Dec. 4, 2018

Machine learning masters the fingerprint to fool biometric systems

Fingerprint authentication systems are a widely trusted, ubiquitous form of biometric authentication, deployed on billions of smartphones and other devices worldwide. Yet a new study from Michigan State University and New York University reveals a surprising level of vulnerability in these systems.

Using a neural network trained to synthesize human fingerprints, the research team evolved a fake fingerprint that could potentially fool a touch-based authentication system for up to one in five people.

Much the way that a master key can unlock every door in a building, these “DeepMasterPrints” use artificial intelligence to match many prints stored in fingerprint databases and could thus theoretically unlock a large number of devices.

The work builds on earlier research led by Nasir Memon, NYU computer scientist, and Arun Ross, Michigan State University professor of computer science and engineering. They coined the term “MasterPrint” to describe how partial fingerprint-based systems can be compromised by using strategically created fake prints.

“As fingerprint sensors become smaller in size, it is imperative for the resolution of the sensor to be significantly improved for it to capture additional fingerprint features,” Ross said. “If resolution is not improved, the distinctiveness of a user’s fingerprint will be inevitably compromised. The empirical analysis conducted in this research clearly substantiates this.”

Devices typically allow users to enroll several different finger images, and a match with any enrolled partial print is enough to confirm identity. Partial fingerprints are less likely to be unique than full prints, and their earlier research
demonstrated that enough similarities exist between partial prints to create MasterPrints capable of matching many stored partials in a database.

In the new study, doctoral student Philip Bontrager and computer scientist Julian Togelius from NYU along with their collaborators, including Memon and Ross, took this concept further, training a machine-learning algorithm to generate synthetic fingerprints as MasterPrints. The researchers created complete images of these synthetic fingerprints, a process that has twofold significance. First, it is yet another step toward assessing the viability of MasterPrints against real devices, which the researchers have yet to test; and second, because these images replicate the quality of fingerprint images stored in fingerprint-accessible systems, they could potentially be used to launch a brute force attack against a secure cache of these images.

The new study was presented at the IEEE International Conference of Biometrics: Theory, Applications and Systems by Philip Bontrager, the first author of the paper.

“These experiments demonstrate the need for multi-factor authentication and should be a wake-up call for device manufacturers about the implications of artificial fingerprint attacks,” Bontrager said.

This research has applications in fields beyond security. Togelius noted that their Latent Variable Evolution method used here to generate fingerprints can also be used to make designs in other industries – notably game development. The technique has already been used to generate new levels in popular video games.

A National Science Foundation grant supported the work. The research team also includes postdoctoral fellow Aditi Roy, who was lead author for the original MasterPrint paper.

Related Website: Story courtesy of MSUToday. Communications contact: Patricia Mroczek