Exploit steals passwords by tapping into keystrokes

September 13 2023, by Peter Grad

Credit: Unsplash/CC0 Public Domain

Add one more threat to the list of risks you take when you use your phone to conduct business at the local coffee shop.

Researchers from universities in China and Singapore uncovered a security gap that permits snoops to lift your password by identifying your keystrokes.

Researchers are calling Wiki-Eve "the first WiFi-based hack-free keystroke eavesdropping system."

The cyberattack demonstrated by the researchers is made possible thanks to a feature in wireless communications called BFI, beamforming feedback information. BFI permits devices to more accurately transmit feedback about their location, sending signals specifically towards the routers that are to receive them, instead of dispersing them omnidirectionally.

But one vulnerability of BFI, a component of the 802.11ac WiFi standard (also known as WiFi 5), is that it transmits data in cleartext. That means there is no need for physical hacking or cracking of an encryption key.

The researchers devised a means of identifying a user's device and capturing the cleartext transmissions.

Unlike older side-channel attacks, Wiki-Eve does not require planting rogue programs that trick a user into logging on to an illegitimate site. It also does not require setting up additional links to sense a target user's keystrokes.

"Since BFI is transmitted from a smartphone to an AP [access point] in cleartext," the researchers said, "it can be overheard by any other Wi-Fi devices switching to monitor mode."

Researchers said Wiki-Eve "achieves 88.9% inference accuracy for individual keystrokes and up to 65.8% top-10 accuracy for stealing

passwords of mobile applications."

Keystroke inference is the determination of what key is being pressed based on BFI data. As a user glides over keys on a keypad, the variations in wireless signals between device and base station can be tracked and identified with the aid of a deep-learning model.

The team ran tests using numerical passwords since they are easier to decipher than alphanumeric passwords.

They demonstrated Wiki-Eve by successfully lifting WeChat Pay passwords from a subject in a nearby conference room.

Wiki-Eve joins a long list of side-channel attack methods. Such methods include acoustic cryptanalysis that interprets sounds produced by a device during transmission, cache attacks that probe access patterns, electromagnetic analysis that uses radiation to decipher information, and thermal attacks that track temperature variations to reveal activities.

The study assumed users were engaging in activity over an unprotected network, common in public spaces such as coffeeshops, airports, train stations and other gathering places offering free WiFi.

The researchers had a simple recommendation for a defense against Wiki-Eve: "Since WiKI-Eve achieves keystroke eavesdropping by overhearing Wi-Fi BFI, the most direct defense strategy is to encrypt data traffic," they said, "hence preventing attackers from obtaining BFI in cleartext."

The researchers presented their study, "Password-Stealing without Hacking: Wi-Fi Enabled Practical Keystroke Eavesdropping," on the preprint server *arXiv*. The team includes researchers from Hunan University and Fudan University in China, as well as Nanyang

Technological University in Singapore.

More information: Jingyang Hu et al, Password-Stealing without Hacking: Wi-Fi Enabled Practical Keystroke Eavesdropping, *arXiv* (2023). DOI: 10.48550/arxiv.2309.03492