2017 IEEE Symposium on Security and Privacy Workshops

Security Implications of Publicly Reachable Building Automation Systems

Oliver Gasser, Quirin Scheitle, Carl Denis, Nadja Schricker, Georg Carle
Technical University of Munich
Chair of Network Architectures and Services
Email: {gasser,scheitle,denis,schrickn,carle}@net.in.tum.de

***Abstract*—In a connected world Internet security is becoming increasingly important. Attacks, which are frequently executed by botnets, can impact people in their everyday life. A ubiquitous kind of attack is the amplification attack, a special type of Denial-of-Service attack. Several protocols such as DNS, NTP, and SNMP are known to be vulnerable to amplification attacks when security practices are not followed. In this work we evaluate the vulnerability of BACnet, a building automation and control protocol, to amplification attacks. To assess BACnet's vulnerability we conduct active traffic measurements on an Internet-wide scale. We find 16 485 BACnet devices, the largest number to date. Additionally, more than 14 k of these devices can be misused as amplifiers, with some generating amplification factors up to 120. To remediate this potential threat we employ a vulnerability notification campaign in close coordination with a CERT. Finally, we also give suggestions to thwart the amplification attack potential of BACnet.**

1. Introduction

In the last years the number of Denial-of-Service attacks increased dramatically in both frequency and data rate. These attacks more and more misuse Internet of Things (IoT) devices or embedded systems. Many of these devices are not properly secured and are therefore an ideal target for misuse and attacks. They can be used directly by being part of a botnet, or indirectly as a reflector or amplifier. An example for direct abuse is the Mirai botnet which attacked the Internet infrastructure company Dyn causing partial outages for Twitter, Amazon, and Netflix [15], and started a DDoS attack which Akamai was unable to mitigate [16]. An example of indirect abuse is the use of open DNS resolvers as amplifiers in the attack on Spamhaus [22].

These examples highlight problems arising from two sources: Firstly, IoT devices without proper security posture may be taken over for arbitrary abuse. Secondly, embedded devices may offer insecure and easy to abuse services such as open DNS resolvers and misconfigured NTP servers. Most of these security problems, however, are only discovered when their exploitation causes fallout. Therefore, we conduct traffic measurements to identify potentially insecure devices before they are being misused in attacks. We focus our measurements on the building automation protocol BACnet [2] and assess its vulnerability to amplification attacks. BACnet is capable of connecting a wide range of devices and offers remote monitoring and control features. Security was not a priority when the BACnet protocol was designed and the recommendation [19] is to never connect BACnet devices to the Internet, but always place them in a segmented, separate network. We investigate BACnet devices reachable in the public Internet.

Our contributions are as follows:

- Conducting exhaustive, Internet-wide scans for BACnet devices, varying port and payload
- Discovering the largest number of BACnet devices to date
- Uncovering and quantifying the potential of BACnet for amplification attacks
- Executing a CERT-backed notification campaign
- Recommending specific security improvement steps

Outline: This paper is structured as follows: In Section 2 we briefly describe the BACnet protocol and our choice of scanning payload. We continue with our scanning methodology and ethical considerations in Section 3. Section 4 details the BACnet deployment evaluation based on our scan results. In Section 5 we analyze in detail how BACnet devices can be used for amplification attacks. Efforts to remediate this issue are discussed in Section 6 and related work is presented in Section 7. Section 8 concludes this paper with a summary and an outlook for future work.

2. The BACnet Protocol

This section provides a brief overview of the BACnet protocol, highlighting aspects important for this research.

BACnet development was started in 1987 [19], with the first release in 1995 by ASHRAE. BACnet was designed as a standalone network protocol, including its own network layer with 16-bit network and device identifiers. BACnet's dedicated network layer implied segmented networks, hence security was not a consideration in protocol design. In 1999, BACnet/IP was defined to use IP as the network layer, which comes with many security implications. Security advice for BACnet/IP to date is to segment BACnet networks.

BACnet/IP uses a rather complex packet structure with multiple internal header layers. In its design, BACnet properties somewhat resemble SNMP MIBs.

DOI 10.1109/SPW.2017.13

2.1. BACnet Payload

For our measurements we use the generic wild-card device ID `0x3fffff` and select the following suitable payloads to identify BACnet devices:

IPv4: We conduct the IPv4 measurements using a *ReadPropertyMultiple* request payload. This type of request allows to specify a list of BACnet property IDs (*e.g.,* `0x46` = model name, `0x79` = vendor name). The queried BACnet device returns a list of corresponding properties.

IPv6: IPv6 support for BACnet was added in 2016 [3]. The standard defines new header types for IPv6, requiring a different payload to identify IPv6-capable devices. We use a *VirtualAddressResolution* request to discover BACnet devices over IPv6. This queries the remote virtual address used in the actual *ReadPropertyMultiple* request.

Amplification: The payload in our amplification scans is amended with additional properties which promise a high amplification factor, such as *PropertyList*.

3. Methodology

This section describes our methodology by giving details on our active scans, the processing of answers, and ethical considerations guiding our research.

3.1. Scan Overview

BACnet is run on UDP ports 47808 – 47823 by default [2]. Using different strategies, we probe those ports via IPv4 and IPv6. We verify responses for valid payloads to filter for actual BACnet devices. Using a different scanning payload, we then further survey these BACnet devices to determine their vulnerability for amplification attacks. Depending on the number of targets, we optimize packet sending rate to (1) minimize network load and (2) achieve tractable scanning duration. Table 1 gives an overview of our scans, listing the number of scanned ports, the used packet rate, the scan duration, the number of targets, received responses ("Resp."), and parsable BACnet payloads ("BACnet").

3.2. Internet-wide IPv4 Scans

We probe the IPv4 address space on the previously mentioned UDP ports using ZMap [9] and a BACnet UDP payload. We exclude IP addresses that are (1) on our blacklist or (2) part of the IANA reserved ranges [13] or (3) not routed according to BGP data from our routers.

For the IPv4 scans we choose a rate of 25 kpps, resulting in a duration of 41 hours for each performed scan. The scans are run from four measurement machines located in a dedicated measurement network.

In a first step, we filter the raw ZMap results for packets with the queried source port. We discard about 20 % of mismatching responses, which stem from source ports such as UDP/53 (DNS) or UDP/39999 (unregistered, but linked to Sygate [6]). These responses might be counter-scans from infected or malicious devices, probing our IP address for vulnerabilities. After this filtering, we count responses from 32 k unique IP addresses. The scan on port 47808 produces about 17 k (53 %) of responses, port 47809 about 3 k (9 %), port 47810 about 1.1 k (3 %), and ports 47811 – 47823 hold about equal shares of the remaining 35 %. This result supports our decision to scan for all 16 official BACnet ports to obtain a complete picture of the BACnet deployment. Scanning only the most prominent port UDP/47808 as *e.g.,* done by Mirian *et al.* [18] misses about 47 % of publicly reachable BACnet IP-port combinations.

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

In a second step, we filter the responses for valid BACnet payloads. We use our tailor-made Python BACnet module which we publish on GitHub [11]. We filter for compliance with the following characteristics, which are required for a genuine response to our packet: The transport type is BACnet/IP (`0x81`), the payload is an original unicast NPDU (`0x0a`), the BACnet version is the only valid version 1 (`0x01`), no reserved NPDU control bit is set, and the application payload type is BACnet-ComplexACK-PDU (`0x03`). After the filtering phase 16 485 (of initially 32 868) valid BACnet responses with payload content remain. Spot-checks on non-compliant packets reveal payloads that are *e.g.,* invalid, mirrored, randomized, or associated to other protocols. These might stem from honeypots, BACnet simulators, or unusual device configurations. Further investigation of these devices would require more intrusive scanning.

By scanning all standardized BACnet ports we also obtain more valid BACnet payloads: Our 16.4 k valid responses exceed Mirian *et al.*'s 12.8 k "valid handshakes" [18].

The distribution of ports after this filtering is more centric towards port UDP/47808 (84.4 % of responses). These responses will be evaluated in detail in Section 4.

3.3. IPv6 Scans

As IPv6 support for BACnet was added in early 2016 [3], we scan for BACnet devices in the IPv6 space.

Since scanning the full address space is not feasible in IPv6, we follow the domain-resolution aspect of our hitlist approach [12]. We also gain IPv6 addresses from responsive IPv4 BACnet devices by querying their rDNS record for `AAAA` records. We query 407 k unique IPv6 addresses, but do not receive any reply. We argue that this is likely due to a lack of IPv6 support in the field. As BACnet simulators do not support IPv6 yet, we can not validate our payload, which we thoroughly check against the BACnet standard.

3.4. Amplification Scans

Based on the subset of responsive BACnet devices, we conduct additional scans to evaluate the amplification

potential of those devices. Compared to previous scans we now request additional BACnet properties. Since these scans might produce more load on target systems we reduce the scanning rate to 100 packets per second. We apply the same filtering steps as for the IPv4-wide scans. This removes about 170 responses from non-scanned IP addresses.

3.5. Ethical Considerations

We follow an internal multi-party approval process before any measurement activities are carried out. This approval process incorporates the proposals of Partridge and Allman [20] as well as Dittrich *et al.* [7]. We assess whether our measurements can induce harm on individuals in different stakeholder groups. As we use a valid payload in accordance to the BACnet standard, it is unlikely for our scans to cause problems on scanned devices. We minimize interference of our scans by following best scanning practices such as maintaining a blacklist and using dedicated servers with informing rDNS names, web sites, and abuse contacts. We consider that publication of IP addresses of possibly vulnerable and amplifying devices may be abused by third parties. The conclusion of this process is that it is ethical to conduct the experiment, but that we will, in contrast to our usual policy, not share data from this work with the public. Instead, we will only make the data available upon request to other researchers for reproducibility and comparison, and to the DFN-CERT for vulnerability notification of affected parties. During our scans we did not receive any complaints.

4. BACnet Deployment

In this section we evaluate the BACnet deployment by analyzing the responses obtained from our scans.

4.1. Vendor Analysis

We find devices from a total of 97 different vendors, with just the top 3 vendors representing $52\,\%$ of all devices. Table 2 shows the five most frequent vendors found in our scans. Mirian *et al.* [18] also find Reliable Controls ($12.7\,\%$) and Tridium ($10.6\,\%$) as their top BACnet vendors, however their share in our evaluation is larger.

4.2. Topological Clustering

We next investigate the distribution of BACnet devices over Autonomous Systems (ASes) and announced prefixes. We use CAIDA's routeviews data [5] to map IP addresses.

We find AS coverage rather sparse, with BACnet devices present in 1439 ASes, with a median of 2 devices per AS. This is a small share of the 55 738 total ASes [5].

We also find our number of 1439 ASes to be in line with Mirian *et al.*, who discover BACnet devices in 1330 ASes.

The BACnet devices from our scans cover 5109 announced prefixes, of which 3021 only contain 1 device. The top 5 prefixes are /16 or larger prefixes of the major Internet service providers highlighted in Table 3.

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

4.3. Geographical Clustering

We also map the IP addresses of BACnet devices to countries using the IP2Location database [1]. While research has shown that IP geolocation databases can introduce significant biases [21], we believe them still to be indicative of the top countries of deployment. We find BACnet devices to be very centrally clustered with $60\,\%$ in the US and $20\,\%$ in Canada. With significantly less devices, Australia ($3\,\%$), France ($2\,\%$) and Spain ($2\,\%$) follow.

5. Amplification Attacks using BACnet

This section describes BACnet's vulnerability to amplification attacks. We evaluate the number of available amplifiers as well as the bandwidth amplification factor (BAF) of BACnet. BACnet supports both single property and multi property requests. To assess the amplification potential, we scan with a generic multiple property payload. From this, we derive (1) empirical BAF for our generic payload, (2) calculated BAF for individual properties in a single property request, and (3) calculated BAF for individual properties when repeatedly requesting the specific property in a multiple property request.

5.1. Amplification Attack Characteristics

An amplification attack is a type of Denial-of-Service attack where (1) the response payload is larger than the request payload. This ratio is called the bandwidth amplification factor [24]. In addition to a BAF >1, there are two other typical characteristics for amplification attacks: (2) the used protocol is stateless and (3) no authentication is required.

BACnet/IP is a UDP-based protocol and does not require any handshake. This stateless property already satisfies characteristics (2) and (3). Since we are free to choose the requested property which the BACnet device will then answer (provided the device supports the property), we can select such properties which will most likely trigger a large response by the queried device. The following section will evaluate which properties provide us with a large BAF. If

such a property is found, characteristic (1) is satisfied and BACnet can be used in amplification attacks.

5.2. Number of BACnet Amplifiers

We find 15 429 responsive BACnet devices with our amplification scans on ports 47808 – 47823. If a device does not support a requested property, it will reply with a four byte error, resulting in a property BAF<1. We quantify the amplification attack threat per BACnet property and device using error-free responses only. We focus the amplification attack analysis on variable length properties (*i.e.,* strings or arrays) as these are more likely to give a larger BAF.

In Table 4 we see stark differences in the number of available amplifiers depending on the requested BACnet property: Most properties provide us with about 14 k amplifiers, whereas three properties are available on significantly fewer devices: 2316 (15.0 %) of BACnet devices tell us their serial number, 1958 (12.7 %) give information about their profile name, and 1389 (9.0 %) provide their list of available properties. We investigated the reason for this and found that many devices answered with the BACnet error *property unknown* for these three properties. This is not surprising as the properties *serial number*, *profile name*, and *property list* were only added in 2012 to the BACnet standard. In conclusion, this analysis shows that we need to take the different numbers of amplifiers into account when trying to assess the potential threat posed by BACnet-based amplification attacks.

5.3. Amplification Factor of Scanning Payload

Figure 1 shows the empirical CDF of the bandwidth amplification factor for our 49 bytes long scanning payload. We can see that more than 90 % of requests generate responses with a BAF ≥ 5. The median BAF is 9, and the maximum BAF is 19.8 (with a response payload length of 942 bytes).

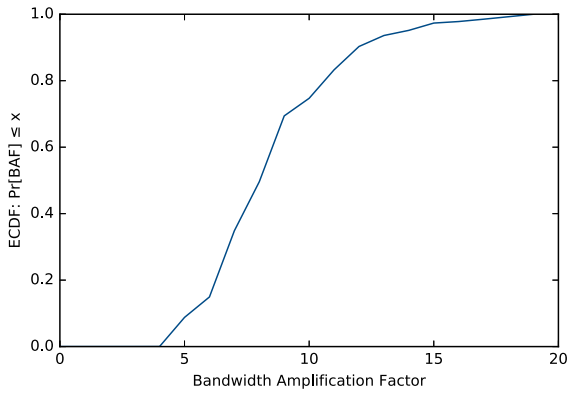

Figure 1: Distribution of BAF for our generic *ReadPropertyMultiple* amplification payload used in scans.

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

5.4. Amplification Factor per Property

We now evaluate the BAF on a per property basis *i.e.,* if we would send a request for a single property. To this end, we first calculate the sending and receiving overhead of BACnet headers and the static part of the payload. The sending ($SEND\_OVERHEAD$) and receiving ($RECV\_OVERHEAD$) overhead caused by BVLC, NPDU, and APDU headers in addition to the static part of the BACnet payload is 19 bytes. When requesting a property we need to add 2 or 3 additional bytes to the sent payload, depending on the property ID ($prop\_id\_len$). With the response property length ($prop\_len$), we can now calculate the BAF for a single property payload as follows:

$$BAF = \frac{RECV\_OVERHEAD + prop\_len}{SEND\_OVERHEAD + prop\_id\_len}$$

Table 4 shows a per-property BAF analysis: Property BAF details the length ratio of returned property and queried property ID. Payload BAF shows the received and sent payload length ratio for a packet requesting only this property.

We can see that *property list* has by far the largest property BAF with an average of 141. On the other hand, more than ten times as many amplifiers are available for properties such as *description*, *location* or *model name*. The property *firmware revision* combines many available amplifiers with a high BAF.

Due to the overhead introduced by BACnet headers, the payload BAF is much smaller than the property BAF.

5.5. Tuning the BACnet Payload

When issuing a request for a single property (as simulated with payload BAF in Table 4), the amplification potential of BACnet is not fully leveraged. Requesting multiple properties in the scanning payload can significantly increase the payload BAF. Figure 1 shows that our multi-property scans generate a median payload BAF of 9, exceeding all single-property mean payload BAFs in Table 4.

To raise the payload BAF even further, we can tailor a payload of multiple requests of the same property with a high property BAF factor. We very carefully test this behavior with a small number of BACnet devices. The devices not only answer the request without error, but also send the property multiple times. This allows us to leverage the

property BAF, minimize the overhead of BACnet headers, and hence boost payload BAF factors up to 120.

Figure 2 shows the distribution of payload BAF when the same property is requested multiple times. In this comparison, we choose the properties *property list* as it provides the largest average BAF and *firmware revision* as it has the most amplifiers with second largest average BAF. Additionally, we include the property triggering the largest response on a per-device level. The influence of BACnet headers decreases when we increase the number of requested properties from 5 to 50.

The majority of the amplifiers answering *firmware revision* requests give us a BAF below 10. About 10 % offer a BAF of about 30 when requesting this property 50 times.

Requesting *property list* five times already generates a larger BAF than 50 requests for *firmware revision*. About half of the 1389 amplifiers generate a BAF of 27 and 55, for 5 and 50 requested properties respectively. This BAF is larger than for SNMP-based amplification attacks and similar to those exploiting open DNS resolvers [24].

The distinctively noticeable steps in Figure 2's *property list* distributions are a result of vendor clustering: Devices produced by Trane, which occur 449 times, always have a *property list* length of 93 bytes. We found that all devices by Reliable Controls send a 188 bytes or longer *property list* This is a consequence of the large number of properties supported by these devices. However, it also means that these devices are particularly valuable targets for attackers who want to misuse them in amplification attacks.

Using the largest property on a per-device level includes all BACnet devices and gives us a higher BAF than *firmware revision*. 30 % of all BACnet devices allow for a BAF of 20 or larger. This type of attack, however, is more complex than simply choosing a single property: A preceding reconnaissance scan to find the largest property for each device and a device-specific payload would be necessary.

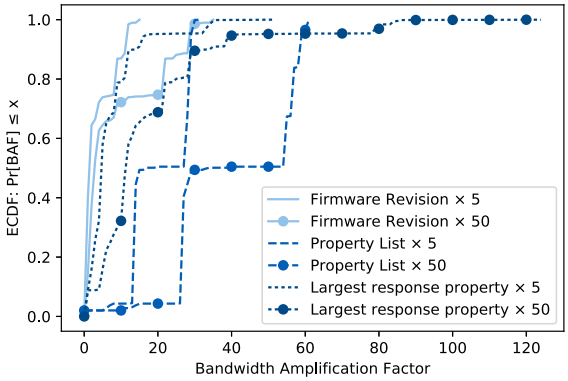

Figure 2: Payload BAF when issuing multiple requests for the same property (within a single Multi-Property packet).

6. Discussion

We use this section to discuss the implications of our results and how to improve the security state of BACnet devices. Accordingly, this section explores: (1) steps we took to notify affected networks and owners, (2) strategies for affected parties to detect and prevent BACnet-based attacks, and (3) action that the community can take to remedy the problem of publicly accessible BACnet devices.

6.1. Vulnerability Notification

We use our measurement results to improve Internet security by notifying the owners of affected BACnet devices. We cooperate with the DFN-CERT, which is the Computer Emergency Response Team for the German National Research and Education Network (DFN). We supply the DFN-CERT with relevant information of the affected systems. The DFN-CERT will then leverage its established international network to coordinate the notification process, especially with the CERT Coordination Center for the United States, in which most BACnet devices are located. By notifying vulnerable systems we hope to reduce the number of publicly reachable and abusable BACnet devices. Li *et al.* show that notification campaigns can drive measurable impact [17].

6.2. Mitigation Strategies

Affected network operators can adopt various strategies to reduce impact of BACnet attacks. First, and preferably, the operator of the device can move the device to a separate, not publicly accessible, network enforced by, *e.g.,* VLAN or VPN. However, this may not be feasible in many very small network scenarios. Second, the network operator may deploy rule-based access filtering to restrict access from the public Internet. Thirdly, at network operator or ISP level, strategies may be deployed to detect ongoing amplification attacks, e.g. by measuring traffic entropy [4]. Detected attacks could be rate-limited by an ISP.

6.3. Standardization Efforts

BACnet standardization could harvest quick wins in mitigating amplification attack potential by not allowing multiple reads of the same property in one packet, which we found critical in achieving a high BAF. However, this comes with a certain complexity and computational cost. We contacted ASHRAE regarding changing the BACnet standard to thwart the attack potential.

7. Related Work

In this section we elaborate on existing related work in the areas of Internet scanning for BACnet and similar protocols, amplification attacks and vulnerability notification.

7.1. Internet-wide Scanning

Both Mirian *et al.* [18] and Feng *et al.* [10] scan for BACnet and other ICS devices. In contrast to them we scan for all 16 standardized BACnet ports. We identify twice as many IP addresses that do not respond on port UDP/47808 for a total of $3.7\,\mathrm{k}$ valid BACnet responses missed by previous research. Neither of them discusses amplification potential of BACnet.

Censys [8], Project Sonar [23], and Shodan [26] perform regular BACnet scans, finding between $5.2\,\mathrm{k}$ and $7.8\,\mathrm{k}$ less devices than our scans.

7.2. Amplification Attacks

In 2014, Rossow [24] investigated numerous UDP protocols for their susceptibility to amplification attacks. He measures amplification factors, verifies the number of available reflectors and estimates how quickly they could be harvested by a malicious actor. We add BACnet to the list of affected protocols and evaluate its potential for amplification attacks.

In 2017, Sargent *et al.* [25] discuss the amplification potential of IGMP. They find $\sim 305\,\mathrm{k}$ amplifiers with a median amplification factor of 2.4. For BACnet, we find less amplifiers but a significantly higher amplification factor.

To detect amplification attacks at the reflector network, Böttger *et al.* propose a protocol-agnostic technique based on BAF and payload entropy [4]. Krämer *et al.* present AmpPot, a honeypot designed to track amplification attacks [14].

7.3. Notification

In 2016, Li *et al.* [17] investigated the effectiveness of reporting vulnerabilities to operators. They identify $45\,770$ devices supporting at least one industrial protocol. They compare remediation rates based on communication method, verbosity, website link, translated messages. They achieve a remediation rate of about $8\,\%$. This measurable impact motivates our notification campaign.

8. Conclusion

We conducted multiple Internet-wide active measurements to identify $16\,485$ BACnet devices. We found that they were heavily clustered in certain ASes and prefixes. Subsequently we uncovered that $14\,\mathrm{k}$ of these devices can be misused for amplification attacks. We evaluated the bandwidth amplification factor for a single property requested once, and a tuned payload where the same property is requested multiple times. Using this tuned payload we achieve amplification factors up to 120. Finally, we initiated a notification campaign through a CERT, and give advice on how to secure BACnet deployments.

Future work: We will conduct BACnet scans regularly to assess the impact of our notification campaign.

Acknowledgments: The authors would like to thank the DFN-CERT for their cooperation in the vulnerability notification, and the anonymous reviewers for their valuable comments. This work has been supported by the German Federal Ministry of Education and Research, project X-CHECK, grant 16KIS0530, and project DecADe, grant 16KIS0538.

References

[1] "IP2Location Geolocation DB," https://ip2location.com, August 2016.

[2] ASHRAE, *BACnet - A Data Communication Protocol for Building Automation and Control Systems*, 1995.

[3] ——, *BACnet - A Data Communication Protocol for Building Automation and Control Systems Addendum 135-2012aj*, www.bacnet.org/Addenda/Add-135-2012aj.pdf, 2016.

[4] T. Böttger, L. Braun, O. Gasser, F. von Eye, H. Reiser, and G. Carle, "DoS Amplification Attacks – Protocol-Agnostic Detection of Service Abuse in Amplifier Networks," in *TMA'15*.

[5] CAIDA, "Routeviews Prefix to AS mapping," www.caida.org/data/routing/routeviews-prefix2as.xml.

[6] Common Vulnerabilities and Exposures, "CVE-2003-0931," 11/2003.

[7] D. Dittrich, E. Kenneally *et al.*, "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research," *US Department of Homeland Security*, 2012.

[8] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman, "A Search Engine Backed by Internet-wide Scanning," in *SIGSAC'15*.

[9] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast Internet-wide Scanning and Its Security Applications," in *USENIX Security'13*.

[10] X. Feng, Q. Li, H. Wang, and L. Sun, "Characterizing Industrial Control System Devices on the Internet," in *ICNP'16*.

[11] O. Gasser, "bacnet.py: BACnet python module to parse BACnet response packets." https://github.com/tumi8/bacnet.py, November 2016.

[12] O. Gasser, Q. Scheitle, S. Gebhard, and G. Carle, "Scanning the IPv6 Internet: Towards a Comprehensive Hitlist," in *TMA'16*.

[13] IANA, "IPv4 Special-Purpose Address Registry," http://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml.

[14] L. Krämer, J. Krupp *et al.*, "AmpPot: Monitoring and Defending Against Amplification DDoS Attacks," in *RAID'15*.

[15] B. Krebs, "Hacked Cameras, DVRs Powered Today's Massive Internet Outage," https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/, October 2016.

[16] ——, "KrebsOnSecurity Hit With Record DDoS," http://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/, September 2016.

[17] F. Li, Z. Durumeric *et al.*, "You've Got Vulnerability: Exploring Effective Vulnerability Notifications," in *USENIX Security'16*.

[18] A. Mirian *et al.*, "An Internet-Wide View of ICS Devices," in *PST'16*.

[19] H. M. Newman, *BACnet: The Global Standard for Building Automation and Control Networks*. Momentum Press, 2013.

[20] C. Partridge and M. Allman, "Ethical Considerations in Network Measurement Papers," *Communications of the ACM*, 2016.

[21] I. Poese, S. Uhlig, M. A. Kaafar, B. Donnet, and B. Gueye, "IP Geolocation Databases: Unreliable?" *ACM SIGCOMM CCR'11*.

[22] M. Prince, "The DDoS That Almost Broke the Internet," https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet/, March 2013.

[23] Rapid7 Labs, "Project Sonar," https://sonar.labs.rapid7.com/.

[24] C. Rossow, "Amplification Hell: Revisiting Network Protocols for DDoS Abuse." in *NDSS'14*.

[25] M. Sargent, J. Kristoff, V. Paxson, and M. Allman, "On the Potential Abuse of IGMP," *ACM SIGCOMM CCR'17*.

[26] Shodan, "Map of Industrial Control Systems on the Internet," https://icsmap.shodan.io/.