GCN
Government Computer News



# LAX goes reliably random

**Game theory algorithm improves security by putting police on unpredictable schedules**

By William Jackson





Police at Los Angeles International Airport are using a computer science doctoral dissertation to help make their operations so unpredictable that would-be terrorists could not target the airport's facilities.

Terrorists can spend 18 to 36 months in surveillance of a potential target looking for vulnerabilities and patterns in security, said James Butts, deputy executive director of law enforcement for Los Angeles airports.

"If they choose you as a target, they are comfortable they can defeat your countermeasures," Butts said. "So one of the best things you can do is not be predictable. We want to minimize their belief that they can have a success here."

If terrorists do not know where the police will be or when, they cannot develop their own countermeasures, giving the police an edge. Since August, the airport has been using an application developed at the University of Southern California's Viterbi School of Engineering to randomize scheduling of vehicle security checkpoints and has more recently expanded its use to K9 patrols.

Midwife to the project was the Center for Risk and Economic Analysis of Terrorism Events (CREATE), a USC-based research center funded by the Homeland Security Department.

There have been no terrorist incidents at LAX since the application, called Armor, went into use, which is the ultimate goal — even if it's hard to prove that something not happening is the direct result of the application. But the more measurable result is what checkpoints and patrols have found at the airport using their randomized schedules.

"So far, we have recovered three firearms, interdicted three cars with drugs and taken into custody one car of people of interest from an intelligence standpoint," Butts said.

The core of the application is a randomization algorithm developed by doctoral student Praveen Paruchuri as part of his dissertation, "Keeping the Adversary Guessing: Agent Security by Policy Randomization."

Paruchuri examined ways to counter the inherent advantage bad guys have over good guys. The good guys — such as those in airport security — have to make the first move by committing themselves to a policy or pattern. The bad guys then have the opportunity to study that pattern to find a way around it. The good guys have to anticipate everything, but the bad guys only have to find one weakness to exploit.

**Playing the game**

The problem is not new. The security situation is analogous to a competitive business environment in which a smaller company has the advantage of looking for weaknesses in a larger company's business strategy.

In game theory, this is known as the Bayesian- Stackelberg game.

"We found this to be a very interesting topic," said Paruchuri's doctoral adviser, Milind Tambe, a professor specializing in artificial intelligence at the Viterbi School.

Work on the randomization algorithm began in 2004 and was completed in late 2006.

The following spring, Paruchuri earned his degree, and in April, the USC team was invited to present the results to law enforcement agencies.

"We had no idea when we were developing this that we would be working with LAX," Tambe said.

"I've been blown away at the welcome we received.

There were 20 or 25 police officers in the room. It seemed like every person there said, 'I have a problem. Can you solve it for me?' " The USC academics were introduced to the law enforcement crowd by Errol Southers, a former FBI agent and associate director of CREATE who also is in charge of intelligence and anti-terrorism at LAX.

"At that time, we were taking measures to lower our level of predictability," Butts said. "We looked at what they were doing and said we might have a use for it."

But what Paruchuri and Tambe had at that point was an algorithm. To turn it into an application required detailed inputs on LAX police missions and operations to get the right results.

“It was not trivial because it took time to figure out what is important, what we needed to pay attention to and what does not need attention,” Tambe said. “We are a university.

We don’t produce software [and] just ship copies off.”

With funding from CREATE, Tambe, Paruchuri, USC assistant professor of systems engineering Fernando Ordonez and a team of graduate students developed Armor.

They were able to demonstrate a version of the application to LAX police in July, and by August, the department began using it to schedule operations.

“We are a low-drag, high-speed organization,” Butts said of the speed with which the new tool was adopted. “It’s a work in progress. As we use it, there are improvements being made. But we consider it a viable tool at this point.”

**Stand-alone app**

Armor is a stand-alone application running on a Windows operating system, Tambe said.

“It is not integrated into any other scheduling system.”

It has a simple user interface with a randomize button that is used to schedule security checkpoints and the order of cars to be inspected in addition to patrol schedules and break times for officers.

There have been a few bumps in implementing the program. Because it takes away much of officers’ discretion on which cars will be searched, airport employees now are more subject to searches. “Employees weren’t used to being searched,” Butts said. “That was a paradigm change.” But officers are enthusiastic about the system, even though it has changed the way they perform their jobs.

Change can be difficult, Butts said, but “it depends on how you couch the change. We presented this as something to help them be more professional.”

Armor’s use is being gradually expanded at LAX, and Butts said officials are considering using it at Ontario Airport, another airport in the Los Angeles system. Tambe said he has talked with some federal officials about using Armor. He said there also is interest in seeing the software commercialized. Although the tool requires customization for each new customer, the task is not great.

“In the beginning, when we were turning the algorithm into an application, we didn’t know what to ask,” Tambe said. “Now we know exactly what we need to do. We know exactly what questions we need to ask and what we need to know.”

**More news on related topics:** IT Security, Homeland Security, Software Applications