Anthony Kabala

Emerging Threat from BACnet Over IP Protocol Vulnerability

An esoteric protocol, long thought of as having little security implication has gone from obscurity, to the most dominant protocol in Building Automation Systems. With a market share greater than 60% globally in 2018, BACnet's popularity shows no signs of slowing down and is projected to increase market shares in the foreseeable future [1].

Building Automation Systems (BAS) manage heating ventilation and air-conditioning (HVAC), lighting and power, fire alarm and fire suppression, building access and intrusion detection, and closed circuit TV monitoring devices and controllers for buildings [2]. These systems used to be independently managed and were not only not interoperable between different systems such as HVAC and fire alarm but also were not interoperable within the same system such as an existing HVAC system in a building and a new HVAC system being installed into a building, even if the system was by the same vendor. This was due to these systems being vendor specific and having proprietary protocols that at times did not have backwards compatibility. Several public standards developed to create an easier to manage and more interoperable whole building system that could be implemented by most vendors. BACnet is one of these open-source public standards and has become the leading protocol for BAS system communications.

Building Automation Control networking (BACnet) is a public standard networking protocol for BAS system communications [3]. Most of the BAS systems are supported by the BACnet protocol including HVAC, lighting, fire alarm and fire suppression, and building access and intrusion detection devices [4]. BAS systems originally were isolated systems that connected directly to devices such as thermostats, motors, and pumps for example; but has evolved to now interact with the network using several different protocols including Internet Protocol (IP) that devices such as thermostats can now use to communicate over Ethernet [3, 4]. Because the BACnet protocol was originally designed around isolated systems, the BACnet standard called for an unauthenticated and unencrypted protocol [2]. In order to use BACnet over IP, it is encapsulated within a User Datagram Protocol (UDP) packet causing BACnet data to be unverified because the UDP protocol is a connectionless protocol [3]. IP compatible BACnet devices are the most widely used BACnet IP devices because they are more affordable since they don't need to be able to create IP packets; they just communicate with IP routers that form the IP packets and interact with the network. This allows BACnet to function over the internet.

The BACnet protocol is object-oriented in that it is designed to contain information for different objects such as a temperature sensor or the state of a smoke alarm and can access and manipulate these

objects properties [3]. Several BACnet object types that can be manipulated like this are of particular interest due to the threat their manipulation poses. Files that can be accessed and manipulated by the BACnet protocol are described by the File object type [3]. The Life_Safety_Point object describes objects used for fire, smoke, and temperature alarms as well as other safety and security indicating alarms [3]. While a system is active, BACnet can also be used to create new objects in real time without confirmation. BACnet also allows non-standard object types to be written [3].

BACnet over IP can also remotely manage devices using a virtual terminal similar to TELNET in that it is a terminal based program that can sent commands over the internet [3]. These commands can start or stop devices through the DeviceCommunicationControl command and restart devices through the ReinitializeDevice command [3]. Devices can also have their configuration completely overwritten through the BACnet protocol using the AtomicReadFile and AtomicWriteFile commands [3]. Commands can be prioritized to control when they are executed. This is useful for functions that are time specific such as reversing a motor only after it has had time to come to a complete stop. Giving commands a priority above 6 causes them to be immediately executed and is typically only for emergencies, but can be sent to a device at anytime using the BACnet protocol commands, and if used as an attack could actually damage the motor unless the motor has mechanical stops to prevent such damage [3].

There are several different types of protocols that control different types of devices on BAS systems in addition to BACnet. The two next most predominant protocols implemented are KNX and LonWorks [1]. Even though these other devices are running on these other protocols, they can still be accessed using the BACnet protocol using a BACnet gateway that converts from the BACnet protocol to several other protocols including KNX and LonWorks. This allows the BACnet protocol to functionally communicate with the majority of devices on a BAS system allowing an external device to send commands into the BACnet network to which devices on the BACnet network will execute these commands [2, 3].

Given the design of BACnet over IP, it can be seen that the protocol itself is inherently insecure due to being unauthenticated and unencrypted over a network. However, recent addenda to the BACnet protocol do actually add security to the standard. These security features include authentication and encryption. Some of these addenda are officially a part of the BACnet standard as of the BACnet-2016 release while others are still undergoing public review [5]. These security features are added to the standard as optional. So, most vendors do not implement them [2]. The problem that BACnet faces, even though it has security as a part of its current standards, is that the life cycle for BAS systems is very long and the need for interoperability with legacy systems causes these new security standards to

be seldom if not never implemented on current systems [2, 6] At times BAS systems may never be updated in there life cycle, which can be from 10 to 20 years, due to the high cost of updating or replacing BAS systems [2]. This is why the unauthenticated and unencrypted properties of the majority of BACnet systems are a significant vulnerability to existing BACnet over IP systems.

The insecure design of BACnet makes it vulnerable to several authentication and traffic based attacks. There are several publicly available scripts and application tools that allow openly accessible BACnet over IP devices to be searched for over the internet and on local networks. Many of these tools either sniff traffic on the network or send out request packets that cause BACnet over IP enabled devices to respond with their properties. These include Nmap NSE scripts as well as the Shodan search engine which can crawl the internet or a local network for publicly available BACnet devices by sending out request packets or searching for known ports used by BACnet over IP including UDP port 47808 [2]. From 2016 to 2017 over 16,485 BACnet over IP devices were found that can be accessed from the internet [7]. The BACnet Discovery Tool finds BACnet objects and there properties on a local area network. A packet sniffer can be used to view BACnet packets and give a detailed analysis of the objects and their properties from which these packets originated from such as CAS BACnet Wireshark Report Tool.

Once an attacker has determined the accessibility they have to the BACnet protocol through these exposed networks they can use many of the BACnet commands described earlier to attack a building’s BAS system. BAS systems can be found in many different kinds of buildings including schools, religious centers, airports, stores, warehouses, financial institutions, and government buildings.

The impact an attacker could have one of these buildings would depend a lot on how dependent the infrastructure of the building is setup with relation to the BAS system of the building. For example a data center that depended on the HVAC system to keep the servers from overheating to the point of damage would be a high impact attack from the vulnerability of the BACnet over IP protocol. In this scenario if an attacker couldn't gain access to the BACnet network over the internet then they still might have the option to attack the network from within. The attacker could accomplish this using a BACnet device that is highly accessible such as a thermostat on a wall in an openly accessible part of a building such as a waiting room. The attacker could then use an authentication attack to pretend to be the BACnet controller to send legitimate commands to the devices on the BACnet network. To turn off the cooling system for the data center room the attacker could first send commands to pretend to be the temperature sensor alarms for the room showing the temperature to be at a safe level which would be easily determinable from packet sniffing the actual sensor data from the room thermostat object data. At the same time the attacker could disable the actual temperature sensor in several ways. The attacker

could either simply stop the device entirely using a protocol based denial of service attack that still uses legitimate commands such as DeviceCommunicationControl or use the AtomicWriteFile command to simply rewrite the thermostat's object data making it non-functional. If this did not work the attacker could use a traffic based attack to flood the device continuously by sending a reset command over and over to the legitimate sensors using the ReinitializeDevice command to keep the actual thermostat from relaying the real temperature of the room essentially disabling the device and any alarm it may set off if the temperature gets too high in the room. The attacker could then turn the air-conditioning system off for the data server room and even turn the heating system on. This same attack could be used similarly on a building that stores perishable goods in which the refrigeration storage room could have its cooling system shutoff. There are many potential attacks that can be implemented on a BAS system using vulnerabilities in the BACnet protocol with varying degrees of damage, this is why it is important for a buildings facilities management and IT departments to work together to create a viable mitigation plan for there sites.

To mitigate the vulnerabilities of the BACnet protocol in a network a cost to benefit plan would need to be taken into account. That is because the mitigation options have a large range of costs to implement depending on the BAS system of the building. The most costly mitigation for the vulnerabilities in BACnet over IP would be to replace the BAS system bringing all the BACnet devices and controllers up to the most recent protocol implementation that comes with encryption and authentication implemented in the protocol by the vendors. Depending on the buildings BAS system scope this may not even be possible since not all the BAS systems that a particular building may need to perform its desired functions may even be available that have BACnet protocol that utilizes encryption and authentication. Therefore another option would be to limit access to the BACnet network to only communicate on its own subnet or subnets within a building or through a firewall to the rest of the buildings network. If remote management of the BAS system is needed over the internet a VPN can be setup to connect to the buildings network. This would be the simplest VPN setup for the BACnet over IP and may already be implemented for the buildings network infrastructure already. However this would still expose the BACnet over IP within the buildings network to be vulnerable to compromised computers on the buildings network such as a userss computer exposed to a virus, or worm [8]. A different approach that also utilizes a VPN is to add an authenticated web interface that is the only application permitted through the BACnet subnet firewall to the BACnet network [8]. Intrusion Detection Systems could also be implemented within a BACnet subnet, but given the design of the BACnet protocol it may not be effective because many of the attacks using the BACnet protocol are legitimate commands. There has however been recent research by Peacock (2019) into designing an

intrusion detection system that has been shown to be able to provide more conclusive evidence that a BACnet system has been or is under attack. Assuming the BAS system is not upgraded to exclusively use an authenticated and encrypted version of the BACnet over IP protocol the BACnet network within the building would still be vulnerable. To secure this type of BACnet over IP the building's infrastructure would need to be secured physically from unauthorized access including the BACnet devices that could be used as potential access points into the BACnet over IP network by an attacker. So in conclusion the BACnet protocol is no longer an obscure networking protocol that can be ignored if a buildings operations are to be kept secure and unobstructed from attackers.

References

[1] Research Study Indicates BACnet Global Market Share over 60%. (2018, January 22). Retrieved July 27, 2019, from https://www.prweb.com/releases/2018/01/prweb15115222.htm

[2] Peacock, M. (2019). Anomaly Detection in BACnet/IP managed Building Automation Systems.

[3] Merz, H., Hansemann, T., & Hübner, C. (2018). *Building automation: Communication systems with EIB/KNX, LON and BACnet* (2nd ed.). Springer, Cham.

[4] Electric, Schneider. (2015, November). Guide to Open Protocols In Building Automation [Web log post]. Retrieved July 27, 2019, from https://blog.se.com/wp-content/uploads/2015/11/SE-Protocols-Guide_A4_v21.pdf

[5] ASHRAI BACnet ADDENDA AND COMPANION STANDARDS. (2019, July 8). Retrieved July 27, 2019, from http://www.bacnet.org/Addenda/index.html

[6] Addressing IP Security Concerns when Deploying a BACnet System. (2018). *Control Network Newsletter*. Retrieved 2018, from https://www.ccontrols.com/enews/2018/0418story3.htm Previously published in BACnet Europe

[7] Gasser, O., Scheitle, Q., Rudolph, B., Denis, C., Schricke, N., & Carle, G. (2017). The amplification threat posed by publicly reachable BACnet devices. *Journal of Cyber Security and Mobility*, *6*(1), 77-104.

[8] Neilson, C. (2013). Securing a Control Systems Network. *ASHRAE Journal*, B18-B22. Retrieved July 27, 2019, from http://www.bacnet.org/Bibliography/BACnet-Today-13/Neilson-2013.pdf