NEWTON
SECURITY INC

Elevators as Access Control Portals

Background Information

In the face of ever increasing real estate costs government agencies and corporations are moving their offices into high-rise facilities that are shared with other tenants. While this partially solves the problem of costs associated with facility location and maintenance, it creates a new problem in the area of access control and security. In this new corporate office environment there is a very real threat of unauthorized personnel gaining access to secure areas of multi-tenant facilities that must be mitigated through the use of security personnel, hardware and technology, or some combination of the two. This paper discusses the specific security issues and how they have been successfully mitigated with technology such as T-DAR® (Tailgate Detection and Alarm Recording) systems for elevator cabs and lobbies.

Problem Description

In any modern multi-storied building elevators are common use devices and are generally available to all of the tenants and their visitors within that facility. Although this makes for a convenient solution for gaining access to any floor of the building, it opens a veritable Pandora's Box of security vulnerabilities that must be addressed. Access control equipment manufacturers have made significant headway in the amount of flexibility available for controlling elevators for security purposes; however, one problem continues to plague the system. The problem is that there is no effective way to ensure that those persons who are authorized on a given floor are, in fact, the only persons that exit the elevator on that floor.

For the purposes of illustration we will use a building in Washington, D.C. This building is eleven stories tall and houses seven different tenants, and is occupied as follows:

- Floor One is comprised of the main lobby, elevator lobby, loading dock, mail room, and various shops and café/restaurants
- Floor Two houses a dental office, a small accounting firm, and a psychiatrists office
- Floor Three is occupied by a District of Columbia government agency responsible for medical assistance
- Floors Four through seven houses a US Department of Defense procurement organization that maintains classified information regarding weapons

procurement and stockpile data. This organization maintains a reception desk on floor seven only.

- Floor Eight is occupied by a political action committee
- Floors Nine though Eleven are occupied by a law firm that specializes in technology patent application and protection. This law firm maintains a reception desk on floor eleven only.
    - The elevators in this building are equipped with a card reader that must be used at all times to gain access to floors four through seven. The card reader is required for all other floors only after normal business hours. Additionally, the stairwell doors are locked to prevent entry to a floor from the stairwell.

As you can see from the above tenant list this building contains classified information, confidential patient information, personal and corporate financial information, and high-value intellectual property and trade secrets. Although all of these tenants are amenable to the idea of each of the other tenants occupying the same facility, they still must be diligent in the protection of the information in their custody. It is incumbent upon each of these organizations to ensure that no unauthorized persons are able to gain access to the materials under their control; this prohibition must include the other tenants as well as outsiders.

Elevator Call vs. Elevator Dispatch

The term elevator call refers to the action of an elevator called to a specific floor where a person has pushed either the up or down arrows on the elevator call station in the elevator lobby of that floor. Elevator dispatch refers to the action of an elevator that has been dispatched to a specific floor when a person inside of the elevator cab pushes the floor selection button on the elevator cab control panel. The following is a discussion of the two distinct problems that can occur when these aforementioned actions occur.

Elevator Dispatch

Common Security Violation scenario: *It is the end of the lunch hour and many of the employees are returning to work. Seven people get into the elevator on the first floor and begin pushing floor selection buttons. One person presents a card reader and then selects floor 5; other passengers press buttons for various floors. When the cab stops at floor five, the employee who is authorized for the fifth floor and properly presented their card exits the cab to the right and the doors begin to close. A second person on the elevator stops the doors from closing and exits the elevator cab to the left. The remaining people on the elevator continue on to their respective offices*.

In the above scenario an unauthorized person tailgated into a secured space where classified information is stored in front of five eye witnesses who did not realize that a security violation has occurred. Because there is no reception desk on the fifth floor, the only person equipped with the knowledge to understand that a violation was occurring has left the scene, having exited the elevator cab five to ten seconds earlier.

Elevator Call

Common Security Violation scenario: *Just after 6pm on a Friday the building is mostly deserted and the elevators are in card access-only mode requiring that a card with proper access authority be presented to gain access to any given floor with the exception of the lobby. A person leaving the large law firm on the tenth floor pushes the down arrow in the elevator lobby and waits patiently for the elevator to come. When the elevator does arrive, they begin to enter the cab and almost bump into a man in a suit carrying a briefcase. The law firm employee feels embarrassed for having been in a hurry and does not challenge the man as he exits the elevator cab and enters the law firm.*

In the above scenario an unauthorized person entered one of the elevator cabs at the lobby level and simply waited for that cab to be called. If the cab stopped at a floor other than the floor desired the occupant could simply feign embarrassment and repeat the process until the desired result was obtained. Even if this intruder is challenged, they can simply feign ignorance and claim they are a visitor in the building and they are lost.

In both of the above scenarios unauthorized personnel were afforded unfettered access to very sensitive facilities even though authorized persons were present. This can be attributed to the fact that as a polite society it is difficult for us resist the urge to be accommodating and to mind our own business. The only persons that are truly effective at enforcing security policies and procedures are well-trained security officers. Unfortunately, well-trained security officers represent a large recurring expense that are often hard to justify in the absence of a significant event.

Solution

The addition of a T-DAR Elevator Control System to an existing elevator system on the floors that require card access will directly and immediately solve the problem of undetected entry during normal operation of the elevators. The system will alarm both locally and remotely, as well as documenting the event via digital video recording. This information is then communicated to a central control center for processing. The application of the T-DAR system to elevator exits on secure floors compensates for the security shortcomings that were detailed in the above scenarios.

The patent-pending T-DAR system utilizes 3 Dimensional Stereo Machine Vision analysis to evaluate each access cycle to guarantee that only one person passes through the portal for each valid access card presented. The system is able to discriminate between carried items, carts, luggage, and so-forth, allowing the unimpeded access of authorized persons carrying out day-to-day tasks. The system is comprised of three primary components: the Controller, the Camera Head, and the Annunciator. The Controller performs all of the video processing as well as logic operations regarding input/output data from the access control system and the elevator control module. The stereo camera head is the portion of the system that monitors the selected scene for activity. Then annunciator provides local audio (voice) and visual (strobe) annunciation

of violations. The stereo head and annunciator components are mounted just outside the exit of the elevator, while the controller is mounted in a secure location and communicates with the access control system and the security station.

The T-DAR camera head is mounted on the ceiling in just onside of the doors and continually looks down upon the threshold of the cab entrance/exit to monitor for persons exiting and entering. If a person were on the elevator and attempted to exit at a floor they did not present a card for, the system would initially warn them with voice annunciation and if they continued to exit the system would enter full alarm mode complete with remote annunciation and event video display sent to the security station.

The system consists of the following components: a stereo-optic camera head for overhead image capture, a Pentium processor/controller for system processes, and an annunciator box for local audible and visual notification of alarm events. The system is interfaced with the existing access control system for the purpose of gathering access and door position information, and for communicating alarms. Additionally, an event camera is connected to the system to allow the capture of alarm event information for review by authorities when responding to alarms; if a current CCTV system and DVR recorders is installed; the T-DAR system will notify the DVR to record the data and no separate event camera is required.

Summary

This document has discussed the need for and how T-DAR® (Tailgate Detection and Alarm Recording) systems have been implemented for elevator systems in building with both secure and non-secure floors. With the application of 3 Dimensional Stereo machine vision technology, it is now possible to accurately detect and document security violations as they occur.

Additionally, the T-DAR product is well suited for virtually any application requiring tailgate/piggybacking detection. The T-DAR system is deployed in commercial, corporate, government and military environments worldwide.

For questions on this application note, or for more information on T-DAR and other machine vision-based security solutions, please contact the author via e-mail at dwoody@newtonsecurityinc.com

NEWTON SECURITY INC.
443 SW 41ST STREET, RENTON, WA 98055 USA
TEL: (425) 251-9494 FAX: (425) 251-6236
www.newtonsecurityinc.com