NISTIR 7009

BACnet Wide Area Network Security Threat Assessment

David G. Holmberg

U.S DEPARTMENT OF COMMERCE
National Institute of Standard and Technology
Building Environment Division
Building and Fire Research Laboratory
Gaithersburg, MD 20899-8631

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

NISTIR 7009

BACnet Wide Area Network Security Threat Assessment

David G. Holmberg

U.S DEPARTMENT OF COMMERCE
National Institute of Standard and Technology
Building Environment Division
Building and Fire Research Laboratory
Gaithersburg, MD 20899-8631

July 2003

U.S. Department of Commerce
Donald L. Evans, Secretary

National Institute of Standards and Technology
Arden l. Bement, Jr., Director

1 Scope and Objectives

This technical report addresses inter-networked building automation and control systems (BAS or BCS) using the BACnet protocol [ANSI/ASHRAE, 2001]. The report deals with threats from known sources due to communication connections to the corporate LAN and the public Internet as well as physical threats to the building automation equipment and attached computers. Weaknesses of the protocol, BACnet 2001, and of the physical implementation will be examined.

The BACnet system security environment is discussed followed by detailed threat analysis and possible countermeasures. The objective is to have a document that summarizes the threats toward and weaknesses of a BACnet network. This document can in turn be used for Common Criteria (CC) Protection Profile (PP) development and for guidance in selecting security solutions.

2 Table of Contents

3 Introduction

In today's networked economy the goal is the availability and productive use of information. The marketplace will not tolerate the cost and inconvenience of proprietary and competing technologies. Customer demands and competition drive companies to the higher efficiencies that networking provides. Competitors are driven to work together on open standards in order to enable networking: sharing resources and knowledge to create new opportunities and enable new services.

The building control systems market is no different. Networking technology development, customer demands, innovation in services, and open communication standards are driving the industry toward inter-networked buildings with ever-increasing services made possible by the flow of information. This information flow is not just between equipment on the building control system (BCS) subnetwork, but between the BCS subnet and corporate LAN, and between the building and off-site service partners: equipment vendors; gas, electric, and water utilities; security contractors; energy service contractors; telecommunication service providers; financial service providers; government regulating agencies; etc.

One hindrance to this flow of information is not a lack of creative minds to dream up new services nor lack of an educated workforce to develop enabling technology, but the presence of mistake and malice, error and evil. The growing interconnectedness of networks means that systems are open to disruptions from a larger number of machines, software, and users that can foul the system with faults, bugs, and error. And it is now very clear that we must also deal with a growing population of Internet-savvy criminals bent on financial gain, foreign governments looking for military and trade secrets, crackers determined to make mischief or wield control, and terrorists committed to taking lives and destroying property.

The ongoing development of the BACnet standard is opening the door for lower cost and more efficient building control systems that provide expanded services. This report seeks to address the security implications within the world of BACnet implementations. The report begins with an overview of BACnet and typical BACnet BCS installations along with a discussion of the security environment and review of threats to that system. The report then goes into detail on the threats, and finally possible countermeasures.

4 BACnet Building Control

4.1 The BACnet Standard

BACnet itself is a living standard undergoing constant growth and revision under the auspices of ASHRAE Standing Standard Project Committee (SSPC) 135. This committee is made up of building control industry vendors, BCS users, academics and government representatives. The BACnet standard has been designed specifically to meet the communication needs of building automation and control systems for applications such as heating, ventilation, air conditioning control, lighting control, access control, and fire detection systems.

In early 2001 the Network Security Working Group (NS-WG) was formed in response to concerns over access controls on life safety objects. It was soon recognized that security issues in BACnet were much wider in scope and needed addressing on a holistic level. The events of 9/11/01 served to intensify the efforts of the NS-WG. As part of the effort to address security concerns in BACnet, the need for a complete threat assessment was identified, leading to this report.

There are presently two ways that BACnet can be "spoken" over the public network, and these two methods are prescribed in the BACnet standard in Annex H and Annex J (BACnet/IP). For Annex H communication, a BACnet message destined for a remote BACnet network that must traverse a public network is sent by a tunneling mechanism. A device called a "BACnet/Internet Protocol Packet-Assembler-Disassembler" (B/IP PAD) exists on both networks, keeps track of all other B/IP PADs, and inspects the destination network (DNET) field of packets to see if they are destined for a remote network. If so, the B/IP PAD encapsulates the Link layer Service Data Unit (LSDU) portion of the BACnet message into a UDP (User Datagram Protocol) packet that is then sent to the B/IP PAD on the remote network for delivery on that network.

For Annex J "BACnet/IP" communication, each device on a BACnet/IP network "speaks IP", also using UDP transport. The BACnet/IP network may include more than one IP subnet and be spread out over more than one physical location. Devices may send directed messages as well as broadcast messages just as in a normal BACnet network. However, since IP does not support broadcasts, a special device is required—the BACnet Broadcast Management Device (BBMD). In essence this device plays a role similar to the B/IP PAD but only for broadcast messages that need to be forwarded on to other IP subnets across the public network.

In addition to these methods for communicating across the Internet, communication to remote BACnet networks is also possible via a temporary point-to-point (PTP) connection.

4.2 BACnet networks

4.2.1 Current network configurations

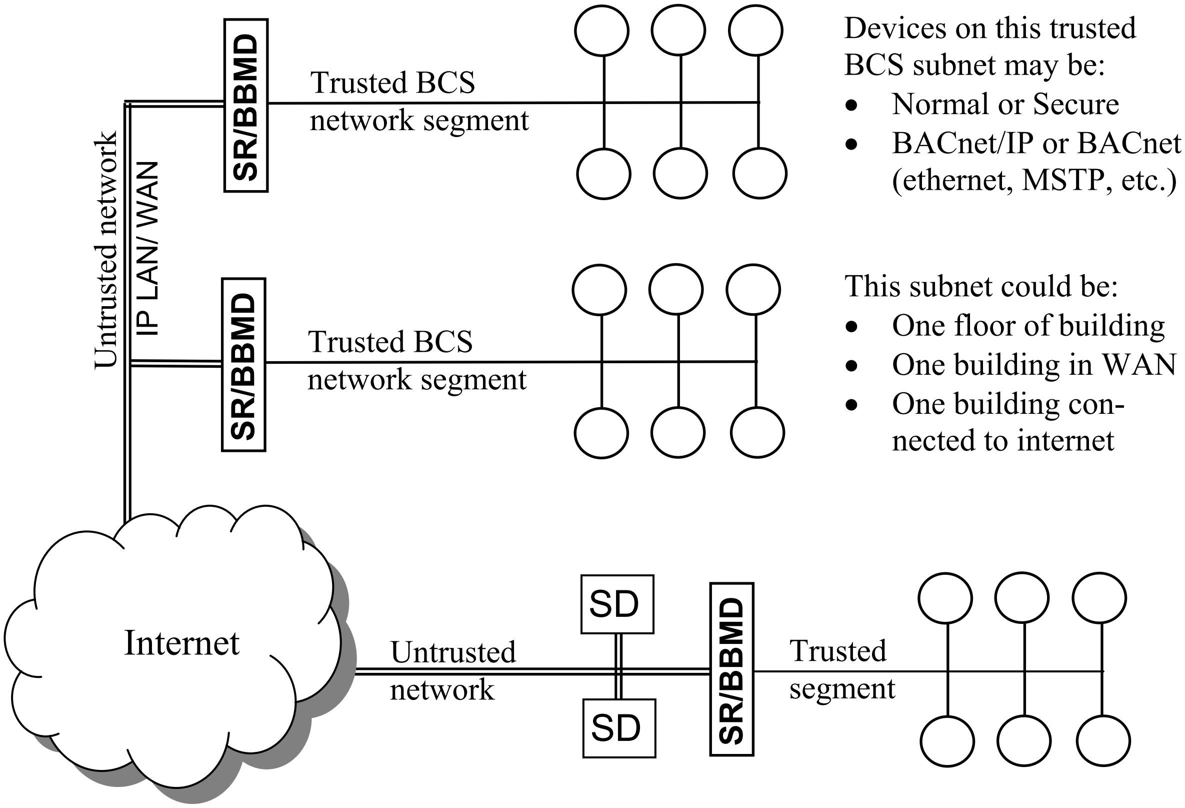
Most building control systems (BCS) today are not connected to the internet—they are secure due to isolation. However, some networks may have "back doors" via modem connections to controllers, or perhaps Internet access, also likely via modem in many facilities, to the operator work station (OWS). Physical security remains the biggest concern.

However, in many multi-building installations where a central control capability is desired, or where there is some outlying equipment to monitor, it is more and more common to connect the separate BCS networks using existing cables and IP protocol. This connection may be entirely confined behind a corporate firewall, but more likely includes the public Internet . How are such network connections secured? If they are secured, it is most commonly done by using virtual private networking (VPN) technology from building firewall to building firewall across the Internet . A router implementing this technology takes BCS traffic at one end-node, encrypts it (using IPsec), and sends it to a router at the far end that decrypts the traffic and delivers it to the destination BCS network. While BACnet provides a means for device communication over an IP network using BACnet/IP, there is still no available implementation of the BACnet standard's Clause 24 security features (guidelines on implementing authentication and encryption).

4.2.2 Future secure network configurations

Work is proceeding on implementing security into the BACnet protocol (see section 6.1). With secure services built into the BACnet protocol, new kinds of network configurations are likely. Figure 1 presents a conceptual secure configuration. There are secure devices (SD) and some of these are secure routers (SR). There is an untrusted network across which building control communication must flow—this could be the corporate LAN or some WAN or the Internet. There are also trusted segments of the network which sit behind the secure routers. These are segments of the BCS, perhaps the entire BCS of one building, or perhaps one floor of a building that uses the IP backbone of the building for higher-level BCS traffic. The trusted BCS segment might use IP protocol (i.e. have BACnet/IP devices), or some other protocol (ARCnet, MSTP, etc.), and the segment might be trusted simply because the devices on it are too "computationally challenged" to implement security or because we believe them to be physically secure and thus trustable. The fundamental point is that there are trusted segments connected to an untrusted network, and every device sitting on the untrusted network has to know how to protect traffic going out across that network. Good discussion of detailed scenarios for this network configuration can be found in Robin (2003).

If a normal device, sitting on a trusted network segment behind a SR, wants to send a message to another device across the untrusted medium, then the SR picks up the message, wraps it in a security envelope, and passes it on to the SR across the way. A SR can also act as a BBMD and handle a broadcast on the local (trusted) network by wrapping it in the security envelope and sending it along to every SD and SR it knows. The SR can control traffic into the trusted network behind it because, as router, all traffic destined for



SR/BBMD
Trusted BCS network segment
Devices on this trusted BCS subnet may be:
• Normal or Secure
• BACnet/IP or BACnet (ethernet, MSTP, etc.)
Untrusted network
IP LAN/ WAN
SR/BBMD
Trusted BCS network segment
This subnet could be:
• One floor of building
• One building in WAN
• One building connected to internet
Internet
SD
Untrusted network
SD
SR/BBMD
Trusted segment

Figure 1 A conceptual BACnet secure network configuration; SR = secure router, SD = secure device. All BACnet devices on untrusted network are secure.

the network behind it must pass through it and the SR can examine headers and contents of individual packets.

In summary, the Secure Router:

- Handles the security layer (authentication via signatures or encryption) to protect BACnet/IP traffic across the untrusted network (LAN/Internet).
- As a router, separates the trusted network from the untrusted and thus can act as a BACnet firewall, performing network layer or application level packet filtering.
- Can implement a detailed authorization policy, controlling which external devices have access to which devices on the trusted network.
- Could present a virtual network to the outside, combining network address translation (NAT) capability with the authorization policy so that an external device only sees devices it's authorized to see at an IP address determined by the SR.
- Acting as a BBMD can handle BACnet/IP broadcasts securely.

If it is not clear, there are good reasons to be connected to the "untrusted" network. The benefits of being connected to the corporate LAN are lower cost installation and maintenance. The benefits of being connected to the Internet are the use of the network to communicate with remote BACnet devices and external service providers as well as allowing outside access to the BCS.

Robin (2003) also discusses the network scenario of a highly secure device that demands additional protection (e.g., the access control panel). Although on a trusted network segment it still requires login and only certain devices or users may access it. In this case, there is a layering effect where messages are still passed as usual from one device logging into the secure device with the additional security wrapper applied whenever those messages cross the untrusted network.

A recent report by Drexel University [Eisenstein et al., 2003b] addresses the complex issue of life safety systems tied into the BCS—a scenario that does not fit well with the scenarios presented above. Presently all life safety systems (fire) are in parallel to the HVAC and other elements of the BCS, with separate wiring and only connections at the highest controller level to allow the BCS to get status information. Can this parallel network be integrated with the non-life safety BCS? It may not be possible due to code requirements that the life safety system be always available and have redundant communication channels. Nonetheless, Drexel gives suggestions for how the security issues might be addressed: stronger firewalls, separation of network (or subnet) traffic using private virtual LANs, and parallel routers/switches for redundancy.

Not shown in Fig. 1 are some elements of the network that complicate security efforts. There may be a corporate firewall or network address translation (NAT) features that will require communication between the building services staff and IT staff, but will also provide greater protection against IT threats. There may be other external connections from a trusted network that bypass the SR, i.e. a modem connection. Also not shown are physical security implementation details. Are the controllers in secure locations? Is there a security policy that governs operator access to the system (passwords, keys), maintenance procedures, presence of tamper evident seals, etc.? Threats coming via the network or through the physical door are examined next.

5 Threats

What are the dangers to the present day building control system? If the system is not connected to the WAN then the dangers are fairly well known: human error, insider threat, physical break-ins, faulty equipment. But there is a growing uneasiness about the dangers of the Internet, as well as a growing awareness that we need to be uneasy.

5.1 Attackers and Points of Attack

What is the BCS threatened by and where is it threatened? Some potential threats are:

> *Hackers*, both mischievous and malicious, may be college kids out to play with building systems (e.g. turning lights off), or criminals. Criminal activities include denial of service (DoS) attacks, theft, destruction of property, perhaps spying by competitors and others.

Disgruntled employees may be hackers using knowledge of the networks, computers, and protocols to perform unauthorized actions, or using physical access to do the same.

Criminals (thieves, terrorists, competitors, employees, etc.)—Criminal scenarios include simply gathering information that would give knowledge of the buildings and how to break in, or maybe getting into the security system and having doors open. DoS attacks could be used for a variety of purposes including: making a political statement, interfering with business, etc. Terrorists could use low security on a network to shut down facility operation (i.e. as a smokescreen or disruption) that facilitates other destructive activity. When considering a US government building internetwork, this seems a very real threat.

Competitors. Monitoring the network could be used for corporate research; for example, gathering info about how a company uses electricity, from which utility, and for what loads. The curious party could be a competing utility, or a manufacturer of more electrically efficient equipment.

Human error. This can affect control system implementation (thus the need for commissioning), key sharing, network administration, physical security, upgrades, flaws in software and hardware development, etc.

These threats can be classified according to location of attack (network connection, physical location of equipment, within procedures and programs). The following subsections look at specific threats within these rough classifications: IT, protocol, physical. But first, perhaps it is worthwhile to discuss what is *not* considered a threat to the BCS, given the above attackers and the typical BCS network.

5.2 What is not a threat

What does a typical BCS network look like? Most installations today have a dedicated BCS network with centralized control via an operator's terminal in the facility manager's office. There is no Internet (or LAN) connection, and thus no IT threat. However, the trend today is toward greater connectivity to enable new services, convenience, and savings on infrastructure costs. Newer buildings have network connections to the Internet. But even so, most BCS networks still have few resources that are of value to the typical "hacker".

The most prevalent attacks today are *allowed by* known vulnerabilities in popular software packages (e.g. OS, email) or known vulnerabilities in common protocols (e.g. SMTP) that *result in* allowing outsiders to: get valuable information (credit card numbers, personal information, company proprietary information, etc.), gain access to system resources (e.g. storage space, CPU power, entire machine), and use those resources for such things as launching distributed denial of service (DDoS) attacks on other networks.

Considering these attack vulnerabilities and scenarios it is clear that the typical BCS is not a desirable target. System resources are limited (storage space, CPU power, common OS and software packages, etc.), and valuable information is limited to the BCS system itself (configuration data, router tables) but no financial or personal information. However, this may change: as the BCS is connected to more and more service providers—giving access to more information either stored locally or providing a secured path to outside service providers' networks; and as the overall intelligence contained on the BCS network increases to accommodate smarter distributed controls and sensors. It is with this in mind that this document has been prepared, and for this reason that we look at general IT threats.

5.3 IT threats

Taking the network scenario of Figure 1, there will be web interfaces (routers and servers), BACnet/IP controllers (connected to interesting devices that are network accessible), and operator workstations that may have vulnerable OS as well as configuration files and other interesting data and resources.

The following table is adapted from a Drexel report on network security [Eisenstein et al., 2003a] and lists known IT threats to a BACnet network connected to the public Internet. The threats are classified into broad threat categories, and the following are provided for each: relevant methods of attack, applicable protocol, potential countermeasures.

The BACnet protocol currently uses the connectionless User Datagram Protocol (UDP) for both Annex H and BACnet/IP communications. However, it is possible that Transmission Control Protocol (TCP) transport will be utilized for some service in the future, and so threats specific to TCP have been included. Even if TCP/IP is never used as part of the BACnet protocol, it still can be used to gain access to the building control system web servers, get access through the corporate firewall, and be used for denial of service attacks on the external network on which the BCS may depend.

The class of attacks identified as "General" consists of IP related attacks which are found in both UDP and TCP networks as well as other attacks arising from lack of sufficient encryption of data and insecure key exchange mechanism.

Descriptions of the various attacks listed in Table 1 are discussed in more detail in Appendix A of the Drexel report [Eisenstein et al., 2003a]. Further discussion of countermeasures relative to BACnet is provided in section 6.

Table 1. BACnet IT threat summary and recommended countermeasures

Category	Method of Attack/ Description	Applicable Protocol	Recommended Countermeasures
Password Attacks This type of attack includes gaining a password either by	Brute Force	General	Set limit on the number of unsuccessful login attempts
	Dictionary	General	
	Trojan Horse	General	Install anti-virus software with updated patches

guessing, insufficient encryption or replay	Default Passwords	General	Change default usernames and passwords immediately
	Password replay	General	Time stamping (e.g. with Kerberos)
Data Confidentiality	This category deals with the protection of data and user identity privacy due to insufficient encryption	General	Use of encryption and choice of encryption algorithm (AES)
Data Integrity	This category is concerned with maintaining the integrity of the data from third party attacks and alterations once the data has been sent over the network	General	Use of Kerberos and/or IPSec for authentication and encryption services
Denial of Service In this category of attacks, a third party, either remotely or as a valid user of an internal organization, tries to bring down a network by flooding it with useless packets	Ping of Death	General	Intrusion Detection (whether in a BACnet object or not), see section 6.2.4 Firewalls: see [Eisenstein et al., 2003a] Appendix A for detailed discussion of how to use a firewall to fight specific attacks Use Kerberos for authentication and encryption.
	UDP Flood	UDP	
	Fraggle Attack	UDP	
	RPC Attack	UDP	
	WINS Attack	UDP	
	SYN Attack and ICMP Flooding	TCP	
	Smurf Attack	TCP	
	IP Source Route Spoofing	TCP	
	Land Attack	TCP	
	Man-in-middle Hijacking	TCP	
	Malformed Packet Vulnerability	General	
	Port exhaustion attack	general	
Spoofing attacks In this type of threats the attacker forges the source address and makes it look like the attack was initiated by another machine	ARP Spoofing	General	Configure firewall to drop external packets with internal source addresses and to reject internal packets with external source addresses.
	IP Spoofing (Source address spoofing)	General	
	DNS spoofing	General	
Eavesdropping, Snooping and Port Scanning This is a passive category of attacks. Passive because the attacker does not actively alter or bring down a network. He usually uses various tools for scanning or wiretapping to gain information being passed over the network. He may then use this information for active attacks.	Network Traffic analysis	General	Use Intrusion Detection System (IDS) Configure firewall: see [Eisenstein et al., 2003a] Appendix A for detailed discussion of how to use firewall to fight specific attacks
	Password Capture	General	
	Network Address scanning	General	
	UDP Scan	UDP	
	RPC Scan	UDP	
	TCP Null Scan	TCP	
	IDENT Scan	TCP	
	SNMP Reconfiguration	TCP	
	TCP Xmas Scan	TCP	
	SNMP Data Configuration	General	
	Operating system Detection	General	
	Network Reconnaissance	General	
Access Control	In this category actual physical access is not gained but the attacker intends to harm the network using either a valid user account or remotely using other tools	General	Intrusion Detection System Intrusion Detection Object (IDS/IDO, Section 6.2.4) Activity Logging

Non-Repudiation	To prevent a valid user (or an attacker) later denying responsibility of an event or a communication that he performed.	General	Activity log or time stamp required Intrusion Detection Object (IDO)
Exploitation attack	Buffer Overrun: These kind of attacks are usually due to software limitations or flaws in coding and design	General	Install the latest software patches and upgrades
PTP modem	Using modem to connect to network (corporate LAN) at an operator workstation behind the firewall.	General	Prohibit modem connections behind firewall, or only allow dial-out function.
Physical attack This category assumes physical access to network devices has been gained	Using physical access to network to: wiretap, perform traffic analysis, install rogue software, view confidential information, etc.	General	See following sections on physical attacks (5.6) and countermeasures (6.3).

5.4 Generic vulnerabilities in the BACnet Protocol

Table 1 gives generic IT threats, all of which may be used to directly or indirectly threaten a building control system. In Table 2 is a short list of threats that are specifically BACnet protocol vulnerabilities. Within the BACnet standard there are some warnings given about these: to password protect some of these services (e.g. ReinitializeDevice), or to make properties non-writable via WriteProperty but instead only accessible using VT Services (assuming the operator terminal is password protected), or a suggestion to implement Clause 24 methods for security. Some of these vulnerabilities cannot be protected against *except* by use of authentication which presently is proprietary. There is work going on now to address this issue to allow network-visible, standard means of dealing with authentication and authorization.

Table 2. BACnet protocol threat summary and countermeasures

Category	Name	Attack Description	Defense
Snooping	Device Object information	Use Read Property service to gain knowledge of device (status, location, vendor, software), device objects (sensor and actuator information), and services supported to understand network and plan active attacks (e.g., on some particular object, using some supported service). Potentially useful Device Object properties: • system-status • device info properties: vendor-name, vendor-identifier, model-name, firmware-revision, application-software-version, location • protocol-services-supported • object-list	Authentication, especially of external BACnet users.

	General information gathering	Using the ReadProperty Service (as above with the Device Object) to gather property information. Using Who-Has and Who-Is services to scope out devices and objects on the network. Using Initialize-Routing-Table to get existing router tables to scope out internetwork configuration.	Authentication, especially of external BACnet users.
Application Service Attacks	Write to commandable properties using Priority = “1”	Change the Present_Value of some objects to disrupt the building control system, turning off equipment, turning on other equipment, and doing it with override authority. This attack can be generalized to the use of the WriteProperty service to harmfully change any property.	Write Property source authentication.
	Spoof any device	Any device can claim to be any other device using the I-Am service	Authentication of user/device.
	Unrestrained Who-Is	A rogue device sends out multiple globally broadcast Who-Is service requests with no specified device instance range limits so that all devices on the internetwork respond with I-Am messages and flood the network.	Authentication of remote devices; IDO.
Network Layer Attacks	Initialize-Routing-Table	Use the Initialize-Routing-Table message to rewrite a routing table of a router (update, change, or replace completely) or to query the contents of the current routing table. This could be used to disable network communication, including blocking alarm notifications and other high priority traffic. This could also be used to reroute traffic to a compromised router, or to simply gain information about the network configuration.	Authentication, especially of external BACnet users.
	I-Am-Router-To-Network	The I-Am-Router-To-Network message can be used to redirect network traffic to a compromised router. This could be used to drop, modify, or read messages in transit.	Authentication, IDO to monitor network for suspicious activity.
Network Layer Denial of Service (DoS) Attacks	Disabling router connection	Use a Router-Busy-To-Network message with spoofed router source address to break a communication path. This can be repeated at regular intervals to maintain the disruption. A PTP connection can be broken by issuing a spoofed Disconnect-Connection-To-Network message.	Authentication of user/device.
	Network Layer message sent as Unicast	For example, use an Initialize-Routing-Table message to router A (but not broadcast as the protocol requires) telling router A that router B should get messages destined for certain networks that actually router A is the correct path. Router B (with the correct router table) then returns the message to A and a loop is created. This can be done with multiple routers and messages to clog the network and deny service.	Check that broadcast MAC address is being used. Decrement Hop Count faster. Notify admin if Hop Count *is* decremented.

	Broadcast-as-SADR malformed network layer message	Perform a global broadcast of a network layer message that has both an unknown message type in the Message Type field, and a spoofed source address set equal to the global broadcast address. Each router receiving the broadcast will both pass it on, as well as check the NPCI and, not understanding the message, reply to X'FFFF' with a Reject-Message-To-Network message. This will effectively deny service to the network, even of critical messages if the attacker sets the network priority to B'11' in the NPCI.	Discard messages with broadcast as source address.
Application Layer DoS Attacks	Broadcast-as-SADR confirmed service request	Perform a global broadcast of a confirmed service request such as CreateObject, and use SADR equal to the broadcast address. Either the receiving device will consume resources creating objects, or it will broadcast a Result(-) response.	Discard messages with broadcast as source address.
	Reinitialize Device Service	This service could be used to reboot any unsecured device, or broadcast to all devices, and or combined with SADR using broadcast address. At worst, devices are rebooted, at best the network is flooded with error messages.	Authentication; don't accept broadcast confirmed messages; discard messages with broadcast as source address.

5.5 BACnet Annexes H, J, and Clause 24

5.5.1 Annex H and Annex J

The vulnerabilities of Annex H (Combining BACnet Networks with Non-BACnet Networks) and Annex J (BACnet/IP) are those of being connected to the public Internet (threats as discussed earlier) and some specific to the B/IP PAD of Annex H and of the BACnet Broadcast Management Device (BBMD) used in BACnet/IP.

For Annex H, the B/IP PAD sits on the network listening for messages from remote B/IP PADs as well as from local devices sending messages to remote networks. There is a need for authentication of B/IP PADs to each other to provide security from unauthorized sources. There should also be a firewall upstream of the B/IP PAD and perhaps intrusion detection on the network. Drexel recommends that some B/IP PADs be developed that integrate firewall capabilities for those cases where the BACnet network is connected directly to the public Internet . These firewalls should conform to existing Protection Profiles as discussed in their report [Eisenstein et al., 2003a].

The threat situation is similar for the BACnet/IP BBMD. In addition to the above recommendations, there are many BBMD specific messages that must be implemented with authentication: Write-Broadcast-Distribution-Table, Read-Broadcast-Distribution-Table, Register-Foreign-Device, Read- Foreign-Device-Table, Delete-Foreign-Device Table-Entry, Distribute-Broadcast-To-Network, Original-Broadcast-NPDU, etc. Authenticating foreign devices is important to protect the network from unauthorized users. Authentication of most of the messages can help prevent denial of service attacks as well as other unauthorized actions.

Countermeasures including authentication, Intrusion Detection Systems, firewalls, and proper security design (security policy) of the network will be discussed in the section on countermeasures following this section.

5.5.2 Network Security Clause 24

BACnet's Network Security clause (Clause 24) provides optional "limited security" measures such as "peer entity, data origin, and operator authentication, as well as data confidentiality and integrity." The issues of key distribution, access control, and non-repudiation are not addressed in the BACnet standard. The following vulnerabilities were pointed out in both the Drexel University [Eisenstein et al., 2003a] and the Pennsylvania State University [Zachary et al., 2002] reports.

5.5.2.1 Symmetric key size

BACnet currently requires a 56-bit Data Ecryption Standard (DES) key encryption for session keys. It has been demonstrated that these keys can be broken in times on the order of 1 day. Longer key lengths should be used, although the determination of key length also should consider data sensitivity and lifetime.

As discussed in the next section on countermeasures, use of the recently standardized Advanced Encryption Standard (AES) perhaps should be required in BACnet.

5.5.2.2 Clause 24 authentication protocol analysis

The authentication protocol specified in BACnet Clause 24 is known to be vulnerable to certain attacks including [Zachary et al., 2002]: Man-in-the-middle attacks, type flaws, parallel interleaving attacks, replay attacks, and implementation dependent flaws. The most serious of these is the replay attack—an attacker can break an old session key and reuse it since there is no means of knowing the freshness of the key.

In order to address this vulnerability, the protocol must be improved. As discussed in the next section on countermeasures, use of Kerberos will provide a stronger authentication protocol.

5.5.2.3 Key management

Clause 24 specifies private key distribution as a "local matter". Distribution of private keys could be done by physically entering them into a keypad at the device, or by using public key cryptography, or by some other means. In addition to the issue of key distribution is the issue of key storage on the local device.

The Drexel report recommends following the guidelines of NIST standard FIPS PUB 140-2 "Security Requirements for Cryptographic Modules" for all cryptographic matters: key exchange, key management (generation, distribution, storage, zeroization), physical security, etc. Drexel also makes the case that public key cryptography would be too computationally intensive to implement in embedded controllers at this time. Finally, use of Kerberos would address some of these concerns. These options will be discussed further in the section on countermeasures.

5.6 Other (non-IT) threats

Non-network threats include physical security, faults, error, and failure. For physical security, the attackers may be the same as those listed earlier, and they may be acting with the same motives. Only the methods are different. Some methods of attack might be:

- Legitimate user violating limits of authorization for malicious reasons (insider threat). This could involve tampering with equipment in order to cause erroneous operation or destruction. For spying or theft purposes someone could also install equipment or software to monitor network traffic or collect sensitive information on a work station, etc.
- Intruder purposely penetrating system (outsider threat). Same scenarios.
- Intruder acting without coherent or logical plan. As with a hacker on the network, an intruder may have no specific purpose other than to meddle.
- Social engineering: an attacker using tricks to get insiders to reveal passwords or other private information to gain access (physical or network).

In addition to these attacks are the threats of error, fault, and failure:

- Administrator error. A legitimate user accidentally messing up an unprotected system. This could be in setting up user privileges, BCS network configuration, failing to patch software for security protection, not following security policy guidelines, etc.
- Equipment failure. A device on the network faults or fails. This can be hardware design, hardware failure, or software bugs. Power failure could also lead to one system affecting others, e.g. AC failure leads to network overheating.
- Natural disaster. Fire, flood, wind, electrical storm.

6 Countermeasures

To a large degree, there are known and already commercially available measures that can be taken to increase network and physical security. For example, the Network Reliability and Interoperability Council [www.nric.org] publishes “best practices” guidelines for dealing with various known IT threats. Beyond that, there are changes planned for the BACnet standard itself to improve protocol security. This section gives more details on some of the countermeasures introduced in the threat section above.

6.1 Approach to addressing threats in BACnet

This sub-section gives a brief overview of the direction that the BACnet Network Security Working Group (NS-WG) is taking to address security issues. In a conference call in October, 2002, the NS-WG came to an agreement about how to approach the many threats to a BCS. The decision was made to divide the work into two parts: Group 1—what can be done now with available technology to secure current BCS installations, and Group 2—changes needed to secure the BACnet protocol itself.

Group 1 work is focused primarily on the new threats of the Internet, the IP threat. Current BACnet network configurations need to be identified (this document addresses that), and then secure network configurations need to be established. The goal is to use existing IT security features to address this IT threat and apply those to the special needs of the BCS. The Drexel report [Eisenstein et al., 2003a] is focused on this issue. Their recommendations are included in the following subsection 6.2. In the Pennsylvania State study performed for NIST [Zachary et al., 2002] the authors prepared a BBMD Protection Profile. This along with firewall PPs recommended by Drexel can be used to aid in designing BCS security policies and specifying security hardware functionality.

A second Drexel report [Eisenstein, et al., 2003b] addresses BACnet security for life safety systems. That report gives some additional input on what kind of secure network configuration is necessary for life safety systems and especially as vendors start to integrate the life safety system network with the rest of the BCS.

Following this threat assessment document, there is a plan for a document covering "how to secure a BCS installation" that addresses steps that building owners can take to protect their building control systems. These steps will include: implementing a security policy, installing firewalls and other IT measures for increasing security (NAT, IDS, etc), and how to make secure connections to off-site devices using VPN or other technologies.

Beyond these reports, there is a need for BACnet user education via other mediums and in various forums to educate building owners, as well as vendors, on how to implement security. Education not only gives knowledge to building owners, but also creates the market demand required for product vendors to produce secure network devices.

Group 2 work covers the BACnet specific security threats. As seen in Table 2 in the last section, many of the BACnet vulnerabilities can only be addressed by authenticating the source BACnet user, or by examining packet headers for misuse—the function of firewalls and intrusion detection systems. Authorization and encryption are two other issues that need to be addressed for improved security in the standard.

At the NS-WG meeting in Honolulu (July, 2002) the issue of authentication was discussed. Previously the WG had agreed to pursue an industry standard authentication protocol. Robin [2002] presented a review of three options: Kerberos, IPsec, and SSL. The general conclusion in that document was that, of the three, Kerberos is best suited to the way BACnet communicates and therefore warranted further study. However, while Kerberos is well tested and provides very good security, it is also difficult to set-up and administer.

Accordingly, the NS-WG is investigating possibilities for a simpler security mechanism that will provide at least basic security, that does not require significant changes to the way BACnet communicates, and which is relatively easy to set-up and administer. Along with this, secure network configuration is being discussed. The concepts of secure routers and secure networks of Fig. 1 are discussed in more detail in [Robin, 2003].

Besides addressing authentication methods and secure network configurations, there has been some work towards addressing a network-visible form of authorization. Keith Corbett [2002] proposed a Network Access Control Object to handle role-based authorization. This, along with any implementation of an Intrusion Detection Object, is farther down the road.

6.2 IT threat countermeasures

6.2.1 Firewalls

There are two primary types of firewall technologies in wide use today: packet filters and proxies. In addition, Network Address Translation (NAT) and Virtual Private Networks (VPNs) are also used, mainly in conjunction with packet filtering and proxying to secure internal networks [Eisenstein et al., 2003a].

A packet filter monitors packets entering or exiting the internal network from/to the external network, dropping packets that violate security or use unacceptable protocols and routing acceptable packets. It may also be configured to send alarms or do other useful administrative tasks. If a packet filter is “stateful” it will also be able to connect incoming packets to outgoing requests and to monitor higher level activity and thus allow for stricter security policy requirements.

Proxy services and NAT perform similar functions—adding a level of indirection between the internal and external networks. Servers on the external network send packets to the proxy which passes them on to an internal host. The proxy keeps track of which external server is connected at which IP address and port number and assigns these dynamically to internal hosts as needed. The proxy can look beyond packet headers into packets and is also stateful so that it can provide application level filtering.

The topology of the network itself can be configured in various ways to suit the security needs of various size networks. Perhaps a single packet filtering router is sufficient for a small network with minimal security, whereas a large higher security facility would have multiple routers (allowing a semi-secure area between routers) with a proxy server and IDS (see below). In the case shown in Fig. 1 earlier, there is a corporate firewall that will filter out much of the harmful network traffic before it reaches the building control system. It may be deemed unnecessary to use an additional firewall at the BCS entry point. However, it may also be found that a BBMD/firewall/router (BFR), as discussed earlier in 4.2.2 and 6.1, or multiple BFRs within a building network, would be very helpful in increasing security. Additional details on firewall architectures and firewall PPs can be found in the Drexel report [Eisenstein et al., 2003a].

6.2.2 Authentication protocol and optional encryption services

In addition to the report by Robin [2003], the Drexel report gives some more detailed discussion on the authentication issue. They give a detailed review of both IPsec and Kerberos and also of the KINK protocol which uses Kerberos to distribute session keys for IPsec use. Their recommendation is that Kerberos be used for local authentication, replacing the current Clause 24 authentication protocol while also providing data integrity and confidentiality, but caution that Kerberos may not meet all needs and that the gaps be filled using IPsec.

6.2.3 Cryptographic security

6.2.3.1 Key management

As discussed under Threats, Clause 24 does not specify private key distribution mechanisms, nor give guidelines on key management. Drexel recommends adhering to FIPS 140-2 “Security Requirements for Cryptographic Modules” [FIPS, 2002]. It may be included in the BACnet standard by reference stating that all key management issues will conform to FIPS 140-2 at a specified level, e.g. at the minimum security level of 2 out of the four levels given in FIPS 140-2.

FIPS 140-2 identifies requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity and a diversity of application environments. Four security levels are specified for each of 11 requirement areas. These 11 areas are sections 4.1— 4.11 of the standard: crypto module specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; key management; electromagnetic interference/electromagnetic compatibility; self-tests; design assurance; mitigation of other attacks.

Each security level offers an increase in security over the preceding level. Level 1 only requires use of production level cryptographic module (e.g., encryption card) that may be used in any general purpose computing system. Level 2 enhances physical security requirements by requiring tamper resistance installation as well as use of an operating system that complies with specified Common Criteria (CC) protection profiles and which has been evaluated at the CC evaluation criteria level EAL2. In addition, operator role-based authentication is required.

6.2.3.2 Cryptographic algorithm

The Drexel report [Eisenstein et al., 2003a] gives three reasons for recommending use of AES over the existing specified DES encryption algorithm:

(i) Superior security: The key length (56-bits) of DES is not long enough to provide adequate protection. This has been demonstrated by the DES-III challenge, where it took only 22 hours and 15 minutes to recover the key (RSA, 1999).

(ii) Speed: AES is faster than DES in software implementation (Schneier, 1999) and can be implemented in 8-bit processors with limited RAM on board.

(iii) Hardware implementation: Although DES can be processed in hardware faster than AES, and although AES was selected primarily for its speed when implemented in software, AES is still very fast when implemented in hardware.

AES was chosen by NIST as a replacement for DES primarily due to the small key length and slow speed of DES software implementation. The Drexel report gives additional information and references for each of these items.

The algorithm in all likelihood will be determined by Kerberos (for secure BCS facilities that opt for a Kerberos implementation) or by some standard hash algorithm (used in the password based security scheme). Additionally, security to off-site devices will be enhanced using VPN connections or perhaps other means, each of which provides standard encryption services. This is to say, the BACnet standard will not specify which cryptographic algorithm to use except indirectly as with Kerberos (which still used DES as of version 5).

6.2.4 IDS/IDO

An intrusion detection system (IDS) can be implemented to increase network security. There are two primary types of IDS: network based and host-based. The network based system acts similarly to a network level firewall. It cannot detect most internal attacks since it only examines packets at the IP level [Eisenstein et al., 2003a]. At the same time there is considerable evidence that shows internal attacks are more serious than external ones, and host-based IDS can watch for these. The host-based IDS supports the authentication and authorization mechanisms by watching the activities of users and devices and looking for pre-programmed misbehavior. It can look for users exceeding authorization, and log activities of devices and users. The IDS can then implement rules for certain infractions such as shutting out a device or user and sending audit reports to the network administrator via email or other method.

The best architecture for a secure BACnet system would have a host-based IDS running on a central dedicated PC [Eisenstein et al., 2003a]. High-level devices on the network would then report information to the host and the host would process all the data to look for abuse signatures. Rather than setting it up so that each controller on the network examines its own traffic, reporting the data to a central host limits the processing and storage requirements on lower-level controllers as well as allowing the central host to see network wide activity. The host also can store a log of activity.

In the Drexel report, Drexel recommends that the BACnet committee implement an Intrusion Detection Object (IDO). This object would serve the function of collecting BACnet activity at individual devices and reporting this to the central IDS host. The local device monitors BACnet traffic for sensitive commands such as: DeleteObject, Reinitialize-Routing-Table, or ReinitializeDevice. This activity would be reported via the IDO, along with device info, network addresses, and a priority flag, to the central IDS. Drexel makes the points that this BACnet object would: serve to limit the burden on local devices, build a log of network activity, and serve a complementary and necessary role next to the proposed Network Access Control Object [Corbett, 2002]

The IDO has potential and should be investigated further. The need for auditing and logs of user activity has already been identified by the NS-WG.

6.2.5 Other countermeasures

As mentioned above, there is a place for access controls, logging of user and device activities. Kerberos does not provide for role-based authorization, however it is required within FIPS 140-2 for encryption security. The NS-WG will likely implement a BACnet specific authorization scheme [Corbett, 2002]. The proposed IDS discussed above would then provide the activity logging services as deemed necessary for the security of a given network.

An additional countermeasure that would become part of a security policy is the use of software patches on vendor software.

6.3 Physical threat countermeasures

Physical threats discussed above include intruders and insiders tampering with equipment in order to gain access to network devices and information for various unauthorized activities or man-made disasters.

Countermeasures to physical threats are quite well established and not specific to a BACnet network. The Drexel report [Eisenstein et al., 2003a] gives some detailed information on tamper-resistant measures that might be implemented in a network. The BBMD Protection Profile prepared by Penn State [Zachary et al., 2002] also gives an example of how physical security might be incorporated into a Protection Profile.

7 References

ANSI/ASHRAE Standard 135-2001, “BACnet 2001”, ASHRAE 1791 Tullie Circle, NE Atlanta, GA 30329, www.ashrae.org.

Corbett, K., 2002, “Network Access Control Object,” BACnet committee SSPC 135 document number KAC-012-2.

Eisenstein, B., Reddy, T. A., Woldu, A., Wagle, R., 2003a, “Investigation into Computer Network Security for Integrated Building Automation and Control Systems,” Drexel University contractor report, NIST GCR 03-845.

Eisenstein, B., Reddy, T. A., Woldu, A., Wagle, R., 2003b, “Security of Life Safety and Access Control Systems in an Integrated Building System Environment,” Drexel University contractor report, NIST GCR 03-850.

FIPS 140-2-l, 2002, “Security Requirements for Cryptographic Modules,” available at http://csrc.nist.gov/cryptval/140-2.htm.

Robin, D., 2002, “Internet Security Protocols For BACnet,” BACnet committee SSPC 135 document number DR-028-1.

Robin, D., 2003, “BACnet Security Messages,” BACnet committee SSPC 135 document number DR-029-2.

Zachary, J., Brooks, R., Thompson, D., 2002 “Secure Integration of Building Networks into the Global Internet,” The Pennsylvania State University contractor report, NIST GCR 02-837.

8 Acknowledgements

Special thanks is due members of the BACnet Network Security Working Group for their input on this document, specifically Joel Bender and Dave Robin. Additional input from Agami Reddy at Drexel is appreciated.