3-D printers help override biometric security measures

April 10 2020, by Peter Grad

Credit: Talos

Fingerprint recognition: It was once thought to be the ultimate fool-proof measure to secure computers, laptops and mobile devices.

Since Apple ushered in the era of fingerprint detection in 2013 with the release of the iPhone 5s boasting the first TouchID system, virtually all

major device manufacturers soon jumped on board.

But the technology was not foolproof. In fact, barely 48 hours after the release of iPhone 5s, hackers were able to override the security measure using what they called "easy everyday means." In this instance, they lifted a fingerprint from a sheet of glass and created a latex glove with the print.

Still, fingerprint recognition technology improved, becoming increasingly popular with users tired of having to remember ever-more complex passwords to gain access to their devices.

But a study published Wednesday may shatter the myth of biometric security. The cybersecurity organization Cisco Talos Intelligence Group found that spoofing fingerprints can be achieved with an 80 percent success rate, and that expensive equipment is not needed to pull it off.

With fingerprint scans commonly used in smartphones, computers, USB devices and home and office locks, millions of users are vulnerable.

The security team acknowledged that successfully breaking and entering a device through biometrics was fairly complex. But they were nevertheless able to achieve the feat with a readily available 3-D printer that recreated a finger and print with a simple mold and glue.

The testers found that Mac products were more vulnerable to biometric override than units running Windows 10. But they noted that they were able to make more attempts at breaking into Apple iPads because they knew the codes to override the five-entry limit on fingerprint attempts. Without those codes, their success rate would have been notably lower.

"Reaching this success rate was difficult and tedious work," the researchers said in a blog post on the Talos site. "We found several

obstacles and limitations related to scaling and material physical properties. Even so, this level of success rate means that we have a very high probability of unlocking any of the tested devices before it falls back into the pin unlocking."

The proliferation of low-cost 3-D printers made it easier for malicious actors to bypass fingerprint barriers. Their use "made it possible for anyone to create fake fingerprints," Talos researchers said. "Moreover, with the democratization of the usage of fingerprint authentication, the impact of biometric data copies is even bigger than in the past."

General consumers may be reassured that hackers must overcome significant barriers to break through security—they must obtain a user's fingerprint and then the user's device—the likelihood of being targeted is not high.

"The results show fingerprints are good enough to protect the average person's privacy if they lose their phone," Talos researchers said. But they cautioned, "However, a person that is likely to be targeted by a well-funded and motivated actor should not use fingerprint authentication."

Biometrics detection has long been a staple of Hollywood science fiction.

In 1989, "Back to the Future II" made predictions 25 years into the future: Among them, Marty McFly (Michael J. Fox) used fingerprints to unlock doors, and bully Biff Howard Tannen paid his taxi cab fare with a fingerprint scan.

In "Dredd," creators envisioned the Lawgiver, a handgun with a three-mile range that explodes in the hands of a user whose fingerprints are not recognized.

In 2002, optical recognition identified people and possible predicted criminal tendencies. When Chief of PreCrime John Anderson, played by Tom Cruise, is hunted down by the bad guys, he gets an eye transplant to avoid detection and carries his original eyeballs to retain access to his former office.

Talk about keeping an eye out for danger.

More information: blog.talosintelligence.com/202 … rprint-research.html