Securing Physical Security Systems on the IP Network

By Bob Beliles and Dave Twinam

Among the most important new challenges IP networking brings to physical security systems is ensuring that physical security assets are not compromised.

When properly used and configured, IP networks deliver formidable security protection. Network security features authenticate and segment users, monitor anomalous behavior and implement policy-based responses.

The key to securing networked safety and security systems requires a little research on your part and communication with your IT counterpart. Let's examine a few scenarios and the network security mechanisms that warrant evaluation and implementation with physical security devices.

Virtual local-area networks (VLANs) provide a logical separation of video surveillance and other physical security information from other network applications.

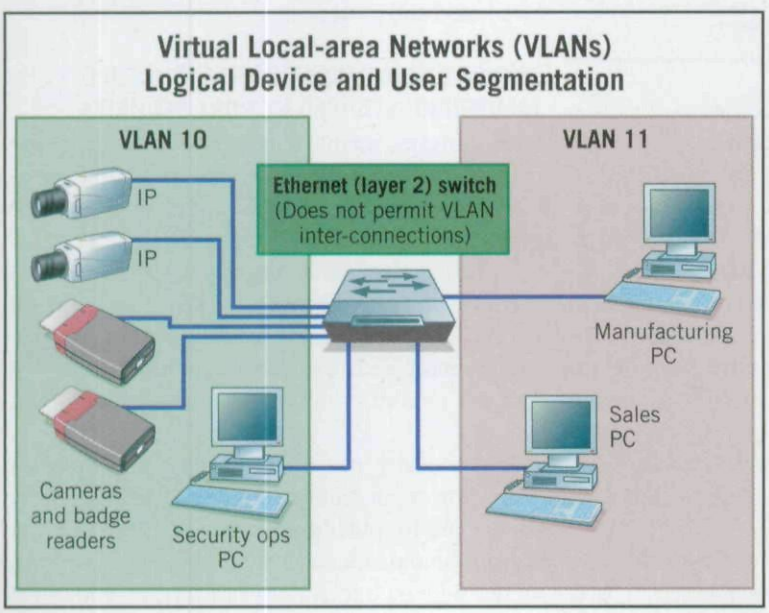

DIAGRAM COURTESY OF CISCO SYSTEMS INC.

UNAUTHORIZED ACCESS: PASSWORD MANAGEMENT, USER RIGHTS AND PRIVILEGES

Surprising as it may seem, many businesses overlook password management. Be sure that all physical security devices use something other than the vendor-provided default password. Additionally, passwords should be changed regularly to meet various compliance requirements and best practices.

A networked security system also should provide user rights and privileges that delineate between casual users, system operators and administrators. In some cases, non-safety-and-security personnel may be granted access to certain devices, such as lobby cameras.

It's imperative that these casual or secondary users are not given the same capabilities as operators or system administrators, particularly for control of pan/tilt/zoom cameras.

LOGICAL ISOLATION: USER AND APPLICATION SEGMENTATION WITH VLANS

Virtual local-area networks (VLANs) represent one of the more popular approaches used in commercial and enterprise networks today to segment users, applications and devices (including PCs, servers, IP phones and cameras).

Simply put, VLANs provide a logical separation of video surveillance and other physical security information from other network applications, such as financial network applications, IP telephony and general Web browsing.

A single network wire or a network switch can support multiple applications that are virtually isolated, as if the application(s) were on a separate wire or a separate switch. Even in large campus-

spanning physical security operations, you can logically group all your video surveillance cameras, access control devices, and safety and security monitoring and recording platforms into one or a handful of protected VLAN groups.

VLANs are one way to ensure that only specific employees can view security video or gain access to the security server log files. Network administrators can put all security devices and users into one VLAN and general business users into other VLANs.

For example, IP phones generally are placed in their own VLAN, which also allows for the prioritization of latency-sensitive voice traffic over other forms of network application traffic, such as e-mail or Web browsing. In many cases, organizations can augment their security posture by using VLANs for their video surveillance applications.

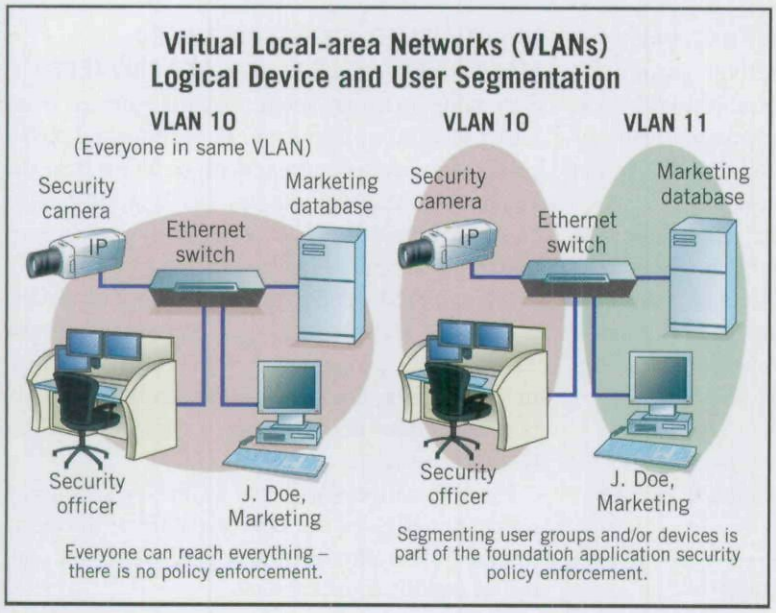

DIAGRAM COURTESY OF CISCO SYSTEMS INC.

VLANs are one way to ensure that only specific employees can view security video or gain access to the security server log files.

By default, all physical connections — Ethernet ports on a router or a network switch, for example — are initially configured to be the same VLAN. Systems integrators or IT departments must configure the router or switch to define which physical ports and devices are on a given VLAN.

Setting up VLANs requires careful thought and strategic planning. For example, it would be ill-advised to set up per-camera or per-security-device VLANs. This would put an unnecessary burden on the network infrastructure by requiring more routers, consume more IP addresses, and entail a lot more network configuration, with the potential result of subpar performance.

It also should be noted that although VLANs enable user or application segmentation, VLANs by themselves should not be considered a security feature. But in combination with other features, they can be part of a highly secure security deployment.

BLOCKING ACCESS FROM UNAUTHORIZED DEVICES USING ACCESS CONTROL LISTS

Network (or logical) access control lists (ACLs), supported by all business-class routers and switches, can be used to enforce security policies. Much like security access control lists, which regulate who can enter a building under certain conditions, logical ACLs are a sequential list of permit and deny statements.

Network routers and switches can use these to protect the network and network-connected devices, such as badge readers, cameras or network video recorders. ACLs can be used to block access or commands from unauthorized devices. Likewise, ACLs can be used to keep a device (such as a recorder) from sending information to an unauthorized device.

Network or security managers can create one or more ACLs that would permit access to video or the security server audit logs from devices that are physically located in a security operations center or that are part of an authorized user VLAN.

By tying the ACL to a user group VLAN, valid security system users can remotely access information, regardless of the PC used (once the user has been successfully authenticated).

You will want to discuss the options for what and how to implement ACLs with your IT counterpart, because a large number of options are available on how devices, and their transmitted information, can be filtered and protected.

PREVENTING NETWORK INFRASTRUCTURE TAMPERING: STOPPED BY PORT SECURITY

One valid concern that a security director may have is that the system may be compromised by someone simply plugging a PC into an Ethernet interface (port) on a router or switch that has been configured to be on the physical security system VLAN.

However, given that many switches are in locked wiring closets, tampering is generally not an issue. In any case, networks have another feature that also can minimize the problem of tampering: port security.

Port security provides an additional layer of protection to restrict unauthorized devices from connecting to router or switch ports. Port security registers and maintains a record of the hard-coded, unique address burned into an Ethernet chip of the

network device connected to a particular Ethernet switch port (this address, referred to as a MAC address, is different from the IP address, which can be changed easily).

If a different device is connected to a switch or router using port security, the unauthorized device connection is disabled and thus cannot be used to access video surveillance or physical access control information. Moreover, if a violation does occur, an alert can be sent to a network or physical security manager about the unauthorized action.

Therefore, it is strongly recommended to consider activating port security on all network switch ports that connect cameras, readers, control panels, servers and recorders. Additionally, security managers may want to configure port security to send an alert message to the appropriate physical security operations manager in the event of an attempted unauthorized action.

PHYSICAL DEVICE TAMPERING: NETWORK MANAGEMENT MESSAGING

While port security guards against unauthorized connections to network routers and switches, additional network features can protect against tampering with cameras, badge readers or other "edge" devices.

Most switches and routers have system management features that can generate a message to the network manager or any other specified recipient or application. These messages can be triggered by a number of user-defined events, including the loss of connectivity.

Network managers don't want to get a message every time a laptop PC is connected to the network, but physical security cameras, badge readers, recorders and servers are not moved (disconnected and reconnected) on a regular basis.

Consider having a message or alert sent to security managers in the event of a loss in connectivity. As an added benefit, this also will provide security managers with a real-time notice that a device may have failed, enabling quicker remediation before an incident occurs and the related surveillance record is lost.

SECURING THE INFORMATION THROUGH ENCRYPTION

In the past, encryption technology was expensive and computer-intensive, and therefore not widely available on networked physical security cameras, access control panels, readers and other devices. However, today some vendors offer encryption of the video or other information at its source. As a result, even if a connection is compromised, the information cannot be used by unauthorized parties.

If organizations decide to deploy encryption in end-point devices, security managers must be sure to discuss it with their IT counterparts. There are several approaches to encryption.

Simply encrypting the camera video or other security system information (payload encryption) is one approach. Security managers also can encrypt the entire IP packet, including the address information and the payload.

IT may need to make additional network configuration changes for encrypted physical security traffic to flow through the IT network.

Encryption also is an important consideration when logging onto a security system. You may change passwords regularly, but if the password is sent without encryption, it can be captured and used by an unauthorized party.

Also consider that encryption will add some latency to the transmission of the information, because it must be encrypted before it can be sent across the network and decrypted either at each point along its path through the network or at least at its destination.

EXTERNAL AND INTERNAL NETWORK ATTACKS DENIED WITH FIREWALLS

Network attacks can seriously affect network performance and business productivity.

Firewalls provide an extra layer of protection against these attacks by separating trusted from untrusted network sources.

Many businesses deploy firewalls at the point where the business network connects to the outside

Industry-standard 802.1x protocol provides a common method to validate the identity of the device and then provide support for further authentication of the network device.

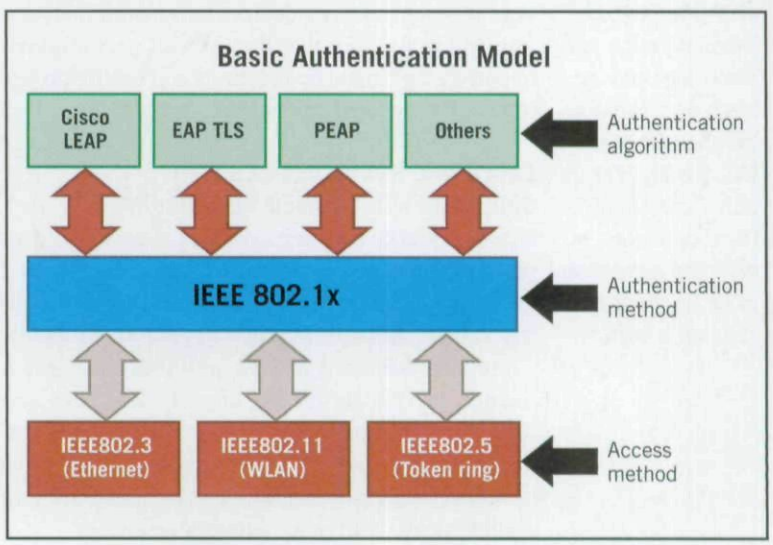

DIAGRAM COURTESY OF CISCO SYSTEMS INC.

world, such as the connection to a service provider or the Internet. This firewall application can help prevent malicious outsiders from accessing and compromising the security system. But it would not stop a malicious user who is inside your business from doing the same.

That is why you may wish to consider putting a firewall on connections or devices that can or do connect your security application to other corporate connections, for example, on a router interface that can tie VLANs together.

Firewall capabilities vary from one network device to the next, and they can interfere with legitimate physical security information transmissions if not configured properly. Hence, you will need to understand what network protocols are used by your physical security devices to transmit information and make sure that the firewall is configured to permit legitimate connections and ensure proper traffic (bandwidth) engineering of the video.

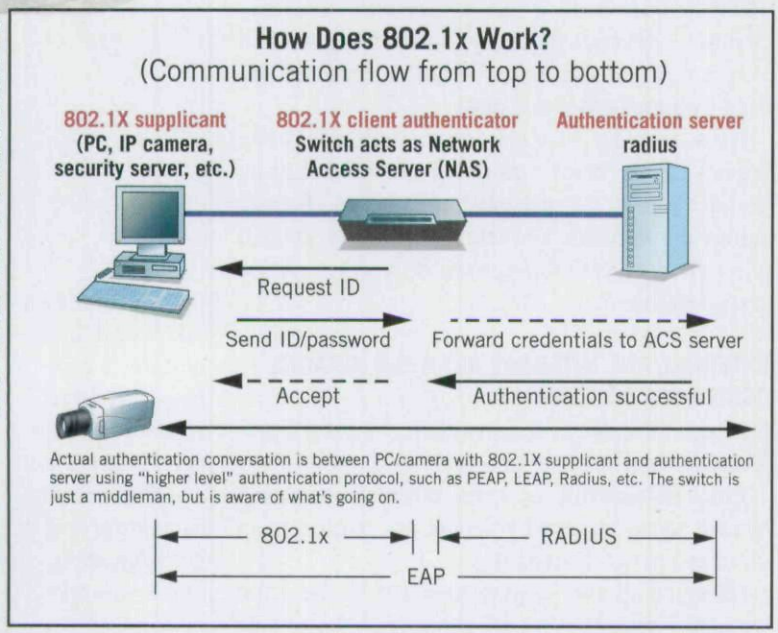

DIAGRAM COURTESY OF CISCO SYSTEMS INC.

With the 802.1x protocol, each network edge device, such as a camera, an encoder or a PC, has an 802.1x supplicant that communicates with the reciprocal 802.1x client that runs on a switch.

EXCLUDING ROGUE DEVICES WITH 802.1X IDENTITY-BASED NETWORKING

How can you be sure that a device connected to your physical security system or the network is really yours? Establishing trust is a core tenet of any security system, and trust requires validation of identity.

Industry-standard 802.1x provides a common method to validate the identity of the device and then provide support for further authentication of the network device. In other words, a device must establish its identity before it can be connected and communicate with other network resources.

It requires that each network edge device, such as a camera, an encoder or a PC, has an 802.1x supplicant that communicates with the reciprocal 802.1x client that runs on a switch.

The 802.1x protocol is used to prevent a myriad of network security issues, including address spoofing, by which a rogue device poses as a valid physical security device, and various types of denial-of-service attacks, which prevent a network device from properly communicating by overwhelming it or starving it of information.

802.1x also provides the network with a powerful tool for device-differentiated network services. These can complement an edge device's capabilities, making the device or its related application that much more powerful and effective.

When purchasing networked physical security products, look for their ability to support 802.1x. If they do, not only can they ensure to a greater degree that no rogue devices are attached to the network, but they also can use various 802.1x extensions built into various products to allow them to do more and be more effective.

MULTI-LAYERED APPROACH IS BEST

As with all security approaches, a multilayered approach tends to provide the best level of security. Network security does not rely solely on routers, switches and other infrastructure devices; network security must protect cameras, encoders, servers, and readers as well.

An end-to-end systems-based approach aligned to industry frameworks and best practices is highly recommended.

The features discussed in this article can go a long way toward helping ensure that networked physical security systems remain uncompromised. Do your homework.

Your physical security system should be integrated, collaborative and adaptive. It can then help network and security administrators better manage security risks while enabling auditors to satisfy internal and external compliance requirements.

Work with the IT group in developing a comprehensive approach to security, and you will be able to realize the many benefits of an IP-enabled physical security system. ■

Bob Beliles is senior manager, market management, physical security for Cisco Systems Inc., San Jose, Calif. Dave Twinam is Cisco's manager, engineering, enterprise solutions engineering.