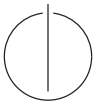
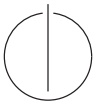



Technische Universität München
Department of Informatics

Bachelor's Thesis in Informatics

Active Security Evaluation with Network Scans

Nadja Schricker

Technische Universität München

Department of Informatics

Bachelor's Thesis in Informatics

Active Security Evaluation with Network Scans

Aktive Sicherheitsevaluation mit Netzwerk-Scans

Author	Nadja Schricker
Supervisor	Prof. Dr.-Ing. Georg Carle
Advisor	Oliver Gasser
	Quirin Scheitle
	Carl Denis
Date	October 17, 2016

Informatik VIII
Chair for Network Architectures and Services

I confirm that this thesis is my own work and I have documented all sources and material used.

Garching b. München, October 17, 2016

Signature

Abstract

Increasingly buildings are equipped with automation systems, which are controlled centralized, for heating, ventilation and security purposes. This thesis analyzes the network security situation of building automation systems via network scans.

A modified ZMap module is developed following a detailed study of the building automation protocol BACnet. This tool is used to identify building automation systems which are connected to the Internet. The thesis shows how detailed the detected systems can be analyzed via the data, which was collected in the scanning process. The detection of device types in use is part of the analysis, as well as market shares of vendors. This thesis breaks down the network structure of the reachable building automation systems and clusters them into5 Autonomous Systems (ASes), subnets and also to their geographical location. Traceroutes are used to give a closer look at the infrastructure of detected devices. The results of this evaluation are then put into relation to data which is already available. The IPv6 distribution of BACnet devices is analyzed via another scanning module.

The scan for building automation systems delivers 17 765 responses. After the execution of a filtering mechanism 13 596 packets were used for a detailed analysis of the detected systems. Even the identification of device types is possible via evaluation of requested properties and a check against publicly available data sheets. The analysis of the scanning data shows, that the detected BACnet devices are located in 1367 ASes and 4360 subnets. The evaluation via IP2Location documents that the building automation systems can be found in 80 countries, but 92.28 % of the devices are located in just ten countries. The execution of Traceroutes to the detected IPs proves that more than 4003 devices are reachable directly without any additional hop in their subsystem. This indicates that those devices are not protected via a firewall. A reverse DNS lookup of all IPs, which responded to the scan, detected 9585 valid DNS entries. The further analysis showed that the bulk carry the IP encoded in the DNS name, which indicates that the devices use dial up networks to access the Internet. A look to the BACnet IPv6 deployment reveals that either these devices have not yet been deployed or the security situation in IPv6 is more sophisticated than in IPv4.

This thesis gives evidence that building automation systems using the BACnet protocol can be reached via Internet. Scans, as well as traceroutes, can provide detailed knowledge about the devices and their network infrastructure. To provide a better security concept for Industrial Control Systems future studies should exploit the information details which are already available via state of the art scanning tools, because a detailed analysis of devices and their network structure will empower a more specific vulnerability notification.

Zusammenfassung

Immer mehr Gebäude sind mit Automatisierungssystemen für Heizung, Klimatisierung und Sicherheit ausgestattet, die zentral koordiniert werden. Diese Arbeit analysiert Gebäudeautomatisierungssysteme hinsichtlich ihres Netzwerksicherheitsstandards.

Durch die detaillierte Beleuchtung des Automatisierungsprotokolls BACnet wird ein modifiziertes ZMap Modul entworfen. Damit werden Gebäudeautomasierungssysteme aufgespürt, die direkt mit dem Internet verbunden sind. Diese Arbeit zeigt wie detailliert die erkannten Systeme anhand der durch den Scan gewonnenen Informationen analysiert werden können. Die Erkennung von Gerätetypen ist hierbei ebenso Teil der Analyse, wie die Diagnose von Herstelleranteilen. Die Netzwerkstrukturen der erreichbaren Systeme und eine Clusteranalyse bezüglich Autonomer Systeme und Subnetze werden ebenso ausgewertet wie die geographische Position. Außerdem wird die Möglichkeit Traceroutes als weiteres Analysetool zu verwenden, beleuchtet. Die Ergebnisse werden nach Abschluss der Evaluation mit den Daten anderer Studien verglichen. Die Verbreitung von BACnet Geräten im IPv6 Bereich wird mit einem weiteren Scan Modul analysiert.

Der Scan liefert 17 765 Antworten von Gebäudeautomatsierungssystemen. Nach der Anwendung eines Filtermechanismuses können 13 596 für eine detaillierte Analyse verwendet werden. Es ist sogar möglich Gerätetypen mithilfe der im Rahmen des Scans abgefragten Eigenschaften und Datenblättern zu identifizieren. Die Analyse der Antwortpakete zeigt, dass sich die Geräte in 1367 Autonomen Systemen (ASen) und 4360 Subnetzen befinden. Die Auswertung der IPs bezüglich geographischer Lage offenbart das zwar in 80 verschiedenen Ländern Gebäudeautomatiserungssysteme vertreten sind, der Großteil von 92.28 % jedoch in nur 10 Ländern lokalisiert ist. Die Verwendung von Traceroutes beweist, dass 4003 Geräte direkt erreichbar sind, ohne dass ein weiterer Hop im selben Subnetz stattfindet. Diese Erkenntnis legt nahe, dass die Geräte nicht durch eine Firewall geschützt sind. Ein reverse DNS Lookup der fast 18 000 antwortenden IPs liefert 9585 gültige Einträge. Die genauere Analyse macht deutlich, dass im Großteil der Fälle die IP im DNS Namen eingebettet ist. Diese Erkenntnis legt nahe, dass die Geräte ein Dial Up Netzwerk für den Internetzugriff verwenden. Ein Blick auf die Verbreitung von BACnet im IPv6 Bereich zeigt, dass solche Geräte entweder noch nicht verbreitet sind oder die Sicherheitssituation dieser Geräte auf einem anderen Niveau ist.

Die Studie zeigt, dass Gebäudeautomatisierungssysteme, die das BACnet Protokoll verwenden, im Internet erreichbar sind und Scans, ebenso wie Traceroutes ein Detailinformationen über die Geräte liefern. Spezifische Benachrichtigungen an betroffene Admins könnten die Sicherheitslage industrieller Kontrollsysteme verbessern. Details über die verwendeten Geräte und die Netzwerkinfrastrukturen hierfür können aus existenten Scanning Tools gewonnen werden.

Contents

1 Introduction 1
- 1.1 Goals of the thesis . . . 2
- 1.2 Outline . . . 3

2 Related Work 5
- 2.1 Industrial Control System Detection . . . 5
- 2.2 Security Research . . . 6
- 2.3 Existing Data . . . 7

3 Approach 9
- 3.1 Preparation of the Scanning Environment . . . 9
- 3.2 BACnet Scanning . . . 9
  - 3.2.1 Protocol Research and Payload Selection . . . 9
  - 3.2.2 Data Collection . . . 10
  - 3.2.3 Evaluation . . . 10
- 3.3 Comparison of Results . . . 11
- 3.4 IPv6 . . . 11

4 BACnet: Protocol 13
- 4.1 Protocol Background . . . 13
- 4.2 Payload Choice . . . 14
  - 4.2.1 Service Choice . . . 15
- 4.3 ReadProperty Packet . . . 15
  - 4.3.1 BACnet Virtual Link Control (BVLC) . . . 16
  - 4.3.2 Network Protocol Data Unit (NPDU) . . . 16
- 4.4 ReadPropertyMultiple Packet . . . 20
  - 4.4.1 Payload Structure . . . 20
- 4.5 Possible Answers . . . 21
  - 4.5.1 Complex Acknowledgment . . . 21
  - 4.5.2 Error . . . 22
  - 4.5.3 Reject . . . 22

5 Test Scans 25
5.1 Setup . . . 25
5.1.1 Evaluation . . . 27

6 Large Scale Scans 29
6.1 Scan Structure and Results . . . 29
6.2 Results and Evaluation . . . 29
6.2.1 Vendor Shares . . . 31
6.2.2 Device Types . . . 34
6.2.3 Clustering . . . 36
6.2.4 Network Infrastructure Analysis via Traceroutes . . . 43
6.2.5 Caveats . . . 45
6.3 Security Mechanisms in BACnet . . . 46

7 Comparison of Results 47
7.1 Scanning Payload . . . 47
7.2 Sonar . . . 48
7.3 Censys . . . 49

8 IPv6 51
8.1 Virtual-Address-Resolution Packet . . . 51
8.2 Virtual-Address-Resolution-ACK . . . 52
8.3 Results and Evaluation . . . 52

9 Conclusion and Future Work 55

Appendix 59

A Scanning Environment 59
A.1 Blacklist . . . 59

Bibliography 65

List of Figures

6.1 Number of devices per prefix 37
6.2 Number of devices in ASes 37
6.3 Geographic location based on IP2Location 40
6.4 Number of hops in destination AS 44
6.5 Number of hops in destination subnet 45

List of Tables

4.1 BACnet/IP ReadProperty BVLC 16
4.2 BACnet/IP ReadProperty Control Byte 17
4.3 BACnet/IP ReadProperty NPCI 17
4.4 BACnet/IP ReadProperty APDU Type 18
4.5 BACnet/IP ReadProperty APDU Response 18
4.6 BACnet/IP Tag 19
4.7 BACnet/IP ReadProperty APDU Structure 20
4.8 BACnet/IP ReadProperty Packet Structure 20
4.9 Control Byte Confirmed ACK 21
4.10 APDU Type Complex Acknowledgement 22
4.11 List of Properties 23
4.12 BACnet/IP Complex Acknowledgement Packet Structure 23

5.1 BACnet/IP Property IDs 26
5.2 Test Scans: Comparison of Results 28

6.1 Large Scale Scans: Comparison of Results 30
6.2 Top 10 vendors according to Vendor ID 31
6.3 Top 10 automation vendors by revenue of their automation segment [1] 33
6.4 Top 5 conglomerates by number of devices 33
6.5 Top 10 devices according to Model Name 34
6.6 Top 10 Autonomous Systems hosting ICS according to Leverett [2] . . 38
6.7 Top 10 Autonomous Systems hosting BACnet devices 38
6.8 Top 10 countries with Modbus devices according to Durumeric et al. [3] 39
6.9 Top 10 countries hosting BACnet devices 40
6.10 Timezones for devices in top ten countries 42
6.11 Top 10 domain label 43
6.12 Number of hops in destination AS 44

7.1 Properties Requested by Scanning Modules 48
7.2 Comparison of Scanning Results 48

8.1 Virtual-Address-Resolution Packet 52

8.2 Virtual-Address-Resolution-ACK Packet 52

Chapter 1

Introduction

Literature suggests that most Industrial Control Systems (ICS) encounter large security lacks and are vulnerable to cyber attacks [4]. Water and energy supply, transportation and building automation are examples which rely on the functionality of ICS. Frequently those components are often physically distributed and need to be organized in a centralized manner to enable a synchronized operation. As a consequence there is a growing need for interconnection. Remote access to components is necessary to control and coordinate the systems [5]. Protocols in use are decades old and often do not address any security standards. According to Stouffer [5] some systems have the characteristics that include a risk to the environment and even human lives. The knowledge about ICS being connected to the Internet is no longer a secret and draws the attention of hackers.

In 2013 hackers with relations to the Iranian government, executed attacks to financial institutes in the USA and subsequently targeted and affected a flood-control dam north of New York [6]. The security exposures are not limited to specific countries, but are global. The Bundesamt für Informationstechnik (BSI) publishes a yearly report about the IT security in Germany, one part is the security of Industrial Control Systems. In 2014 the report of the BSI references a directed attack via spear fishing and social engineering on a steel mill [7]: The attacker showed knowledge about the classical IT environment and about ICS components. He impacted controlling components and prevented the managed shutdown of a blast furnace. The BSI report of 2015 references a growing awareness of the problem in the industrial environment, but at the same time qualifies the risk potential as even higher than in 2014 [8].

In December 2015 an Ukrainian electricity distribution company suffered a service outage of serveral hours [9]. As it turned out this was due to a cyber attack on the distribution grid. Shortly after that a group of hackers, who are specialized on ICS security, reported on the “Chaos Communication Congress” that they performed an attack on train control systems [10]. They recognized, that the routing devices in use are often accessible via default credentials, outdated software is in place and physical

security is not guaranteed. This could even result in a remote control of the switch stands by an attacker. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported 295 security incidents in the United States in 2015 [11], 11 % due to network scanning and probing. According to this report 231 device vulnerabilities had to be handled in 2014, but this number significantly increased to 486 in 2015 [11]. The SANS Analyst Program, disclosed that these notifications are essential to 59 % of the administrators of Industrial Control System, because this amount of participants monitor CERT notifications using an active vulnerability scanner [12]. Automation is increasing in all sectors. The building automation market had 29.78 Billion USD revenue in 2013, the prognosis is that this value will in increase to 55.48 in 2020 [13]. As a consequence this segment has become an attractive target for cyber attacks. ICS-CERT reported in 2013 that an intruder used the vulnerability of the Niagara platform to manipulate set points and modify temperature settings [14]. In 2013 researchers also hacked the building control system at the Google Australia office in Sydney. They could not only control heating and air conditioning, but also access blueprints of the building [15]. In both cases the building automation systems were based on the "Building Automation and Control Networks" (BACnet) protocol. In February 2016 the IBM X-Force broke into a building automation system. According to an article in the Building Automation Monthly [16] the force detected a Router which should grant remote access to the building and used URL manipulation and path traversal to access the login credentials. They moved onwards via an NMAP scan and found an open administrator port leading to a device which held the credentials of the building automation server. Afterwards IBM started to offer the project "Penetration testing of building automation systems" [17]. AS a consequence the question applies if the security of building automation systems is really in such a bad shape. Or if it could even be possible to detect vulnerable components online via a scan for a building automation protocol. This research will therefore investigate the security standards in building automation via scans for components which are using the building automation protocol BACnet.

1.1 Goals of the thesis

This thesis will investigate the following research questions:

1. Scanning and analysis of results

- Is it possible to detect building automation systems in the public Internet via state-of-the-art scanning tools?
- Is it possible to classify device types in use?
- Can the devices be clustered according to ASes, subnets, geographic location?

2. Network infrastructure analysis of the targets

   - Is it possible to gain additional information by executing traceroutes to identified devices?

3. Evaluation of results and comparison with other tools

   - What are the differences between the results of this study and other tools?
   - What are the reasons for these differences?

4. Analysis of IPv4 vs. IPv6 usage

   - Is IPv6 deployed in ICS?

1.2 Outline

The thesis is structured as follows: Chapter 2 includes an overview of related work about ICSs and especially BACnet security, vulnerability notifications in this environment and existing scanning data.
Chapter 3 introduces the methods and materials used for the protocol research the scans and the evaluation.
Chapter 4 provides an overview about the origins of the BACnet protocol and especially about the transfer to the IP layer. The protocol structure is introduced and analyzed in order to identify an effective scanning payload.
After identifying several possible payloads, chapter 5 describes the executed test scans to evaluate which payload would offer the highest information density and reach the maximum of devices.
Chapter 6 describes the Large Scale IPv4 scan and presents the results, as well as the evaluation of the scanning activity. The results of the active scans are compared to existing data in chapter 7.
Chapter 8 analyzes the BACnet distribution in IPv6.
The conclusion drawn from the presented results, is presented in chapter 9.

Chapter 2

Related Work

This chapter focusses on the work which is related to this thesis. It presents the results of existing researches and the data, which has been already available to point out the relation between previous work and this thesis.

2.1 Industrial Control System Detection

In 2011 Eireann P. Leverett published his dissertation "Quantitatively Assessing and Visualising Industrial System Attack Surfaces" at the University of Cambridge [2]. He showed that Industrial Control Systems are in fact connected to the public Internet and are accessible. The author did not execute any scans by himself, but based this work on data present in Shodan [18]. Shodan is a search engine which is described in more detail in chapter 2.3. The device categorization was done via domain expertise and exploit information was collected via Metasploit and ExploitDB. The geolocation was done via the device information gained via Shodan and the Google geocode service, which provides longitude and latitude of each country. On top, the author collected information about the operating system by accessing available HTTP interfaces of devices. During this work 7489 devices were detected in total. The author also provides a top ten of the Autonomous Systems with the largest count of ICS. It is necessary to take into account, that back when this research was done, Shodan was only focused on four ports and most SCADA protocols could not be detected. This work will focus on building automation components only. The development of a specific scanning tool is part of the thesis and the collected data about Autonomous System distribution will be compared to Leverett's results in section 6.2.3.1.

A research at Freie Universität Berlin in 2014 [19] documents the accessibility of electronic control units in Europe. The "SCADA Systems and Computer Security" team at the university used Shodan as the main data resource. The list of search words

included 123 strings containing parameters such as product name and manufacturer. Ping, Traceroute, Whois and Reverse DNS were used to further analyze the devices, their connectivity and the owner. The geo location was done via GeoIP Lite. The paper documents 79 269 Industrial Control Systems in Europe. To analyze the threat situation of these systems the researchers synchronized the collected device data with weakness and exploit data bases. The outcome was that 9368 ICS are vulnerable according to those data bases. This work is not based on results, which are presented by Shodan, but it focusses on the development of an own scanning tool, which detects Building Automation Systems. The evaluation is based on the data which is collected via an active scan and the location of the detected devices is done via IP2Location [20].

Another research of the SCADACS team [21] focuses on Siemens PLCs. The team developed an SNMP scanner for this project. As a result they detected, that it is possible to inject malware into a PLC, which does not require a program restart and makes it possible to use the device as a gateway into the local network. Therefore all other components of the ICS are exposed. This work will focus on devices which use the open protocol standard BACnet. Therefore it is not limited to components which are produced by specific vendors, but capable to detect devices independent of the manufacturer.

The project SHINE (Shodan Intelligence Extraction) [22] took place in 2014. The goal was to detect vulnerable systems. The approach was to extrapolate meta data from the Shodan engine, such as IP address, location (including latitude and longitude) and protocol type. Keywords such as “Modbus" and infrastructural circumstances such as Uninterruptable Power Supply were decisive for the categorization of the devices. The results are based on the protocols Siemens SIMATIC/ICCP (port 102), DNP3 (port 20000), Modbus/TCP (port 502), Ethernet/IP (Port 44818) and BACnet (port 47808). The team detected 586 997 industrial systems, out of which 13 475 were Building Automation Systems [23]. This work will perform a scan for BACnet devices and evaluate informations such as device types, geographical location and network infrastructure in more detail.

A research team at the University of Michigan developed a cloud-based service called “Censys". It is a search engine to analyze data which was collected via Zmap Scans [3]. Part of the analysis was the detection of Industrial Control Systems which are using the Modbus protocol. 32 622 devices located in more than 1880 ASes and 117 countries were discovered. 92 % of the devices even answered a device identification request. This thesis will focus on the BACnet protocol and compare the geographical distribution with the results of the University of Michigan in section 6.2.3.2.

2.2 Security Research

In 2012 Celeda et al. [24] published a study about flow-based analysis of building automation system networks. The analysis of the data flow shall enable the early detection of

network anomalies. The researchers were capable of detecting scans, BACnet spoofing and Denial of Service (DoS) attacks via their extension of BACnetFlow. BACnetFlow is a tool which was developed earlier by Krejci et al. [25] and is based on the Flow Mon exporter engine. This thesis will analyse the current security situation of BACnet devices in the Internet to find out of if security mechanisms such as the BACnet Flow are used.

Kaur et al. [26] analyzed the possibility to secure BACnet networks via a "Snort-Based Normalizer" in 2015. Therefore the team created a BACnet testbed with virtual machines which represent BACnet devices. Scenarios with 10 000 and 100 000 messages were created. It turned out that the Normalizer was capable to differentiate between conforming and non conforming BACnet traffic in all cases. All complaint messages reached their destination and non-complaint messages were dropped or modified correctly. Also flooding was detected as not successful as soon as the Normalizer was in use. Part of this research is the development of a scanning tool for BACnet capable devices and the analysis of the protocol compliance of the response packets.

In 2016 a collaboration of researchers of different American Universities founded the "Berkeley Security Notifications Team" to explore the effectivness of vulnerability notifications [27]. Industrial Control Systems were identified via ZMap Scans for the ICS protocols DNP3, Modbus, BACnet, Tridium Fox and Siemens S7. The group of participating IPs was selected via scans done on three consecutive days. Only Industrial Control Systems which were present on every day, were selected, to avoid IP churn. In this way 45 770 ICSs were selected. 79.7 % of those had WHOIS contact details, 5.6 % WHOIS had abuse contacts. All hosts with abuse contacts where randomly assigned to notification groups. The groups differed in notification style and party to notify. Notifications were done via National CERTs, US-CERT and directly to the WHOIS abuse contact. The messages sent to the WHOIS contacts varied in the level of detail. The shortest message only contained the information that the vulnerability was detected via scanning and what the impact could be. In another notification a link to a website with detailed information was included. The third type was a verbose message with detailed information. The outcome was, that notifications containing very detailed informations and sent to the WHOIS contacts developed the highest resonance. 11 % of the notified parties addressed their security issues. This research focuses on the analysis of ICS which are using the BACnet protocol. It evaluates device details as well as the network infrastructure of the detected systems.

2.3 Existing Data

Shodan [18] allows to search for ports, specific metadata and strings. Shodan offers a specific category for Industrial Control Systems. The protocols introduced are Mod-

bus, Siemens S7, DNP3, Tridium Niagara Fox, BACnet, EtherNet/IP, GE-SRTP, Hart IP, PCWorx, MELSEC-Q, FINS, Crimson v3.0, CODESYS, IEC 60870-5-104 and ProConOS. The protocol search results are not only dependent on the specific ports but on a combination of the port and specific search strings. Shodan offers also a “Map of Industrial Control Systems on the Internet" [28]. It is based on the findings of the project SHINE (Shodan Intelligence Extraction) [22]. According to the findings in this project 586 997 Industrial Control Systems could be found, out of which 13 475 were building automation devices [23]. This work will focus on the detailed analysis of the cyber situation of building automation components using the BACnet protocol. Detailed scans will be scheduled to determine the number of reachable devices and collect detailed information about every device. The data gained via the scans will include the type, the vendor and the location of the device.

Scans.io [29] is a repository for data which was gained via internet wide scans. The operator is a team at the University of Michigan. The researchers schedule scans regularly including one for BACnet devices. The search engine Censys has been developed by this team to offer the possibility to access the scanning data. Censys [30] allows to search for ports, protocols (name+port) and attributes. An attribute can be the location, tags or metadata. Censys even allows to combine search requests. A possible search request for this use case would be “protocols: 502/Modbus AND location.country_code: DE”, which would detect the Modbus capable devices in Germany. The search result offers the possibility to visualize metadata such as country and Autonomous System. Afterwards it is possible to build a report. The order criteria of the results can be selected by the user. Selection criteria such as location or even heart bleed vulnerability are possible. However Censys is limited regarding protocol formats. In April 2016 the tool only supports some ICS relevant protocols: BacNet, Fox, Modbus, Siemens S7 and DNP3 without encryption. Other industrial protocols such as IEC 60870-5 are not supported. Another scan which is relevant in this context are the results of project Sonar done by Rapid7 [31]. A BACnet scan is scheduled regularly and the results are also published on Scans.io [29]. The results of both scans have not been analyzed in detail yet. Part of this thesis is the development of a modified ZMap module which detects BACnet devices. The results of this scan will be compared to the data which is available on scans.io in chapter 7.

Chapter 3

Approach

The thesis is based on data which was collected via several scanning processes. First of all it was necessary to prepare the scanning environment and research the BACnet protocol to determine the best payload for a scan. Afterwards the data of building automation systems which are connected to the Internet was collected via scan and in the end the collected data was evaluated.

3.1 Preparation of the Scanning Environment

All scanning activity was executed via a server at the TU Munich. The server in use was planetlab7, an 8 core Intel Xeon W3565 3.2 GHz with 12 GB RAM and the IP address 138.246.253.7. To provide information to anybody noticing the scan of his system, the environment was prepared in the following way: The DNS entry was already present, but a website informing about the scanning activities and the background of the scan had to be created. This website provided information about the purpose of the scan, the responsible parties and contact details. The possibility to request blacklisting was also explained in detail, but until the end of this research no abuse complaint or blacklisting request arrived.

3.2 BACnet Scanning

The first part of the thesis focuses on the BACnet devices which are accessible via IPv4.

3.2.1 Protocol Research and Payload Selection

A detailed research about the building automation protocol BACnet provided the base for an active scan, which should collect the necessary information to evaluate the security

situation of building automation systems. This research was primarily done via sources which were publicly available. Later the results were validated via a comparison with the BACnet Standard [32]. The goal was to find a scanning method, which achieves the maximum information gain with minimal intrusiveness. The scanning tool for this thesis was ZMAP [33]. ZMAP includes a BACnet module per default. The payload is a ReadProperty packet for the Object ID. Due to the fact that the Object ID is part of every answering ComplexACK, this module doesn't offer additional information for a detailed diagnostic of the answering BACnet device. Test scans were scheduled to find the payload which provides the best combination between detecting as many BACnet devices as possible and gain as much information about those devices during the process. The ZMAP module has therefore been expanded to enable the request for other properties and to send a ReadPropertyMultiple packet instead of a ReadProperty packet.

3.2.2 Data Collection

After determining the best payload to detect and analyse the building automation systems, large scale scans were scheduled. These scans were done with the extended ZMAP module and targeted the whole IPv4 address space, which was announced at this point in time, excluding a specified blacklist, which is part of the appendix A.1. This blacklist was developed during earlier scanning activities of the chair. For each answering packet all contained data was collected in a CSV file.

3.2.3 Evaluation

The main part of the evaluation was done in Jupyter Notebook including the Python libraries pandas, numpy, math, matplotlib, netaddr, ipaddr, datetime, struct and warts. Additionally the following tools were in use: The collected data was filtered for valid packets via a python script written by Oliver Gasser [34]. The analysis of subnet and AS distribution was done via the Prefix to AS mappings of CAIDA [35] and the script by Oliver Gasser. The geo location of the devices was determined via the timezone which was calculated by the date and time provided in the answering packets and a lookup in the TimeZoneDB database [36] and the country evaluation of IP2Location [20]. To provide information about the network structure of the detected devices, several tools were in use. MassDNS [37] accomplished the reverseDNS lookup, a script by Patrick Sattler [38] absolved the preprocessing to categorize networks, and Scamper [39], which delivered the traceroutes to each device.

3.3 Comparison of Results

The results of the IPv4 scan have been compared with the available data on Scans.io [29]. To enable a comparison of the scans done by Censys and Sonar, the blacklist which was in use for the IPv4 scans during this thesis was matched on the results. Afterwards the results published on Scans.io were also filtered via the script of Oliver Gasser [34]. Again the evaluation of differences was done via a Jupyter Notebook with Python libraries.

3.4 IPv6

After the evaluation of the IPv4 distribution of BACnet devices, the research focussed on IPv6. Again a protocol analysis had to be performed to select the sensible payload. Potential targets were selected by a reverseDNS lookup with MassDNS [37] for the IPv4 addresses which answered the IPv4 scan and a lookup for the IPv6 addresses of the resulting domain names. The ZMAPv6 module developed in context of the research "Scanning the OPv6 Internet: Towards a Comprehensive Hitlist" [40] was used to send the specific payload to the detected devices.

Chapter 4

BACnet: Protocol

This chapter gives a short overview of the history of BACnet, introduces the protocol structure and provides details about the payload which was selected for the active scan and the possible response types.

4.1 Protocol Background

The Standard Project Coommittee (SPC 135) within the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) started the development of BACnet in 1987 [41]. The first edition of the standard was released in 1995 and was asopted as global standard ANSI/ASHRAE 135-1995 in 2003.

BACnet is a protocol used in building automation. The product range includes devices for HVAC (Heating, Ventilation and Air Conditioning), life safety such as pull stations, fire detectors and sirens [42] to all kinds of security equipment such as sensors, CCTV (Closed Circuit Television) and access control [43]. Messages can therefore e.g. be input and output values for window states (open/closed), temperature sensors, event and alarm functions generated by motion sensors and data for configuration purposes [44]. As soon as buildings are spread out to a wider area the centralized monitoring gets important, which enables interconnection between building automation systems. BACnet provides its own network layer, but it also supports a transport via other data links. Currently transportation of BACnet messages is possible via ARCnet, Message Token/Passing, Point to Point, LonTalk, ISO 8802-3, ZigBee and Ethernet [43]. Due to the fact, that Ethernet is quite common and offers the fastest way of transportation, the IP network is widely used as a backbone that interconnects isolated BACnet networks [24]. Originally BACnet/Ethernet was designed to tunnel BACnet messages from one IP subnet to another [41]. Therefore the BACnet devices themselves don't need IP support. Only

one Router per Network is capable of receiving, translating and forwarding IP messages. Due to the fact, that computational power increased and became inexpensive, some vendors developed the idea of producing BACnet devices with native IP support. 1999 ASHRAE published Annex J, a specification of BACnet/IP which enables the usage of these devices [45]. Due to the wide distribution of the IP network nowadays, this thesis will focus on BACnet/IP. It is based on the User Datagram Protocol (UDP) and uses the port range 47808-47817 [41]. The default port is 47808.

4.2 Payload Choice

The BACnet application layer is based on objects and services [41], differentiated in five categories: object access (read, write, create, delete), device management (discover, time synchronization, initialize, backup and restore database), alarm and event (alarms and changes of state), file transfer (trend data, program transfer) and virtual terminal (human machine interface via prompts and menus) [43]. The selection of the service is essential for the success of the scan. Four criteria were essential for our selection of the used service:

- Maximum coverage of the Internet connected BACnet devices via a minimum number of packets
- Maximum information gain concerning the reachable devices via the scanning process
- Minimum impact on reached devices
- Minimum intrusiveness

All packets which would manipulate the status or the properties of a device have not been considered, because the usage would not be complaint to the proposition to perform a scan with a read approach.
To minimize the intrusiveness operations which would require a login for the system have also been dismissed.
BACnet/IP offers unicast and broadcast messages, latter can be subdivided in local, remote and global. The protocol was designed to interconnect one or more IP subnets assigned to a single BACnet network number and a B/IP Broadcast Management Device (BBDM) [46]. The function of the BBDM device is to maintain the broadcast communication between devices which are members of the subnet and devices outside the network. Therefore the usage of a broadcast message would not support the purpose of reaching as many BACnet devices as possible, because it is not capable of crossing IP gateways [47].
Another complexity is, that many services require the specification of a the destination BACnet network number. The precondition for the usage of such a service would be

the detection of the network number of each BACnet device and would increase the effort significantly.

4.2.1 Service Choice

One possibility for a potential scan is the “Who has” packet. This packet is used to deliver the Object Identifier of a BACnet device [48]. This is a broadcast possibility to detect all devices which are having an object with a specific identifier and name. In exchange all devices with this object deliver an "I have" packet and an object identifier. Due to the fact, that only devices which are having this object would answer a request, a scan would need different packets to cover all BACnet devices which are reachable via the Internet. Also the selection of a property which is part of the preconditions to be be compliant to the BACnet standard would maximize the number of reachable devices, this packet is still a broadcast message and could be intercepted, trying to cross network borders. Additionally the information gain with this packet is limited, because the answer would only contain the requested property.

Another possibility to detect a large number of BACnet devices is to use the “Who is” service. This packet is predestined to detect network addresses of devices which are hooked up to the same network. As a scanning payload this packet would serve the purpose to detect many devices, but the answering packets would not offer any additional information other than the network address. The service which serves all of the selection criteria best is the “ReadProperty" service. This is the only service which is required by standard to be processed by all BACnet devices [49] and should therefore reach all addressed devices. Another advantage is the fact, that this message can be sent to a Wildcard Object ID 4194303, which makes it obsolete to address every single ID. Therefore it is possible to send a unicast packet, which is not intercepted at network borders to a broadcast ID which will be processed by every device irrespective of its own ID. Due to the fact that the “Read Property" service can be used to ask for every single property of the countering device, the information gain via scanning can be driven to a maximum. Additionally the intrusiveness of this request is low because the information is freely available and doesn’t require a login mechanism.

4.3 ReadProperty Packet

The “ReadProperty” packet consists of three parts, the BACnet Virtual Link Control (BVLC), the Network Protocol Data Unit (NPDU) and the Application Protocol Data Unit (APDU).

4.3.1 BACnet Virtual Link Control (BVLC)

The complexity of BACnet/IP is, that not all BACnet devices are capable of interpreting this packet directly, instead a BACnet/IP PAD (BACnet/Internet-Protocol Packet-Assembler-Disassembler) is necessary. For the scan it is necessary to simulate this translation by using the BACnet Virtual Link Layer (BVLL) which grants the connection between the BACnet Network Layer and the underlying communication subsystem [32]. The specification of the layer is done via the "BACnet Virtual Control" (BVLC) functions. The "American Society of Heating, Refrigerating and Air-Conditioning Engineers"(ASHRAE) specifies the BVLC layer as follows:

Type:
This field was designed to provide the virtual link layer implementation, BACnet/IP is represented by value 0x81 [41].

Function:
The function of the following Network Protocol Data Unit (NPDU) which will follow is described in this field. BVLC functions can be subdivided in two categories: Message Distribution and BBMD Table Management [41]. Original-Unicast-NPDU (0x0a) defines, that the data is sent directly via UDP, using the BACnet port number, to another BACnet/IP device [47].

Length:
This field specifies the length of the whole BACnet packet in bytes. Per default the BVLC is calculated with 4 bytes and therefore the calculation for this field content is (packet length-4) [41].
The BVLC part of the “ReadProperty” packet is visualized in table 4.1.

Table 4.1: BACnet/IP ReadProperty BVLC

BVLC	
Type	0x81
Function	0x0a
VLC Length	0x0010

4.3.2 Network Protocol Data Unit (NPDU)

The NPDU subdivides itself in a header - the Network Protocol Control Information (NPCI)- and the Application Protocol Data Unit.

4.3.2.1 Network Protocol Control Information (NPCI)

The NPCI is responsible for the specification of the BACnet version and the transportation information which is independent of the overlaying data link transport layer [50].

NPDU Version:
The BACnet version in use is 1 [44]. 1 byte is destined to represent the version, therefore the field content is 0x01.

NPDU Control:
8 bit are reserved for the Control functionality. Table 4.2 is documenting the bit-encoding. The only Bit which has to be set is the definition of a reply expectation, because the Read Property packet expects an "Complex ACK" as a response.

Table 4.2: BACnet/IP ReadProperty Control Byte

Bit		Specification
0...	....	NSDU contained
.0..	....	Reserved (has to be 0)
..0.	....	Destination Specifier: DNET, DLEN, DADR, HOP Count (0 if absent)
...0	....	Reserved (has to be 0)
....	0...	Source Specifier: SNET, SLEN and SADR (0 if absent)
....	.1..	Reply Expectation (1 if reply is expected)
....	..0.	Priority (0 if not a Life Safety or Critical Equipment message)
....	...0	Priority (0 for normal messages)

The NPCI of the ReadProperty packet is visualized in table 4.3.2.1.

Table 4.3: BACnet/IP ReadProperty NPCI

NPCI	
Version	0x01
Control	0x04

4.3.2.2 Application Protocol Data Unit (APDU)

BACnet defines 8 PDU types [41], the APDU is either of fixed or of variable length depending on the packet content.

APDU Type and Packet Segmentation:
The type gives evidence about the structure and the contained fields of the APDU. 8 Bit are reserved for the configuration of type and segmentation. The configuration is visible in table 4.4.

Table 4.4: BACnet/IP ReadProperty APDU Type

Bit		Specification
0000	....	APDU Type (Confirmed Request)
....	0...	Segmented request (0 for unsegmented)
....	.0..	Segments to follow (0 for no segments)
....	..0.	Segmented response accepted (0 for not accepted)
....	...0	Reserved (has to be 0)

APDU Response:
This research focused on a packet type which does not allow segmentation. The background for this decision is, that many devices do not allow segmentation and therefore will not send an unsegmented answer, but reject the packet because they do not allow segmentation. Therefore the 8 Bit for the APDU Response, which specify the maximum response segments and the maximum size of the APDU, were chosen as visible in table 4.5. 0x0101 as selection of the size means that a response with up to 1476 octets is accepted, which is supposed to fit a frame according to ISO 8802-3 [51].

Table 4.5: BACnet/IP ReadProperty APDU Response

Bit		Specification
0000	....	Response Segments Maximum (0 for unspecified)
....	0101	Maximum Size of Response APDU

Invoke ID:
The Invoke ID is used to identify the packet in combination with source and destination address [52]. To enable the correct identification the scanning module has to increment this value for each session.

Confirmed Service Choice:
This thesis focuses on the “ReadProperty” service. It is necessary to distinguish between two types: the “ReadProperty” queries for one property which is represented by the value 0x0c and the “ReadPropertyMultiple”, which will deliver more than one property at a time, this service is triggered with the value 0x0e [53]

Context Tag 0:
Because BACnet encompasses packets with variable length, are Context Tags necessary. Context Tagging in BACnet is working in different ways depending on the length of the context. For a length<5 the tag is structured as visible in table 4.6. There are two classes of tags, application and context specific. The Tag Number states precisely which application data type will follow [54]. In this case the Class Specification is 0, because as specified in the class field, this is no application specific tag, but a context specific tag represented by value 0. The last field is either in use to show the length of subsequent data, to specify the value or represent the presence of additional embedded tags [54].

Table 4.6: BACnet/IP Tag

Tag Number	Class Specification	Length, Value, Type of Encoding
4 bit	1 bit	3 bit

Object Identifier:
The Object Identifier is one out of three properties which have to be present in every BACnet device [49]. 4 Bytes divide themselves in Object Type and Object Instance. The construction was detailed by the ASHRAE member Karg in 2012 [55, page 2] in the following way:
10 bit are in use to specify the type of an object, the definition is done by the vendor. BACnet standard types are enumerated from 0 to 127, non-standard types can be symbolized with 128 to 1023. Examples are the "Analog Input", which enables a censor input or specifies the "Device" object type. It includes informations such as vendor, supported services or firmware revision, this type is represented by the value 8. [49]. The next 22 Bit specify the Object Instance, the assignment of instance number and object is done by the vendor. The only value which is configurable and has to be constant also in case of a power outage or a reset, is the Device Object. Honeywell as an example uses the last two octets of the MAC address for instance number generation [56, page 19]. Those values are defined for each BACnet network separately, because this identifier should be unique in a network. A value in the range of 0-4194303 is possible, but the BACnet standard states, that no device should have the ID 4194303 [55, page 1]. ZMap [33] is using exactly this value for the probe module. The log includes the comment, that this is the packet all BACnet devices should respond to [57]. A paper about BACnet MS/TP [58] states, that the ID 4194303 can be used as a wildcard to address devices without knowledge about their device ID. Therefore we will also be using this value in this study.

Context Tag 1:
The second Tag has also the number 0, because this is no application specific tag, but a context specific tag represented by value 1 as specified in the class field.

Property Identifier:
16 Bit are reserved for the Property ID therefore a value between 0-65535 is possible. Part of this work was the comparison of scanning results for different properties. The details of this analysis are presented in chapter 5.

The APDU which has to be sent is visualized in table 4.7.

The resulting UDP Payload for the test scan with the ReadProperty packet is visible in table 4.8.

Table 4.7: BACnet/IP ReadProperty APDU Structure

APDU	
APDU Type	0x00
APDU Response	0x05
Invoke ID	0x68
ServiceChoice	0x0c
ContextTag1	0x0c
Object Type+Instance	0x023fffff
ContextTag2	0x19
Property Instance	dynamic

Table 4.8: BACnet/IP ReadProperty Packet Structure

Read Property Packet			
BVLC		Type	0x81
		Function	0x0a
		VLC Length	0x0010
NPDU	NPCI	Version	0x01
		Control	0x04
	APDU	APDU Type	0x00
		APDU Response	0x05
		Invoke ID	0x68
		ServiceChoice	0x0c
		ContextTag1	0x0c
		Object Type+Instance	0x023fffff
		ContextTag2	0x19
		Property Instance	dynamic

4.4 ReadPropertyMultiple Packet

Another possible payload is the usage of the ReadPropertyMultiple service.

4.4.1 Payload Structure

This packet is organized similarly to the ReadProperty packet. The type of service (0x0e instead of 0x0c) and the length value in the BACNet Virtual Link Control, the UDP, the IP and the Ethernet Header have to be adjusted, after the tagged list with the wanted values is added. For a maximum information gain in one scan, this thesis focusses on the combination of all property values which were successfully tested with a ReadProperty packet and showed information potential.

4.5 Possible Answers

The ReadProperty/ReadPropertyMultiple packet can trigger three different responses:

- Complex Acknowledgement
- Error
- Reject

4.5.1 Complex Acknowledgment

The best case of a possible answer to the ReadProperty/ReadPropertyMultiple packet is a Complex Acknowledgement (ComplexACK). It provides the information, that a confirmed service has been executed and delivers the requested data [41].

4.5.1.1 BACnet Virtual Link Control (BVLC)

The BACnet Virtual Link Control layer only varies according to the packet length. It depends on the length of the transmitted value and the necessary tagging.

4.5.1.2 Network Protocol Data Unit (NPDU)

The value of the BACnet version is also 1.
The definition of the Control Byte works as in the Read Property packet, similar to the specification in table 4.2. The only difference is, that in case of the Complex Acknowledgement no answer is required, therefore no Bit is set. See table 4.9 for a detailed description.

Table 4.9: Control Byte Confirmed ACK

Bit		Specification
0...	....	NSDU contains
.0..	....	Reserved (has to be 0)
..0.	....	Destination Specifier: DNET, DLEN, DADR, HOP Count (0 if absent)
...0	....	Reserved (has to be 0)
....	0...	Source Specifier: SNET, SLEN and SADR (0 if absent)
....	.0..	Reply Expectation (1 if reply is expected)
....	..0.	Priority (0 if not a Life Safety or Critical Equipment message)
....	...0	Priority (0 for normal messages)

4.5.1.3 Application Protocol Data Unit (APDU)

The Complex Acknowledgement Type Byte is structured as can be seen in table 4.10.

Table 4.10: APDU Type Complex Acknowledgement

Bit		Specification
0011	....	APDU Type (Complex Acknowledgement)
....	0...	Segmented Request (0 for unsegmented)
....	.0..	Segments follow (0 for no segments)
....	..0.	Segmented response accepted (0 for not accepted)
....	...0	Reserved (has to be 0)

The values Invoke ID, Confirmed Service Choice and Context Tag 0 are not different from the Read Property Request structure.

Object Identifier:
The Object Type is Device, as in the Read Property packet. The Object Instance will be the Device ID of the answering BACnet device.

Context Tag 1:
This Tag is defined as Context Tag 1 in the Read Property packet.

Property Identifier:
This is the Object Identifier again, represented by value 75.

List of Properties:
The specification of the list is subdivided in three parts, the opening tag, the actual property identification with the specific tag and a closing tag, as visible in table 4.11. Table 4.12 shows an example structure for a ComplexACK answering a ReadProperty packet.

4.5.2 Error

An Error is a packet which provides the reason why a confirmed request failed [41]. A possible error could be, that the property which is requested is not known by the addressed device.

4.5.3 Reject

A Reject provides the reason why a confirmed request was rejected, typically due to protocol errors which prevented the addressed device of interpreting the request

correctly [41]. Should an addressed device not be capable of parsing the “ReadProperty” service, it could answer with an “Unrecognized Service” message.

Table 4.11: List of Properties

Opening Tag:		
Number: 1	0001	....
Class: Context Specific Tag	....	1...
Length: 1	....	.001
Property Identifier:		
e.g. Status	0111	0000
Opening Tag:		
Number: 3	0011	....
Class: Context Specific Tag	....	1...
Type: Opening Tag	....	.110
Application Tag:		
Number: Enumerated	1001	....
Class: Application Tag	....	0...
Length: 1	....	.001
Property:		
e.g. Operational	1001	0001
Closing Tag:		
Number: 3	0011	....
Class: Context Specific Tag	....	1...
Type: Closing Tag	....	.111

Table 4.12: BACnet/IP Complex Acknowledgement Packet Structure

Complex ACK Packet		
BVLC	Type	0x81
	Function	0x0a
	VLC Length	
NPDU	Version	0x01
	Control	0x04
APDU	APDU Type	0x30
	Invoke ID	0x68
	Service Choice	0x0c
	Context Tag 0	0x0c
	Object Type+Instance	?
	Context Tag 1	0x19
	Property Instance	0x4b

Chapter 5

Test Scans

This chapter describes all test scans, which were performed to determine the best payload for a following large scale scan of the whole announced IPv4 range.

Test scans were scheduled to answer the following questions:

- Is it possible to use “ReadProperty” and “ReadPropertyMultiple” packets to scan for BACnet devices?
- How many response packets are valid and contain information which can be used for the evaluation?
- Which properties would prove to be most useful to answer the scientific questions of this thesis?
- Is there a difference in the number of detected devices depending on the questioned property?
- Does the number of detected devices decrease if a “ReadMultipleProperty” packet is used instead of “ReadProperty” packet?

5.1 Setup

Originally the test scans were intended to encompass only the “Münchner Wissenschaftsnetz” (MWN), but a first scan did not detect a single device. Therefore the test group had to be specified in a different way. Scans are regularly scheduled to feed Censys with current data and the results are published on Scans.io [29]. One of these scans is done with the BACnet module of ZMAP. The latest available results when the test scan was done were the results of the July 1, 2016. To create a meaningful test group, 1000 candidates were randomly selected out of the answering IPs.
All scans were performed with a modified ZMAP module at a rate of 1000 packets per

second via the server introduced in chapter 3.
The first observations focused on the "ReadProperty" packet. Due to the fact, that this service is required to be implemented by every BACnet device [49] it seemed to be the most promising payload in order to reach the maximum number of Internet connected BACnet devices.
ZMAP [33] offers a BACnet module which is based on a "ReadProperty" packet. This module was modified to meet the requirement requesting different properties and comparing the results.
The property selection was done following two considerations: First, how many BACnet devices would really respond to the request and secondly what is the information gain of the requested property. Which of them would be the most useful to answer the scientific questions. The properties listed in table 5.1 were tested.

Property	ID
Local Date	`0x38`
Local Time	`0x39`
Location	`0x3a`
Model Name	`0x46`
Object Name	`0x4d`
Object Type	`0x4f`
System Status	`0x70`
Vendor Identifier	`0x78`
Vendor Name	`0x79`

Table 5.1: BACnet/IP Property IDs

The properties Local Date and Local Time should enable the identification of the time zone where the device is operating, Location should help to cluster the detected devices geographically and the other properties should help to identify the device type. The comparison between different properties according to answering rate and possible information content was done via 9 scans. Two properties turned out to be of no further interest, due to the contained information:

- System Status:
  All answering devices delivered the status operational, value 0.
- Object Type:
  All answers presented the Object Type device (value 8), as only this object type was specified in the request packet.

For comparison reasons, another test was scheduled with the original ZMAP module, which uses the property Object ID. The code for the Object Identifier is 0x75 [53]. Also this property does not deliver additional information, because the ID is part of every answer of a BACnet device. This scan served the following two purposes: On the one hand, to eliminate the risk of a decision based on the assumption that 100 % of the

testing candidates would still be present when the test scans are scheduled. On the other hand, to facilitate a justified decision for one or another property.
The packet for the third test run was a ReadPropertyMultiple packet with a combination of the remaining properties:

- Local Time
- Local Date
- Location
- Model Name
- Object Name
- Vendor Identifier
- Vendor Name

5.1.1 Evaluation

It turned out, that all of the packets could be used as a potential payload for a scan for BACnet devices. Every test resulted in an answering rate higher than 89 %. Therefore it was necessary to categorize the different packets, for a further evaluation of the validity and the information content of the response. A filter mechanism was developed to determine validity, type and information content of a packet. The categorization was based on the expectation of a correct ComplexACK answering packet. Therefore all packets were filtered in the following way:

1. BVLC Type is BACnet/IP (that is part of the standard ZMAP module)
2. BVLC Function is Original-Unicast-NPDU
3. NPDU Version is 1
4. NPDU Control shows no expectation for an answer
5. APDU Type is ComplexACK
6. APDU Service Choice is readPropertyMultiple

This filter mechanism offered the results visible in table 5.2. Thereby the column Hit Rate shows the percentage of answers based on the 1000 candidates selected in section 5.1. The existing ZMAP module is displayed separately and the other scanning modules are ordered according to their hit rate. The column Valid Answers shows how many candidates out of these 1000 delivered packets which met the expectations raised in the filtering mechanism. It is significant that the hit rate and the time flow seem to be congruent. The scans which have been performed on the 7th of July 2016 received responses of more than 91 % of the devices, scans which were performed on the July, 16

Table 5.2: Test Scans: Comparison of Results

Scanning Time	Scanning Module	Answers	Valid Answers
07-07-2016 09:58	ZMAP Module	91.7 %	73.6 %
07-07-2016 17:47	Vendor Name	92.0 %	73.6 %
07-07-2016 18:17	System Status	91.7 %	73.4 %
07-07-2016 18:14	Local Time	91.5 %	71.3 %
07-07-2016 18:16	Local Date	91.5 %	71.1 %
07-07-2016 18:33	Model Name	91.5 %	73.3 %
07-07-2016 18:12	Vendor ID	91.2 %	73.2 %
16-07-2016 09:24	Location	89.8 %	60.2 %
16-07-2016 09:27	Object Name	89.5 %	71.6 %
16-07-2016 09:29	Object Type	89.5 %	71.6 %
16-07-2016 09:32	Multiple Property	89.1 %	71.3 %

only received rates up to 90 %. One reason for that could be IP churn. Another possible reason was discovered after the scanning process. The project which investigated the effectiveness of vulnerability notifications [27] took place shortly before the test scans were scheduled. In this project multiple parties were notified about vulnerabilities in their systems, the addressed parties in the building automation sector had been selected via a ZMAP scan for BACnet usage. A decreasing number of detectable BACnet devices over time could also be explained as a consequence of successful notification mechanisms.

It turned out, that the “ReadPropertyMultiple” packet delivered a volume of information via only one scan. The difference in the amount of answers was less than 3 % and the explanation with the time congruency seemed more than likely. Therefore we decided to use the “ReadPropertyMultiple” for the large scale scan followed by a “ReadProperty” scan for a single property, to enforce the theory that the decreasing hit rate was time congruent. The property in use was Vendor Name, which had the highest hit rate.

Chapter 6

Large Scale Scans

This chapter describes the scans which where done on the whole announced IPv4 range and presents the results as well as the evaluation.

6.1 Scan Structure and Results

To discover publicly accessible BACnet devices, a large scale scan was scheduled to cover the whole announced IPv4 range, except IPs which were part of a given blacklist, which is part of the appendix A.1. Therefore the scan targeted 2 814 698 553 IPs. The scanning rate was 25 000 packets per second and the cooldown time amounted to 10 minutes. Chapter 5 describes the outcome of the comparison of all performed test scans. One conflict between two selection criteria remains: It is either possible to select the packet with the highest hit rate or the packet with the highest information content. One observation in the test scans was that the hit rate is decreasing while time moves on. This observation seems to be valid and independent from the packet selection. To enforce this assumption the large scale scan focuses on two payloads: The ReadPropertyMultiple packet to request all properties which proved to be useful in chapter 5 and the ReadProperty packet which requests the vendor name and showed the highest hitrate in the testscans.

6.2 Results and Evaluation

The result of the large scale scan is also part of a research carrying the title ”Öffentlich erreichbare Gebäudeautomatisierung: Amplification-Anfälligkeit von BACnet und Deployment-Analyse im Internet und DFN“ [34] in cooperation with the advisors. The tool for the evaluation was written by Oliver Gasser in this context. The filtering is done in the following way:

1. BVLC Type is BACnet/IP
2. BVLC Function is Original-Unicast-NPDU
3. NPDU Version is 1
4. NPDU Control: reserved bits are untouched
5. BACnet Address Layer: source and destination MAC Address are correct
6. APDU Type is ComplexACK
7. APDU Service Choice is ReadProperty/ReadPropertyMultiple

BACnet is an open protocol standard. Due to the fact, that the use cases are variegated and the number of vendors of BACnet capable devices is increasing, BACnet International offers the "BACnet Testing Laboratories" for detailed testing and conformance certification for devices to verify protocol compliance [59].
This scan and the according evaluation are based on the BACnet Standard [32] in the first place, but the range of accepted answers was expanded, due to the fact that some devices were not fully compliant to the standard. One example was the bit which specifies that a packet expects an answer. According to the standard this bit in the Control Byte should have been 0, but some devices sent answers which contained correct values for the properties, but set this bit to 1. To be capable of diagnosing these packets anyway, rule 4 was modified.
Please see ”Öffentlich erreichbare Gebäudeautomatisierung: Amplification-Anfälligkeit von BACnet und Deployment-Analyse im Internet und DFN“ [34] for a detailed description of the filter mechanism and the categorization of the dropped packets. After filtering the packets, a comparison of the two payloads provides the results visible in table 6.1.

Table 6.1: Large Scale Scans: Comparison of Results

Scanning Time (UTC)	Scanning Module	Answers	Valid Answers
10-08-2016 10:12	ReadPropertyMultiple	17 765	13 596
11-08-2016 17:46	ReadProperty (Vendor Name)	17 647	13 603

This evaluation enforces the assumption that there is a correlation between the time, when a scan was initiated, and its efficiency. The “ReadPropertyMultiple” scan was scheduled first and produced 118 responses more than the “ReadProperty” packet, which was initiated afterwards. Due to the fact, that the difference in the number of detected devices sending valid answers does only amount to 7 and the ReadPropertyMultiple packet delivers a multiple of information, the evaluation focuses on the ReadPropertyMultiple packet.

6.2.1 Vendor Shares

Some controls companies look back on a long history with the BACnet protocol and influenced the protocol [41]. 12 209 answering packets included a valid vendor identification (vendor id). The evaluation based on the 901 vendor IDs which have been issued by ASHRAE [60] shows a distribution visible in table 6.2:

Table 6.2: Top 10 vendors according to Vendor ID

Position	Vendor ID	Vendor Name	Count	Percentage
1	35	Reliable Controls Corporation	2188	17.92 %
2	36	Tridium Inc.	1835	15.03 %
3	8	Delta Controls	1473	12.06 %
4	5	Johnson Controls, Inc (JCI)	1394	11.42 %
5	24	Automated Logic Corporation	1065	8.72 %
6	7	Siemens Schweiz AG	648	5.31 %
7	2	The Trane Company	595	4.87 %
8	16	United Technologies Carrier	412	3.37 %
9	80	Fr. Sauter AG	255	2.09 %
10	17	Honeywell Inc	206	1.69 %

6.2.1.1 Introduction of the Top 5 Vendors

The Top 5 vendors sell 65.15 % of the devices. The vendor overview in brief:

Reliable Controls Corporation:
The Reliable Controls Corporation is newer to the BACnet standard than most of the other vendors. Although the company was founded in 1986, they started to develop their BACnet product line in 2001 [41]. In 2016 Reliable Controls advertises “Internet-Connected Building Controls” on their website [61] and sells only BACnet devices.

Tridium Inc.:
The whole company is built around the Niagara Framework. It enables the interconnection of several Industrial Control System technologies. In 2012 a research of the Washington Post revealed that at least 11 million devices and machines in 52 countries are linked via Niagara and vulnerable to attacks [62]. Billy Rios reported vulnerabilities in the Niagara Framework: Unauthenticated users can retrieve the device passwords and readable passwords can be used to gain administrative access to the device [63]. He reported the issue to ICS-CERT and security patches were provided by Tridium. [64]. The break-in into the building management system of Google Australia by Billy Rios and

Terry McCorkle was possible because the Tridium Niagara AX system in this building had not been patched up, also the fix was already available [65]. Tridum is part of Honeywell, which was vehemently opposed to BACnet at the beginning in the early nineties, but now has a BACnet product line [41].

Delta Controls:
Delta Controls started its support for the BACnet protocol in 1993 [41]. This company provides building automation solutions for heating, ventilation, lighting control and access control and claims to have more than 100 000 BACnet devices in more than 80 countries [66]. The further analysis of the device locations in section 6.2.3.2 shows, that the detected BACnet components can be found in exactly 80 countries.

Johnson Controls, Inc (JCI):
Newman [41] explains the history of BACnet and this company as follows: "Johnson Controls sent representative to the BACnet comittee from the start, in 1993 they were the first vendor which had an actual BACnet software. When BACnet was published in 1995 Johnson Controls decided to give the customers the opportunity to have any protocol implemented in their product." Therefore this company is not exclusively focussed on BACnet devices. Metasys Systems are classical building control systems and have been issued multiple times with vulnerability reports. Billy Rios revealed that it is possible to compromise these systems, because the security of authentication processes is not granted, which results in Web Services being available to unauthenticated users [63]. He reported the issues to ICS-CERT and achieved that Johnson Controls provided a patch for the issue [67].

Automated Logic Corporation:
The Automated Logic Corporation started in 1995 to adopt BACnet in all their new products [41]. According to the information on the website [68] the Automated Logic Corporation is part of United Technologies.

6.2.1.2 Comparison to Statistics

The automation magazine Control Global [1] published an order of the leading automation vendors, based on their revenue. The Top 10 are presented in table 6.3.

A comparison with the evaluation the vendor distribution based on the Vendor ID, shows some differences. Honeywell does not even appear in the Top 10 vendors according to the id although it is ranked on position nine by Control Global. This indicates that an evaluation which is based on the Vendor ID only does have some inaccuracies. Honeywell is one example, but this is also the case for more other conglomerates and happens for example as a result of a merger between two companies. While both companies were separated, both applied for a Vendor ID and after the merger both might still use the old Vendor IDs. One example is Tridium. Although it is part of

Table 6.3: Top 10 automation vendors by revenue of their automation segment [1]

Position	Vendor Name	Sales in Billion US$
1	Siemens	13.4
2	ABB	11.17
3	Emerson	9.54
4	Schneider Electric	7.51
5	Rockwell Automation	6.3
6	GE	3.84
7	Mitsubishi Electric	3.81
8	Danaher	3.53
9	Honeywell	3.49
10	Yokogawa Electric	3.27

Honeywell International since 2005 [62], the vendor ID in use is still 36, representing Tridium Inc. Another example is the Automated Logic Corporation, also the company is part of the United Technologies Corporation [68] the devices still have the vendor id 24. The consideration that some companies are subsidiaries of others presents a slightly different distribution. Tridium, Novar [69] and Alerton [70] are parts of Honeywell. United Technologies Corporation is owning the subsidiaries Carrier and Automated Logic Corporation. Setting this into account, 71.95 % of the devices are produced by 5 conglomerates as visible in table 6.4.

Table 6.4: Top 5 conglomerates by number of devices

Position	Vendor Name	Count	Percentage
1	Honeywell (Tridium, Alerton, Novar...)	2375	19.45 %
2	Reliable Controls Corporation	2188	17.92 %
3	United Technologies (Automated Logic, Carrier...)	1477	12.10 %
4	Delta Controls	1385	12.06 %
5	Johnson Controls Inc.	1063	11.42 %

The differences between the vendor distribution done via the evaluation of the scanning results in table 6.4 and the distribution according to Control Global in table 6.3 could have multiple reasons. The three companies with the highest revenue in their automation segment, Siemens, ABB and Emerson do not appear in the Top Five of the scanning results. One explanation could be that the automation sector in most companies does not only include components for building automation, but also solutions for other automation processes. Part of the Siemens automation segment are also CNC automation systems or motion control systems [71]. Another reason might be the structure of the building automation systems.

6.2.2 Device Types

An analysis of the device types in use offers an idea about typical building automation systems which have responded to the scan. BACnet International, which offers conformance certification for devices [59], differentiates between eight device types. Those are according to Newman [72]:

- BACnet Operator Workstation (B-OWS)
- BACnet Advanced Operator Workstation (B-AWS)
- BACnet Operator Display (B-OD)
- BACnet Building Controller (B-BC)
- BACnet Advance Application Controller (B-AAC)
- BACnet Application Specific Controller (B-ASC)
- BACnet Smart Actuator (B-SA)
- BACnet Smart Sensor (B-SS)

Part of the requested properties in the ReadPropertyMultiple scan, do help to identify device types. The combination of vendor name, vendor ID and model name give a first impression about the identification of the devices.
The top ten of the devices according to the model name, make up 42 % of the market and are visible in table 6.5

Table 6.5: Top 10 devices according to Model Name

Position	Model Name	Vendor Name	Count	Percentage
1	NiagaraAX Station	Tridium	1774	13.1 %
2	MACH-ProWebSys	Reliable Controls Corp.	641	4.7 %
3	Tracer SC	Trane	595	4.4 %
4	MACH-ProWebCom	Reliable Controls Corp.	565	4.2 %
5	MACH-ProCom	Reliable Controls Corp.	449	3.3 %
6	LGR25	Automated Logic Corp.	443	3.3 %
7	MACH-ProSys	Reliable Controls Corp.	422	3.1 %
8	DSM_RTR	Delta Controls	369	2.7 %
9	DSC_1616E	Delta Controls	243	1.8 %
10	EY-AS525F001	Fr. Sauter AG	209	1.5 %

6.2.2.1 Introduction of the most common Devices

The following overview categorizes the devices which have been detected most frequently. In most cases the evaluation of the properties Vendor Name/ID and Model

Name, which were part of the response packets, were sufficient to identify device types. The identification was done via the analysis of the informations about producer and model and a lookup in publicly available product data sheets.

NiagaraAX Station:
Niagara AX is a framework which enables to control and interconnect devices of different vendors. It is the predecessor of Niagara 4 and allows to connect attached devices, to model them in software and to use a programming application to monitor and control the informations in those devices [73]. According to the user guide a Niagara AX station is "the main unit of server processing".

MACH-ProWebSys:
The MACH-ProWebSys is a combination of three devices, a BACnet Building Controller (B-BC), a BACnet Operator Workstation (B-OWS) and a web server [74]. It also has the capability to control 12 modules and produce 8 output signals.

Tracer SC:
The Tracer SC is a building automation system which can be used to control HVAC systems, lighting and other systems via a web interface [75]. The model name Tracer SC doesn't provide a detailed information about the specific type of the device, but only that it is a part of the Tracer SC. Therefore it is necessary to take a closer look at another property which was requested via the scan: the object name.

MACH-ProWebCom:
Another Reliable Controls product is MACH-ProWebCom. It is the smaller model of the MACH-ProWebSys and also unites the function of Building Controller (B-BC), a BACnet Operator Workstation (B-OWS) and a web server [76], but can only control 8 modules.

MACH-ProCom:
The MACH-ProCom is also distributed via Reliable Controls and is a Building Controller(B-BC) [77].

LGR25:
LGR is a product line of routers by the Automated Logic Corporation having the specification BACnet Advanced Application Controller (B-AAC) [78].

MACH-ProSys:
The MACH-ProSys is a Building Controller(B-BC) and the larger variant of the MACH-ProCom, another product by Reliable Controls [79].

DSM_RTR:
The model name DSM_RTR represents a Building Controller (B-BC) of Delta Controls, which is designed for routing applications such as connecting a BACnet site to the Internet or connect Ethernet Networks to gain a Wide Area Network (WAN) [80].

DSC_1616E:
The DSC_1616E is another component produced from Delta Controls and can be identified via the combination of model name and vendor identification directly. Due to its data sheet [81] it is a BACnet Building Controller (B-BC) which is capable of controlling Boilers, Chillers and a variety of HVAC control systems.

EY-AS525F001:
Sauter produces the EY-AS525F001, which is based on the device identification a BACnet Building Controller (B-BC). The data sheet describes the device as a modular automation station (AS) which can be used to regulate, control and monitor operational systems such as HVAC systems [82].

It turns out, that is in most cases possible to identify the specific type of a device via Vendor and Model Name, which are present in the response packet. Anyway, it is necessary to take into account, that an analysis of the Model Name does not build a specific representation of the device types which are accessible. Some names such as the EY-AS525F001 create a precise picture of the connected BACnet device, whereas others such as the Trane Tracer SC only allow to diagnose that the addressed device is part of a Tracer SC automation system. Also the value count which should provide a detailed picture of the world wide device distribution, does not take into account that numbers of concrete, determinable devices are compared with numbers of components of a building automation systems, which can not be identified precisely.

6.2.3 Clustering

This section takes a closer look at the structure how BACnet devices are organized. The purpose is to find out whether any kind of clustering becomes visible.

6.2.3.1 Subnets and Autonomous Systems

All destination IPs have been mapped to their subnet and their AS membership via the Prefix to AS mappings of CAIDA [35]. All detected devices are distributed between 4630 subnets. Figure 6.1 relates the number of the devices per prefix to the number of prefixes. It visualizes the cummulative distribution of the prefixes and shows a clustering, because most of the devices can be found less than 2000 prefixes.

Gasser et al. [34] clustered the BACnet devices with regard to the Autonomous System affiliation. They discovered that devices are located in 1367 ASes. AS 7018 by AT&T Services is the AS with the most BACnet devices. 1291 devices are present in this AS. Figure 6.2 visualizes the cumulative distribution of devices in combination with the number of ASes. A clustering is visible for 200 ASes, where 80 % of the BACnet devices can be found.

Figure 6.1: Number of devices per prefix

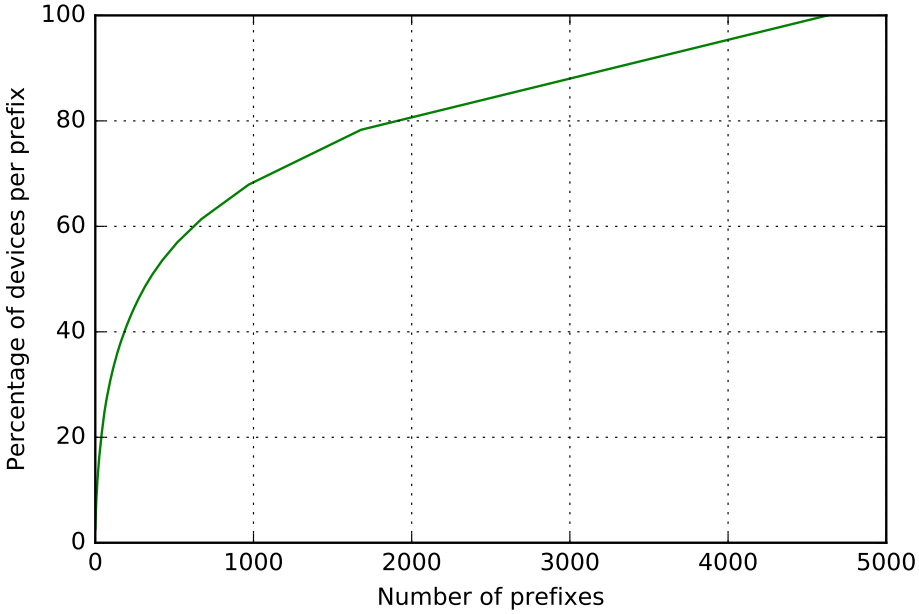
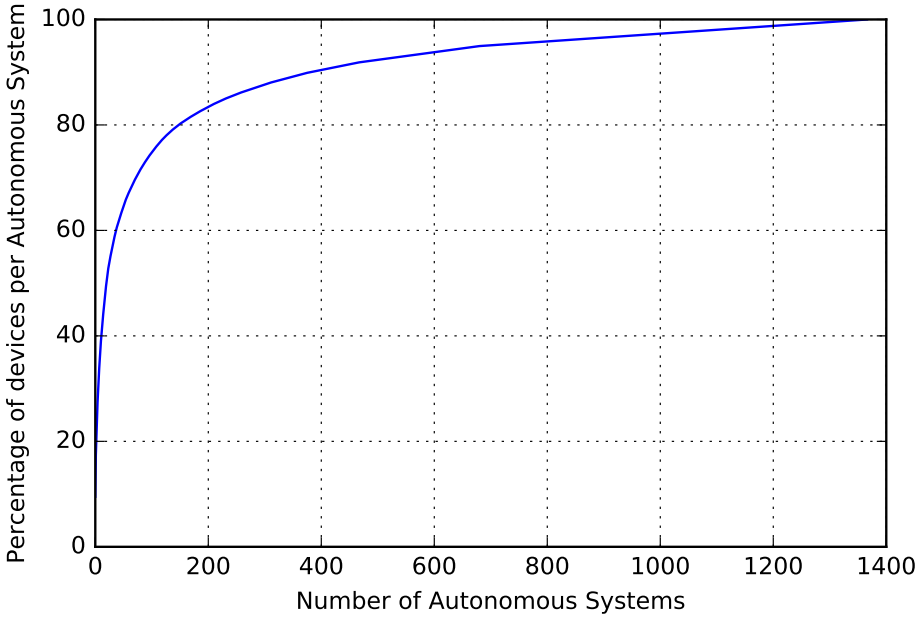


Figure 6.2: Number of devices in ASes



In 2011 Leverett [2] provided a list of the Top Ten Autonomous Systems with the most Industrial Control Systems. Although he discovered only 7489 devices in total, a trend according to AS clustering is visible in his results, which are presented in table 6.6.

Table 6.6: Top 10 Autonomous Systems hosting ICS according to Leverett [2]

Pos.	ASN	Organisation	ISO	Count	Percentage
1	22 394	Cellco Partnership DBA Verizon Wireless	US	405	5.41 %
2	7132	AT&T Services	US	360	4.81 %
3	1134	KPN Mobile Network Operator	NL	220	2.94 %
4	8786	Telenor Norge AS	NO	195	2.60 %
5	3292	TDC Data Networks	FI	188	2.51 %
6	7018	AT&T Services, Inc.	US	156	2.08 %
7	19 262	Verizon Online LLC	US	138	1.84 %
8	209	Quest Communications	US	129	1.72 %
9	3301	TeliaNet Sweden	SE	121	1.62 %
10	6389	BellSouth.net Inc.	US	100	1.34 %

Leverett states that 26.87 % of all Industrial Control Systems can be found in 10 ASes. This thesis is giving evidence, that building automation systems are even less distributed between Autonomous Systems. 37.53 % of all detected BACnet devices were found in 10 ASes, as presented in table 6.7. The AS data and the according descriptions were collected via a lookup in the CAIDA AS Rank Database [83]. The comparison of both statistics shows, that the ASes 209, 7132 and 22 394 are present in both statistics.

Table 6.7: Top 10 Autonomous Systems hosting BACnet devices

Pos.	ASN	Organisation	ISO	Count	Percentage
1	7018	AT&T Services, Inc.	US	1291	9.50 %
2	7922	Comcast Cable Communications, LLC	US	1082	7.96 %
3	22394	Cellco Partnership DBA Verizon Wireless	US	522	3.84 %
4	852	Telus Communications	CA	486	3.57 %
5	6327	Shaw Communications	CA	348	2.56 %
6	577	Bell Canada	CA	333	2.45 %
7	209	Quest Communications	US	285	2.10 %
8	701	MCI Communications	US	270	1.99 %
9	5650	Fronteir/Verizon	US	266	1.96 %
10	20115	Charter Communications	US	219	1.61%

A look to the ten ASes which harbour the most devices also reveals a geographical trend. While Leverett's results are showing, that most devices are located in 5 Autonomous Systems in the USA and the others seem to be located in Scandinavia and the Netherlands, the building automation systems are distributed between Canada and the United States of America. Our analysis gives evidence that AT&T Services, Comcast Cable

Communications, Cellco Partnership DBA Verizon Wireless, Qwest Communications, MCI Communications, Fronteir/Verizon and Charter Communications harbour 21.3 % of all detected devices. All organisations are located in the USA.
Telus Communications, Shaw Communications and Bell Canada are registered in Canada and have a share of 8.58 % of the devices.

6.2.3.2 Geographic Location

2015 Durumeric et al. [3] presented an analysis of Industrial Control Systems which used the Modbus Protocol and were connected to the internet. Part of the evaluation was an analysis of 10 countries which harboured the largest amount of Modbus devices. The results of this research are presented in table 6.8. 67 % of all Modbus capable devices were located in the top 10 countries. The fact, that Europe is presented as one country is fogging, because countries like Spain, France, Denmark and Sweden are part of Europe.

Table 6.8: Top 10 countries with Modbus devices according to Durumeric et al. [3]

Position	Country	Count	Percentage
1	United States	4723	24.70%
2	Spain	2513	7.58%
3	Italy	1220	6.39%
4	France	1149	6.03%
5	Turkey	884	4.63%
6	Canada	822	4.30%
7	Denmark	732	3.83%
8	Taiwan	682	3.57%
9	Europe	615	3.22%
10	Sweden	567	2.97%

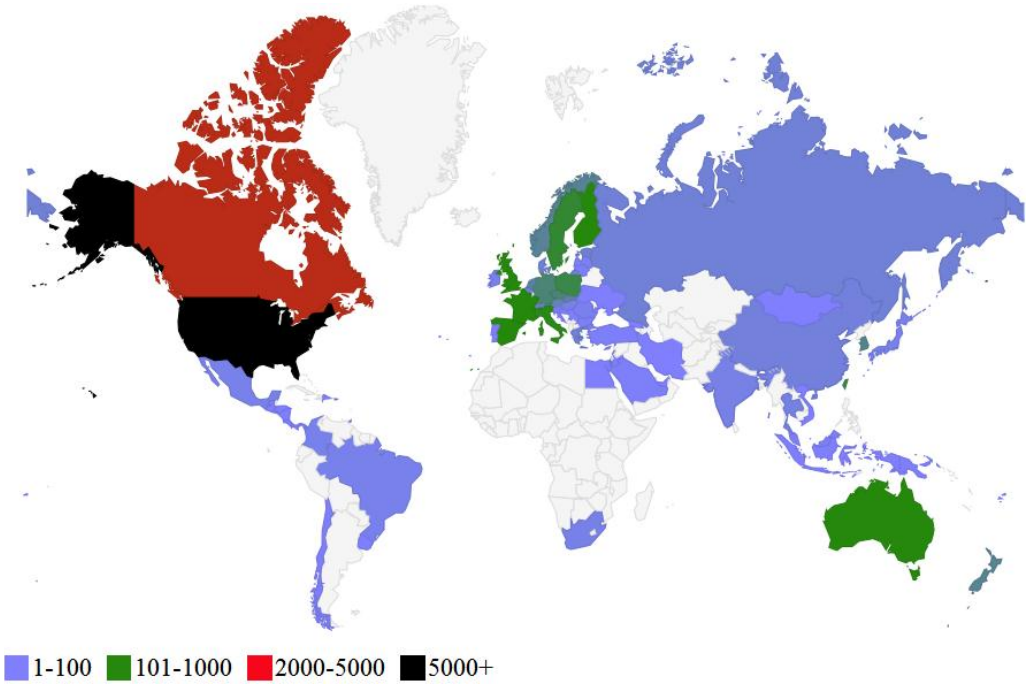
Our work is presenting the results for each member of the European Community separately. The tool IP2Location [20] was used to determine the geographic location of a device. It matches a given IP address to a country code. We found out that 10 countries do harbour 92.28 % of the devices, as visible in table 6.9.

A comparison between both statistics is showing, that the United States harbour the biggest quantity of devices. A quarter of the Modbus devices and more than 60 % of the BACnet devices are located there. While building automation systems seem to be concentrated mostly in North America, Europe and Australia, Industrial Control Systems are also spread out in countries such as Taiwan and Turkey. BACnet devices are present in 80 countries. With a representation of 92.28 % of the devices in 10 countries, the remaining 7.72 % are spread out between 70 countries. Figure 6.3 shows, how BACnet is distributed in Europe, Australia and North. The distribution in Russia, Africa and South America is minor in relation to the country size.

Table 6.9: Top 10 countries hosting BACnet devices

Position	Country	Count	Percentage
1	United States	8458	62.22%
2	Canada	2513	18.48%
3	France	324	2.38%
4	Spain	295	2.17%
5	Australia	249	1.83%
6	Finland	213	1.57%
7	Great Britain	149	1.10%
8	Italy	128	0.94%
9	Sweden	114	0.84%
10	Poland	102	0.75%

Figure 6.3: Geographic location based on IP2Location



The ReadPropertyMultiple packet also included a request for the property Location. The idea was to determine the device location versus an analysis of the response values of this property. The evaluation showed that 5855 delivered an empty location value, 1834 responded “unknown” and 1480 packets delivered “Device Location”. The other values did not indicate any form of clustering. Therefore we assume that “unknown”

and “Device Location” are default values and Location is a free text field and not capable of providing a precise information for device clustering on a geographical level.

The third approach to determine the geographical location of the devices was to capitalize time zones. The properties Local Date and Local Time were also part of the scanning results. Packets which didn't deliver any values for these properties had to be separated. Afterwards the answers which included non parseable values were dismissed.
26 packets which could not be parsed correctly according to the property Local Time seemed to be special. A closer look at the AS which harbours the relevant IPs revealed that all the packets do have their origin in Taiwan: i.e. two universities and one provider. One of the universities is the National Tsing Hua University (NTHU). An online lookup shows that Delta Electronics is proud to have a energy optimizied building at this university [84]. None of the responding packets which were originated in the university AS, had a Vendor ID or Vendor Name which indicated that the producer was Delta Electronics. All devices claimed that their vendor is BroadWin Technology Inc and that they are WebAccess BACnet Server. ICS CERT reports that the WebAccess components had multiple vulnerabilities which have been adressed in a newer version by Advantech, a company in Taiwan which took over the BroadWin Technology components [85]. At the Hitcon 2015 in Taiwan the threat researchers Miaoski and Hilt reported, that they were capable of accessing the web interface of one of the WebAccess components of one of the universities [86]. 11 729 devices delivered parseable values for local date and local time.
The analysis of the properties Local Date and Local Time showed, that another 24 devices reported the very same value, exactly 12 o'clock at the 31th of August 2005. A deeper inspection of the packets showed that all of the answers carry the same properties for Vendor and Model Name. This feeds the suspicion that KMC Controls delivered their TC-BAC components with this timestamp as a default value.
5 devices delivered the timestamp 12 o'clock at the 8th of January 2015. All are Insight components by Siemens Building Technologies, so this is likely to be seen as another predefined default value.
The next step was to sanitize the timestamps according to their sensibility in context with the 24 time zones. Therefore the arrival timestamp of the UDP packet was compared to Local Date and Local Time which were contained in the packet. All values have been rounded related to the hour. After the omission of all packets with a time delta less than -12 hours or more than +14 hours 11 202 packets remained. The analysis showed that 285 devices provided UTC timestamps, but the majority is not operated in the UTC timezone according to the country code provided by IP2Location. 139 devices carried the Vendor Name Triacta Power Technologies, Inc. Suggesting the IP2Location mapping is correct, only 14 Triacta devices delivered a time difference which fitted the detected timezone. Therefore we are seeing it likely, that the vendor delivers devices which are synchronized with UTC. The testing report by the BACnet Testing Laboratories [87] confirms that the detected components Powerhawk 4224, 4324, 6303 and 6312 are ca-

pable of a UTC time synchronisation. All detected 106 Powerhawk 6312-120V-2P-24 provided UTC timestamps and are localized in the same AS: 3651, the SPRINT-BB6 AS. This could mean that they are operated by the same admin, who defined UTC time synchronization as a default property.
All detected time differences have been put in relation to the calculated location. The IP2Location mapping which was done in the first place, delivers country codes for each detected IP address. The possible GMT offsets were afterwards specified for each country via a database lookup in the Timezone DB [36]. Table 6.10 visualizes the IP2Location mapping in column "Country" and provides the number of devices with valid timestamps and the percentage of those delivering a time difference which matched the local timezone, detected via IP2Location.

Table 6.10: Timezones for devices in top ten countries

Country	Devices with valid timestamps	Percentage with local timezone
United States	6887	94.45%
Canada	2097	96.47%
France	310	88.71%
Spain	281	95.73%
Australia	205	99.02%
Finland	183	87.98%
Great Britain	129	91.47%
Italy	107	97.20%
Sweden	103	91.26%
Poland	82	91.46%

More than 87 % of the devices are indicating a local time which matched to the detected timezone. Due to the fact that most processes in building automation such as heating, ventilation and lighting are dependent on the run of the day, it is more than likely, that administrators will set the devices to local time. This indicates that the IP2Location mapping is correct.

6.2.3.3 Reverse DNS Lookup

For the sake of additional analysis of clustering, a reverse DNS lookup of the answering IPs was performed. The tool massDNS [37] detected 9585 valid DNS entries. An analysis with the Preprocessing Script by Patrick Sattler [38] shows that 68.5 % of the detected Domain Names are distributed between 10 Domain Labels, as visible in table 6.11.

Obviously the labels belong to communication providers. This suggests that the devices are not operated by companies which are having their own label, but by end customers. The fact, that in 5999 cases the IP is encoded in the Domain Name is supporting this

Table 6.11: Top 10 domain label

Position	Domain Label	Count	Percentage
1	static	1200	12.39%
2	comcastbusiness	948	9.79%
3	hfc	946	9.77%
4	sbcglobal	943	9.74%
5	rr	674	6.96%
6	biz	654	6.66 %
7	lightspeed	547	5.65%
8	telus	269	2.78%
9	bell	234	2.42%
10	verizon	229	2.36%

assumption. This extract should be used for the selection of a vulnerability notification form.

6.2.4 Network Infrastructure Analysis via Traceroutes

To analyze the network infrastructure of the detected devices, traceroutes have been performed with the tool Scamper [39]. It is significant that the addressed host only replied in 5755 cases. The largest number of hops with a resulting destination reply was 31, but in this case 4 hops did not reply, the shortest path counted 5 hops. The complete path to the addressed devices only became transparent in 1797 cases, in every other path at least one hop provided no response.

To determine the infrastructure in which the building automation systems were present, we analyzed in which Autonomous System the destination and the prevenient hops were found. Therefore the IP addresses which were included in the traceroutes, have been matched to ASes via the Prefix to AS mappings of CAIDA [35].

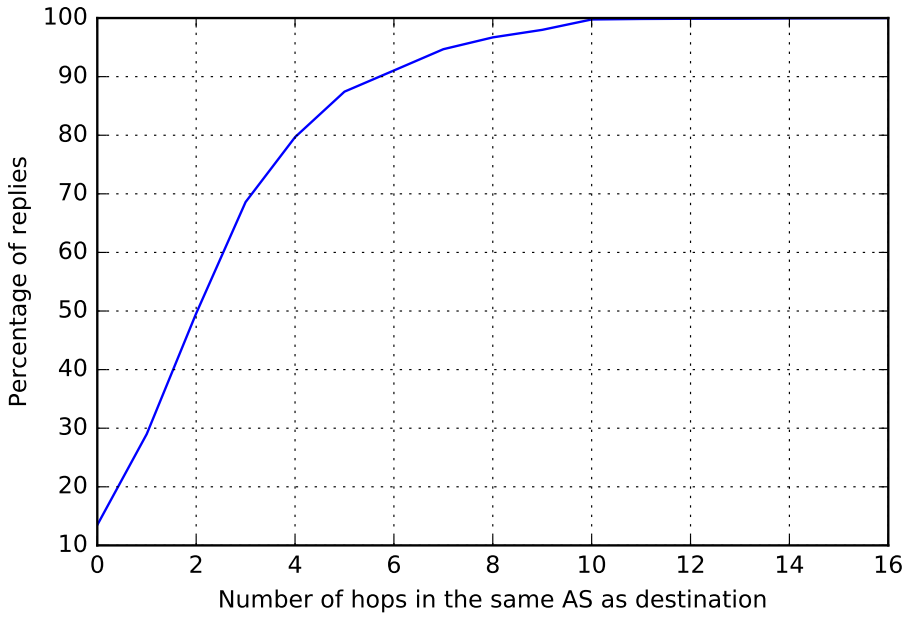
A look at the Autonomous System membership of the different hops showed, that only 13.48 % of the detected building automation systems were reachable directly without access of another hop in their AS. In all other cases at least one other hop was a member of the same Autonomous System as the destination IP of the device. Table 6.12 shows the relation between the number of devices and the number of hops which were in the same Autonomous System as the destination IP of the device. In one case 17 hops led to the same Autonomous System as the destination IP.

Figure 6.4 visualizes the cumulative distribution of devices related to their number of hops which had been in the same AS as the destination IP address. It shows, that the percentage of the devices does not decrease with the number of hops, but that it increases until it is having the maximum at 2 Hops within the same AS as the destination.

Table 6.12: Number of hops in destination AS

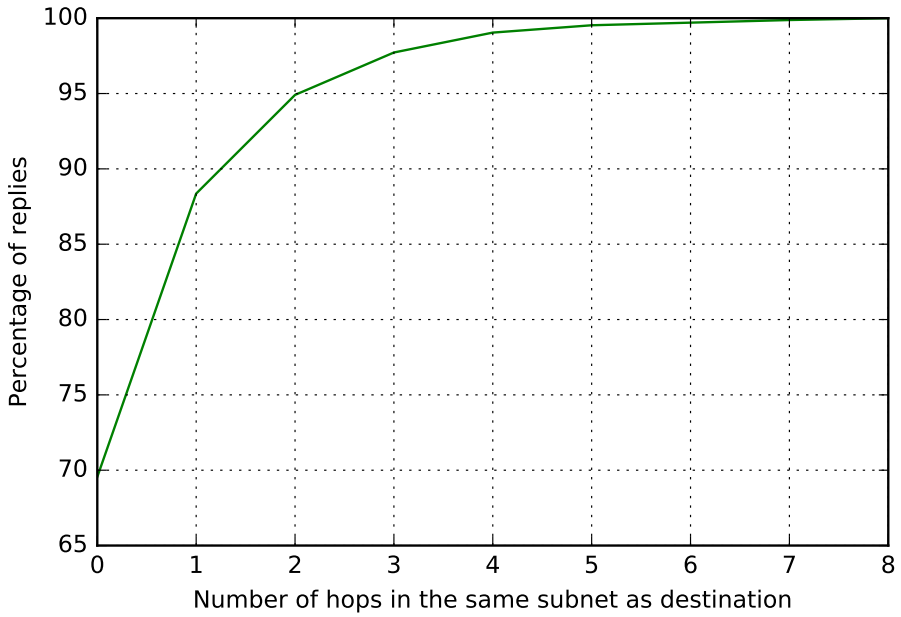
Pos.	Number of Hops in Destination AS	Count of Devices	Percentage of Devices
1	2	1185	20.59 %
2	3	1094	19.01 %
3	1	893	15.52 %
4	0	776	13.48 %
5	4	637	11.07 %
6	5	447	7.77 %
7	7	209	3.63 %
8	6	208	3.61 %
9	8	116	2.02 %
10	10	102	1.77 %
11	9	74	1.29 %
12	11	5	0.09 %
13	15	3	0.05 %
14	12	2	0.03 %
15	16	2	0.03 %
16	14	1	0.02 %
17	17	1	0.02 %

Figure 6.4: Number of hops in destination AS



The Prefix to AS mappings of CAIDA [35] was also in use to detect the BGP rooted subnets for every hop. Figure 6.5 visualizes the cumulative distribution of the devices in relation to the number of hops in the destination subnet. In 1752 cases at least one hop before the targeted building automation system was a member of the same subnet as the destination. This indicates that the systems received the scanning payload and responded not only to the ReadPropertyMultiple packet, but also to the traceroute, although a firewall was present. It turned out, that 4003 devices, were reachable without another hop in the same subnet. This observation indicates that those devices are not protected via a firewall, except the device was in a NAT, were the last hops would not become transparent visible. This would be detectable via an analysis of the answers of the destination IP. In case the destination IP would answer two times with different TTL values, and as conclusion a NAT is suspected.

Figure 6.5: Number of hops in destination subnet



6.2.5 Caveats

Our observations put emphasis on the impression that not everybody is unaware of the growing interest of hackers in building automation systems. We were seeing response packets, which were not complaint to the BACnet standard. A closer look at the AS in which those packets had their origin revealed that universities in other countries owned theses ASes. The scan discovered responses of two IPs which could be matched to a domain operated by CERT Analysts in Alberta [88]. The packets revealed that

two MACH-ProWebSys controller distributed by Reliable Controls replied to the "Read-PropertyMultiple" packet. Multiple organizations implemented honey pots to detect potential aggressive behaviour. The Telecooperation Group at the Technische Universität Darmstadt developed 2015 [89] a mobile ICS honey pot that supports Modbus and shall be extended to S7 and SNMP. Their intention is to provide an on-the-go security status of monitored networks. This is just one example were researchers constructed an industrial control honey pot. KORAMIS did even go one step further, they developed a simulation on protocol level combined with the infrastructure of a transport company. The project is called HoneyTrain [90].

6.3 Security Mechanisms in BACnet

Addendum g to ANSI/ASHRAE Standard 135-2004 [91] introduced and linked network security to the BACnet standard. The goal was to provide peer entity, data origin, and operator authentication, as well as data confidentiality and integrity. Fact is, that the security layer is simly optional and was not implemented by vendors [41].

Chapter 7

Comparison of Results

At present two other parties perform regular BACnet scans. The team at the University of Michigan, which supports the search engine Censys [30] with the detected data, and Rapid7 in context with the project Sonar [31]. The results of both scans are available at scans.io [29], an evaluation of the results was not done yet. This chapter compares the scanning results of this thesis against the scanning results of the following BACnet scans.

7.1 Scanning Payload

As part of Project Sonar, Rapid7 performs regular BACnet scans [31]. The tool in use is ZMAP expanded with a "ReadPropertyMultiple" packet. During the run of this thesis John Hart added a pull request for this packet to ZMAP [92], at the 10th of August 2016. The BACnet scans which were performed by the operator team of Censys are titled "47808-bacnet-device_id-full_ipv4". This suggests that they use the BACnet ZMAP probe module which only requests the device property [33], but as a further analysis of the ZGrab results shows, that the properties Firmware Revision, Model Name, Object Name, Vendor ID and Vendor Name must also be part of the request.
The performed scan during this thesis, did also use a "ReadPropertyMultiple" packet, without the properties Application Software Version, Description and Firmware Revision.
Table 7.1 compares all scanning tools according to the requested properties, thereby a tick in there symbolizes that a property was requested.

The analysis of the scans done by Sonar and Censys and the comparison to the scanning results of this research highlights some differences, visible in table 7.2. The scans are ordered according to their starting time. "All Answers" is the number of all packets, which the scan delivered. To make the results comparable, the blacklist which was in

Table 7.1: Properties Requested by Scanning Modules

Property	ZMAP	Censys	Sonar	This Thesis
Application Software Version	-	-	✓	-
Description	-	-	✓	-
Firmware Revision	-	✓	✓	-
Local Time	-	-	✓	✓
Local Date	-	-	✓	✓
Location	-	-	✓	✓
Model Name	-	✓	✓	✓
Object Name	-	✓	✓	✓
Vendor Identifier	-	✓	✓	✓
Vendor Name	-	✓	✓	✓

use for this scan has been applied on both the Sonar and the Censys results. Both scans have also been focussed to the list of announced prefixes, which limited the IPs for our scan. Therefore the column “After Adjustment” visualizes how many packets did remain after both lists have been applied. Section 7.2 and 7.3 describe how the results in the column “Valid” were calculated.

Table 7.2: Comparison of Scanning Results

Scanning Date	Scanning Module	All Answers	After Adjustment	Valid
01-08-2016	Sonar	19 397	19 376	414
10-08-2016	This Thesis	17 765	17 765	13 596
12-08-2016	Censys	16 997	16 976	10 998

7.2 Sonar

The Sonar results are published on scans.io [29]. The CSV data includes timestamps, source addresses and payload of the received packets. The payload data was filtered via the tool developed by Gasser et al. [34].
The Sonar scan delivers the highest amount of answers. After the results were reduced to the announced prefixes and IPs which were part of our blacklist were removed, 19 376 packets remained. A further analysis of the received packets shows, that most of them can not be used for an analysis. In 9753 cases APDU type was not ComplexACK, the biggest groups being 4824 answers with Error messages, 2385 Confirmed Request APDUs, asking for properties of the sender, 1898 rejected the packets with the reason “Unrecognized Service”. Therefore these packets were also dropped.
93 packets did not include the Bacnet Virtual Link Layer Type BACnet/IP and had to be removed. Another 17 answers were dropped due to the fact, that they were not unicast messages. 327 packets included an invalid NPDU version. After applying the filtering

mechanism via the script only 9514 packets remained. 8991 of these packets deliver exactly the same payload. After a typical ComplexACK header the tags for the requested properties follow, but every tag is populated with the value “910191” which represents a Property Access Error with the error class object and the code “Unknown Object”. 69 packets deliver an “Unknown Property” error for all requested properties. 28 answers include Property Access Error with the error class property and the code “Unknown Object”. 12 more deliver a Property Access Error with the error class property and the code “Other”. After the removal of all the packets which included an error, only 414 valid packets remained. This raises the assumption, that the packet, which is send by Rapid7 in the first place, is not BACnet conform.

7.3 Censys

The results which are collected to provide data for the search engine Censys are also available on scans.io [29]. In this case the received payload is not directly accessible. A list with the source IPs is published. According to this list 16 997 response packets arrived. After reducing the IPs to the announced prefixes and removing the blacklist 16 976 answers remain. Due to the fact that the payload is not published we have to rely on the ZGrab results which are available on scans.io. According to the ZGrab filter mechanism only 10 998 packets are valid.
It is significant that the total of all answers is close to the results of the scan, which was performed during this thesis, but that the number of packets which were marked invalid is much higher. Possible reasons could be, that different properties are part of the request or that filter mechanisms in use do work differently.
809 IPs have answered the Censys scan, but not our scan. A clustering according to subnet or AS is not visible. A look at the ZGrab results shows that only 369 are marked as valid.
1598 IPs which have responded to our scan, but did not answer the Censys scan. 335 are located in AS 701 which is owned by Verizon business, 173 can be found in AS 7018, operated by AT&T Services, Inc., which turned out to be the AS with the most BACnet devices in our scan. An analysis of the 1598 packets, which were only uniquely received via our scan, shows that 958 are valid.
The differences in the answering IPs may be due to the requested properties. IP churn could also be a reason. Due to the fact, that the scans to feed Censys are performed regularly and this thesis only performed two large scale scans with different payloads, blacklisting could also have influenced the outcome.

Chapter 8

IPv6

ASHRAE added the specification for IPv6 support in February 2016 [93]. Therefore BACnet/IPv6 is relatively new. Due to the fact that the standard enforces a new packet structure, it is questionable if any devices which implement BACnet/IPv6 are present in the market. Nevertheless is a scan for devices which use BACnet/IPv6 part of this theses. A brute force scan in IPv6 is due to the size of the address space impractical. The interface ID portion of the address has 64 bit and therefore even a scan of an IPv6/64 subnet would require to cover 2^{64} adresses [94]. This research took another approach. 13 596 valid answers have been received during the IPv4 scan for BACnet devices. The translation of the IPv4 source addresses to hostnames has been described in chapter 6.2.3.3. Another lookup via massDNS [37] enabled the resolution of IPv6 addresses. In total 49 addresses for a potential IPv6 scan have been discovered. In the definition of BACnet IPv6 [93] ASHRAE introduced a new BACnet Virtual Link Layer (BVLL) for IPv6. The difference to the existing layer for IPv4 is, that an Original-Unicast packet requires the knowledge of the destinations virtual address. Consequently it is not possible to simply reuse the ReadPropertyMultiple packet used for the IPv4 scan. The possibility to request the destination's virtual address is a Virtual-Address-Resolution packet. Thereby a scan has to consist of two packets:

1. Virtual-Address-Resolution (to detect the destinations virtual address)
2. ReadPropertyMultiple (including the destinations virtual address detected via packet 1)

8.1 Virtual-Address-Resolution Packet

The Virtual-Address-Resolution packet is structured as follows:
The BVLC layer is structured similar to the BACnet/IP layer with the fields type, function and length. The type BACnet/IPv6 is represented by 0x82 and the function is 0x06

for Virtual-Address-Resolution and the length field represents the length in bytes. In addition, a Source-Virtual-Address has to be specified. Clause H.7.2 on p.856 has been changed [93] and specifies the usage of a device instance as Virtual MAC (VMAC) address as follows: if a device instance is present, it will be used as VMAC address with two leading zeros. If the device does not have an instance number, a random value between 0 and 419303 shall be chosen and transmitted as VMAC address with a leading zero followed by a one. Thereby the resulting values of the generated adresses are 419303 to 8388607. The analysis of the IPv4 instance numbers in Gasser et al. [34] has shown, that the Instance ID 0x3fffff (4194303) does have the highest probability in BACnet/IP, whereas the other values seem to be apportioned. To evade an Instance ID conflict we used the random value 0x651789. The scan was scheduled with a modified ZMAP module for IPv6 which delivers a UDP packet, to the BACnet port 47808. The UDP payload in use is represented in table 8.1.

Virtual-Address-Resolution		
BVLC	Type	0x82
	Function	0x06
	Length	0x0007
	Source-Virtual-Address	0x651789

Table 8.1: Virtual-Address-Resolution Packet

8.2 Virtual-Address-Resolution-ACK

The Virtual-Address-Resolution-ACK is the expected answer to a Virtual-Address-Resolution packet and delivers the requested virtual address. The packet structure as defined in the BACnet standard [93] is visible in table 8.2.

Virtual-Address-Resolution		
BVLC	Type	0x82
	Function	0x07
	Length	0x000A
	Source-Virtual-Address	?
	Destination-Virtual-Adress	0x651789

Table 8.2: Virtual-Address-Resolution-ACK Packet

8.3 Results and Evaluation

None of the 49 addressed hosts sent an answer to the Virtual-Address-Resolution packet.

Therefore the suspicion that IPv6 devices are not spread out is enforced.

Chapter 9

Conclusion and Future Work

This thesis gives evidence that it is possible to detect Industrial Control Systems in the Internet via state-of-the-art scanning tools. The scan for building automation systems delivered 17 765 responses. After the execution of a filtering mechanism 13 596 packets could be used for further analysis of the answering systems.
The identification of device types was possible via requested properties and an adjustment with publicly available data sheets.
The analysis of the scanning data showed, that the detected BACnet devices were distributed in 1367 ASes and 4360 subnets.
The geographical location was determined via IP2Location. This showed that the building automation systems can be found in 80 countries, where 92.28 % of the devices are concentrated in only 10.
The execution of traceroutes to the detected IPs proofed that more than 4003 devices were reachable directly without any other hop in their subsystem. This indicates that those devices are not protected via a firewall.
A reverse DNS lookup of the answering IPs detected 9585 valid entries. The further analysis showed that the bulk has the IP encoded in the DNS name, which indicates that the devices use dial up networks to access the Internet.
A look at the BACnet IPv6 deployment revealed that either are devices not yet deployed or the security situation in IPv6 is better than in IPv4.
The security exposure of Industrial Control Systems is not something new: researchers have alerted admins and vendors multiple times in the past already. The topic ICS security needs to stay in focus. The automation of buildings and the need to connect systems which are constantly remote is increasing. During this thesis Li et al. [27] and Stock et al. [95] published researches which compared notification methods based on information content and notified party. The result of both investigations is, that the biggest challenge in context of the notification process is how to address a party which is capable of addressing the issue, ideally the owner of the vulnerable system.
A detailed analysis of the network structure in which the devices are installed could

therefore provide the possibility of a higher chance to reach the significant parties. This research has shown, that 5999 IPs belong to dial up networks. An admin using a dial up network to connect his BACnet device to the internet, has to be notified in a different way, than somebody who is having his own static IP and the related WHOIS contacts. This thesis also substructured the network according to ASes. Setting this knowledge into account could also help to reach the owner of a vulnerable system. One example is the DFN-CERT AS, which was investigated in detail in the paper of Gasser et al. [34]. In this case the knowledge about the AS affiliation of devices provided another option to address the concerned party.
The research by Li et al. [27] has shown that the level of detail in a vulnerability notification is vital.
Our research reviled that it is possible to detect building automation systems via state-of-the-art scanning tools and gain detailed information about the systems with a network analysis.
For the sake of security improvements for Industrial Control Systems future studies should exploit this knowledge and enhance it according to other ICS protocols. A detailed analysis of devices and their network structure can empower a more specific vulnerability notification.
Forseeable damage should be prevented via a personalized notification campaign, which carries all details which were detected via a scan. This data should also be combined with the device specific information to direct the specific warnings which are published by ICS-CERT to the affected party and make vendors aware of their responsibility.

Appendix

Appendix A

Scanning Environment

The scan was performed for the announced IPv4 range, except the following blacklist.

A.1 Blacklist

0.0.0.0/8
5.9.0.0/16
5.9.212.112/26
5.9.243.48/26
5.103.118.161/32
10.0.0.0/8
46.4.0.0/16
46.4.8.254/32
46.4.221.0/26
50.16.210.77/32
50.16.218.163/32
50.84.165.226/32
50.84.165.229/32
50.84.165.230/32
62.8.242.40/29
62.8.242.128/25
62.108.40.57/32
62.146.208.0/21
62.153.170.128/26
64.81.65.209/32
66.231.96.0/19
66.232.79.143/32
67.50.173.0/24

68.15.179.160/28
70.42.235.0/24
71.39.117.84/32
74.217.199.0/24
75.148.20.224/29
77.40.163.0/24
77.86.22.240/28
78.33.153.148/32
78.46.0.0/16
78.47.0.0/16
78.47.100.25/32
78.142.157.130/27
78.142.175.162/29
80.65.162.64/26
80.81.242.156/32
80.153.19.148/32
80.154.101.8/29
81.19.156.34/32
81.91.21.0/24
81.187.32.0/21
82.118.32.0/19
85.10.192.0/18
85.16.64.114/32
87.139.226.66/32
87.193.187.2/28
88.198.0.0/16
90.146.60.113/32
91.213.132.0/24
93.190.87.0/24
94.103.96.0/20
94.142.244.80/32
94.142.244.82/32
94.142.245.56/30
95.157.63.22/32
95.230.66.109/32
96.90.231.120/29
100.64.0.0/10
112.118.25.176/32
124.102.209.93/32
127.0.0.0/8
128.95.181.0/24

128.95.188.0/24
128.128.0.0/16
128.173.8.0/22
128.208.237.0/24
129.79.0.0/16
129.123.0.0/16
129.247.81.0/24
131.215.0.0/16
134.4.0.0/16
134.61.0.0/16
134.68.0.0/16
134.94.0.0/16
134.130.0.0/16
136.243.0.0/16
137.226.0.0/16
138.133.194.212/32
138.201.0.0/16
140.142.227.0/24
140.142.235.0/24
140.182.0.0/16
141.209.171.21/32
142.213.192.208/28
142.239.0.0/16
143.106.0.0/16
144.39.0.0/16
144.76.0.0/16
148.251.0.0/16
149.62.56.0/21
149.159.0.0/16
149.160.0.0/16
149.166.0.0/16
151.236.221.41/32
153.195.172.118/32
156.56.0.0/16
164.106.0.0/16
165.8.0.0/16
165.9.0.0/16
165.10.0.0/16
165.11.0.0/16
169.254.0.0/16
172.16.0.0/12

173.10.172.16/29
173.79.223.0/27
174.133.16.2/32
174.134.253.168/29
174.136.100.2/32
176.9.0.0/16
176.9.214.88/26
177.8.96.0/20
177.220.0.0/17
178.63.0.0/16
178.250.168.0/24
184.23.146.3/32
185.5.184.0/23
185.12.64.0/22
185.54.120.0/22
186.193.238.86/32
188.40.0.0/16
188.138.95.7/32
191.248.50.42/32
192.0.0.0/24
192.0.2.0/24
192.12.19.0/24
192.31.43.0/24
192.41.208.0/24
192.43.243.0/24
192.54.249.0/24
192.88.99.0/24
192.168.0.0/16
192.206.180.0/24
193.47.99.0/24
193.97.129.0/24
193.141.96.0/24
193.149.32.0/19
194.39.121.0/24
194.49.60.0/24
194.77.40.240/29
194.97.64.0/19
194.97.128.0/19
195.24.96.0/19
195.30.0.0/16
195.72.124.0/22

195.244.224.0/19
198.18.0.0/15
198.51.100.0/24
198.82.169.0/24
198.82.247.0/24
198.180.160.0/24
198.199.222.0/24
200.150.105.0/24
200.159.123.0/24
200.160.0.0/16
201.16.252.0/24
203.0.113.0/24
204.113.91.0/24
204.155.26.0/23
205.134.174.160/28
205.134.191.160/28
207.170.251.32/27
208.81.245.240/29
209.62.92.114/32
209.237.229.222/32
212.117.97.0/24
212.121.143.0/24
212.123.124.0/22
212.227.183.33/32
213.133.96.0/19
213.166.55.0/25
213.193.78.110/32
213.215.219.178/32
213.215.233.138/32
213.218.180.111/32
213.218.180.112/32
213.239.192.0/18
213.239.197.104/32
213.239.197.105/32
213.239.197.117/32
213.239.197.118/32
213.239.197.118/32
216.196.64.0/19
217.6.188.104/29
217.7.234.135/32
217.7.252.153/32

217.86.140.139/32
217.91.23.37/32
217.92.231.81/32
217.92.235.109/32
217.111.204.38/32
217.198.148.84/32
223.16.34.188/32
223.16.38.179/32
224.0.0.0/4
240.0.0.0/4
255.255.255.255/32

Bibliography

[1] Control Global. (2016) Leading automation vendors worldwide in 2014, based on revenue (in billion U.S. dollars). Retrieved September 26, 2016. [Online]. Available: https://www.statista.com/statistics/257058/ranking-of-the-leading-automation-vendors-worldwide/

[2] E. P. Leverett, "Quantitatively Assessing and Visualising Industrial System Attack Surfaces," Ph.D. dissertation, University of Cambridge, 2011.

[3] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman, "A Search Engine Backed by Internet-Wide Scanning," in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15. New York, NY, USA: ACM, 2015, pp. 542–553.

[4] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security Issues in SCADA Networks," *Comput. Secur.*, vol. 25, no. 7, pp. 498–506, Oct. 2006.

[5] K. A. Stouffer, J. A. Falco, and K. A. Scarfone, "Guide to Industrial Control Systems (ICS) Security," National Institute of Standards & Technology, Gaithersburg, MD, United States, Tech. Rep., 2011.

[6] E. Larson, P. Hurtado, and C. Strohm, "Iranians Hacked From Wall Street to New York Dam, U.S. Says," March 2016, retrieved September 9, 2016. [Online]. Available: http://www.bloomberg.com/news/articles/2016-03-24/u-s-charges-iranian-hackers-in-wall-street-cyberattacks-im6b43tt

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI, "Die Lage der IT-Sicherheit in Deutschland 2014," Tech. Rep.

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Die Lage der IT-Sicherheit in Deutschland 2015," Tech. Rep., November 2015.

[9] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the Cyber Attack on the Ukrainian Power Grid," Tech. Rep., March 2016.

[10] Krempl, Stefan. (2015) 32C3: Automatische Zugsicherung und vernetzte Bahntechnik im Hackervisier. Retrieved September 15,

2016. [Online]. Available: http://www.heise.de/newsticker/meldung/32C3-Automatische-Zugsicherung-und-vernetzte-Bahntechnik-im-Hackervisier-3056484.html

[11] "ICS-CERT Monitor January/February/March 2015," Tech. Rep., 2015. [Online]. Available: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

[12] D. Harp and B. Gregory-Brown, "The State of Security in Control Systems Today," Tech. Rep., June 2015.

[13] (2016) Total market value of the global building automation and controls market in 2013 and 2020 (in billion U.S. dollars)). Retrieved September 26, 2016. [Online]. Available: https://www.statista.com/statistics/420761/global-smart-homes-market-value/

[14] U.S. Department of Homeland Security: Industrial Control Systems Cyber Emergency Response Team, "ICS-CERT Monitor January/February/March 2013," Tech. Rep., 2013.

[15] K. Zetter, "Researchers Hack Building Control System at Google Australia Office," June 2013, retrieved September 12, 2016. [Online]. Available: https://www.wired.com/2013/05/googles-control-system-hacked/

[16] P. Zito. (2016) Guess who Just Hacked a Building Automation System? Retrieved September 12, 2016. [Online]. Available: http://blog.buildingautomationmonthly.com/ibm-hacks-what-is-most-likely-a-tridium-system/

[17] "Penetration testing a building automation system," 2016, retrieved September 12, 2016. [Online]. Available: https://regmedia.co.uk/2016/02/10/567584334543.pdf

[18] (2016) Shodan. Retrieved March 03, 2016. [Online]. Available: https://www.shodan.io

[19] J.-O. Malchow and J. Klick, "Erreichbarkeit von digitalen Steuergeräten - Ein Lagebild," in *Proceedings of the 21st DFN-Workshop 2014*, 2014.

[20] IP2Location. [Online]. Available: https://www.ip2location.com

[21] J. Klick, S. Lau, D. Marzin, J.-O. Malchow, and V. Roth, "Internet-facing PLCs as a network backdoor," in *CNS*. IEEE, 2015. [Online]. Available: http://dblp.uni-trier.de/db/conf/cns/cns2015.html#KlickLMMR15

[22] B. Radvanovsky. (2014) Project SHINE (SHodan INtelligence Extraction). Retrieved April 9, 2016. [Online]. Available: http://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014,2016-04-09

[23] F. Y. Rashid, "Project SHINE Reveals Magnitude of Internet-connected Critical Control Systems," October 2014, retrieved September 9, 2016. [Online]. Available: http://www.securityweek.com/project-shine-reveals-magnitude-internet-connected-critical-control-systems

[24] P. Celeda, R. Krejci, and V. Krmicek, "Flow-based Security Issue Detection in Building Automation and Control Networks," 2012.

[25] R. Krejci, P. Celeda, and J. Dobrovolny, "Traffic measurement and analysis of building automation and control networks," 2012.

[26] J. Kaur, J. Tonejc, S. Wendzel, and M. Meier, "Securing BACnet's Pitfalls," in *ICT Systems Security and Privacy Protection: 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, Proceedings*. Springer, 2015.

[27] F. Li, Z. Durumeric, J. Czyz, M. Karami, M. Bailey, D. McCoy, S. Savage, and V. Paxson, "You've Got Vulnerability: Exploring Effective Vulnerability Notifications," in *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, Aug. 2016, pp. 1033–1050.

[28] (2014) Map of Industrial Control Systems on the Internet. Retrieved April 6, 2016. [Online]. Available: https://icsmap.shodan.io

[29] Censys Team. (2016) Internet-Wide Scan Data Repository. [Online]. Available: https://scans.io/

[30] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman. (2015) Censys. Retrieved March 03, 2016. [Online]. Available: https://www.censys.io,2016-03-18

[31] Rapid7 Labs. Project Sonar. [Online]. Available: https://sonar.labs.rapid7.com/

[32] R. American National Institute/American Society of Heating and A.-C. Engineering, *BACnet - A Data Communication Protocol for Building Automation and Control Systems*, 1995.

[33] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast Internet-wide Scanning and Its Security Applications," in *Proceedings of the 22Nd USENIX Conference on Security*, ser. SEC'13. Berkeley, CA, USA: USENIX Association, 2013.

[34] O. Gasser, Q. Scheitle, C. Denis, D.-I. G. Carle, and N. Schricker, "Öffentlich erreichbare Gebäudeautomatisierung: Amplification Anfälligkeit von BACnet und Deployment-Analyse im Internet und DFN," 2016.

[35] Center for Applied Internet Data Analysis, "Routeviews Prefix to AS mappings Dataset." [Online]. Available: http://www.caida.org/data/routing/routeviews-prefix2as.xml

[36] (2016) TimeZoneDB database. Retrieved October 10, 2016. [Online]. Available: https://timezonedb.com/download

[37] Q. Scheitle, "MassDNS - A high-performance DNS stub resolver in C." [Online]. Available: https://github.com/quirins/massdns/network

[38] P. Sattler, "Parsing geographical locations from DNS names," February 2016.

[39] M. Luckie, "Scamper: a Scalable and Extensible Packet Prober for Active Measurement of the Internet," in *Proceedings of the 10th ACM SIGCOMM conference on Internet Measurement*. ACM, November 2010, pp. 239–245.

[40] O. Gasser, Q. Scheitle, S. Gebhard, and G. Carle, "Scanning the ipv6 internet: Towards a comprehensive hitlist," in *Proc. 8th Int. Workshop on Traffic Monitoring and Analysis*, Louvain-la-Neuve, Belgium, apr 2016. [Online]. Available: https://net.in.tum.de/pub/ipv6-hitlist/

[41] H. M. Newman, *BACnet: The Global Standard for Building Automation and Control Networks*, ser. Sustainable Energy Series. Momentum Press, 2013.

[42] Chipkin Automation Systems. (2012) BACnet: Life Safety Objects. Retrieved July 07, 2016. [Online]. Available: http://www.chipkin.com/bacnet-life-safety-objects/

[43] BACnetInternational, *Introduction to BACnet for Building Owners and Engineers*, 2014.

[44] C. Hübner, H. Merz, and T. Hansemann, *Gebäudeautomation - Kommunikationssysteme mit EIB/KNX, LON und BACnet*, 2009.

[45] *Addendum to ANSI/ASHRAE Standard 135-1995, BACnet — A Data Communication Protocol for Building Automation and Control Networks*, 1999.

[46] S. H. Hong and S. Lee, "Design and Implementation of Fault Tolerance in the BACnet/IP Protocol," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 11, pp. 3631–3638, Nov 2010.

[47] H. M. Newman, "Broadcasting BACnet," *ASHRAE Journal Vol. 52, No. 11, November 2010*, 2010.

[48] WAGO Innovative Connections, *WAGO-I/O-SYSTEM 750, BACnet - Objekte, Eigenschaften, Dienste*, 2010.

[49] W. Swan, "The Language of BACnet," *Engineered Systems*, 1996.

[50] G. Thomas, "Introduction to BACnet® Routers," *the Extension Vol. 9, No. 6, November 2008*, 2008.

[51] "ISO/IEC/IEEE International Standard for Ethernet," *ISO/IEC/IEEE 8802-3:2014(E)*, pp. 1–3754, April 2014.

[52] V. Boed, *Networking and Integration of Facilities Automation Systems*. CRC-Press, 1999.

[53] ProSoft Technology, *BACnet Protocol Manual*, 2010. [Online]. Available: http://www.prosoft-technology.com/content/download/716/6544/version/6/file/bacnet_edition_2_protocol_manual_.pdf

[54] H. M. Newman and M. D. Morris, *Direct Digital Control of Building Systems*, 1994.

[55] S. Karg, "The BACnet Device ID," *Foundations, A BACnet Publication, June 2012*, 2012.

[56] Honeywell International Inc, *BACnet Protocol Installation and User's Manual*, 2010. [Online]. Available: https://customer.honeywell.com/resources/techlit/TechLitDocuments/63-0000s/63-2697.pdf

[57] D. Adrian. Add a BACNet probe. Retrieved June 6, 2016. [Online]. Available: https://github.com/zmap/zmap/commit/d146df0fc43c08ee480328546a2c2d9677837017,2016-06-20

[58] S. Karg, "Improving BACnet MS/TP - Harder, Better, Faster, Stronger," *ASHRAE Journal, Vol. 52, No. 11, November 2010*, 2010.

[59] BACnet International. (2012) BACnet Testing Labs - Product Listing. Retrieved July 24, 2016. [Online]. Available: http://www.bacnetinternational.net/btl/,2016-07-24

[60] American National Institute/American Society of Heating, Refrigerating and Air-Conditioning Engineering. (2016) Vendor IDs. Retrieved June 6, 2016. [Online]. Available: http://www.bacnet.org/VendorID/index.html

[61] (2016) Reliable controls. Retrieved September 9, 2016. [Online]. Available: http://www.reliablecontrols.com/

[62] R. J. O'Harrow, "Tridium's Niagara Framework: Marvel of connectivity illustrates new cyber risks," *The Washington Post*, July 2012.

[63] B. Rios, "Owning a Building," 2014.

[64] "Advisory (ICSA-12-228-01A)," 2014, retrieved September 8, 2016. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-12-228-01A

[65] "Researchers hack Google Australia headquarters building," 2013, retrieved September 12, 2016. [Online]. Available: http://www.news.com.au/finance/business/researchers-hack-google-australia-headquarters-building/story-fn5lic6c-1226636518107

[66] (2016) Delta controls. Retrieved September 9, 2016. [Online]. Available: http://www.deltacontrols.de/

[67] "Advisory (ICSA-14-350-02)," 2015, retrieved September 9, 2016. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-14-350-02

[68] Automated Logic. Retrieved September 27, 2016. [Online]. Available: http://www.automatedlogic.com/

[69] (2016) novar.com. Retrieved September 27, 2016. [Online]. Available: http://www.novar.com/

[70] Alerton Building Automation Resources. Retrieved September 27, 2016. [Online]. Available: https://alerton.com/en-US/about/Pages/default.aspx

[71] (2016) Automation Systems. Retrieved September 26, 2016. [Online]. Available: http://w3.siemens.com/mcms/automation/en/automation-systems/Pages/Default.aspx

[72] H. M. Newman, "BACnet Explained," *ASHRAE Journal Vol. 55, No. 11, November 2013*, November 2013. [Online]. Available: http://www.bacnet.org/Bibliography/BACnet-Today-13/Newman-2013.pdf

[73] Tridium, *NiagaraAX-3.x USer Guide*, 2007. [Online]. Available: http://www.controlequiputah.com/Literature/Honeywell/docUser.pdf

[74] Reliable Controls, *MACH-ProWebSys*, 2009. [Online]. Available: http://www.reliablecontrols.com/products/catalog/pdfs/Catalog_MPWS_En_Imp.pdf

[75] *Tracer SC System Controller*, 2015. [Online]. Available: https://www.trane.com/content/dam/Trane/Commercial/global/controls/equipment-controls/BAS/TracerSC/documents/BAS-PRD024A-EN_05092015.pdf

[76] Reliable Controls, *MACH-ProWebCom*, 2010. [Online]. Available: http://www.reliablecontrols.com/products/catalog/pdfs/Catalog_MPWC_En_Imp.pdf

[77] Reliable Controls, *MACH-ProCom*, 2007. [Online]. Available: http://www.reliablecontrols.com/products/catalog/pdfs/Catalog_MPC_En_Imp.pdf

[78] United Technologies Corporation, *ME812u, ME812u-E, ME812u-LGR Router/Controller*, 2013.

[79] Reliable Controls, *MACH-ProSys*, 2007. [Online]. Available: http://www.reliablecontrols.com/products/catalog/pdfs/Catalog_MPS_En_Imp.pdf

[80] Delta Controls, *System Managers*, 2009. [Online]. Available: http://controlconceptsonline.com/datasheets/DSM-RTR.pdf

[81] Delta Controls, *System Controllers*, 2009. [Online]. Available: http://controlconceptsonline.com/datasheets/DSC-1616.pdf

[82] Fr. Sauter AG, *EY-AS 524, 525: Modular automation station, modu524/525*, 2015.

[83] Center for Applied Internet Data Analysis, "AS Rank: AS Ranking ," retrieved October 6, 2016. [Online]. Available: as-rank.caida.org

[84] Green Buildings. Retrieved September 9, 2016. [Online]. Available: http://deltaww.com/about/csr_GreenBuilding.aspx?secID=5&pid=6&tid=8&hl=en-US

[85] "Advisory ICSA-16-014-01," retrieved September 14, 2016. [Online]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-16-014-01

[86] Miaoski and Hilt, Stephen, "Building Automation and Control," 2015, retrieved September 14, 2016. [Online]. Available: https://hitcon.org/2015/ENT/PDF/Building%20Automation%20and%20Control_miaoski.pdf

[87] "Product Listing," Tech. Rep., 2012, retrieved September 23, 2016. [Online]. Available: http://www.bacnetinternational.net/btl/listings/triacta%20power%20technologies%20inc/BTL_Listing_23929_Triacta_4000-6000.pdf

[88] (2016) WHOIS results for gov.ab.ca. Retrieved September 19, 2016. [Online]. Available: https://dig.whois.com.au/whois/gov.ab.ca

[89] E. Vasilomanolakis, S. Srinivasa, and M. Mühlhäuser, "Did you really hack a nuclear power plant? An industrial control mobile honeypot." in *CNS*. IEEE, 2015. [Online]. Available: http://dblp.uni-trier.de/db/conf/cns/cns2015.html#Vasilomanolakis15a

[90] Koramis GmbH, "White Paper: Projekt HoneyTrain Aufbau, Durchführung und Ergebnisse," Koramis GmBH, Saarbrücken, Deutschland, Tech. Rep., 2015.

[91] R. American National Institute/American Society of Heating and A.-C. Engineering, *Addendum g to ANSI/ASHRAE Standard 135-2004, BACnet — A Data Communication Protocol for Building Automation and Control Networks*, 2006.

[92] J. Hart, "Add BACnet 'read property multiple' probe." [Online]. Available: https://github.com/zmap/zmap/pull/360

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

[94] J. Davies, *Understanding IPv6*. Pearson Education, 2012.

[95] B. Stock, G. Pellegrino, C. Rossow, M. Johns, and M. Backes, "Hey, You Have a Problem: On the Feasibility of Large-Scale Web Vulnerability Notification," in *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, Aug 2016, pp. 1015–1032.