Setting the Mantrap

Carroll McCormick reports on the automated technology under development which aims prevent 'piggybacking' and 'tailgating' at security checkpoints

A weakness in any door unlocked by key, keypad, card swipe or biometric identification is that once it is opened for an authorised person, others can also pass through, if the first is unwilling or unable to stop them.

There are two types of sneaking through doors behind others - 'piggybacking', where an authorised person holds a door open for someone who is unauthorised (or for someone who simply does not want to bother opening the door according to the official script), and 'tailgating', where someone slips through undetected behind the authorised person.

"At the base level, once the door is open, the person holding the door is the only access control system," said John W Bramblet, President and Chief Executive Officer of Newton Security Inc, a Washington State-based company which develops and provides computer-based security applications.

Transport Canada's Aerodrome Security Measures address this weakness by requiring all doors leading to restricted terminal areas to be manned by security guards, who check airport personnel IDs and visually prevent 'tailgating' or 'piggybacking'.

An alternative to guarded doors is an automated system designed to detect more than one person passing through a door per authorised opening. Newton Security has designed one called the Tailgate Detection Alarm and Recording System (T-DAR). Built into a specially-designed vestibule with an entrance and exit door, which Newton Security calls a 'mantrap', T-DAR uses 3D imaging to count how many people are inside it. If T-DAR detects just one person in the vestibule and the ID check is approved by the airport access system, the exit door to the restricted area unlocks and the entrance door instantly locks. If it detects more than one person, the exit door remains locked, thus preventing 'tailgating' or 'piggybacking'.

The Kelowna, Winnipeg and London International Airports have, under Transport Canada exemptions, installed mantraps. These are integrated into their airport access control systems and Canada's new Restricted Area Identification Card (RAIC) system, in use for airport personnel at 29 airports since early this year. This positively identifies users by comparing real-time biometric readings with biometric templates stored on their RAIC cards. The result is a substitute for guarded doors that has been judged secure by Transport Canada and the US Transportation Security Administration (TSA), the body which inspects security arrangements at Canadian airports with trans-border traffic.

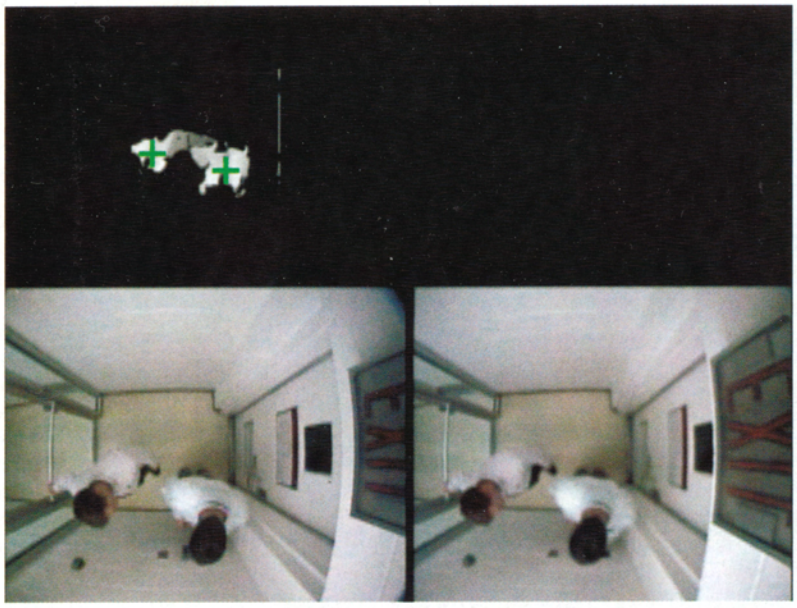
Horizon Air employee Lily Oltmanns in the Kelowna airport persontrap. Note the cardswipe, fingerprint and biometric readers and the surveillance camera bubble. (N DRACHENBERG)

"TSA has inspected us twice," said Kelowna airport fire and security chief Neil Drachenberg. "We passed both tests and the person traps [as Kelowna calls them] haven't been raised as an issue. They are well aware of them and find them acceptable. I consider persontraps a mature technology."

Added a Transport Canada spokesperson: "The implementation of [RAIC] ... has provided the opportunity for airports to look at alternatives to the remaining manual function - that of the guard controlling the piggybacking and/or tailgating."

Moreover, on a local level RAIC allows each user airport to custom-programme its access control systems, so that each employee is only able to open specific doors to restricted terminals areas between specific hours and on specific days. Outside these set parameters the doors simply do not open for them. Add to that the regular updates Transport Canada can send airports on changing security clearances for each of the 100,000 or so employees in the national system, the checks and balances for mantraps are considered to be very secure indeed.

"If Transport Canada revokes a clearance, our system knows immediately, and that individual can't get through the person trap. If we decide that an employee can no longer use our person trap, independent of any Transport Canada action, we can



Overhead view of a mantrap generated by the T-DAR stereo camera head. The bottom left and right images are the raw input video and the top left image is the 3-D or stereo. (ADT)

deny them access to the person trap. That authority resides with us. It is not only scalable [as to who can use it and when] in terms of day-to-day operations, it is scalable in terms of threat level. We can rescale the person trap in a very short time and shut it down in an instant," explained Kelowna Airport General Manager Roger Sellick.

Kelowna only lets employees use its mantraps once they have been with the airport for a year, and London, like the other airports contacted by *Airports International* about the RAIC programme, only allows 'local' employees to use them.

Acceptance of the devices in the three Canadian airports is high. "It is a 20-30 second process to go through. Employees love the mantrap," says London airport CEO Steve Baker. "We will be installing more in the next couple of years."

But why are mantraps not more widespread in Canada? (Vancouver International Airport reports it will be installing mantraps this year, while the airport at Victoria has put its plan for them on the back burner.) The apparent disinterest in mantraps in US airports – only the Reagan National Airport has T-DAR, for example - despite the apparent problem with 'piggybacking' and 'tailgating' (see sidebar), may be partly attributed to the fact that installing one does not save on door-staffing costs. But in Canada, where each door to a restricted area must be guarded full-time (to the tune of C$116,000 (US$110,000) a year per door at Kelowna, for example), the full cost of a mantrap - T-DAR, portal, biometric readers, cameras, locks, etc, is just under $50,000, according to Roger Sellick. The return on investment can be calculated to the minute.

T-DAR is the operative technology in automated immigration gates in the United Kingdom, Australia, Japan, Nigeria and about 1,000 non-airport locations around the world, these being high-security locations such as data centres and banks. Yet despite the obvious trust shown in their effectiveness, incorporating them at entrances to restricted areas in airport terminals has been slow. In the US, said Don Woody, Director of Operations with Newton Security Inc: "The slant on all reports of late has been to the effectiveness of passenger screening. Very little has to do with access control."

Neil Drachenberg, who has given talks on Kelowna's mantraps to the RAIC committee and the Canadian Air Transport Security Authority, said: "There is a lack of knowledge of them out there. I think people are afraid of change. We have demonstrated them to many people and we always get a favourable response. We have run many tests with two people and the door just won't open. It is way more effective than a guard at the door."

'Piggybacking' in the USA

Airports in the US are reportedly not required to staff the doors leading to restricted areas in a move to prevent 'piggybacking' and 'tailgating'. Federal regulations say only that access has to be restricted to authorised people.

The result, according to the scarce amount of publicly-available information on airport security audits (these are said to have dried up after 9/11 when the responsibility for them passed from the Federal Aviation Administration to the Department of Homeland Security), is a vulnerability to 'piggybacking' and 'tailgating' which appears to be still with us.

An American Association of Airport Executives (AAAE) summary of a US Department of Transportation's Inspector General report on tests conducted between December 1998 and April 1999 in at least eight airports, notes that out of 75 'piggybacking' attempts, 71 were successful. These figures may be seem like so much pre-9/11 trivia, but Colleen Chamberlain, Director of Transportation Security Policy with the AAAE said: " 'Piggybacking' remains a concern and an issue sometimes with secure access... one that our airports are trying to deal with."

Don Woody, Director of Operations with Newton Security Inc, noted: "Prior to 9/11, everyone was writing reports on access control systems. Now everything has to do with screening and luggage." Has concern about 'piggybacking' and 'tailgating' simply gone out of fashion these last few years? "I think this is a correct assessment as far as the Transportation Security Administration (TSA) is concerned," said Colleen Chamberlain.

In May 2004, the TSA announced Phase I of a pilot programme expressing its intention to test new technologies (including anti-'piggybacking' technology) designed to ensure that only authorised personnel have access to non-passenger-controlled areas. Ten airports were included in Phase I, and five international airports were added in Phase II, announced in April 2005.

Cardswipe, fingerprint and biometric readers add essential layers of security to the core function of mantraps, in which T-DAR determines if there is more than one person trying to get through. (YWG)