June 2005

IP-based Security Solutions

Prepared for

The New Jersey Technology Council's Mid-Atlantic Defense/Homeland Security Showcase

By John W. Govel

As voice, video and data converge, Ethernet has become an ideal network communication standard for distributing information. Extending well beyond the boundaries of telecommunications and IT, this pervasive LAN technology has facilitated the development of new products and services that are now emerging in the security industry. The evolution of digital communication is radically changing the way electronic security systems are being designed and implemented. As traditional analog security devices advance to a digital platform, they have begun migrating to the network, thus redefining the architecture of security systems integration.

IP-based security components offer benefits far superior to traditional closed-circuit systems while further leveraging the TCP/IP network infrastructure already existing in most organizations. More than a transition from analog to digital, the conversion of video and intrusion event signals into binary packets fundamentally changes the way video surveillance and access control systems can be deployed and operated. Real-time sharing of critical information is an essential ingredient in an effective and well-coordinated security initiative. And by creating a robust infrastructure of IP-enabled security devices, data from these components can be readily distributed over a local or wide area network to authorized agencies at the federal, state or local level, regardless of geographic locale. Advancements in wireless technology further extend this functionality, enabling local law enforcement or first responders to remotely monitor and control IP-based electronic security systems during a crisis or emergency.

IP-based Security Technology

> *IP-based video surveillance and access control are emerging applications, similar to VoIP, where circuit-switched communication has transitioned to packet-switched technology. Offering instant connectivity to remote video cameras and secured facilities, this technology can dramatically improve the level of defense and homeland security in the public and private sector.*

System Architecture

Relative to the pace of technological innovation in the computer industry, the evolution of electronic security systems over the past decade has been prosaic. The most significant event was the introduction of the digital video recorder or DVR in the mid-1990s. Representing a tremendous improvement over magnetic tape and video cassette recorders, DVRs ushered the security industry into the digital age. But the DVR has its limitations; not the least of which is its reliance on analog video inputs tethered to each camera in the system. In other words, a coaxial or twisted-pair cable network independent of any existing TCP/IP infrastructure. Although IP-addressable, the vast majority of digital recorders are not designed as network appliances and perform inefficiently over an IP network. In a traditional CCTV system, a DVR is required in every standalone facility where remote connectivity to one or more of the local video streams is required; an expensive proposition. DVRs are also not particularly scalable since most brands are marketed in either 8, 16 or 32 channel increments.

IP-base security systems are designed to be modular, intuitive and relatively simple to configure. Users familiar with standard network protocols can easily connect these devices to an existing router, assign an IP address and immediately access the device over the network. Since these components take advantage of existing CAT5 infrastructure, the need for bulky, expensive coaxial cable runs can be altogether eliminated when installing network video cameras. Innovative IP-based access control systems offer similar cost savings since multiple sites can be linked together over a network allowing remote programming, diagnostics and maintenance.

IP-based Video Surveillance

IP-based video surveillance systems are comprised of three basic components; (i) IP-addressable network cameras, (ii) network video encoders and, (iii) video management software. For new installations, network cameras are normally specified, whereas customers with existing CCTV cameras will utilize video encoders to compress and digitize the analog feeds and thereby gain the same network connectivity from their legacy equipment. Video signals from these devices are then transmitted over ordinary CAT5 cable to a network router and on to a high-speed modem to facilitate remote accessibility.

Network cameras and video encoders are compatible in the same system and, when used together, result in hybrid video systems that effectively combine both analog and IP video components. Hardware decoders are also available for use in network video applications that require a composite analog video signal. For example, adding a video camera to an existing analog CCTV system is often more economical when an existing TCP/IP network is used to transport the video, rather than a dedicated coaxial cable. Once the video signal is compressed and digitized at the camera location, it can then be transmitted over a public or private domain. An existing TCP/IP network could thus carry the digital video packets to a routing switch located in a legacy control center where the signal would then be decoded back to analog and terminated into a standard video matrix or recorder. Assigning a unique IP address to a specified video surveillance camera permits ready access to that video stream by authorized users across jurisdictions and geographic borders.

Among the growing number of network cameras and encoders available today, some designs offer analog video outputs allowing a video signal to loop through the device and terminate into an NTSC monitor or digital recording device. Another innovative feature now being introduced on select video encoders is on-board storage capability in the form of flash-port or USB connections. The implications of this design are far-reaching. Moving intelligence out to the edge of the network is core to the very nature of an IP video system deployment. When functions like authentication, motion-detection, bandwidth allocation and alarm triggering are resident in the device itself, the need for a centralized management console or head-end is significantly reduced. But enabling the device to locally record the data altogether eliminates the need for a centralized recording station.

Compact external hard drives can now record up to 100 GB of data or literally months of compressed MPEG-4 video. Combined with a video encoder, the palm-sized form factor of these network video nodes could radically change the way video systems are deployed and configured.

Live *and* recorded video from any camera could thus be readily accessed over a web browser from anywhere at anytime, at a very low cost. Archiving at the device also introduces fault-tolerance to a system previously void of redundancy. This concept represents next generation video surveillance and could truly revolutionize the security industry.

Video Compression

A single uncompressed digital video stream consumes bandwidth at more than 150 Mbps; an overwhelming amount of data processing for most fast Ethernet networks. IP video systems therefore utilize special codecs or compression/decompression algorithms to encode video signals into Ethernet packets. This process enables the video to be viewed over a web browser or from any PC equipped with appropriate video management software. In either scenario, the video streams are normally decoded to the desktop using an ActiveX control delivered via a plug-in application or embedded in software that can reside on any PC with local or remote access to the IP video network.

Selection of the underlying video compression technology is an important decision in the design of any IP video surveillance system. In our opinion, MPEG-4 is currently the optimal codec for this type of application since, compared to other compression methods, it supports high-quality video streams over minimal bandwidth. Several MPEG-4 network cameras and encoders are now commercially available, each having their own unique characteristics. Continued advancement in video compression technology is accelerating development of these devices and rapidly increasing their visibility in both the security and IT channels.

Since most manufacturers utilize their own proprietary MPEG-4 codec based on ASP, SP or short-header mode (H.263), the features and transmission capabilities of each device vary considerably. While most can achieve CIF resolution (352 x 240) or better, many can now offer 4CIF or D1 resolution (720 x 480) at full frame rates. Bandwidth requirements can range from 400 Kbps to approximately two Mbps, for a full-motion, high-resolution video stream. The benefits of MPEG-4 are superior to older M-JPEG compression and we believe this technology will become the de facto industry-standard within a short period of time. Economics will also play an important role in the broad acceptance of IP video components and we are now at the threshold where the cost of deploying a network video system is equal to or less than an investment in traditional CCTV equipment.

Advances in Video Archiving

To manage and record IP video streams, application software is typically installed on a standard PC and configured to recognize the MAC address of each IP video device on the network. Video streams are then software decoded and displayed on a VGA monitor in a variety of split-screen formats. These same files can be digitally archived on any hard drive or attached storage configuration. Manufacturers of IP video components routinely bundle software with each device, allowing the user to view, manage and record their digital video. Independent, third-party software developers have also emerged as the industry increasingly demands more advanced video management and recording capabilities. Accordingly, several software programs now available are able to decode proprietary codecs from various manufacturers for integration into their platforms. Developers of these programs are also continually adding new hardware components to their list of compatible devices and this open architecture is one reason why networked video systems will eventually displace the digital video recorders (DVRs) that are currently status-quo in traditional CCTV systems.

The recording of video data is an essential aspect of most surveillance systems. Applications certainly exist where archiving is not required, but it must be an available option. As IP-based video evolves, new technology is continually being applied to improve upon the video management and recording function. For instance, network cameras and encoders can now be securely viewed through web portals designed to allow remote viewing of live and/or recorded video data from any high-speed Internet connection. Solutions can either be locally installed or hosted by third-party service providers that can tailor a package of viewing and archiving services to the specific needs of individual customers. This concept of virtual security services represents yet another innovative application facilitated by the emergence of IP-based video surveillance technology.

IP-based Access Control

The ability to monitor and restrict access to a facility is an essential component in any comprehensive security program. Until now, the architecture of both enterprise-class and entry-level access control systems has been designed around a server/software configuration and proprietary wiring. But similar to the evolution of video surveillance, traditional access control systems are now moving to the network, offering expanded functionality and scalable features that only TCP/IP enabled devices can deliver.

Operating as network appliances, IP-based access control systems are designed to attach to any network and communicate via a standard Internet web browser. Unlike traditional access systems requiring the installation of application software onto a dedicated server, these revolutionary self-contained systems are engineered with on-board integrated circuitry that controls operations without the need for software. At the heart of the system, a Linux-based controller board functions as the brain of the system, utilizing an open-source database server to manage and store records. Communicating over Ethernet, interface cards known as network nodes talk to the controller board and link peripheral devices such as card readers, intercoms, temperature modules and network cameras to the system. Since the network nodes communicate with the controller over TCP/IP, they can be situated anywhere on the network, translating to tremendous cost savings on installation and service. This distributed architecture particularly favors large campus or multi-site deployments where controlled facilities are connected over a LAN, WAN or the Internet. Traffic between the controller and the nodes is also authenticated, further ensuring secure connectivity outside a VPN or other private Intranet.

A distinct advantage to deploying an IP-based access control system is remote accessibility which allows configuration, programming and diagnostics to be performed from a centralized, off-site location. This feature can be instrumental when implementing an emergency response plan that addresses a sudden increase in threat levels. Since all remote locations on an IP access control system are connected, an administrator can create various profiles that define how access levels operate. A single system command can then be used to generate a uniform increase or decrease in the level of security at all locations. These systems also scale marginally providing users increased functionality as their needs grow. Add-on modules that control or interface with IP intercoms, network cameras, badging stations and environmental monitors can be layered onto the system at minimal cost and configuration.

Challenges and Solutions

> *Deploying IP video components requires a combination of skills blended from traditional security and TCP/IP networking applications. While the technology offers distinct advantages over analog systems, configuring these devices presents unique challenges that must be addressed to consistently meet industry expectations.*

Despite their plug-and-play nature, the deployment of IP-based security components requires some degree of customization; certainly at the enterprise level. Devices like network cameras and video encoders are not yet commoditized, but IP video technology is forcing the industry in that direction. As these components become more familiar to the IT channel, networking VARs are embracing the technology and beginning to develop vertical market applications alongside Wi-Fi, network security, VoIP, mobile solutions and other applications that currently drive tech spending. Ultimately, this process will shape industry standards and result in system specifications that promote interoperability and open architecture.

Several factors influence how data is securely transmitted and archived over a network and this issue is particularly relevant to the physical security function. A robust, protected IP infrastructure is an integral part of any network security system and a certified networking professional should be involved in the design and specification of the underlying TCP/IP network that will be transmiting the data. Authentication, encryption and fault-tolerance are concerns that must be addressed in order to ensure the system cannot be easily compromised.

Internet accessibility to IP-based security devices is one of the strongest selling features of the technology. Remotely connecting to a network device behind a firewall does, however, require modifications to the network. The user must first assign a unique HTTP port to each device on the LAN and subsequently open the corresponding port in the firewall. The router can then be configured to port-forward requests, channeled through the public IP address, to the specified device. ActiveX controls that drive MPEG-4 video streams must also be considered. Any PC connecting to an MPEG-4 video source normally requires an ActiveX applet to be loaded on the PC in order to view the video stream. This is normally accomplished via a signed pop-up plug-in, embedded in the device, which can readily be accepted and downloaded by the user. Likewise, PCs running older versions of MS Windows will occasionally be prompted to download a more recent MS Service Pack containing updated dll files that support the streaming video.

Another compelling advantage of IP-based security components compared to traditional analog systems is their ‘future-proof’ design or the ability to be upgraded as the technology improves. Product manufacturers are continually optimizing their firmware by adding new product features made available through the release of scheduled upgrades. Embedded firmware is usually modified via an upgrade wizard or installation program residing on the device. Expanded functionality of the products will often broaden their use for other applications. IP-based security devices can also take advantage of practical network innovations like wireless access points or power-over-Ethernet that delivers DC voltage over ordinary CAT5 cable. These features and complementary products can significantly improve the performance and return on investment of an IP-based security system deployment.

IP Security Market Dynamics

> *Never before has the security industry encountered changes on the magnitude of what is presently occurring. As security systems move to the network, a new breed of service provider is emerging that will alter the competitive landscape. Technology companies are now positioning to take full advantage of this fundamental shift.*

Industry Convergence

Mirroring the radical transformation of the telecommunications sector, the security industry is currently being upended by the dynamic convergence of IT and electronic security. As video surveillance and access control platforms migrate to the network, new technologies driving this transition are enabling IT companies to aggressively enter the market and compete for the business. Conventional security system providers, unfamiliar with network architecture and protocols, are being forced to redefine their core competencies in order to understand these new technologies. Characterized by exceedingly long product life cycles and relatively high profit margins, the security industry now faces a severe competitive threat from technology companies already seasoned in gorilla-warfare from the fallout in tech spending several years back. Entrants like IBM, Cisco, EMC and dozens of other leading technology firms are obvious signs that the race is on to displace the incumbents in the growing market for high-tech security solutions.

Market Development

The visibility of IP video surveillance and access control is rapidly growing, and every major security trade publication has expanded editorial coverage on the technology. Subsequently, the channel is becoming populated with a variety of resellers. Most vendors remain uncertain as to how they will strategically market the technology; particularly in light of the steep learning curve for traditional security dealers. Early advances are being made by large IT distributors trained at selling network appliances to tech-savvy VARs. But beyond their logistical expertise, these organizations are typically unable to add value to IP-based electronic security applications that require solution selling. Similarly, the security channel remains fragmented and relatively unsophisticated. It is therefore uncertain which industry will generate the greatest momentum in the emerging market for IP-based security systems.

Industry experts predict that security professionals will readily embrace IP security solutions once the cost of deploying the technology falls to a specific price point. That critical mass is nearing and high-performance, low-cost devices now surfacing in the market represent the type of catalyst that could generate significant momentum in the broad adoption of IP-based security systems. The benefits of using TCP/IP enabled security devices are too significant to ignore and the explosion of broadband availability in the residential and commercial sectors will further erode any boundaries keeping these systems off the network.

As the deployment of IP video becomes widespread, more advanced software applications will also emerge. Provisioned by Internet service providers, these web-based platforms will offer virtual services on demand, thus replacing many traditional closed-circuit systems. Beyond basic monitoring and archiving, advanced software solutions will ultimately incorporate complex video analytics or remote video auditing for analysis that can be used in a variety of applications. Already, digital video data can be analyzed by intelligent software designed to recognize changes in traffic patterns or potentially hazardous situations. But beyond these primary functions, IP video components and specialized software can also be used to collect data from a defined environment, extract and process select criteria and generate accurate reports for analysis. Applying these same algorithms, law-enforcement officials will be able to establish a remote monitoring system for almost any environment that will automatically notify authorities when a sophisticated set of criteria are identified. IP-based technology in security applications will absolutely change the way public and private organizations allocate resources and manage their security operations.