GOETHE UNIVERSITÄT FRANKFURT AM MAIN

ATHENE National Research Center for Applied Cybersecurity

Wie Kryptographie das Internet (nicht) sicherer macht

Prof. Dr. Haya Shulman

ATHENE | Goethe-Universität Frankfurt | Fraunhofer SIT

Cybersicherheitslage in Deutschland 2022

Bundesamt für Sicherheit in der Informationstechnik

„Die Bedrohungslage im Cyber-Raum ist angespannt, dynamisch und vielfältig und damit so hoch wie nie."

BSI-Lagebericht 2022, 25. Oktober 2022

bitkom research

„203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen"

bitkom, 31. August 2022

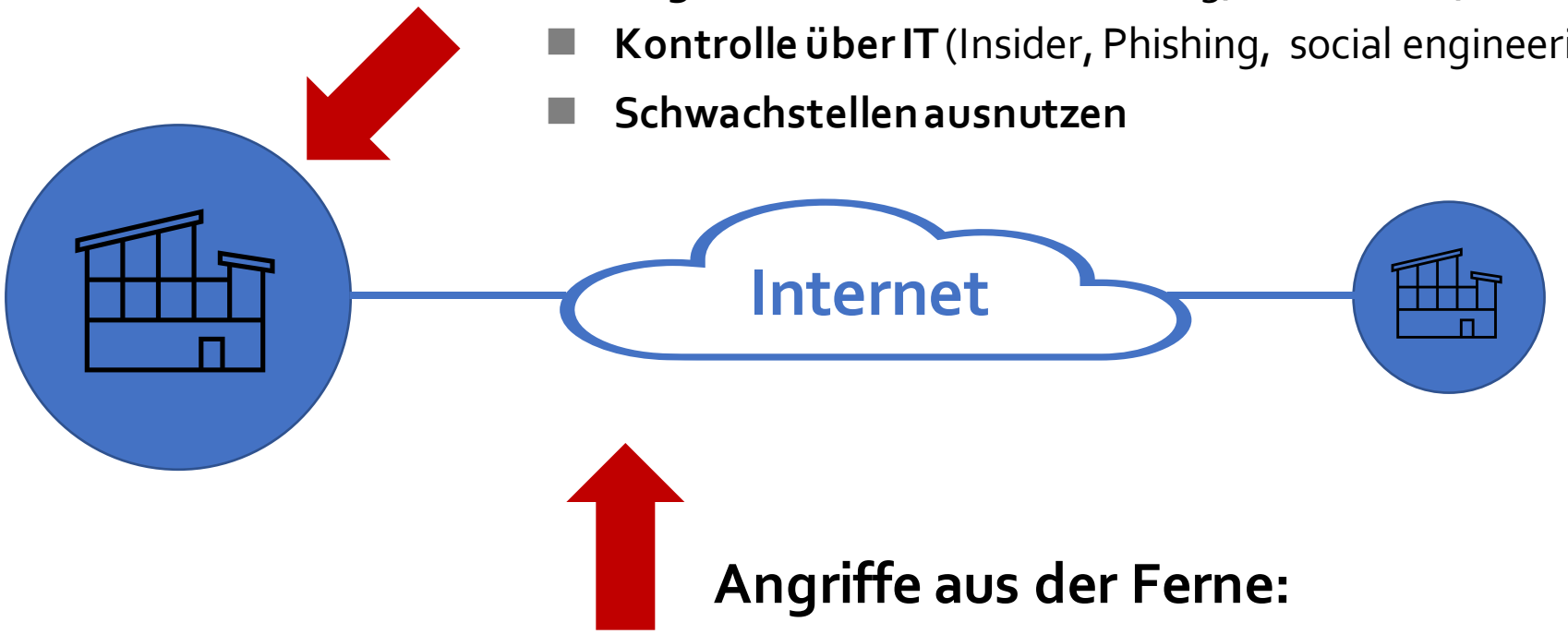
- **Digitalisierung vergrößert Angriffsfläche**
- **Geopolitische und wirtschaftliche Lage erhöht Gefahr**
- **Kriminelle und fremdstaatlich gesteuerte Angreifer**

(c) Wikipedia/Ulrich Latzenhofer, 2010

Was sind die wesentlichen Angriffsvektoren?

Infiltrieren der Zielorganisation:

- **Zugriff auf Passwörter** (Phishing, Infostealers, Darknet, …)
- **Kontrolle über IT** (Insider, Phishing, social engineering…)
- **Schwachstellen ausnutzen**



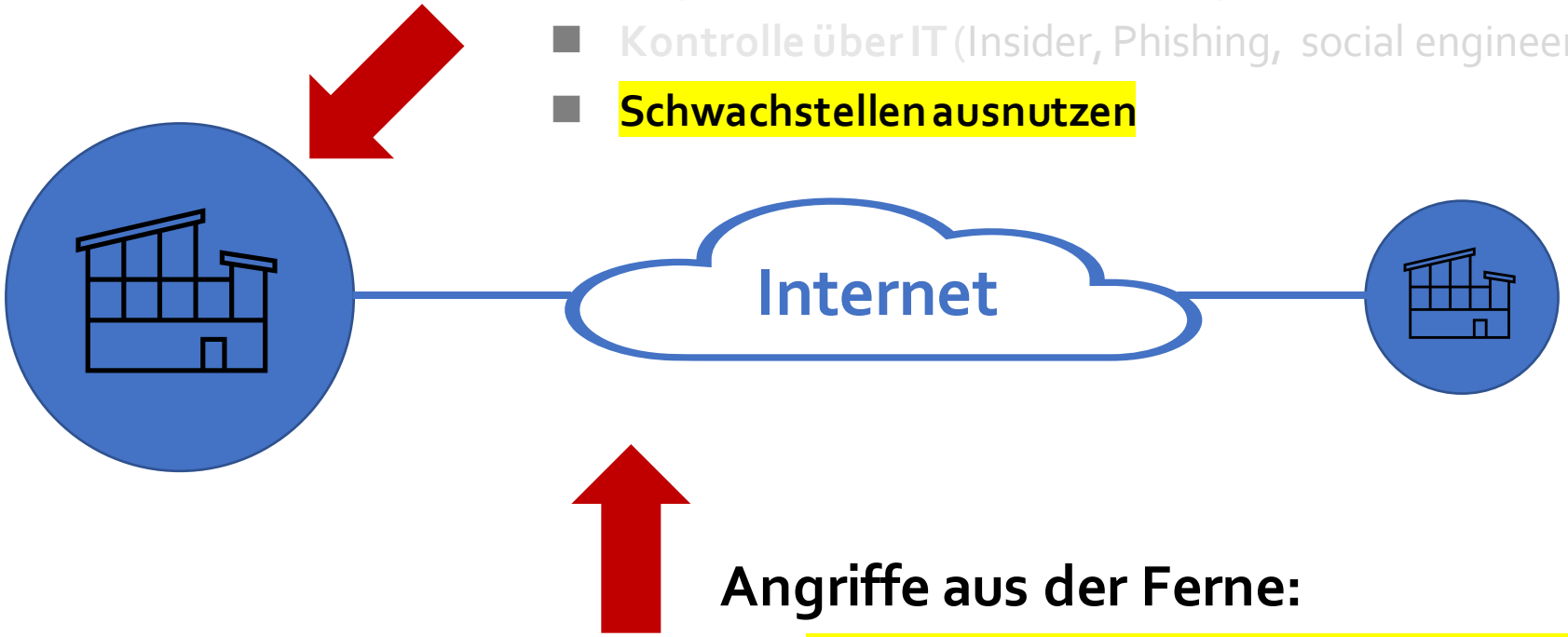
Angriffe aus der Ferne:

- **Verkehrsumlenkungen (Hijacks)** im Internet
- **DDoS** (Distributed Denial of Service)

Die Angriffsvektoren für heute

Infiltrieren der Zielorganisation:

- **Zugriff auf Passwörter** (Phishing, Infostealers, Darknet, …)
- **Kontrolle über IT** (Insider, Phishing, social engineering, …)
- **Schwachstellen ausnutzen**



Angriffe aus der Ferne:

- **Verkehrsumlenkungen (Hijacks)** im Internet
- **DDoS** (Distributed Denial of Service)

Gliederung

Wie sicher sind Router und Routing?

1. **Sicherheitsanalyse in SOHO-Router**
   - Abhängigkeiten von Komponenten von Drittparteien (Bibliotheken, Module) führen zu Verwundbarkeiten
   - Implementierungsfehler unterbrechen die Erreichbarkeit von Netzen

2. **RPKI Validierung kann abgeschaltet werden**
   - Generische Verwundbarkeiten in Protokollspezifikationen
   - Verwundbarkeiten in spezifischen Implementierungen

3. **Schlussbemerkung: Sichere und vertrauenswürdige IT**

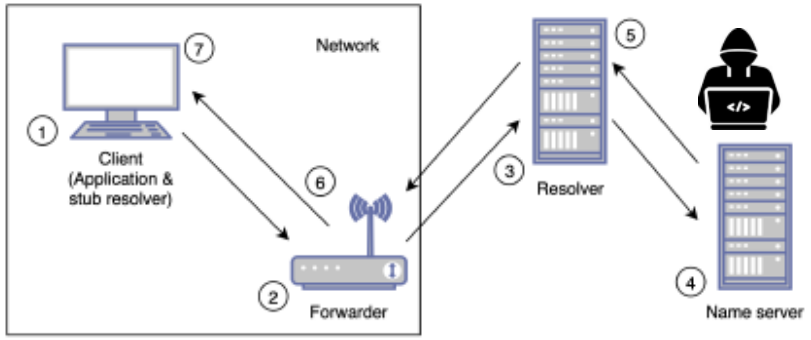
Abhängigkeit von verwundbaren Bibliotheken

"Be strict when sending and tolerant when receiving" [RFC1958]

- **DNS folgt dem Ende-zu-Ende-Prinzip im Internet [RFC3597, RFC1035]**
  - Zwischen-Hosts (Resolver) sollen nur die Daten interpretieren, die sie brauchen
  - Alles andere soll unverändert weitergeleitet werden
  - Grundlegend, damit DNS ein weites Spektrum an Anwendungen unterstützen kann

- **DNS-Transparenz kann für Injection-Angriffe ausgenutzt werden**
- **Aber**, DNS-Records können beliebige Werte enthalten

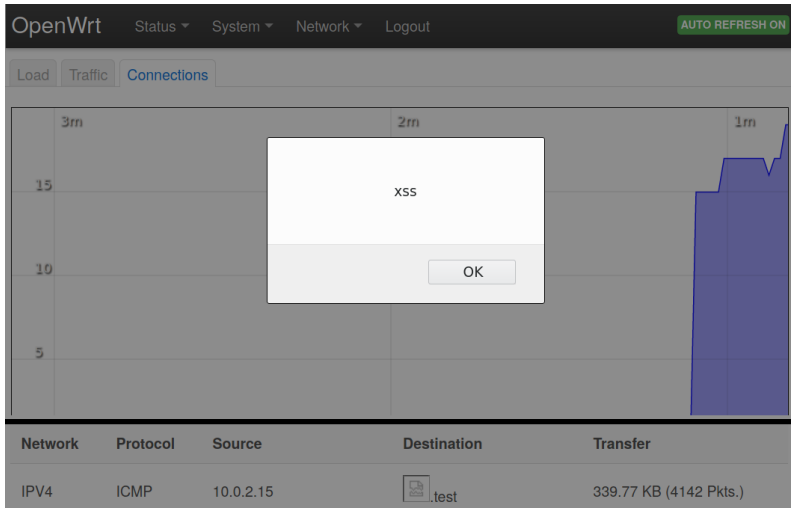
```
attacker.com                  IN CNAME victim.com\000.attacker.com
victim.com\000.attacker.com   IN A     6.6.6.6

victim.com                    IN A     1.1.1.1
```



Abhängigkeit von verwundbaren Bibliotheken

- **XSS-Verwundbarkeit in OpenWRT**
  - OpenWRT ein linux basiertes Betriebssystem für Router
  - Nutzt verwundbare uClibc
  - Injection in Web-basiertes Admin-Interface → Zugriff zu Router-Einstellungen

- **Wieso**? DNS kommt scheinbar vom Betriebssystem
  → Entwickler neigen dazu, ihm zu vertrauen



Security Advisory 2021-08-01-1 - XSS via missing input validation of host names displayed (CVE-2021-32019)

NANOG 83

30TH USENIX SECURITY SYMPOSIUM

Studie zu Schwachstellen in Routern

Abhängigkeit von verwundbaren Komponenten

% of Identified	% of Total	Absolute	Generic match	Vulne-rable	Router
41.62%	0.59%	405	x	x	Tenda
24.25%	0.34%	236	x	x	Huawei
15.42%	0.22%	150	x	x	Fritzbox
12.13%	0.17%	118	x	x	Mercusys
1.54%	0.02%	15	x		Linksys AC2200
1.34%	0.02%	13			Xiaomi Mi router
1.23%	0.02%	12		x	Draytek
1.13%	0.02%	11			Speedport Smart
0.72%	0.01%	7		x	Netgear R6120
0.21%	0.00%	2			D-Link DIR-600
0.10%	0.00%	1			Teltonika
0.10%	0.00%	1			Linksys AC1000
0.10%	0.00%	1		x	Centurylink
0.10%	0.00%	1			ASUS ROG
100.00%	1.42%	973	-	95.48%	Identified
-	98.58%	67482	-	-	Not Identified
-	100.00%	68455	-	1.36%	Total

- **Unsere Forschung zeigt:**
  - 15 (43%) der beliebten Router sind verwundbar
  - 11 Router erfüllen nicht Standards
- **Hersteller warten oft mit Patches**
  - Unwirtschaftlich für Hersteller
- **Pentests sind zu eng**
  - Schwachstellen sind oft in IT-Anbieter, APIs, Komponenten von Drittparteien

Vendor	Model	Has cache	version.bind	Attacks: Any attack	Misinterpretation injection: direct \.	direct \000	CNAME \.	CNAME \000	TXID forward	Fixed UDP port	CD=1 to disable DNSSEC	Non-standard
Home/SOHO routers												
Asus	GT-AC2900	✓	dnsmasq	-	-	-	-	-	-	-	-	-
AVM	Fritz!Box 6660	✓	-	✓	✓	-	-	-	-	-	-	-
AVM	Fritz!Box 7312	✓	-	✓	✓	-	-	-	-	-	-	-
AVM	Fritz!Box 7520	✓	-	✓	✓	-	-	-	-	-	-	-
AVM	Fritz!Box 7590	✓	-	✓	✓	-	-	-	-	-	-	-
Cudy	WR1300	✓	-[1]	-	-	-	-	-	-	-	-	-
D-Link	N150 (DIR-600)	✓	-[1]	-	-	-	-	-	-	-	-	-
D-Link	N300 (DWR-920)	✓	-[1]	-	-	-	-	-	-	-	-	-
DrayTek	Vigor2120	✓	-	✓	✓[5]	✓[5]	-	-	✓	-	✓	(h)
Edimax	N300	-	-	✓	-	-	-	-	-	✓(1027)	-	(h)
Linksys	E5350 (AC1000)	✓	dnsmasq-2.40	-	-	-	-	-	-	-	-	-
Linksys	EA8300 (AC2200)	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Mercusys	MW305R	-	-	✓[2]	-	-	-	-	no[2]	-	-	(h)
Netgear	AC1200 / R6120	-	-	-	-	-	-	-	-	-	-	-
Netis	AC1200	✓	dnsmasq-2.79	-	-	-	-	-	-	-	-	-
STRONG	Wi-Fi Router 300	-	-	✓	-	-	-	-	-	✓(1027)	-	(h)
Tenda	AC10v3	✓	-	✓	✓	✓	-	-	-	✓(62066)	✓	(f),(h)
Tenda	F3	✓	-	✓	✓	✓	-	-	-	✓(50387)	✓	(f),(h)
TP-Link	Archer C7 (AC1750)	-	-	-	-	-	-	-	-	-	-	-
TP-Link	TL-WR841N	-	-	-	-	-	-	-	-	-	-	-
Trendnet	TW100-S4W1CA	✓	-	✓	-	-	-	-	-	✓(5530)	✓	(f),(h)
Xiaomi	MiRouter4A	✓	dnsmasq-2.71	-	-	-	-	-	-	-	-	-
Zyxel	Speedlink 5501	✓	dnsmasq-2.57	-	-	-	-	-	-	-	-	-
ISP-branded home routers												
Actiontec	MI424WR	-	-	✓	-	-	-	-	no[2]	✓(1024)	-	(h)
CenturyLink	C3000Z	✓	-	✓	✓	✓	-	-	✓	✓[3]	✓	(g),(h)
Telekom	Speedport Smart 3	✓	-[1]	-	-	-	-	-	-	-	-	-
Vodafone	Station TG3442DE	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Small business routers												
Bintec	RS353a	✓	-	✓	-	-	✓	✓	-	-	-	(f),(h)
Cisco	RV260	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Grandstream	GWN7000	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Synology	RT2600AC	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Ubiquiti	EdgeRouter4	✓	dnsmasq-2.78	-	-	-	-	-	-	-	-	-
Mobile/4G routers												
Huawei	5G CPE 5 Pro 2	✓	-	✓	-	✓[5]	-	-	-	-	-	(g)
Level421	TARKAN	✓	dnsmasq-2.51	-[4]	-[4]	-	-[4]	-	-	-	-	-
Teltonika	RUT950U022C0	✓	dnsmasq-2.81	-	-	-	-	-	-	-	-	-
SUM(✓)	35 100%	28 80%	-	15 43%	8 23%	5 14%	1 3%	1 13%	4 11%	7 20%	5 14%	11 31%

✓: vulnerable/yes. -: not vulnerable/no. [1]: hidden dnsmasq version, [2]: uses sequential TXIDs, [3]: Port selected randomly at boot. [4]: ISP network vulnerable. [5]: Query section mismatch. (f): CNAME chain merging. (g): EDNS can cause broken responses. (h): No TCP support.

Studie zu Schwachstellen in Routern

Fehler/Bugs

- **Unsere Forschung zeigt:**
  - Verwendung von ungenutzten Flags führte zum Absturz der Router
  - Netze wurden vom Internet getrennt wegen Bug in Routingsoftware
- **Hersteller: FRR**
  - Ähnliche Fehler in CISCO

Fehlerhafte Router stoppen BGP-Experiment

Ein Forscherteam hat die Nutzung bisher ungenutzter Flags aus dem BGP-Routingstandard getestet. Dabei haben reihenweise Router ihre Verbindungen abgebrochen. Das Experiment wurde nun gestoppt.

in Pocket speichern | merken

5. Februar 2019, 14:15 Uhr, Hanno Böck

(Bild: Mstyslav Chernov, Wikimedia Commons/CC BY SA 3.0)

Eine visuelle Darstellung des BGP-Netzwerks (Symbolbild)

Gliederung

Wie sicher sind Router und Routing?

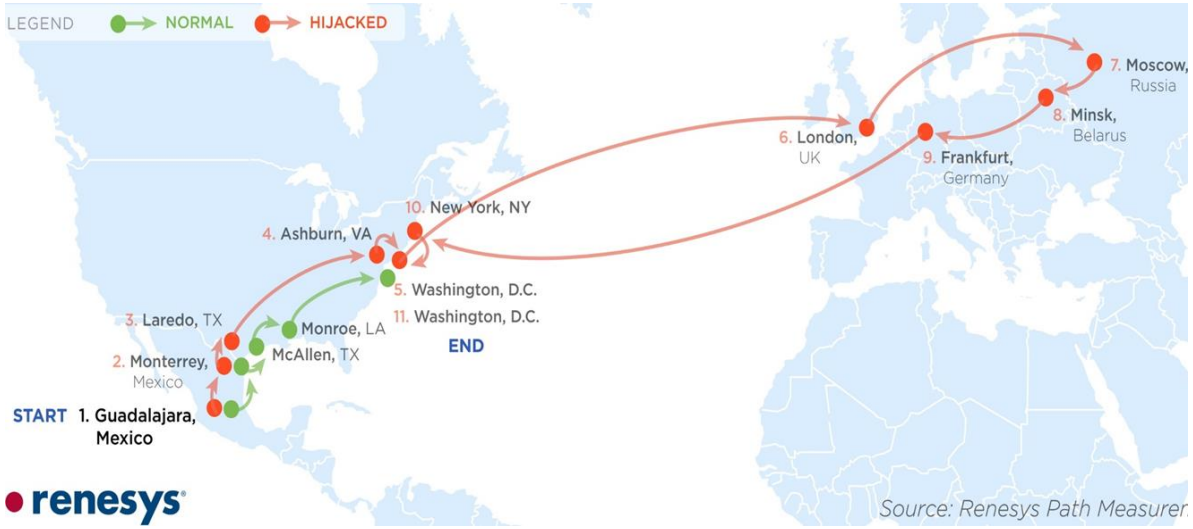
1. **Sicherheitsanalyse in SOHO-Router**
   - Abhängigkeiten von Komponenten von Drittparteien (Bibliotheken, Module) führen zu Verwundbarkeiten
   - Implementierungsfehler unterbrechen die Erreichbarkeit von Netzen

2. **RPKI Validierung kann abgeschaltet werden**
   - Generische Verwundbarkeiten in Protokollspezifikationen
   - Verwundbarkeiten in spezifischen Implementierungen

3. **Schlussbemerkung: Sichere und vertrauenswürdige IT**

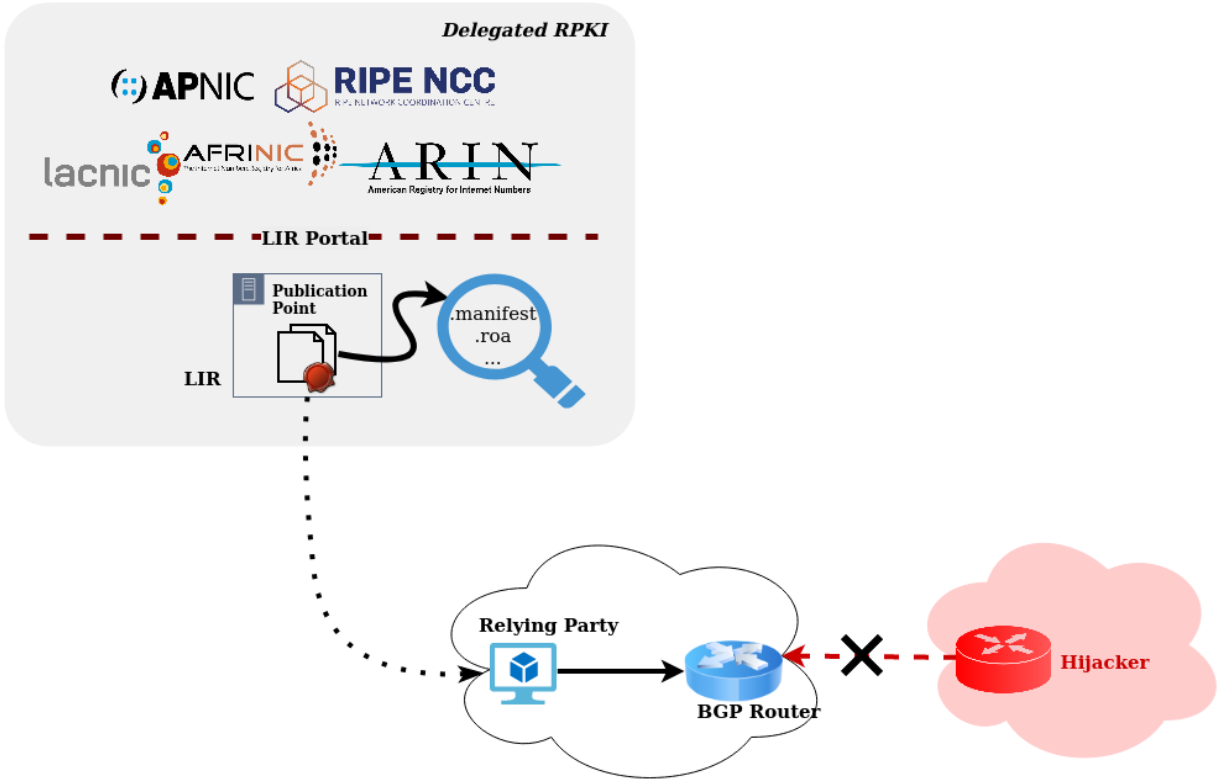
Studien von Internet Infrastruktur
Angriffe auf Kommunikation: Kommunikationsumleitung

- Kriminelle können die Kommunikation abhören und manipulieren
- Problem: die Router können nicht zwischen Hijacks und nicht-Hijacks unterscheiden



- Hijacks ermöglichen das Abfangen von Internet-Verkehr
- Wird ausgenutzt für, z.B. Diebstahl von Crypto-Währungen, Nachrichten mitzulesen, Spam/Phishing zu verteilen

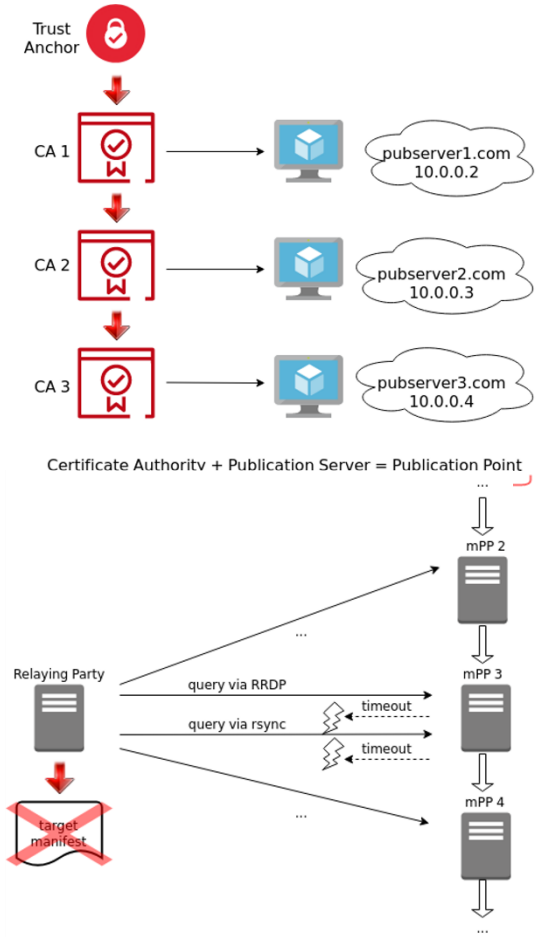
Resource Public Key Infrastrukture (RPKI)



- RPKI schützt Routing-Tabellen vor Manipulation
- Router können BGP-Routen gegen Zertifikate prüfen
- RPKI verbessert die Qualität der Routing-Tabellen und minimiert Fehlkonfigurationen
- RPKI kann abgeschaltet werden durch **generische** und **implementierungsspezifische** Schwachstellen (z.B. CVE-2022-3029)

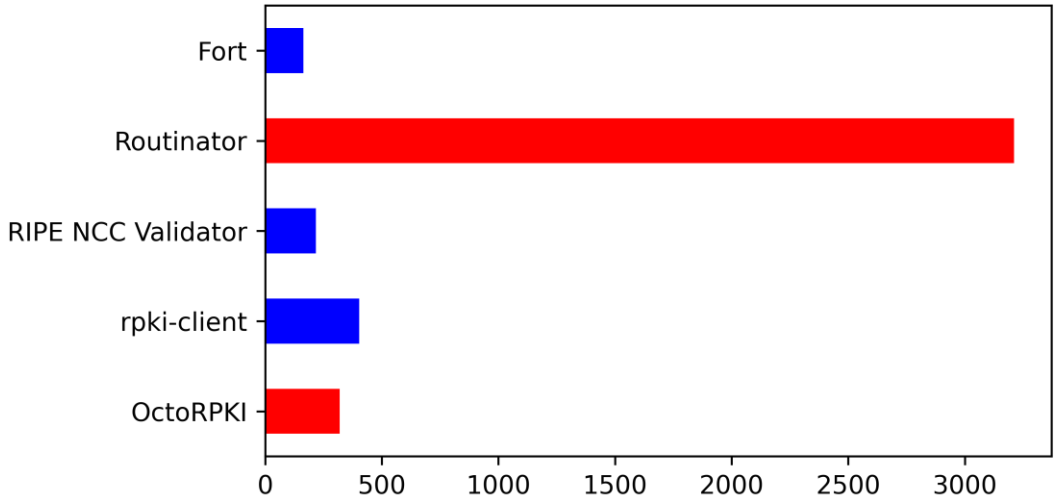
Generische Downgrade-Angriffe auf RPKI

- Angreifer setzt Repository mit RPKI Objekten auf
- Zertifikate-Kette:
  - Jedes Zertifikat zeigt auf Repository und auf das nächste Zertifikat
- Router verwenden Validators, um BGP-Route zu validieren, jede Route: „valid"/„invalid"/„unknown"
- Validator lädt alle RPKI-Objekte (inkl. Zertifikate) von allen Repositories
- Bleibt im Verfolgen langer Ketten hängen
- Kann keine weiteren RPKI Objekte herunterladen
- Präfixes mit fehlenden Objekten werden nicht validiert
- **Alle Anwendungen waren verwundbar**
- Auch Anwendung spezifischer Schwachstellen (z.B. CVE-2022-3029)



Implementierungs-spezifische Downgrade-Angriffe auf RPKI

- Routinator & OctoRPKI
  - können aus der Ferne abgeschaltet werden
  - sind die am häufigsten bzw. dritthäufigsten genutzten Validators



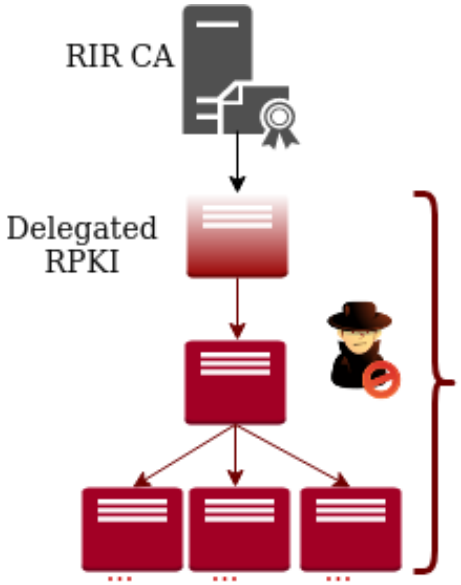
Verwundbarkeiten von Validators

- Trigger in Routinator:
  RPKI Objekte, die nicht base64-codiert sind
  - Routinator stürzt in dem Fall ab
  - Fällt nicht auf rsync zurück

- CVE 2022-3029 adressiert diesen Fehler

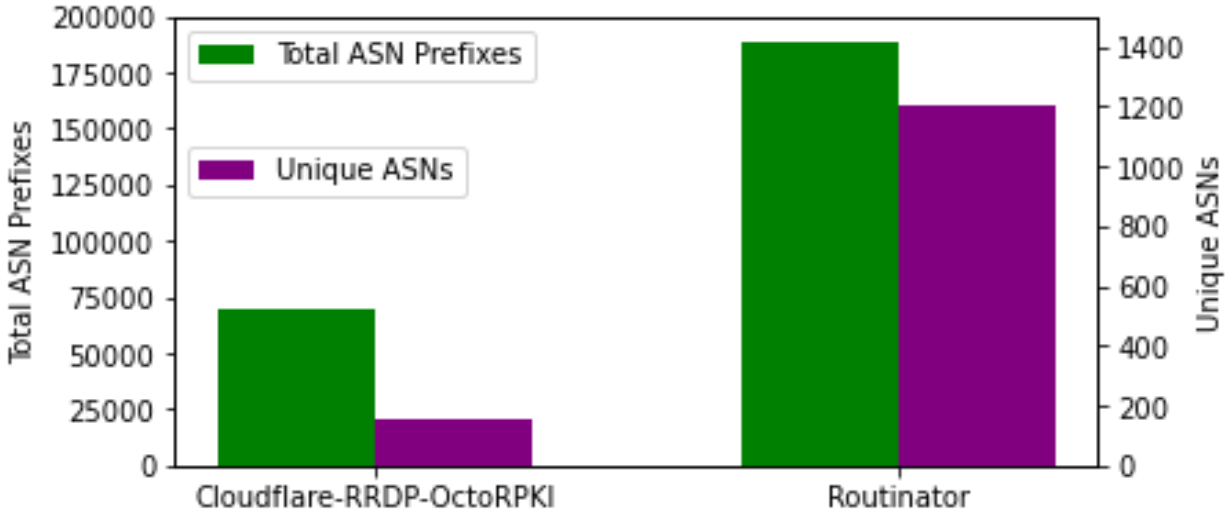
```
routinator::collector::rrdp Fatal: failed to write
    file /var/lib/routinator/rpki-cache/rrdp/
    malpubpoint.com/.../repo/testbed/0/ABC.crl:
    Encoded text cannot have a 6-bit remainder.
routinator::error Fatal error. Exiting.
```

- Trigger in OctoRPKI:
  Folge von Repositories, die die zuvor definierte Grenze von Max.Iterations überschreiten
  - OctoRPKI stürzt ab, wenn der Default Parameter überschritten wird
  - Nach Neustart wird *Max.Iterations* ignorier



Folgen für die Routing-Sicherheit

- Routinator ist in 75.5%, OctoRPKI in 9.4% aller Netze, die RPKI unterstützen
- Also: 84.9% aller Netze, die RPKI unterstützen, sind verwundbar
- Für insgesamt 257‘851 Prefixe kann ihr RPKI-Schutz aus der Ferne durch Fehler und/oder Angreifer abgeschaltet werden



Gliederung

Wie sicher sind Router und Routing?

1. **Sicherheitsanalyse in SOHO-Router**
   - Abhängigkeiten von Komponenten von Drittparteien (Bibliotheken, Module) führen zu Verwundbarkeiten
   - Implementierungsfehler unterbrechen die Erreichbarkeit von Netzen

2. **RPKI Validierung kann abgeschaltet werden**
   - Generische Verwundbarkeiten in Protokollspezifikationen
   - Verwundbarkeiten in spezifischen Implementierungen

3. **Schlussbemerkung: Sichere und vertrauenswürdige IT**

Sichere und vertrauenswürdige IT

Wie schützen wir uns vor nicht-vertrauenswürdiger IT?

- **Security by Design und Zertifizierung setzen vertrauenswürdigen Hersteller/Anbieter voraus**
- **Schutz vor nicht vertrauenswürdiger IT?**
  - Wann stellt sich die Frage?
    - Erhebliches Risiko beim Einsatz
    - Einfluss fremder Macht, die Werte nicht respektiert
    - Keine ausreichenden technischen Maßnahmen
- **Verbote national kaum machbar, §9b BSIG für KRITIS**
- **Warnungen §7 BSIG, „Vertrauen" als Kriterium umstritten**
- **Dringend nötig: Erweiterung §7 BSIG**

Wie Deutschland mit nicht vertrauenswürdiger IT besser umgehen kann, von Haya Shulman, Michael Waidner, FAZ vom 24.10.2022

Sichere und vertrauenswürdige IT

Woher bekommen wir vertrauenswürdige IT?

- **Security by Design und Zertifizierung setzen vertrauenswürdigen Hersteller/Anbieter voraus**
- **Vertrauen in Hersteller setzt voraus**
  - Kein Einfluss fremder Mächte, die Werte nicht respektieren
  - Ausreichende technische Maßnahmen
  - Security by Design, Zertifizierung, …
- **Verfügbarkeit solcher Hersteller und Produkte setzen voraus**
  - Wissen, Fähigkeiten, Forschung
  - Finanzielle Ressourcen
  - Ausreichender Markt

תודה רבה!

Merci beaucoup!

çok teşekkürler

谢谢

Thank you very much!

Vielen Dank!

Dank je wel!

Muchas gracias

ありがとうございます

Dziękuję!

zor spas

شكرا لك

Grazie mille!