Physical Access Control systems

The role of perimeter security, discussed in the September and October issues, is to deter, deny and delay intrusion. This article discusses how access to a property is controlled.

What is Physical Access Control.

Access control refers to **the practice of restricting entrance to a property, a building, or a room.** Physical access control can be achieved by a guard or a receptionist by mechanical means such as locks and keys, or through technological means such as access control systems. An access control system determines who is allowed to enter or exit, where they are allowed to exit or enter, and when they are allowed to enter or exit. Mechanical systems like keys and locks do not allow restriction of the key holder to specific times or dates. Mechanical locks and keys do not provide records of the key used on any specific door and the keys can be easily copied or transferred to an unauthorized person. Electronic access control uses 'intelligence' to overcome the limitations of mechanical locks and keys. A wide range of 'credentials' can be used to replace mechanical keys. The electronic access control system grants access based on the 'credential' presented. When access is granted, the door is unlocked for a predetermined time and the transaction is recorded. When access is refused, the door remains locked and the attempted access is recorded. The system will also monitor the door and alarm if the door is forced open or held open too long after being unlocked.

Access Control System Components

- Point of Control
- Lock
- Reader
- Credentials
- Control system

Point of Control.

This could be a door, turnstile, parking gate, elevator, or other physical barrier where granting access can be electronically controlled.

Turnstile

Door

Lock

The electronic access control point can contain several elements. At its most basic there is a stand-alone electric lock. The lock is unlocked by an operator with a switch.

Door Lock

To automate the process of unlocking, operator intervention is replaced by a reader.

Reader

Readers send the information (Credentials) on the card to the control system that verifies the information against an access list.

Reader

Types of readers

- Basic, non-intelligent readers that simply read card number or PIN and forward it to the control system.
- Semi-intelligent readers that have all inputs and outputs necessary to control the door hardware (lock, door contact, exit button), but do not make any 'access decisions'. When a user presents a card or enters PIN, the reader sends this information to the main controller and waits for its response.
- Intelligent readers that have all inputs and outputs necessary to control door hardware. They also have memory and processing power necessary to make 'access decisions' independently.

The reader could be a keypad where a code is entered, it could be a card reader or it could be a biometric reader.

Some readers may have additional features such as LCD and function buttons for data collection purposes such as clock-in/clock-out events for attendance reports, camera,speaker,microphone for intercom, and smart card read/write support.

Credential

A credential is a physical/tangible object, a piece of knowledge, or a facet of a person's physical being, that allows the individual access to a given physical facility. Typically, credentials can be:

- Password, pass-phrase or PIN
- Smart card
- Biometric measurement such as finger print
- A combination of the above.

A typical credential is an access card, key fob, or other key. There are many card technologies including magnetic stripe, bar code, Wiegand, 125 kHz proximity, 26 bit card-swipe, contact smart cards, and contactless smart cards. Also available are key-fobs which are more compact than ID cards and attach to a key ring. Typical biometric technologies include fingerprint, facial recognition, iris recognition, retinal scan, voice, and hand geometry.

Finger print scan

Access Control System Operation

When a 'credential' is presented to a reader, the reader sends the information, to the control system, a highly reliable processor. This system compares the credentials with a control list, grants or denies the presented request, and sends a transaction log to a database. When access is denied based on the control list, the door remains locked. If there is a match between the credential and the control list, the control panel operates a relay that in turn unlocks the door. This illustrates a single factor transaction. Credentials can be stolen or passed around (by one person to another), thus subverting the access control list. To prevent this, two- factor authentication is used. In a two factor transaction, the presented credential and a second factor are needed for access to be granted.

Trends in Access Control – Report from ISC West 2012

- **Web-based solutions.** Apps that allow integrators to configure access control systems more easily in the field. Integrators will not need to stay at a site for an extended period of time to configure the access system.

- **Desire to ‘virtualize’** access control systems as IT departments have become more involved in the selection of corporate security technologies.
- **The future is IP**. This will reduce ‘total cost of ownership’ as the technology allows for remote upgrades and diagnostics. Secondly, IP will help users boost the performance of their systems as a result of these proactive management features.
- Use of **"hybrid"** access control systems where some people will be using smart cards while others will be taking advantage of NFC.
- **Biometrics** for high security applications needing more than one-factor authentication. Biometrics can allow organizations to streamline identity and access control management at their facilities. Fingerprint-based systems have emerged as the most popular type of biometric readers, thanks to their ease of use and lower cost, while iris scan systems have a niche for high-end applications.
- Growing demand for **NFC technology**.
- Increase in the demand for **‘managed access control offerings’**. These service offering are advantageous for both end users and integrators, because end users do not have to make an upfront technology investment and it also allows integrators to make more recurring monthly revenue.
- **Emergency Management** - to define a situation when personnel are required to assemble at a corporate mustering point where employees can badge in to verify that they have left the premises.
- **Visitor Management** - enables authorized personnel to enter information about anticipated visitors into the access control system so that when the visitor arrives, he can quickly receive appropriate authorization. Additionally, an e-mail can be sent automatically to the person whom he is visiting to advise that person of his arrival. The visitor information is linked to the card holder, so it provides an audit trail.
- **Integration is the key**. *By interconnecting access control with intrusion detection or video surveillance systems, physical security systems become more powerful*. By integrating access control with other security systems, the system can become much more intuitive. If a door is open in a certain hallway, the screen just shows that.
- **Human Resources Interface** – integration with human resource systems. Integrating those systems helps reduce data entry errors by eliminating the need to input employee information into each system separately. It also helps ensure that when an employee is terminated, that employee's ability to access the premises is deleted simultaneously.
- **Sensors** to determine the speed, size, and directionality of people and vehicles moving in protected areas are being used in high end applications. Using this capability, a system can be configured to take actions like, say, sending a video image to Security, if it identifies a vehicle larger than a car approaching. Systems that use sensors in this manner are becoming increasingly intelligent, in being able to detect when someone crosses a boundary. That could possibly indicate that someone has left the property or, depending on directionality, that a potential intruder has stepped onto the property.

Trends that seem to be impacting other technology segments within the industry also appear to be making an impact in access control, including the shift towards IP, the utilization of managed services, adoption of cloud-based solutions, the proliferation of Near Field Communications, and the convergence of IT with physical security.