Mobile Banking application security

Learning from the HCE security experience to improve security of mobile banking applications
## Contents

1. **Introduction** ................................................................................................................. 3  
   1.1 What are Mobile Banking applications? ................................................................... 3  
   1.2 What are the mobile banking security challenges? .............................................. 3  
   1.3 What can Riscure do for you? ............................................................................. 3  

2. **Recurring attacks and security challenges** ................................................................. 5  

3. **Protection mechanisms and implementation challenges** ........................................ 6  
   3.1 Business implication of lack of countermeasures or bad implementation .......... 7  

4. How does HCE Mobile Payment knowledge relate to Mobile Banking, Mobile Payment in transportation and Mobile Acquiring (mPOS)? ................................................................. 7  

5. **References** .................................................................................................................. 9
1 Introduction

In this paper we present the critical security challenges that Mobile Banking applications face in today’s market. Additionally, we summarize our experience when evaluating both HCE Mobile Payment and Mobile Banking applications, and present evidence that certain HCE security approaches are worth embracing in Mobile Banking application development.

1.1 What are Mobile Banking applications?

Modern payment and banking solutions running on ubiquitous mobile devices and smartphones have seen a vast growth over the past years. They enable customers to perform daily banking activities, perform transactions and administrative tasks in an efficient, quick, and seamless manner.

1.2 What are the mobile banking security challenges?

Despite the increase in usability that these solutions provide, several challenges arise from an information security point of view.

First, banking solutions are applications running on mobile devices. Applications do not typically run in confined secure environments; instead, they share resources with other (potentially malicious) applications. This feature often enables attackers to manipulate the banking application’s stored data, banking infrastructure and banking activities.

Second, these applications must implement Strong Customer Authentication (referred to as SCA by regulatory bodies in the EU). SCA is achieved through two-factor authentication (2FA) methods implemented via an additional component. The 2FA component has historically been an additional dedicated hardware device (2DA), which is being replaced either by an additional application on the mobile device (2AA), or by functionality included into the single banking application (1AA). 2AA and 1AA are considered deterioration to the security provided by 2DA solutions.

Finally, no security requirements were mandated for banking solutions until recently. This resulted in a concerning lack of security in such solutions, as demonstrated by several publications, both academic and from industry. Within the European Union, a change is expected with the adoption of the Revised Payment Services Directive (PSD2) and associated Regulatory Technical Standards (RTS), which define security regulations for mobile banking solutions.

1.3 What can Riscure do for you?

The challenges with the security of mobile banking applications we just described, show a strong resemblance to those that HCE mobile payment applications faced in the past years. In fact, mobile banking and HCE solutions can be approached similarly in terms of security technologies, solutions and best-practices.

As the leading HCE mobile payment security lab, Riscure can support banks and mobile application solution providers by:
• Help to increase the security capabilities and knowledge of both development and security teams with the design and development and security testing of mobile banking solutions through our Training Academy.
• Support the Mobile Banking application developers and banks in improving the security of their mobile solutions. Riscure provides security evaluation services such as lightweight security quick scans, penetration testing to in depth security evaluation and certification of the mobile solution.

In the next sections we elaborate on the security challenges and protections, and discuss business implications and our recommendations for the development of a secure Mobile Banking product.


2 Recurring attacks and security challenges

In the context of mobile security there are a number of recurring attacks requiring different attacker capabilities, such as:

- **Network attacks.**

  Network attacks rely on intercepting and altering the communication traffic between an application and the banking back-end services. This is possible when the application does not verify the identity (e.g. cryptographic certificates) of the services it communicates with. As a result, an attacker can modify transaction details or obtain access to client credentials.

- **Impersonation/repackaging attacks.**

  These attacks are performed by downloading the mobile application (e.g. via the application store), modifying the binary code to add malicious functionality, and redistributing it via phishing. In this scenario, an attacker aims to modify the application to send secrets to a malicious server or to display false information to the client during transactions.

- **Instrumentation attacks.**

  Instrumentation attacks require obtaining elevated privileges on the victim’s mobile device. This allows an attacker to modify the execution of the application, and thus to have complete control over its data. As a consequence, an attacker can modify transaction details on-the-fly or exfiltrate any information. Instrumentation attacks are usually a precursor to more specialized attacks, such as relay attacks.

- **Cloning attacks.**

  Cloning attacks allow an attacker to copy the relevant data from a victim device into another device under their physical possession. As a result, the attacker can impersonate the victim and perform transactions on the victim's behalf.

*These types of attacks are widely known in the security community thanks to the many available publications and in-depth research by Riscure.*

Some of them rely on the ability to obtain elevated privileges on the mobile device. The standard security mechanisms offered by mobile device platforms (e.g. Android OS) aims to ensure that applications cannot maliciously impact each other. However, subtle bugs and platform vulnerabilities (which are outside the control of mobile banking vendors) can grant elevated privileges to attackers, as reported in [1], [2], and [3]. Therefore, such a scenario is a concrete threat to all mobile applications.

From the black hat perspective, it is widely known that malicious parties are spreading Android malware [6] that uses platform vulnerabilities to attack other applications. The malware is disguised as a game or other seemingly benign applications, and distributed via the application store. When a victim opens the malicious application, it attacks the mobile device in the background without any visible effect.

Over the years, independent security researchers as well as security labs have discussed, and often demonstrated, what can be achieved when attacking HCE mobile payment solutions. The presentation “Can't Touch This: Cloning Any Android HCE Contactless Card” [4] (2017) shows that multiple HCE solutions are susceptible to cloning attacks. Riscure also describes several attacks and the required tooling, together with possible mitigations, in 2016 (see [5]).

Other publications show vulnerabilities and related attacks discovered when testing real-world solutions (spinner, appauth, apptan, n26-roots, cron, nomorp) [7][8][9][10][11][12].
All items addressed in this section equally apply to HCE mobile payment and mobile banking applications. Therefore, Riscure can leverage existing knowledge and expertise from the HCE domain and apply it directly to mobile banking solutions.

3 Protection mechanisms and implementation challenges

Mobile applications can be protected by implementing security mechanisms aimed to increase the attacker effort, for instance:

- **Anti-rooting checks.**
  Prevent the application from running on a rooted mobile device. If the mobile device is rooted, an attacker can obtain elevated privileges to attack the application.

- **Anti-emulation checks.**
  Prevent the application from running in an emulator. Emulators typically provide an attacker with information useful to understand and implement the first steps of an attack.

- **Integrity checks.**
  Verify that the binary code of the application has not been tampered with. These checks can be either static (i.e. performed over the files of the application) or dynamic (i.e. performed over the application in memory).

- **Obfuscation of the binary code.**
  A mechanism to decrease the readability of the code, which increases the efforts required by attackers to understand the business logic of the application.

- **TLS certificate pinning.**
  Protects the network communication between the mobile application and the back-end services by verifying the authenticity of the back end services before setting up a secure connection.

- **White-box cryptography.**
  Cryptographic implementation that increases the effort required by an attacker to extract cryptographic keys used by the application.

- **Trusted Execution Environment (TEE).**
  The security critical functionality is moved into a secure execution environment. This greatly increases the amount of effort required by an attacker to impact the business logic.

- **Third-party attestation platforms usage (e.g. Google SafetyNet, Samsung Knox Attestation).**
  Offers additional verification of mobile devices and its integrity.

Security mechanisms must be implemented or integrated adequately. A minor flaw in their implementations may severely impact the overall security of the mobile application. Additionally attackers are benefitting from publicly available off-the-shelf tooling which can be used to analyze and attack mobile solutions.
3.1 Business implication of lack of countermeasures or bad implementation

Based on the implemented countermeasures, the time required for an attacker to subvert the mobile application security can vary greatly. At the lowest side of the spectrum, a mobile banking application with no countermeasures can be attacked in a matter of hours. At the highest side of the spectrum, a well-protected mobile banking application requires several weeks of effort in order to mount an attack. These timeframes are based on the expertise and resources available to a highly specialized attacker or criminal organizations. However, only the identification of an attack requires this attacker profile, whereas repeating the identified attack may take just a few hours of a much less specialized attacker. This is because attacks on solutions which are not well protected can typically be implemented in a point-and-click manner and distributed on the Internet.

At the very least, the lack of security countermeasures results in a negative image to the solution vendor or bank, as was the case for the two CCC presentations about the strength of Application TANs and the shortcomings in the N26 application [10].

In order to cope with a fast moving security landscape, HCE mobile payment applications have steadily improved their approach to security. What we have witnessed as a security lab is the shift from few disparate security mitigations (e.g. non consistent obfuscation, no integrity checks) to a well-documented and implemented layered security framework. The steady growth has resulted in robust applications which can withstand targeted attacks.

4 How does HCE Mobile Payment knowledge relate to Mobile Banking, Mobile Payment in transportation and Mobile Acquiring (mPOS)?

Securing a mobile application can be done by following a similar approach, regardless of whether it is an HCE payment application, a mobile banking application, a public transport application or a mobile acceptance application (i.e. a mobile Point Of Sale). The set of best practices and security countermeasures can be applied to any mobile solution.
Indeed, the security mechanisms previously listed do not make any assumptions with regards to the use case of an application. Instead, they focus on the availability of underlying technologies (e.g. TEEs, platform specific device attestation) and generic techniques aimed to protect applications (e.g. obfuscation, integrity checks, anti-rooting checks).

Practical advice: Do not reinvent the wheel!

Typically, third-party security evaluations are common in many established markets with high security needs and standards/requirements (such as credit cards, mobile payment, passports, driver’s licenses, payment terminals, etc.).

Experienced players, usually having their own security testing teams, in such established markets have demonstrated the capability to develop secure innovative products. These players report a significant benefit from the continuous collaboration and interaction with third-party security evaluation laboratories enabling them to obtain more in-depth understanding of their attacker model, relevant threats and vulnerabilities and ways of testing security solutions.

Markets in which (1) third-party independent security evaluations, (2) proven requirements or standards, and (3) validations against these standards/requirements are not present, often reveal that the active players have limited security awareness and security maturity. These disruptors still need to build and improve the necessary capabilities to develop resilient solutions (such as IoT, medical, smart metering, automotive, etc.).

Developing secure mobile solutions is easily underestimated and in practice often proven difficult to get right.

For those looking to strengthen the security of their mobile solution(s), to reduce risk or prepare for potential new (government) regulations or enter new markets, we advice to follow the established route by benefitting from the experience of secure mobile application developers, mobile security solution providers and independent security labs. These organizations have vast and daily experience with mobile application security, security requirements and security needs in new markets, that can help you avoid costly compromises or redesigns of mobile solutions.

As an independent security lab, Riscure is active in both mature and disruptive markets (such as cards and mobile payments, content protection, smart grid, IoT, medical and automotive security). We have a proven track record supporting our clients for increasing their security development capabilities, enabling our clients to develop secure solutions and perform security evaluations to assess the robustness of their solutions against accepted standards, proprietary requirements and tailored attacker profiles.

Contact Riscure at securitieservices@riscure.com to see how we can support you to assess and improve the security of your solution(s)
5 References
