Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Security Implications of Publicly Reachable Building Automation Systems

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

Thursday 25th May, 2017

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Outline

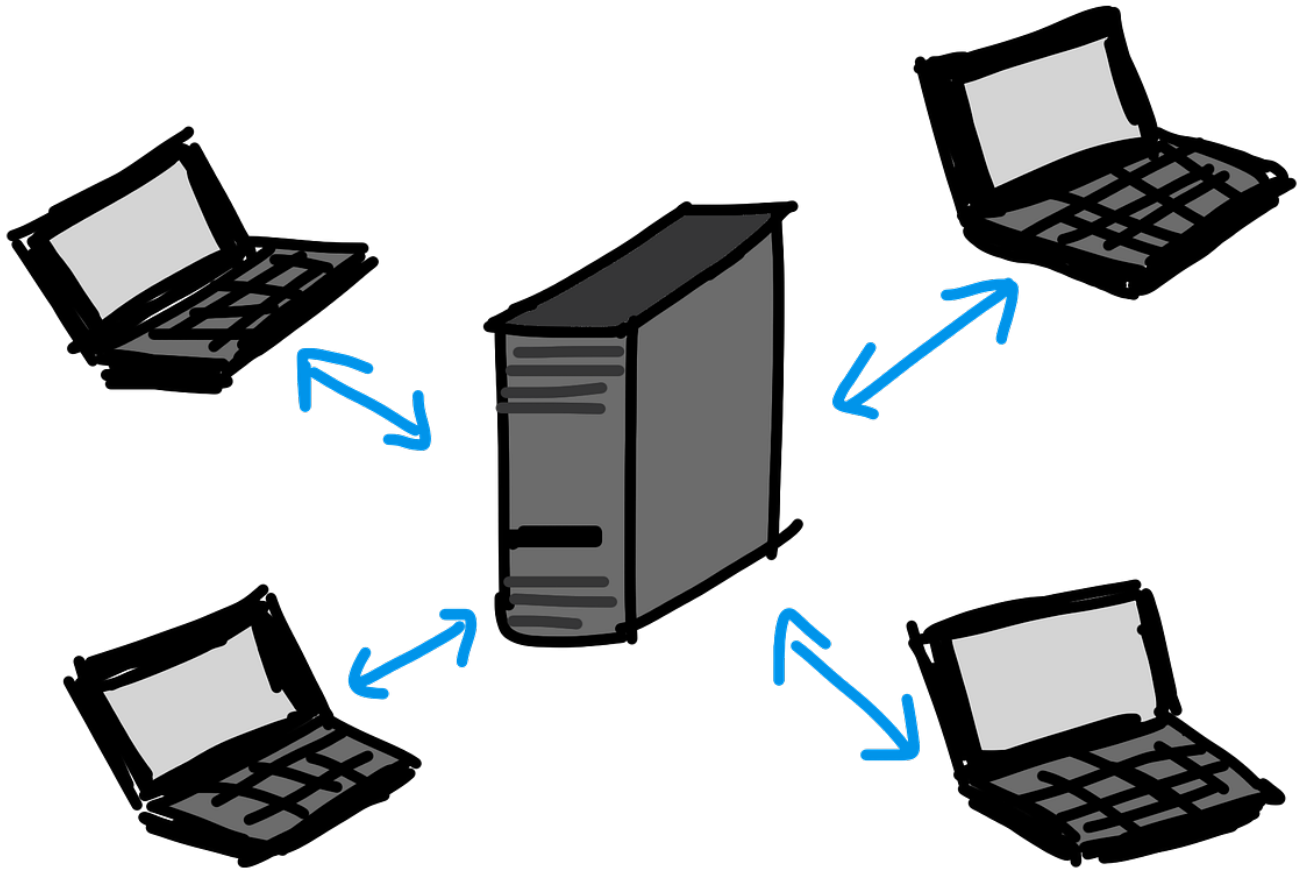
Motivation

Building Automation Protocol

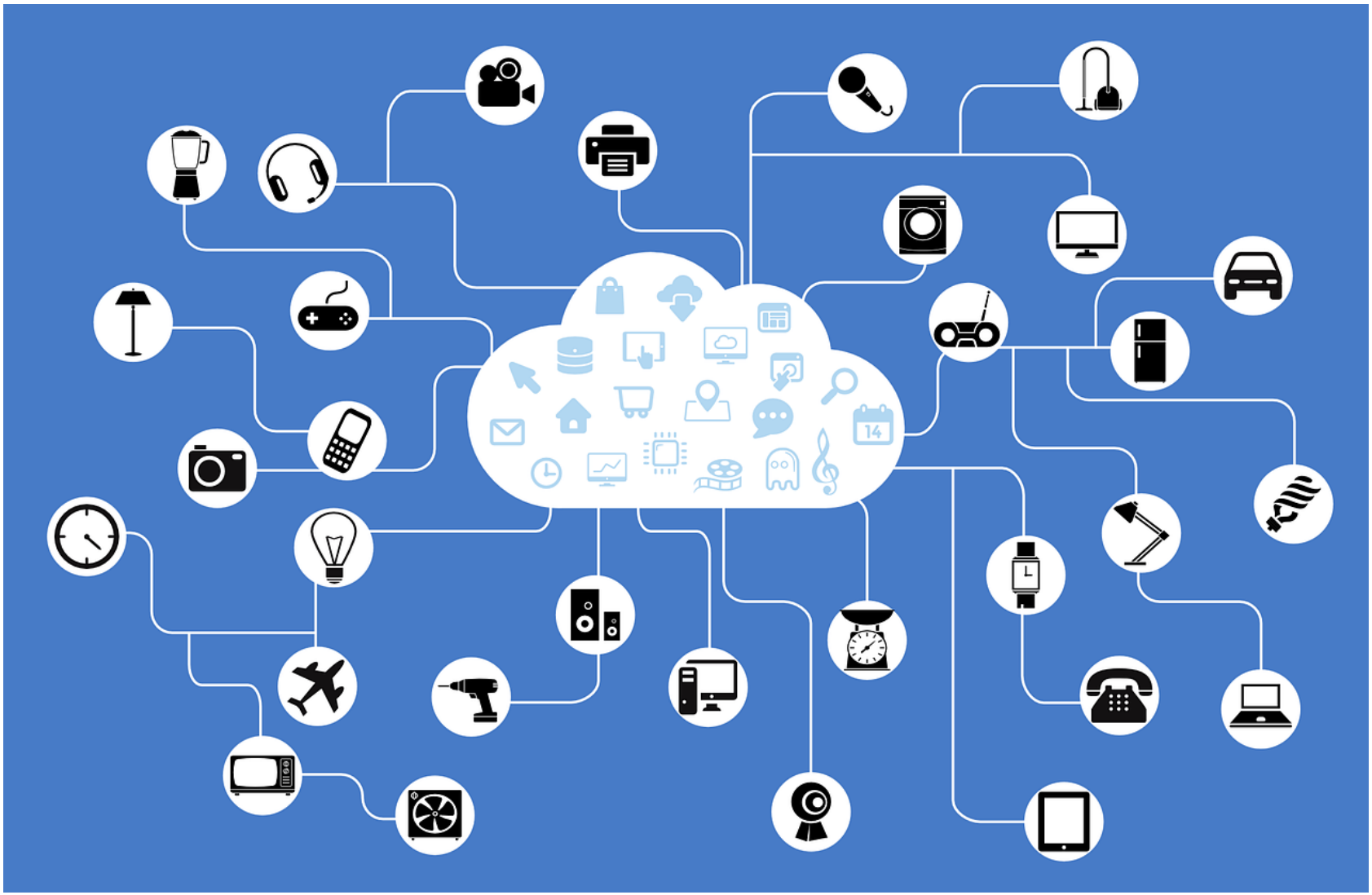
Finding Building Automation Devices

Security Implications

The Internet?



The Internet



Internet of Things

- More and more embedded systems and devices
- Implications of network connectivity unclear to most users
- Security risk
  - Data theft
  - Privacy
  - Manipulating operation of devices
  - Misuse for attacks (*e.g.*, Mirai botnet)

Our goal

- Find publicly accessible building automation systems
- Evaluate deployment
- Analyze security implications

BACnet

History:

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

BACnet

History:

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

Use cases:

- Heating
- Ventilation
- Air conditioning
- Security systems

BACnet protocol

- Request-response protocol
- Various services, *e.g., ReadProperty*
- UDP-based

Finding BACnet devices

BACnet scanning:

- Scan for 16 BACnet ports
- ZMap with custom UDP payload
- IPv4 and IPv6 scans

Finding BACnet devices

BACnet scanning:

- Scan for 16 BACnet ports
- ZMap with custom UDP payload
- IPv4 and IPv6 scans

Minimizing scan intrusiveness:

- Non-modification of BACnet devices
- Blacklist from previous scans
- Limited packet rate
- Dedicated measurement network
- Website explaining measurements

Finding BACnet devices

BACnet scanning:

- Scan for 16 BACnet ports
- ZMap with custom UDP payload
- IPv4 and IPv6 scans

Minimizing scan intrusiveness:

- Non-modification of BACnet devices
- Blacklist from previous scans
- Limited packet rate
- Dedicated measurement network
- Website explaining measurements

→ No abuse emails ✓

What did we find?

No one would attach a BACnet device to the Internet, right?

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

What did we find?

~~No one would attach a BACnet device to the Internet, right?~~ **Wrong**

What did we find?

~~No one would attach a BACnet device to the Internet, right?~~ **Wrong**

Found more than 16 k publicly reachable BACnet devices

What did we find?

~~No one would attach a BACnet device to the Internet, right?~~ **Wrong**

Found more than 16 k publicly reachable BACnet devices

Significant clustering

- Top 5 ASes $\approx$ 30 % of total 1439 ASes
- 60 % in US, 20 % in Canada
- Top 3 vendors $\approx$ 50 % of total 97 vendors

Security implications

What are the security implications of publicly reachable BACnet devices?

Security implications

What are the security implications of publicly reachable BACnet devices?

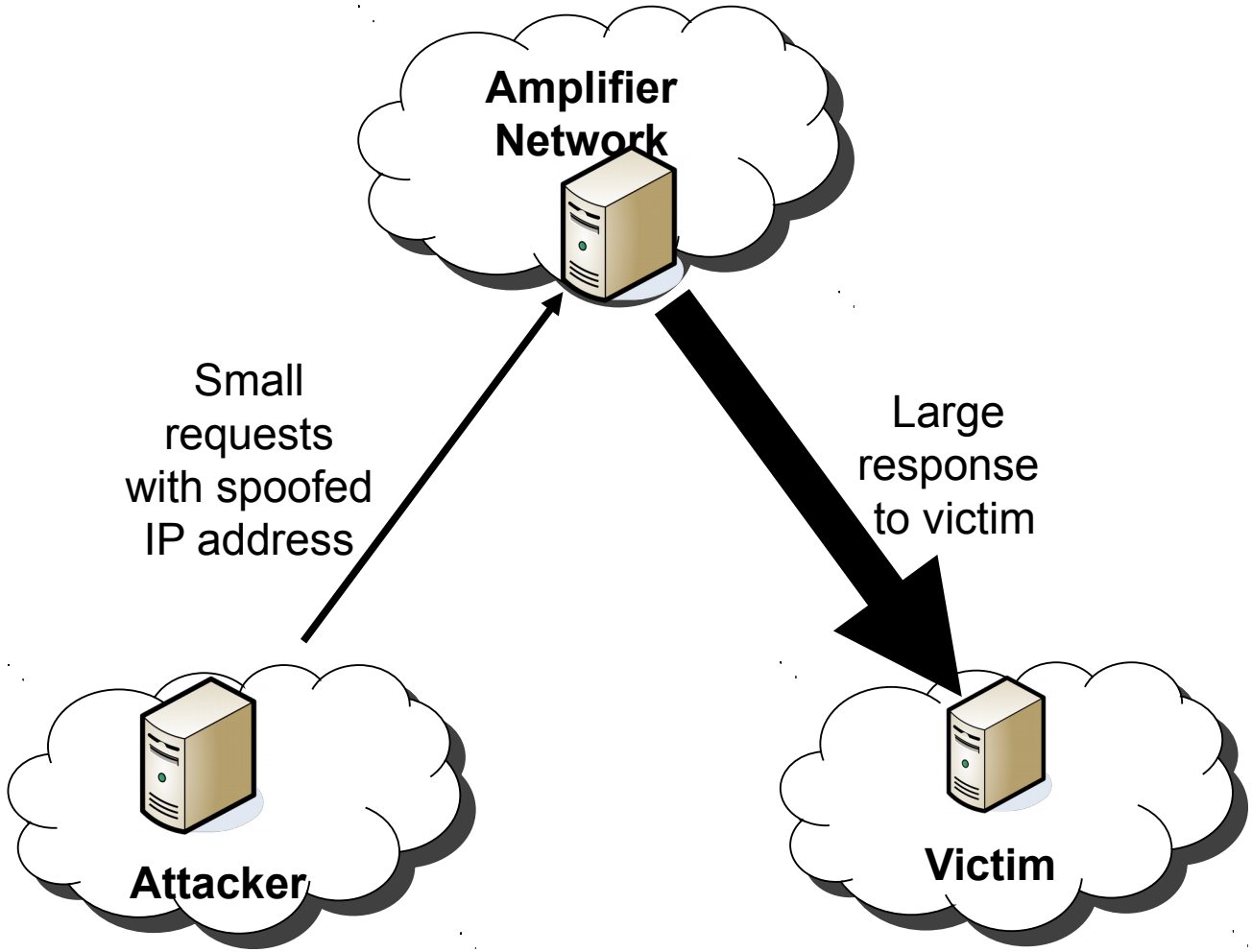
- Unauthorized data access
- Privacy (*e.g.*, presence detection)
- Manipulation of devices (*e.g.*, disable heating)
- Misuse for attacks

Security implications

What are the security implications of publicly reachable BACnet devices?

- Unauthorized data access
- Privacy (*e.g.*, presence detection)
- Manipulation of devices (*e.g.*, disable heating)
- **Misuse for attacks**

Amplification attacks



Amplification attack characteristics

- Connectionless:

Amplification attack characteristics

- Connectionless: BACnet $\rightarrow$ UDP-based ✓

Amplification attack characteristics

- Connectionless: BACnet $\rightarrow$ UDP-based ✓
- No authentication:

Amplification attack characteristics

- Connectionless: BACnet $\rightarrow$ UDP-based ✓
- No authentication: BACnet $\rightarrow$ No handshake necessary ✓

Amplification attack characteristics

- Connectionless: BACnet $\rightarrow$ UDP-based ✓
- No authentication: BACnet $\rightarrow$ No handshake necessary ✓
- Amplification:

Amplification attack characteristics

- Connectionless: BACnet $\rightarrow$ UDP-based ✓
- No authentication: BACnet $\rightarrow$ No handshake necessary ✓
- Amplification: BACnet $\rightarrow$ **?**

BACnet amplification factor

Amplification attack: small request and large response

BACnet:

- Request size: Header overhead + ID of requested property
- Response size: Depends on requested property

BACnet amplification factor

Amplification attack: small request and large response

BACnet:

- Request size: Header overhead + ID of requested property
- Response size: Depends on requested property

Example:

- Request: *What is your location?*
- Response: *Fairmont Hotel, San Jose, California, USA.*

Maximizing the amplification factor

Requesting one property is nice, but. . .

- Header overhead rather large
- Not all devices might have the requested property

Maximizing the amplification factor

Requesting one property is nice, but...

- Header overhead rather large
- Not all devices might have the requested property

ReadPropertyMultiple request

- Send a list of requested property IDs
- Reduce header overhead
- Higher chance that device has some of requested properties

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Maximizing the maximized amplification factor

It can’t get any worse, right?

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Maximizing the maximized amplification factor

~~It can't get any worse, right?~~ **Wrong**

Maximizing the maximized amplification factor

~~It can't get any worse, right?~~ **Wrong**

- Request: *Location? Location? Location?*
- Response: *Fairmont Hotel, San Jose, California, USA. Fairmont Hotel, San Jose, California, USA. Fairmont Hotel, San Jose, California, USA.*

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Maximizing the maximized amplification factor

~~It can't get any worse, right?~~ **Wrong**

- Request: *Location? Location? Location?*
- Response: *Fairmont Hotel, San Jose, California, USA. Fairmont Hotel, San Jose, California, USA. Fairmont Hotel, San Jose, California, USA.*

Request **the same property** multiple times within one request

- Choose property with highest amplification factor
- Reduce header overhead even more
- Maximized amplification factor, similar to DNS Open Resolvers

Amplification attacks using BACnet

- Connectionless: BACnet $\rightarrow$ UDP-based ✓
- No authentication: BACnet $\rightarrow$ No handshake necessary ✓
- Amplification:

Amplification attacks using BACnet

- Connectionless: BACnet $\rightarrow$ UDP-based ✓
- No authentication: BACnet $\rightarrow$ No handshake necessary ✓
- Amplification: BACnet $\rightarrow$ Freely choose requested property ✓

Amplification attack mitigation

- Ingress filtering against IP address spoofing
- Throttling BACnet traffic
- Standardizing that each property can be requested only once
- BACnet devices should not be reachable from the public Internet
  - Notification campaign in cooperation with DFN-CERT

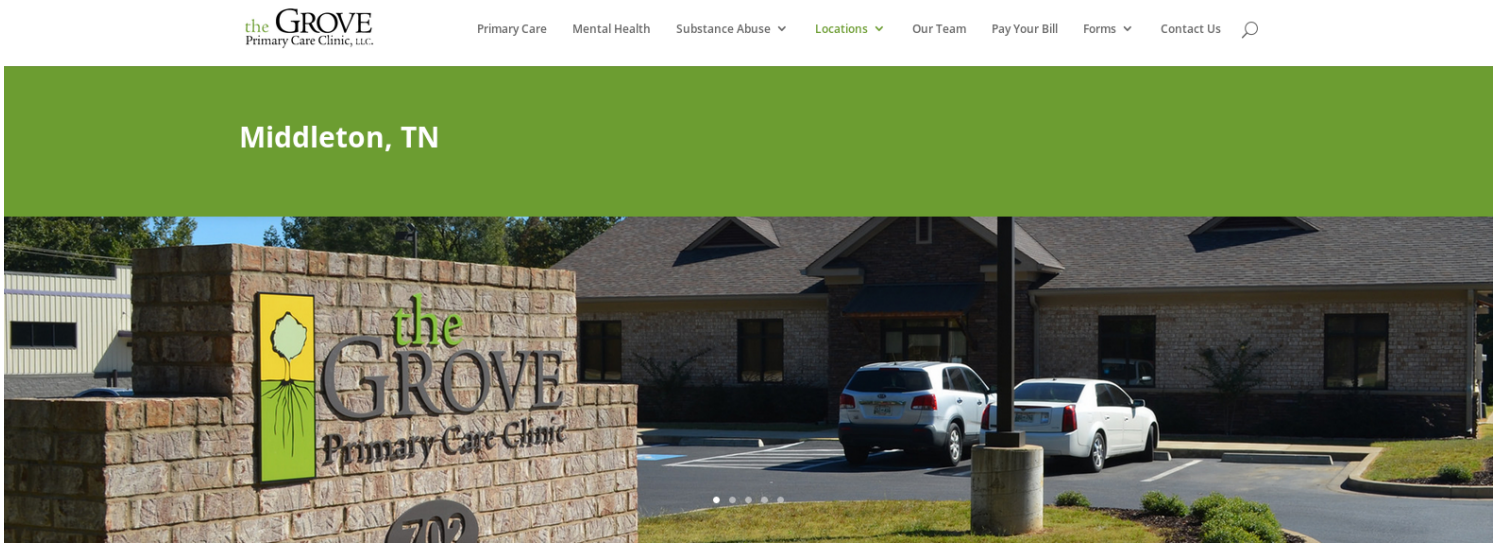
BACnet: Real-world location response

BACnet: Real-world location response

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

BACnet: Real-world location response

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



BACnet: Real-world location response

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

BACnet: Real-world location response

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

BACnet: Real-world location response

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

BACnet: Real-world location response

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

Conclusion

- Largest Internet-wide BACnet scans to date
- Analysis of BACnet's amplification potential
- Notification campaign in cooperation with CERT
- Release of BACnet Python module as open-source

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Conclusion

- Largest Internet-wide BACnet scans to date
- Analysis of BACnet's amplification potential
- Notification campaign in cooperation with CERT
- Release of BACnet Python module as open-source

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

Amplification factors

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

Table 1: Overview of all BACnet scans.

Type of scan	Ports	Rate	Duration	Targets	Resp.	BACnet
IPv4-wide	16	25 kpps	41 h	2.4 G	32 868	16 485
IPv6 hitlist	1	5 kpps	2 min	407 k	0	0
Amplification	16	100 pps	3 min	16 k	15 598	15 429

Table 2: Top 5 BACnet vendors in results.

Pos.	Vendor ID	Vendor Name	Count	%
1	35	Reliable Controls Corporation	3740	24.8
2	36	Tridium Inc.	2079	13.8
3	8	Delta Controls	2004	13.3
4	5	Johnson Controls Inc.	1328	8.8
5	24	Automated Logic Corporation	1051	7.0

Table 3: Top 5 ASes by count of BACnet devices.

Pos.	ASN	Organization	Count	%
1	7018	AT&T Services, Inc.	1510	9.2
2	7922	Comcast Cable Communications, Inc.	1450	8.8
3	22394	Cellco Partnership DBA Verizon Wireless	774	4.7
4	852	TELUS Communications Inc.	697	4.3
5	6327	Shaw Communications Inc.	454	2.8

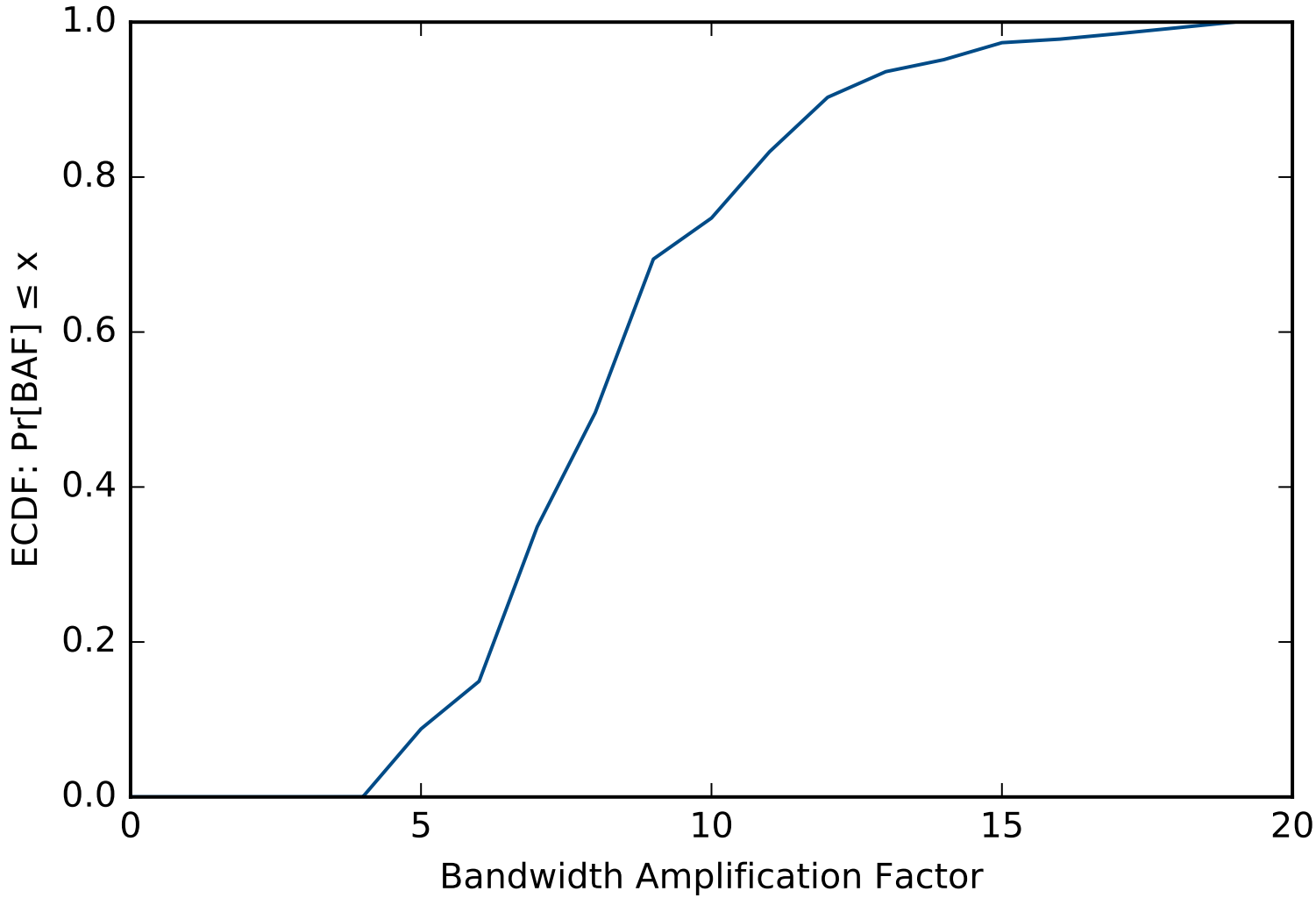


Figure 1: Distribution of BAF for our generic *ReadPropertyMultiple* amplification payload used in scans.

Table 4: Property BAF and payload BAF as mean over *all*, top *50 %* and top *10 %* amplifiers.

		Property BAF			Payload BAF		
Property	Amplifiers	all	50 %	10 %	all	50 %	10 %
model_name	14 072	6.2	8.3	8.5	1.5	1.7	1.7
vendor_name	14 072	9.0	13.9	14.5	1.8	2.2	2.3
firmware_revision	14 072	11.2	19.6	35.0	2.0	2.8	4.2
app_sw_version	14 071	5.9	10.3	14.0	1.5	1.9	2.2
object_name	14 039	6.8	9.1	11.0	1.6	1.8	2.0
description	13 741	5.5	10.9	13.0	1.4	1.9	2.1
location	13 360	2.5	5.1	7.5	1.1	1.4	1.6
serial_number	2316	4.9	5.6	5.0	1.4	1.4	1.4
profile_name	1958	5.0	7.0	7.0	1.5	1.8	1.8
property_list	1389	141.0	193.8	200.0	7.3	9.7	10.0

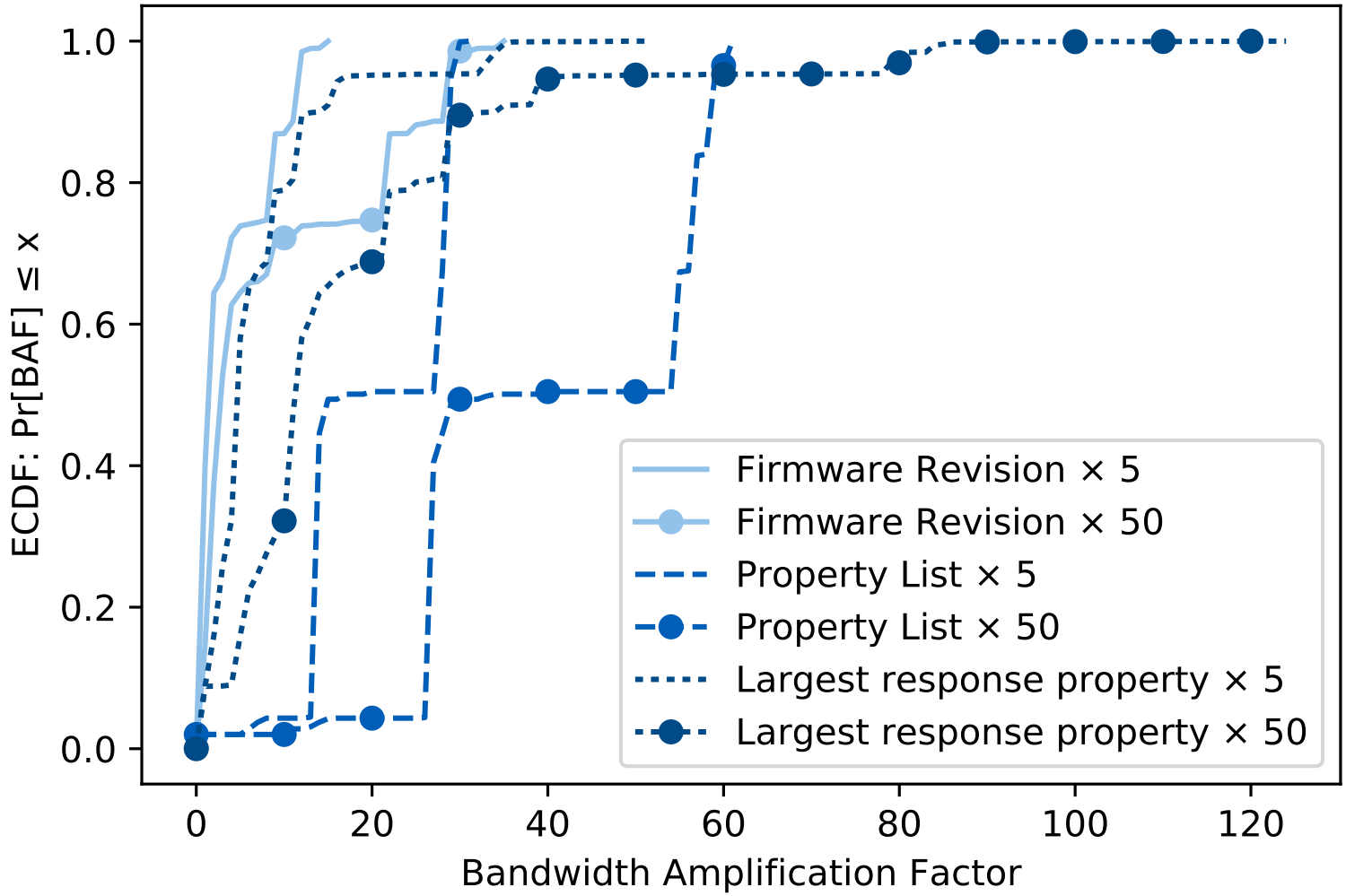


Figure 2: Payload BAF when issuing multiple requests for the same property (within a single Multi-Property packet).