August 20, 2014 | By Ioana Patringenaru

Researchers Find Security Flaws in Backscatter X-ray Scanners

computer science Ph.D. student Keaton Mowery and Computer science professor Hovav Shacham. Photos by Erik Jepsen/UC San Diego Publications
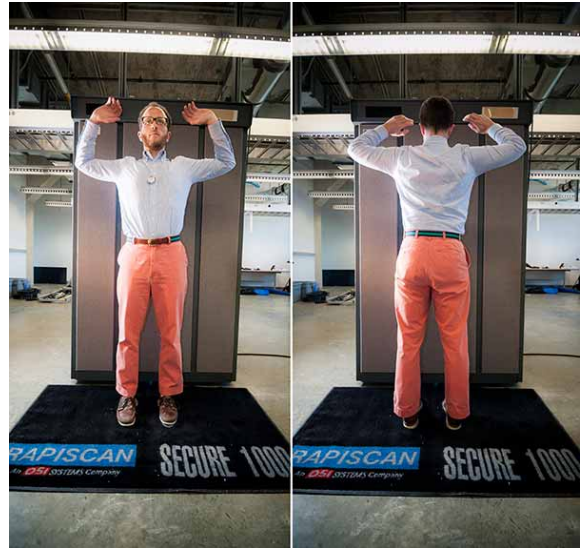
A team of researchers from the University of California, San Diego, the University of Michigan, and Johns Hopkins University have discovered several security vulnerabilities in full-body backscatter X-ray scanners deployed to U.S. airports between 2009 and 2013.

In laboratory tests, the team was able to successfully conceal firearms and plastic explosive simulants from the Rapiscan Secure 1000 scanner. The team was also able to modify the scanner operating software so it presents an "all-clear" image to the operator even when contraband was detected. "Frankly, we were shocked by what we found," said J. Alex Halderman, a professor of computer science at the University of Michigan. "A clever attacker can smuggle contraband past the machines using surprisingly low-tech techniques."

The researchers attribute these shortcomings to the process by which the machines were designed and evaluated before their introduction at airports. "The system's designers seem to have assumed that attackers would not have access to a Secure 1000 to test and refine their

attacks," said Hovav Shacham, a professor of computer science at UC San Diego However, the researchers were able to purchase a government-surplus machine found on eBay and subject it to laboratory testing.

Many physical security systems that protect critical infrastructure are evaluated in secret, without input from the public or independent experts, the researchers said. In the case of the Secure 1000, that secrecy did not produce a system that can resist attackers who study and adapt to new security measures. "Secret testing should be replaced or augmented by rigorous, public, independent testing of the sort common in computer security," said Shacham.

Professor Hovav Shacham stands in front of the backscatter x-ray scanner as you would during a security check. Photos by Erik Jepsen/UC San Diego Publications

Secure 1000 scanners were removed from airports in 2013 due to privacy concerns, and are now being repurposed to jails, courthouses, and other government facilities. The researchers have suggested changes to screening procedures that can reduce, but not eliminate, the scanners' blind spots. However, "any screening process that uses these machines has to take into account their limitations," said Shacham.

The researchers shared their findings with the Department of Homeland Security and Rapiscan, the scanner's manufacturer, in May. The team will present their findings publicly at the USENIX Security conference, Thursday Aug. 21, in San Diego. Details of the results will be available at radsec.org on Aug. 20.

To contact the research team, e-mail radsec-team@umich.edu.

MEDIA CONTACT

Ioana Patringenaru, 858-822-0899, ipatrin@ucsd.edu

UC San Diego's Studio Ten 300 offers radio and television connections for media interviews with our faculty, which can be coordinated via studio@ucsd.edu. To connect with a UC San Diego faculty expert on relevant issues and trending news stories, visit https://ucsdnews.ucsd.edu/media-resources/faculty-experts.