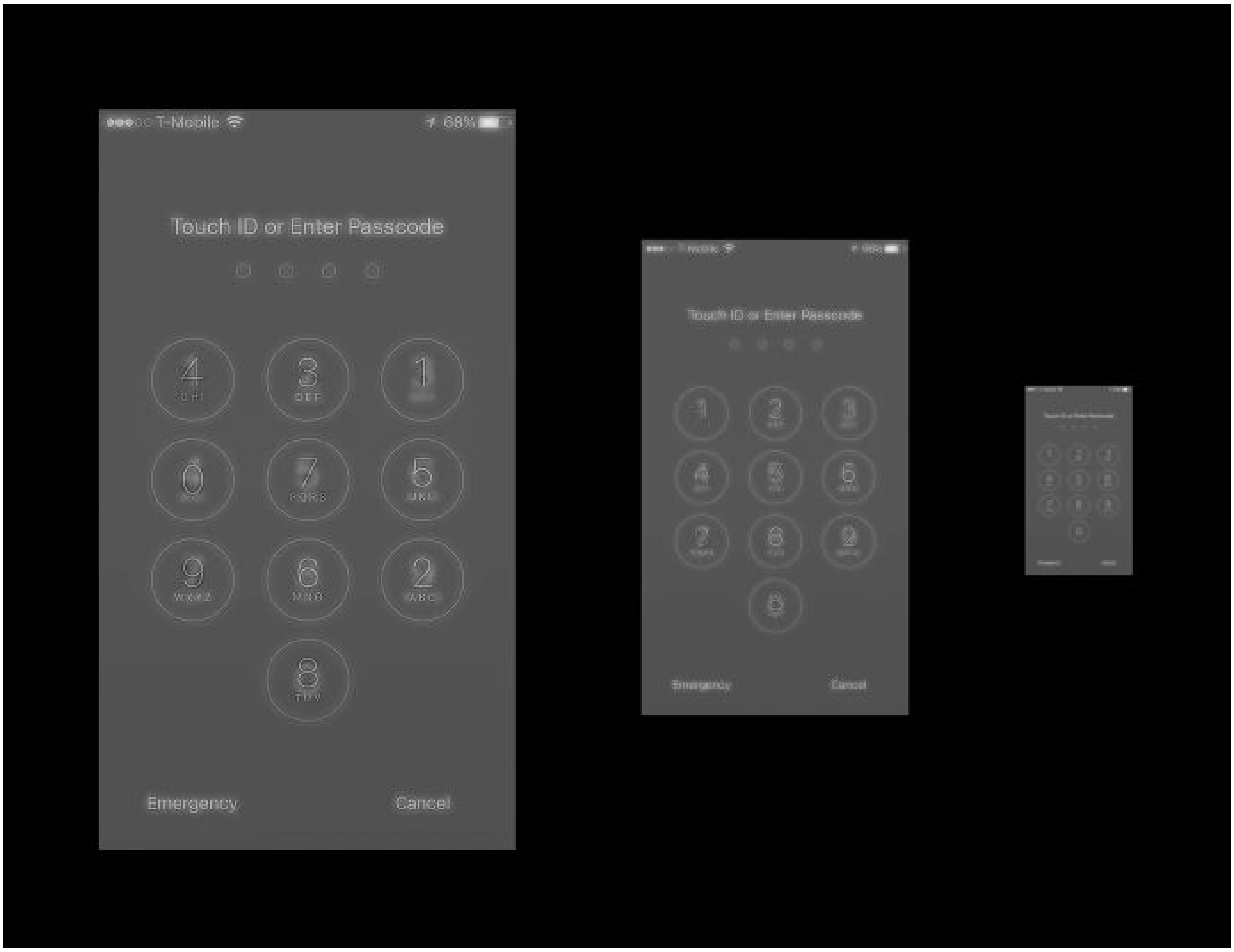
TechXplore

Tricking the eye to defeat shoulder surfing attacks

August 22 2017



IllusionPIN foils identify theft by deploying a hybrid-image keyboard to confuse would-be hackers. Credit: NYU Tandon School of Engineering

Every ATM or smartphone user can attest to the discomfort of having a stranger standing close enough to observe a financial transaction—and potentially note a PIN or account number. Now researchers at the NYU Tandon School of Engineering have announced a first-of-its-kind application to combat such "shoulder-surfing," whether in person or via a building's video camera.

Nasir Memon, NYU Tandon professor of computer science and engineering, explained that the technology, called "IllusionPIN," deploys a hybrid-image keyboard that appears one way to the close-up user and differently to an observer at a distance of three feet or greater. The underlying technology blends one image of a keyboard configuration with high spatial frequency and a second, completely different, keyboard configuration with low spatial frequency. The visibility of each image is dependent on the distance from which it is viewed.

"The traditional configuration of numbers on a keypad is so familiar that it's possible for an observer to discern a PIN or access code after several viewings of surveillance video," said Memon. "On a device running IllusionPIN, the user—who is closest to the device—sees one configuration of numbers, but someone looking from a distance sees a completely different keypad."

IllusionPIN reconfigures the keypad for each authentication or login attempt.

The research team, which also includes NYU Tandon doctoral candidates Athanasios Papadopoulos, Toan Nguyen, and Emre Durmus, simulated a series of shoulder-surfing attacks on smartphone devices to test the effectiveness of IllusionPIN at various distances. In total, they performed 84 attempted shoulder-surfing attacks on 21 participants, none of which was successful. For contrast, they also mounted 21 shoulder-surfing attacks on unprotected phones using the same distance parameters; all 21 attacks were successful. The team also determined that IllusionPIN makes it nearly impossible to steal PIN or other authentication information using surveillance footage.

Awareness of the threat potential posed by shoulder surfing has increased significantly over the past decade, since the advent of the first smartphones. And while there are no reliable statistics on the prevalence of shoulder surfing attacks, a 2016 study conducted by Memon and Nguyen found that 73 percent of mobile device users surveyed reported that they had observed someone else's PIN (although not necessarily with malicious intent), and a 2017 study of shoulder surfing awareness presented at the ACM Conference on Human Factors in Computing Systems reported that 97 percent of those surveyed claimed awareness of a shoulder surfing incident in everyday life, and that in the majority of cases, victims were unaware that they were being observed.

"PIN authentication is popular for good reasons, namely that it is easy to use and to remember," said Memon. "Our goal was to increase the resilience of PIN authentication without straining the device or compromising user experience."

More information: Athanasios Papadopoulos et al. IllusionPIN: Shoulder-Surfing Resistant Authentication Using Hybrid Images, *IEEE Transactions on Information Forensics and Security* (2017). DOI: 10.1109/TIFS.2017.2725199

Provided by NYU Tandon School of Engineering

Citation: Tricking the eye to defeat shoulder surfing attacks (2017, August 22) retrieved 10 April 2024 from https://techxplore.com/news/2017-08-eye-defeat-shoulder-surfing.html