Visa and Apple Pay vulnerabilities leaves iPhone users open to payment fraud

September 30 2021

Credit: Pixabay/CC0 Public Domain

Vulnerabilities in Apple Pay and Visa could enable hackers to bypass an iPhone's Apple Pay lock screen and perform contactless payments, according to research by the University of Birmingham and University

of Surrey.

Experts in the University of Birmingham's School of Computer Science and the University of Surrey's Department of Computer Science found their approach could also be used to bypass the contactless limit allowing transactions of any amount to be performed. Their results will be presented in a paper at the *2022 IEEE Symposium on Security and Privacy.*

The researchers discovered the vulnerability occurs when Visa cards are set up in 'Express Transit mode' in an iPhone's wallet. Transit mode is a feature on many smartphones that enables commuters to make a swift contactless mobile payment at, for example, an underground station turnstile, without fingerprint authentication.

The weakness lies in the Apple Pay and Visa systems working together and does not affect other combinations, such as Mastercard in iPhones, or Visa on Samsung Pay.

Using simple radio equipment, the team identified a unique code broadcast by the transit gates, or turnstiles. This code, which the researchers nicknamed the 'magic bytes' will unlock Apple Pay. The team found they were then able to use this code to interfere with the signals going between the iPhone and a shop card reader. By broadcasting the magic bytes and changing other fields in the protocol, they were able to fool the iPhone into thinking it was talking to a transit gate, whereas actually, it was talking to a shop reader.

At the same time, the researchers' method persuades the shop reader that the iPhone had successfully completed its user authorisation, so payments of any amount can be taken without the iPhone's user's knowledge.

Dr. Andreea Radu, in the School of Computer Science at the University of Birmingham, led the research. She said: "Our work shows a clear example of a feature, meant to incrementally make life easier, backfiring and negatively impacting security, with potentially serious financial consequences for users.

"Our discussions with Apple and Visa revealed that when two industry parties each have partial blame, neither are willing to accept responsibility and implement a fix, leaving users vulnerable indefinitely."

Co-author Dr. Ioana Boureanu, from the University of Surrey's Centre for Cyber Security, added: "We show how a usability feature in contactless mobile payments can lower security. But, we also uncovered contactless mobile-payment designs, such as Samsung Pay, which is both usable and secure. Apple Pay users should not have to trade-off security for usability, but —at the moment— some of them do."

Co-author Dr. Tom Chothia, also in the School of Computer Science at the University of Birmingham, said: "iPhone owners should check if they have a Visa card set up for transit payments, and if so they should disable it. There is no need for Apple Pay users to be in danger but until Apple or Visa fix this they are."

More details of a £1000 payment being taken from a locked iPhone are available at practical_emv.gitlab.io

Provided by University of Birmingham