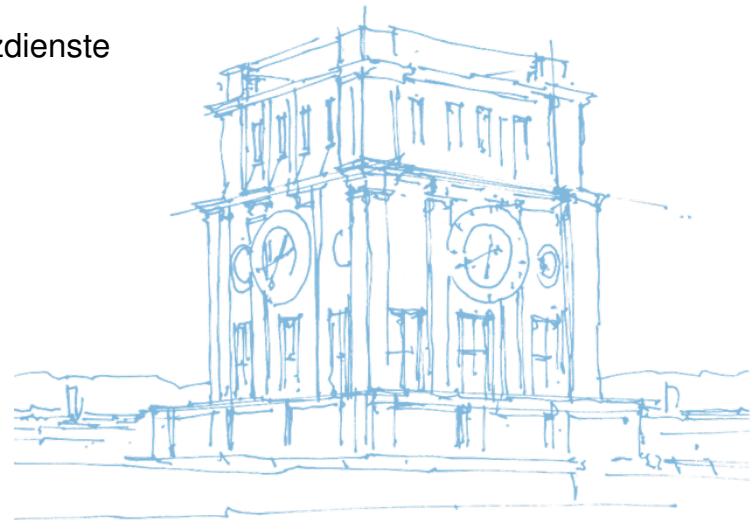
Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München

Öffentlich erreichbare Gebäudeautomatisierung: Amplification-Anfälligkeit von BACnet und Deployment-Analyse im Internet und DFN

Oliver Gasser, Quirin Scheitle, Carl Denis, Nadja Schricker, Georg Carle

14. Februar 2017

Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München



Überblick

Einführung und Motivation

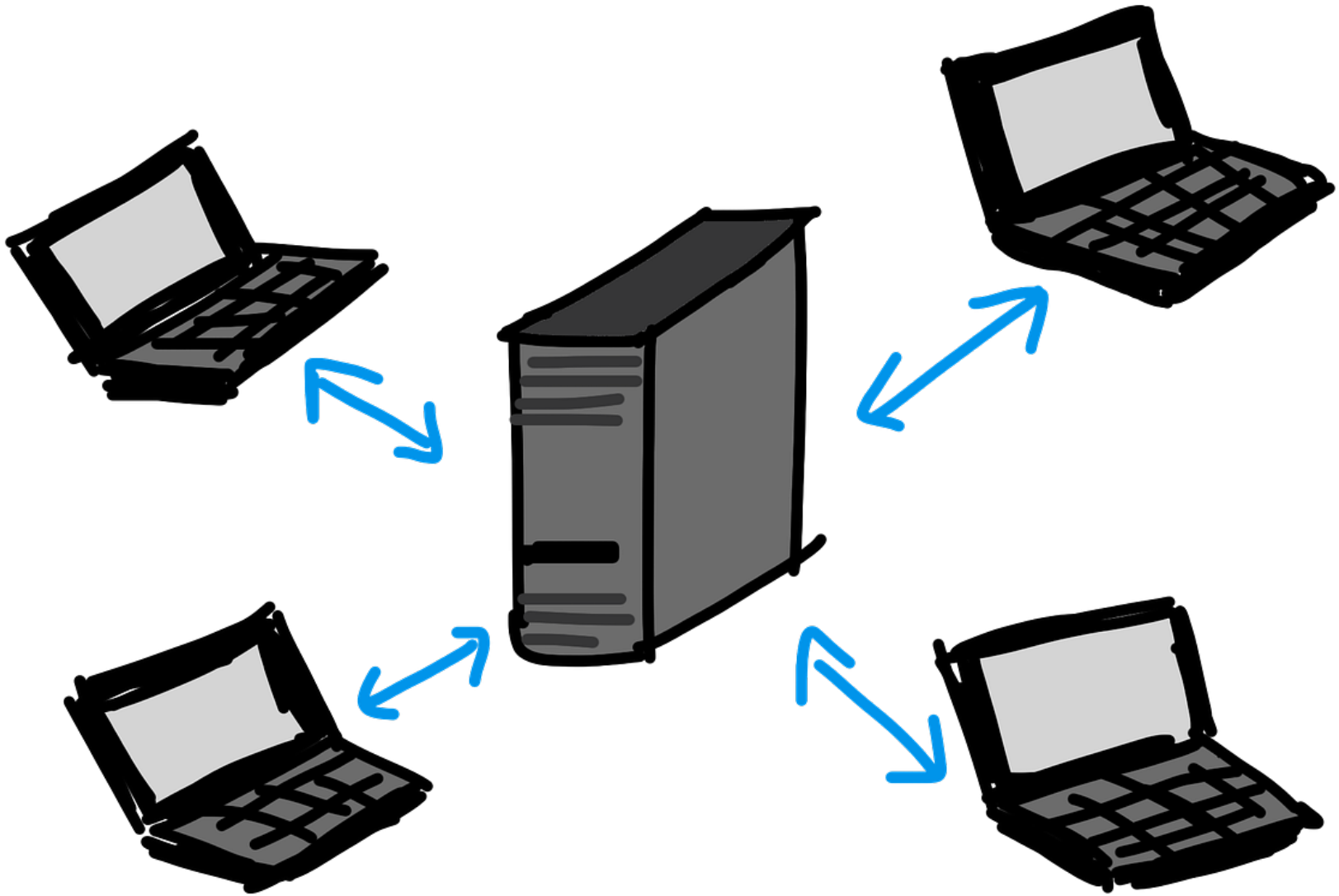
Das BACnet-Protokoll

Finden von BACnet-Geräten

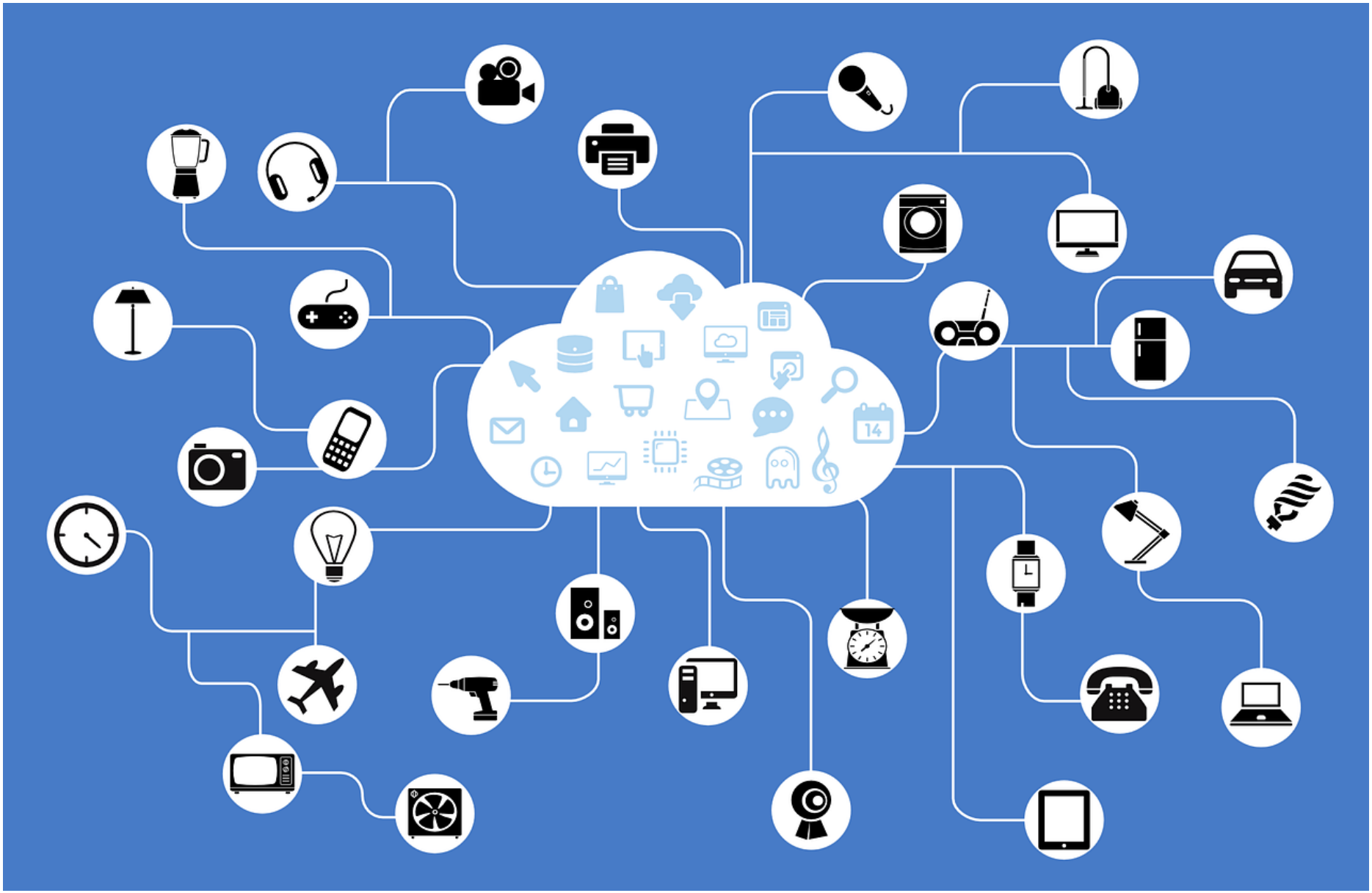
BACnet-Deployment

Amplification-Angriffe

Das Internet



Internet der Dinge



Risiken des Internet der Dinge

Immer mehr eingebettete Systeme im Internet

Sicherheitsrisiko

- Datendiebstahl & Manipulation
- Missbrauch für Angriffe

Beispiele

- Manipulation von Heizungsanlagen
- Mirai-Botnetz: Direkter Missbrauch von kompromittierten Überwachungskameras
- Spamhaus-Angriff: Indirekter Missbrauch von offenen DNS-Servern

Unser Ziel

- Finden von öffentlich erreichbaren Gebäudeautomatisierungsgeräten
- Analyse des BACnet-Deployments
- Aufzeigen des Missbrauchspotentials

BACnet

BACnet-Historie

- 1995: Building Automation and Control Networks
- 1999: BACnet/IP
- 2016: BACnet/IPv6

Einsatzgebiete

- Heizung
- Lüftung
- Klimatisierung
- Sicherheitstechnik

BACnet-Protokoll

Anfrage-Antwort-Protokoll

Verschiedene Dienste

- z.B. *ReadProperty*

Komplexes Paketformat

- Mehrstufige Header
- Markierte Payload mit Tags

BACnet/IP: UDP/47808

Finden von BACnet-Geräten

Internet-weite Scans nach BACnet/IP-Geräten

Minimieren der Aufdringlichkeit

- Nicht-Verändern des BACnet-Geräts
- Blacklist aus früheren Scans
- Drosseln der Scan-Geschwindigkeit
- Dediziertes Mess-Subnetz mit eigenem WHOIS-Eintrag
- Webserver mit Erläuterung der Untersuchung

Finden von BACnet-Geräten

Internet-weite Scans nach BACnet/IP-Geräten

Minimieren der Aufdringlichkeit

- Nicht-Verändern des BACnet-Geräts
- Blacklist aus früheren Scans
- Drosseln der Scan-Geschwindigkeit
- Dediziertes Mess-Subnetz mit eigenem WHOIS-Eintrag
- Webserver mit Erläuterung der Untersuchung

$\rightarrow$ Keine Abuse-Nachrichten erhalten

Analyse des BACnet-Deployments

Mehr als 13 000 BACnet-Geräte

- Hersteller
- Modelle
- Subnetze
- Autonome Systeme
- Geographische Verteilung

Hersteller

Abfrage von Hersteller-ID und -namen

Pos	Hersteller	Vorkommen	Häufigkeit [%]
1	Reliable Controls Corporation	2188	17,92
2	Tridium Inc.	1835	15,03
3	Delta Controls	1473	12,06
4	Johnson Controls Inc.	1394	11,42
5	Automated Logic Corporation	1065	8,72

Top 5 decken 65 % ab

Modelle

Abfrage des Modellnamens

Konsistenz mit Hersteller

- Reliable Controls $\rightarrow$ MachPro
- Tridium $\rightarrow$ NiagaraAX
- ...

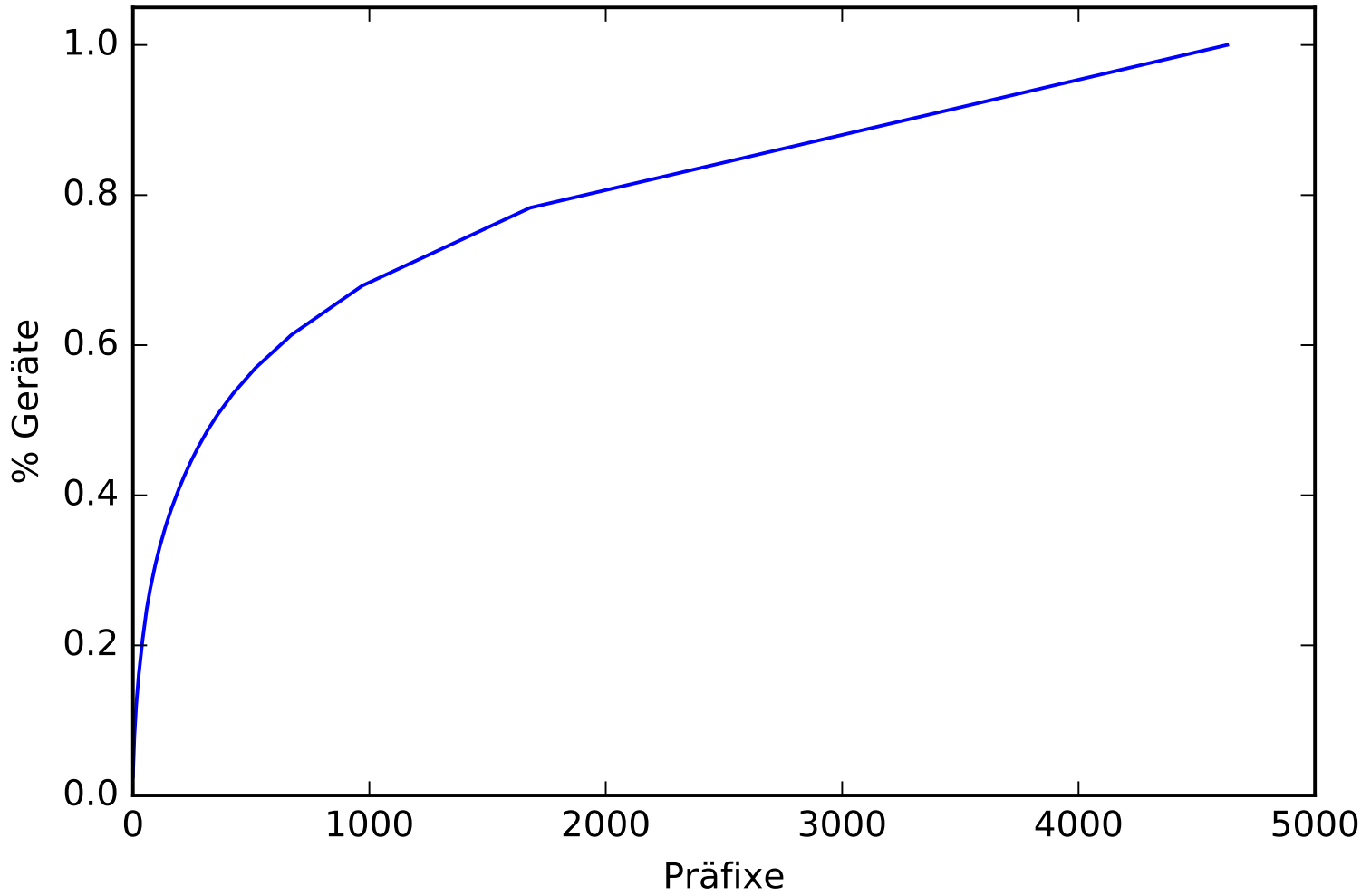
Häufung von BACnet-Geräten

Ziel: Finden von BACnet-Häufungen

Abbilden von IP-Adressen auf

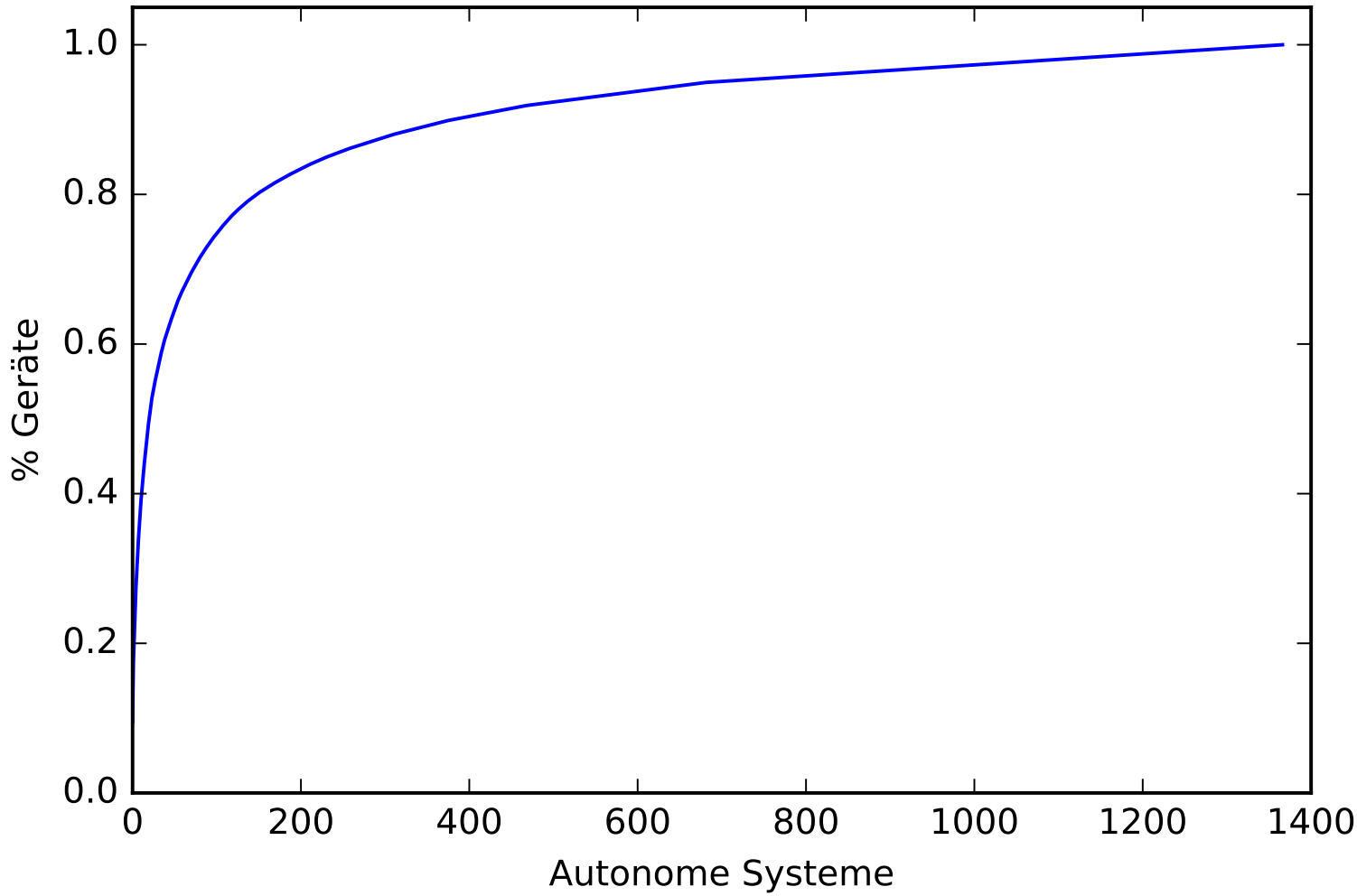
- Subnetze
- Autonome Systeme
- Länder

Subnetze



65 % der Geräte in 1000 Subnetzen

Autonome Systeme



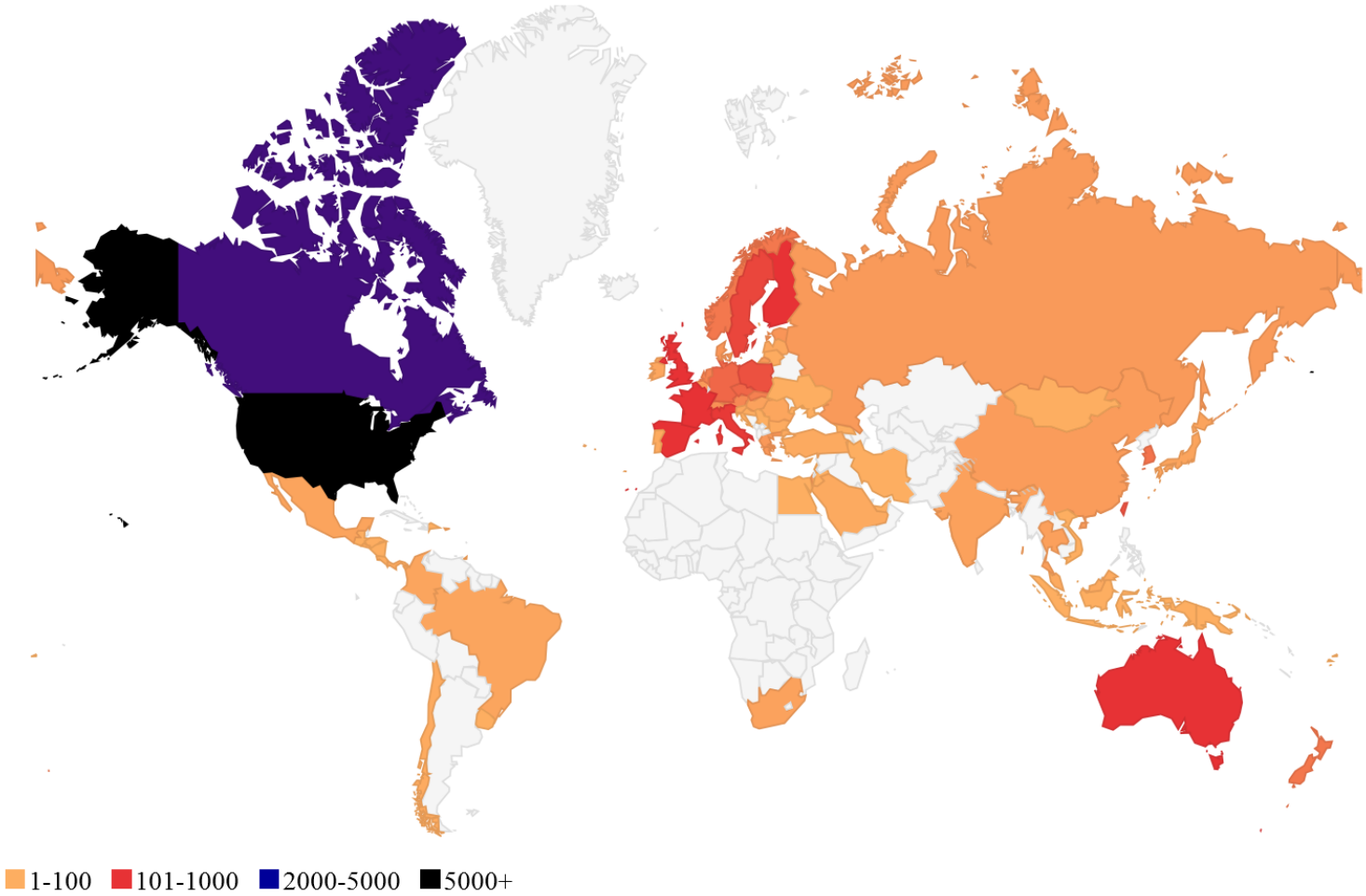
80 % der Geräte in 200 ASen

Autonome Systeme

Pos	Autonomes System	Vorkommen	Häufigkeit [%]
1	AT&T	1291	9,5 %
2	Comcast	1082	8,0 %
3	Verizon	522	3,8 %
4	Telus	486	3,6 %
5	Shaw	348	2,6 %

Top 5 decken 27 % ab

Länder



Top 5 decken 87 % ab

Zusammenfassung: Deployment

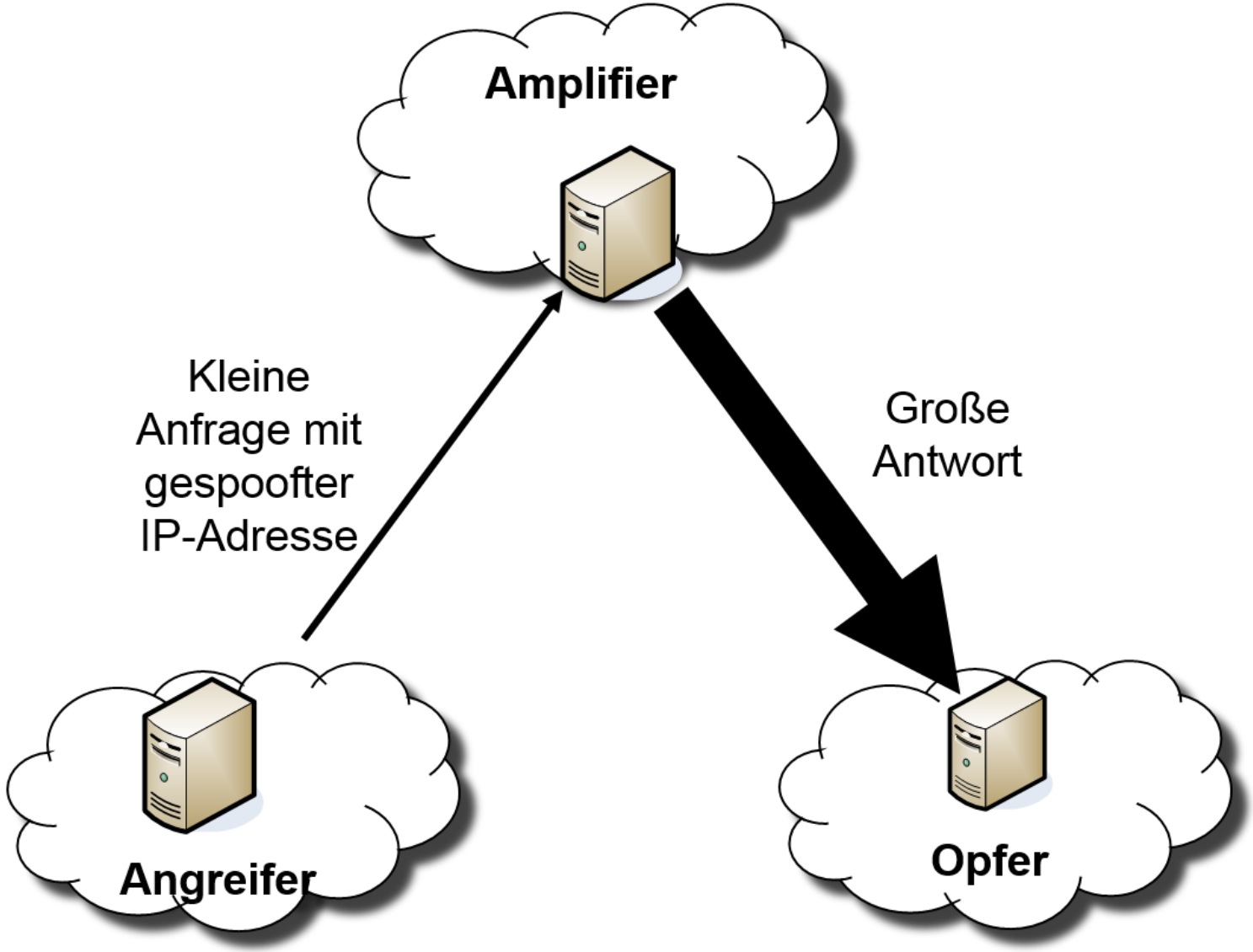
- 13 000 BACnet-Geräte offen im Internet erreichbar
- Markt von wenigen Herstellern dominiert
- Starke Häufung in ASen und Ländern

Zusammenfassung: Deployment

- 13 000 BACnet-Geräte offen im Internet erreichbar
- Markt von wenigen Herstellern dominiert
- Starke Häufung in ASen und Ländern

Frage: Können BACnet-Geräte für Angriffe missbraucht werden?

Amplification-Angriff



Charakteristika eines Amplification-Angriffs

- Zustandsloses Protokoll
  BACnet $\rightarrow$ UDP-basiert ✓

Charakteristika eines Amplification-Angriffs

- Zustandsloses Protokoll
  BACnet $\rightarrow$ UDP-basiert ✓
- Keine Authentifizierung
  BACnet $\rightarrow$ kein Handshake notwendig ✓

Charakteristika eines Amplification-Angriffs

- Zustandsloses Protokoll
  BACnet $\rightarrow$ UDP-basiert ✓
- Keine Authentifizierung
  BACnet $\rightarrow$ kein Handshake notwendig ✓
- Antwort ist größer als Anfrage
  BACnet $\rightarrow$ angefragte Property frei wählbar ✓

Amplification-Angriffe mit BACnet

In einer Anfrage können mehrere Properties angefragt werden

- Anfrage: Hersteller? Modell? Ort?
- Antwort: Tridium. NiagaraAX. Rothenbaumchaussee 10, Hamburg.

Amplification-Angriffe mit BACnet

In einer Anfrage können mehrere Properties angefragt werden

- Anfrage: Hersteller? Modell? Ort?
- Antwort: Tridium. NiagaraAX. Rothenbaumchaussee 10, Hamburg.

Dieselbe Property kann in einer Anfrage mehrmals angefragt werden

- Anfrage: Ort? Ort? Ort?
- Antwort: Rothenbaumchaussee 10, Hamburg. Rothenbaumchaussee 10, Hamburg. Rothenbaumchaussee 10, Hamburg.

Amplification-Angriffe mit BACnet

Beispielantwort

- Hwy 57; Located in the silver box on the electrical pole in front of Grove Primary Care Clinic. Pole 688

Abfragen derselben langen Property
$\rightarrow$ erhöhen des Amplification-Faktors

- BACnet: $\approx$ 30x
- DNS: $\approx$ 40x

Zusammenfassung: Amplification-Angriffe

- BACnet-Protokoll anfällig für Amplification-Angriffe
- Dieselbe Property kann mehrmals angefragt werden
- Amplification-Faktor $\approx$ 30x

Empfehlungen

- BACnet-Geräte sollten nicht im öffentliche Internet erreichbar sein (Abgekoppeltes Subnetz, VPN, Firewall)
- Erkennen von Amplification-Angriffen durch Entropieüberwachung
- Drosseln von BACnet-Verkehr
- Standardisierung: Jede Property max. einmal pro Anfrage

Nächste Schritte

- Weitere Untersuchung der Amplification-Angriff-Anfälligkeit
- Benachrichtigung der Betreiber via DFN-CERT
- Kontinuierliche Beobachtung des BACnet-Deployments

Ende

Vielen Dank für Ihre Aufmerksamkeit!

Oliver Gasser <gasser@net.in.tum.de>
https://www.net.in.tum.de/~gasser/