

# Automated threat recognition software could speed airport security

May 10 2022

---



Body scanners used to ensure the security of hundreds of thousands of American travelers every year will be improved through software designed at Sandia National Laboratories. Credit: Andrea Starr, Pacific Northwest National Laboratory

Imagine moving through airport security without having to take off your

shoes or belt or getting pulled aside while your flight boards—while keeping all the precautions that ensure the safety of passengers and flight crews.

This is the challenge tackled by a team including researchers from Sandia National Laboratories—a challenge that led to development of the Open Threat Assessment Platform, which allows the Transportation Security Administration to respond more quickly and easily to threats to air travel safety.

"When we wanted to change how we screen in response to new threats," said Andrew Cox, a Sandia R&D systems analyst who leads the OTAP project. "The technology was too rigid. TSA compensated by adding procedures. There's a shoe bomber and you have to take your shoes off; liquid explosives arrived, and TSA had to limit liquids and gels."

The platform designed for TSA and Department of Homeland Security's Science and Technology Directorate will work similarly to Apple's iPhone, providing a common set of interfaces and data standards, which allow a variety of vendors to provide security upgrades and programs that will integrate seamlessly into the OTAP—like [building blocks](#) that can be changed out when needed for a specific [threat](#). The intent is to promote innovation, evolve towards a non-proprietary approach to technology, and expand the number of vendors participating in the aviation security market.

Sandia optical engineer Ed Jimenez said that TSA will be able to work through OTAP to collect data continuously and improve algorithms every few months. The standardization and modularized design with an open architecture should not only benefit the travel industry but make a better experience for air travelers.

"When you put an object in your bag that's mistakenly flagged as a

threat, the enhanced algorithm has the potential to not ring as a false positive alarm," Jimenez said. "You won't have to open the bag and slow down the line."

The OTAP project, led by Sandia, gathered together a dozen aviation security industry partners including algorithm developers, X-ray vendors and software specialists to create Open Platform Software Library (OPSL). In parallel, Pacific Northwest National Laboratory created a High-Definition Passenger Imaging System, which scans a body. In 2017, Sandia joined forces with PNNL, as well as several algorithm programmers, to combine the scanner with OPSL, creating a new full body machine that will more effectively detect threats. Additionally, OPSL could be combined with PNNL's shoe scanner and other algorithms to allow travelers to keep their shoes on.

That work earned Sandia an Interagency Partnership Award, Mid-Atlantic Region in October, from the Federal Laboratory Consortium for collaboration with PNNL, NASA, TSA and DHS's Science & Technology Directorate (Screening at Speed Program and Transportation Security Laboratory). The OTAP project was sponsored by the TSA, which was looking for a system that could be used throughout the [airline industry](#), and by DHS's Science and Technology Directorate, through the Screening at Speed Program.

The team is using automated threat recognition software to look at improving sensors—CT and AIT systems—by testing with real bags, toiletries and laptops, and simulated explosives, to demonstrate system accuracy. They hope to be in select airports conducting tests and evaluations later this year.

Provided by Sandia National Laboratories

Citation: Automated threat recognition software could speed airport security (2022, May 10)  
retrieved 20 April 2024 from  
<https://techxplore.com/news/2022-05-automated-threat-recognition-software-airport.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.