New tamper-detecting seal is tough to fool

July 8 2015, by Nancy Salem

Jason Hamlet was on the Sandia National Laboratories team that developed SecuritySeal, a device that attaches to a container and detects tampering. The technology, which is based on physical unclonable functions, or PUFs, is available for licensing. “We are looking for commercialization partners,” Jason said. “We want this to be licensed and moved to the next level.” Credit: Randy Montoya

A critical area of security is ensuring that something inside a container stays there. Sandia National Laboratories has made the job easier with an innovative technology that detects signs of tampering.

"In our world, one advance by an adversary can make a security technology obsolete overnight," said Dianna Blair, manager of Sandia's Global Technology Engagement, Research & Analysis Department. "The key is to stay ahead of the adversaries."

Sandia has a long history of research into tamper detection and continues to advance the field, providing technologies to the International Atomic Energy Agency and others.

One next-generation technology is SecuritySeal, a patented method of tagging and sealing containers or doors.

"You might have to guarantee that cargo has not been tampered with or that nuclear materials in storage haven't been diverted," said Sandia cybersecurity specialist Jason Hamlet.

The tool is based on national security research focused on arms control and treaty verification, said electronics engineer Todd Bauer, a principal investigator with Hamlet on the SecuritySeal project.

"In nonproliferation treaties, a weapon system is dismantled and the component parts are stored in different containers," Bauer said. "How do you know without continuous visual surveillance that no one has gone into the containers? This tool can remotely monitor treaty compliance with assurance."

SecuritySeal is placed on a closed container so that any attempt to open it is detected cryptographically. "When you come back in the future you can verify that it had not been opened," Bauer said.

Moving technology into the marketplace

Hamlet and Bauer came up with the idea in 2009 and worked on it for several years with support from the Laboratory Directed Research and Development program. The technology is based on physical unclonable functions, or PUFs, the small defects that are part of any manufacturing process, a function of materials properties and tolerances.

Microelectronics is no exception. "Electrical characteristics exist in microelectronics that were not designed, small variations from one device to another that exist due to the manufacturing process," Hamlet said. "A PUF is a measurement of those variations, which are uncontrollable, unclonable and unique to individual devices. It's a kind of fingerprint."

The prototype is a little bigger than a credit card and would fit a truck or cargo container. But it could be larger or small enough to fit a prescription medication bottle. "Seal a truck, seal a pallet, seal a box or a bottle," Bauer said. "You will know if the container has been opened and that what is in it is what is supposed to be in it."

SecuritySeal is available for licensing and is in the U.S. Department of Homeland Security's Transition to Practice program, which helps broaden the use of cybersecurity technologies developed through federally funded research and development. The program connects researchers, the federal government and the private sector to drive technology from research labs to the marketplace.

"We are looking for commercialization partners," Hamlet said. "We want this to be licensed and moved to the next level."

Resistance properties of the network change if someone tries to lift, slide or remove the film from the surface to which it is adheres, and the PUF

response is altered so the tamper is detected. A digital reader checks the device remotely and can infer a change in signature if the tag-seal fails to properly respond. Knowledge of the private key is needed to generate the right response. If the PUF changes, the private key changes and the tag-seal can't provide the correct response.

A deterrent to adversaries

"Tamper-indicating seals are a critical part of the regime I work in," Blair said. "SecuritySeal might not stop tampering, but it will help us monitor if a protected volume has been accessed. It addresses a key vulnerability. If a seal can be counterfeited, an intruder could take it off and replace it with one that looks just like it. SecuritySeal has a unique signature that cannot be counterfeited. It has a strong deterrence factor."

But the device, which could be manufactured either with custom parts or with cheaper commercial, off-the-shelf components, has other potential uses including protecting pharmaceuticals, cargo, criminal evidence containers, ballot boxes or consumer goods against warranty fraud.

"The market is quite broad for this technology," Bauer said. "There are many ways to seal and protect assets, starting with padlocks. Our goal is to raise the bar. This helps keep everyone a little more honest."

Provided by Sandia National Laboratories

Citation: New tamper-detecting seal is tough to fool (2015, July 8) retrieved 6 May 2024 from https://phys.org/news/2015-07-tamper-detecting-tough.html