Credit Card Giant Trusts Arxan to Secure HCE Enabled Mobile Payment

One of the credit card giants is embarking on the journey to endorse new mobile payment technology with support for Host Card Emulation (HCE) that will enable them to bypass the hardware-based mobile payment system. Their engineering team has developed a Software Development Kit (SDK) to support clients who wish to develop their own mobile payment application.

Prior to HCE, payment credentials needed to be stored in a highly restricted part of the smartphone controlled by mobile carriers, the Secure Element (SE). Carriers have long been the gate- keepers for who and what get access to a phone's secure element and have typically charged fees for accessing it. Now, with HCE, phones can still conduct mobile payments without carrier's control and constraints.

Challenge: HCE will allow a smartcard to be emulated on the mobile phone without using an SE, which introduced following key security risks that were not present in SE-based NFC services:

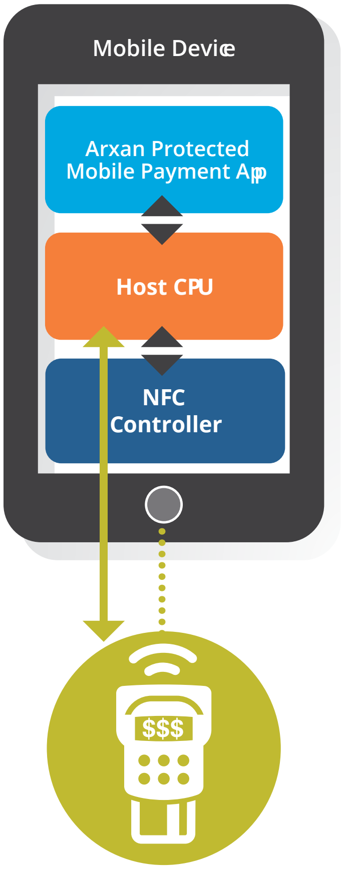
- Attacker could gain access to sensitive information such as payment credentials and cardholder information
- Malware applications could attack the OS and exploit the device and mobile payment app
- Malicious user could gain access to information stored within the mobile payment application and use it to make fraudulent payments

> Arxan's solution provided the risk mitigation techniques and software-based security mechanisms that compensate for the lack of hardware-based security inherent in HCE-based NFC applications.

Solution: In order to mitigate the key security risks inherent to HCE, Arxan offered a comprehensive application protection solution:

1. Robust Arxan Cryptographic Key/Data Protection to protect sensitive cardholder and payment information

2. Automated Arxan Code Protection comprised of unique patented guarding technology to protect the confidentiality of the application and combat applicatio tampering by:
   - **Defending** applications against compromise
   - **Detecting** attacks at run-time
   - **Detering** attacks with self-repair, custom responses, and/or alerts



Results: Arxan's solution provided the risk mitigation techniques and software-based security mechanisms that compensate for the lack of hardware-based security inherent to HCE-based NFC applications. It provided comprehensive application protection, safeguarding the integrity and confidentiality of both the application and cryptographic keys.

Arxan's state-of-the-art Cryptography Key/Data Protection solution ensured the keys are never present either in the static form or in runtime memory.

Arxan Code Protection solution "hardened" the application, making it extremely difficult for an attacker to gain access to the source code and all of the security control or modify the behavior of the application at run-time.

About Arxan Technologies

Arxan is the trusted global leader of Application Attack Prevention and Self-Protection products for Internet of Things (IoT), Mobile, Desktop, and other applications. We help protect our customers against financial loss, brand damage, fraud, IP theft, stolen credentials, fraudulent transactions, unauthorized access, non-compliance with regulatory and industry standards, and more. Our unique patented guarding technology **1. Defends** applications against attacks, **2. Detects** at run-time when an attack is being attempted, and **3. Deters** attacks to stop hackers, send alerts, or repair making customers' applications truly resilient. We are currently protecting applications running on more than 500 million devices across a range of industries, including: financial services, automotive (connected automobiles), healthcare (connected medical devices), digital media, gaming, high tech/independent software vendors (ISVs), and others. The company's headquarters and engineering operations are based in the United States with global offices in EMEA and APAC. **Learn more at www.arxan.com.**