NIST TN 1615

Authentication and Authorization of Building Information Users in BACnet

Stephen J. Treado
Alan B Vinh
Steven T. Bushby

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

NIST TN 1615

Authentication and Authorization of Building Information Users in BACnet

Stephen J. Treado
Alan B Vinh
Steven T. Bushby

Building Environment Division
Building and Fire Research Laboratory

September 2008

U.S. Department Of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Acting Director

Abstract:
Building automation systems frequently monitor critical building information that would be extremely useful for emergency responders including the status of alarms, locations of occupants, temperature, and air quality conditions. Emergency response can be improved by providing access to this information during building emergencies. This report describes a proposed authentication and authorization methodology for providing controlled access to building information to approved external entities such as police, fire and public safety officials, while at the same time preventing unauthorized access and use of the information. Enhancements to the BACnet building automation system communication protocol are proposed to provide this functionality.

Keywords: access control, authentication, authorization, BACnet, building control systems, emergency responders, protocol, security

1. Introduction

As building automation systems become more sophisticated and powerful, the possibility of tapping into and distributing building information in real time to remote monitoring stations and emergency responders becomes more attractive. The components of a building automation system incorporate many sensors, detectors and cameras that could provide critical information about conditions inside a building to emergency responders and public safety officials. Building automation systems include heating, ventilation and air-conditioning (HVAC), lighting, access control, fire detection, and security systems. The availability of critical building information could help to improve the efficiency and effectiveness of incident responses, and minimize safety risks to emergency responders. Typical building information might include types and locations of alarms, building floor plans and system schematics, locations of occupants, locations and types of hazardous materials, and real-time data about conditions in the building. This emerging concept has been discussed previously in (Holmberg, et al., 2006).

In order to make this sort of building information system a reality, several issues must be addressed. The building information must be collected, transferred and presented in a standard, understandable manner. The proper infrastructure must be in place to enable the building information to be accessed from remote locations, including dispatch centers and incident command posts. This may require both wired and wireless links at various locations. Another critical element is the secure dissemination of the building information only to authorized users. This consideration is not unlike that faced by designers and implementers of information technology (IT) and ecommerce systems, which necessarily must incorporate identity verification, data security, privacy and authority mechanisms to function effectively. However, building information has some unique characteristics that prevent IT-centric authentication methods from being adopted wholesale, and require some special considerations.

This report focuses on the development of a method to authenticate remote users of building information and determine what information they are authorized to access, or what actions they are authorized to perform, generally referred to as authorization. A typical use case would be allowing public safety officials at a remote dispatch center, firehouse or police station to access building information in real-time. Another related use case would be to allow emergency responders en route or on the scene of an incident to access building information to help plan or coordinate their response. The proposed methodology involves enhancements to the BACnet building automation system communication protocol standard (ASHRAE, 2004), along with additional components as will be described.

2. Overview of Building Information Data Flow and User Authorization

There are many different aspects to building information, including information that is relatively static, and information that is dynamic. Some building information, such as sensor readings and video streams, is dynamic and would be provided by the building automation system, while the static building information, such as floor plans and

equipment schematics, would reside in a building information model. While the specifics of the integration of the static and dynamic building information are beyond the scope of this report, the delivery of the dynamic information is based on enhancements to the BACnet protocol.

The proposed method for enabling and controlling access to building information is based on the following key elements:

- A strong and secure proof-of-identity credential for each remote user– it is suggested that this be a version of a federal Personal Identity Verification (PIV) card, or similar credential;
- A hierarchical structure of public safety personnel databases;
- Role-based authorization;
- A building information services and control system (BISACS) with secure connection capability; and
- A secure link between the BISACS and the BACnet building automation system (BAS) using a building services interface, in this case functioning as a BACnet Services Interface (BSI).

A strong identity credential is an essential element of a system for securely controlling access to building information. The right to access building information is tied directly to identity, and the associated roles, along with other factors such as jurisdiction, duty status, incident status and chain-of-command. For example, access rules might limit access to building information only to personnel currently on duty, or only in certain jurisdictions, or only when an incident involving the specific building is underway. The federal PIV card provides a good model for a strong identity card, and for the purposes of this discussion, it is assumed that this or a similar format will be used. NIST Special Publication 800-73-1 (Dray, 2006) describes the characteristics of the federal PIV cards, including format, data elements, keys and certificates. It would be the responsibility of the issuing agency to properly verify and control the issuance of PIV cards for public safety personnel.

The issuing jurisdictions would create and manage the public safety databases that contain the identity information and rights and privileges of each individual. Public safety personnel would be enrolled in their local jurisdiction's database, which would be part of a hierarchical network of public safety databases spanning multiple jurisdictions. Negotiations between jurisdictions and mutual recognition and acceptance of databases would have to be implemented in accordance with higher-level policies and with adequate assurances for security and accuracy.

Figure 1 presents a schematic depiction of the functional components of the building automation system, the BSI, the databases, and the remote clients (e.g., dispatch centers, etc.) as they relate to the process of providing building information to remote users. This

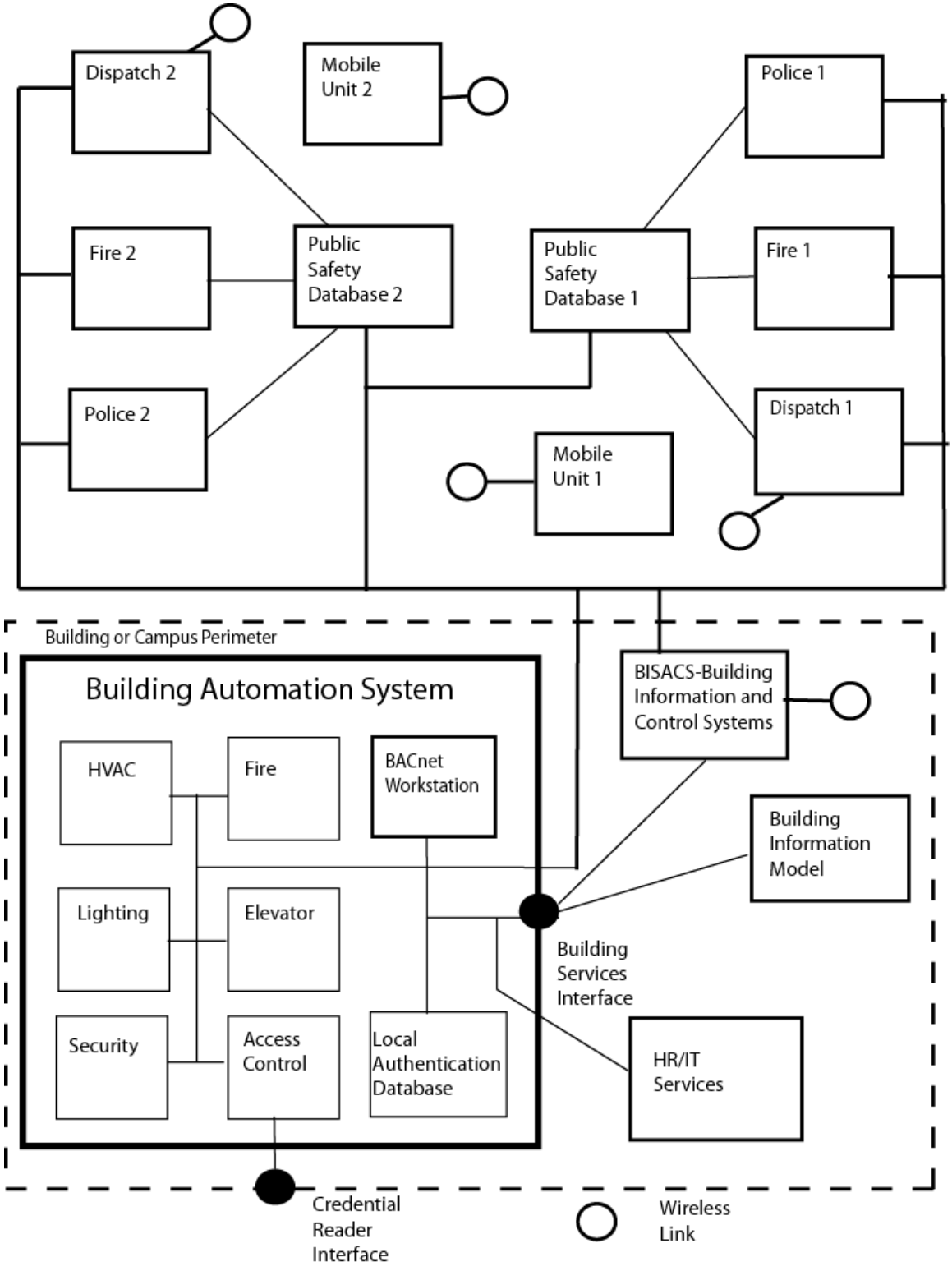

Figure 1. Schematic diagram of building automation system, building information server and public safety network

is an example configuration, and does not show all of the detail or possible network configurations. It is meant to represent the necessary functions rather than specific hardware or software elements. This figure does not show all the possible or usual information exchange functions that might be going on at any point in time, such as email or web surfing.

The general idea is that there is a BACnet BAS network internal to the building, a network link to other building information systems such as human resources and IT, and a network link to the outside world. The reason for the link to IT and human resources (HR) is for sharing common information on user credentials, rights and roles. In addition, specific applications that involve remote user access to building systems by authorized users via the internet or other network can do so directly without interacting with the BISACS. This would include BACnet Web Services, for example.

Public safety operations such as police, fire and dispatch also have network connectivity, as well as wireless communication capabilities. The communication between the building and the public safety operations would be handled by the BISACS and the BSI. This configuration has several advantages. First, all of the remote users would interact with the building through the BISACS, so the protocols can be standardized, and communication maintained in a secure manner. The method for establishing a secure connection to the BISACS is described in (Vinh, 2007), and is based on an exchange of certificates and web services. The BAS would communicate with the BISACS through the BSI, also using web services, so that that information exchange can be handled in a standardized and secure manner. Using the BISACS as the middleman avoids the need to provide multiple interfaces between the building and the outside, as well as eliminating the requirement for the BAS to maintain extensive databases related to remote users of building information. The BSI would provide any building information aggregation and translation functions, and would be tailored to each building as required.

The BAS in Figure 1 is shown with two prototypical interfaces. The *credential reader interface* connects to the credential readers for the access control system. These would typically be located at access points such as doors and gates, but other uses are also possible. For physical access control, users present their identity credential to the credential reader at the desired access point. Local users are usually enrolled at the site, so their identity information and rights and privileges can be verified using the local database contained in the BAS. For logical access control, including remote users, the credential reader would be part of the work station or remote terminal device. Remote users would be enrolled into a public safety database through their corresponding jurisdiction. The BAS may also exchange information or access external databases through the *building services interface*. This external interface provides for information exchange, sharing of resources, and network visibility across the enterprise.

It is through the building services interface, in conjunction with the BISACS, that remote users would need to authenticate their identity in order to be allowed access to building information from the BAS, via the BIS. The difference between remote logical access and physical access is that the authentication and authorization information would be

collected in a public safety database rather than in the BAS database. The public safety database would need to be a secure implementation under the control of authorized public safety officials, who would manage the collection and modification of identity information, rights and privileges of the public safety personnel enrolled under their jurisdiction. There will likely be a hierarchical structure of multiple public safety databases spanning police, fire and public safety districts, municipalities and geographical regions.

Figure 2 shows a more detailed overview of the BISACS structure and functionality. The BISACS base server is the main route for accessing building information and can be configured to manage data transfer going in or out of the building. In addition to the building services interface (in this case a BACnet Services Interface), a sensor network services interface (SNSI) is shown on the building side. The SNSI is just another network being accessed through the BISACS, which is capable of providing an interface to multiple building networks of different flavors. As indicated in figure 2, notice that the BISACS may be configured to support a host of "services interfaces" (SI); these services interfaces serve as access points to their respective devices or network of devices. Alerts and commands can be monitored or generated from outside of the building, and are managed through the BISACS. One or more BISACS proxy servers may be implemented to facilitate scalability and to provide redundancy.

Figure 3 shows the BISACS communication and user validation processes in greater detail. To gain access to the BISACS, the remote/external user must connect and log into one of the nodes that is a part of the BISACS network. Although the user authentication process may pass through a BISACS Proxy Server (BPS), the accessing of the data store is actually done at the BISACS Base Server node (BBS). Notice that any drill down processing or commands/requests to access or control a device have to go through the BBS. The data stores containing the user information and certificate information may reside locally or externally to the building; this includes information for internal users such as employees of a building and/or external users such as first responders. The BISACS can be configured to handle the authentication of internal and external users, and maintains secure communication for each session. The BISACS server itself has a secure communication link to the BSI. More details about the BISACS can be found at the BISACS Web Page (http://cic.nist.gov/bisacs/index.html).

From the point of view of remote user authentication and information management using the BISACS approach, the BACnet standard would need to accommodate the building services interface (BSI), and implement a set of standard commands and data structures relevant to the exchange of building information.

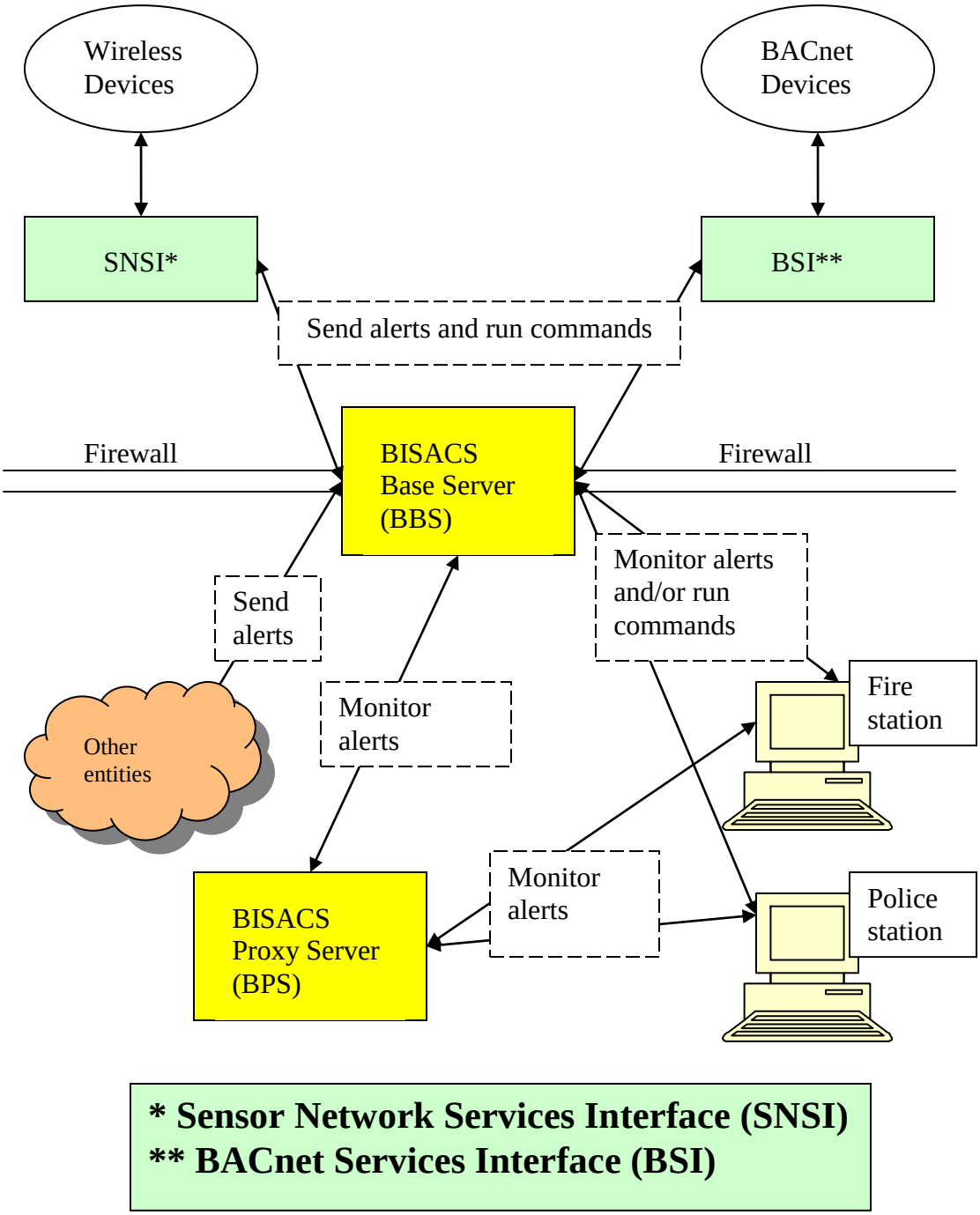

Figure 2. BISACS overview diagram

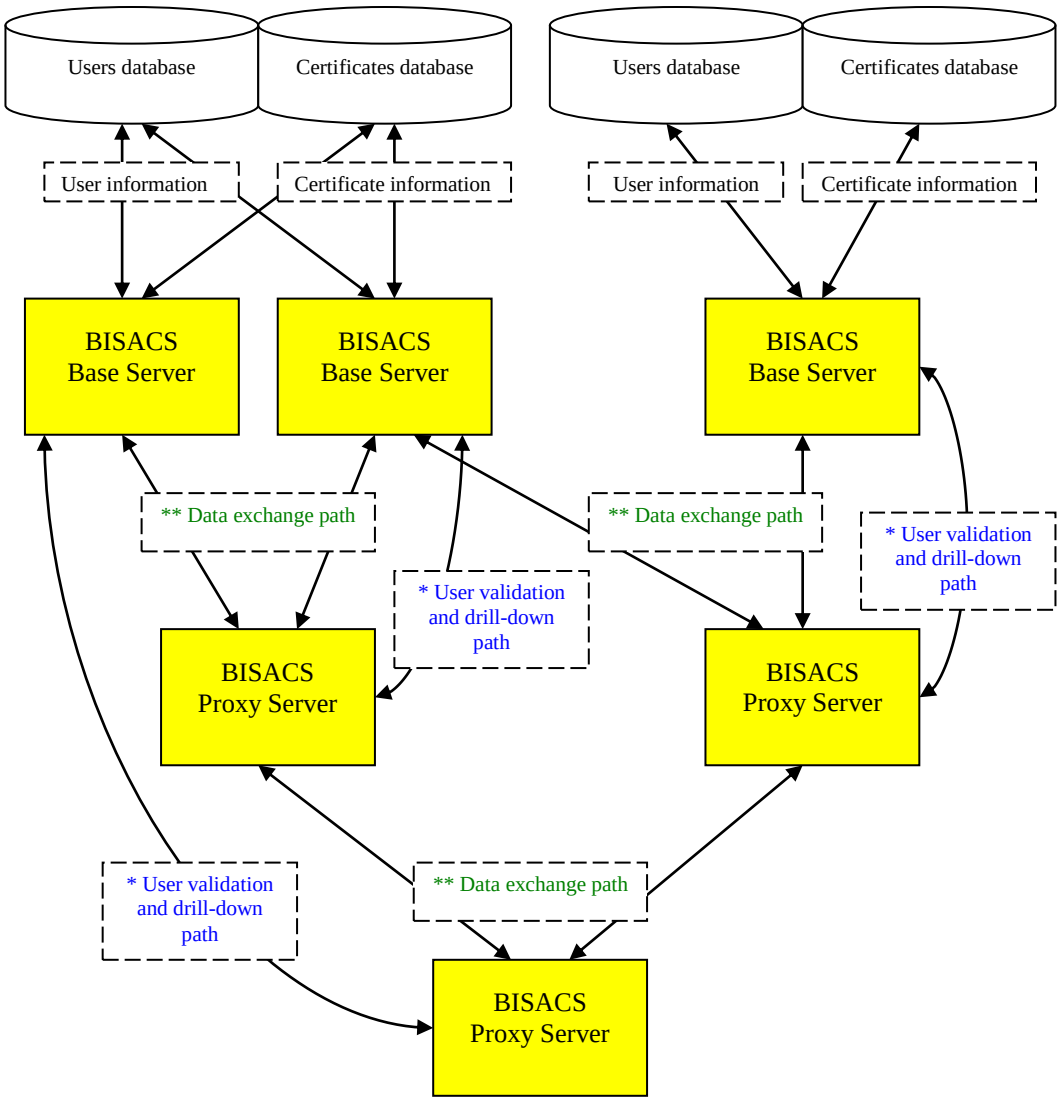

Figure 3. BISACS communication and data flow diagram

There are several other considerations that are relevant to the development of the BACnet authentication and authorization framework. These are:

1. Build on the proposed network security mechanisms that are being developed by the BACnet committee;
2. Harmonize with, and reuse the appropriate physical access control data structures;
3. Provide a means to integrate with IT network authorization infrastructures and human resources databases, including Active Directory and Lightweight Directory Access Protocol; and
4. Provide a means for enabling and controlling access to BACnet networks by external entities, such as authorized emergency responders.

The following is an outline of a proposed framework for providing user authentication and authorization in BACnet. The proposed framework includes a new BACnet object, a Logical Access Rights object, along with a methodology for assigning and determining access rights and roles to users.

3. Authentication and Authorization Considerations for BACnet BAS

Authentication and authorization are two inherently related concepts that are singled out in their treatment in BACnet in order to simplify the functions with which they are associated. As such, and in the context of users, *authentication* is associated with identity verification, while *authorization* is associated with rights and privileges. In other words, first we determine *who* you are, and then we determine *what* you are allowed to do (and *when* you are allowed to do it). While this distinction may seem somewhat arbitrary, it does provide a convenient way of separating the two functions into discrete steps. Authentication also carries with it a related concept of the verification of the authenticity of network communications, including the integrity of the message, and the identity of the sender. This is a slightly different use of the term authentication that should not be confused with user authentication.

3.1 Physical Access Control in BACnet

The Life Safety and Security Working Group of the BACnet committee has developed enhancements to the BACnet standard to accommodate physical access control systems. These enhancements have been summarized in (Ritter, et al., 2006), and include new BACnet objects to represent access entities, access points, access zones and access rights. This framework includes both user authentication and authorization as it relates to controlling physical access to locations and resources. There are obvious parallels between physical access and logical access, but also some important differences. Physical access control involves a transaction in which a user requests entrance through an access point. This transaction involves presentation of a credential, identity verification, followed by a check of access rights and rules to determine if entry should be granted. In the proposed BACnet addendum for physical access control (Addendum j

to Standard 135-2004), this process is implemented through the use of seven new BACnet objects, as follows:

1. Authentication Factor Input;
2. Access Door;
3. Access Point;
4. Access Zone;
5. Access Credential;
6. Access User; and
7. Access Rights.

These objects contain all of the network visible information required to implement a physical access control system. The access user represents a person or thing that is trying to pass through an access point. Thus, the transaction always commences at an access point and involves a tangible object, it involves a single type of request, and the flow of information is inherently well defined. Also, the access rights are implemented within the access control system, specifically to allow an access decision to be made.

If we broaden our view of access control to include logical access, the relatively tightly bounded problem of physical access control is transformed into a much larger and more complicated domain. Users can be people, devices or processes, and the requested services can be anything that might be done using BACnet. Requests for services can be generated anywhere within the system, and the number and variety of possible unique service requests are substantial. The goal would be to enable, but not require, each service request to be verified as to the identity and rights of the requestor, using a network visible framework.

3.2 Authentication and Authorization Provisions of the BACnet Network Security Proposal

There are several references to authentication and authorization in the BACnet network security proposal that is undergoing public review (Proposed Addendum g to Standard 135-2004). Two possible mechanisms for performing authentication or authorization that are mentioned in the proposal are based on the use of a User ID or an Application Specific key. Both the authorization mechanisms and the use of the application specific keys are left as local matters. However, formalizing these mechanisms may prove to be the most efficient way to add authorization to the BACnet standard.

3.3 Logical Access Control in BACnet

BACnet service requests are generated in two general ways. Most service requests are generated by processes, and consist of reading or writing to object properties, event logs, or other routine operations. The other main class of service requests comes from users

through an operator work station or other control panel. In either case, the actual BACnet messages are exchanged between BACnet devices that are acting on behalf of the source entities. This suggests that the BACnet device level is the logical location for user authentication and service request authorization, and more specifically, the message source device has the responsibility for authorization. The BACnet device would know which objects it contains, and would be configured to only send service requests from processes that are authorized. Work stations or other user interfaces would first authenticate the user by evaluating their credentials, determine their identity, and then only allow them to send service requests for which they are authorized. This process would be essentially the same as the process for physical access control, except it would utilize logical access rights instead of physical access rights.

The authorization process referred to in the above would be accomplished by examining the users' logical access rights, which would be contained in Logical Access Rights objects, as will be detailed below. The authorization would either be for a user, a device, or a user/device combination, so access rights would be compiled in that manner. For convenience, the term user will be assumed to represent any of these variations. This general process is based on several assumptions, as follows. First, it is assumed that network communications are secure in accordance with the proposal for BACnet network security. This means that it is possible for a receiving device, or any device for that matter, to determine if a message is valid, which device sent the message, that the message source was a trusted device, and the message was not spoofed or tampered with. This assumption can be justified either on the basis of the strength of the network security proposal, or on practical considerations related to the need to compartmentalize the simultaneous development of BACnet network security and authorization.

Another assumption is that the initial system configuration is properly executed and system operation is properly programmed so that the appropriate roles, rights and privileges can be associated with users. This assumption can be justified on the grounds that the system must be implemented properly in order to function properly. There is a chicken and egg aspect to this, much as there is with general network security. If the system is broken, it will not function properly, irrespective of authorization considerations.

Based on these assumptions, the major hurdle to overcome is defining the data structures and messages required to enable service request authorizations. Within the context of BACnet, logical access rights could apply to all information and capabilities in a device or they could be applied at a finer granularity such as on an object basis, on an individual property basis, or even to the allowed ranges of property values. This represents a tremendous range of granularity, the need for which must be determined, and perhaps justified. We can start from the assumption that maximum granularity is desired, and proceed from there; limiting or eliminating unneeded granularity should be straightforward.

Another issue that needs to be addressed is whether placing the burden of service request authorization on the sending device is sufficient, or whether it should be possible for the

receiving device to verify that the requesting entity is authorized. There may be some critical sub-systems that require such a double check before executing important commands. Incorporating this feature has implications on the data and message structures, since the recipient device will need sufficient information about the requesting entity to initiate the authorization check. Since the service request is coming from the source device rather than the original source entity, the access rights will need to be compiled on a user/device basis. A related issue is that the service request authorization process is considered to be optional, not required. This means that, obviously, some requests will have had the authorization check performed, and others will have not.

3.4 Summary of Proposed Authentication and Authorization Mechanism for BACnet BAS

The proposed solution for BACnet authentication and authorization is based on a system using BACnet User ID's, BACnet application specific keys (ASK), roles and a new BACnet Logical Access Rights object, as summarized in the following:

1. User authorization rights would be specified in logical access rights objects;
2. Access rights could include devices, objects, properties and fields as desired;
3. Sets of user authorization rights would be collected into user roles;
4. Each set of devices that form a trusted group would share an ASK;
5. The appropriate ASK would be distributed to each authorized device upon initial configuration and updated as required;
6. Service requests would include user ID, role and the ASK;
7. Source devices providing the appropriate ASK would be assumed to have verified and provided the correct user ID, and would be assumed to have performed a user authorization check before issuing each service request; and
8. Receiving devices could optionally verify authorization rights using user ID or role.

The advantages of this approach are that authorization would be optional, and that it will require a minimal amount of additional message overhead. The specific method used to verify access rights would not be prescribed at this time, but the data structures, in the form of Logical Access Rights Objects, would be network visible

Regarding authorization of remote users, particularly emergency responders or consumers of building information, their rights could be assigned based upon predefined external roles (e.g., Incident Commander, Dispatch, etc.) which are associated with specific internal access rights and roles, as defined for each BACnet installation. The mapping of roles to rights would be negotiated by the BACnet external interface (BACnet Services Interface, BSI). Authentication of remote users who are not enrolled locally would be handled via a public safety or other remote database.

3.5 Logical Access Rights Object

The purpose of the Logical Access Rights Object is to associate specific rights to users and/or devices grouped into roles. Thus, the rights will be assigned to credentials, and the credentials will be grouped into roles. This will allow roles to be named and referenced within the larger context of the BACnet network. The basic structure is as follows:

Access Right- Source entity (user, device)
Device- Service allowed (time, date, condition)
Object- Service allowed (time, date, condition)
Property- Service allowed (time, date, condition, priority)
Field- Range allowed (time, date, condition)

A blank entry is considered to be a wild card (i.e., if no objects are listed, access to all objects is allowed). The services allowed are limited to those that are possible for the corresponding element.

Multiple logical access rights are allowed for any user or group of users. In order to handle combined logical access rights of users and devices, such as would occur with a person at a work station, logical access rights would be combined using AND logic. Access rights can be grouped to represent a role. In this manner, users can be assigned to roles which can subsequently be used for authorization decisions. This would be useful if the source device was not capable of performing a strong authentication check, but was able to provide basic information about the user's role. In this case, the user ID would not be known, but the user would have had to provide some authentication data, such as a PIN or password that indicated that they were authorized to access the system at some level. The receiving device could then evaluate the rights assigned to that role, or choose to deny access based upon network or application specific policies.

4. Example Use Case

The procedure for authenticating remote users of building information requires the initial implementation of a public safety database, a building information services and control system (BISACS), and a building services interface (BSI). At the public safety side, each of the public safety personnel at a specific organization, such as the city, county or state police department, or local fire department, would be issued a PIV card, in accordance with the requirements described in FIPS 201-1 (Federal Information Processing Standards, NIST, 2006), or similar procedures. It is essential that strict identity verification be conducted before a PIV card is issued, to prevent any fraudulent cards from being created. This is the reasoning behind the recommendation for the use of the federal PIV guidelines, since these have been extensively reviewed, and are considered a best practice for providing for a process to control the issuance of identity cards.

Once the public safety personnel have been issued a PIV card, the public safety database can be implemented. Essentially, each of the public safety personnel would be enrolled

in an organization specific database, which would include their identity information along with their rights and privileges. This process is similar to enrollment in a physical access control system, except that the rights and privileges would include more than access points and zones, but would encompass logical access rights as well. There is no reason why the database could not do double duty both for physical access control and logical access control. All the typical security safeguards and login verifications would be required for the management of the organization specific public safety database, to ensure the validity of the information.

On the building side, a building information server would be established and configured for the specific building, or multiple buildings. The BISACS would exchange information with the BAS via the BSI, using a web services implementation that would publish dynamic building information, such as alarms and alerts to the BISACS for retransmission to remote consumers, such as public safety personnel. The BISACS would also provide static building information, such as floor plans and equipment schematics, as provided by the building information model through the BSI.

For the application of providing building information to emergency responders, the flow of information would be one-way; from the BAS to the BISACS. The building information, including both the static and dynamic components, would be available to authorized users only. This authorization would be handled by the BISACS. For the case of remote commands to the building, the BISACS would transfer the commands to the BSI, which would translate them into specific messages to the appropriate building automation system controllers. For example, smoke dampers could be opened remotely, or building elevators operated from outside of the building to provide emergency egress.

5. Conclusions

A structural framework and data model have been developed for allowing the transfer of building information to emergency personnel outside of the building, and the remote control of building systems. The methodology incorporates a building information services and control system server, a building services interface and a user authentication capability to provide for secure access to building information only by authorized users. The data models and communication protocols required to implement the system have been identified, as well as the required functionality and operating procedures necessary to enable wide scale use.

The use of the type of system described here could greatly improve the ability of emergency responders to formulate and execute effective response plans during emergency events. This should result in reduced loss of life and property damage for building owners and occupants, as well as reduce the risks to emergency personnel.

References:

ASHRAE, ANSI/ASHRAE Standard 135-2004, BACnet- A Data Communication Protocol for Building Automation and Control Networks, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Atlanta, GA, 2004

Dray, J., Guthery, S., Schwarzhoff, T., NIST Special Publication 800-73-1 Interfaces for Personal Identity Verification, National Institute of Standards and Technology, Gaithersburg, MD 20899, 3/2006

FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, National Institute of Standards and Technology, Gaithersburg, MD 20899, 3/2006

Holmberg, D., Davis, W., Treado, S., Reed, K., Building Tactical Information System for Public Safety Officials, NISTIR 7314, National Institute of Standards and Technology, Gaithersburg, MD 20899, 1/2006

Ritter, D., Mundt, H., Isler, B., Treado, S., Access Control in BACnet, ASHRAE Journal Article, American Society of Heating, Refrigerating and Air-Conditioning Engineers, Atlanta, GA, 2006

Vinh, A., Building Information Services and Control System (BISACS): Technical Documentation, Revision 1.0 NISTIR 7466, National Institute of Standards and Technology, Gaithersburg, MD 20899, 9/2007