Öffentlich erreichbare Gebäudeautomatisierung: Amplification-Anfälligkeit von BACnet und Deployment-Analyse im Internet und DFN

Oliver Gasser, Quirin Scheitle, Carl Denis, Nadja Schricker, Georg Carle
{gasser,scheitle,denis,schrickn,carle}@net.in.tum.de
Technische Universität München

Zusammenfassung

Mit der Durchsetzung des Internet-Protokolls in der Kommunikationstechnik wurden auch viele industrielle Steuersysteme um IP-Fähigkeiten erweitert. Sicherheit war bei Protokollen für Steuersysteme oft implizit durch lokale Verkabelung realisiert. Durch die IP-Fähigkeit können diese Protokolle nun über weite Distanzen und öffentliche Netze betrieben werden. Dies kann leicht zu unsicheren Konfigurationen führen, in denen Steuersysteme wichtiger Anlagen über das Internet erreichbar sind. In dieser Studie untersuchen wir die Verbreitung von BACnet, einem verbreiteten Protokoll zur Gebäudeautomatisierung, im öffentlichen Internet. Mit Hilfe von aktiven Netzwerk-Scans finden wir über 13 000 BACnet-Geräte in über 1300 Autonomen Systemen. Wir klassifizieren die erkannten Geräte nach Hersteller und Funktion. Außerdem analysieren wir das Protokoll auf seine Anfälligkeit für Amplification-Angriffe. Durch spezielle BACnet-Anfragen können wir einen Amplification-Faktor von 30 erreichen. Abschließend unterbreiten wir Vorschläge zum Schutz vor Amplification-Angriffen.

1 Einleitung

Steuergeräte aus dem Industrie- und Automatisierungsbereich werden zunehmend ans Internet angeschlossen, um Automatisierbarkeit und Fernwartbarkeit voranzutreiben. Der Betrieb von Steuergeräten ohne Zugangskontrolle am Übergang zum Internet birgt zweierlei Gefahren. Einerseits sind dies Folgen für

das ungeschützte System selbst: Nicht autorisierte Zugriffe oder eine Unterbrechung des Betriebs können sogar eine Gefahr für Leib und Leben zur Folge haben. Andererseits können diese Systeme zum weiterführenden Angriff auf Dritte benutzt werden, etwa durch Anfälligkeiten für Amplification-Angriffe. Viele Forschungsprojekte [28, 10, 23, 4] und prominente Beispiele wie etwa der Amplification-Angriff auf Spamhaus [24] oder CloudFlare [25] unterstreichen die Probleme durch *Distributed Reflective Denial of Service* Angriffe, welche auf derartigen Amplification-Anfälligkeiten beruhen. Steuersysteme sind durch IP-Zugriffsregeln oder VPN-Lösungen schnell und effektiv zugriffsbeschränkbar, allerdings zeigen Studien immer wieder, dass auf eine Vielzahl von Systemen frei über das Internet zugegriffen werden kann.

Forschungsbestrebungen der letzten Jahre beschäftigten sich intensiv mit Sicherheitsprotokollen [5, 13, 15] und offenbaren auch ein verstärktes Interesse an industriellen Kontrollsystemen [6, 20, 11]. Die Welt der Gebäudeautomatisierung bleibt dabei meist unbeachtet und es existiert noch keine detaillierte Analyse über die Art der verfügbaren Geräte. Mit Werkzeugen wie ZMap [14] stehen sehr effiziente Scanner zur Verfügung, die eine Internetweite Suche nach BACnet-Geräten in wenigen Stunden ermöglichen. Auf scans.io sind Ergebnisse von Scans nach BACnet-Geräten von Project Sonar [26] seit Juni 2014 verfügbar und seit Dezember 2015 werden im Projekt Censys [12] auch regelmäßige Scans nach BACnet-Geräten im Internet durchgeführt.

In dieser Veröffentlichung werden folgende neue Aspekte beleuchtet:

- Klassifikation erreichbarer BACnet-Geräte
- Anfälligkeit des BACnet-Protokolls für Amplification-Angriffe
- Aufbau eines aussagekräftigen BACnet-Pakets zum Scannen
- Vergleich des Deutschen Forschungsnetzes (DFN) mit dem Rest des Internets in Bezug auf BACnet-Geräte

Die selbst entwickelten Werkzeuge zur Analyse der BACnet-Pakete sind auf GitHub [16] für die Öffentlichkeit zugänglich.

Weitergehend ist diese Arbeit wie folgt aufgebaut: In den Abschnitten 2 und 3 beschreiben wir Hintergründe zum BACnet-Protokoll und die Durchführung unserer Scans. In Abschnitt 4 werten wir die Scans aus, beschreiben die erhaltenen Scan-Antworten und analysieren die Art und Verteilung der gefundenen Geräte. Darüber hinaus vergleichen wir unsere Ergebnisse mit

denen anderer Forschungsgruppen zu vergleichbaren Protokollen. Wir vergleichen auch die Verteilung der Geräte im DFN mit der im restlichen Internet. In Abschnitt 5 beschreiben wir unsere Untersuchung zu möglichen Amplification-Angriffen mittels erreichbarer BACnet-Geräte. Wir beleuchten auch kurz welche Maßnahmen ein Internetdienstanbieter in Bezug auf Amplification-Angriffe mit BACnet ergreifen kann. Verwandte Arbeiten werden in Abschnitt 6 beschrieben. Abschnitt 7 schließt diese Arbeit mit einer Zusammenfassung und einem Ausblick ab.

2 Das BACnet-Protokoll

In diesem Abschnitt beschreiben wir die für diese Arbeit relevanten Eigenschaften des BACnet-Protokolls.

BACnet (Building Automation and Control Networks) ist ein Protokoll zur Gebäudeautomatisierung. Es wurde 1995 erstmals durch die American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) standardisiert [2]. Typische Einsatzgebiete sind Heizung, Lüftung und Klimatechnik (HLK), aber auch im Bereich Sicherheitstechnik finden BACnet-Geräte Anwendung. Hierbei reicht die Palette der unterstützten Geräte von einzelnen Sensoren, die durch Controller überwacht und gesteuert werden können, bis zu vollständigen Automatisierungssystemen, die eine Vielzahl von Servern, Controllern und Sensoren kontrollieren. Insbesondere bei großen Gebäudekomplexen ist ein zentralisiertes Management oft wünschenswert, um gezielt auf Ereignisse reagieren zu können und verschiedene Standorte intelligent zu vernetzen. BACnet definiert mehrere Service-Klassen, das Auslesen und Setzen von Objektwerten ist genauso möglich wie Datentransfers oder Zugriffe per Virtual Terminal. Durch die vielen Service-Klassen ergibt sich für einen Scan nach BACnet-Geräten eine Vielzahl an Möglichkeiten. Ein Ziel ist daher, einen Pakettyp zu finden, der möglichst viele Geräte findet, ohne diese übermäßig zu belasten. Der sogenannte *ReadProperty*-Service empfiehlt sich hierbei aus mehreren Gründen. Zunächst ist der Service eine Grundvoraussetzung für eine Qualifizierung als BACnet-Gerät [30], dementsprechend ist davon auszugehen, dass zumindest der Großteil der adressierten Geräte diesen Service unterstützt. Weiterhin ist die Anfrage wenig intrusiv, da ohne Anmeldung öffentliche Geräteeigenschaften abgefragt werden. Diese abgefragten Eigenschaften ermöglichen weiterhin eine detailliertere Analyse der erreichten Geräte. Final ist ausschlaggebend, dass das spezifische Gerät nicht über eine konkrete Objekt-ID (siehe

Abschnitt 2.1.3) adressiert werden muss. Stattdessen kann eine generische ID verwendet werden, auf die Geräte unabhängig von ihrer eigenen Objekt-ID antworten. Als Erweiterung des *ReadProperty*-Pakets verwenden wir ebenfalls ein *ReadPropertyMultiple*-Paket, welches das gleichzeitige Auslesen von mehreren Eigenschaften erlaubt. In beiden Fällen antwortet das angesprochene Gerät mit einem *ComplexACK*, welches die abgefragten Eigenschaften enthält.

2.1 Paketformat

BACnet bietet die Möglichkeit unterschiedliche Transportschichten (z.B. LonTalk, ZigBee und Ethernet) zu benutzen, um verteilte Standorte miteinander zu verbinden [3]. Diese Studie setzt den Schwerpunkt auf die Protokollvariante BACnet/IP welche zum Transport UDP auf Port 47808 verwendet. Der BACnet-Standard erlaubt auch Alternativ-Ports, für die Scans wird hier der Standard-Port verwendet. Die Struktur der *UDP-Payload* ist in Tabelle 1 zu sehen. Dabei lässt sich das Paket in drei Teile unterteilen: BACnet Virtual Link Control (BVLC), Network Control Unit (NPDU) und die Application Data Unit (APDU).

Tabelle 1: BACnet/IP *ReadProperty* Paketstruktur

	ReadProperty Packet	
BVLC	Type	1 Byte
	Function	1 Byte
	Length	2 Byte
NPDU	Version	1 Byte
	Control	1 Byte
APDU	Type	1 Byte
	Response	1 Byte
	Invoke ID	1 Byte
	Service Choice	1 Byte
	Context Tag 0	1 Byte
	Object Type & Instance	4 Byte
	Context Tag 1	1 Byte
	Property Instance	2 Byte

2.1.1 BACnet Virtual Link Control (BVLC)

Die Spezifizierung, welches Schicht-2-Protokoll für BACnet verwendet wird, passiert im BACnet Virtual Link Control Layer des Pakets.
Es ist notwendig den Typ der nachfolgenden *Network Protocol Data Unit* im Feld Funktion zu definieren. Der Transport des Pakets soll über die BACnet Port-Nummer 47808 zu den im Scan spezifizierten IP-Adressen erfolgen. Dementsprechend setzen wir den Typ auf *Original-Unicast-NPDU*.
Das Längenfeld spezifiziert die Anzahl der Bytes der gesamten BACnet-Payload.

2.1.2 Network Protocol Data Unit (NPDU)

Im Feld *Network-Protocol-Version* wird die aktuelle BACnet Version spezifiziert, wobei die einzig gültige Versionsnummer die 1 ist.
Das *Control-Byte* gibt an, ob optionale Felder wie eine Schicht-2-Zieladresse im Paket-Header enthalten sind. Da wir eine generische Objekt-ID verwenden (siehe Abschnitt 2.1.3), ist eine Spezifizierung der Zieladresse hier nicht erforderlich. Das *ReadProperty*-Paket ist eine Anfrage auf welche ein *ComplexACK* als Antwort erwartet wird. Entsprechend wird in unserem Anfragepaket im *Control-Byte* ausschließlich das dritte Bit für "Antwort erwartet" gesetzt.

2.1.3 Application Protocol Data Unit (APDU)

Die höherwertigen vier Bit des APDU Typs spezifizieren die Art der APDU, in diesem Fall handelt es sich um einen *Confirmed-Request*. Die niederwertigen vier Bit spezifizieren ob eine Segmentierung des Pakets erfolgt, wie viele Segmente folgen werden und ob eine segmentierte Antwort erwartet wird. Für den Scan wurde weder eine Segmentierung verwendet noch zugelassen, dementsprechend wurde keines der Bits gesetzt.
Die Parameter für die erwartete Antwort werden im Feld APDU Response gesetzt. Die oberen vier Bit spezifizieren die Anzahl der akzeptierten Segmente, nachdem keine segmentierten Antworten akzeptiert werden, ist hier kein Bit gesetzt, was dem Wert *Undefined* entspricht. Die niederwertigen vier Bit geben die Größe der erwarteten Antwort an.
Die *Invoke ID* dient der Zuordnung von Anfrage und Antwort und kann auf einen Wert im Bereich `0x00-0xff` gesetzt werden.
Für diese Studie wird das *ReadProperty*-Paket verwendet. Der entsprechende Wert für die *Service Choice* ist dementsprechend `0x0c`.

Context-Tags beschreiben den Typ und die Länge von nachfolgenden Informationen.
Objekt-ID und Typ belegen vier Byte, die oberen zehn Bit definieren den Typ eines Objektes. BACnet-Standard-Typen sind von 0 bis 127 nummeriert. Weitere nicht standardisierte Typen belegen die Werte 128 bis 1023. In dieser Studie wird der Typ *Device* verwendet, da ausschließlich Eigenschaften eines Objektes diesen Typs abgefragt werden. Die darauffolgenden 22 Bit spezifizieren die Objekt-ID. Für diesen Scan werden alle Bit welche die Objekt-ID repräsentieren auf 1 gesetzt, denn dadurch werden alle BACnet-Geräte unabhängig von ihrer Objekt-ID adressiert. Somit ist für die Paketkonstruktion kein Wissen über die ID des entfernten Gerätes notwendig.
Nach dem nachfolgenden Tag wird die abzufragende Eigenschaft definiert, hier wird der Herstellername mit dem Wert `0x79` repräsentiert.

2.1.4 ComplexACK-Paket

Die erwartete Antwort ist ein *ComplexACK* mit der abgefragten Eigenschaft. An den Paketteilen BVLC und NPDU ändert sich lediglich die Länge. In der *Application Data Unit* wird ein geänderter Typ spezifiziert, in diesem Fall *ComplexACK*. Zudem ändert sich das Tagging und der Eigenschaft-ID folgt der entsprechende Wert der Eigenschaft.

2.1.5 ReadPropertyMultiple-Paket

Der Aufbau des *ReadPropertyMultiple* Pakets unterscheidet sich lediglich durch die Service-Wahl und die unterschiedlichen Eigenschaften. Dadurch ändern sich Tagging und Länge. Die abgefragten Eigenschaften in diesem Scan sind Herstellername, Hersteller-ID, Zeit, Datum, Ort, Modellname und Objekt.
Die erwartete Antwort ist auch hier ein *ComplexACK*-Paket, das sich lediglich durch die Anzahl der beantworteten Geräteeigenschaften, sowie die Paketlänge unterscheidet.

3 Erkennen von BACnet-Geräten

In diesem Abschnitt beschreiben wir die aktiven Netzwerk-Scans, die zur Untersuchung der Verbreitung des BACnet-Protokolls im Internet durchgeführt wurden.

Tabelle 2: Basis-Statistiken zu den durchgeführten Netzwerkmessungen.

			Antworten	
Scan-Typ	Scan-Dauer	Ziele	Empfangen	Gültig
BACnet Multi Prop.	31 h	2,8 G	17 765	13 596
BACnet Single Prop.	31 h	2,8 G	17 647	13 603

3.1 Durchgeführte Scans

Für die Untersuchung des BACnet-Protokolls wurden zwei Arten von aktiven Scans durchgeführt: (1) *ReadProperty* und (2) *ReadPropertyMultiple*.

Die Scans wurden von einem Rechner mit 8-Kern Intel Xeon W3565 (3,2 GHz) und 12 GB RAM von einem Netzbereich durchgeführt, der spezifisch für Netzwerkmessungen vorgesehen war. Sie wurden nacheinander ausgeführt, um wechselseitige Interferenzen zu verhindern. Als Scan-Software wurde ZMap [14] eingesetzt. Für den Scan wurde ein neues ZMap-Modul geschrieben, das BACnet-Pakete verschickt, diese empfängt und rudimentär vorfiltert. Weitere Filterschritte der Antwort-Pakete wurden in der Nachbearbeitung vorgenommen (siehe Abschnitt 3.2). Mit diesem ZMap-Modul wurden aktive Messungen auf UDP-Port 47 808 (Standard BACnet-Port) durchgeführt. Die Ziel-IP-Adressen für die BACnet-Scans waren alle BGP-annoncierten Präfixe abzüglich einer Blacklist (siehe Abschnitt 3.4). Die Senderate lag bei den BACnet-Scans bei 25 000 Paketen pro Sekunde. Ein Überblick über die zwei Messungen und Statistiken dazu sind in Tabelle 2 zu finden.

3.2 Filtern der Antworten

Die empfangenen Antworten wurden gefiltert, um die gültigen Antworten zu erhalten. Bei BACnet besteht dieser Prozess aus mehreren Schritten, in denen untersucht wird, ob das Antwortpaket eine gültige *BACnet-ComplexACK-PDU* enthält:

1. BACnet-Transport-Typ muss BACnet/IP sein
2. BACnet-Funktion muss Original-Unicast-NPDU sein
3. BACnet-Version muss `1` sein

4. BACnet-Control-Byte darf keine reservierten Werte gesetzt haben
5. BACnet Quell- und Ziel-MAC-Adress-Felder validieren
6. BACnet-Payload-Typ muss *BACnet-ComplexACK-PDU* sein
7. BACnet-Service-Choice muss *ReadPropertyMultiple* sein

Nachfolgend werden die Filterschritte anhand des *ReadPropertyMultiple*-Pakets beschrieben. Für das einfache *ReadProperty*-Paket werden diese Schritte analog angewandt.

Alle empfangenen Pakete enthielten als BACnet-Transport-Typ BACnet/IP, weshalb durch diesen Schritt keine Pakete entfernt wurden. Dies wurde bereits durch den Filter in unserem BACnet-ZMap-Modul sichergestellt.

Durch den zweiten Filter wurden bereits einige Antworten entfernt: Vier Hosts schickten eine vermeintliche Broadcast-Nachricht. Die gesendete *Payload* entsprach jedoch einer Unicast-Nachricht, eine konforme Antwort müsste den gleichen Typ haben. Aus diesem Grund wurden diese vier Pakete aus der Auswertung entfernt. Weitere 16 Hosts schickten nicht-standardisierte Werte im Feld BACnet-Funktion.

Im dritten Schritt wurden Pakete mit ungültiger BACnet-Version aus den Ergebnissen ausgefiltert. Die einzig gültige BACnet-Version ist Version 1. Die ungültigen BACnet-Versionen, die in den Antworten vorkamen und herausgefiltert wurden, waren 246 (230 mal), Version 0 (122 mal) und 87 (vier mal).

Der vierte Filter behandelt das BACnet-*Control-Byte*. Hierbei finden wir über 800 BACnet-Geräte, die anzeigen, dass sie auf ihr Paket eine Antwort erwarten. Einige dieser Geräte senden aber trotz dieses unüblichen Verhaltens eine gültige Antwort, weshalb wir diese Pakete nicht ausfiltern. Keines der Pakete hat andere reservierte Bits im *Control-Byte* gesetzt, weshalb durch diesen Filterschritt keine Antworten entfernt werden.

Im fünften Schritt entfernen wir ein Antwortpaket, das den ungültigen Wert Null für die Länge des Ziel-MAC-Adress-Feldes verwendet.

Im sechsten Schritt filtern wir alle Pakete aus, die als Payload-Typ nicht *BACnet-ComplexACK-PDU* haben. Dadurch entfernen wir 1859 *Reject*-Pakete, 822 *Confirmed-Request*-Pakete, 753 *Error*-Pakete, 179 *Abort*-Pakete und 147 *Unconfirmed-Request*-Pakete.

Im letzten Schritt überprüfen wir das Service-Choice-Feld. Wir stellen sicher, dass dieses Feld auf *ReadPropertyMultiple* gesetzt ist, da wir im Multi-Property-Scan mehrere Eigenschaften auslesen wollen. Somit entfernen wir

31 Antworten die uns alle ein identisches *ReadProperty*-Paket mit einer leeren *Description-Property* geschickt haben. Diese 31 Pakete wurden alle vom selbem /24-Präfix aus einem Universitätsnetz verschickt. Dies sind Indizien für BACnet-Honeypots.

Nach den sieben Filterschritten bleiben von den ursprünglichen 17 765 Antwortpaketen noch 13 597 gültige Antworten übrig.

Mehr Informationen zum BACnet-Paketaufbau sind in Abschnitt 2.1 zu finden.

3.3 Vergleich der BACnet-Scan-Arten

Scans mit einem Multi-Property-Paket liefern mehr Informationen über das BACnet-Gerät zurück als Scans mit Single-Property-Paket. Um sicherzustellen, dass wir durch die Multi-Property-Scan-Methode keine Geräte übersehen, die diese Art von Anfrage nicht beantworten, führen wir einen Vergleich durch: Wir gleichen die Ergebnis-IP-Adressen des Multi-Property-Scans mit den IP-Adressen des Single-Property-Scans ab. Die Ergebnisse zeigen, dass es 847 IP-Adressen (4,8 %) gibt, die im Multi-Property-Scan vorkommen, aber nicht im Single-Property-Scan. Dem gegenüber gibt es 729 IP-Adressen (4,1 %), die nur im Single-Property-Scan enthalten sind. Das zeigt, dass die gewählte Scan-Methode einen geringen Einfluss auf die Menge der antwortenden Geräte hat. Deshalb fokussieren wir uns bei den übrigen Analysen in Abschnitt 4 auf die Antworten der aussagekräftigeren Multi-Property-Pakete.

3.4 Minimieren der Aufdringlichkeit

Um die Aufdringlichkeit der Scans zu minimieren, wurde eine Blacklist aus früheren Scans verwendet, es wurden nur per BGP annoncierte Präfixe gescannt und die Scan-Geschwindigkeit wurde auf 25 000 Pakete pro Sekunde gedrosselt. Außerdem wurde auf der Scan-Maschine ein Webserver eingerichtet, der interessierte Administratoren über die Scan-Aktivitäten informierte. Durch das gewählte Scan-Paket wurde sichergestellt, dass die Konfiguration der BACnet-Geräte nicht verändert wurde, sondern lediglich allgemeine Informationen wie Hersteller und Produktname des Geräts abgefragt wurden. Im Rahmen der Scans erhielten wir keine Abuse-Nachrichten.

4 Analyse des BACnet-Deployments

In diesem Abschnitt werden die durchgeführten Netzwerk-Scans evaluiert und die gefundenen BACnet-Geräte analysiert.

4.1 Instanz-ID

Die Instanz-ID (*Instance-ID*) gibt in BACnet die Instanznummer des jeweiligen Geräts in dem Subnetz an. Diese ID identifiziert das Gerät in diesem lokalen Subnetz und muss deshalb lokal einzigartig sein. Abbildung 1 zeigt die kumulative Verteilungsfunktion der Instanz-IDs von gültigen Antworten. Wir sehen, dass es sich um eine Long-Tail-Verteilung handelt: Einige wenige Instanz-IDs werden sehr häufig verwendet, der Rest teilt sich gleichmäßig auf. Die häufigste Instanz-ID `0x3fffff` kommt in 4868 gültigen Antwortpaketen vor. Hierbei zeigt sich, dass die meisten Geräte dieselbe generische Instanz-ID (`0x3fffff`) verwenden, wie wir in unserer Anfrage. Die nächsthäufigen Instanz-IDs sind `1000`, `10000` und `1`. Diese IDs scheinen vom Gerätehersteller vorkonfiguriert worden zu sein.

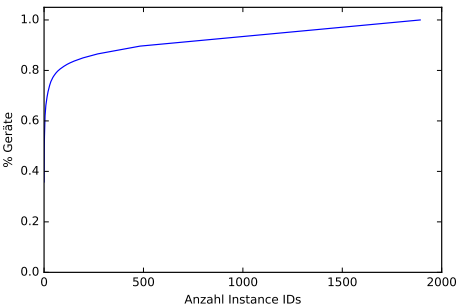


Abbildung 1: Kumulative Verteilung der Instanz-ID-Werte.

4.2 BACnet-Fehlermeldungen

In den folgenden Abschnitten untersuchen wir die Antworten bezüglich den abgefragten Eigenschaften. Da nicht alle Eigenschaften von allen Geräte unterstützt werden, schicken manche Geräte eine Fehlermeldung für diese Eigenschaft zurück. Da das Paket an sich ein gültiges BACnet-Paket ist, werden diese Pakete nicht im Filterschritt (siehe Abschnitt 3.2) entfernt. Tabelle 3 zeigt, wieviele Geräte je Eigenschaft mit einer Fehlermeldung antworten.

Tabelle 3: Fehlermeldungen pro abgefragter Eigenschaft.

	Local Date	Local Time	Location	Model Name	Object Name	Vendor ID	Vendor Name
Unkn. Object	1382	1379	1379	1380	1379	1379	1379
Unkn. Property	433	433	545	0	0	0	0
Unkn.	5	5	5	5	5	5	5
Incons. Serv. Params	2	2	2	2	2	2	2
Unsupp. Object Type	1	1	1	1	1	1	1
Service Req. Denied	1	1	1	1	1	1	1

Tabelle 4: Die 10 häufigsten Hersteller-IDs.

Pos	Hersteller-ID	Herstellername	Vorkommen	Häufigkeit [%]
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.	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

Wir bekommen insgesamt sechs verschiedene Fehlermeldungen von BACnet-Geräten. Der überwiegende Teil sind vom Typ *Unkown Object*. Außerdem finden wir bei den Eigenschaften zu Datum, Zeit und Ort um die 500 Geräte, die diese Eigenschaft nicht kennen. Bei den folgenden Auswertungen werden die Fehler vorher ausgefiltert, um die Analyse nicht zu beeinflussen.

4.3 Gerätehersteller und -modelle

In diesem Abschnitt analysieren wir die BACnet-Geräte anhand der abgefragten Eigenschaften.

Um die Geräte besser einordnen zu können, analysieren wir zuerst die Vendor-IDs. Tabelle 4 zeigt die Top 10 Hersteller-IDs. Der Name der Hersteller wurde mit Hilfe der offiziellen Hersteller-ID-Liste ermittelt[1].

[1] `www.bacnet.org/VendorID/BACnet%20Vendor%20IDs.htm`

Die ersten fünf Hersteller decken bereits über 65 % der 12 209 gültigen Hersteller-IDs ab.

Reliable Controls ist ein US-amerikanischer Hersteller von Steuereinheiten für Gebäudeautomatisierung, die über das Internet erreichbar sind. Eine Analyse der dazugehörigen Herstellernamen in der abgefragten Eigenschaft zeigt, dass diese ausschließlich Reliable Controls zugeordnet werden. Der abgefragte Modellname beinhaltet zum Großteil die Zeichenfolge *MachPro*, eine Modellreihe von Steuereinheiten für Gebäudeautomatisierung von Reliable Controls.

Tridium ist ein Hersteller von Steuereinheiten zur Integration von Internet-of-Things-Geräten. Auch hier bestätigt eine Analyse der abgefragten Eigenschaft, dass die BACnet-Controller in der Tat von *Tridium* stammen. Als Modell wird hauptsächlich die *NiagaraAX Station* eingesetzt.

Delta Controls ist ein Hersteller von Gebäudeautomatisierungssystemen, von dem laut eigenen Aussagen in über 80 Ländern BACnet-Installationen betrieben werden. Die abgefragte Eigenschaft Hersteller-ID bestätigt wiederum, dass die BACnet-Controller von Delta Controls gefertigt wurden. Hierbei ist die Streuung bei den Modellnamen größer als bei Reliable Controls und Tridium: Das am meisten verwendete Modell *DSM_RTR* kommt 369 Mal zum Einsatz.

Zusammenfassend kann man sagen, dass die Konsistenz der abgefragten Eigenschaften Hersteller-ID und Herstellername sehr hoch ist.

4.4 Clustering von BACnet-Geräten

In diesem Abschnitt untersuchen wir die Verteilung von BACnet-Geräten über Präfixe und Autonome Systeme (AS). Dafür bilden wir die Antwort-IP-Adressen mit Hilfe von CAIDAs *Prefix to AS Mappings* [9] auf Präfixe und ASe ab.

Abbildung 2a zeigt die kumulative Verteilung von BACnet-Geräten in Autonomen Systemen: In 200 ASen sind bereits 80 % aller BACnet-Geräte zu finden.

Dem gegenüber zeigt Abbildung 2b, dass BACnet-Geräte in Präfixen gleichmäßiger verteilt sind als in ASen.

Tabelle 5 zeigt die fünf Autonomen Systeme mit den meisten BACnet-Geräten. Alle fünf ASe gehören zu großen Telekommunikationsunternehmen in den USA und Kanada. Dies erhärtet die Vermutung, dass ein Großteil der im Internet auffindbaren BACnet-Geräte im Endkundenbereich bei der Steuerung von Gebäudeautomatisierungsgeräten im Einsatz ist. Fast 4 von 10 dieser Geräte sind Niagara AX (19 %) und MACH-Pro (18 %) Steuereinheiten.

Zusätzlich zur Verteilung auf Subnetz- und AS-Ebene wurde im Rahmen dieser Analyse noch die geographische Verbreitung von BACnet-Geräten untersucht. Dazu wurden die IP-Adressen von antwortenden Geräten mit der Ortsbestimmungsdatenbank *IP2Location* [1] auf Länder abgebildet.

Tabelle 6 zeigt die Länderverteilung der in dieser Untersuchung gefundenen BACnet-Geräte. Diese werden den von Durumeric et al. gefundenen Modbus-Geräten [12] gegenübergestellt. Da beide Protokolle für die Kommunikation mit Steuergeräten im Einsatz sind, könnte eine ähnliche Verteilung angenommen werden. Abgesehen davon, dass bei beiden Protokollen die meisten Geräte in den USA gefunden werden, sind die Verteilungen unterschiedlich. Bei BACnet-Geräten stehen in den USA und in Kanada zusammen schon mehr als 80 % aller Geräte. Der Drittplatzierte Frankreich kommt in der BACnet-Verteilung nur noch auf 2,4 %. Die Verteilung von Modbus-Geräten hingegen ist ausgeglichener. Obwohl auch dort die USA mit über 24 % dominieren, sind die weiteren Ränge weitaus weniger stark abgestuft. Deutschland taucht weder bei BACnet noch bei Modbus in den Top 10 auf. Wir finden in unseren Untersuchungen 78 BACnet-Geräte in Deutschland.

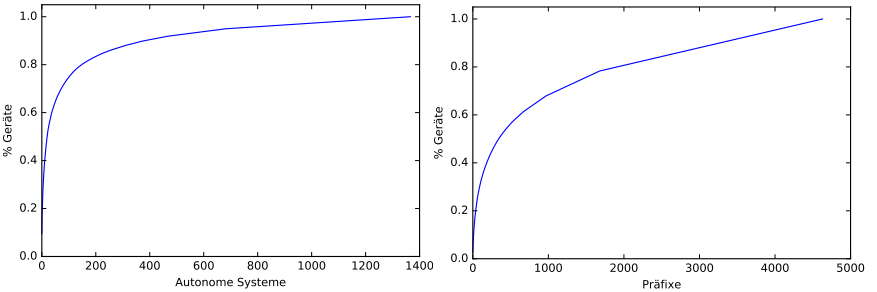
Abbildung 3 zeigt die geographische Verteilung von BACnet-Geräten auf einer Weltkarte, Länder mit BACnet-Geräten sind eingefärbt. Die Grafik zeigt eine Erreichbarkeit von BACnet-Geräten in einem Großteil industrialisierter Länder.

4.5 BACnet-Geräte im DFN

Da BACnet-Geräte in über 13 000 Autonomen Systemen gefunden werden, untersuchen wir, ob diese auch im Deutschen Forschungsnetz (DFN) zu finden sind. Dafür identifizieren wir zuerst die ASe, die ans DFN angebunden sind. In diesen ASen finden wir insgesamt nur fünf BACnet-Geräte, allesamt im selben Universitätsnetzwerk.

Im Vergleich mit dem Rest des Internets schneidet das DFN gut ab: Auf 1 Million IP-Adressen kommen im DFN 0,41 BACnet-Geräte. Im Rest des Internets ist diese Zahl mit 4,82 mehr als zehn Mal so hoch.

Das DFN ist ein besonderes Netz, da es eine Reihe von Universitäten und Forschungseinrichtungen verbindet. BACnet-Geräte sind vor allem in Netzen großer nordamerikanischer Telekommunikationsanbieter wie AT&T zu finden. DFN-Nutzer scheinen BACnet entweder weniger zu verwenden oder bei der Verwendung besser abzusichern.



(a) AS-Verteilung (b) Subnetz-Verteilung

Abbildung 2: Kumulative Verteilung von BACnet-Geräten in Netzbereichen.

Tabelle 5: Top 5 Autonome Systeme nach Anzahl von BACnet-Geräten.

Pos	ASN	Autonomes System	Organisation	Vorkommen	Häufigkeit
1	7018	ATT-INTERNET4	AT&T Services, Inc.	1291	9,5 %
2	7922	COMCAST-7922	Comcast Cable Communications, Inc.	1082	8,0 %
3	22394	CELLCO	Cellco Partnership DBA Verizon Wireless	522	3,8 %
4	852	ASN852	TELUS Communications Inc.	486	3,6 %
5	6327	SHAW	Shaw Communications Inc.	348	2,6 %

Tabelle 6: Länderverteilung von BACnet- und Modbus-Geräten.

(a) BACnet-Geräte.

Pos	Land	Vorkommen [%]
1	USA	62,2
2	Kanada	18,5
3	Frankreich	2,4
4	Spanien	2,2
5	Australien	1,8

(b) Modbus-Geräte [12].

Pos	Land	Vorkommen [%]
1	USA	24,7
2	Spanien	7,6
3	Italien	6,4
4	Frankreich	6,0
5	Türkei	4,6

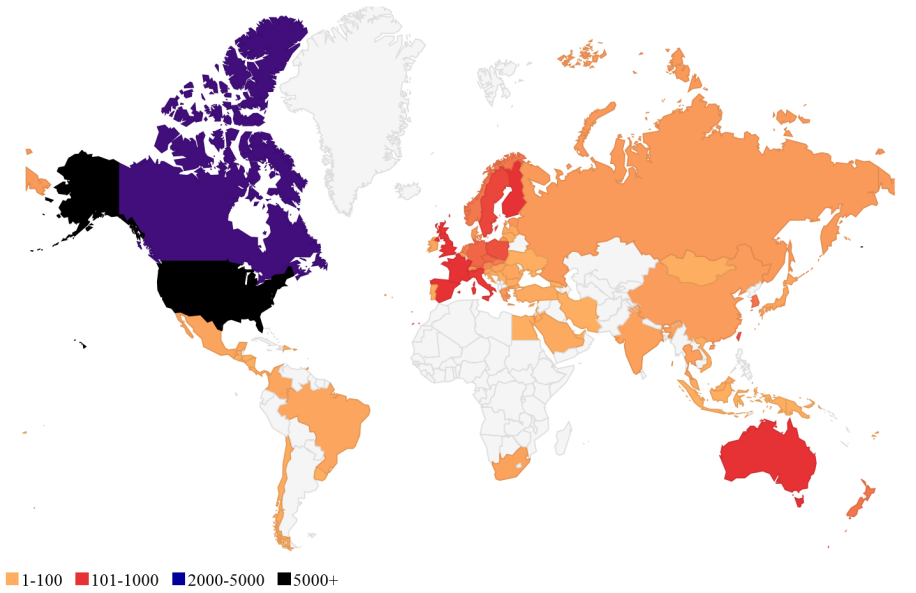


Abbildung 3: Geographische Verteilung von BACnet-Geräten (erstellt mit Google Charts)

5 BACnet für Amplification-Angriffe

Im folgenden Abschnitt wird untersucht, inwiefern das BACnet-Protokoll für Amplification-Angriffe missbraucht werden kann.

Die *ReadPropertyMultiple*-Abfrage des BACnet-Protokolls erlaubt die Abfrage mehrerer Eigenschaften, wobei auch die gleiche Eigenschaft wiederholt abgefragt werden kann. Durch die umfangreichen Antworten kann dadurch ein hoher Amplification-Faktor erreicht werden. Zur Validierung dieser Möglichkeit wählen wir eine kleine Testgruppe von 10 Geräten, um wenige Geräte mit der hohen Netz- und Rechenlast solcher *ReadPropertyMultiple*-Abfragen zu belasten. Von den 10 abgefragten Geräten antworten alle auf die *ReadPropertyMultiple*-Abfrage, 2 sogar mit mehreren Paketen. Die daraus resultierenden Amplification-Faktoren reichen von 4,5 bis 30,9, mit 11,5 als Durchschnitt. Dieser Amplification-Faktor ist geringer als bei DNS, wo im Durchschnitt ein Faktor von 40 erreicht wird [28].

Die Stichprobe bestätigt das oben erläuterte Problem und gibt einen durchschnittlichen Amplification-Faktor an. Zu beachten ist, dass vermutlich außer-

halb unserer Stichprobe noch Geräte existieren, die noch höhere Amplification-Faktoren bieten. Zudem kann durch Experimentieren mit mehreren Eigenschaften leicht ein Maximalwert pro Gerät ermittelt werden. Dieser ist konfigurationsabhänging, da sich der Amplification-Faktor primär aus der Byte-Länge des zurückgegebenen Feldwertes berechnet.

Durch diese Lücke gewinnen öffentlich erreichbare BACnet-Installationen weitere Relevanz für Angreifer, die diese als Reflektoren nutzen wollen.

5.1 Erkennung und Vermeidung von BACnet-basierten Distributed Reflection Denial-of-Service (DRDoS)

Bei der Erkennung und Vermeidung von Amplification-Angriffen gelten zunächst die generellen Regeln für BACnet-Geräte, wie diese in Abschnitt 6.3 vorgestellt werden. Diese umfassen primär den Betrieb in VPNs oder abgekoppelten Netzen. Unabhängig davon diskutieren wir Maßnahmen, um die spezifische Amplification-Anfälligkeit zu erkennen und zu beheben. Im Rahmen der BACnet-Standardisierungsarbeit kann die *ReadPropertyMultiple*-Abfrage anders definiert werden, um das wiederholte Abfragen derselben Eigenschaft im selben Paket nicht zu erlauben. Diese Änderung würde den möglichen Amplification-Faktor bereits deutlich senken. Eine weiterführende Änderung wäre, der gegen Amplification-Anfälligkeit oft angeführte Vorschlag, die Anfragen gleich groß wie die erwartete Antwort zu gestalten. Dadurch kann der Amplification-Faktor bis auf 1 gesenkt werden.

Außerdem können an Netzübergängen verschiedene Maßnahmen zur Erkennung und Unterdrückung von Amplification-Angriffen getroffen werden. So können *ReadPropertyMultiple*-Abfragen in einem ersten Schritt entweder ganz unterbunden oder zumindest wiederholte Abfragen derselben Eigenschaft blockiert werden. Weiter möglich sind Rate-Limiting-Ansätze, die den Schaden möglicher Angriffe stark reduzieren können. Zusätzlich zum Amplification-Faktor könnte die Ähnlichkeit von Paketen für die Erkennung von Angriffen verwendet werden [31].

6 Verwandte Arbeiten

In diesem Abschnitt werden verwandte Arbeiten in den Gebieten Internetweite Scans, Amplification-Angriffe und BACnet-Sicherheit vorgestellt.

6.1 Internet Scanning

Durumeric et al. stellen mit Censys eine offene Plattform für Internet-Scans zur Verfügung und haben für 16 Protokolle ihre Ergebnisse im Jahr 2015 ausgewertet [12]. Als industrielles Protokoll wird Modbus betrachtet, das unter anderem auch für Heizungs-, Lüftungs- und Klimatechniksysteme verwendet wird. Wir vergleichen unsere Ergebnisse mit den Modbus-Ergebnissen von Durumeric et al. und finden, dass BACnet-Geräte sehr viel ungleichmäßiger auf Länder verteilt sind als Modbus-Geräte.

Rapid7 führt im Rahmen von Project Sonar [26] unter anderem Scans auf das BACnet-Protokoll durch, hat aber keine Analysen dazu veröffentlicht.

Li et al. [19] haben 2016 die Effektivität von Benachrichtigungen über Schwachstellen betrachtet. Im Rahmen dieser Studie wurden industrielle Kontrollsysteme über Scans identifiziert. Konkret wurden die Protokolle DNP3, Modbus, BACnet, Tridium Fox und Siemens S7 abgedeckt. Die Autoren teilten die 45 770 zu benachrichtigenden Systeme in verschiedene Gruppen ein, die auf unterschiedliche Weisen benachrichtigt wurden. Die Studie differenziert zwischen benachrichtigten Partei, also WHOIS Kontakten, National CERT oder US-CERT und Informationsgehalt der Nachricht. Das Ergebnis war, dass Nachrichten an WHOIS Kontakte mit dem hohem Detaillierungsgrad die größte Erfolgsquote aufwiesen. 11 % der auf diese Weise adressierten Parteien haben ihre Sicherheitslücken geschlossen.

Aus den Arbeiten von Durumeric et al., Project Sonar und Li et al., sowie aus unseren eigenen Ergebnissen geht hervor, dass eine substanzielle Anzahl von Kontrollsystemen ungeschützt über das Internet erreichbar sind.

6.2 Ausnutzbarkeit des Protokolls für Amplification-Angriffe

Rossow [28] hat im Jahr 2014 eine Vielzahl von UDP-Protokollen auf ihre Ausnutzbarkeit für Amplification-Angriffe evaluiert. Dabei wurde unter anderem ein Amplification-Faktor bestimmt, geprüft wieviele Geräte erreichbar sind und wie schnell ein Angreifer eine relevante Anzahl von Reflektoren finden kann. Zudem werden Gegenmaßnahmen wie netzbasierte Paketfilterung oder Überarbeitung des Protokolls vorgeschlagen. Wir erweitern die Liste von angreifbaren Protokollen um BACnet, welches als dediziertes Protokoll für Gebäudeautomatisierung, anders als etwa DNS und NTP, nicht im öffentlichen Internet verfügbar sein muss.

6.3 Isolation von Systemen und Netzwerken

Für den Bereich der industriellen Kontrollsysteme geben Stouffer et al. [29] einen sehr guten Überblick über Anforderungen dieser Netzwerke. In seiner Arbeit werden mögliche Netzarchitekturen besprochen. Der einfachste und effektivste Schritt bei der Absicherung von Kontrollsystemen ist dabei, dem ursprünglichen Sicherheitskonzept einer isolierten Verkabelung auch auf IP-Schicht möglichst gut nachzukommen. Zentraler Bestandteil hierbei sind vertrauenswürdige Zellen zur Isolation der Geräte von anderen Netzwerken, wie etwa einem Büro-Netzwerk, öffentlichem WLAN oder dem Internet. Wichtig ist hierbei auch der physische Schutz gegen unberechtigten Zugang an Leitungen und Endgeräten.

Auch Neilson von ASHRAE [21] fordert die komplette Netzisolation eines BACnet-Netzwerks und geht sogar so weit, dies als die grundlegende Annahme vor jeglicher anderen Absicherung vorauszusetzen. Die Verbindung von mehreren Standorten soll nur über VPN gesicherte Verbindungen realisiert werden. Für Fernwartungszwecke schlägt Neilson vor, den Zugriff neben der VPN-Absicherung noch durch einen besonders gehärteten Jumphost abzusichern. Als weiteren Angriffsvektor sieht er Insiderangriffe auf das Kontrollnetzwerk, da von jedem Gerät oder Netzanschluss ein Angriff ausgehen kann. Erst hier kommen aus seiner Sicht die weiteren Sicherheitsmaßnahmen wie starke Passwörter, das Einspielen von Sicherheitsupdates oder Sabotage-Alarme ins Spiel.

Die Wichtigkeit der Abschottung von Netzabschnitten sowie der präzisen Absicherung von Fernwartungszugängen wurde durch den millionenfachen Diebstahl von Kreditkartendaten in der US-Kaufhauskette Target unterstrichen. Bei diesem Angriff waren gestohlene Zugangsdaten eines Heating, Ventilation and Air-Conditioning (HVAC)-Unternehmens der erste Schritt [18, 27].

Gleichwohl Kapitel 24 des BACnet-Standards [2] Sicherheitsmechanismen für Integrität, Vertraulichkeit und Authentisierung beschreibt, geht aus einer Publikation von Newman [22] hervor, dass keine dieser Mechanismen derzeit in kommerziell verfügbaren Produkten umgesetzt sind.

6.4 Überwachung eines BACnet Netzwerks

Celeda et al. [8] veröffentlichten 2012 eine Studie zur Flow-basierten Überwachung im Bereich Gebäudeautomatisierung. Hierbei soll eine Analyse des Datenflusses eine frühzeitige Erkennung von Anomalien im Netzwerk ermöglichen. Durch die Erweiterung des Tools BACnetFlow gelang es den Forschern

sowohl Scans, als auch Spoofing und DoS Angriffe zu identifizieren.

Kaur et al. [17] analysierte 2015 die Möglichkeit BACnet-Netzwerke durch einen „Snort-Based Normalizer“abzusichern. Hierzu wurde ein BACnet-Testbed mit mehreren virtuellen Maschinen aufgebaut von denen jede ein BACnet-Gerät repräsentierte. Wie sich herausstellte, war es dem Normalizer tatsächlich möglich zwischen konformem und nicht konformem BACnet-Datenfluss zu differenzieren.

Caselli et al. [7] evaluieren in zwei BACnet-Netzwerken der Universität Twente und des Lawrence Berkeley National Laboratory ihr System zur Erkennung von Angriffen. Sie beobachten mit einem für Bro selbst entwickelten BACnet-Parser das Netzwerk und reichern Informationen zu entdeckten BACnet-Geräten automatisiert mit Informationen aus Herstellerinformationen und einem standardisierten Dokumentationsformat an. Daraus leiten sie automatisiert Regeln für Alarme ab und konnten so eine Fehlbedienung erkennen.

7 Zusammenfassung und Ausblick

Wir haben mit aktiven Scans über 13 000 BACnet-Geräte im Internet gefunden. Wir finden eine starke topologische und geographische Konzentration, bei der ein Großteil der Geräte in wenigen Autonomen Systemen und Ländern verteilt sind. Diese Konzentration scheint mit dem Einsatz von BACnet-Geräten zur Gebäudeautomatisierung in den Netzen großer Internetdienstanbieter zusammenzuhängen. Gleichzeitig verteilt sich der Rest der Geräte über den Großteil der industrialisierten Länder. Weiter haben wir die Anfälligkeit von BACnet für Amplification-Angriffe mit einem Faktor von über 30 ermittelt sowie Abwehrmaßnahmen diskutiert.

Zukünftige Arbeiten können die systematische Benachrichtigung der Betreiber ungesicherter BACnet-Geräte umfassen. Ebenso erscheint eine weitere Analyse der Einsatzmuster von BACnet-Geräten im Internet vielversprechend, beispielsweise wie oft diese in Dial-Up-Netzen oder Unternehmensnetzen betrieben werden.

Danksagung: Wir bedanken uns bei den Gutachtern des Programmkomitees für das hilfreiche Feedback. Diese Arbeit wurde im Rahmen der BMBF-Projekte X-CHECK (Kennzeichen 16KIS0530) und AutoMon (Kennzeichen 16KIS0411) gefördert.

Literatur

[1] ip2location Country Database. https://www.ip2location.com, August 2016.

[2] BACnet – A Data Communication Protocol for Building Automation and Control Systems. Standard, ASHRAE/ANSI, 1995.

[3] BACnet International. *Introduction to BACnet for Building Owners and Engineers*, 2014.

[4] A. Bartholemy and W. Chen. An Examination of Distributed Denial of Service Attacks. In *International Conference on Electro/Information Technology (EIT)*. IEEE, 2015.

[5] K. Bhargavan and G. Leurent. Transcript collision attacks: Breaking authentication in TLS, IKE, and SSH. In *Network and Distributed System Security Symposium (NDSS)*, Februar 2016.

[6] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry. Attacks Against Process Control Systems: Risk Assessment, Detection, and Response. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, 2011.

[7] M. Caselli, E. Zambon, J. Amann, and R. Sommer. Specification Mining for Intrusion Detection in Networked Control Systems. In *25th USENIX Security Symposium*, 2016.

[8] P. Celeda, R. Krejci, and V. Krmicek. Flow-based Security Issue Detection in Building Automation and Control Networks. In *UNICE 2012: Information and Communication Technologies*, 2012.

[9] Center for Applied Internet Data Analysis. Routeviews Prefix to AS mappings Dataset. http://www.caida.org/data/routing/routeviews-prefix2as.xml (aufgerufen am 21.08.2016).

[10] J. Czyz, M. Kallitsis, M. Gharaibeh, C. Papadopoulos, M. Bailey, and M. Karir. Taming the 800 Pound Gorilla: The Rise and Decline of NTP DDoS Attacks. In *Proceedings of the 2014 Conference on Internet Measurement Conference*, IMC '14, 2014.

[11] Z. Drias, A. Serhrouchni, and O. Vogel. Taxonomy of Attacks on Industrial Control Protocols. In *2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS)*, Juli 2015.

[12] 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*. ACM, 2015.

[13] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, et al. The Matter of Heartbleed. In *Proceedings of the 2014 Conference on Internet Measurement Conference*.

[14] Z. Durumeric, E. Wustrow, and J. A. Halderman. ZMap: Fast Internet-wide Scanning and Its Security Applications. In *22nd USENIX Security Symposium*, 2013.

[15] B. Fogel, S. Farmer, H. Alkofahi, A. Skjellum, and M. Hafiz. POODLEs, More POODLEs, FREAK Attacks Too: How Server Administrators Responded to Three Serious Web Vulnerabilities. In *Proceedings of the 8th International Symposium on Engineering Secure Software and Systems*, ESSoS '16. Springer, April 2016.

[16] O. Gasser. bacnet.py GitHub-Repository. `https://github.com/tumi8/bacnet.py`, 2016.

[17] J. Kaur, J. Tonejc, S. Wendzel, and M. Meier. Securing BACnet's Pitfalls. In *30th IFIP TC 11 International Conference on ICT Systems Security and Privacy Protection*. Springer, Mai 2015.

[18] B. Krebs. Target Hackers Broke in Via HVAC Company. `http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/` (aufgerufen am 21.08.2016), 2014.

[19] 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*, Austin, TX, 2016. USENIX Association.

[20] A. P. Mathur and N. O. Tippenhauer. SWaT: a water treatment testbed for research and training on ICS security. In *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*. IEEE, 2016.

[21] C. Neilson. Securing a Control Systems Network. *ASHRAE Journal*, 55(11), 2013.

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

[23] A. Pras, J. J. Santanna, J. Steinberger, and A. Sperotto. DDoS 3.0 - How Terrorists Bring Down the Internet. In *17th International GI/ITG Conference on Measurement, Modelling and Evaluation of Dependable Computer and Communication Systems*, 2016.

[24] M. Prince. The DDoS That Almost Broke the Internet. `https://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet` (aufgerufen am 21.08.2016), März 2013.

[25] M. Prince. Technical Details Behind a 400Gbps NTP Amplification DDoS Attack. `https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/` (aufgerufen am 21.08.2016), Februar 2014.

[26] Rapid7 Labs. Project Sonar. `https://sonar.labs.rapid7.com/`.

[27] J. Rockefeller. A “Kill Chain” Analysis of the 2013 Target Data Breach. Statement to the U.S. Senate, Committee on Commerce, Science and Transportation, März 2014.

[28] C. Rossow. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. In *Network and Distributed System Security Symposium (NDSS)*, 2014.

[29] K. Stouffer, J. Falco, and K. Scarfone. Guide to Industrial Control Systems (ICS) security. *NIST special publication*, 800(82), 2011.

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

[31] F. von Eye, T. Böttger, H. Reiser, L. Braun, O. Gasser, and G. Carle. Detektion und Prävention von Denial-of-Service Amplification Attacken – Schutz des Netzes aus Sicht eines Amplifiers. In *22. DFN-Konferenz: Sicherheit in vernetzten Systemen*, Norderstedt, Deutschland, Februar 2015.