BUSINESS - OFFICIAL

4th Nov 2021

Author: ThothTrust Private Limited

The Path Of NFC Stickers

The use of wireless tagging have been around us since 1973 when Mario Cardullo's[1,2,3] 16-bit memory transponder was awarded was granted a patent for Radio Frequency (RF) and another patent was awarded to Charles Walton[1] in 1983 which becomes what we commonly know as RFID technology.

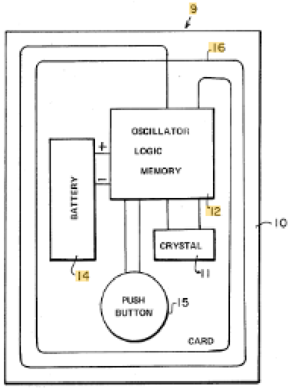


FIG. 1.

NFC technology is a branch of RFID technology that allows contactless transfer of data over a short distance of an average of 4 cm in distance using the 13.56 MHz frequency channel with an ISO standard for the NFC technology known as the ISO-14443.

It has been used in commercial, entertainment and industrial applications ranging from banking cards for contactless payments to NFC tracking tags and stickers for shipment tracking, quality control during product manufacturing, product attestation and also for bootstraping[4] other connections to aid initial setup of other devices or perform.

Different NFC stickers contain different NFC capable microchips inside them that comes with a wide variety of communication protocol and application protocols as well as security from logical and physical tampering and modification.

Security for NFC was mostly an after-thought and security features like encryption and access control parameters for protecting different memory region with passwords are bolted on as needed.

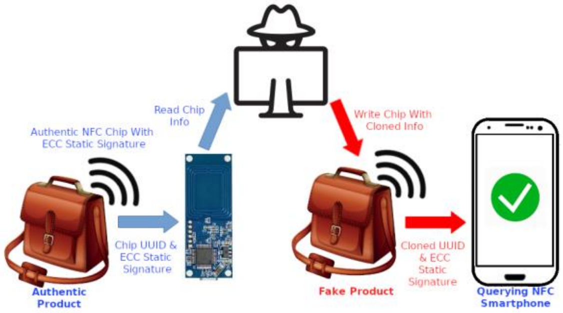
Most NFC tags and stickers do not encrypt communication using standardized strong encryption and message authentication algorithms like the Advanced Encryption Standard (AES) and other NIST standardized Message Authentication Codes.

NXP Semiconductors (NXP) initially created a proprietary Crypto-1 encryption algorithm which was quickly broken by researchers in 2008 from Radboud University Nijmegen[5,6,7,8,9] and NXP attempted to sue the university to prevent the cryptographic flaws from being published in an academic paper.

Reasons given for not including strong cryptography and security may range from the lack of silicon real estate to embed crypto-accelerators inside the tiny NFC chips as well as the amount of power that these cryptographic algorithms would have to draw to power the NFC chip which makes operation slower.

As more security related information are being embedded into NFC chips and more NFC chips are being purposed for security related operations in many business areas including transit ticket, business transactions, industrial process tracking as well as attestation to genuine products, security is now an important issue that was not addressed since inception.

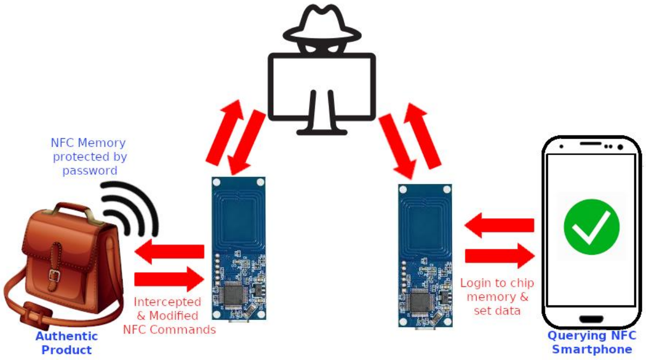
The ECC based originality signature or ECC based digital signature schemes[10] employed by many NFC chips utilizes a one-time digitally signed certificate during manufacturing or personalization of the chip. Essentially, this is a static signature programmed into the chip digitally signed over the UUID issued to the chip and whenever authentication of the chip's provenance is required, this same digital signature and certificate is repeatedly sent over the contactless interface to the querying device.


Read Chip Info
Authentic NFC Chip With ECC Static Signature
Write Chip With Cloned Info
Chip UUID & ECC Static Signature
Cloned UUID & ECC Static Signature
Authentic Product
Fake Product
Querying NFC Smartphone

Static digital signatures are known to be easily susceptible to replay attacks where an attacker positioned between the NFC chip and the querying device could copy and replay the same digital signatures and data packets which makes deploying static digital signatures a huge risk as these replay attacks may occur at any point in time and at any location.

Most NFC stickers and tags do not encrypt communication between chip and querying device or use proprietary algorithms to secure their communications. This presents a security risk where these information could be leaked with little effort by attackers by scanning them with an NFC reader. Attempts to roll out custom cryptography that have not been well studied can also be dangerous as have been seen from NXP's Crypto-1. The good news is some of the most recent NFC tags now feature AES-128 encryption for certain higher end product families.

Access control to memory regions of the NFC chip utilizing passwords may not be secure if a method to establish an encrypted and authenticated session between the chip and the querying device cannot be executed. Plain passwords or the use of proprietary obfuscation of password on NFC memory region without proper communication security poses a risk where data sniffing and bruteforcing passwords to NFC tag memory region can occur over the air.


NFC Memory protected by password
Intercepted & Modified NFC Commands
Login to chip memory & set data
Authentic Product
Querying NFC Smartphone

The latest TAGthenticate NFC sticker brings to the market a totally different game. The TAGthenticate NFC stickers has an Infineon security chip as the NFC chip with a full fledge JavaCard Operating System certified to Common Criteria EAL 6+ security certification.

Customers and developers get the same high-grade JavaCard security as any banking card or ID card with support of AES-256, ECC-521 and RSA-2048. RSA-4096 can be included upon customer request during bulk order. The ICAO eMRTD PACE-GM key exchange is also supported to allow secure channel establishment between chip and querying device out of the box.

As TAGthenticate NFC sticker is a fully fledged Common Criteria certified JavaCard NFC module in a slim and tiny form factor no more than 350 µm thick (bare module), no security is compromised for your business and industrial applications. Simple or complex logic with huge memory (> 200 KB) is available for large information storage in a secure environment.

Strong security via utilizing the strong cryptographic algorithms existing in the JavaCard environment to securely establish connections, attesting product provenance and performing secure authentication and access control to protected information in the chip. Customers can program the TAGthenticate NFC sticker like any commercial JavaCard solution in-house or use existing JavaCard solutions.

TAGthenticate NFC stickers is a culmination of all the positive attributes one wishes for easy and secure contactless access to information and transactions in a tiny, slim and portable form factor.

References:

[1] RFID World. The History of RFID Technology – Looking Back at Its First Patents. [Online]. Available: https://rfidworld.ca/the-history-of-rfid-technology-looking-back-at-its-first-patents/1543

[2] M. Spivey. (2015, Dec.) Who is Mario W. Cardullo? [Online]. Available: https://gatewayrfidstore.com/who-is-mario-w-cardullo/

[3] M. Cardullo., W. Parks. (1973). Transponder apparatus and system (U.S. Patent No. 3,713,148). U.S. Patent and Trademark Office. https://patents.google.com/patent/US3713148A/en

[4] NFC Forum. (2014, July.) NFC And Bluetooth: The Perfect Pair. [Online]. Available: https://nfc-forum.org/nfc-and-bluetooth-the-perfect-pair/

[5] M. Almeida, "Hacking Mifare Classic Cards", in BlackHat Regional Submit Sao Paulo, 2014. [Online]. Available: https://www.blackhat.com/docs/sp-14/materials/arsenal/sp-14-Almeida-Hacking-MIFARE-Classic-Cards-Slides.pdf

[6] F. D. Garcia, "Dismantling MIFARE Classic", in ESORICS, 2008. [Online]. Available: http://www.cs.ru.nl/~flaviog/publications/Talk.Mifare.pdf

[7] EE Times. (2008, July.) NXP to sue researchers over Mifare chip 'hack'. [Online]. Available: https://www.eetimes.com/nxp-to-sue-researchers-over-mifare-chip-hack/

[8] MIFARE. (2015, Oct.) Security Statement on Crypto1 Implementations. [Online]. Available: https://www.mifare.net/en/products/chip-card-ics/mifare-classic/security-statement-on-crypto1-implementations/

[9] Radhoud University Nijmegen. (2008, Mar.) PRESS RELEASE: Security Flaw in Mifare Classic. [Online]. Available: https://www.ru.nl/dis/removed-during-reorganisation/research/rfid/press_release/

[10] NXP Semiconductors. (2018, Feb.) Knowledge Base: NFC for consumables and accessories. [Online]. Available: https://community.nxp.com/t5/NXP-Designs-Knowledge-Base/NFC-for-consumables-and-accessories/ta-p/1109230