Can mobile phones be secured with a fingerprint?

No two people are believed to have identical fingerprints, but researchers from New York University and Michigan State University have found that partial similarities between prints are common enough that the fingerprint-based security systems used in mobile phones and other devices can be more vulnerable than previously thought.

The vulnerability lies in the fact that fingerprint-based authentication systems feature small sensors that do not capture a user’s full fingerprint. Instead, they scan and store partial fingerprints, and many phones allow users to enroll several different fingers in their authentication system. Identity is confirmed when a user’s fingerprint matches any of the saved partial prints. The researchers hypothesized that there could be enough similarities among different people’s partial prints that one could create a “MasterPrint.”

Arun Ross, MSU professor of computer science and engineering and co-author of the study, said a number of electronic devices such as smartphones are beginning to incorporate fingerprint sensors for user authentication. The sensors embedded in these devices are generally small and the resulting images are limited in size. To compensate, these devices often acquire multiple partial impressions of a single finger during enrollment to ensure that at least one of them will successfully match with the image obtained from the user during authentication. This introduces a vulnerability that needs to be carefully addressed.
As fingerprint sensors become smaller in size, it is imperative for the resolution of the sensor to be significantly improved in order 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.”

Ross said the research team is currently investigating ways to address the vulnerability highlighted in this work. This could entail developing effective anti-spoofing schemes; carefully selecting the number and nature of partial impressions of a user during enrollment; improving the resolution of small-sized sensors to facilitate extraction of more discriminative features; developing matchers that utilize both minutiae and texture information; and designing more effective fusion schemes to combine the information presented by multiple partial impressions of a user.

Nasir Memon, NYU professor of computer science and engineering and the research team leader, said the MasterPrint concept bears similarity to a hacker who attempts to crack a PIN-based system using a commonly adopted password such as 1234.

"About 4 percent of the time, the password 1234 will be correct, which is a relatively high probability when you’re just guessing," said Memon.

The researchers, whose work was funded by the National Science Foundation, undertook their analysis using 8,200 partial fingerprints. Using commercial fingerprint verification software, they found an average of 92 potential MasterPrints for every randomly sampled batch of 800 partial prints. (They defined a MasterPrint as one that matches at least 4 percent of the other prints in the randomly sampled batch.)

On the contrary, they found just one full-fingerprint MasterPrint in a sample of 800 full prints. “Not surprisingly, there’s
a much greater chance of falsely matching a partial print than a full one, and most devices only rely on partials for identification," said Memon.

The team analyzed the attributes of MasterPrints culled from real fingerprint images, and then built an algorithm for creating synthetic partial MasterPrints. Experiments showed that synthetic partial prints have an even wider matching potential, making them even likelier to fool biometric security systems than real partial fingerprints. With MasterPrints derived from real human fingerprints, the team reported successfully matching between 26 and 65 percent of users, depending on how many partial fingerprint impressions were stored for each user and assuming a maximum number of five attempts per authentication. For synthetic MasterPrints, the matching possibilities were even higher.

The higher the number of partial fingerprints a smartphone stores for each user, the more vulnerable it is.

The researchers emphasize that their work was done in a simulated environment, but note that improvements in creating synthetic prints and techniques for transferring digital MasterPrints to physical artifacts in order to spoof an operational device pose significant concerns. The high matching capability of MasterPrints points to the challenges of designing trustworthy fingerprint-based authentication systems, and reinforces the need for multi-factor authentication schemes to enhance the security of these systems. The researchers believe this work may inform future designs. Meanwhile, unlocking a mobile device with a code remains more secure, Memon said.


Portions of this story courtesy of New York University Tandon School of Engineering.

Related Website: Arun Ross bio
New York Times tech story
Communications contact: Patricia Mroczek