Quarkslab engineer discovers a security backdoor in contactless cards from a Chinese manufacturer

PARIS, August 19th, 2024. Quarkslab, an innovative French company focusing on offensive and defensive cybersecurity, announced today the discovery of a security backdoor present in millions of contactless cards from Shanghai Fudan Microelectronics Group Co. Ltd. (https://www.fm-chips.com/), a leading chip manufacturer in China. The affected cards are widely used in public transportation and the hospitality industry globally.

MIFARE* is well-known brand for a wide range of contactless IC products, produced and licensed by NXP Semiconductors N.V. (NASDAQ: NXPI). The MIFARE contactless ICs have a typical read/write distance of 10 cm and are used in more than 750 cities, in over 50 countries, and in more than 40 different applications worldwide, including contactless payments, transport ticketing and access control. The product line has been tremendously successful, with more than 12 billion contactless and dual interface sold according to the vendor. By 2010 more than 3.7 billion cards had been manufactured and deployed worldwide.

According to NXP in 2019, at its 25th anniversary, more than 1.2 billion people in over 750 cities worldwide used MIFARE products on a daily basis

The MIFARE Classic* card family, originally launched in 1994 by Philips Semiconductors (now NXP Semiconductors), are widely used and have been subjected to numerous attacks over the years. Security vulnerabilities that allow "card-only" attacks (attacks that require access to a card but not the corresponding card reader) are of particular concern as they may enable attackers to clone cards, or to read and alter their content, just by having physical proximity to them for a few minutes. Over the years, new versions of the MIFARE Classic* family have addressed the different types of attacks discovered by security researchers.

In 2020, the FM11RF08S, a new variant of MIFARE Classic*, was released by Shanghai Fudan Microelectronics, the leading Chinese manufacturer of unlicensed "MIFARE compatible" chips. This variant features specific countermeasures designed to thwart all known card-only attacks and is gradually gaining market share worldwide. Many organisations are using these cards without knowing they are as they are labelled MIFARE.

While conducting some security research experiments, Philippe Teuwen, Security Researcher at Quarkslab, identified some interesting idiosyncrasies of the FM11RF08S cards. Firstly, he discovered an attack capable of cracking FM11RF08S keys in a few minutes if they are being reused across at least three sectors or three cards. Further research revealed a hardware backdoor that allows authentication with an unknown key. He then used the new attack to obtain ("crack") that secret key and found it to be

common to all existing FM11RF08S cards. With the knowledge of the backdoor and its key, he devised a method to crack all the keys of a FM11RF08S, in about 15 minutes if all the 32 keys are diversified, much less if only a few keys are defined. Then he found a similar backdoor, protected with another key, in the previous card generation (FM11RF08). After this second secret key was also cracked it was discovered that the key is common to all FM11RF08 cards, as well as other models from the same vendor (FM11RF32, FM1208-10), and even some old cards from NXP Semiconductors N.V. (NASDAQ: NXPI) and Infineon Technologies AG (FSE: IFX / OTCQX: IFNNY).

"Near Field Communications technologies are widely deployed worldwide and have a multitude of uses these days. They are the cornerstone of some critical applications such as public transportation, personal identification, physical access control and payment systems, and they are pervasive in the hospitality industry. But even mature technologies that have been studied for decades and had their security improved over time can be subject to attack or manipulation by different types of threat actors" said Fred Raynal, Quarkslab CEO. "Philippe's discovery reaffirms the need for organizations to perform regular thorough security audits of the contactless technologies they employ. The need is particularly acute for organizations with complex supply chains where supply chain attacks may be a serious concern in their threat model"

Although without prior access to an affected card, the backdoor requires just a few minutes of physical proximity to the card to conduct an attack, an entity in a position to carry out a supply chain attack could execute such attacks instantaneously at scale.

Quarkslab published a summary of the findings in the company's blog**final URL to be provided**. The new attack and all associated discoveries were revealed in a research paper published last Friday, August 16th. on the Cryptology ePrint Archive of the International Association for Cryptologic Research (IACR).
The associated tools have been merged in the Proxmark3 open-source project, allowing potentially affected users to test their cards.

About Quarkslab

- All trademarks, trade names, or logos mentioned or used are the property of their respective owners. Every effort has been made to properly capitalize, punctuate, identify and attribute trademarks and trade names to their respective owners.