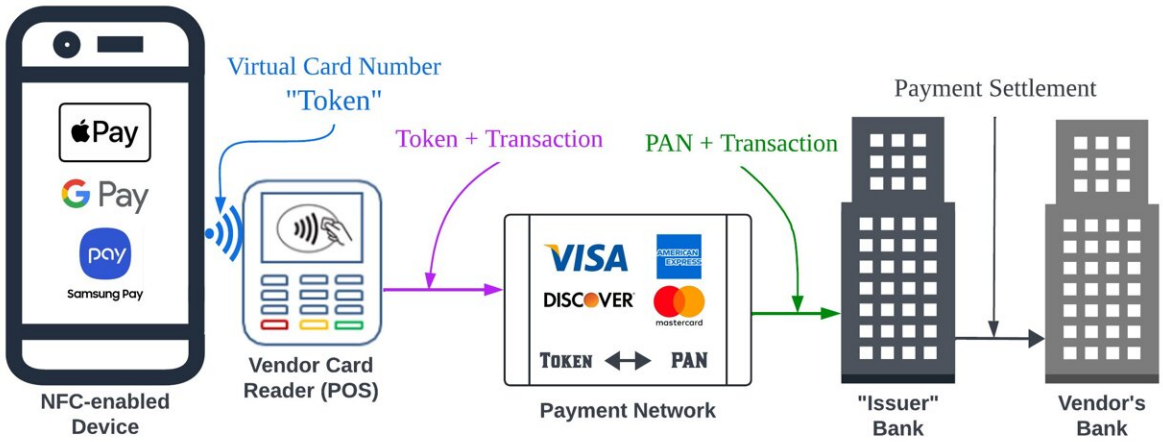
New study reveals loophole in digital wallet security—even if rightful cardholder doesn't use a digital wallet

August 14 2024



This diagram illustrates the typical digital wallet and credit card envrionment. Credit: Raja Hasnain Anwar, UMass Amherst

Digital wallets—like Apple Pay, Google Pay and PayPal—are projected to be used by more than 5.3 billion people by 2026. While these wallets promote increased security over traditional payment methods, reliance on outdated authentication methods and prioritizing convenience over security leaves digital wallets vulnerable, according to new research led by computer engineers at the University of Massachusetts Amherst.

"What we have discovered is [that] these digital wallets are not secure," says Taqi Raza, assistant professor of electrical and computer engineering and an author on the paper. "The main reason is that they have unconditional trust between the cardholder, the wallet and the bank."

In the normal digital wallet ecosystem, users start by inputting their credit or debit card number, called the primary account number (PAN), into the digital wallet. The user's identity is authenticated as the rightful cardholder with a piece of information, such as a zip code or the last four digits of their social security number.

Then, whenever a purchase is made, the wallet hides the PAN and shares a "token" with the vendor. The vendor attaches the token to the transaction. This information goes back through the bank's payment network, converting the token back to the PAN. The bank then settles the payment with the vendor on behalf of the customer without ever revealing the PAN to the vendor.

Unfortunately, there are ways that bad actors can circumnavigate this system to make purchases with other people's credit cards. The major U.S. banks and digital wallet companies impacted by this are described in the paper. These companies were informed of the study findings prior to its publication and given ample time to make necessary security improvements. The researchers used their own cards to complete their tests and no fraudulent activity was performed in these security tests.

First, there is the issue of the initial authentication. "Any malicious actor who knows the [physical] card number can pretend to be the cardholder," says Raza. "The digital wallet does not have sufficient mechanism to authenticate whether the card user is the cardholder or not." He emphasizes that existing authentication methods can easily be bypassed.

Another issue is that, once a victim reports their card stolen, the banks only block transactions from a physical card, not ones made through a digital wallet. Banks assume that their authentication system has sufficient security to prevent attackers from adding someone else's card to their wallet, which, as Raza points out, is not the case.

Once stolen card numbers are saved in a digital wallet, it is virtually impossible for the cardholder to deactivate them. "Even if the cardholder requests a card replacement, banks do not re-authenticate the cards stored in the wallet," says Raza. "What they do is they simply change the virtual number mapping to the new physical card number."

Here is a fictional example: The victim's credit card number ends in 0123. An attacker adds 0123 to their digital wallet and starts making purchases. Again, digital wallets work by sending a virtual number to the vendor, so vendors receive the virtual number ABCD and take this number to the bank to get payment associated with account 0123.

The victim discovers the fraudulent payments and asks the bank to issue a new credit card. The bank sends a new card with the number 4567 and, on the back end, remaps the virtual number: ABCD no longer links to 0123, it now links to 4567. The wallet automatically starts showing the new card to its user without any verification for the new card to be updated in the wallet. Vendors then go to the bank with ABCD, which has now been linked to 4567, the new and active number, and the purchase goes through.

The researchers also tested this loophole on the digital wallet side of the equation and found similar vulnerabilities. "We want [the digital wallet companies] to take some responsibility as well because they are at the forefront of how these transactions happen," says Raja Hasnain Anwar, a doctoral candidate in electrical and computer engineering and lead study author. "We want them to have solid coordination. That's the whole point

of the paper: there's not. There's a lack of coordination."

He highlights that many of these issues stem from new features offered by the banks. "For example, you could share your card within a family—one card could be added to multiple mobile phones," he says.

"Or if you have a Netflix subscription, the credit card company doesn't want you to lose that subscription, so they will keep on charging your card, even though that card is locked. If the banks are trying to move all of their payment platforms digitally, they need to put in more effort to make that secure. They cannot just rely on existing technology to take care of it."

"It's security versus convenience," adds Raza. "And we found the banks give more priority to convenience than security. Security is taken for granted because they believe that the user-device verification being used is sufficient for wallet security. It's not."

While this specific loophole has been resolved, researchers still recommend following security best practices: turn on email notifications when a card is added/removed from the wallet, turn on transaction alerts for credit cards, regularly check credit card statements and review devices linked to credit cards through the bank's web portal or mobile app account settings.

More information: Anwar et al. In Wallet We Trust: Bypassing the Digital Wallets Payment Security for Free Shopping (2024). www.usenix.org/conference/usen … 4/presentation/anwar

Provided by University of Massachusetts Amherst