RFID cards could turn into a global security mess after discovery of hardware backdoor

Security researchers at Quarkslab have discovered a backdoor in millions of RFID cards developed by Shanghai Fudan Microelectronics (FMSH). When properly exploited, this backdoor could be used...

By Alfonso Maruccia

Aug 26, 2024 03:16 PM · 2 min. read · View original

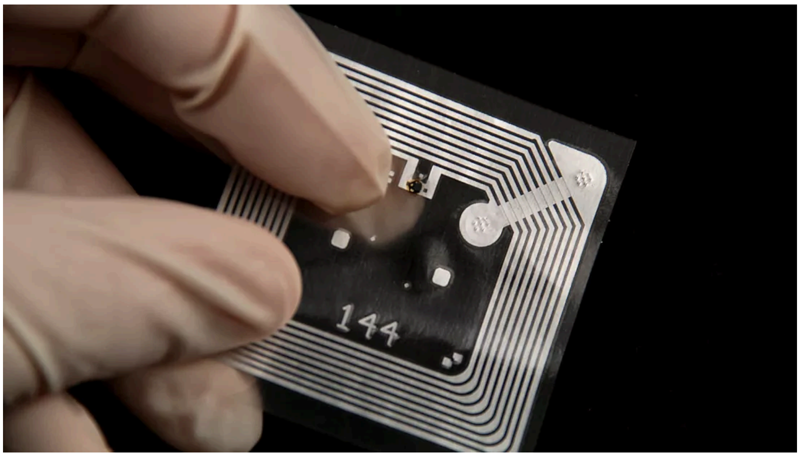
WTF?! Chinese-made chips used in popular contactless cards contain hardware backdoors that are easy to exploit. These chips are compatible with the proprietary Mifare protocol developed by Philips spin-off NXP Semiconductors and are inherently "intrinsically broken," regardless of the card's brand.

Security researchers at Quarkslab have discovered a backdoor in millions of RFID cards developed by Shanghai Fudan Microelectronics (FMSH). When properly exploited, this backdoor could be used to quickly clone contactless smart cards that regulate access to office buildings and hotel rooms worldwide.

According to French researchers, "Mifare Classic" cards are widely used but have significant security vulnerabilities. These chip-based contactless cards have been targeted by various attacks over the years and remain vulnerable despite the introduction of updated versions.

In 2020, Shanghai Fudan released a new variant that provides a compatible (and likely cheaper) RFID technology through the Mifare-compatible FM11RF08S chip. It featured several countermeasures designed to thwart known card-only attacks, but introduced its own security issues.

Quarkslab analyst Philippe Teuwen discovered an attack capable of cracking FM11RF08S "sector keys" within a few minutes, but only if a specific key is reused across at least three sectors or three cards.



Armed with this new knowledge, the researcher made a subsequent, puzzling discovery: the FM11RF08S cards contain a hardware backdoor that allows certain authentication through an unknown key. He ultimately cracked this secret key and discovered that it was used by all existing FM11RF08S cards.

Furthermore, the previous generation of Mifare-compatible cards (FM11RF08) had a similar backdoor protected by another secret key. After cracking this second key, Teuwen found that it was common to all FM11RF08 cards and even to "official"

Mifare cards manufactured by NXP and Infineon.

The newly discovered FM11RF08S backdoor could enable an attacker to compromise all user-defined keys by simply accessing the card for a few minutes, Teuwen said. Customers should be aware that RFID cards based on FM11RF08 and FM11RF08S chips are also used outside the Chinese market, with numerous hotels in the US, Europe, and India employing this significantly insecure technology.

"It is important to remember that the MIFARE Classic protocol is intrinsically broken, regardless of the card," Teuwen said.

Recovering the keys will always be possible if an attacker has access to the corresponding reader. More robust (and hopefully backdoor-free) alternatives for RFID-based security are already available on the market.

Serving tech enthusiasts for over 25 years.
TechSpot means tech analysis and advice you can trust.