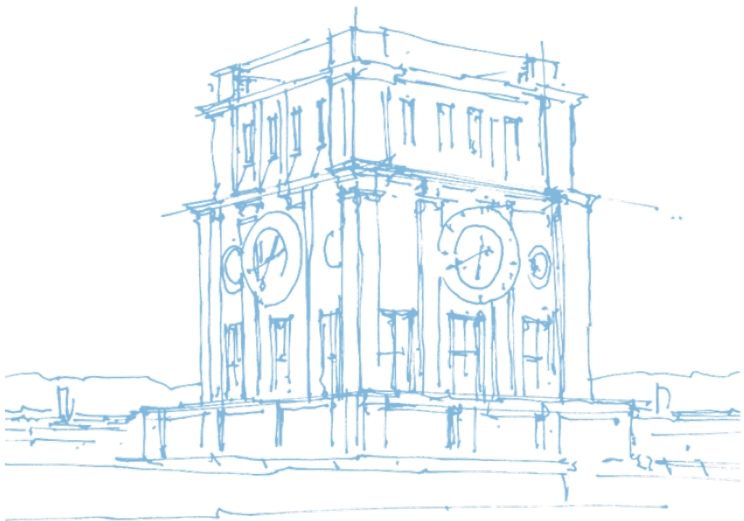
Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München

BACnet – Wie Gebäudeautomatisierung das Internet bedroht

Oliver Gasser

30. November 2017

Lehrstuhl für Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München



Gemeinsame Arbeit






Gebäudeautomatisierung @ TUMi8

Orchestrierung und Crowdsourcing in Smart Spaces

- “Crowdsourced Context-Modeling as Key to Future Smart Spaces”, NOMS 2014 [2].
- “Distributed Smart Space Orchestration”, NOMS 2016 [3].

Smart Neighborhoods

- “Enabling Sustainable Smart Neighborhoods”, SustainIT 2013 [4].

Worum geht es in diesem Vortrag?

Es geht **nicht** um die vielen positiven neuen Möglichkeiten von IoT

Worum geht es in diesem Vortrag?

Es geht **nicht** um die vielen positiven neuen Möglichkeiten von IoT

Es geht um die Gefahren, die mit IoT einherkommen

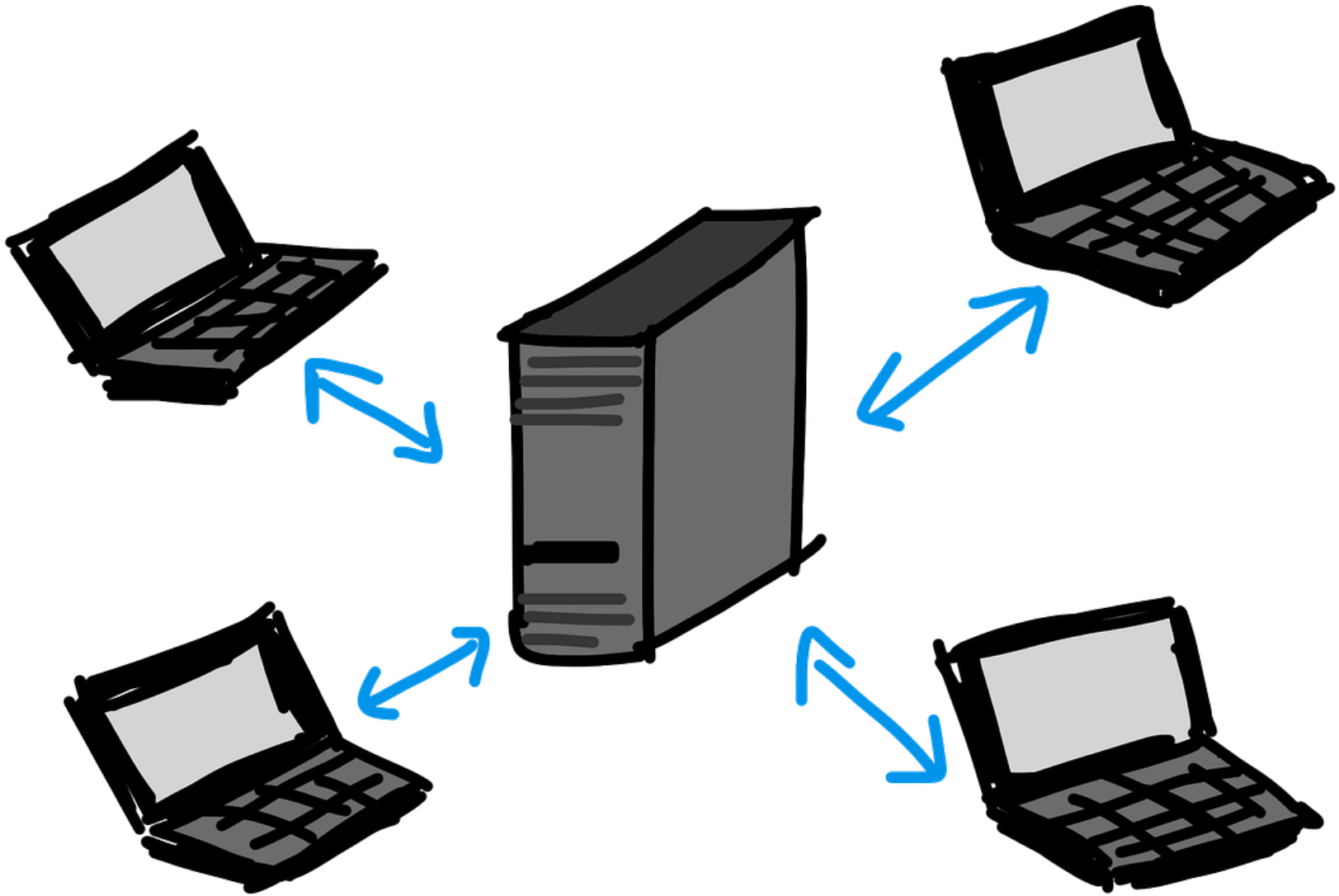
Worum geht es in diesem Vortrag?

Es geht **nicht** um die vielen positiven neuen Möglichkeiten von IoT

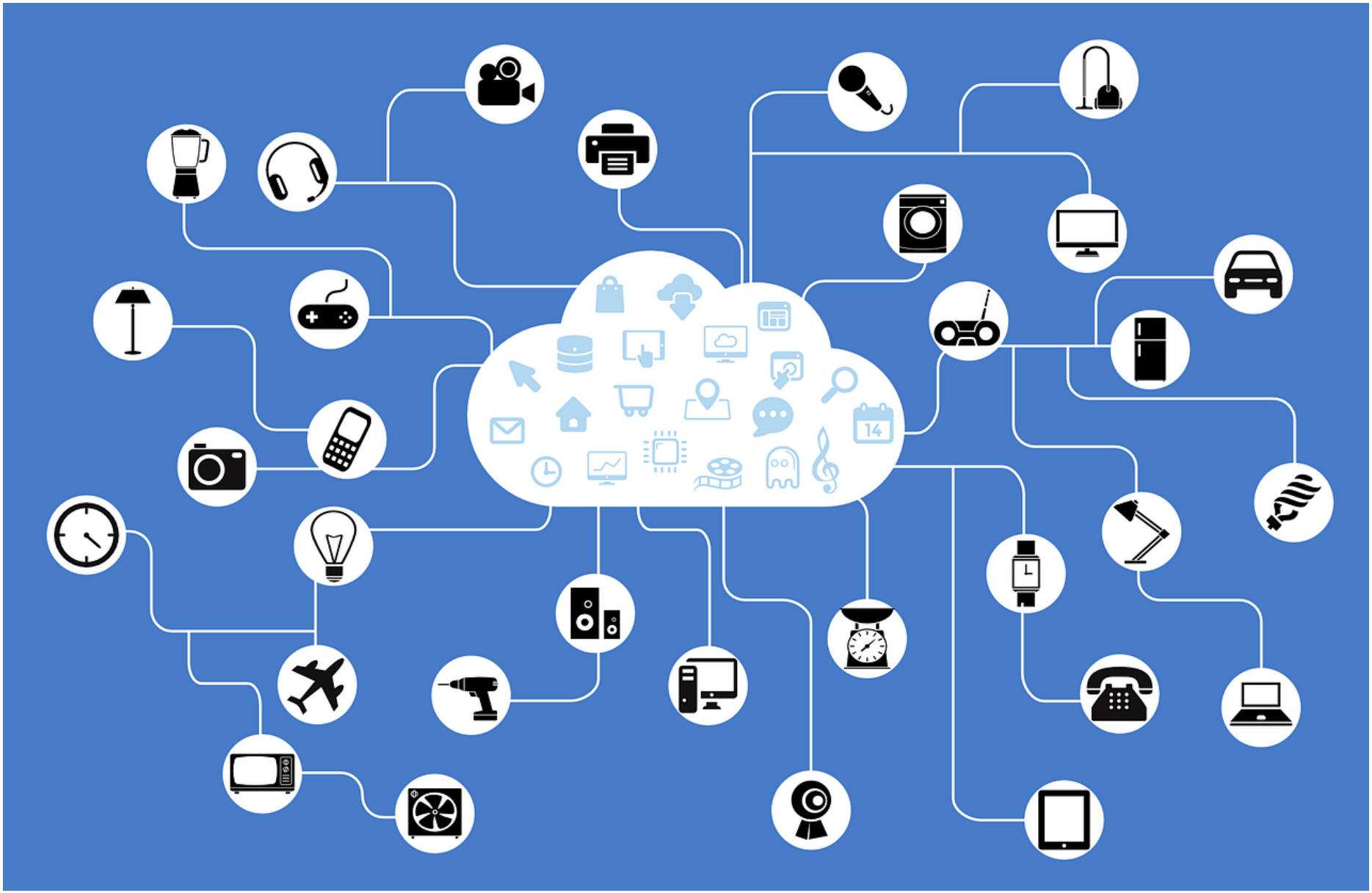
Es geht um die Gefahren, die mit IoT einherkommen

Die Gefahren von IoT am Beispiel von BACnet

Das Internet vor 20 Jahren



Das Internet heute



Risiken des Internet der Dinge

Immer mehr eingebettete Systeme im Internet

Implikationen von Internet-Zugriff meisten Nutzern nicht bewusst

Sicherheitsrisiken

- Datendiebstahl
- Privatsphäre
- Manipulation der Geräte
- Missbrauch für Angriffe (z.B. Mirai-Botnetz)

Unser Ziel

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

BACnet

BACnet-Historie

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

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-basiert

Finden von BACnet-Geräten

Internet-weite Scans nach BACnet/IP-Geräten

- Scan auf 16 BACnet-Ports
- ZMap mit spezieller UDP-Payload
- IPv4- und IPv6-Scans

Finden von BACnet-Geräten

Internet-weite Scans nach BACnet/IP-Geräten

- Scan auf 16 BACnet-Ports
- ZMap mit spezieller UDP-Payload
- IPv4- und IPv6-Scans

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

- Scan auf 16 BACnet-Ports
- ZMap mit spezieller UDP-Payload
- IPv4- und IPv6-Scans

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

→ Keine Abuse-Nachrichten erhalten ✓

Was haben wir gefunden?

Niemand würde BACnet-Geräte direkt ans Internet anschließen, oder?

Was haben wir gefunden?

~~Niemand würde BACnet-Geräte direkt ans Internet anschließen, oder?~~ **Doch**

Was haben wir gefunden?

~~Niemand würde BACnet-Geräte direkt ans Internet anschließen, oder?~~ **Doch**

Mehr als 16 k öffentlich erreichbare BACnet-Geräte

Was haben wir gefunden?

~~Niemand würde BACnet-Geräte direkt ans Internet anschließen, oder?~~ **Doch**

Mehr als 16 k öffentlich erreichbare BACnet-Geräte

Starkes Clustering

- Top 5 Autonome Systeme beinhalten $\approx$ 30 % aller Geräte
- 60 % in USA, 20 % in Kanada
- Top 3 Hersteller machen $\approx$ 50 % aller Geräte aus

Konsequenzen für die IT-Sicherheit

Welche Konsequenzen haben BACnet-Geräte für die Sicherheit im Internet?

Konsequenzen für die IT-Sicherheit

Welche Konsequenzen haben BACnet-Geräte für die Sicherheit im Internet?

- Datendiebstahl
- Privatsphäre
- Manipulation der Geräte
- Missbrauch für Angriffe

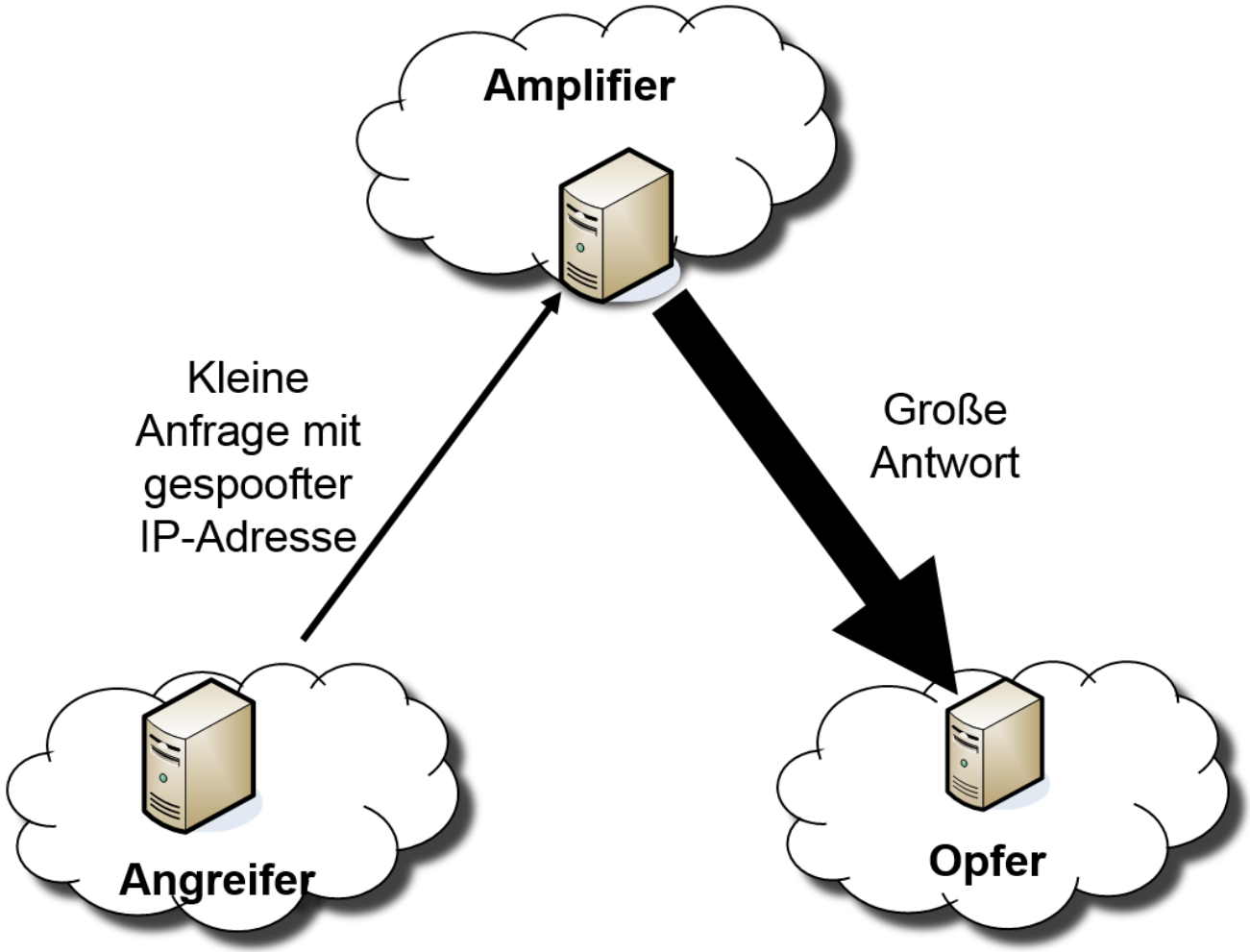
Konsequenzen für die IT-Sicherheit

Welche Konsequenzen haben BACnet-Geräte für die Sicherheit im Internet?

- Datendiebstahl
- Privatsphäre
- Manipulation der Geräte
- **Missbrauch für Angriffe**

Amplification-Angriff

Spezielle Art von DDoS-Angriff



Charakteristika eines Amplification-Angriffs

- Zustandsloses Protokoll

Charakteristika eines Amplification-Angriffs

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

Charakteristika eines Amplification-Angriffs

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

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

Charakteristika eines Amplification-Angriffs

- Zustandsloses Protokoll
  BACnet $\rightarrow$ UDP-basiert ✓
- Keine Authentifizierung
  BACnet $\rightarrow$ kein Handshake notwendig ✓
- Antwort ist größer als Anfrage
  BACnet $\rightarrow$ **?**

BACnet Amplification-Faktor

Amplification-Angriff: Kleine Anfrage und große Antwort

BACnet Amplification-Faktor

Amplification-Angriff: Kleine Anfrage und große Antwort

BACnet:

- Anfragegröße: Header-Overhead + ID der angefragten BACnet-Property
- Antwortgröße: Abhängig von der angefragten BACnet-Property

BACnet Amplification-Faktor

Amplification-Angriff: Kleine Anfrage und große Antwort

BACnet:

- Anfragegröße: Header-Overhead + ID der angefragten BACnet-Property
- Antwortgröße: Abhängig von der angefragten BACnet-Property

Beispiel:

- Anfrage: *ID 58? (Location?)*
- Antwort: *Fraunhofer SIT, Rheinstraße 75, 64295 Darmstadt.*

Maximierung des Amplification-Faktors

Eine Property anfragen ist schön und gut, aber. . .

- Header-Overhead ist relativ groß
- Nicht alle Geräte unterstützen die angefragte Property

Maximierung des Amplification-Faktors

Eine Property anfragen ist schön und gut, aber. . .

- Header-Overhead ist relativ groß
- Nicht alle Geräte unterstützen die angefragte Property

ReadPropertyMultiple-Anfrage

- Schicke Anfrage mit einer Liste an Properties
- Verringert Header-Overhead
- Höhere Wahrscheinlichkeit, dass eine der Properties unterstützt wird

Maximierung des Amplification-Faktors

Eine Property anfragen ist schön und gut, aber...

- Header-Overhead ist relativ groß
- Nicht alle Geräte unterstützen die angefragte Property

ReadPropertyMultiple-Anfrage

- Schicke Anfrage mit einer Liste an Properties
- Verringert Header-Overhead
- Höhere Wahrscheinlichkeit, dass eine der Properties unterstützt wird

Beispiel:

- Anfrage: *ID 58? ID 70? ID 121? (Location? Modellname? Herstellername?)*
- Antwort: *Fraunhofer SIT, Rheinstraße 75, 64295 Darmstadt., Niagara AX, Tridium Inc.*

Maximaximierung des Amplification-Faktors

Es kann doch nicht noch schlimmer kommen, oder?

Maximaximierung des Amplification-Faktors

~~Es kann doch nicht noch schlimmer kommen, oder?~~ **Doch**

Maximaximierung des Amplification-Faktors

~~Es kann doch nicht noch schlimmer kommen, oder?~~ **Doch**

- Anfrage: *ID 58? ID 58? ID 58?*
- Antwort: *Fraunhofer SIT, Rheinstraße 75, 64295 Darmstadt. Fraunhofer SIT, Rheinstraße 75, 64295 Darmstadt. Fraunhofer SIT, Rheinstraße 75, 64295 Darmstadt.*

Maximaximierung des Amplification-Faktors

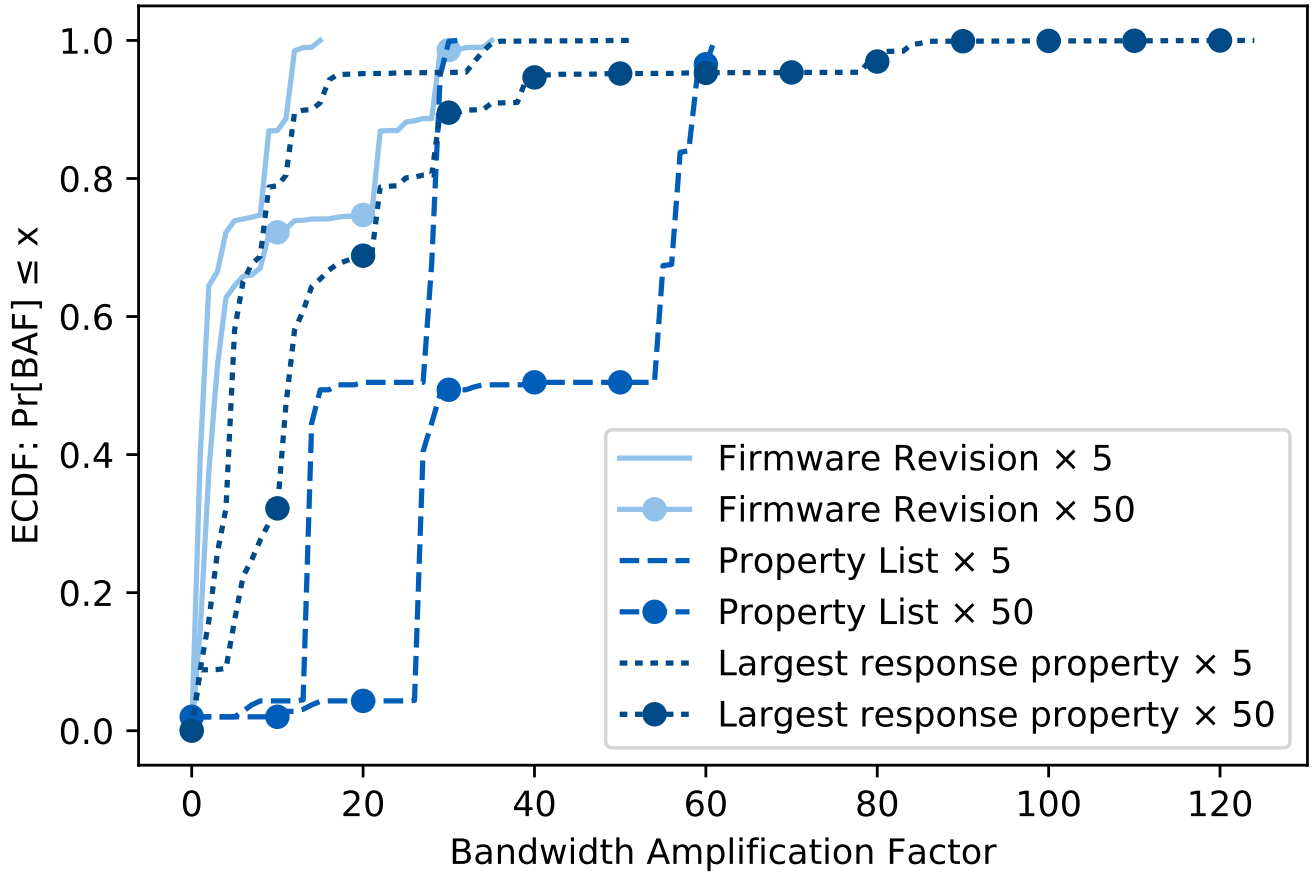
~~Es kann doch nicht noch schlimmer kommen, oder?~~ **Doch**

- Anfrage: *ID 58? ID 58? ID 58?*
- Antwort: *Fraunhofer SIT, Rheinstraße 75, 64295 Darmstadt. Fraunhofer SIT, Rheinstraße 75, 64295 Darmstadt. Fraunhofer SIT, Rheinstraße 75, 64295 Darmstadt.*

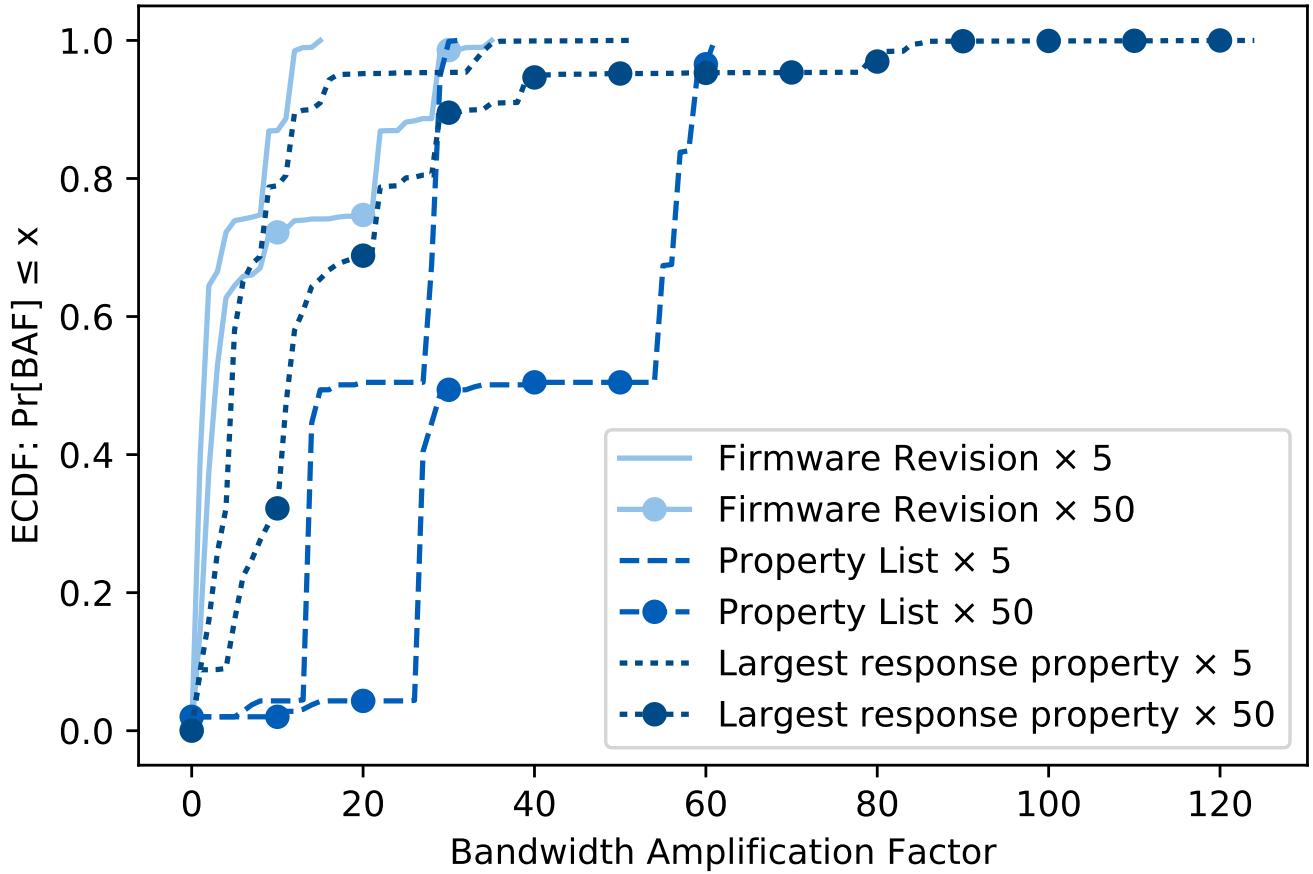
Mehrmaliges Anfragen **derselben Property** innerhalb einer Anfrage

- Property mit höchstem Amplification-Faktor auswählen
- Verringert Header-Overhead zusätzlich
- Maximiert Amplification-Faktor

Amplification-Faktor bei BACnet



Amplification-Faktor bei BACnet



- 30 % der Geräte erlauben Amplification-Faktor von 20 oder größer
- Property List gibt größten Amplification-Faktor, aber nicht alle Geräte unterstützen diese Property
- Vergleichbar mit offenen DNS Resolvern

Amplification-Angriffe mit BACnet

- Zustandsloses Protokoll
  BACnet $\rightarrow$ UDP-basiert ✓
- Keine Authentifizierung
  BACnet $\rightarrow$ kein Handshake notwendig ✓
- Antwort ist größer als Anfrage
  BACnet $\rightarrow$ **?**

Amplification-Angriffe mit BACnet

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

Empfehlungen

- BACnet-Geräte sollten nicht im öffentlichen Internet erreichbar sein
  - Abgekoppeltes Subnetz
  - VPN
  - Firewall
- Drosseln von BACnet-Verkehr
- Standardisierung: Jede Property max. einmal pro Anfrage

Notification-Kampagne

Was können wir als Forscher tun, um die Situation zu verbessern?

Notification-Kampagne

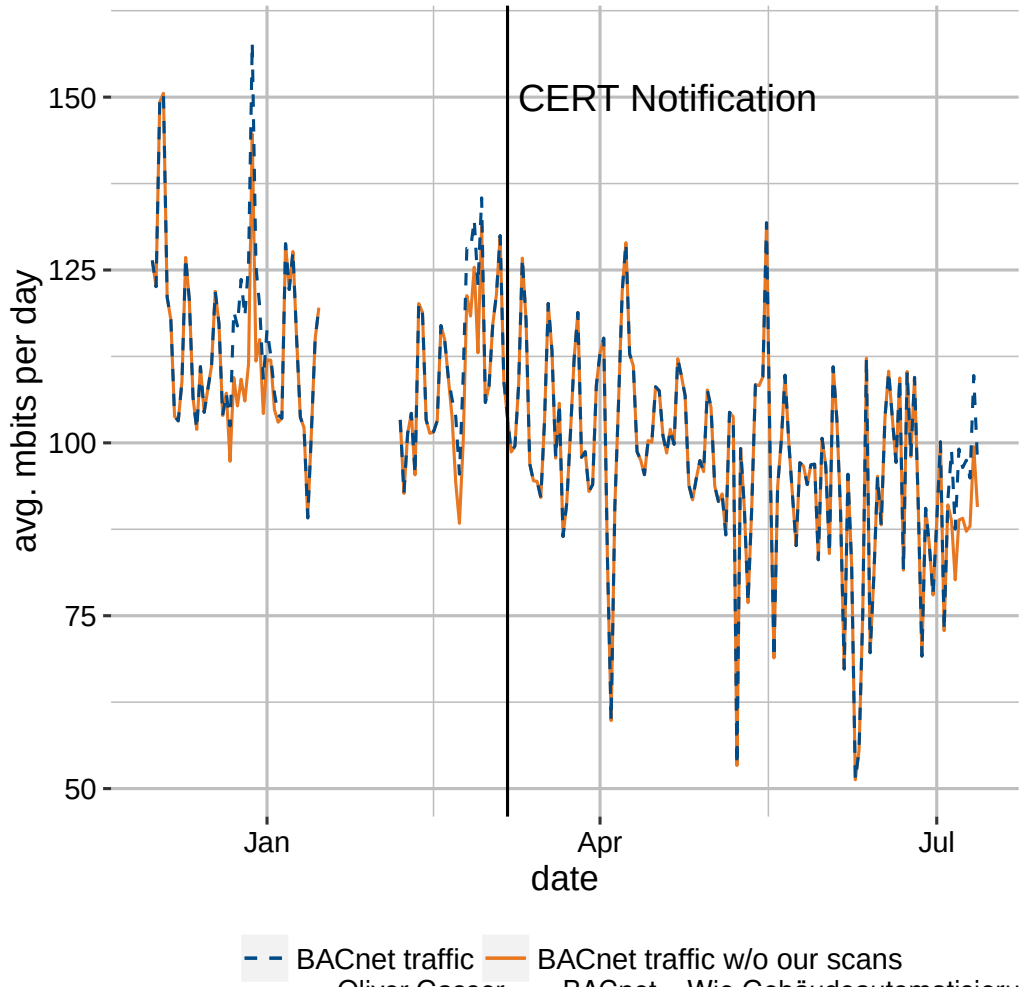
Was können wir als Forscher tun, um die Situation zu verbessern?

- Notification-Kampagne in Kooperation mit dem DFN-CERT im März 2017
- Leichter Rückgang des BACnet-Verkehrs an deutschem IXP

Notification-Kampagne

Was können wir als Forscher tun, um die Situation zu verbessern?

- Notification-Kampagne in Kooperation mit dem DFN-CERT im März 2017
- Leichter Rückgang des BACnet-Verkehrs an deutschem IXP



Passive Verkehrsanalyse

Wird BACnet für Angriffe verwendet?

Passive Verkehrsanalyse

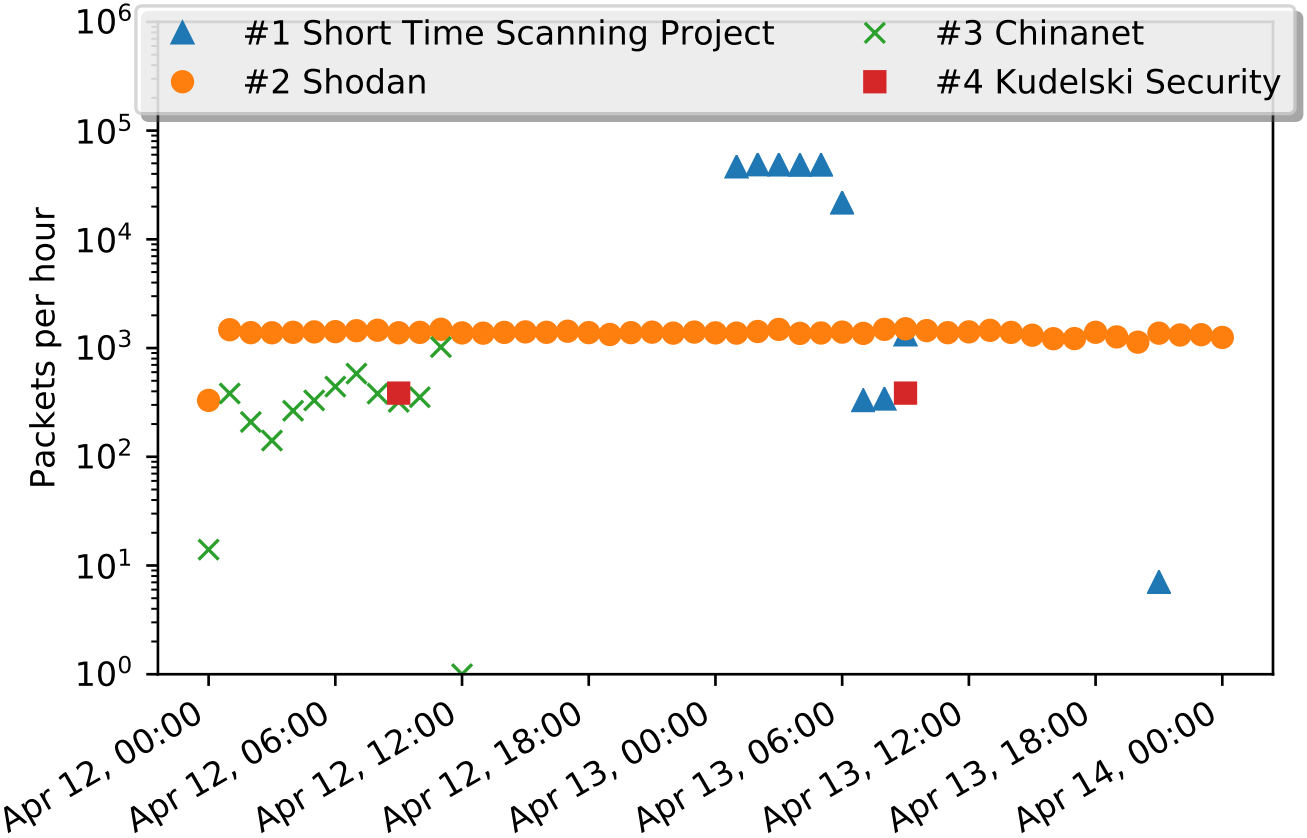
Wird BACnet für Angriffe verwendet?

- Analyse des MAWI-Datensatzes (April 2017)
- Nur BACnet-Scan-Traffic, keine bidirektionale Kommunikation

Passive Verkehrsanalyse

Wird BACnet für Angriffe verwendet?

- Analyse des MAWI-Datensatzes (April 2017)
- Nur BACnet-Scan-Traffic, keine bidirektionale Kommunikation



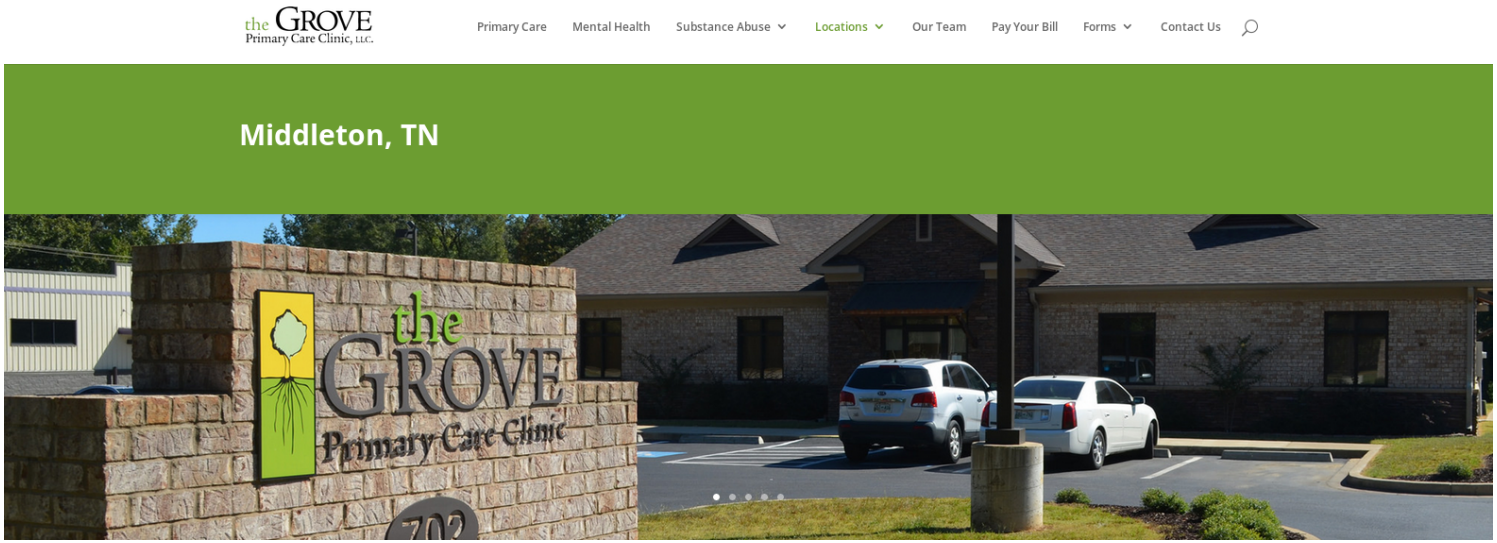
Reale Antwort auf Location-Anfrage

Reale Antwort auf Location-Anfrage

Hwy 57; Located in the silver box on the electrical pole in front of Grove Primary Care Clinic. Pole 123

Reale Antwort auf Location-Anfrage

Hwy 57; Located in the silver box on the electrical pole in front of Grove Primary Care Clinic. Pole 123



Reale Antwort auf Location-Anfrage

Hwy 57; Located in the silver box on the electrical pole in front of Grove Primary Care Clinic. Pole 123

Reale Antwort auf Location-Anfrage

Hwy 57; Located in the silver box on the electrical pole in front of Grove Primary Care Clinic. Pole 123

Reale Antwort auf Location-Anfrage

Hwy 57; Located in the silver box on the electrical pole in front of Grove Primary Care Clinic. Pole 123

Reale Antwort auf Location-Anfrage

Hwy 57; Located in the silver box on the electrical pole in front of Grove Primary Care Clinic. Pole 123

Zusammenfassung

Mehr als 16 k BACnet-Geräte im Internet erreichbar

BACnet-Protokoll ist anfällig für Amplification-Angriffe

Notification-Kampagne um Situation zu verbessern

Mehr Detailinformationen:

- “The Amplification Threat Posed by Publicly Reachable BACnet Devices”, Gasser et al., JCSM’17 [1].

Ende

Vielen Dank für Ihre Aufmerksamkeit!

Für Rückfragen oder bei Interesse an Kooperationen gerne melden bei

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

Bibliographie

[1] O. Gasser, Q. Scheitle, B. Rudolph, C. Denis, N. Schricker, and G. Carle.
The Amplification Threat Posed by Publicly Reachable BACnet Devices.
Journal of Cyber Security and Mobility, 2017.

[2] M.-O. Pahl and G. Carle.
Crowdsourced Context-Modeling as Key to Future Smart Spaces.
In *Network Operations and Management Symposium 2014 (NOMS 2014)*, May 2014.

[3] M.-O. Pahl, G. Carle, and G. Klinker.
Distributed Smart Space Orchestration.
In *Network Operations and Management Symposium 2016 (NOMS 2016) - Dissertation Digest*, May 2016.

[4] M.-O. Pahl, H. Niedermayer, H. Kinkelin, and G. Carle.
Enabling Sustainable Smart Neighborhoods.
In *3rd IFIP Conference on Sustainable Internet and ICT for Sustainability 2013 (SustainIT 2013)*, Palermo, Italy, Oct. 2013.