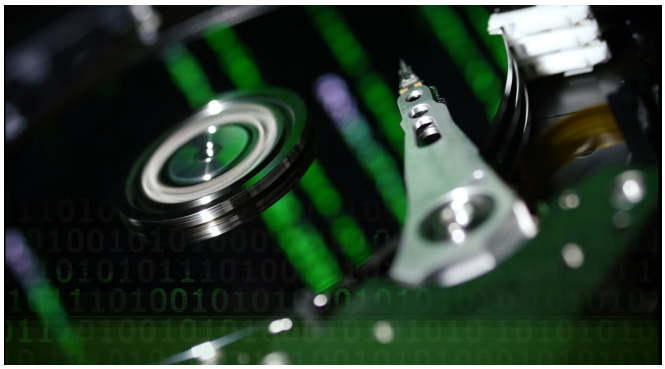
Sonic cyber attack shows security holes in ubiquitous sensors

14 March 2017



Credit: University of Michigan

Sound waves could be used to hack into critical sensors in a broad array of technologies including smartphones, automobiles, medical devices and the Internet of Things, University of Michigan research shows.

The new work calls into question the longstanding computer science tenet that software can automatically trust hardware sensors, which feed autonomous systems with fundamental data they need to make decisions.

The inertial sensors involved in this research are known as capacitive MEMS accelerometers. They measure the rate of change in an object's speed in three dimensions.

It turns out they can be tricked. Led by Kevin Fu, U-M associate professor of computer science and engineering, the team used precisely tuned acoustic tones to deceive 15 different models of accelerometers into registering movement that never occurred. The approach served as a backdoor into the devices—enabling the researchers to control other aspects of the system.

"The fundamental physics of the hardware allowed us to trick sensors into delivering a false reality to the microprocessor," Fu said. "Our findings upend widely held assumptions about the security of the underlying hardware.

"If you look through the lens of computer science, you won't see this security problem. If you look through the lens of materials science, you won't see this security problem. Only when looking through both lenses at the same time can one see these vulnerabilities."

The researchers performed several proof-of-concept demonstrations: They used a $5 speaker to inject thousands of fictitious steps into a Fitbit. They played a malicious music file from a smartphone's own speaker to control the phone's accelerometer trusted by an Android app to pilot a toy remote control car. They used a different malicious music file to cause a Samsung Galaxy S5's accelerometer to spell out the word "WALNUT" in a graph of its readings.

All accelerometers have an analog core—a mass suspended on springs. When the object the accelerometer is embedded in changes speed or direction, the mass moves accordingly. The digital components in the accelerometer process the signal and ferry it to other circuits.

"Analog is the new digital when it comes to cybersecurity," Fu said. "Thousands of everyday devices already contain tiny MEMS accelerometers. Tomorrow's devices will aggressively rely on sensors to make automated decisions with kinetic consequences."

Autonomous systems like package delivery drones and self-driving cars, for example, base their decisions on what their sensors tell them, said Timothy Trippel, a doctoral student in computer science and engineering and first author of a new paper on the findings.

"Humans have sensors, like eyes, ears and a nose. We trust our senses and we use them to make decisions," Trippel said. "If autonomous systems can't trust their senses, then the security and reliability of those systems will fail."

The trick Trippel and Fu introduced exploits the same phenomenon behind the legend of the opera singer breaking a wine glass. Key to that process is hitting the right note—the glass' resonant frequency.

The researchers identified the resonant frequencies of 20 different accelerometers from five different manufacturers. Then instead of shattering the chips, they tricked them into decoding sounds as false sensor readings that they then delivered to the microprocessor.

Trippel noticed additional vulnerabilities in these systems as the analog signal was digitally processed. Digital "low pass filters" that screen out the highest frequencies, as well as amplifiers, haven't been designed with security in mind, he said. In some cases, they inadvertently cleaned up the sound signal in a way that made it easier for the team to control the system.

The researchers recommend ways to adjust hardware design to eliminate the problems. They also developed two low-cost software defenses that could minimize the vulnerabilities, and they've alerted manufacturers to these issues.

The university is pursuing patent protection for the intellectual property and is seeking commercialization partners to help bring the technology to market.

The researchers will present a paper on the work April 26 in Paris at the IEEE European Symposium on Security and Privacy. The paper is titled "WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks."

More information: Paper: WALNUT: Acoustic Attacks on MEMS Sensors, spqr.eecs.umich.edu/walnut/

Provided by University of Michigan