riscure

Tap on Phone

Security implications of accepting transactions on smartphones

One of the most exciting innovations in the payment chain for retailers today is the potential of utilizing smartphones for Point-of-Sale terminals, also referred to as mobile PoS (mPoS). What originally started as a complex process, particularly with the chip card migration in the United States, has quickly become a huge opportunity for organizations and individuals alike.

In this whitepaper we explore the rise of smartphones being used as mPoS terminals as well as the relevant technologies, standards, and security challenges that must be faced as a result.

inforequest@riscure.com www.riscure.com

Introduction

The financial sector is rapidly adopting new technologies, both increasing market access and revolutionizing consumer options. A big development in the past few years is the ability for customers to use their smartphone for payments on Point-of-Sale (PoS) terminals, providing convenience and ease-of-use.

The next evolution of this type of technology is proving to be the use of Commercial Off-The-Shelf (COTS) smartphones, where a merchant's smartphone accepts payment directly from the card, completely eliminating the need of a PoS device and further increasing flexibility for customers and businesses.

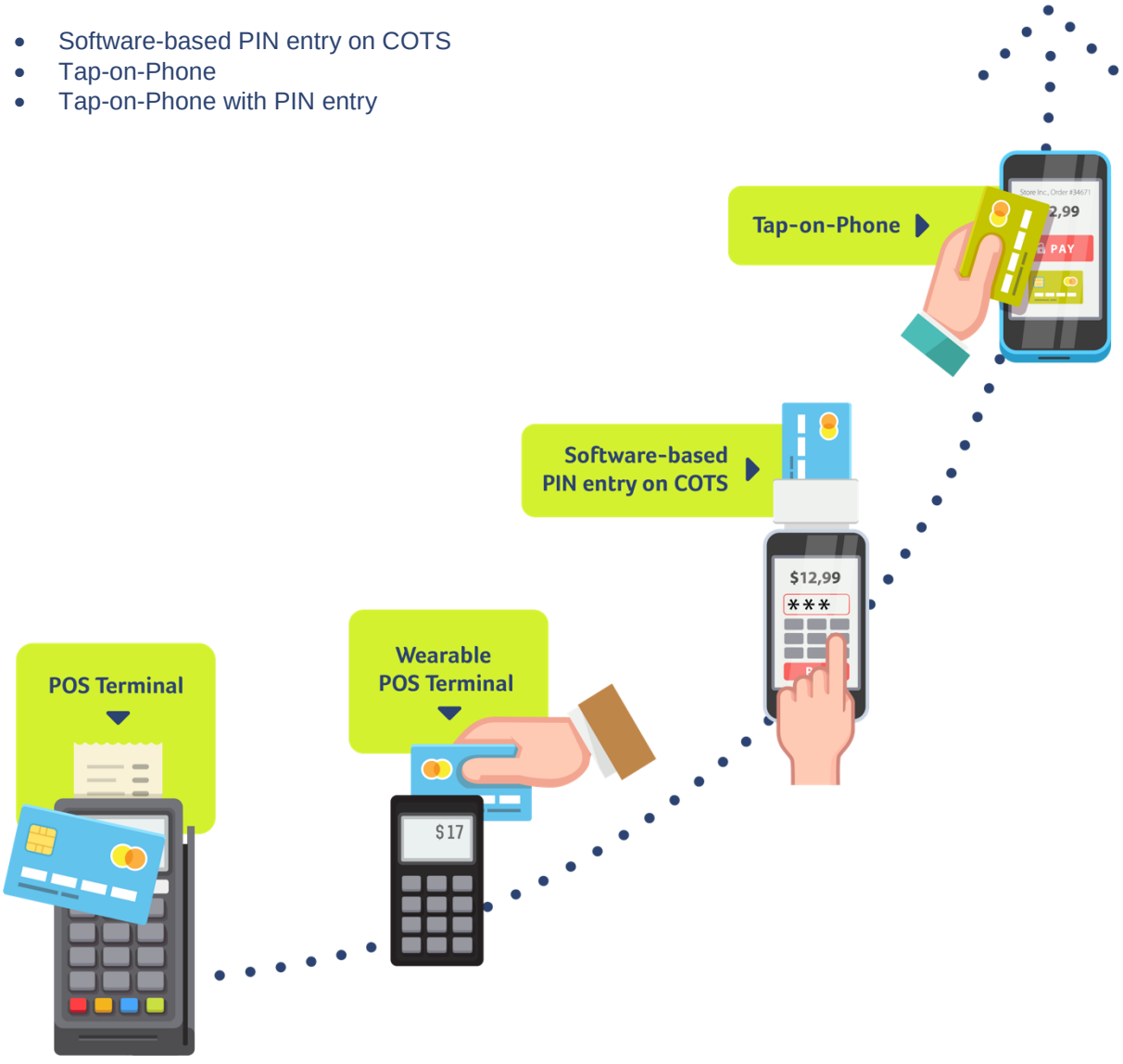
These off-the-shelf devices have already upended the industry, giving consumers a new way of making payments and giving merchants an easy way to meet demand. With the prospect of saving money and increasing customer satisfaction on the line, the next question for businesses is: how to keep this smartphone technology secure?

How COTS Smartphone Payments Work

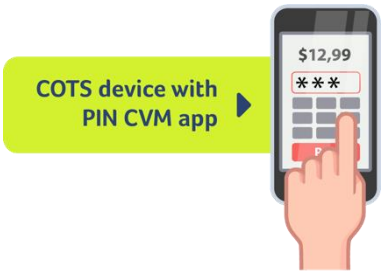
Using smartphones to perform payments is nothing new. Host Card Emulation technology, the ability for phones to perform a payment transaction on an approved PoS device, has been around for years, proving successful for both merchants and customers. What *has* changed over the years, however, is the type of solutions available, in order to accept these payments.

There are three new types of solutions in which smartphones can be used for payments:

- Software-based PIN entry on COTS
- Tap-on-Phone
- Tap-on-Phone with PIN entry



Software-based PIN entry on COTS (SPoC)



With this technology, an external dongle is the main component, connected to the COTS smartphone over Bluetooth or USB. The external dongle acts as a secure card reader with the ability to encrypt the PIN and communicate it securely to the backend for PIN verification. This design is covered by the PCI Software-based PIN entry on COTS (SPoC[1]) program (Payment Card Industry (PCI SSC), 2018).

The Secure Card Reader is an independent hardware module that ensures unprotected card data is never accessible by the COTS smartphone. However, the COTS smartphone does process the PIN, which can lead to new security challenges.

Tap-on-Phone

A further simplified revision removes the need for the external dongle: Tap-on-Phone solutions. This architecture takes advantage of the Near Field Communication (technology that allows devices to exchange information simply by placing them next to one another) interface available on most modern COTS smartphones and accepts contactless payments without the need for a card reader.

This solution is highly beneficial for those supporting low value transactions, below the applicable Cardholder Verification Method limit, as it does not require a PIN to be entered. Note that this limit differs per country, but typically varies between €25 and €50 in most European countries to $100 (AUD) in Australia and £30 in the United Kingdom.

The main benefit of such solutions results from the simplified design, the departure from PIN entry requirements and consequent needs to secure PIN data. However, this also introduces the disadvantage that only low-value transactions can be accepted.

Tap-on-Phone with PIN entry

The last technology combines the PIN entry security with the Tap-on-Phone contactless ability. This architecture brings together the benefits from both as it enables contactless payments above the CVM limit to be accepted without the need for an external dongle. However, the security needs for such type of solutions are also most challenging.

[1] During the security requirement definition phase by PCI for SPoC, Riscure contributed as a thought leader and mobile security expert.

Benefits of Smartphones for Accepting Payments

Although security may be a big concern, the advantages of utilizing COTS smartphones for accepting payments far outweigh the negatives. Some of the benefits include:

Convenience for the merchant

- The biggest advantage of accepting mobile payments on smartphones is the convenience for consumers and merchants. By using smartphones businesses not only speed up the entire checkout process, such solutions are also more flexible and easier to update.

Integration of loyalty programs

- Smartphone based mPoS solutions provide a much easier way to integrate loyalty and reward programs. This gives merchants an easy way to offer rewards points and coupons to customers during each transaction that they make.

Reduces expenses

- Acceptance devices based on COTS smartphone technology are considered lower cost compared to traditional PoS devices, making them more affordable for micro- and smaller merchants.

Access to data

- Another benefit of Tap-on-Phone technology is that it provides valuable customer data, such as how often they shop at the store, how much they spend, etc. in which merchants can take immediate action. All of this information can be used in marketing strategies, including targeting customers based on shopping patterns and demands.

Security Concerns with mPoS Technology

Although mPoS technology has great potential, security is crucial for its commercial success. Insecure technologies can not only compromise systems, but they can also damage consumers' trust and destroy companies' reputations.

While traditional PoS terminals are dedicated devices, designed and built to accept and process transactions according to necessary security requirements[2], securing COTS smartphones becomes more difficult as they are not typically created with security as their main purpose nor do they consider the applicable security requirements. As mPoS becomes more mainstream, it is vital for solution developers and other stakeholders to recognize the security challenges associated with it in order to choose the correct solution(s) to mitigate these risks and develop sufficiently secure solutions.

Security threats for existing NFC Technology

Contactless payment through NFC-enabled payment cards and terminals has become increasingly common in the past years, with adoption rates in many countries of 50% and above in 2017 and 2018 for all card-based payments [4].

---

[2] Widely recognized standards are for example the PCI PTS requirements and certification of traditional PoS terminals.

Despite the convenience and ease-of-use, there are still security threats on the NFC technology embedded in such contactless payment cards. Several security research publications are available describing amongst others:

- Skimming
  - Credit card data is captured by a portable NFC reader, which could later be used to facilitate fraudulent payment transactions.
- Relay attacks
  - Real credit card information is intercepted during communication and is forwarded to a 'dummy credit card' which connects with a legitimate terminal performing the transaction.
- Unauthorized transactions
  - Transactions are initiated without the cardholder being aware as a result of the contactless nature.

The relevance of the NFC related threats mentioned above, is that they also manifest within Tap-on-Phone solutions. This means that part of the security threats related to Tap-on-Phone, are not new as they are inherent to the NFC technology embedded in payment cards. However, the scale and feasibility of such attacks can change (increase) due to the adoption of Tap-on-Phone technology.

Security Threats for Tap-on-Phone Solutions

The threat model for Tap-on-Phone solutions is extended from traditional mobile payment solutions that use mobile wallets. When the merchant is considered malicious, additional attack vectors become possible due to physical access to the COTS smartphone. Undetectable modifications can be performed to the device, aiding the installation of malware. Main threats considered relevant for Tap-on-Phone solutions include:

- Fake Payments
- Unauthorized transactions
- Refund attacks
- Collect card data
- Block merchant account
- Relay attacks

Fake payment
In this scenario, transactions from certain cards, or users, are intentionally ignored by the Tap-on-Phone solution. The Tap-on-Phone application will show normal behaviour but refrain from processing the transaction(s) as the transaction is never communicated to the backend. To the merchant, this will look like shoplifting, as it will not leave any trace in the system.

Unauthorized (unintentional) transactions
While the credit card is in proximity of the Tap-on-Phone solution, additional transactions are executed next to the legitimate transaction. These unauthorized transactions can be processed directly or later, essentially 'cloning' the card for a limited period of time.

Refund attack
An attacker with control of the Tap-on-Phone application can generate refund transactions. This can be exploited when acquiring goods at the merchants and then generating a refund remotely.

Collect card data
Data transmitted over the NFC interface between the card and the mobile handset can be intercepted by malware on the phone. This data includes the PAN, expiry data, service code and discretionary data. Such data facilitates attackers to perform Card Not Present Fraud (CNPF). While the CVV/CVC cannot be recovered by the handset, this data could easily be obtained by visual inspection.

Block merchant account
An attacker in control of a Tap-on-Phone solution can generate several fake payments, change transactions amounts and perform additional transactions, such that the merchant account is detected as malicious by the backend. As a result, the merchant account can be blocked. Although the attacker does not profit directly from this attack, the ability of the merchant to do business is affected and their reputation can be damaged.

Relay attacks
In relay attacks, a compromised Tap-on-Phone solution is used to relay messages between a legitimate mPoS terminal and a customer through a 'mule' present at the legitimate mPoS terminal, which can lead to several attacks. The most likely scenario is where a legitimate cardholder is unknowingly paying for the transaction performed by the 'mule'. The payment in the compromised Tap-on-Phone and non-compromised mPoS needs to happen at the same time to account for the unpredictable number provided by the uncompromised PoS.

Security threats are an issue regardless of the type of technology used, but it is vital that the benefits outweigh the risks for both consumers and merchants. As Tap-on-Phone solutions are just being introduced to the market, the security of such solutions is prone to develop further in the time to come as security standards, security technologies but also attacker capabilities evolve.

Current Security Standards

Although this new technology faces security challenges, there are already best practices available to ensure businesses and customers stay safe.

Responding to the growing popularity of Tap-on-Phone solutions, the Payments Card Industry Security Standards Council (PCI SSC) has developed standards that address concerns from across industries regarding both software-based PIN entry and contactless solutions, both on merchants' COTS devices. [5] [6] These requirements cover solutions that require external SCRP dongles approved by PCI. The documentation consists of six modules, which address different aspects of mPoS acceptance such as CVM method, remote attestation, back-end systems, and the external card reader.

Both Visa and MasterCard have also recently released their own security standards. Visa published their Tap-to-Phone security requirements [10] in 2018 in order to manage the risks associated with payment acceptance on COTS devices. The program is mandatory and Visa lists functional and security requirements for both the mobile application and the supporting NFC hardware.

The security requirements address various topics for the Tap-on-Phone solution, including cryptography, secure storage of the keys, replay resistance, and protection of the application against unauthorized modifications. The security requirements also specify security features protecting the mobile application that have to be implemented and evaluated, such as anti-rooting and anti-tampering, code obfuscation, and attestation. As of October 2018, Visa has introduced the option for solution developers to include PIN Capture in the Tap-on-Phone solution.

Mastercard has developed a similar guide for enabling acceptance on mobile COTS devices [1][2][3]. Like Visa, Mastercard provides security requirements for Tap-on-Phone solutions, with the main difference being that Mastercard, at the moment of writing this whitepaper, does not support PIN entry for Tap-on-Phone solutions.

Securing Tap-on-Phone Solutions

Properly securing a Tap-on-Phone solution is not a straightforward task and requires a good understanding of PoS technology and mobile security technology. For Tap-on-Phone solutions providers, this means staying educated on the most updated options and utilizing outside security providers if necessary. Some current options for Tap-on-Phone security solutions include:

- Software-based security countermeasures
- Trusted Execution Environment
- Secure Element

Software-based security countermeasures

Even on an open platform like Android, where untrusted apps can be loaded and the operating system can be rooted, it is possible to protect applications against eavesdropping or manipulation by Malware. Several security mechanisms are available, often complementary to each other. Layered security relying on multiple countermeasures can significantly increase the effort and skills required by an attacker to develop a successful attack. Examples of these security mechanisms include:

- Anti-analysis
- Anti-rooting
- Anti-instrumentation
- Anti-cloning
- Anti-key-recovery

These security mechanisms are described in more detail in our whitepaper on Cloud-Based Payment app security [8].

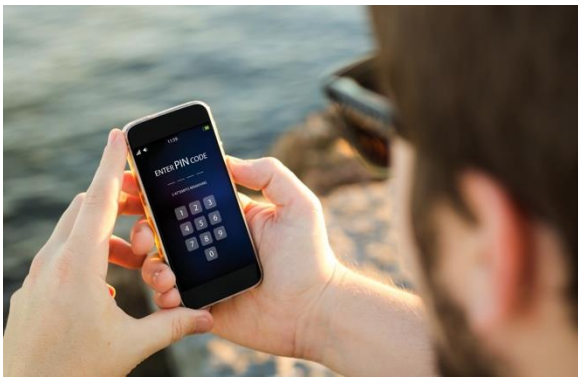
The main advantages of such software-based security countermeasures include that the same solution is applicable to a large number of devices as there is no dependency on the underlying platform and smartphone vendor. Secondly, the developer has full control over the update process of the solution.

Trusted Execution Environment

Most modern smartphones are equipped with a so-called Trusted Execution Environment (TEE), which is part of the smartphone platform and essentially offers hardware support for software security. The TEE is an isolated execution environment to the Android environment and hosts isolated Trusted Applications.

A well-known example of this type of environment is a feature on smartphones that locks down the touchscreen at the moment the user enters his PIN code. This prevents attackers having root access in Android from eavesdropping and is relevant for Tap-on-Phone solution developers aiming to integrate PIN entry for higher value transactions.

The main advantage of the TEE is its logical and physical separation from the Android environment. Since this is a platform feature, there is a dependency on the underlying platform for the solution developer, potentially limiting the smartphone devices or device models on which the solution can be deployed. Secondly, the update cycle of the underlying platform is out of control of the Tap-on-Phone solution developer, as the smartphone manufacturer manages this.



Secure Element

Secure Elements (SE) often come embedded in smartphones or integrated in the mobile System-On-Chip (SoC) of the smartphone. Such Secure Elements provide a security robust environment for processing transactions; the security level is equivalent to modern Smart Cards. Similar to TEE, the SE is part of the smartphone platform and as such introduces a dependency on the specific handset(s). This dependency can complicate the introduction of a payment service, as collaboration between the solution developer and handset vendor is needed. Therefore this solution is less popular or feasible.

Conclusion and next steps

While the use of smartphones for making payments is commonly accepted, using smartphones as PoS terminals is a disrupting technology in the Point-of-Sale terminal ecosystem that will only continue to gain traction in the coming years.

With any new technology comes the potential for new risks, cyber attackers already finding unique opportunities to compromise systems and steal sensitive information enabling financial fraud. Even though there are security options currently available for Tap-on-Phone solutions, these often include complex software-based countermeasures and require a proper design, integration and configuration in order to result in a secure solution.

For most solution developers, merchants and businesses interested in developing and adopting Tap-on-Phone payment solutions, the best way to ensure security of the system and data is to utilize the expertise of independent third-party security experts who specializes in this innovative mobile technology.

How Riscure Can Help

Riscure is an international security laboratory, well recognized and respected for its Mobile Security expertise. Riscure is recognized by many certification schemes and payment networks, including Visa, Mastercard, Discover, American Express, EMVco and others, to perform security assessments of a wide variety of mobile payment and acceptance solutions.

Working with all involved stakeholders, from final solution developers and mobile security solution providers, to smartphone and mobile Operating Systems vendors, Riscure is perfectly positioned to support its clients and partners in their secure development and solution certification process.

Riscure offers a broad, efficient and flexible offering for solution developers aiming to secure and certify their solutions. With our services and expertise, we actively support our customers on each stage of their solution development process in order to reduce risks of reputational damage, delayed time-to-market and security certification costs.

Our security services for the mobile financial industry include:

Tap-on-Phone Security
Cloud-Based Mobile Payment Security
Payment solutions for Smartphone OEMs
Mobile (biometric) Identity and Authentication
Mobile Banking Security

Interested to learn more about our offering and how to secure of your own Mobile solution?
Visit our website at www.riscure.com or contact us at: inforequest@riscure.com.

Works Cited

[1] MasterCard. (2016). *Mastercard best practices for mobile point of sale acceptance.*

[2] MasterCard DigiSec Lab. (2017). *Embedded Contactless Secure Reading for MPOS Pilots Programs Draft Security Principles v1.0.5.* Mastercard.

[3] Mastercard. (June 2018). *Tap on Phone Pilot Approval v1.1a.* Mastercard.

[4] Nederland, B. (n.d.). *Annual Report 2017.*

[5] Payment Card Industry (PCI SSC). (2018). *Software-based PIN entry on COTS - Security requirements V1.0 .*

[6] Payment Card Industry (PCI SSC). (2018). *Software-based PIN Entry on COTS - Test requirements v1.0.*

[7] PYMNTS.com. (n.d.). *Visa: Why The US Is Finally Ready For Contactless*. Retrieved from https://www.pymnts.com/visa/2018/contactless-cards-payments-mobile-wallet-pos-emv-apple-pay/

[8] Riscure. (2018). *Analyzing the security of Cloud-Based Payment apps on Android.*

[9] Riscure. (2018). *Mobile Banking application security - Learning from the HCE security experience to improve security of mobile banking applications.*

[10] Visa. (October 2018). *Visa Ready Program for mPOS: Visa Ready Tap to Phone Solution Requirements - with Optional PIN Capture v1.1.*

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90
www.riscure.com

Riscure North America
550 Kearny St., Suite 330
San Francisco, CA 94108 USA
Phone: +1 650 646 99 79
inforequest@riscure.com

Riscure China
Room 2030-31, No. 989,
Changle Road, Shanghai 200031
China
Phone: +86 21 5117 5435
inforcn@riscure.com