Security Products

Seamless Visitor Management

Using wireless access control provides necessary security tools

By John Hayde Apr 01, 2010

The most efficient visitor management and access control systems for corporations or private communities contain at least one element of wireless technology.

One of the biggest limitations of most security software systems is that they can only be used from a PC at a security station, whether that is a concierge desk or a guardhouse. But using wireless technology adds mobility to a corporation's security. Besides providing an added layer of protection, wireless technology also saves time and presents the visitor or guest with a seamless experience.

Devices for Multi-Processing

Many private communities provide security software that protects the homes, family and assets of its members, which may include CEOs, celebrities or political figures. Meanwhile, corporations are liable for the protection of their employees and company information.

Providing these layers of protection calls for all entrance and destination points to be able to communicate with each other in real time, particularly during periods of increased traffic or congestion, such as public events. This is where implementing wireless technology into a security system can present a major advantage. For example, in a gated community, while one officer or guardhouse processes a lane of traffic, another lane can be processed with a wireless handheld device. Similarly, while a corporation's guard is entering a visitor's information into the computer to print a badge, another guard may use a handheld device to process a second visitor and print another badge, eliminating wait time and increasing efficiency.

Lightweight ruggedized handheld devices use a security application that can run on operating systems such as Windows Mobile 6.1, MacOS and Android from Google. Combined with wireless Internet technologies like 3G networks, Wi-Fi or WiMax, wireless handheld solutions provide security officers with the proper tools to process visitors in any location, as opposed to being tethered to a desk or having to rely on radio or phone communications. Handheld technology enables security personnel to complete many actions in transit or heighten the security of a community.

Guards can process visitors while walking down a lane of cars, document security incidents and upload photos taken from the handheld device in real time. Completing the process, hosts who are expecting visitors can choose to receive text messages or e-mails on their wireless Blackberry, iPhone or other device, notifying them of a visitor's arrival. There is no delay in transmitting or receiving information.

At the Touch of Your Fingertips

Since many corporations have used the same software for years, they might not realize that with a few simple software updates, their current system can go wireless in a short time.

First of all, security officers must go through a training process to understand how to use both wireless technology and the individual handheld device. After becoming familiar with the tools and the technology, even business processes offered by staple security systems can be accessed via handheld solutions as well. Wireless ruggedized handheld technology can process a broad range of jobs, including scanning bar codes on visitor badges or arriving products, search capabilities—such as scanning an identity against terrorist lists, sex-offender lists or previous employee lists— guest check-in, guest car pass printing and guest pass deactivation.

Wireless technology truly provides a business' security force with the following abilities on the go:

Incident tracking on site. Incidents happen every day in business and within communities. Whether that incident is minor, like a traffic violation, or more significant, like a security breach, proper documentation is paramount to security. Wireless technology via handheld devices allows security officers to log incidents on site and review previous incidents as necessary. The need for extensive note taking is eliminated. Thanks to built-in cameras, officers no longer have to rely on their memory to recall information after the fact.

Data tracking. When security officers report to work, they log in and all transactions conducted by that individual are automatically tracked back to the individual's specific profile. This ensures data is tracked efficiently and permanently stored even with personnel changes. Data also can be disseminated resourcefully. For example, security officers can view a list of all upcoming events or activities and work ahead by printing visitor badges, tags and car passes via a wireless handheld device.

Reliability of wireless technology. All data on the handheld devices and main software is stored on a remote server, often referred to as a thick client. A network feature constantly monitors the connection to the server. If the connection is broken, due to a poor Internet connection or failed wireless network, for example, the application will attempt to reconnect so that no data is lost.

To maintain 100-percent uptime, many wireless devices can be configured to operate on the local wireless device database and synchronize every few minutes with a remote server. This type of data replication proves invaluable in the case of spotty wireless connections to the host server.

About the Author

John Hayde is the head of the commercial division at CapSure Inc.