

surveillance/cctv

# Protecting your IP network from external threats

Roy Alves, country manager, Axis Communications

**N**early all network video installations transmit sensitive information that should be protected from unauthorised users and potential hackers. There are several ways to provide security within a wired or wireless network and between different networks and clients. Everything from the data to the use and accessibility of the network should be controlled and secured.

Today, IP surveillance systems can be made just as secure as those used by banks for ATM transactions. Network cameras and video servers are currently being used in highly sensitive locations such as the air and sea ports security purposes.

## Secure transmission

Some of the most common ways to secure communications on a network and the Internet include authentication, authorisation, IP address filtering, VPNs and Hypertext Transfer Protocol over Secure Socket Layer (HTTPS). Some of these methods secure the data as it travels over the network, while others secure the network path itself. Authentication identifies the user to the network and is most commonly done by providing verifiable information like a username and password, and/or by using an X509 (SSL) certificate.

The 802.1X standard is a new port based authentication framework available for even higher levels of security in a both wired and wireless system. All users' access requests are filtered through a central authorisation point before access to the network is granted.

Authorisation analyses the authentication information and verifies that the device is the one it claims to be by comparing the provided identity to a database of correct and approved identities. Once the authorisation is complete, the device is fully connected and operational within the network.

IP address filtering is another way to restrict communication between devices on a network or the Internet. Network cameras can be configured to only communicate with computers at pre-determined IP addresses – any computer from an IP address that is not authorised to interface with the device will be blocked from doing so.

Privacy settings prevent others from using or reading data on the network. There are a variety of privacy options available, including encryption, virtual private networks (VPNs) and Secure Socket Layer/Transport Layer Security (SSL/TLS). In some cases, these settings can slow down network performance because data has to be filtered through multiple applications before it is accessed at its final destination. This could have a negative impact on the performance of an IP surveillance installation, which often requires real-time access to video.

Additional network security can be created with the use of firewalls. Firewall software normally resides on a server and protects one network from users on other networks. The firewall examines each packet of information and determines whether it should continue on to its destination or be filtered out. The firewall serves as a gatekeeper, blocking or restricting traffic between two networks, such as a video surveillance network and the Internet.

## Wireless security

Wireless network cameras can create additional security needs. Unless security measures are in place, everyone with a wireless device in the network's range is able to access the network and share services.

To better secure IP surveillance installations with a wireless component, users should look at using Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP creates a wireless network that has comparable security and privacy to that of a wired network. It uses keys to prevent people without the correct key from accessing the network, which is the security commonly found in home networks. Data encryption protects the wireless link so that other typical local area network (LAN) security mechanisms – including password protection, end-to-end encryption, VPNs and authentication – can be put in place.

However, WEP has several flaws making it unsuitable for use in a corporate environment. The standard uses a static key, making it easy to hack into the network with inexpensive off-the-shelf software. For additional protection, wireless IP surveillance should employ WPA, which changes

the encryption for every frame transmitted. WPA is considered the base level of security for corporate wireless networks, but for even higher security, WPA2 should be used. WPA2 uses Advanced Encryption Standard (AES), the best encryption available for wireless networks today.

## Protecting system access

In addition to protecting data, it is critical to protect access to the system via a Web interface or an application housed on a PC server. Access can be secured with user names and passwords, which should be at least six characters long – the longer the better. Passwords should also mix lower and upper cases and use a combination of numbers and letters. Additionally, tools like finger scanners and smart cards can also be used to increase security.

Viruses and worms are also a major security concern in IP surveillance systems, so a virus scanner with up-to-date filters is recommended. This should be installed on all computers and operating systems should be regularly updated with service packs and fixes from the manufacturer. Network cameras and video servers with read-only memory will also help protect against viruses and worms. Viruses and worms are programs that write themselves into a device's memory. By using network cameras and video servers with read-only memory, these programs will not be able to corrupt the devices' internal operating systems.

Employing the outlined security measures makes an IP surveillance network secure and allows users the flexibility of off-site access without the worry that video will fall into the wrong hands. Understanding and choosing the right security options – such as firewalls, virtual private networks (VPNs) and password protection – will eliminate concerns that an IP surveillance system is open to the public.

Technology and products for providing IT and network security is an enormous industry today, providing appropriate security for the most demanding applications within government, military and the financial world. All this technology can be used in an IP surveillance installation.

*For details contact Axis Communications.*