Survey: Security in Smart Building Networks

Michaela Mohl
Betreuer: Holger Kinkelin
Seminar Future Internet SS2014
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik, Technische Universität München
Email: mohl@in.tum.de

KURZFASSUNG

Heutzutage werden vor allem bedeutende, industrielle Gebäude und jene mit infrastruktureller Wichtigkeit immer weiter automatisiert. Das Ziel dieser Gebäudeautomatisierung ist es, durch Automatisierung Gebäude zu konstruieren die sicherer, ökologischer und komfortabler sind. Zu Begin des Einsatzes waren dies in der Regel geschlossene Autonome Systeme. Diese konnten nur durch direkt vor Ort manipuliert werden.

Durch die Verbreitung von Gebäudeautomationssystemen und des Internets hat sich der Trend dahingehend entwickelt, dass sogar Systeme dieser Art durchgehend vernetzt werden. Beispielsweise könnten verschiedene Gebäude einer Firma so verbunden werden, dass Fernzugriffe ermöglicht werden. Optional ist diese Verbindung durch Anschluss an das Internet realisierbar. Dadurch eröffnen sich jedoch Problemstellen und Gefahren, die das Netzwerk im Gegenzug zu den anfangs geschlossenen Systemen unsicherer machen.

Das Ziel dieser Arbeit ist es, die Sicherheitslücken zu präsentieren und Lösungsmöglichkeiten für den Schutz zu analysieren. Dies wird anhand einer Einführung in den Aufbau von Gebäudeautomationssystemen und in einen der Marktführer BACnet dargestellt. Um sich vor Angriffen schützen zu können, müssen die potentiellen Angreifer bekannt sein. Diese werden mit ihren Angriffsarten erörtert.
Zudem werden Sicherheitseigenschaften von verschiedenen Gebäudeautomationssystemen, BACnet, KNX und LonWorks, beschrieben und verglichen.
Im Rahmen der Arbeit wird sich herausstellen, dass BACnet seiner Konkurrenz im Punkt Sicherheit deutlich voraus ist und vor allem einen individuelleren Schutz ermöglicht.

Schlüsselworte

BACnet, Security, Smart Building Networks, Building Automation Systems, BAS, KNX, LonWorks, LonTalk

1. EINLEITUNG

Bedeutungsvolle Gebäude, wie zum Beispiel Flughäfen, nutzen seit längerem Gebäudeautomationssysteme. Früher waren diese Systeme nur direkt vor Ort an der Arbeitsstation manipulierbar. Illegaler Zugriff lies sich durch Restriktion authorisierter Personen einschränken.

Heutige Gebäudeautomationssysteme werden zunehmend vernetzt. Es könnten beispielsweise alle Systeme deutscher Flughäfen verbunden werden. Alternativ könnte auch ein Fernzugriff auf einen Flughafen ermöglicht werden.

Diese Verbindungen bergen die Gefahr des illegalen Zugriffes und der Manipulation, da die Menge der Angriffspunkte wesentlich angestiegen ist. Damals gab es nur den direkten Eingriff über die Arbeitsstation, mittlerweile hat sich dies durch die Internetanbindung vervielfacht.

Das Ausmaß eines solchen Angriffes kann enorme Schäden verursachen. Falls ein umfangreiches System in einem Flughafen angegriffen werden sollte, könnte der Angreifer beispielsweise den Feueralarm aktivieren und gleichzeitig alle automatischen Türen verriegeln. Dies könnte im schlechtesten Fall zu einer Massenpanik führen und Menschenleben gefährden.

Um die Problemfelder eines Gebäudeautomationssystems zu erkennen, muss dessen Struktur bekannt sein. Dies wird anfänglich veralgemeintert in Kapitel Zwei erklärt, danach in Kapitel Drei gibt es detallierte Erläuterung von dem Marktführer BACnet.

In Kapitel Vier werden die potentiellen Angreifer und Angriffsarten analysiert, zudem, in Kapitel Fünf und Sechs wird der Schutz, drei gängiger Gebäudeautomationssysteme gegen Angriffe betrachtet und verglichen.

2. SMART BUILDING NETWORKS

Das folgende Kapitel stellt eine Einführung in die Thematik dar. Beginnend wird der Begriff Smart Building Networks erläutert. Abschließend wird die Struktur von diesen dargestellt. Dies geschiet basiert auf den Quellen [1] und [2].

2.1 Smart Building Networks

Unter einem Smart Building Network oder auch der Gebäudeautomatisierung versteht man die netzwerkgestützte Regelung und Optimisierung von Heizung, Lüftung, Licht und Klimaanlage. Diese existieren in vor allem größeren und wichtigeren Industriegebäuden, können aber auch in kleineren Industrien oder sogar in Privathäusern vorgefunden werden, auch wenn sich der finanzielle Aufwand für letztere nur eingeschränkt lohnt.

2.1.1 Struktur eines Smart Building

Ein Gebäudeautomationssystem kann in drei logische Ebenen aufgeteilt werden. Hierbei wird zwischen Rolle und Verantwortlichkeit getrennt. Die folgende Erklärung erfolgt

doi: 10.2313/NET-2014-08-1_09

anhand der Grafik [1] und beginnt mit der untersten Ebene.

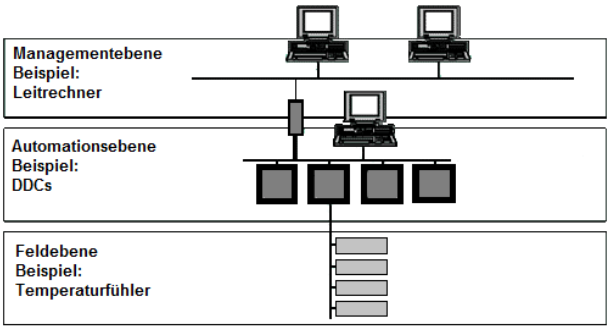

Abbildung 1: Die Ebenen [2]

- Feldebene

  Die Feldebene besteht aus simplen Sensoren, beispielsweise Temperaturmessgeräten, und Aktoren, wie Heizungsventilen. Diese sammeln Informationen, welche an die Automationsebene weiter geleitet wird. Sie können aber auch Befehle aus der darüberliegenden Ebene erhalten und diese ausführen. Beispielsweise kann auf oberen Ebenen der Befehl "Alle Lichter sollen um 19 Uhr ausgeschalten werden" implementiert sein, dies wird dann auf den unteren Ebenen ausgeführt.

- Automationsebene

  Bei der Automationsebene handelt es sich um eine Zwischenebene, die die Daten der Feldebene evaluiert und die verarbeiteten Informationen an die übergeordnete Ebene in Echtzeit weiterleitet. Mit den Direct-Digital-Controls (DDCs)[1] wird es ermöglicht, mehrere Feldgeräte zusammenzufassen, um komplexere Befehle auszuführen und mehr Daten zu sammeln, die miteinander einen höheren Informationsgehalt erzielen. Beispielsweise können an diesen DDC mehrere Lichtschalter angeschlossen werden, um einmalig die Lichter mit einem Befehl zu löschen. Auf dieser Ebene befindet sich in der Regel ein BUS, der den Leitrechner der übergeordneten Ebene mit den Direct-Digital-Controls aus dieser Ebene verbindet.

- Managementebene

  Die Managementebene ist übergeordnet und verantwortlich für die Betriebsführung, Meldeüberwachung und das Energiemanagement. Sie übernimmt eine organisierende Rolle. Beispielhaft könnte ein Gebäudeautomationssystem derart aufgebaut sein, dass ein oder mehrere Leitrechner übergeordnete Funktionen übernehmen, welche durch die Managementebene realisiert wird. Ein Leitrechner ist ein System, welches alle Informationen der untergeordneten Ebenen sammelt und reguliert. Dieses stellt eine Schnittstelle zur Interaktion mit Menschen dar.

[1] Direct-Digital-Controls sind Computerähnliche Module die eine Menge von Feldgeräte verbinden und Informationen in Echtzeit weiterleiten.

3. BACNET

Alle Informationen aus diesem Kapitel über BACnet entstammen den Quellen [1], [2], [3] und [4].

BACnet (***B**uilding **A**utomation and **C**ontrol **Net**works*) ist ein Datenkommunikationsprotokoll für Gebäudeautomatisierung und deren Kontrollnetzwerke.

Dieses Protokoll wurde von der ***A**merican **S**ociety of **H**eating, **R**efrigerating and **A**ir-Conditioning **E**ngineers* (ASHRAE) ab 1987 entwickelt. Ihr Ziel war ein Standardprotokoll für die Gebäudeautomatisierung zu etablieren, welche mit der BACnet ISO-Norm 16484-5 im Jahr 2003 erfolgreich umgesetzt wurde.

3.1 BACnet Konzept

Aufgrund der Notwendigkeit, die unterschiedlichen Komponenten in einem Gebäude mit einem standardisierten Kommunikationsprotokoll ansprechen zu können, entstand BACnet. Hierbei sollten Interoperabilität und Herstellerunabhängigkeit gewährleistet werden.

BACnet ist ein Gebäudeautomatisierungssystem, das sich problemlos in die drei gerade genannten Ebenen eingliedern lässt. Es hat übergeordnete Dienste, die es anbietet, und sogenannte Objekte, die Element des Systems sein können wie beispielsweise ein Feldgerät. Diese Dienste werden im Weiteren erklärt.

Für alle drei Ebenen kann BACnetals Software verwendet werden. Jedoch zeigt BACnet seine Stärken im Einsatz auf den beiden übergeordneten Ebenen, der Automationsebende und der Managementebene, weshalb es zum Großteil nur hier benutzt wird. In diesen Fällen kann BACnet mit einem anderen System, beispielsweise LonWorks oder KNX, auf der Feldebene zusammenarbeiten.

3.1.1 Dienste

BACnet bietet 38 Dienste an, die in die folgenden sechs Klassen eingeordnet werden können:

- Objektzugriff

  Diese Dienstklasse beinhaltet typische Ein- und Ausgabeoperationen wie Lesen und Schreiben. Außerdem sollen Objekte damit angelegt und gelöscht werden können.

- Device- und Netzwerkmanagement

  Dem Betreiber wird es durch diese Funktionen ermöglicht, einen automatischen Neustart mit Standardkonfigurationen des Netzwerks durchzuführen.

- Alarm- und Eventfunktionen

  Wenn ein BACnet Device Alarmzustände, Betriebszustände oder eine Form von Fehlerzustand erkennt, so werden diese von den Alarm- und Eventdiensten behandelt. Ein BACnet Gerät verfügt über drei Zustände: "*normal*", "*offnormal*" und "*fault*".

- Remote Device Management

  Dies ermöglicht Fernzugriffe auf verschiedene Eigenschaften. Beispielsweise kann ein Gerät damit neu

doi: 10.2313/NET-2014-08-1_09

gestartet werden. Darunter fallen noch zwei weitere spezielle Dienste, nämlich das *Dynamic Device Binding*, welches erlaubt, Geräte per Broadcast zu ermitteln, und das *Dynamic Object Binding*, das es ermöglicht, Objekte dynamisch zu ermitteln.

- Virtual Terminal

  Das Virtual Terminal wird eher selten verwendet. Dieses ist für das Nutzen einer virtuellen Schnittstelle des Gerätes geeignet.

- Netzwerk-Sicherheit

  Es können individuell Sichheitsmechanismen eingefügt werden, welche im Kapitel [5] "Sicherheit im BACnet" näher erläutert werden.

Wichtig sind diese Informationen zu den Diensten deshalb, da all diese eine Angriffsmöglichkeit auf das System bieten. Dieser Dienstmissbrauch muss unterbunden werden. Zum einen könnte das System direkt manipuliert werden, indem beispielsweise ein Objekt gelöscht wird. Zum anderen wäre ein nicht erkannter Eingriff möglich, der später die Fernzugriffsdienste ausnutzen könnte.

3.1.2 Schichten

BACnet nutzt das OSI-Modell als Referenzmodell. Auf den untersten zwei Schichten, der Bitübertragungs- und der Sicherungsschicht, wird BACnet nicht verwendet. Hier werden andere Protokolle, wie zum Beispiel LonTalk, eingesetzt.

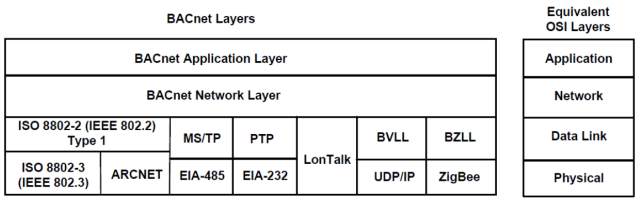

Abbildung 2: Die BACnet Schichten im Vergleich zum OSI Model [4]

Die Transport-, Sitzungs- und Darstellungsschicht, also Schicht 4-6 im OSI-Modell, beziehungsweise deren Funktionen sind, soweit erforderlich, in die BACnet-Anwendungsschicht mit integriert.

4. SICHERHEITSASPEKTE IN DER GEBÄUDEAUTOMATION UND BACNET

Es gibt zwei Gründe warum Gebäudeautomationssysteme grundsätzlich geschütz werden sollten.
Auf der einen Seite möchte man wertvolle Informationen versteckt halten, auf der anderen Seite sollen unterstützte Funktionen nicht missbraucht werden.

Das bedeutet, dass alle Informationen, über die das System verfügt, nur authorisierten Personen zur Verfügung stehen darf. Beispielhaft könnte ein Gebäudeautomationssystem mit einer Datenbank verbunden sein, die mit sensiblen Daten versehen ist oder gar selbst vertrauliche Daten sammelt. Diese sollten unter keinen Umständen von Dritten eingesehen oder abgehört werden.

Auch lässt sich erklären, wieso der Missbrauch von Funktionen vermieden werden muss. Das Eingangsbeispiel aus der Einleitung ist einleuchtend. Kein unbefugter Dritter darf Zugriff auf die Türenverriegelung und den Feueralarm eines Flughafens haben, da ansonsten eine Panik nach Belieben verursacht werden kann. Der Normalzustand des Flughafens wäre nicht mehr gewährleistet.

In diesem Kapitel werden die potentiellen Angreifer und die möglichen Angriffsarten, basierend auf den Quellen [5], [6] und [7], für ein Gebäudeautomationssystem diskutiert.

4.1 Die Angriffe

Um ein System dieser Art gegen unerwünschte Eingriffe von Außen zu schützen, muss bekannt sein, welche Angriffspunkte das System aufgrund ihrer Dienste anbietet und welche Arten von Angriffen, die damit einhergehen, existieren können.

4.1.1 Die Angreifer

Neben dem klassischen **Hacker** gibt es noch drei weitere Personengruppen, die in den Betracht kommen sollten, falls versucht wird, potentielle Angreifer eines Gebäudeautomationssystems zu klassifizieren.

- Kriminelle

  Hierunter lassen sich Terroristen oder Diebe beispielsweise aufzählen, die sich Zugang zum System verschaffen möchten, um ein poltisches Statement zu bewirken.

- Ehemalige Mitarbeiter

  Verschiedene Berichte [5] zeigen, dass verärgerte, ehemalige Mitarbeiter zu einer ernsthaften Bedrohung gehören. Das liegt vor allem daran, dass diese Personen in der Regel ein grundsätzliches Verständnis über das Systems besitzen, welches sie aus Frust im Affekt ausnutzen könnten, um Schaden anzurichten.

- Konkurrenz

  Die Überwachung eines Gebäudeautomationssystems der Konkurrenz könnte für Unternehmensforschung und Optimierung genutzt werden.

Generell lässt sich sagen, dass es wichtig ist, dass grundlegende Sicherheitsmechanismen existieren sollten. Da die Anzahl der Gefahrenquellen beachtlich ist, sollte das System zumindest in der Lage sein, Sicherheitsmechanismen im Nachhinein hinzuzufügen und auszuführen.

4.1.2 Die Attacken

Es existiert eine breite Menge von Attackarten, die im Folgenden diverenziert werden. Diese unterscheiden sich grundsätzlich nicht von klassichen Attacken, im Folgenden wird jedoch der Zusammenhang mit BACnet und Gebäuteautomationssystemen beschrieben.

- Passwort-Attacken

  Durch Raten oder durch Brute-Force wäre es möglich, den unauthorisierten Zugriff auf eine Arbeitsstation zu

doi: 10.2313/NET-2014-08-1_09

gewinnen. Arbeitsstationen in diesem Zusammenhang sind (Leit-)Rechner, die sich verteilt in den zwei oberen logischen Ebenen befinden können.
Aufgrund dieser Passwort-Attacken sollte in Gebäudeautomationssystemen den Nutzern ein Autorisationsdienst angeboten werden, der einen gesicherteren Zugang zum System ermöglicht.

- Denial of Service

  Eine Dienstverweigerung durch Überlastung des Systems existiert auch in der Gebäudeautomatisierung. Dies geschieht durch eine unüberwindbare Menge unnützer Nachrichten.
  BACnet und LonWorks sind relativ anfällig für diese Art von Angriffen, da beide Systeme mit invaliden oder leeren Nachrichten an die Grenze ihrer Kapazitäten gebracht werden können.

- Spoofing Attacken

  Es exisitiert eine Vielzahl von Möglichkeiten, wie innerhalb eines BACnet-Systems gespooft werden könnte. Unter dem Spoofing-Angriff wird von einer fälschlichen Kommunikation ausgegangen, indem der Angreifer sich dem Kommunikationspartner gegenüber als eine bekannte Identität ausgibt, um damit Informationen zu erhalten, die er unter anderen Umständen nicht gewinnen könnte. Nur die Authentifikation sicherer BACnet-Nachrichten kann dies unterbinden.

- Abhörattacken, Snooping und Port-Scanning

  Abhörattacken sind lohnenswert für Diebe, um beispielsweise Informationen über den Zustand der Sicherheitseinrichtungen des Gebäudes zu gewinnen, was bei einem physikalischen Einbruch in das Gebäude zum Vorteil der Einbrecher führen würde. BACnet ist aufgrund seiner Struktur anfällig gegenüber Attacken dieser Art, da die simpleren Geräte im Netzwerk kaum in der Lage sind, sich eigenständig zu schützen.

- Exploit-Attacken

  Das Ausnutzen von Fehlern in der Hardware oder der Software ist einer der geringfügigeren Sicherheitsproblemen, kann jedoch zu dauerhaftem Fehlverhalten des Systems führen. Dies ist eine mögliche Angriffsart, wobei diese eher selten zu fatalen Fehlern führt. Aufgrund dessen ist dies nicht Hauptaugenmerk bei der Verteidigung von Gebäudeautomationssystemen.

Die Menge potentieller Angriffsarten ist beachtlich. Somit muss ein passender Schutz für Systeme dieser Art gefunden werden. Allerdings kann trotz der Tatsache, dass all diese Angriffsarten bekannt sind, nicht einfach bereits existierende Schutzsoftware verwendet werden, da die Struktur der Gebäudeautomationsysteme stark von der klassischen Netzwerkstruktur abweicht.

Deshalb muss ein individueller Schutz gefunden werden. Bei diesem Schutz muss darauf geachtet werden, dass alle Elemente des Systems äquivalent geschützt werden und Veränderungen unproblematisch vollzogen werden können.

4.2 Sicherheitsanforderungen

Um überhaupt eine sichere Umgebung schaffen zu können, muss ein Konzept von Sicherheitsanforderungen existieren. Um diese Bedingungen zu erfüllen, müssen zahlreiche Sicherheitsmechanismen implementiert sein.
Einer der Hauptaspekte ist hierbei, dass die übertragenen Daten geschützt werden müssen. Außerdem muss dafür gesorgt werden, dass die Managementebene vor unautho-risiertem Zugriff gesichert ist. Das letztere kann durch bekannte Authentifikationalgorithmen geschehen.
Um sicherzustellen, dass Daten unverändert übertragen werden, gibt es drei grundlegende Prinzipien, die beachtet werden müssen.

- Vertraulichkeit

  Das Offenlegen vertraulicher Daten muss in jedem Fall vermieden werden.

- Datenintegrität

  Es muss sichergestellt werden, dass Daten nicht von unauthentifizierten Dritten verändert werden. Falls dies nicht garaniert werden kann, muss zumindest auf eine Veränderung hingewiesen werden.

- Datenverbindlichkeit

  Als letztes muss garantiert werden, dass die gesendeten Daten zum aktuellen Zeitpunkt gültig sind. Dritte dürfen weder in der Lage sein, Nachrichten zu injezieren, noch diese wiederholt auszugeben.

Das sind die allgemeinen Punkte, die zu beachten sind, wenn ein Gebäudenetzwerk gegen Angriffe geschützt werden soll. Im Folgenden wird detailliert dargestellt, welche Sicherheitsmechanismen BACnet implementiert. Dies wird darauffolgend mit alternativen Lösungen konkurrierender Systeme, hier KNX und LonWorks, verglichen.

5. SICHERHEIT IM BACNET

Nun werden,anhand der Quelle [8], die Maßnahmen beschrieben, die ASHRAE einrichtet und einrichten wird, um BACnet vor unerwünschten Zugriffen zu schützen.
Der Sicherheitsaspekt war bis vor kurzem noch nicht im Augenmerk der ASHRAE. Das liegt vor allem daran, dass Gebäudeautomationssysteme erst kürzlich miteinander oder mit dem Internet verbunden wurden. Diese Verbindungen können Risiken mit sich bringen.

Grundsätzlich sollten sowohl die Anlage durch eine Firewall, als auch das Wide Area Network durch ein Virtual Private Network geschützt sein.

Fraglich ist, ob dies ausreichend ist, denn wie gut das System vor Angriffen von außen geschützt ist, liegt an vielen Details. Diese wären die Firewall-Einstellungen, Einbruchserkennung und die Überwachung der drahtlosen Zugriffe auf das interne Netzwerk.
Falls eines der oben genannten Punkte eine Schwachstelle in der Verteidigung darstellt, ist es möglich, dass das gesamte System kompromitiert wird. Ein Angreifer könnte somit Daten sammeln oder gar die Kontrolle gewinnen und die Kommunikation im System stören.

doi: 10.2313/NET-2014-08-1_09

Mit sicheren BACnet-Nachrichten wäre das BACnet-Gerät des Angreifers nicht mehr zum Datensammeln geeignet, da Nachrichten verschlüsselt sind. Desweiteren kann die Kommunikation nicht gestört werden, da das angegriffene Objekt keine gültige Nachricht verfassen kann.

Um die Schwachstellen zu schützen und BACnet generell sicherer zu machen, hat das BACnet-Komitee eine Anzahl von **Zielen** bekannt gegeben.

- Schutz aller BACnet-Geräte

  Damit keine Schwachstelle im System existiert, muss jedes BACnet-Gerät gleichwertig geschützt sein. Das heißt, dass der Overhead, die Codemenge und die zu erwartetende Leistung minimal gehalten werden muss. Erst dadurch sind auch simplere Geräte in der Lage, diese Standards zu erfüllen.

- Art von Angriffen

  Das System sollte, je nach Bedarf, vor den folgenden Angriffsarten geschützt sein: Replay, Spoofing und Denial of Service.

- Gesicherte Kommunikation innerhalb des Netzes

  Interne Netzwerkkommunikation, beispielsweise Broadcast-Nachrichten, sollten geschützt werden. Dies wird durch Signaturen und Verschlüsselung erreicht. Es soll der Advanced Encryption Standard (AES) eingehalten werden.

- Grundkonzept BACnet

  BACnet zeichnet sich durch Interoperabilität aus. Dies soll trotz Veränderungen beibehalten werden. Desweiteren ist es wünschenswert, dass diese Veränderungen leicht zu implementieren und in der Zukunft noch austauschbar sind, also interoperabel.

Handelsübliche Lösungen wie IPsec oder Kerberos führen leider nicht zu befriedigenden Lösungen, da IPsec große Overheads besitzt und beide Ansätze keine Interoperabilität zulassen.
Somit muss eine maßgeschneiderte Lösung für Gebäudeautomationssysteme gefunden werden. Wie das gestaltet werden könnte, wird im Folgenden erläutert.

5.1 BACnet-Netzwerk-Sicherheits-Architektur

Im Folgenden wird erläutert wie der Marktührer BACnet strkturiert wurde um sich gegen Angriffe zu schützen.

Damit BACnet in der Lage ist, die oben genannten Ziele umzusetzten, müssen vier sicherheitsspezifische Fähigkeiten hizugefügt werden.

Die **Geräte-Authentifizierung** wird durch das Verwenden von Nachrichten-Signaturen erreicht.

Die **Datenkapselung** wird durch geteilte Schlüssel und das Verschlüsseln von Nachrichten bewerkstelligt.

Desweiteren soll mit Hilfe geteilter Schlüssel die **Nutzer-Authentifizierung** stattfinden.

Außerdem soll eine **Nutzer-Autorisierung** eingerichtet werden.

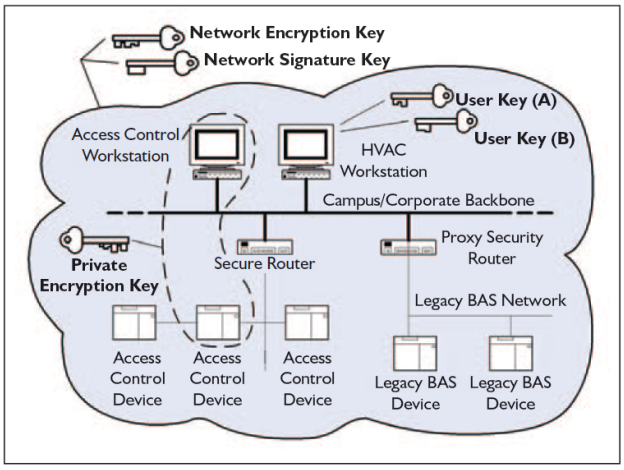

Abbildung 3: Die vier Schlüssel im BACnet [8]

Die oben gezeigte Grafik erläutert den Schlüsseleinsatz in BACnet. Die Managementebene wird hier als "Workstation" bezeichnet. Die Automationsebene wird mit dem BUS und den Routern dargestellt. Auf der Feldebene sind hier "Devices" verschiedenster Art aufgeführt. In BACnet werden vier verschiedene Schlüssel genutzt:

- Ein Signatur-Schlüssel, den sich alle Elemente in dem Netzwerk teilen. Dieser ist in der Skizze der "Network Signature Key".
- Ein Verschlüsselungs-Code, der allen im Netz bekannt ist. Dieser wird als "Network Encryption Key" bezeichnet.
- Es existieren private Verschlüsselungs-Codes, die nur eine Teilmenge der Netzwerkbeteiligten besitzen. In der Zeichnung ist ein Beispiel, wie bei der Kommunikation zwischen dem einen Access Control Device und der Access Control Workstation ein eigener "Private Encryption Key" verwendet wird.
- Als letztes gibt es noch Nutzer-Schlüssel, die eindeutig für eine Gruppe von Nutzern sind. Im Bild wären das der "User Key" A und B.

Zusammenfassend lässt sich über diese Schlüssel sagen, dass sie einen grundlegen Schutz bieten. Selbst mit dem Besitz von einem Schlüssel kann ein Eindringling nicht viel Informationen gewinnen beziehungsweise manipulieren.

Auch wenn der Eindringling den "Network Signature Key" erhält kann er nicht alle Nachrichten lesen. Da ein Teil der Nachrichten noch von einem "User Key" oder einem "Private Encryption Key" geschützt sind. Wenn jedoch ein illegaler Zugriff auf eine Arbeitsstation vorgefallen ist, kann eine Menge von Schlüsseln kompromitiert worden sein.

doi: 10.2313/NET-2014-08-1_09

5.2 Nachrichtenschutz

Da die Verschlüsselungsarchitektur nun erläutert wurde, wird anschließend noch erklärt, wie die versendeten Nachrichten verschlüsselt werden.

Im Folgenden wird beschrieben, wie ein grundlegender Schutz für BACnet-Nachrichten durch gewisse Techniken hinzugefügt werden kann.
Jede Nachricht soll mit Hilfe von HMAC und MD5 signiert werden. Außerdem sollen drei Identifikationsnummern enthalten sein, eine für die Quelle, eine für das Ziel und eine Nachrichten-ID. Zusätzlich soll noch ein Zeitstempel angehängt werden.
Durch diese zusätzlichen Informationen können bereits einfache unerwünschte Eingriffe vermieden oder zu mindest erkannt werden. Beispielsweise kann durch den Zeitstempel und die IDs Spoofing entdeckt oder sogar verhindert werden, jedoch müsste darauf geachtet werden, dass die Uhren der Geräte ungefähr gleich sind.

Weitere Schutzmechanismen können bei Bedarf hinzugefügt werden. Dies ist jedoch für diese Arbeit nicht von Belangen.

5.3 Nachrichten

Nun wird dargestellt, wie die Verschlüsselungen in eine Nachricht und den zugehöhrigen Header eingefügt werden. Zudem wird die Strukturierung der Nachricht erläutert.

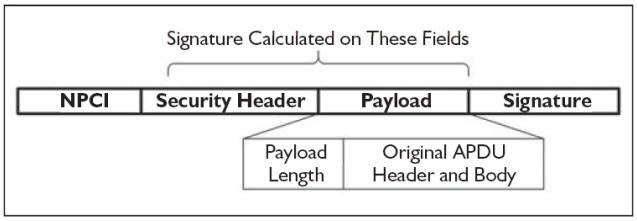

Abbildung 4: Ein Beispiel für die Sicherheitsvorkehrungen innerhalb einer Read Property Nachricht [8]

In der Abbildung 4 ist beispielsweise aufgeführt, wie eine Read Property Nachricht mit Sicherheitsvorkehrungen umhüllt wird.

Der Read Property Nachrichtenteil **A**pplication **P**rotocoll **D**ata **U**nit, ist der Inhalt der zu übertragenden Nachricht, welcher in die Payload platziert wird. Der Security Header gibt an, dass die APDU in der Payload enthalten ist.
Der eigentliche Nachrichten-Netzwerkschicht-Header wird zum **N**etwork **P**rotocol **C**ontrol **I**nformation aktualisiert, um darauf hinzustellen, dass diese Nachricht nun eine Netzwerkschicht-Nachricht ist.
Die Signatur wird mit Hilfe der Sicherheits-Header und der Payload berechnet und der Nachricht angehängt.

5.4 Nutzer-Autorisierung

Für die Nutzer-Autorisierung soll ein einfacher Mechanismus eingefügt werden. Dieser Mechanismus bietet ein 16-Bit-Nutzer-ID-Feld, das einen Nutzer identifiziert, welcher eine Operation anfragt. Desweiteren soll eine Nutzer-ID-Challenge-Sicherheitsnachricht existieren, die die gewünschte Nutzer-ID verifiziert.

Dies bietet den einfachsten Schutz und sollte in der Zukunft noch weiter ausgebaut werden.

5.5 Einordnung BACnet

Generell kann man über BACnet urteilen, dass es schon relativ wichtige Zwischenziele im Punkt Sicherheit erreicht hat. Vor allem gegen Spoofing- und Denial of Service-Angriffe ist BACnet gut geschützt. Jedoch hat BACnet ein Problem bei der Verteidigung. Ein Leitrechner in der Abbildung 3, beispielsweise die Access Control Workstation oder die HVAC [2] Workstation, besitzen in der Regel eine höhere Anzahl von Schlüsseln. Sollte also ein Gerät dieser Art angegriffen worden sein, sind somit alle Schlüssel, die dieses Gerät besitzt, zugänglich. Daher müssen die Leitrechner besonders stark geschützt werden.

Im folgenden wird diskutiert wie die Konkurrenz von BACnet mit diesen neuen Gefahren umgeht.

6. ALTERNATIVEN ZU BACNET

BACnet besitzt zwei Hauptkonkurrenzsysteme: LonWorks und KNX.
Wie sich diese im Aspekt der Sicherheit zu BACnet unterscheiden wird in diesem Kaptiel anhand den Quellen [7] differenziert.

6.1 LonWorks

Die **L**ocal **O**perating **N**etwork Technologie der Firma Echelon ist ein genormtes Bussystem. Die eingesetzten Geräte besitzen eine eigene Intelligenz und kommunizieren mitteinander in einem lokalen Netz. Diese Dezentralisierung ist der Unterschied zum BACnet.

LonWorks bietet einen vierstufigen Challenge-Response-Authentifizierungsmechanismus.
Ein Sender, der den Wunsch hat, eine Übertragung authentifizieren zu lassen, bestätigt die Authentifizierungsbits seiner Nachricht. Der Empfänger antwortet mit einer 64-Bit Zufallszahl. Die Antwort des Senders darauf ist ein 64-Bit Hashwert. Dieser wurde mit Hilfe der vorherigen Zufallszahl und eines geteilten Schlüssels gehasht. Der Empfänger kontrolliert den erhaltenen Wert. Desweiteren wird die Identität des Nutzers verifiziert und die Daten werden auf Aktualität und Integrität geprüft.

Jedoch hat LonWorks die folgenden **Sicherheitslücken**:

- Da die Daten unverschlüsselt übertragen werden, kann keine Vertraulichkeit sichergestellt werden.
- Bei der Authentifizierung wird nur der Sender überprüft, nicht der Empfänger. Dies ermöglicht Spoofing vom Empfänger.
- Jeder Knoten kann nur einen Schlüssel besitzen. Somit müssen alle Knoten, die miteinander kommunizieren

[2]HVAC steht für Heating, Ventilation and Air Conditioning

doi: 10.2313/NET-2014-08-1_09

wollen, denselben Schlüssel verwenden. Im schlechtesten Fall ist durch ein kompromitiertes Gerät jedes weitere Gerät ansprechbar.

- Es ist nicht möglich, Kommunikationsblöcke zu etablieren. Für jede einzelne Datenübertragung ist es also nötig, die vier Challenge-Response-Authentifizierungsnachrichten zu senden.
- Bei einem Multicast würde jeder Empfänger eine eigene Zufallszahl generieren. Der Sender wäre verpflichtet, jede dieser Zahlen zu hashen, was jedoch einen hoher Rechenaufwand bedeutet. Ausgenutzt werden kann dieser hohe Rechenaufwand mit Denial of Service-Attacken.

Zusammenfassend kann man urteilen, dass LonWorks mit den Challenge-Response-Verfahren einen grundlegenden Schutz bietet. Dennoch kann dieses System genau gegenteilig ausgenutzt werden, da es anfällig für Denial of Service-Angriffe ist.

6.2 KNX

KNX ist ein industrielles Kommunikationssystem. Es wird zur informationstechnischen Vernetzung von Geräten verwendet. Somit ist KNX auf der Feldebene einzuordnen und nicht komplett vergleichbar mit BACnet, welches auch übergeordnete Dienste anbietet.

KNX bietet keine Mechnismen, um die Datenintegrität, Datenaktualität oder die Vertraulichkeit zu wahren. Es existiert auch kein Authentifikationsdienst. Geboten wird nur ein simples Zugriffskontrollschemata basierend auf Klartextpasswörtern.

Aufgrund der fundamentalen Struktur von KNX gibt es noch zwei **Sicherheitslücken**:

Es sind keine parallelen Verbindungen möglich. Wenn also eine Verbindung mit zwei Geräten aufgebaut ist, ignorieren diese alle weiteren Anfragen. Somit sind Denial of Service-Angriffe leicht möglich.
Desweiteren können Nachrichten leicht injeziert werden, da die Quellen versendeter Nachrichten gespoofed werden können.

Somit hat KNX den schwächsten Sicherheitsschutz im Vergleich zu den drei erwähnten Systemen.

7. FAZIT

Manche Gebäudeautomationssysteme müssen geschützt werden. Daher gibt es die drei grundlegenden Sicherheitsziele und daraus abgeleitete Sichheitsmechanismen. Diese wurden im BACnet erfolgreich umgesetzt.

BACnet bietet einen Schutz, der eine Teilmenge von Angriffsarten abwehrt. Der Schutz ist je nach Bedarf individuell anpassbar, skallierbar und aktualisierbar. LonWorks und KNX bieten weitaus weniger, wobei KNX hierbei das Schlusslicht bildet. Somit ist BACnet die geeignetste Wahl für Gebäudeautomationssysteme, die vor jeglicher Art von Angriffen geschützt sein müssen. Allerdings sind nicht alle drei Systeme in ihren Einsatzgebieten identisch und daher auch nicht komplett vergleichbar.

LonWorks und KNX müssen in der Zukunft noch ihre Lücken schließen. Vor allem in dem Kombinierten Einsatz mit BACnet muss darauf geachet werden das die Verbindung der Schwachstellen nicht zu zu vielen unschützbaren Punkten führt. Jedoch sollten alle Systeme in der Zukunft weiter den Sicherheitsaspekt im Auge behalten und austauschbare Sicherheitsmechanismen implementieren, da die Gefahr von Angriffen auch in der Zukunft gegeben sein wird und die Anzahl der Angriffen steigen könnte. Desweiteren können die Gebäudeautomationssysteme dann womöglich in tiefere Subssysteme reichen, die noch schützenswerterer sind als die klassischen Elemente der Gebäudeautomatisierung wie Heizung und Licht.

8. LITERATUR

[1] Gebäudeautomation Kommunikationssysteme mit EIB/KNX, LON und BACnet 2., neu bearbeitete Auflage, *Hermann Merz, Thomas Hansemann, Christof Hübner* Carl Hanser Verlag München 2009

[2] *ASHRAE BACnet Interest Group Europe*, `http://www.big-eu.org/bacnet/basics.php`

[3] *BACnet Dominik Ebert*, `https://prof.hti.bfh.ch/uploads/media/BACnet.pdf`

[4] *MBS Software BACnet Kurzübersicht*, `http://www.mbs-software.de/produkte/bacnet/`

[5] D. G. Holmberg, Ph.D., Member ASHRAE: *Enemies at The Gates Securing the BACnet® Building* BACnet® Today A Supplement to ASHRAE Journal, 2003

[6] C. Eckert *IT-Sicherheit*, Oldenbourg-Verlag, 2013, 8. Auflage

[7] Wolfgang Granzer, Wolfgang Kastner, Georg Neugschwandtner and Fritz Praus, *Security in Network Building Automation Systems* Wien

[8] D. G. Holmberg, Ph.D., Member ASHRAE: *Secure Messaging In BACnet®* BACnet® Today A Supplement to ASHRAE Journal, 2005