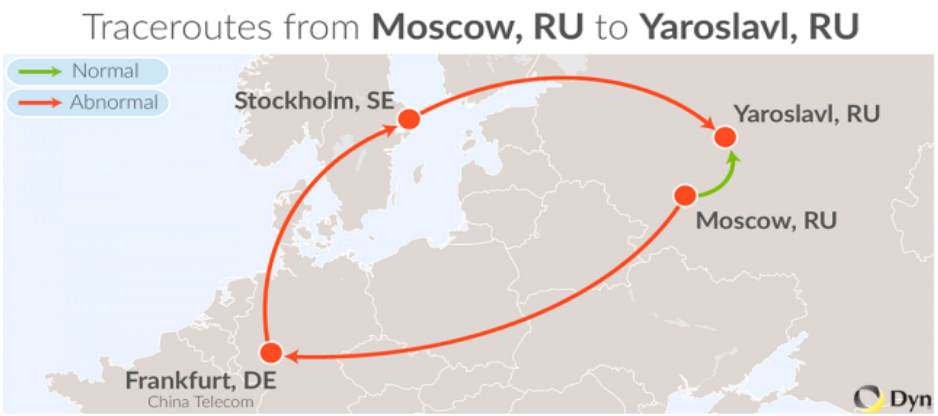
RISK ASSESSMENT / SECURITY & HACKTIVISM

WTF, Russia's domestic Internet traffic mysteriously passes through Chinese routers

Unexplained diversion underscores insecurity of Net's global routing system.

by **Dan Goodin** - Nov 9, 2014 7:00pm CET

Share Tweet 74



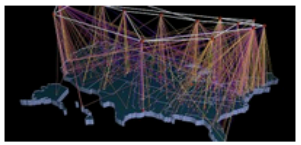
Enlarge

Dyn Research

Domestic Internet traffic traveling inside the borders of Russia has repeatedly been rerouted outside of the country under an unexplained series of events that degrades performance and could compromise the security of Russian communications.

The finding, reported Thursday in a blog post published by Internet monitoring service Dyn, underscores the fragility of the border gateway protocol (BGP), which forms the underpinning of the Internet's global routing system. In this case, domestic Russian traffic was repeatedly routed to routers operated by China Telecom, a firm with close ties to that country's government. When huge amounts of traffic are diverted to far-away regions before ultimately reaching their final destination, it increases the chances hackers with the ability to monitor the connections have monitored or even altered some of the communications. A similar concern emerged last year, when Dyn found big chunks of traffic belonging to US banks, government agencies, and network

FURTHER READING



REPEATED ATTACKS HIJACK HUGE CHUNKS OF INTERNET TRAFFIC, RESEARCHERS WARN

Man-in-the-middle attacks divert data on scale never before seen in the wild.

ETHO

Krassimir Ivandjiiski

CURRENT ISSUE

ata Re-Routes and

ail and the UK Atomic Weapons
Ukraine via insecure connections,
any Dyn.

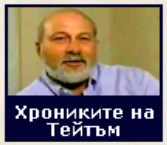
eb traffic originating from Texas,
g an unconventional route to its

com provider Vega "began announcing
n of Internet traffic through Ukraine
omic Weapons Establishment.

port of warheads for the United


Оръжията на Русия


Лобиране в Брюксел


Хрониките на Тейтъм


НАТО - мит и фикция

Kevin Beaumont Follow
InfoSec, from the trenches of reality. Email kevin.beaumont@gmail.com | Twitter: @gossithedog on Twitter.
Apr 24 · 3 min read

Hijack of Amazon's internet domain service used to reroute web traffic for two hours unnoticed

Between 11am until 1pm UTC today, DNS traffic—the phone book of the internet, routing you to your favourite websites—was hijacked by an unknown actor.

The attackers used BGP—a key protocol used for routing internet traffic around the world—to reroute traffic to Amazon's Route 53 service, the largest commercial cloud provider who count major websites such as Twitter.com as customers.

They re-routed DNS traffic using a man in the middle attack using a server at Equinix in Chicago.

From there, they served traffic for over two hours.

ROUTINGANOMALIEN – PREFIX HIJACKING

Mögliche Ursachen für Prefix-Hijacking?

- Angriff?
- Fehlkonfiguration?
- Software-Bug?

ROUTINGANOMALIEN – PREFIX HIJACKING

Mögliche Ursachen für Prefix-Hijacking?

- Angriff?
  - Ja!
- Fehlkonfiguration?
  - Das kann tatsächlich passieren (etwa verursacht durch übermüdete Administratoren an einem Freitag Nachmittag) und scheint ein sehr häufiges Phänomen/Problem zu sein
- Software failure?
  - Möglich, aber wie Topology Disorder sehr unwahrscheinlich

ROUTING ANOMALIES – PREFIX HIJACKING

- Folgen von Prefix-Hijacking:
  - Nachahmung / Immitation von Kommunikationspartnern / Online-Diensten
  - Traffic Blackholing (= eine Art von Denial-of-Service)
  - Man-in-the-Middle (schwierig, aber theoretisch möglich)

UNIVERSITÄT BONN

INHALTE

- Border Gateway Protocol
- Routinganomalien, Angriffsvektoren & Angreifermodel
- Topological-Disorder
  - Angriffszenario “Quantuminsert”
- Prefix-Hijacking
- **Analyse von Routinganomalien**

UNIVERSITÄT BONN

ROUTINGANOMALIEN – ANOMALIEERKENNUNG

Wie können Topology-Disorder und Prefix-Hijacking erkannt werden?

- Möglichkeiten zur Erkennung von Topology-Disorder:
  - Basierend auf einer vollständigen Karte des Internets (mit allen Peering-Verbindungen zwischen den AS)
  - Überprüfe jeden Pfad aller Announcements
    - Problem: eine solche Karte existiert nicht!
  - Basierend auf einer Routing-Historie (und der AS-Verbindungen)
  - Eine neu erscheinende AS-Verbindung kann bereits bekannt sein (und lediglich für einen gewissen Zeitraum nicht genutzt)
  - Was passiert beim ersten Auftauchen einer AS-Verbindung
    - Problem: Diese Methode kann die Zuverlässigkeit von AS-Verbindungen zeigen, eignet sich aber nicht zur Anomalieerkennung

ROUTINGANOMALIEN – ANOMALIEERKENNUNG

Wie können Topology-Disorder und Prefix-Hijacking erkannt werden:

- Möglichkeiten zur Erkennung von Topology-Disorder
  - Basierend auf Routing-Historie, verbunden mit zusätzlichen Quellen über AS-Verbindungen (z.B. IXP oder LG) Daten.
  - Nutzung der Wahrscheinlichkeit für die Erstellung einer Verbindung von AS auf Basis bereits bekannter Verbindungen der AS
    - Gibt zusätzliche Hinweise, aber nur für eine überschaubare Anzahl an AS-Verbindungen

ROUTINGANOMALIEN – ANOMALIEERKENNUNG

Zusätzliche Informationen von IXPs (Internet eXchange Points)

https://www.de-cix.net/customers-partners/customers/de-cix-frankfurt/

ROUTINGANOMALIEN – ANOMALIEERKENNUNG

Zusätzliche Informationen von LGs (Looking Glass)

HURRICANE ELECTRIC
INTERNET SERVICES

Looking Glass

Welcome to Hurricane Electric's Network Looking Glass. The information provided by and the support of this service are on a best effort basis. These are some of our routers at core locations within our network. We also operate a public route server accessible via telnet at route-server.he.net.

Show options

core1.ams1.he.net> show ip bgp summary

Local AS Number	6939
Number of Neighbors Configured	842, 776 up
Number of Routes Installed	2942857 (253085702 bytes)
Number of Routes Advertised	65124013 (5061468 entries) (242950464 bytes)
Number of Attribute Entries	526348 (47371320 bytes)

Neighbor Address	ASN	State	Time	Rt:Accepted	Rt:Filtered	Rt:Sent	Rt:ToSend
72.14.212.34	15169	ESTAB	173d 8h25m	342	0	23778	0
80.249.208.1	1200	ESTAB	147d 2h15m	3	1	66404	0
80.249.208.26	26496	ESTAB	12d10h 0m	493	0	66404	0
80.249.208.27	29075	ESTAB	173d 8h25m	226	0	66404	0
80.249.208.29	8304	ESTAB	4d 1h42m	27	0	66404	0
80.249.208.30	8529	ESTAB	50d 9h14m	4308	33	66404	0
80.249.208.31	16637	ESTAB	40d 9h19m	505	0	66404	0
80.249.208.32	12871	ESTAB	25d 9h57m	14	0	66404	0
80.249.208.33	559	IDLE	1h 9m25s	0	0	0	66404
80.249.208.34	1103	ESTAB	73d16h19m	189	5	66404	0
80.249.208.35	12859	ESTAB	47d18h16m	70	0	66404	0
80.249.208.37	2686	ESTAB	32d 7h33m	356	0	66404	0
80.249.208.38	4589	ESTAB	33d 9h57m	251	0	66404	0
80.249.208.39	112	ESTAB	3d22h 1m	1	0	66404	0
80.249.208.42	9145	ESTAB	41d 9h16m	219	0	66404	0
80.249.208.43	2611	ESTAB	50d 8h48m	55	0	66404	0

https://lg.he.net/

ROUTINGANOMALIEN – ANOMALIEERKENNUNG

Wie lassen sich Topology-Disorder und Prefix-Hijacking erkennen?

- Prefix Hijacking, a.k.a. Multiple Origin ASes (MOAS) Konflikt:
  - Definition:

Let pre$\bar{}$x p being associated with two paths
$asp_1 = (p_1; p_2; :::; p_n)$ and
$asp_2 = (q_1; q_2; :::; q_m)$
then, a MOAS con° ict occurs if $p_n \not\in q_m$.

  - Drei Klassen von MOAS-Konflikten:

OrigTransAS: $p_n = q_j (j < m)$
SplitView: $p_i = q_j (i < n; j < m)$
DistinctPaths: $p_i \not\in q_j (8i\ 2\ [1::n]; j\ 2\ [1::m]$

ROUTINGANOMALIEN – ANOMALIEERKENNUNG

Wie lassen sich Topology-Disorder und Prefix-Hijacking erkennen?

- Prefix Hijacking, a.k.a. Multiple Origin ASes (MOAS) Konflikt:
  - Im Bezug auf Prefixe könnte eine vierte Klasse “Sub-MOAS” definiert werden:

> Let prefix p and prefix q be related in a form that $q < p$ (i.e. q is a real subnet of p) and a MOAS conflict occurs for all IP addresses in $q \cap p$.

ROUTINGANOMALIEN – ANOMALIEERKENNUNG

Wie lassen sich Topology-Disorder und Prefix-Hijacking erkennen?

- Prefix Hijacking, a.k.a. Multiple Origin ASes (MOAS) Konflikt:
  - Basierend auf annoncierten Prefixen
  - Teste für alle Announcements desselben Prefixes, ob es ein MOAS ist

  - Wo gibt es annoncierte Prefixe?

ROUTINGANOMALIEN – ANOMALIEERKENNUNG

Wie lassen sich Topology-Disorder und Prefix-Hijacking erkennen?

- Prefix Hijacking, a.k.a. Multiple Origin ASes (MOAS) Konflikt:
  - Basierend auf annoncierten Prefixen
  - Teste für alle Announcements desselben Prefixes, ob es ein MOAS ist

  - Wo gibt es annoncierte Prefixe?
    - RIPE RIS, RouteViews, PCH, … sammeln und archivieren BGP-Announcements

ROUTINGANOMALIEN – ANOMALIEERKENNUNG

Wie lassen sich Topology-Disorder und Prefix-Hijacking erkennen?

- Wo gibt es annoncierte Prefixe?
  - RIPE RIS
    - Standorte: Amsterdam, London, Paris, Geneva, Vienna, Otemachi (Japan), Stockholm, San Jose, Zurich, Milan, New York, Frankfurt, Moscow, Palo Alto, Soa Paulo
    - http://www.ripe.net/data-tools/stats/ris/
  - RouteViews
    - Oregon, Ashburn, Palo Alto, Nairobi (Kenya), London, Portland, Tokyo, Sydney, Sao Paulo, Atlanta, Fort Collins
    - http://www.routeviews.org/
  - PCH
    - Mehr than 50 Standorte.
    - https://www.pch.net/resources/data.php

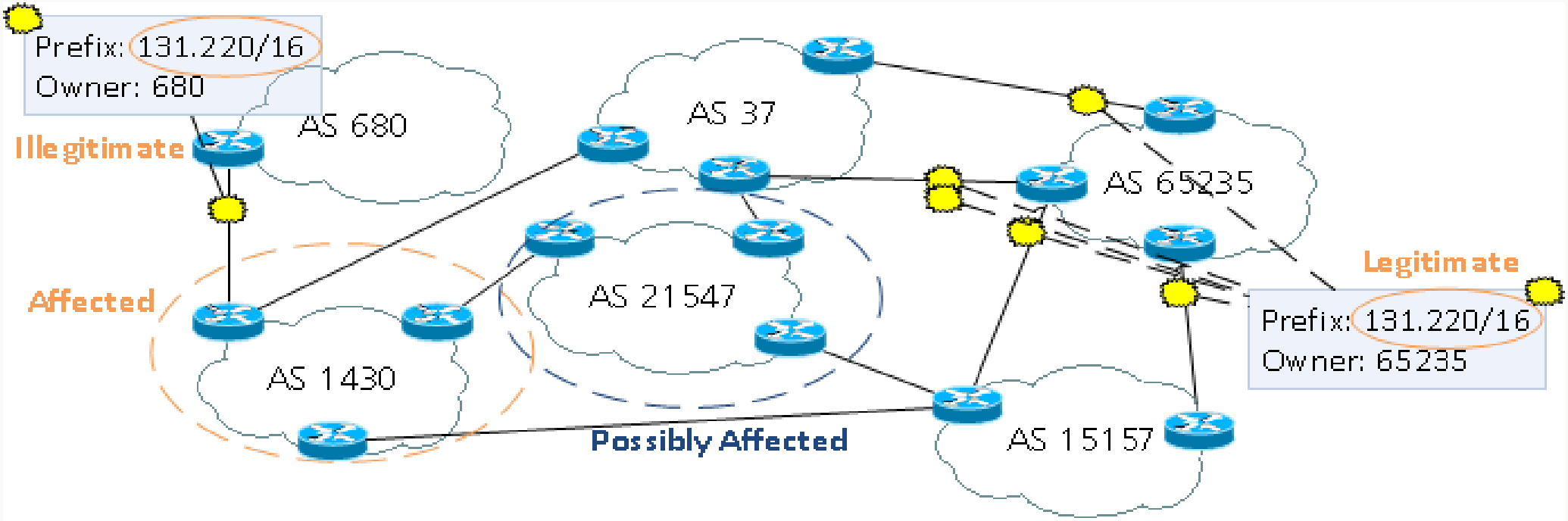
ROUTINGANOMALIEN – PREFIX-HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wieviel Einfluss hat ein Angreifer?

ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS



ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wieviel Einfluss hat ein Angreifer?

$$
\begin{array}{ll}
V & : \text{the set of all ASs (vertices)} \\
A = V \backslash \{t\} & : \text{the set of all possible attackers} \\
 & \text{for a given true origin } t \in V. \\
N = V \backslash \{t, a\} & : \text{the remainder of V for chosen origin} \\
 & t \in V \text{ and attacker } a \in A \\
P_{(t,a,n)} & : \text{the set of connected ASs providing} \\
 & \text{shortest paths to the origins } t \in V \text{ or} \\
 & a \in A \text{ to } n \in N
\end{array}
$$

ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

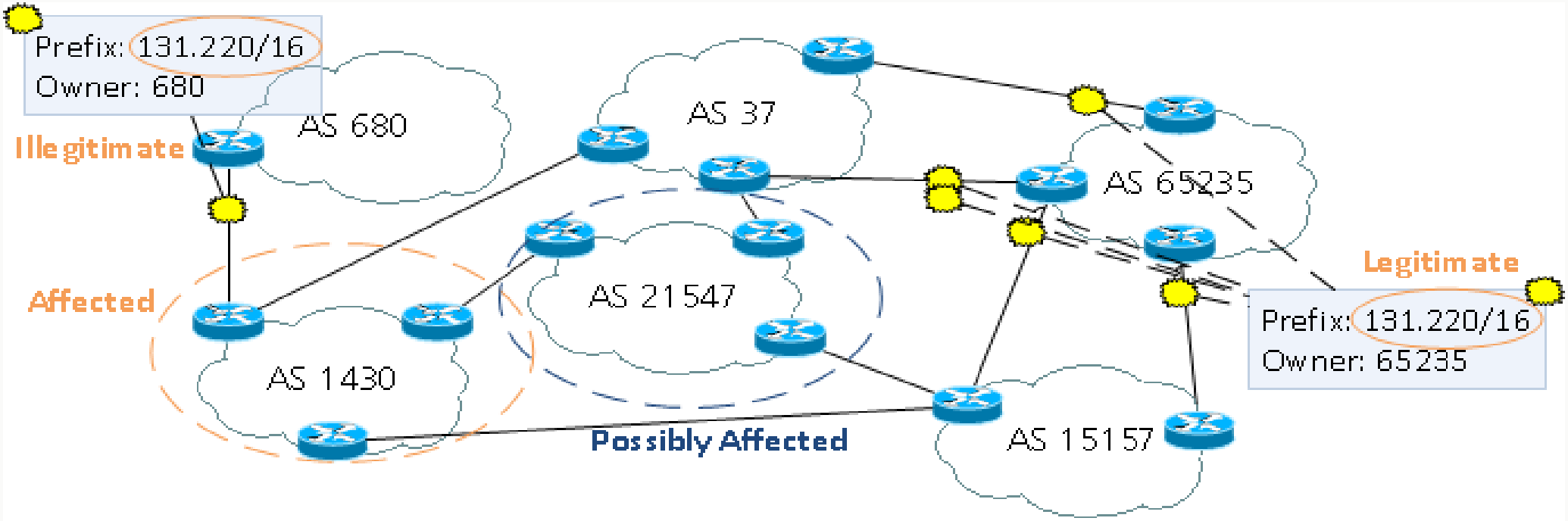
- Wieviel Einfluss hat ein Angreifer?

$$\beta(t,a,n) = \begin{cases} 0 & \text{, if } Case\ 1 \\ \frac{1}{|P_{(t,a,n)}|} & \text{, if } Case\ 2 \\ \sum_{p \in P_{(t,a,n)}} \frac{1}{|P_{(t,a,n)}|} \times \beta(t,a,p) & \text{, if } Case\ 3 \end{cases}$$

Case 1: t is not, but a is directly connected to n.
Case 2: t is and a might be directly connected to n.
Case 3: both, t and a are not directly connected to n.

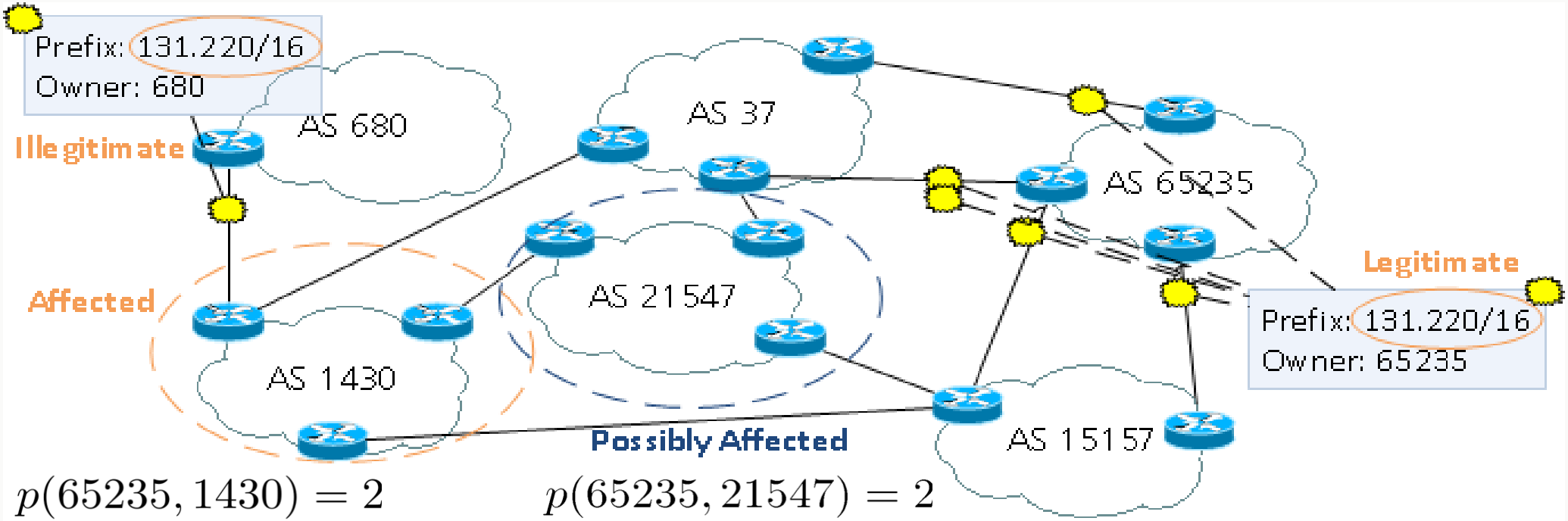
ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS



ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

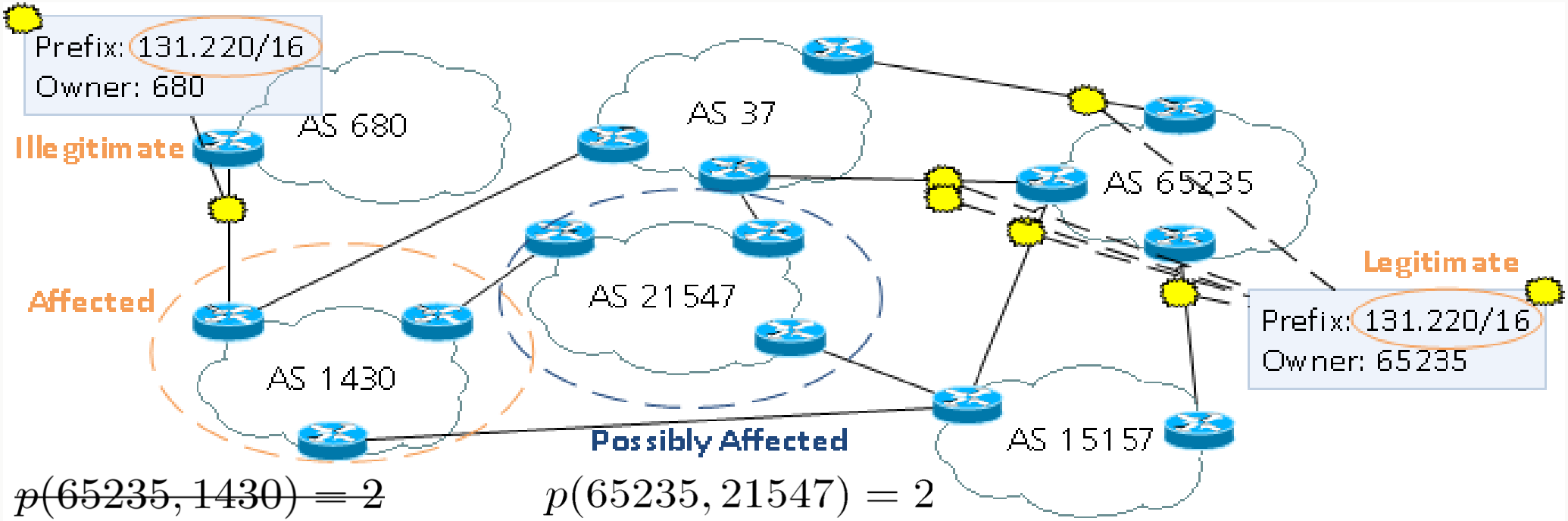


$p(65235, 1430) = 2$
$p(680, 1430) = 1$

$p(65235, 21547) = 2$
$p(680, 21547) = 1$

ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS



~~$p(65235, 1430) = 2$~~

$p(680, 1430) = 1$

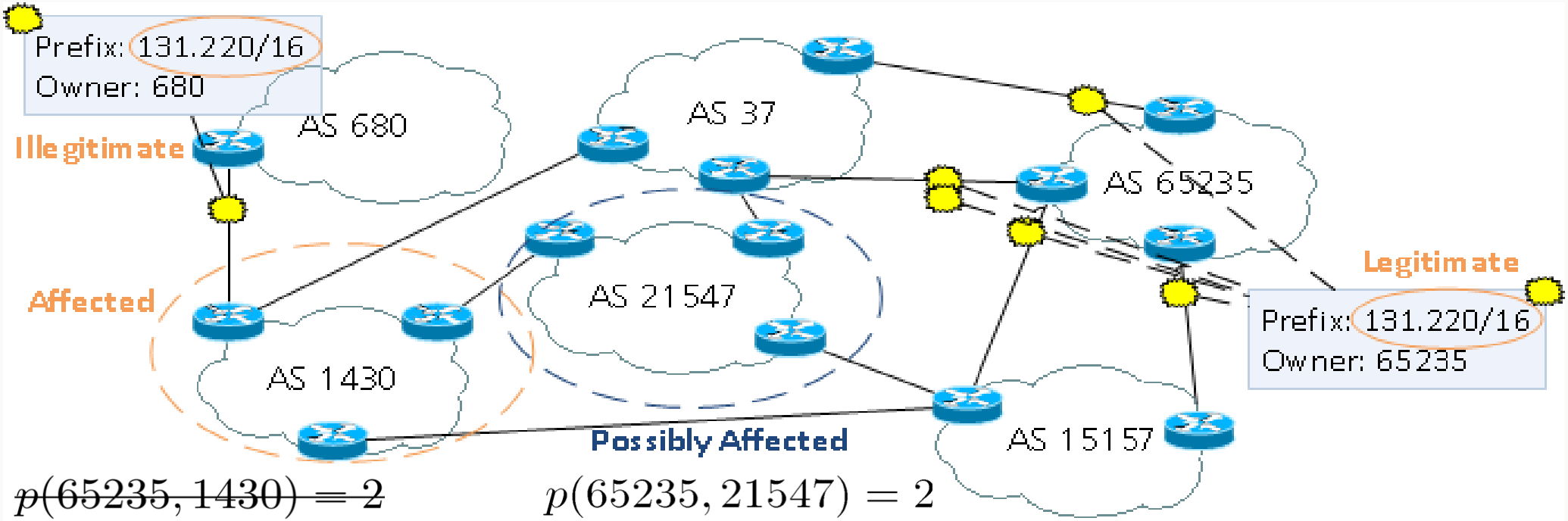
$p(65235, 21547) = 2$

$p(680, 21547) = 1$

Not in tie-break!

ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS



~~$p(65235, 1430) = 2$~~

$p(680, 1430) = 1$

$p(65235, 21547) = 2$

$p(680, 21547) = 1$

$\beta(680, 65235, 21547) = \frac{1}{3}$

ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wieviel Einfluss hat ein Angreifer?

$$\beta(680, 65235, 21547) = \frac{1}{3}$$

- Das ist lediglich der Einfluss von AS 680 bezogen auf AS 21547 für Prefixe, die auch von AS 62543 annonciert werden
- Wie lässt sich der Einfluss (Impact) generalisieren?

ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wieviel Einfluss hat ein Angreifer?

$$\beta(680, 65235, 21547) = \frac{1}{3}$$

- Das ist lediglich der Einfluss von AS 680 bezogen auf AS 21547 für Prefixe, die auch von AS 62543 annonciert werden
- Wie lässt sich der Einfluss (Impact) generalisieren?

$$I(a) = \sum_{t \in V \setminus \{a\}} \sum_{v \in N} \frac{\beta(a, t, v)}{|V \setminus \{a\}||N|}$$

- Äußere Summe über |V| – 1 (True Origins - ohne den Angreifer).
- Innere Summer über |V| – 2 ASes (ohne den Anfreifer und ohne True Origin)

ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wie widerstandsfähig ist ein AS (zur Verteidigung des eigenen Prefixes)?

ROUTINGANOMALIEN – PREFIX HIJACKING

Wie bereits gezeigt, teilt Prefix-Hijacking das Internet in verschiedene Partitionen, eine für jedes Ursprungs-AS

- Wie widerstandsfähig ist ein AS (zur Verteidigung des eigenen Prefixes)?
- Widerstandsfähigkeit (Resilience)

$$R(t) = \sum_{a \in A} \sum_{v \in N} \frac{\beta(t, a, v)}{|A||N|}$$

- Offensichtlich: Die Resilience eines AS ist gleich dem Impact, den das AS als Angreifer hätte, wenn die Rollen vertauscht wären.

UNIVERSITÄT BONN

ENDE

Vielen Dank für die Aufmerksamkeit!

Fragen?

Nächste Vorlesung:

- Montag, 22. Juni 2020

Nächste Übung:

- Dienstag, 16. Juni 2020 – 16 Uhr
- Abgabe des Übungszettels 7 bis morgen – 16 Uhr