Detection of Access Control Tailgate Violations

Closing the gaps in access control systems technology.

Background Information

An access control system’s ability to control and restrict access to pre-defined sensitive or secure areas is the central goal of the system. With a well designed, installed, and maintained system using today’s technology, this goal is easily achievable.

The access control system is perceived as the primary system for controlling individual access to controlled areas. However, the actual primary access control system is the proper usage of the access system by those persons granted entry. These individuals are in control of the door from the time it unlocks until the time it relocks, and can allow any person, authorized or not, to gain access through the open door.

The addition of systems to protect against this loss of access control is critical to ensuring that access is granted only to those persons who’s access has been verified by an authorized system.

Problem Description

The stated purpose of an access control system is to hold doors locked until an authorized person requests access. The system will then unlock the door, allowing the authorized person to enter the controlled area, and will relock when the door closes. This is known as an access cycle and is true of all access control systems, ranging from a simple lock and key systems through keypads, card readers and the most advanced biometric access control systems.

The more common electronic access control systems utilize alarm contacts to monitor the state of the access controlled door or portal, and will alert the system operator when a door has been forced open or has been held open too long. These two alarms are the only way that the system operator can know that the door is open when it should not be open. Furthermore, many system operators view the ‘door held alarm’ as a nuisance alarm: one that is often ignored. This is due to the perception that since the system initially allowed the door to be opened, it must be a valid access and the authorized individual has simply not quickly enough closed the door; thus the one alarm available to the operator to suggest a potential tailgating/piggybacking problem is often disregarded.
One major problem that occurs with all access control systems is that control of the door is turned over to the authorized person for the period of time that the door is unlocked. This person can then allow other persons to enter the controlled area unknown to the access control system, either intentionally by holding the door open for them (the act of Piggybacking), or unintentionally by failing to fully secure the door after passage (the act of Tailgating). Many facilities address this problem through the implementation of policies and procedures, and rely heavily on the authorized persons using the system to ensure adherence to proper access control procedures.

Solution

The addition of a T-DAR® (Tailgate Detection and Alarm Recording) system to an existing access control system will directly and immediately solve the problem of undetected entry during the access cycle. 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 system generates three types of alarms: Tailgate Warning, Tailgate Violation, and Suspicious Entry.

The Tailgate Warning alarm is a pre-alarm condition that is designed to alert users that a tailgate event is about to occur. This alarm occurs when an unauthorized person has transited a doorway but has not proceeded further than an operator selectable distance and the door has not closed behind them. This is annunciated locally, and is in the form of a verbal warning from the system. The warning allows the violator to return through the door without triggering a remote alarm. The event can be digitally recorded and stored at the option of the operator.

A Tailgate alarm occurs when the system has detected a tailgate violation, and is annunciated locally with a horn/siren and flashing light, and remotely with alarm contact output and event video loop replay. A Suspicious Entry is declared when the system cannot clearly determine what event has just occurred. Suspicious Entries are annunciated locally with a verbal message, and remotely with an alarm contact output and event video loop replay. Each event video replay has the time/date, location, and type of alarm displayed in the lower left corner of the screen. If the system is so configured, the access card number of the last authorized individual to access the door will also be displayed.

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 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.

**Implementation**

An excellent example of T-DAR® system usage is one that is currently in operation at Terminal 2, Salt Lake City International Airport in Salt Lake City, Utah. The system has been installed on an oversized (48 inch wide) pedestrian door that leads from the public baggage claim area into the secure baggage make-up area.

There are more than one thousand access and egress transactions processed through this door each day. In addition to normal personnel traffic, the door is used to bring oversized fragile articles such as pet crates/kennels into the baggage claim area and for moving high volume overflow baggage to the explosives detection system located in the secure baggage make up area. This installation typifies the installation of T-DAR on access controlled pedestrian portals, and is a very good demonstration of the capabilities of the system to deal with large volumes of traffic. The airport control center staff use the T-DAR system to detect and respond to tailgating/piggybacking violations that previously may have gone unnoticed.

The T-DAR system has been interfaced with the airport’s existing NexWatch® access control system. The alarm information is processed through the access control field panels, and is ultimately displayed on an alarm monitoring station in the control center. Additionally, the system provides video information to the Pelco® matrix switcher and digital video recorder system. This video stream is then automatically called to the CCTV alarm review monitor in the control center so that the operator may simultaneously evaluate the alarm information from the access control system and the alarm video from the event camera.

**Summary**

This document has discussed the need for and implementation of T-DAR® (Tailgate Detection and Alarm Recording) for access control systems. With the application of 3 Dimensional Stereo machine vision technology, it is now possible to accurately detect and document tailgate/piggybacking violations as they occur.

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

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