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

Evaluating Network Security using Internet Measurements

Oliver Gasser

Tuesday 23rd May, 2017

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

About me

- Scientific researcher / PhD candidate
  - Chair of Network Architectures and Services
  - Technical University of Munich (Germany)
- Co-leader of the Global Internet Observatory project
- Research interests
  - Security protocols (TLS, SSH,. . .)
  - Amplification attacks
  - IPv6 scanning

What will this talk be about?

- Internet-wide measurements
- SSH
- BACnet
- IPv6 scanning

Internet measurements

- Useful tool
- Various techniques
- Focus on empirical security measurements

SSH

- Secure Shell protocol
- Provides encrypted & authenticated remote shell access
- Mostly used on servers and routers to provide administrative access
- Security critical protocol $\rightarrow$ evaluate SSH's security

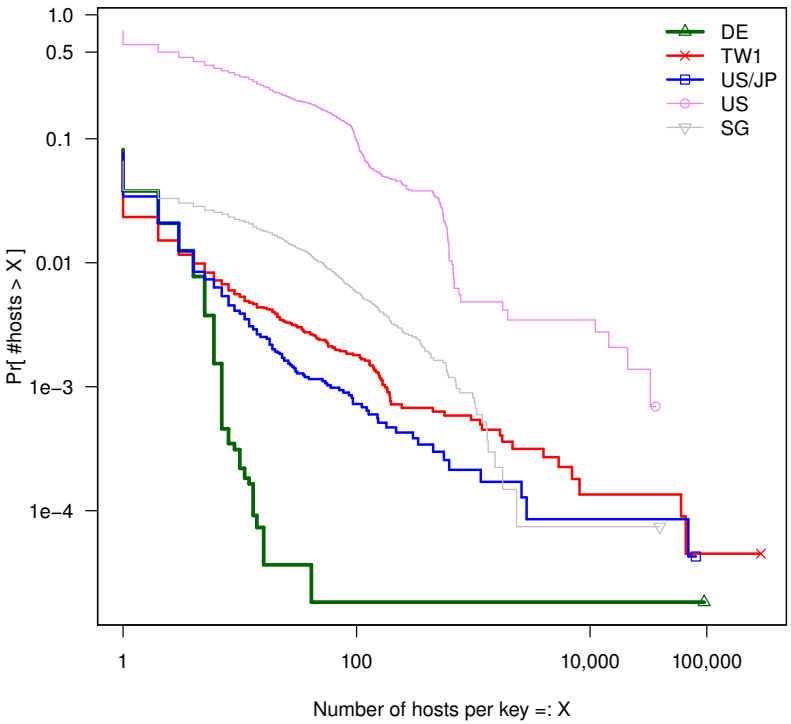
SSH measurements

- Internet-wide SSH scans [1]
- Found ≈15 M servers
  - 42 k servers offer **SSH 1 only**
- Downloaded > 25 M SSH host keys
  - Host keys identify a server similar to a certificate in TLS
  - Co-prime weak keys found (0.015 %, 2.4 % for SSH1)
  - Debian-weak keys found (0.05 %)
- Man-in-the-Middle attack possible with weak keys

[1] Gasser et al.: “A deeper understanding of SSH: results from Internet-wide scans”, NOMS’14.

SSH: Duplicate keys

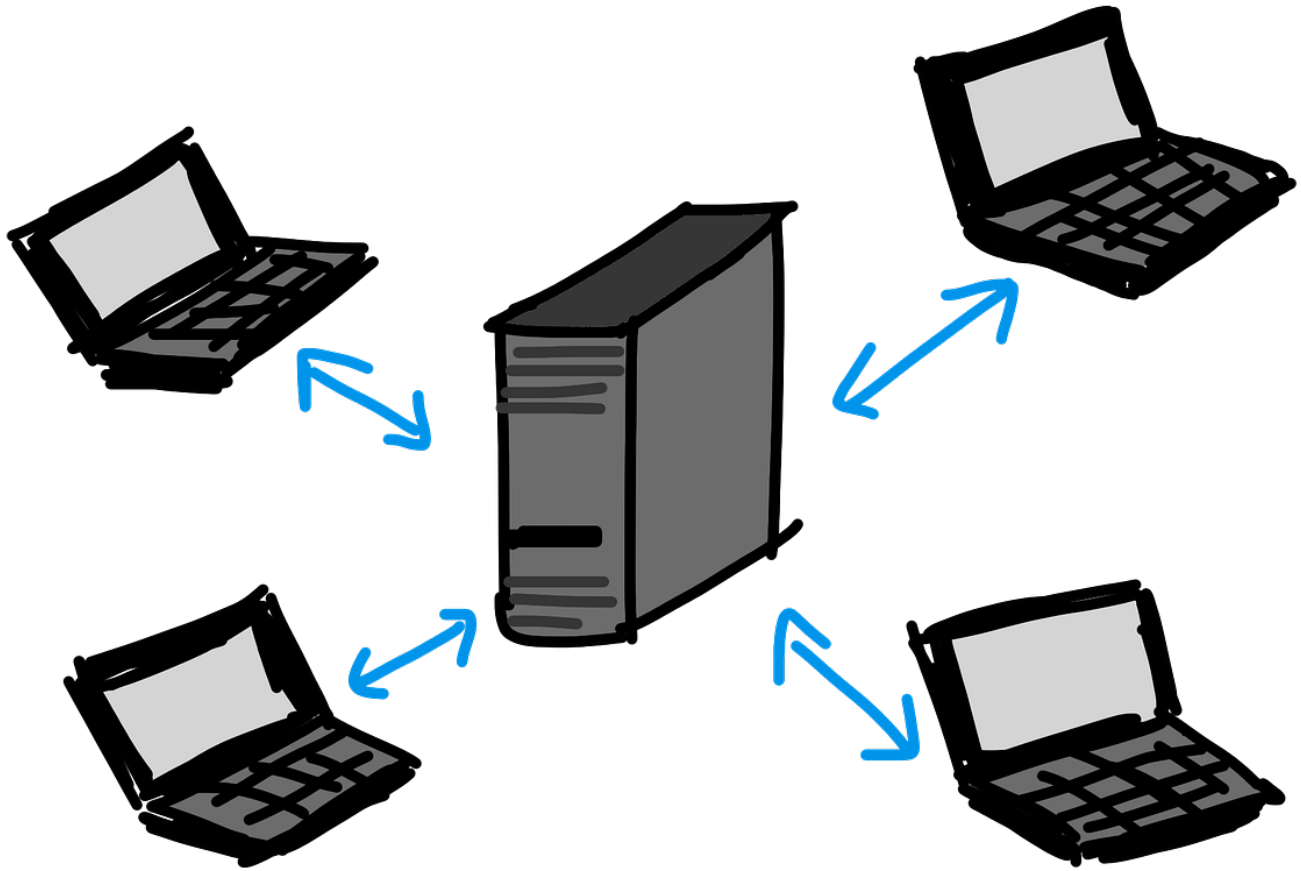
- Same key on multiple servers
- Similar threat of MitM attacks
- Heavily clustered based on Autonomous Systems
  - Web-hosting providers deploy systems with pre-generated keys
  - SSH gateways



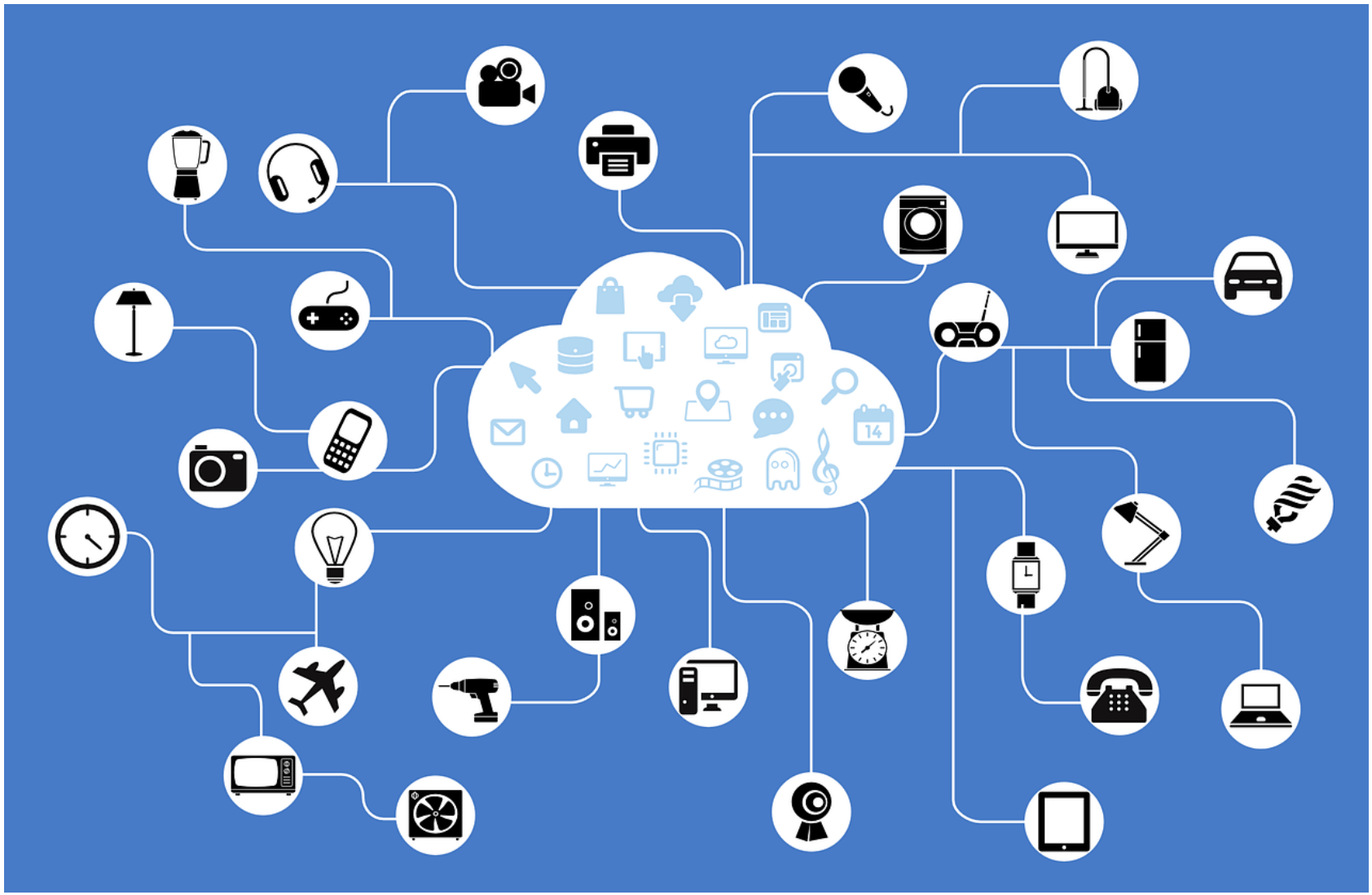
SSH: Lessons learned

- Weak keys
- Duplicate keys
- Man-in-the-Middle attacks possible
- Use public key authentication to thwart MitM
- Take cautionary measures before conducting SSH scans ⌣̈

The Internet?



The Internet



BACnet

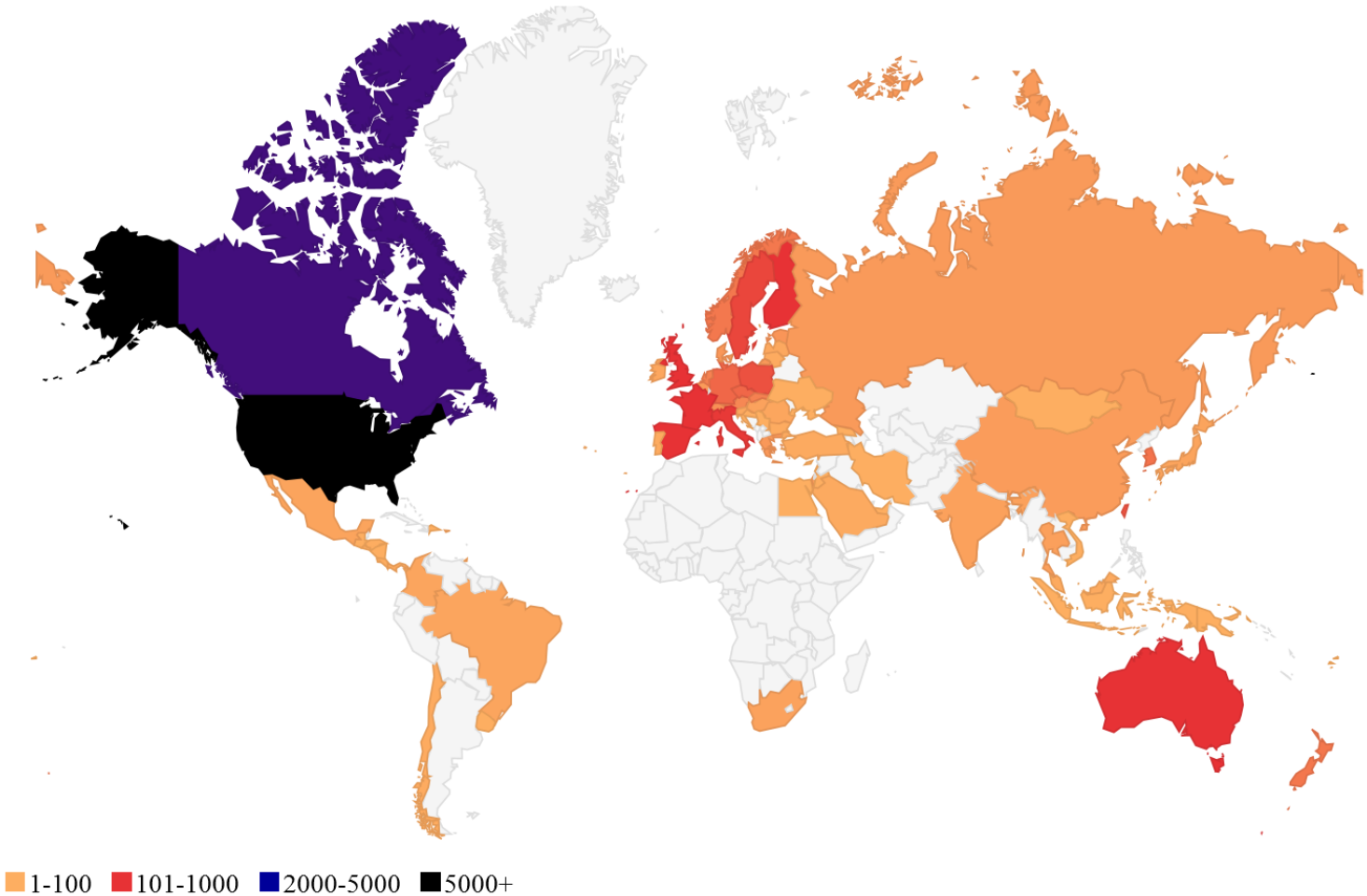
- Building Automation and Control Networks
- Used to control
  - Heating
  - Solar panels
  - Ventilation
  - ...
- Unsolicited access can have real-world consequences
  - Presence detection $\rightarrow$ Break into home
  - Manipulate heating, water flow,...
- Security & safety critical protocol $\rightarrow$ evaluate BACnet 's security

BACnet measurements

- Internet-wide BACnet scans[2]
- UDP-based request-response protocol
  - Retrieve and set properties
  - No security built in
- More than 16k devices found

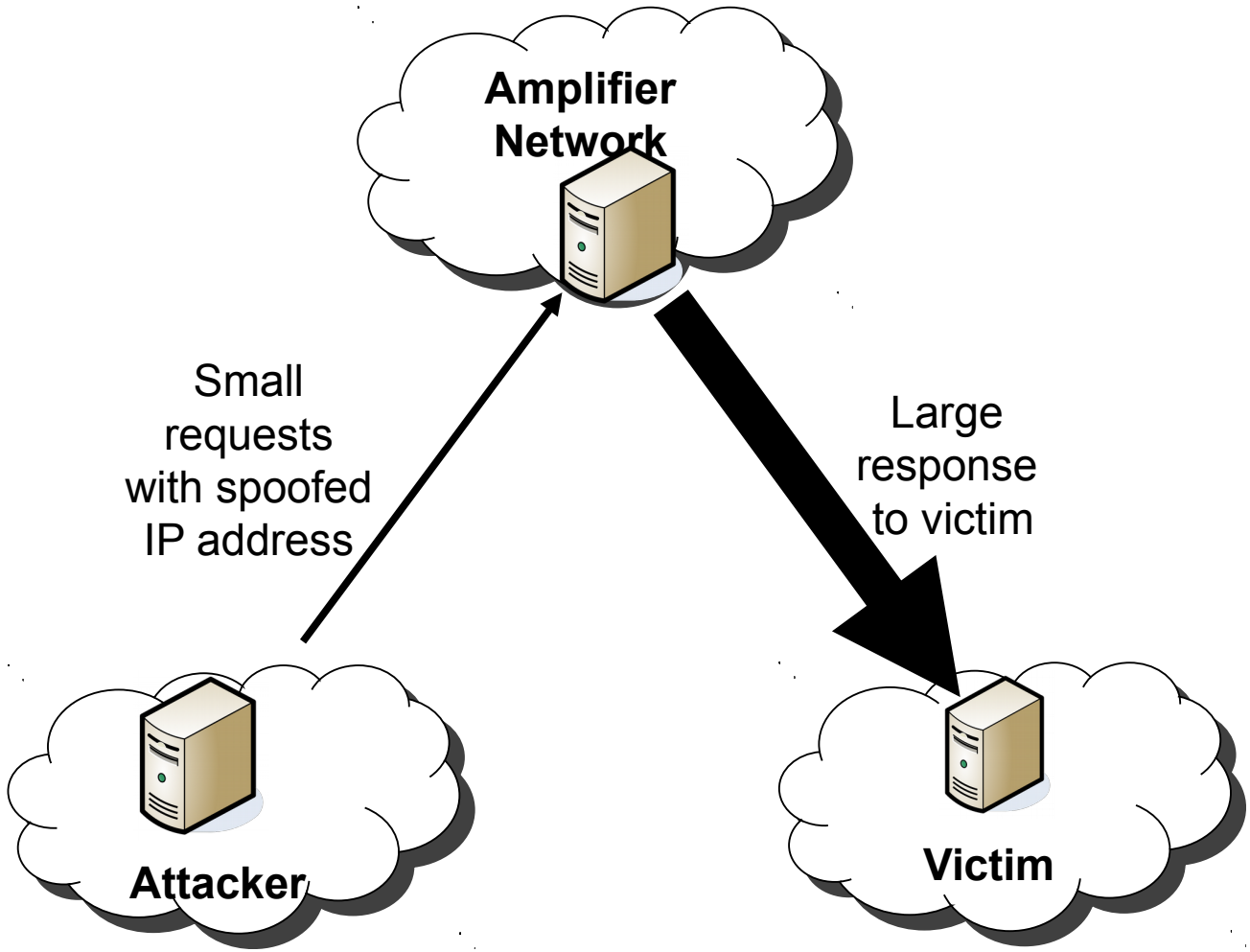
[2] Gasser et al.: “Security Implications of Publicly Reachable Building Automation Systems”, WTMC’17.

BACnet: Deployment



→ Heavily clustered in countries and ASes

Amplification attacks



BACnet + Amplification attacks?

- Connectionless:

BACnet + Amplification attacks?

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

BACnet + Amplification attacks?

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

BACnet + Amplification attacks?

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

BACnet + Amplification attacks?

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

BACnet + Amplification attacks?

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

BACnet: Amplification factor

- About 14k BACnet devices misusable as amplifier
- Request same property multiple times within one request
- Amplification factor similar to DNS Open Resolver
- Operators write **really** detailed location information into BACnet devices

BACnet: Amplification factor

- About 14k BACnet devices misusable as amplifier
- Request same property multiple times within one request
- Amplification factor similar to DNS Open Resolver
- Operators write **really** detailed location information into BACnet devices
  - *Hwy 57; Located in the silver box on the electrical pole in front of Grove Primary Care Clinic. Pole 123*

BACnet + Amplification attacks!

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

BACnet + Amplification attacks!

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

BACnet: Lessons learned

- Never attach your BACnet device to the public Internet
- Direct threats: Information leakage, surveillance,. . .
- Indirect threats: Misused as amplifier
- Notify affected parties via CERTs

IPv6 measurements

- IPv6 adoption[3] $\approx$ 15%
- Vast address space
- Brute-force scanning approach infeasible
- Smart address selection needed

[3] https://www.google.com/intl/en/ipv6/statistics.html

IPv6: Hitlist-approach

- Collect IPv6 addresses from various sources
- Active sources
  - DNS AAAA resolution (Alexa Top 1M, IPv4 rDNS, DNS ANY, DNS zone files)
  - CAIDA IPv6 router DNS names
- Passive sources
  - Raw packet traces
  - Flow data (NetFlow, IPFIX)
- Traceroute

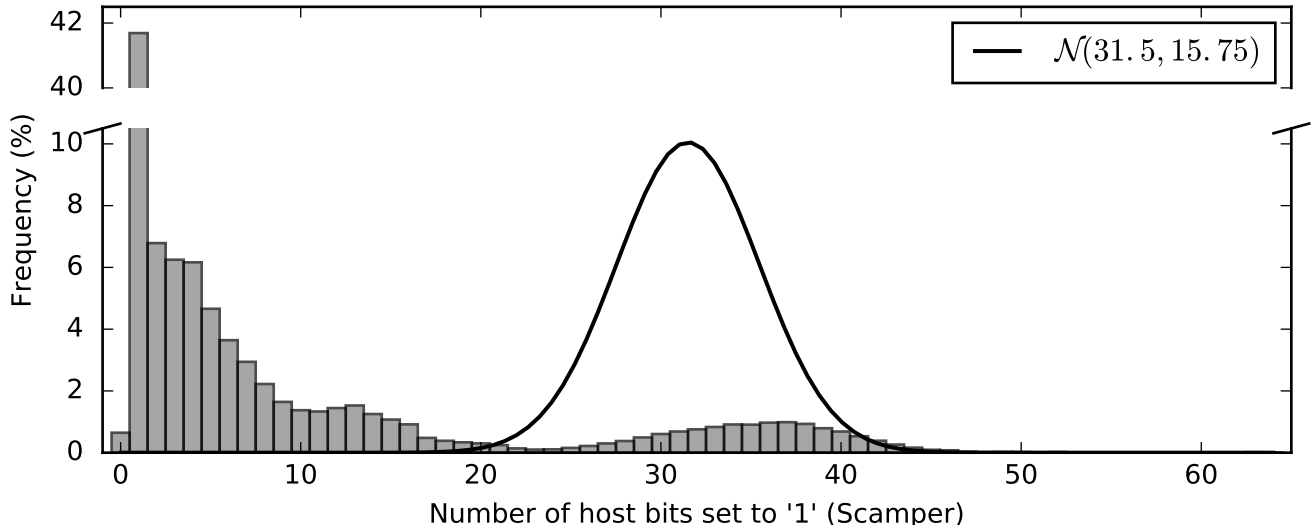
IPv6: Scanning

- ZMap version with IPv6 support[4]
- Collected 150M IPv6 addresses for hitlist[5]
- Evaluated reachability and longevity of addresses
- Classify servers, routers, end-user devices

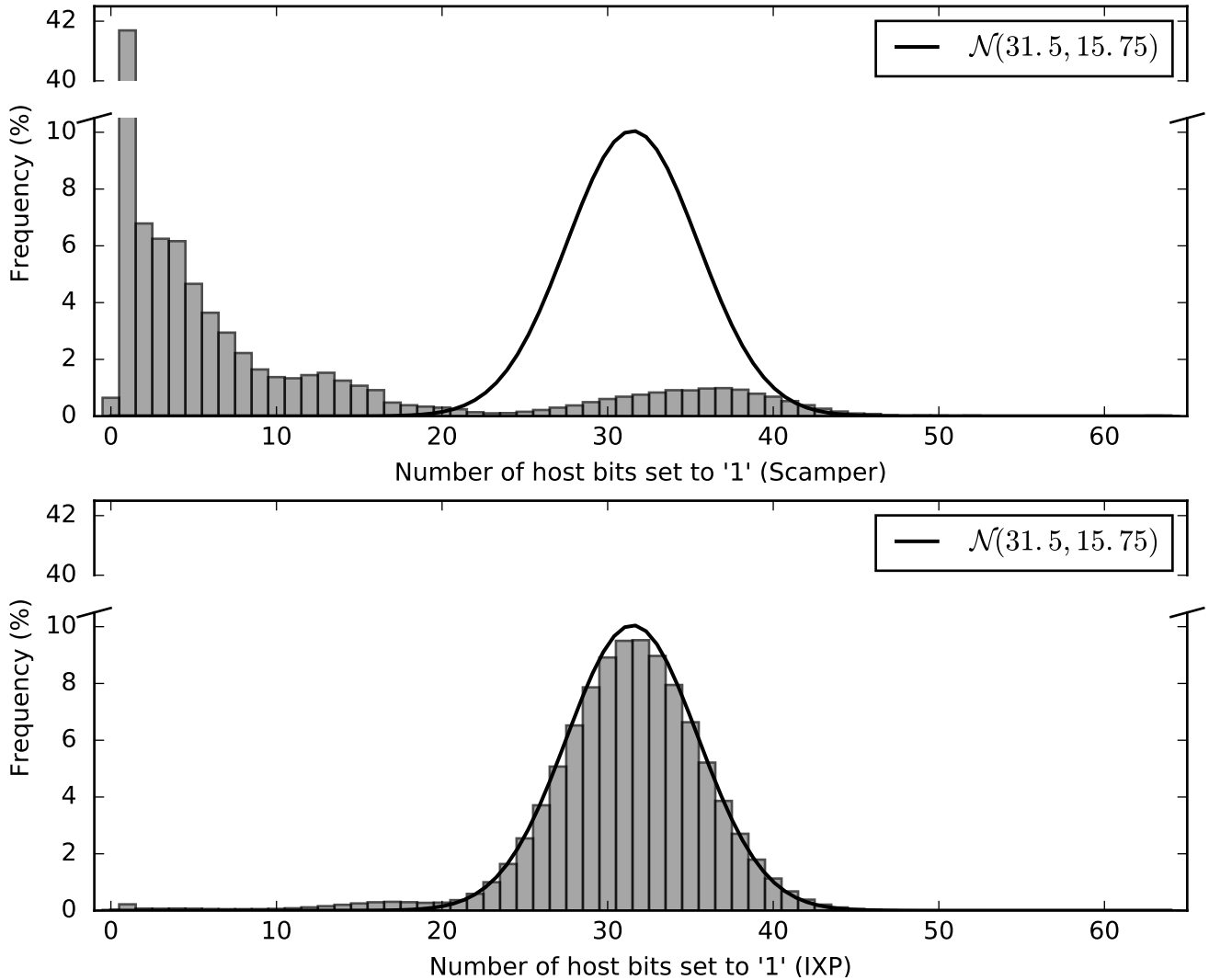
4 `github.com/tumi8/zmap`

5 Gasser et al.: “Scanning the IPv6 Internet: Towards a Comprehensive Hitlist”, TMA’16.

IPv6: Classifying devices



IPv6: Classifying devices



IPv6: Lessons learned

- Address space sparsely populated
- Clients cycle IPv6 addresses quickly $\rightarrow$ privacy extensions
- IP address as a metric
- IPv6 Hitlist service[6] freely usable by researchers

[6] https://www.net.in.tum.de/projects/gino/ipv6-hitlist.html

To conclude

- Measurements: valuable tool to better understand the Internet
- Regular measurements uncover changes
- Proactive scanning + notification of affected parties

To conclude

- Measurements: valuable tool to better understand the Internet
- Regular measurements uncover changes
- Proactive scanning + notification of affected parties

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

Real-world BACnet location response:

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

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

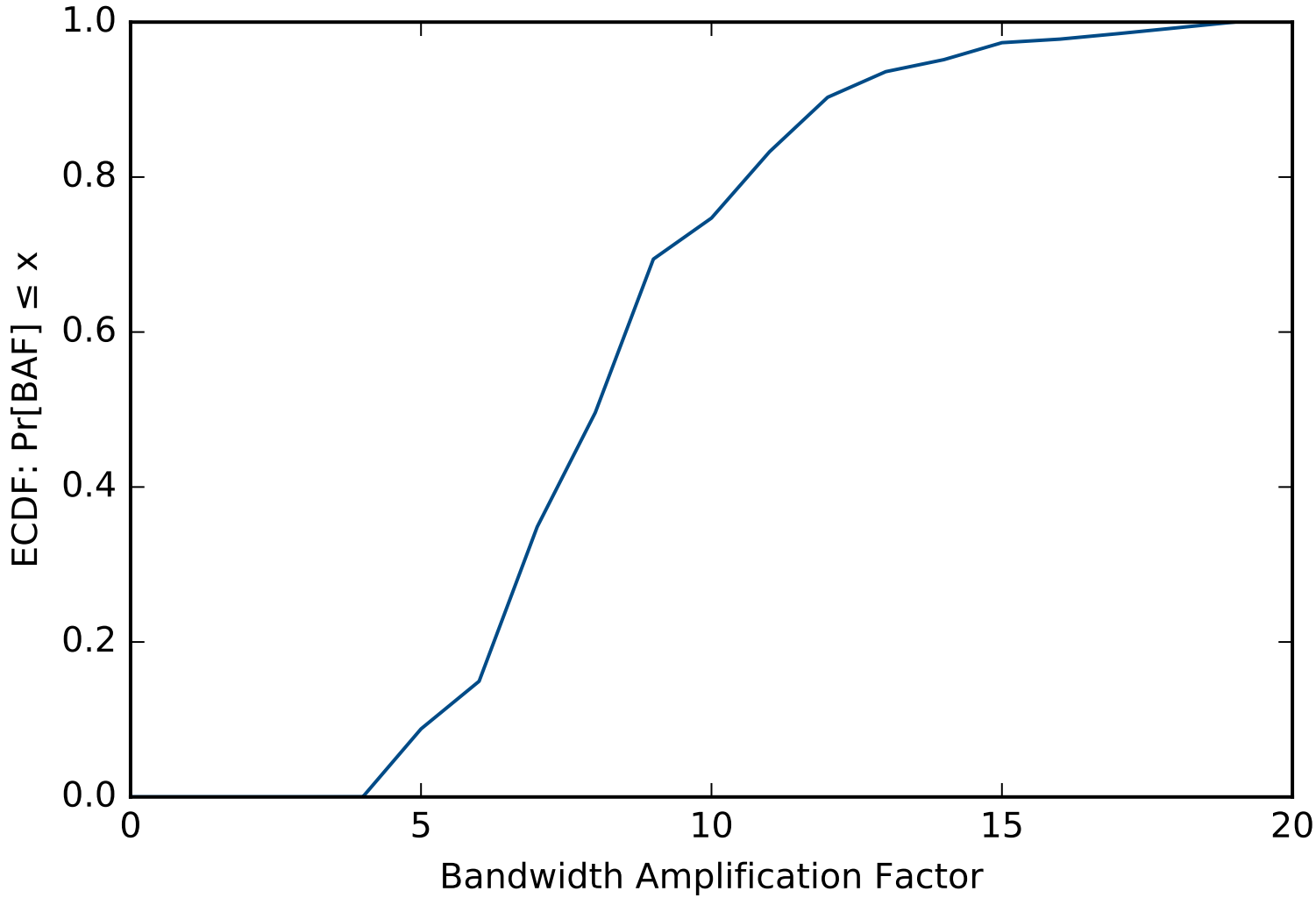


Figure 1: Distribution of BAF for our generic *ReadPropertyMultiple* amplification payload used in scans.

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

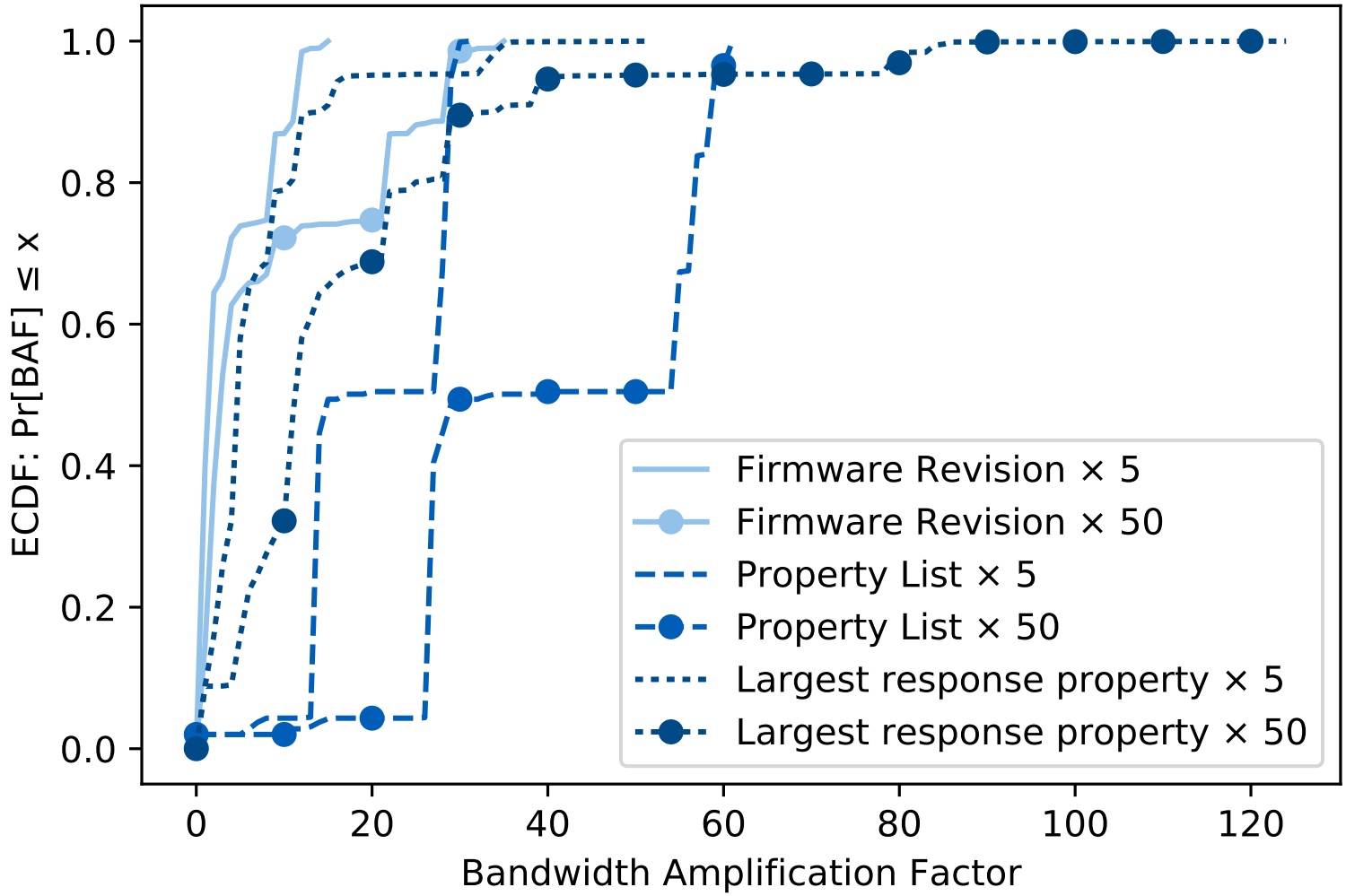


Figure 2: Payload BAF when issuing multiple requests for the same property (within a single Multi-Property packet).

IPv6 needs a different scanning paradigm than IPv4

Active security scans continue to be a valuable tool

- Discover vulnerable devices
- Assess severity and prevalence of security problems

History of IPv4 hit lists

- Opportunistic log file parsing
- Passive taps
- Repeated scans to determine stable IPs
- Scanning it all

Our approach

- Create a tailored hitlist of IPv6 addresses for security scanning

Sources for IPv6 addresses

Passive

- Large European IXP
- MWN: uplink of Munich Scientific Network with $\approx$ 100k users

$\rightarrow$ Evaluate for response rate and stability

Active

- Alexa Top 1M
- Rapid7 IPv4 rDNS
- Rapid7 DNS ANY
- DNS zone files
- CAIDA IPv6 router DNS names

$\rightarrow$ Evaluate for response rate

Traceroute

$\rightarrow$ Evaluate additional IPs learned

Passive sources

Characteristic	IXP	MWN
Targets	**146,722,097**	**2,687,679**
ASes	6,783	7,398
AS coverage	**66.61%**	**72.65%**
ASes unique to source	821	1,436
Prefixes	12,858	15,478
Prefix coverage	**49.87%**	**60.04%**
Prefixes unique to source	2,076	4,696
Combined AS coverage	8,219 (80.71%)	
Combined prefix coverage	25,781 (68.09%)	
ICMP response rate ≈	**13%**	**31%**

Active sources

	Alexa Top 1M	rDNS	DNS Any	Zone Files
File size	22MB	56GB	69GB	2.6GB
Unique addresses	43,822	462,185	1,440,987	424,748
AS coverage	14.0%	47.1%	56.1%	23.3%
ASes unique to source	1	**30**	**685**	5
Prefix coverage	6.57%	26.2%	33.0%	11.62%
Prefixes unique to source	7	65	**1,379**	11
ICMPv6 response rate	**95.3%**	**68.8%**	**72.6%**	**90.6%**
tcp80 response rate	94.2%	28.4%	51.6%	88.3%
tcp443 response rate	75.8%	21.2%	27.8%	58.6%
Combined AS coverage		**7,331 (71.9%)**		
Combined prefix coverage		**12,854 (49.8%)**		

Temporal stability of IPv6 addresses

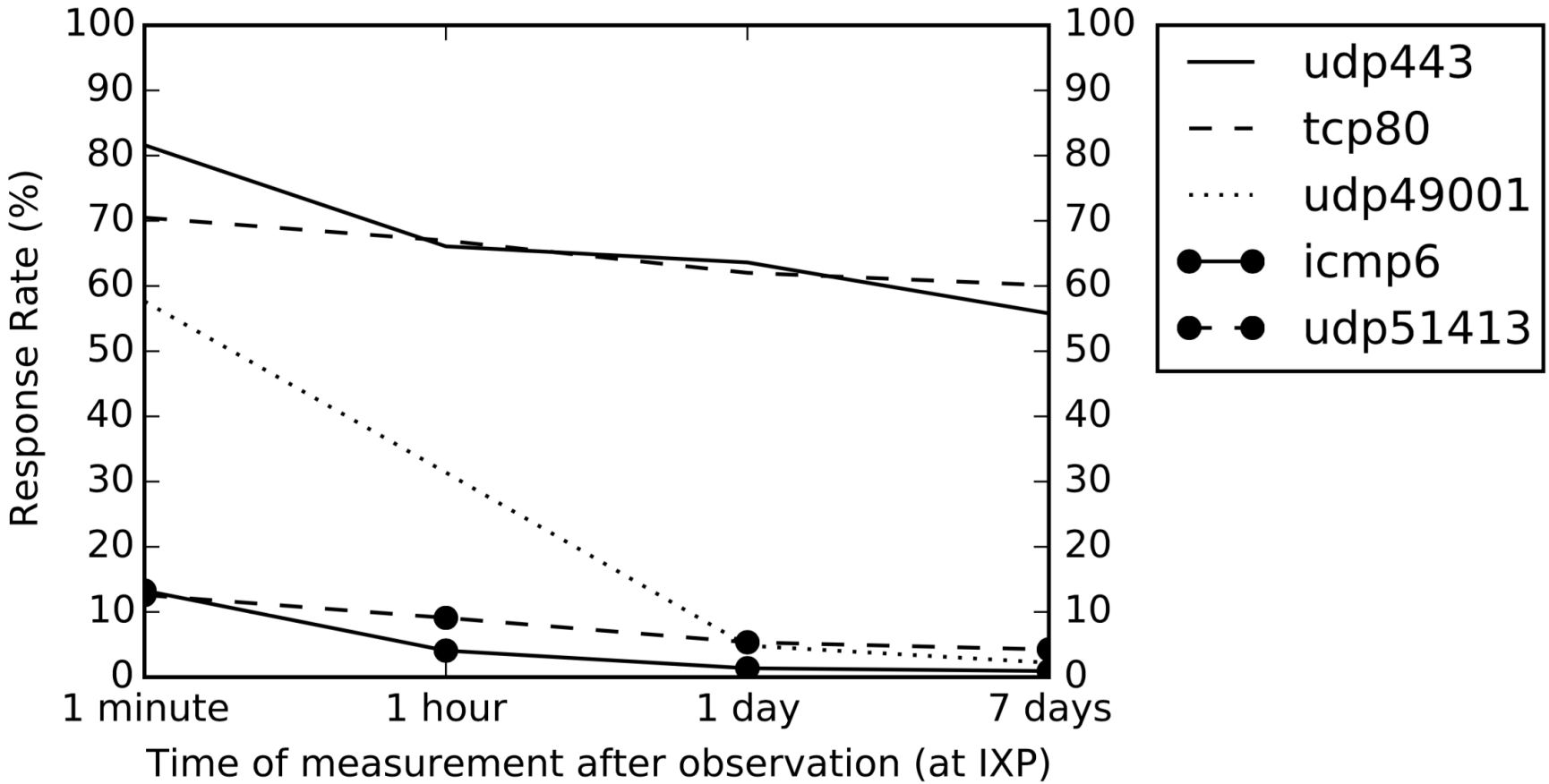
Passive sources:

- Trigger measurement immediately after observation
- Repeat measurement using exponential back-off
- Measure observed port/protocol and ICMPv6
- zmap extended with IPv6 capabilities for high-volume scans

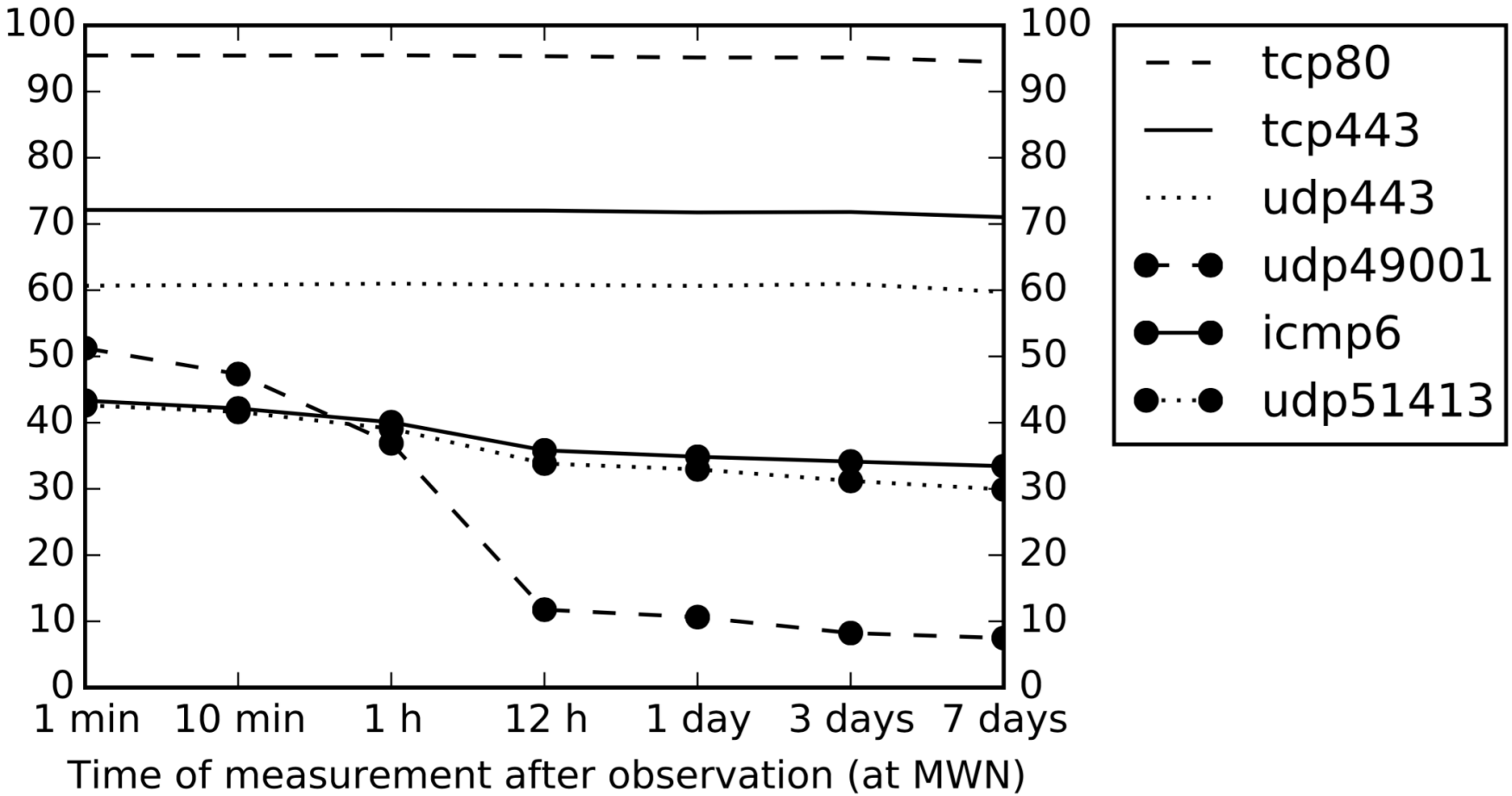
Active sources:

- Scan ICMPv6
- Scan tcp80 and tcp443

IXP response rates

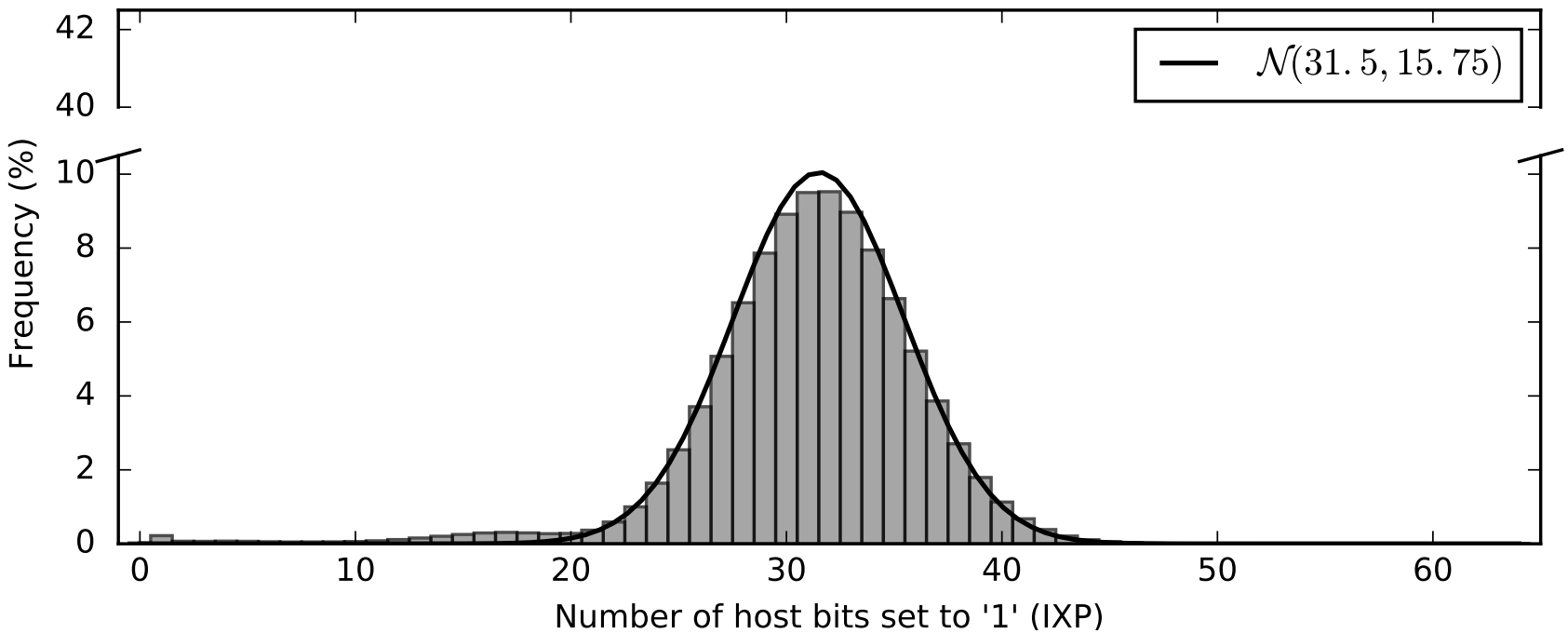


MWN response rates

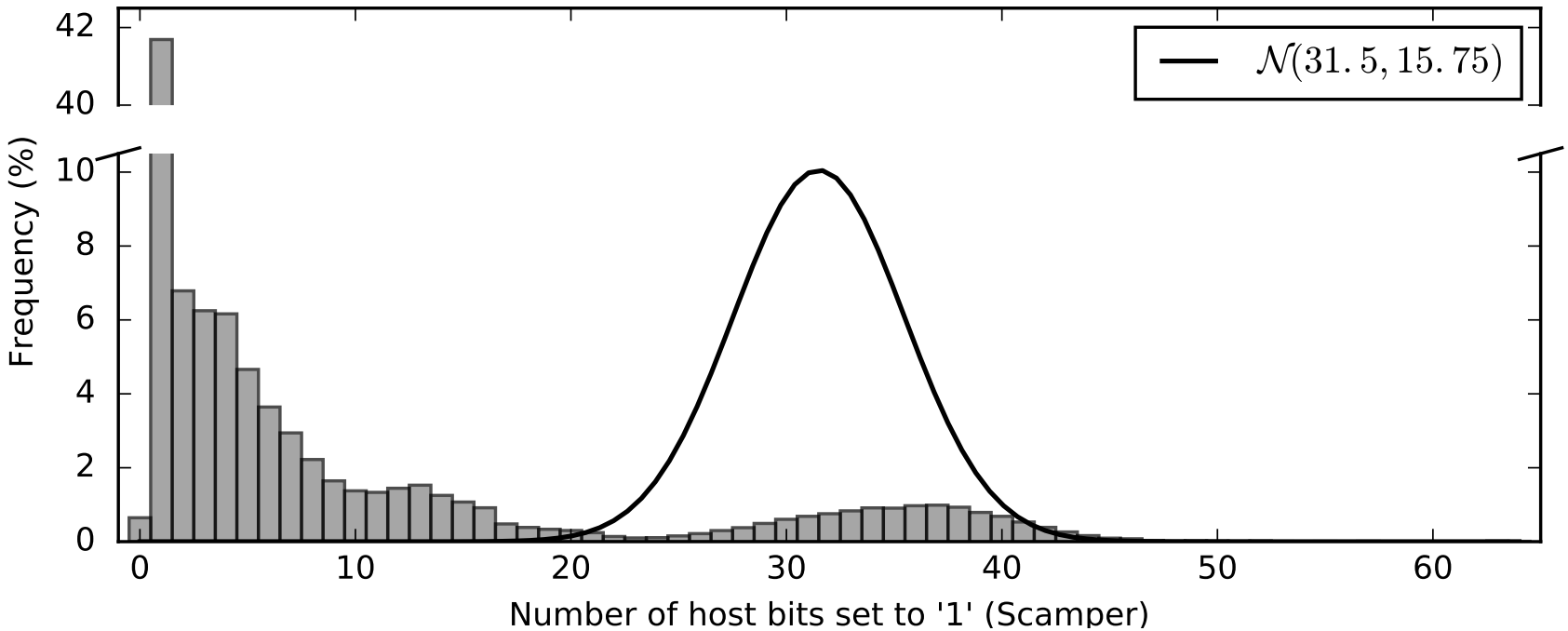


IXP Hamming weight indicates privacy extensions

- Interface ID: Commonly last 64 bits in IPv6 address
- Privacy extensions (RFC 4941): 6th bit zero, other 63 bits random
- *Central limit theorem*: 63 independent single-bit distributions $\rightarrow$ normal distribution $\mathcal{N}(31.5, 15.75)$



Traceroute Hamming weight indicates managed IP assignements



Analyzing EUI-64 IPs (`ff:fe`) in data sets

TABLE IX: Top 5 vendors for EUI-64 IPs.

	IXP		Scamper	
Position	Vendor	Percentage	Vendor	Percentage
1	Samsung	30.7%	Arcadyan	28.4%
2	Apple	11.6%	Huawei	24.4%
3	Sony	5.8%	AVM	16.0%
4	Murata	5.1%	Sercomm	10.5%
5	Huawei	5.1%	Cisco	4.4%

Sources for an IPv6 hitlist

Characteristic	Active sources	Passive sources	Traceroutes	CAIDA
Targets	2,699,573	148,631,234	109,554	102,580
ASes	5,750	8,219	4,170	5,488
Announced prefixes	8,602	17,554	5,367	9,269
AS coverage	56.46%	**80.71%**	41.00%	**53.90%**
ASes unique to source	128	1,276	14	147
Prefix coverage	33.37%	**68.09%**	20.76%	**36.00%**
Prefixes unique to source	346	5,798	53	514
ICMPv6 response rate	**75.5%**	13.3%	n/a	42.0%
Combined unique IPs		**149,619,624**		
Combined AS coverage		**8,531 (83.77%)**		
Combined prefix coverage		**18,502 (71.77%)**		

Specific approach for your scan type

Internet structure finding links and nodes $\rightarrow$ passive, CAIDA, ::1 for missing prefixes

Assessing security posture many server hosts $\rightarrow$ active sources

Internet routers CAIDA, traceroute to active sources

Client protocols passive tap, but be very quick!

Finding active prefixes passive sources