A Taxonomy of Architecture-specific Use Cases, Security Risks and Mitigations in Biometric Solutions for Mobile Devices

Thomas Stols
University of Twente
P.O. Box 217, 7500AE Enschede
The Netherlands
t.stols@student.utwente.nl

ABSTRACT
Biometric solutions for mobile devices are becoming increasingly common. As more biometric applications enter the market, it has become clear that the design choices of a mobile biometric solution could possibly influence the application’s usability and security. By analyzing survey results among experts in the field of biometrics, in this paper we provide a taxonomy of use cases, security risks and mitigations for mobile biometric solutions with different combinations of internal and external architectural components.

Keywords
Biometrics, mobile devices, architecture, use cases, security, privacy, mitigations.

1. INTRODUCTION
On mobile devices, the traditional way to protect sensitive information is by using tokens or PINs (Personal Identification Number), which are easy to implement but constantly under the risk of being stolen or forgotten. Biometrics, the unique biological or behavioral characteristics of a person, is one of the most popular and promising alternatives to solve these problems [11].

Commonly used biometric solutions are able to verify or identify a person by capturing his or her facial or iris images, scanning the fingerprints or recording the voice or speech samples. This input is then compared to a known biometric template, which results in the person being verified/identified or not. In mobile devices, using biometric tokens for authentication is attractive because the authentication process is principally based on characteristics that are unique, measurable and cannot be stolen or transferred easily [10].

1.1 The biometric process
A typical biometric solution operates in one of two modes: verification or identification. The verification mode is used solely to verify that a user’s biometric characteristic matches a specific biometric template, while the identification mode actually attempts to identify the user given one or more biometric templates. To limit the scope of this research, we will be looking at biometric solutions used for verification purposes only.

In order for the verification process to work, a user first has to follow an enrolment process, in which the user is asked to register one or more biometric characteristics. Features from this registration are extracted, a biometric reference template is composed and stored. After enrolment, the verification process can take place in which one or more biometric characteristics of the user are recorded and compared to the biometric reference template. If they match, the user is successfully verified.

1.2 Architecture
When looking at mobile devices in particular, the architecture of a biometric solution can be modelled with four components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enrolment sensor</td>
<td>The sensor component that is used for the enrolment process.</td>
</tr>
<tr>
<td>Verification sensor</td>
<td>The sensor component that is used for the verification process.</td>
</tr>
<tr>
<td>Reference storage</td>
<td>The reference storage, commonly a database of some sort, is where recorded biometric templates are stored at enrolment and retrieved at verification.</td>
</tr>
<tr>
<td>Verification algorithm</td>
<td>The verification algorithm that is used for matching. Algorithms can differ in technique (for instance using fingerprint ridge pattern correlation versus minutiae technology), score calculation and thresholds.</td>
</tr>
</tbody>
</table>

Figure 1 shows how these components are interconnected. These architectural components do not necessarily have to be in the same place. Depending on the design choices and application, sensors can be internal (as part of the end-user application or device) or external (as part of a separate application or device that communicates with an end-user application or device) and likewise, the location for verification processing and template storage could also be internal or external.

2. RESEARCH
This research focuses on finding use cases, security and privacy concerns for biometric solutions in mobile devices.
Past research shows many biometric systems are susceptible to attacks in different parts of the biometric process. For example, Apple's fingerprint identification solution (Touch ID) for the latest iPhones is easily bypassed by replicating a fingerprint on a sheet of plastic [1]. A wide range of attack vectors makes fraud one of the most pressing issues in using biometrics for authentication [14].

In addition, biometric information is considered to be sensitive information. Once a biometric identifier is captured from an individual, and even if it is captured only once, the biometric identifier could easily be replicated, copied and otherwise shared among countless public- and private-sector databases [13]. This sharing could conceivably take place without the individual’s knowledge or consent.

Based on the architecture of the biometric solution, security and privacy risks may vary. When looking at Apple's iPhone-unlocking with Touch ID for example, all components are internal; enrolment, enrolment, verification and storage are done on a single device. Naturally, the layout of these components introduces certain security risks, such as the possibility for enrolment fraud if the mobile device should ever fall into the wrong hands. For other biometric solutions where one or more components are external, different security risks may apply.

This research aims to provide an overview of use cases and security- and privacy-related risks based on the architecture of the biometric solution and proposes mitigations to combat these.

To aid in effectively categorizing architectures, each specific architecture is assigned an architecture code. The architecture code basically is a binary number where each component is represented with either a 0 (internal) or a 1 (external). The architecture code reference table (Table 1) is referred to in following sections of this paper.

2.1 Research questions

This research addresses the following research questions:

- What are the use cases for this specific architecture?
- What security issues can be identified?
- How can the identified security and privacy risks be reduced?

2.2 Research methods

2.2.1 Short literature study

To discover what security- and privacy-related risks mobile biometric solutions are exposed to, a short literature study is performed. During this literature study an inventory is made on what risks are present and what measures can be taken to mitigate these risks.

It is expected that the literature study will result in a list of possible security- and privacy-related risks and mitigations in mobile biometric solutions.

2.2.2 Survey

Experts in the field of biometrics are invited to participate in a survey that aims to gather expert opinions about use cases, security- and privacy-related risks for mobile biometric solutions. Participants are asked to think about use cases for particular design choices and the implications of these choices on security and privacy.

To determine the occupation and expertise of the respondent, respondents are asked about their occupational field and their familiarity with the field of biometrics.

After the initial questions respondents are presented with 16 pages, each containing 3 identical questions regarding a specific architecture design for a biometric solution. To limit the participation time and facilitate processing the results, suggested security- and privacy-related risks are provided to the respondent. These suggested risks are derived from the literature study. In addition, all questions have an open field where comments and suggestions are accepted.

The respondent is asked to:

- List some use cases that he/she knows or envisages.
- Identify security-related risks the particular architecture is concerned with.
- Identify privacy-related risks the particular architecture is concerned with.

An example survey page is depicted in Appendix A.
The survey is sent via e-mail to subscribers of the European Association for Biometrics\(^1\) (EAB) mailing list. In addition, the survey is sent to employees of the SCS group\(^2\) (Services Cyber security and public Safety) of the University of Twente.

The survey is aimed at taking around 20 minutes to complete and it is expected that a minimum of 20 experts will participate. The results of the survey are analyzed and combined to form a complete overview of use cases with their related security and privacy implications.

3. RELATED WORK

Y.W. Ju et al.[4] attempt to examine security threats and countermeasures for authentication models for mobile devices. Their research heavily relies on the guidelines composed by Prof Yong-nyuo Shin et al. [9] which outlines technical and operational countermeasures for telebiometric applications using mobile devices. In the aforementioned research, authentication models are composed based on the component (Biometric sensor, Mobile device, Server) and the role that each component performs (Capturing, Reference, Comparison).

This paper will differ from the research of Y.W. Ju et al. by breaking down authentication models in architectural components and focusing on expert opinions to determine use cases and threats.

4. RESULTS

4.1 Literature study results

4.1.1 Security risks

Using biometric applications for authentication naturally introduces generic security risks like denial-of-service, circumvention, repudiation, contamination and coercion [5]. However, these generic risks are present in all authentication systems and will not be discussed further.

Regarding biometric systems in particular, Ratha et al. [8] analyzed attacks against biometric systems and grouped them into eight classes:

- Presenting a fake biometric (e.g. synthetic fingerprint, iris, face) to a sensor.
- Submitting previously intercepted biometric data (replay).
- Override the feature extractor to produce feature values selected by the attacker.
- Replace genuine features with the ones selected by the attacker.
- Modify the matcher to output an artificially high matching score.
- Attacking (e.g. adding, modifying or removing) the template database.
- Attack the transmission medium between the template database and matcher.
- Override the matcher result (accept or reject).

4.1.2 Privacy risks

The use of biometric identifiers raises privacy concerns. Breebaart et al. [2] subdivide privacy risks in biometric solutions in four categories:

Unauthorized collection

Collection of biometric samples without the subject’s knowledge, for example using hidden cameras.

Unnecessary collection

Biometrics that are employed in situations without or with little benefit from strong user verification.

Unauthorized use and disclosure

Use of biometrics for purposes other than approved by the subject, such as forensic usage, linking or cross-matching databases, monitoring an individual’s daily activity, and alike.

Function creep

Expansion of a system into areas for which it was not originally intended, for example as occurred for national identity numbers.

4.1.3 Mitigations

Generic defences that are effective against security risks can be grouped in these classes:

Presentation Attack Detection (PAD)

Using hardware-based techniques like the integration of dedicated hardware thermoscopes, pulse oximeters, blood flow and spectroscopes to detect liveness [12]. Using software-based techniques like fingerprint skin perspiration [7] and morphology characteristics [6].

Enrolment protection

Requiring a second authentication factor on enrolment to prevent enrolment fraud.

Transmission channel protection

Requiring authentication between sensor, mobile device and third-party components and encrypting transmitted data to mitigate data leaks and modification.

Biometric template protection

Satisfying the requirements of a template protection scheme [3] to mitigate template tampering. Using hardware-based protection in the form of a smard card or stand-alone biometric system-on-device. Using software-based protection (e.g. feature transformations or cryptographic systems) based on some external key; the resultant data is stored in the system database instead of the original biometric template.

Privacy risks may be reduced by:

Establishing trust

Trust, a subjective property, is a prediction or reliance on an action and its consequences, based on what a subject knows about an application or technology. Trust is needed to communicate with external parties, but has to be earned first.

Data minimization

To ensure maximum privacy, the amount of binary data associated with a biometric template should be minimized.

\(^1\)http://www.eab.org
\(^2\)http://scs.ewi.utwente.nl
Unfortunately mechanisms to minimize one risk may cause another risk to increase. If for instance a biometric system closely observes fingerprint patterns to prevent spoofing attacks, the potential risk increases for unnecessary collection or a function creep.

4.2 Survey results

A total of 26 respondents have participated in the survey. 55.6% of the respondents indicate to work as a researcher, 33.3% have a commercial occupation, while the other respondents either work in educational or other fields.

Of the respondents, 66.7% are familiar with biometric systems and their internal workings and 25.9% of the respondents are somewhat familiar with biometrics. The answers of respondents that indicate they have no knowledge of the internal workings of biometric systems are not included in the result analysis.

The results of the survey are outlined in Table 2.

<table>
<thead>
<tr>
<th>Code</th>
<th>Use cases</th>
<th>Security risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>Access control to device and applications on the device, user login, signing low-value transactions, activate a payment card.</td>
<td>Enrolment fraud, fraudulent verification (spoofing), tampering with reference storage, fraudulent matching, frustrating the system in order to get into the fallback procedure.</td>
</tr>
<tr>
<td>1000</td>
<td>Signing banking transactions, governmental authentication systems.</td>
<td>Enrolment fraud, fraudulent verification (spoofing), transmission channel attacks, tampering with reference storage, mobile device knows nothing about the enrolled individual.</td>
</tr>
<tr>
<td>1100</td>
<td>Banking applications, match-on-card applications.</td>
<td>Enrolment fraud, fraudulent matching, transmission channel attacks, tampering with reference storage.</td>
</tr>
<tr>
<td>0100</td>
<td>Application where proving device ownership under supervised conditions is required, remote speaker authentication using a mobile device.</td>
<td>Enrolment fraud, fraudulent matching, transmission channel attacks, tampering with reference storage.</td>
</tr>
<tr>
<td>0110</td>
<td>Applications where a service provider trusts its own storage more than the user device.</td>
<td>Enrolment fraud, fraudulent matching, transmission channel attacks, overriding the reference storage location, corruption of central storage may lead to identity theft or abuse.</td>
</tr>
<tr>
<td>1110</td>
<td>Match-on-card applications with external storage, grant access of a provider-owned app running on a mobile device.</td>
<td>Enrolment fraud, fraudulent matching, transmission channel attacks, overriding the reference storage location, corruption of central storage may lead to identity theft or abuse.</td>
</tr>
<tr>
<td>1010</td>
<td>Access to a provider-owned app on a mobile device.</td>
<td>Enrolment fraud, fraudulent verification (spoofing), fraudulent matching, transmission channel attacks, overriding the reference storage location, corruption of central storage may lead to identity theft or abuse.</td>
</tr>
<tr>
<td>0010</td>
<td>Access to a provider-owned app on a mobile device.</td>
<td>Enrolment fraud, fraudulent verification (spoofing), fraudulent matching, transmission channel attacks, overriding the reference storage location, corruption of central storage may lead to identity theft or abuse.</td>
</tr>
<tr>
<td>0011</td>
<td>Applications where a provider trusts his own storage and processing better, mobile passport check.</td>
<td>Enrolment fraud, fraudulent verification (spoofing), transmission channel attacks, overriding the reference storage location, corruption of central storage may lead to identity theft or abuse.</td>
</tr>
<tr>
<td>1011</td>
<td>Applications where supervised enrolment is required, the provider trusts his own storage and processing better.</td>
<td>Enrolment fraud, fraudulent verification (spoofing), verification channel attacks, overriding the reference storage location, corruption of central storage may lead to identity theft or abuse.</td>
</tr>
<tr>
<td>1111</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>0111</td>
<td>Applications where a mobile device is only used as enrolment fingerprint scanner.</td>
<td>Enrolment fraud, enrolment channel attacks, overriding the reference storage location, corruption of central storage may lead to identity theft or abuse.</td>
</tr>
<tr>
<td>0101</td>
<td>Token ownership application with supervised sensor to avoid fraud.</td>
<td>Enrolment fraud, enrolment channel attacks, tampering with reference storage.</td>
</tr>
<tr>
<td>1101</td>
<td>Supervised token ownership applications, passport.</td>
<td>Transmission channel attacks, tampering with reference storage.</td>
</tr>
<tr>
<td>1001</td>
<td>Applications with supervised enrolment and matching process.</td>
<td>Enrolment fraud, verification fraud (spoofing), transmission channel attacks, tampering with reference storage.</td>
</tr>
<tr>
<td>0001</td>
<td>Applications with outsourced verification processing.</td>
<td>Enrolment fraud, verification fraud (spoofing), transmission channel attacks, tampering with reference storage, system can produce matching pairs independent of biometric data.</td>
</tr>
</tbody>
</table>
result table.

From the gathered responses it is concluded that the suggested privacy-related risks are present across all architectures. Therefore, these risks have not been included in the survey results.

From the survey results we can deduce the following:

- The most use cases are determined for architectures 0000 and 1000. A possible explanation for this would be because commercial and governmental products using these architectures already exist, which raises the respondent’s familiarity with the architecture.

- For other architectures, such as 0110, 1110, 1010 and 0010, the architecture layout apparently affects the usability in such a way that no realistic use cases can be thought of.

- Using a combination of internal and external components opens the possibility for transmission channel attacks.

- Using external reference storage opens the possibility for attackers to override the reference storage location. On the other hand, using internal reference storage opens the possibility for tampering with the reference storage.

- Enrolment fraud, independently of the architecture, is always an issue. Experts indicate that this is mainly because it is difficult to establish trust with an external party and enrolment arguably is the most interesting part of the biometric process to attack.

5. CONCLUSION

As the use of mobile biometric solutions becomes more popular, it has become apparent that the design choices of a biometric solution influence its usability and security. In this paper we have identified architecture-specific use cases, security- and privacy-related risks and mitigations for mobile biometric solutions.

Using an architecture with external components requires trusting an external third-party. On the other hand, using an architecture with internal components requires trusting the user of the mobile device. Carefully choosing a combination of either an internal or external enrolment sensor, verification sensor, reference storage and verification algorithm cannot fully mitigate the wide variety of threats. However, depending on the desired functionality of the application, mitigation against some threats can be accomplished by using external components instead of internal components and vice versa.

Furthermore, countermeasures like Presentation Attack Detection, enrolment protection, biometric template protection, transmission channel protection, establishing trust and data minimization can help increase the security and privacy of the biometric application.

6. FUTURE WORK

Further study can be done on the applicability of mitigations by having their effect examined through a survey of biometric application builders.

7. REFERENCES

APPENDIX

A. EXAMPLE SURVEY PAGE

The survey used in this research asks respondents identical questions for a specific architecture. As an example, the page containing questions about an architecture with merely internal components is depicted in Figure 2 below.

The full survey is available at: https://nl.surveymonkey.com/s/PMGXZYJ

---

**Figure 2. Example survey page**