Secure Messaging In BACnet®

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

The driving force that conceived BACnet (the protocol supported and maintained by ASHRAE Standing Standards Project Committee 135, www.bacnet.org) was the desire to interconnect different building control subsystems, with the focus on HVAC. Since then, BACnet has expanded to include other building subsystems (life-safety, lighting, access control), but the entire world of communications has evolved. The building automation system (BAS), which was an island to itself, has been inundated by the rising tide of interconnected systems. As outlined in the article, "Enemies at the Gates" (ASHRAE Journal, Nov. 2003, p. B24), this interconnectivity brings new security concerns to the BAS.

Presently, many new facilities are wired such that the BAS shares the main facility IP (Internet protocol) backbone (the local area network or LAN) for higher level BACnet/IP or Ethernet communication. Connections also are made to enterprise systems onsite (e.g., accounting, facility resource planning) and off (e.g., utilities), as well as from one building's BAS to another building's BAS with a link across the Internet. These connections bring risk—security is more important now because BAS are sharing networks with untrusted LAN and Web traffic.

Hopefully, your facility has a firewall and your wide area network (WAN) connection is protected by a virtual private network (VPN), but is that enough protection? Off-the-shelf security techniques help increase security but may

not meet your security needs. "Enemies at the Gates" discusses some of the vulnerabilities that need to be addressed for BACnet systems. One needs to examine the quality of local IT security and the value of BAS assets to determine the need for additional security. How well the BAS is protected from outside attack depends on (among other things) such details as firewall configuration, intrusion detection, monitoring wireless access to the internal network, and patching of operating systems and applications on PCs as well as BACnet devices.

In short, IT defenses may be soft, and if someone succeeds in gaining unauthorized access to a facility network, that intruder may have free access to BACnet communications on that network. If any device is vulnerable to attack, it might then be compromised and used to collect information or even act as a BACnet device that proceeds to exert control or disrupt communication. Considering this leads to the realization that additional security within the BACnet protocol itself might be required.

Secured BACnet traffic is especially necessary as BACnet extends its domain into higher security subsystems (life safety and access control). With secured BACnet messages, an intruder's BACnet client would have no way to probe the network since it could not form a valid message. There could be no collection of information from encrypted message contents. Likewise, no spoofing of another device or exerting any control over network devices can occur.

The BACnet security proposal is nearing release by the BACnet standard committee for public review (target date for release is March 2006). The BACnet security proposal adds a level of BACnet specific security to existing IT security, extending the BACnet standard to offer basic security using signatures for integrity protection, and higher security with encryption for confidentiality. A short introduction to the BACnet security proposal follows. *Please note that this proposal is still under development and will likely change both before and after release for public review.*

Goals of the Proposal

The BACnet committee developed the following goals over time and with ongoing discussion. The BACnet security solution should:

1. Provide security on all BACnet media types.
2. Keep overhead minimal to allow use by the smallest of devices.
3. Keep code space and processing power requirements to a minimum.
4. Secure unicast and broadcast messages, network layer messages, and confirmed and unconfirmed service requests.
5. Address the following attacks: replay, redirection, spoofing, and denial-of-service, if possible.
6. Provide different levels of security using signatures and encryption.
7. Aim for the most common requirements (small/medium sites, Internet connections, etc.) while supporting the less common requirements (large sites, strict security requirements, etc.).
8. Allow for simple and flexible implementations. This means that secure devices can be placed on to legacy (untrusted) networks, and physically secure legacy networks can be made secure via BACnet firewall/routers that act as security proxies for physically secure network segments.
9. Reduce the number of security options to support interoperability.
10. Use advanced encryption standard (AES) encryption and allow for extension to other algorithms.
11. Provide support for future user authorization implementation.
12. Consider key revision and distribution.

The potential to adopt off-the-shelf security standards, such as IPsec and Kerberos, has been discussed many times, understanding that this would allow easier acceptance due to confidence in the protocols. However, the above goals could not be met with these security standards. IPsec does not satisfy the first four goals. It only works over IP and has large overhead. It also does not support broadcasts. However, IPsec might be a reasonable solution for installations that require strong security based on proven protocols. Kerberos also does not work on non-IP networks.

The existing BACnet Clause 24 security does not secure general network protocol data unit (NPDU) traffic, nor does it secure broadcast traffic. It does not meet the needs expressed in the goals. Then, because existing security standards such as IPsec also do not meet the needs of BACnet, the BACnet Network Security Working Group began the difficult process of developing a custom BACnet security solution following best security practices.

BACnet Network Security Architecture

The proposed BACnet network security architecture provides device authentication, data hiding, user authentication, and user authorization. To achieve these network security

goals, the BACnet standard is extended with a set of network layer security messages including Challenge Request, Challenge Response, Security Payload, and Security Error. The Security Payload message is used to wrap normal BACnet messages for secure communication.

Device authentication is achieved through the use of message signatures and a shared signature key. Data hiding is achieved through shared keys and encryption of the message in the payload. User authentication is achieved through the use of shared user keys. Standard user authorization via a BACnet object defining authorization rules has not yet been fully developed.

In the BACnet security proposal, the four types of keys are (*Figure 1*) a signature key that is shared by all BACnet devices across the facility; a well-known encryption key that is shared across the facility; private encryption keys that are less widely distributed; and user keys that are unique to each user or group of users.

The signature key is used to sign messages, which provides for device authentication. The signature key is known by all secure BACnet devices in the BACnet internetwork. Knowledge of the signature key allows a device to participate in the secure BACnet network.

Encryption keys encrypt message contents for data hiding. The well-known encryption key is known by all secure BACnet devices in the BACnet internetwork. Knowledge of the encryption key allows a device to participate in encrypted BACnet conversations. The less well-known encryption keys are used by devices that must communicate in a more secure manner amongst themselves.

User keys are used to verify user identity claims in BACnet secure messages. Each user key is known by each device that needs to verify user identity, as well as by each device that is capable of initiating services on behalf of the particular user.

It is anticipated that the security proposal will include a mechanism for initial distribution and revising of keys.

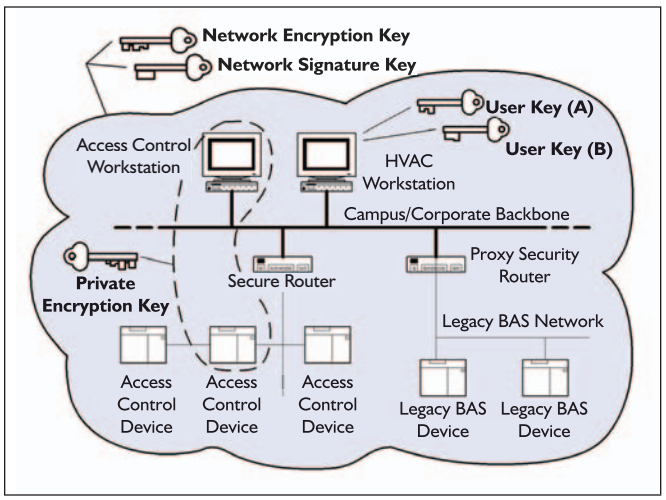

Figure 1: Four types of keys in network.

Control	1 Octet
Key Revision	1 Octet
Encryption Key ID	1 Octet
Source Device ID	3 Octets
Destination Device ID	3 Octets
Message ID	3 Octets
Timestamp	4 Octets
SNET	2 Octets
SLEN	1 Octet
SADR	Variable
DNET	2 Octets
DLEN	1 Octet
DADR	Variable
Authorization Mechanism	1 Octet
User ID	Variable
Service Data	Variable
Padding	Variable
Signature	16 Octets

Table 1: Security header format (from CN-77-16).

Securing Messages

The basic level of security that can be applied to a BACnet message consists of signing each message using HMAC (a keyed-hash message authentication algorithm) and MD5 (a commonly used hash algorithm), and marking each message with the source and destination identification numbers (Device ID), a Message ID, and a Timestamp. A higher level of security is provided by using encryption. The fields of the security header that is attached to all types of security messages are shown in *Table 1* and include: Control, Key Revision, Encryption Key ID, Source Device ID, Destination Device ID, Message ID, Timestamp, source and destination information from network layer header, Authorization Mechanism, and User ID.

All secure messages include the source and destination device IDs as well as network numbers in the security header of the network layer security messages. The inclusion of these values allows the security signature to be calculated on the source and destination device identities to stop redirection and identity switching attacks. Because requiring source network number in every secure message requires that all secure BACnet devices know their network numbers, the security proposal provides a new what-is-network-number message that is used to request the local network number from other devices on the local network.

Figure 2 shows how a BACnet Read Property message would be secured. The Read Property message's application protocol data unit (APDU) portion of the message is placed into the Payload parameter of a Security-Payload message. The original message network layer header (network protocol control information, NPCI) is updated to indicate that this is now a network layer message, and the message type field is added and set to Security-Payload. The security header will indicate that the encapsulated message is an APDU

so this information is not lost. The signature is calculated over the security header and payload fields and tacked on the end of the message.

The Message ID fulfills several purposes in securing BACnet messages. It is used to detect the replay of messages, to associate security responses with security requests, and along with the Timestamp field, provides variability in otherwise identical messages.

Timestamp is used mainly for prevention of message replay but also serves as a source of variability in the message content so that messages that are repeated frequently do not generate the same signature. The clocks of secure devices must be loosely synchronized. If the time stamp on a message is outside the security time window, then the message is returned and clock issues need to be addressed. Within the security time window, Message IDs are checked to confirm that a message has not been replayed.

The signature is included in all secure messages. Additional security is provided by encryption, for which the BACnet security proposal specifies the use of advanced encryption standard (AES). In considering encryption algorithms and the concern of implementing AES on simple devices, the Network Security Working Group noted that AES has been implemented successfully in smart card applications for simple processors. In addition, it was noted that simple BACnet devices only need to use encryption for receiving signature key updates for which decryption time is not a limiting issue. The security proposal will provide a mechanism to support other encryption algorithms in the future.

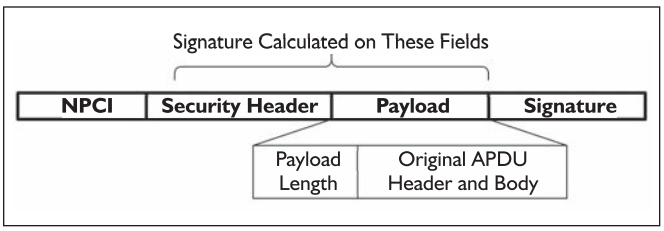

Figure 2: Example of secure wrapping of a read property message—the network layer header (NPCI) is updated to indicate this is now a network layer message of type Security-Payload, and the original read property message (APDU) is placed into the payload.

Network Security Policies

The two network trust levels are trusted and non-trusted. Trusted networks can be so designated by virtue of being physically secure, or by use of protocol security (signatures and/or encryption). Non-trusted networks are those that are physically non-secure and do not use protocol security.

The four corresponding network security policies are plain-trusted (no protocol security), signed-trusted, encrypted-trusted, and plain-non-trusted. A common example of a plain-trusted network is an MSTP (master-slave token passing) network, where all devices are locked up and no direct network connections are available outside of the locked space. A common example of a plain-non-trusted network is the corporate LAN.

Device-Level Security

The proposal does not restrict secure devices to trusted networks. Secure devices may be located on non-trusted networks and rely on end-to-end (device level) security for secure communications. Although secure networks are created by setting the security policy for a network and all devices on a secure network must be configured with the security policy of the network, end-to-end security is determined on a device-by-device and request-by-request basis.

Secure BACnet devices are configured with a network security policy for each attached network and with a base local security policy. The base local security policy dictates the device's minimum level of security for sending or receiving messages. Where this policy differs from the network security policy for the network being communicated over, the higher of the two values dictates the minimum level of security for the communication.

User Authorization

The proposal provides a simple user authorization mechanism. This mechanism provides a 16-bit User ID field that identifies the user or user group requesting an operation. The proposal also provides a new User-ID-Challenge security message that can be used to verify claimed User ID. It is expected that future versions of the security standard will provide additional authorization mechanisms that use standard authorization technologies.

Summary

The security proposal is nearing release for public review. Your participation in the review process is welcome. To check on status of the document, visit www.bacnet.org. If the document is out for public review, it will be available at the Technology and Standards section at www.ashrae.org.

In addition to the BACnet security messaging proposal, work is being done on a BACnet firewall router (BFR) program. The intent is to have a firewall that can do BACnet message filtering, which will become the core of a secure BACnet router. This code is in the public domain and available at http://sourceforge.net/projects/bfr.

BACnet protocol security is coming soon and will offer new protection for BACnet networks that overlap open networks or are vulnerable to attack via untrusted ports and channels. The ability to authenticate devices and users, sign messages, and use AES encryption will ensure that devices and communication can be protected.

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).