Not fare: Hacker app resets subway card for free rides (w/ Video)

September 23 2012, by Nancy Owano

Credit: Wikipedia

(Phys.org)—You have to love the ease and convenience of NFC technology in smartphones. Unless you run a mass transit system in a major city that moves millions of people in and out of trains, morning noon and night, then love alone is not enough. As fares form a crucial part of transit system revenue to keep everything running, system administrators would need to take note of what security hackers accomplished—an app that takes advantage of a weakness in NFC-based subway cards that lets users ride on trains for free. The two researchers, Corey Benninger and Max Sobell, from the Intrepidus Group, figured out a way that replenishes a fare-card balance.

They tested the app's success on two transit systems, New Jersey Path

and San Francisco Muni trains. Benninger and Sobell said that other systems might be vulnerable to such an exploit, in the form of an Android application that could make it possible for holders of a card to get free rides in Boston, Seattle, Salt Lake City, Chicago, and Philadelphia. Those other systems were not tested by the researchers,

Their discovery was announced at the EUSecWest security conference in Amsterdam, where they told those attending that if they ever thought smartphone tricks could get them public transit rides, then they would be correct. "A number of cities are rolling out RFID/NFC enabled access control as they move away from magstripe cards. This comes at a time when smartphones are also being enabled with NFC capabilities," they said.

They also said it was unfortunate that mass transit systems in the cities that could be vulnerable did not appear to understand how the security around the systems needs to be implemented—it is not a matter of bad technology but of proper implementation. Both of these systems tested, they said, were not using the security features of these cards correctly, allowing the two researchers to re-set the cards' data.

The researchers wrote software for mobile phones to accomplish the free-ride exploit without difficulty. When a traveler exhausts the ride-remaining balance, the app can reset the balance to 10 rides remaining, not zero rides. They call their hack app UltraReset. They loaded up UltraReset on their smartphone and wrote data back to a card without the associated payment being required. They said anyone with know-how to rewrite data to the NFC chip can do this.

Benninger said that he coded the app in one night, and, he added, he is not a coder. The app works on Android 2.3 or later. Their demo shows the UltraReset app running on a Nexus S smartphone. "I can do that over and over again if I chose to," said Benninger.

Contactless payment technology supports the exploit. The train tickets have NFC chips built into them, and the hack exploits the Mifare Ultralight chip used in disposable contactless NFC cards. The chip makes the card work like a punch card system, but the card can flip bits on to indicate that a travel unit has been used. In the vulnerable systems, user information on the card is checked but the bits are never turned on. This allowed the two exploiters to rewrite the cards. The bits are supposed to block anyone from reverting the card to its original state, but it would only serve as a security feature if the authorities in charge were to turn that feature on.

The researchers hope that their discovery will eventually allow vulnerable transit companies to work out their card security implementation or adjust their back-end systems to make sure bits in the cards are turned on when travel units are used. San Francisco and New Jersey authorities were informed about this problem, they said, but as far as they know, both systems are still vulnerable, they added. San Francisco was informed in December 2011.

Citation: Not fare: Hacker app resets subway card for free rides (w/ Video) (2012, September 23) retrieved 27 April 2024 from https://phys.org/news/2012-09-fare-hacker-app-resets-subway.html