Enemies at The Gates

Securing the BACnet® Building

By David G. Holmberg, Ph.D., Member ASHRAE

The building automation industry is moving away from isolated building control systems toward building automation systems (BAS) integrated with business applications on a shared "IT" network. This open shared architecture allows not only for integration of diverse building control systems, but also for connections to corporate business applications as well as off-site business partners.

For at least one large BAS vendor, 50% of new jobs share Ethernet wiring with the corporate local area network (LAN). This LAN is connected to the Internet, typically behind a firewall. Another large vendor reports a significant number of jobs where the workstation is a Web server sitting behind a firewall and accessible via any browser using secured communication (https, the secure form of the Internet's hypertext transfer protocol). Many vendors have workstations and even controller level devices that run common operating systems and sit on the corporate LAN. One consequence of this trend is many new BAS are exposed to network attacks that previously were reserved for Web servers, and have resources that make them nearly as attractive to hackers as a desktop PC.

And it is not as if one can seal the doors and forbid outside communication. Networking technology development, customer demands, innovation in services, and open communication standards are driving the building control industry toward inter-networked buildings with ever-increasing services. The information flow is not just between equipment on a BAS subnetwork, or between the BAS subnet and other building equipment across the corporate wide area network (WAN), but is (or soon will be) 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.

'...many new BAS are exposed to network attacks that previously were reserved for Web servers, and have resources that make them nearly as attractive to hackers as a desktop PC.'

What threatens a networked BAS? This article aims to:

- Increase awareness of the threats associated with connecting the building control system (specifically a BACnet system) to a wider network,
- Encourage development of security policies to address building security,
- Present countermeasures available for addressing security threats, and
- Introduce future security direction planned for BACnet.

BAS Network Security

Many different kinds of BAS communication might cross the public Internet: BACnet messages, proprietary http communication between vendor workstation and an operator interface, XML-encoded data from a building controller to a service provider, etc. The messages vary, but all are passed using the Internet Protocol (IP). The BACnet standard provides two ways to pass a BACnet message over an IP network: (1) BACnet/IP (Annex J of the BACnet standard), and (2) Annex H. In both cases a BACnet message is wrapped up in an IP packet for delivery. A good tutorial on this can be found at www.bacnet.org.

For BACnet messages, the BACnet Network Security clause (Clause 24) provides optional security measures such as data origin and operator authentication, and data confidentiality and integrity. However, issues such as key distribution and access control are not addressed. In addition, implementation hurdles due to complexity and other issues have pushed vendors toward other technologies to secure BACnet traffic if needed. As part of the effort to address evolving security concerns in BACnet, the Network Security Working Group (NS-WG) identified the need for a complete BACnet threat assessment. That report[1] presents a detailed review of Clause 24.

BAS communications over IP are not just for new buildings; as existing systems are upgraded to allow "single-seat" control of diverse BAS subsystems, and as connections to outlying equipment become desirable, it is more common to connect separate BAS networks using existing cables and IP protocol. So, BACnet standard network security measures are not applied, even as BACnet IP traffic increases. How then is current BAS traffic secured? *If* it is secured, it is most commonly done by using virtual private networking (VPN) technology from building firewall to building firewall across the Internet (see "Firewalls & VPNs" sidebar). In other words,

IT/BACnet Threats

- **Password Attacks:** Using guessing, brute force, or protocol attacks to gain access to a workstation or secure device.
- **Data Confidentiality:** Most BACnet BAS data is not protected and is available to the outsider who gains access to the network.
- **Data Integrity:** In most BACnet networks, device properties can be modified, data changed or erased, router (or BBMD or B/IP PAD) tables modified, device configuration altered, etc.
- **Denial of Service (DoS):** This is a big one. Many IT attacks flood networks with useless packets. Within the BACnet protocol exist many ways to overload the network with useless valid and invalid packets. Both IT and BACnet DoS attacks can shut down the BAS. Firewalls and intrusion detection can help prevent this.
- **Spoofing Attacks:** Several IT spoof attacks exist (forging the source address so that an attack looks like it was initiated by another machine). Only authentication of BACnet message sources can keep one BACnet device from spoofing another.
- **Eavesdropping, Snooping and Port Scanning:** A passive category of attacks—the attacker does not actively alter or bring down a network. He uses tools for scanning or wiretapping to gain information being passed over the network. He may then use this information for active attacks. Within BACnet, one can read properties to gather information on network architecture, devices, objects, services, system status, security, etc.
- **Exploitation Attack:** IT attacks that exploit flaws in software, such as buffer overruns.
- **Telephone Line Scanning (war dialing):** Scanning for open modems to gain backdoor entrance to the network.

security is provided by the IT department and is layered on top and independent of BACnet communication.

Threats

What are the dangers to today's building control system? If the system is not connected to the WAN, the dangers are fairly well known:

- Human error leading to a potentially insecure, incorrectly configured system,
- Faulty equipment such as a failed cooling system in a room housing vital control or networking equipment,
- Physical break-ins—vandalism, theft, and
- The insider threat—a facility operator performing unauthorized actions.

But what are the threats when we share cabling with the LAN, and through that have a connection to the Internet? What if we have the BAS network sitting right on the Internet with no firewall? Are we opening our building to attack by terrorists, hackers, and other misfits, or are we no less secure since "most attacks come from the inside" anyway?

The 'Who' and 'What' of an Attack

Let's assume for now that someone with ill intent has access to the BAS network. Who are they, and what might they do?

- **Hackers.** They could be students out to play (e.g., turning lights off), or criminals.
- **Criminals** (thieves, terrorists, competitors, etc.). Criminal scenarios include gathering information to gain knowledge of the buildings to break in, or compromising the security system and having doors open. Denial of Service (DoS) attacks could be used for a variety of purposes including: making a political statement, and interfering with business. Terrorists could use low security on a network to shut down facility operation (i.e., as a smokescreen or disruption) to facilitate other destructive activity.
- **Competitors**. Monitoring the network could be used for corporate research. What kind of building control system are you using? How efficiently are you using power? The curious party could be a utility or a controls manufacturer/equipment manufacturer.
- **Disgruntled Employees**. Actually, this threat exists apart from outside access to the network. Various reports have indicated that the majority of damage inflicted on companies is due to unauthorized actions of employees with ready access to systems and information, and results in loss of valuable information, loss of reputation, financial loss, and legal action. Opening the same network to the outside may give a means for a disgruntled employee to hide his tracks or give access to a former employee who has no physical access.

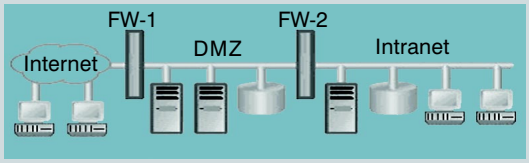
Assuming that the intruder is not an employee with easy access, how would he or she gain access to the BAS network? The most prevalent attacks today are *allowed by* known vulnerabilities in popular software packages (e.g., operating system, e-mail) or known vulnerabilities in common protocols (e.g., SNMP) 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, storing MP3 files, propagating viruses, or gaining privileged access to service partner networks. And while a limited number of applications run on BAS field controllers (operating system: yes, e-mail: no), these BAS devices share the network with other devices that can be

Firewalls & VPNs

A firewall sits between trusted and not trusted networks, or between two distinct internal networks, to provide access control. A typical corporate firewall configuration is shown at right.

Here we see an external firewall (FW-1) facing the Internet that has a rule-based access list (acceptable IP source/destination addresses for DMZ services on a given port) and logging capabilities. It filters incoming packets and disallows any direct communication with the intranet. Behind this first firewall is the "Demilitarized Zone" (DMZ, a standard IT term) where Web servers (including any BAS Web server), ftp servers, e-mail, DNS, and other external-facing servers are located. An intrusion detection system (IDS) would also be located here to monitor the gateway as well as many other network appliances.

All traffic headed for the internal network would be routed through a proxy gateway (in the DMZ). 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 stateful so that it can provide application level



Typical corporate network interface to Internet.

filtering. The internal firewall (FW-2) only allows traffic originating in the DMZ.

Because all traffic passes through the firewall(s), this "security center" is often used as the location for implementing encryption via a Virtual Private Network (VPN). A VPN is essentially an encrypted connection between two boxes on either end of an untrusted network. VPNs protect traffic and provide privacy, authentication and data integrity. While they are often implemented at the firewall (the secure VPN or customer premises based), they may also be managed by an Internet service provider (trusted VPN or network based).

While Trusted VPNs are not encrypted, the service provider routes the connection over a trusted line and also can provide service guarantees (i.e., availability). In contrast, Secure VPNs provide better security and can support remote users.

compromised. A compromised device might be used, for instance, to spoof a BAS controller speaking BACnet or to launch denial of service attacks on the BAS.

The 'How' of an Attack

Many common IT threats can affect the networked building control system. In addition, security vulnerabilities within the BACnet protocol can be used to compromise the BAS. An overview of these is given in the sidebar, "IT/BACnet Threats." A more detailed list, with applicable protocols, and recommended countermeasures, is given in the NIST internal report referenced earlier.[1] These attacks might be used directly on a BAS server or controller device, or might indirectly impact the BAS by shutting down the corporate network.

Countermeasures

So, given these threats, how do you protect your networked BAS? To a large degree, commercially available measures can be taken to increase network security. For example, the Network Reliability and Interoperability Council (www.nric.org) publishes "best practices" guidelines for dealing with various known IT threats.

If you are located in a corporate setting with an IT department, then working with them to address security is the best approach, especially since they regard the LAN as "their network." They own the firewalls, and they can set up VPNs as needed for devices on the BAS to securely access distant BACnet devices, or for non-BACnet traffic needed for communication with off-site service partners.

If you are located in a facility without IT support, BAS security may fall into your hands. Setting up a simple firewall on a dial-up connection along with anti-virus protection might be sufficient, but how do you know? A good approach is to go through the process of developing a security policy (see "Security Policies" sidebar). A security policy will help you follow these principles of network security:

- Know your system (what is your exposure to the not trusted network, what services are you running, and what are the associated risks?),
- Assign least privilege (use access control),
- Apply defense-in-depth (multiple security layers), and
- Use intrusion detection (since prevention is never 100% [see sidebar at right "Intrusion Detection."]).

After assessing and addressing security you'll be confident that you're doing the right thing and aware that security is an ongoing battle. The reality is that security will continue to become more of an issue as the BAS is connected to outside partners' systems. Soon you may be *required* to have a security policy simply to meet legal due diligence requirements of service providers. Until then, you have time to educate yourself and start the process of addressing security.

BACnet Protocol Security Enhancements

And soon you will have available more than standard IT security products to address BACnet security—the BACnet committee's Network Security working group is actively working on building secure messaging into the BACnet protocol, adopting and adapting existing security measures (Kerberos, SHA hash, etc.) when possible. This BACnet protocol security will serve better for addressing BACnet-specific threats such as those given in the sidebar, "IT/BACnet Threats." For instance, message authentication will help protect BAS communication from hostile users/devices on the LAN.

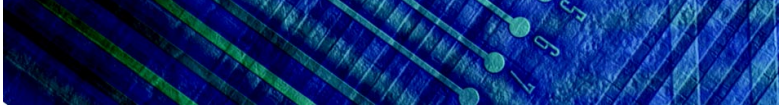
Security Policies

One of the first steps in developing a security policy is a careful risk assessment of both the probability and impact of various threats. For help in risk assessment, see for instance NIST SP 800-30 at http://csrc.nist.gov/publications/nistpubs/index.html. The risk assessment will guide individual policy development, generally classified by program or by issue. Program-level policies: establish the security program, assign responsibilities, state organization security goals, and provide a basis for enforcement. Issue-specific policies define areas of concern (e.g., e-mail, off-site login, personnel, physical security) and state the organization's position and expectations on these issues.

Some Web sites to visit include: http://csrc.nist.gov, http://secinf.net, www.sans.org, and www.windowsecurity.com.

Intrusion Detection

An intrusion detection system (IDS) can be implemented to increase network security. There are two primary types of IDS: network based (e.g., in the DMZ) and host-based (i.e., software running on each desktop PC). 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. 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 e-mail or other method.



Current proposals define a new type of network layer or BVLL (BACnet Virtual Link Layer, defined as part of BACnet/IP) message used to securely communicate messages or session login information—the "BACnet Secure Message." Both session based and non-session-based security configurations are being considered. The session-based scheme would look similar to Clause 24 authentication and encryption, using BACnet secure messages to login, challenge, and then pass messages between two devices. Session-less (or static) security would be enabled by a group of secure devices on a given insecure network sharing a key that is used to pass BACnet secure messages. This could be applied to many situations, such as allowing routers in separate facilities to wrap insecure messages prior to passing across the Internet—a BACnet VPN-like tunnel.

Implementation of BACnet protocol security will add another level of security to the BAS that addresses BACnet vulnerabilities unrecognized by traditional IT security products. The committee has yet to address details of access control in BACnet, and key exchange guidelines. Farther down the road are firewalls designed specifically for protecting BACnet communication and intrusion detection products to monitor BACnet networks and log and report suspicious traffic.

Conclusion

While BACnet secure messages are likely several years away, the time for addressing security is now. Take stock of your current security vulnerabilities and develop a security policy. Then implement that security policy using the many security products currently available. And when the efforts of the NS-WG are realized with the capability in BACnet for secure messaging, future buildings will have a means to address BACnet threats and add another layer of security. Pencil it into your security policy now!

References

1. Holmberg, D.G. 2003. "BACnet wide area network security threat assessment." *NIST Internal Report 7009.*

David G. Holmberg, Ph.D., is a mechanical engineer in the Building and Fire Research Laboratory, Building Environment Division at the National Institute of Standards and Technology (NIST), Gaithersburg, Md. He serves on the Network Security and Utility Interaction Working Groups of ASHRAE Standing Standards Project Committee 135 (BACnet).