Department of Computer Science

Mobile Biometrics in Financial Services: A Five Factor Framework

Giulio Lovisotto, Raghav Malik, Ivo Sluganovic,
Marc Roeschlin, Paul Trueman, Ivan Martinovic

CS-RR-17-03

Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford, OX1 3QD

Mobile Biometrics in Financial Services: A Five Factor Framework

Giulio Lovisotto*, Raghav Malik†, Ivo Sluganovic*, Marc Roeschlin*, Paul Trueman†, Ivan Martinovic*
*University of Oxford, UK
†Mastercard
first.last@{cs.ox.ac.uk|mastercard.com}

***Abstract*—Banks and the wider financial services sector are witnessing sharp increases in the number of users interacting with them through digital channels. In light of these changes, traditional password-based mechanisms are becoming insecure, inconvenient, or both, as evidenced by the rise of digital fraud rates and users who report frustration with authenticating to financial services. Biometrics are an alternative that offer potential usability improvements, while retaining or improving the security guarantees. This paper is motivated by the need for a demystification of the deployment of a biometric system for financial services use cases.**

This paper is based on two separate studies: (1) a longitudinal study of users' attitudes towards the adoption of biometric authentication for online payment use cases; and (2) an opinion survey of a targeted group of financial services professionals. The findings of these studies are two-fold. The user study shows that users (>90%) believe biometrics are more secure and convenient than passwords, and that they are willing to adopt biometrics to replace existing password-based authentication. Nonetheless, the industry survey highlights gaps in experience and importance on different aspects of deploying biometric systems: only 36% of respondents are familiar with biometrics, compared to 88% of them that would be involved in their deployment. These gaps inhibit adoption of biometrics, as they prevent effective communication and collaboration among different entities involved in the process of deployment.

In this paper, we use the insights gathered in the studies to identify five key factors that contribute to the success of a biometric system in financial services. For each factor, we outline and discuss the main challenges and trends that need to be analysed before deployment, combining perspectives from academia, industry groups, and regulators. The Five Factor Framework provides a broad range of guidelines and necessary considerations for the deployment of mobile biometrics in financial services.

I. Introduction

In recent years the financial services industry has seen important changes with the application of emerging technologies and the corresponding shift in user behaviours. The proliferation of powerful computing devices such as mobile phones, tablets and laptops has changed the way users interact with financial services (e.g., banks, e-commerces). In 2015 the number of non-cash transactions totaled an estimated 426 billion, a growth of 10.1% compared to the previous year [1]. Surveys show that mobile banking increased by 20% from 2013 to 2015, and mobile payments are gaining popularity as well [2]. With this growing popularity, password-based authentication is becoming increasingly inconvenient for users. In the following, we will briefly overview the drawbacks of passwords, and introduce the challenge of replacing them in financial services.

Passwords. Passwords have been widely adopted as means of authenticating users across digital channels. Passwords are the most common method as they have several advantages: they are easy to use, cheap to deploy, do not require the user to carry anything, and are easy to revoke and change in case of a compromise. A good overview and comparison between passwords and other web-based authentication methods can be seen in [3]. Unfortunately, with the increase in the number of digital services, users are now expected to remember dozens of credentials. Consequently, passwords have become an impractical authentication mechanism for users. On average, users are registered to more than 90 online accounts, and that number is growing quickly [4]. To cope with managing their accounts, users tend to reuse passwords across different services with up to 51% of passwords are reused [5]. They often select easily guessable ones (up to 80% of passwords can be automatically cracked in less than 3 days [6]). It is therefore unsurprising that users and businesses are struggling with passwords: 21% of users forget passwords after 2 weeks [7], and 25% forget one password at least once a day [8]. Password managers are attempting to relieve users from password fatigue, but recent studies show that they are insecure [9]. Li et al. [10] showed that four out of the five most popular web-based password managers are vulnerable to attacks.

The Need for Usability. Nowadays, users expect simple and convenient experiences. Thus, usability is of key importance for digital retailers. Younger generations, in particular, show heightened frustration when facing inconvenience [12]. This focus on usability has made users intolerant towards solutions that do not meet their expectations. About a third of online purchases are abandoned at checkout because consumers cannot remember their passwords [13]. On the other hand, fraudsters have been exploiting the weaknesses of poor password-based authentication practices for online payments. This resulted in a digital fraud rate that grows in line with the digital commerce rate, that is almost three times higher than the physical fraud rate [14]. The confluence of these security and usability challenges has resulted in a significant rise in interest in biometric recognition technologies. The major advantage of biometrics is their convenience over dedicated tokens and memorised secrets. As outlined in the World Economic Forum (WEF) report [15], biometrics have potential to provide convenience

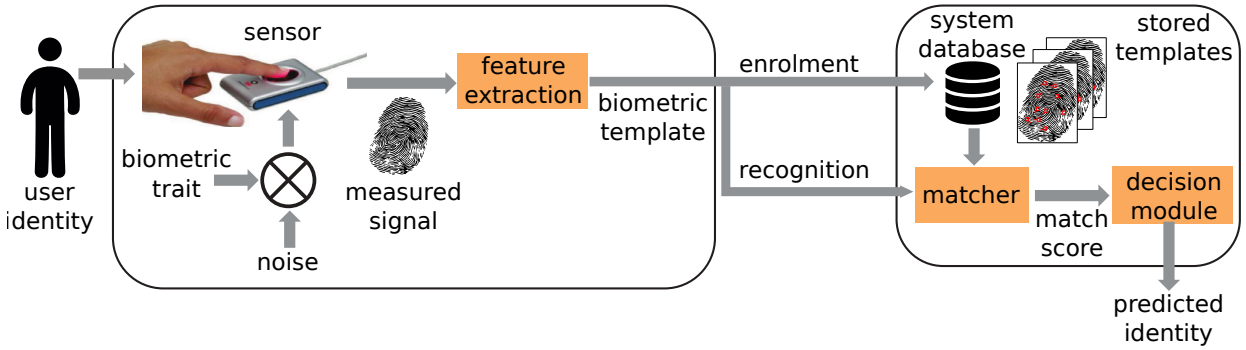


Fig. 1: Building blocks of a biometric recognition system. Adapted from [11].

and security for customers in financial services.

The Challenge in Financial Services. Financial services have the opportunity to move beyond passwords, and our user study confirms that ***90% of users are willing to adopt biometrics in order to replace passwords***. However, even with the availability and maturity of mobile biometric solutions, there is a significant gap in terms of the rate of biometric adoption by industry.

Biometrics have been in use in supervised environments for decades [11]. Border control is the most common example, where a human supervisor oversees the user interaction with the fingerprint scanner. However, the new unsupervised mobile environments generate caution: users are not supervised when they use their mobile device for biometric authentication. Biometric industry standards, protocols and regulations have not evolved to adapt to uncontrolled environments. Survey data from industry professionals, provides insights about this gap. There is a significant knowledge gap amongst decision makers. ***36% of respondents claiming to have experience with biometrics***. On the other hand, ***88% believe they will be involved in implementation decisions*** which reflects the impact that biometric systems have on business objectives ranging from risk management to usability and privacy.

Contributions. This article provides a review and systematisation of knowledge of the current state of mobile biometric recognition systems for financial services. Our contributions are the followings:

- A longitudinal (quantitative and qualitative) study with 449 end users of a deployed biometric recognition system in an online payments use case, investigating their perceptions before, during, and after having used a novel biometric system in a financial context for three months. The study confirms that users are eager to adopt biometrics to replace password-based authentication.
- A targeted survey of financial services professionals primarily working in consumer banking. This survey confirms that these individuals lack knowledge about biometrics and that their views are often biased according to their professional background.
- The identification of key factors of biometric recognition systems that needs to be considered and evaluated in order to ensure the overall success of the system.
- A review of the main challenges and the opportunities that are present in the use of biometric recognition system for financial services, taking into account the perspectives of academia, industry groups, and regulators.

The goal of this working paper is to provide supporting information for decision makers in the industry, in order to accelerate responsible adoption of biometrics in financial services.

II. Background

We start by providing a background on biometric recognition, and an overview of its applications in the financial sector.

Biometric Recognition. Biometric recognition is the automated recognition of individuals based on their physiological and/or behavioural characteristics [16]. These characteristics (or traits) present properties that are distinctive (they are unique to individuals), and reasonably permanent (they do not change significantly over time) [11].

A typical biometric recognition system has different components, shown in Figure 1. Users present their biometric trait to a biometric sensor, that captures it and provides a measured signal. During the measurement, several noise components may alter the user's biometric, such as sensor limitations, environmental changes, or variations in user interaction. After the sensor captures the trait, feature extraction transforms the measured signal into a biometric template: a compact but expressive representation of the biometric trait. A biometric system is composed of two separate phases. The first phase is enrolment, where the biometric system acquires the user's biometric trait, extracts the template, and stores it in a database, along with an identifier linking the template with the user's identity. The second phase is recognition, where the biometric system acquires the user's biometric trait, extracts the template, and compares the template with the one(s) in the database. There are two possible types of recognition:

- *authentication*: (called *verification* in ISO 2382 [17]) where the user initially claims his identity, presents his trait to the sensor, and the system compares his template with the stored template associated to the claimed idenity (*1 to 1* comparison).
- *identification*: where the user simply presents his trait to the sensor, and the system compares the user template with all stored templates to determine the user's identity (*1 to N* comparison).

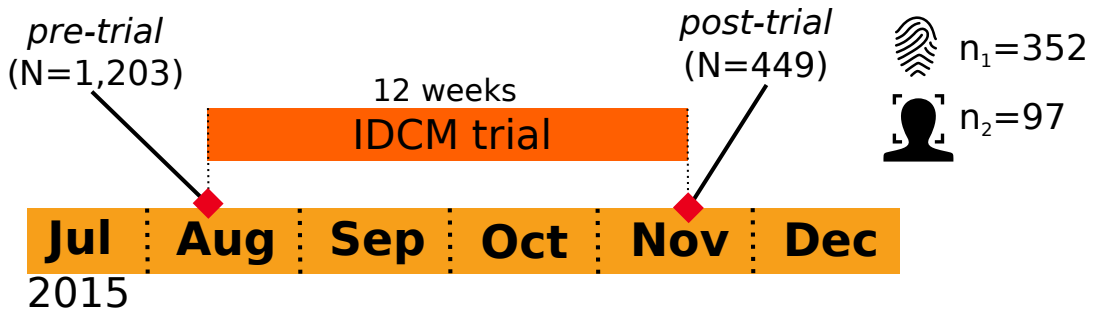


Fig. 2: Timeline of the user study. The study was carried out over a period of 3 months between August and November 2015. Participants used Mastercard *Identity Check Mobile* (IDCM) for biometric authentication of online payments. A total of 449 users completed both pre- and post-trial survey (352 used fingerprint recognition, 97 used face recognition).

Further introductory information on biometrics can be found in the work of Jain et al. [16].

User Authentication in Financial Services. Today, there are many ways in which users can interact with their banks. These include in-branch visits, contact centre calls, online banking and mobile apps. Authentication processes in these various channels vary significantly. In-person interactions often rely on validation of identity documents, whilst digital interactions may rely on passwords, PINs or other knowledge-based authentication (e.g., security questions).

Nowadays, 3-Domain Secure (3DS) protocol [18] is the typical authentication procedure for online payments. We report the flow of a 3DS transaction in the e-commerce use case in Figure 3. The procedure works with the following steps: the client initiates an authentication request by providing their payment card details at the checkout page (1), the retailer forwards the request to the bank for user authentication (2), the bank replies to the request notifying the retailer that further interaction is required for authentication (3), and the retailer forwards this information to the client (4). Afterwards, the client initiates a challenge request with the bank (5), and the bank replies presenting a challenge to the client (e.g., passwords, one-time passwords via SMS) (6). If the challenge is successfully completed, the bank forwards notifies the retailer that the transaction is authorised (7-8), and the retailer forwards the authorisation message to the payment network (9-10).

The challenge of steps 5-6 in Figure 3 presents weaknesses when it is deployed in real-world systems. Previous studies showed that many poor practices are common: password transmitted unencrypted, storage of cleartext passwords, and weak or non-existing password composition policies [19]. Real examples of malware reading SMS [20] confirm that SMS are not secure, to the point that NIST discouraged using them as a 2nd factor [21]. Additionally, researchers have highlighted additional challenges of popular implementations of 3DS protocol [22] (Verified-by-Visa[1] and Mastercard SecureCode[2]). For instance, browser implementations are using Iframes that do not easily allow customers to recognise who is asking for

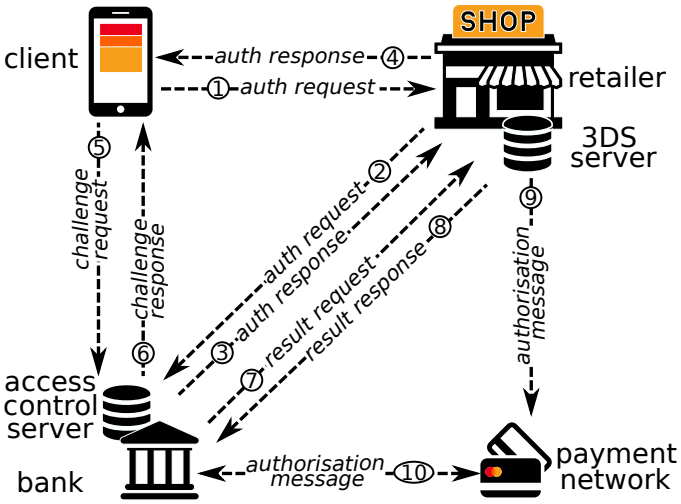


Fig. 3: 3DS Protocol, outline of the *Challenge Flow* steps. Adapted from EMV 3-D Secure - Protocol and Core Functions Specification [18].

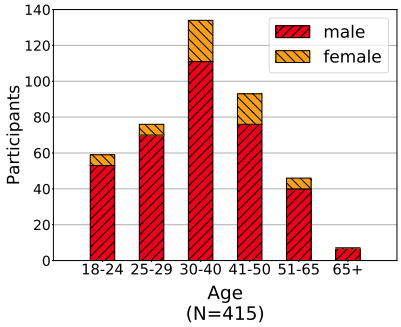
their password. Another example are the malpractices in how issuers perform authentication: some verify their customers online asking for the card ATM PIN, or their date of birth [22].

Moving to biometrics. Biometric recognition could be used in place of traditional mechanisms in order to authenticate users. Biometrics have the potential to improve security and convenience, as they do not require users to memorise secrets, or to carry dedicated tokens with them. A wise use of biometrics in the mobile setting is to use both biometric trait and device ownership as two separate, but linked, factors for authentication. In this case, to impersonate users, adversaries need to obtain not only the user's biometric, but also the device where the user enrolled with that biometric. Current market solutions are focusing on popular fingerprint and face recognition. Apple Pay[3] already allows customers to initiate contactless payments with fingerprints through TouchID[4]. HSBC is introducing face recognition in order to verify customer identities when opening new accounts [23].

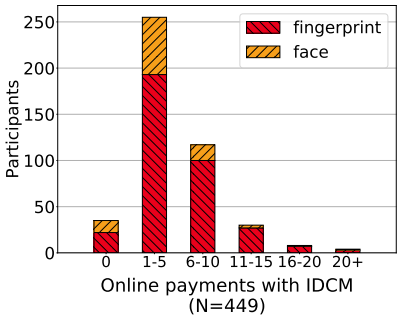
Two industry standards for biometric systems are al-

[1]http://www.visa.co.uk/products/protection-benefits/verified-by-visa/
[2]https://www.mastercard.co.uk/en-gb/consumers/features-benefits/securecode.html

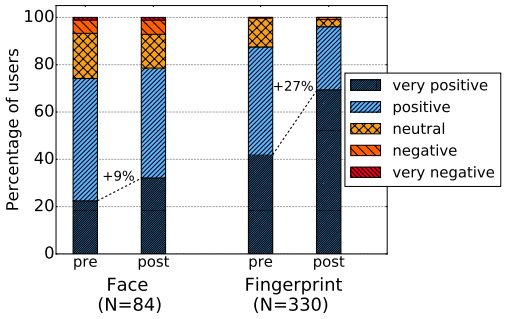
[3]http://apple.com/uk/apple-pay/
[4]http://support.apple.com/en-gb/HT201371



(a) Age and gender distribution of survey participants.



(b) Online payments participants carried out with biometric authentication.



(c) Change in biometrics perception of participants after the trial.

Fig. 4: Results of the user study.

ready present: FIDO Universal Authentication Framework [24] (UAF), and IEEE Biometric Open Protocol Standard [25] (BOPS). However, the shift from traditional methods to biometrics is a challenging process that involves multiple parties. Financial services companies are directly responsible for the deployment of these systems, and in order to do so they must consider the impact of several stakeholders. In particular, the groups that should be taken into account are: (i) consumers, (or *end users*), who will be using the system, (ii) industry groups, such as NIST, FIDO, ISO, EMVCo[5] that provide guidelines for the deployment of such systems, (iii) regulators, that issue user privacy legislation and authentication/payment services regulations, and finally (iv) the financial services companies themselves, as their opinions about biometrics are directly reflected in their deployment decisions. In this paper, we will analyse and compare perspectives of these stakeholders.

III. User Study

In order to understand the customers' perspectives about the adoption of a real-world biometric authentication system for the online payments use case, we conducted a long-term attitudinal study. The study included 449 participants, and was carried out over the course of three months.

Motivation. This study aims to gather insights into the perception and attitudes of users towards the use of biometrics for authentication. The main aspects that are of interest to us were the perceived usability, security, and users' propensity to adopt them compared to the current password/PIN-based solutions. We also want to understand whether and how users' perceptions changed after trialling biometrics for authentication in a real-world use case. This requires the study to include two separate surveys: the first one should be completed before trialling biometric authentication, and the second one after the trial.

Structure. We invited cardholders of a bank in the Netherlands to trial Mastercard's biometric solution, Mastercard Identity Check Mobile (IDCM), within the use case of e-commerce payment authentication. IDCM is a mobile phone application that provides biometric recognition, either using face or fingerprint as biometric traits.

[5]http://www.emvco.com/

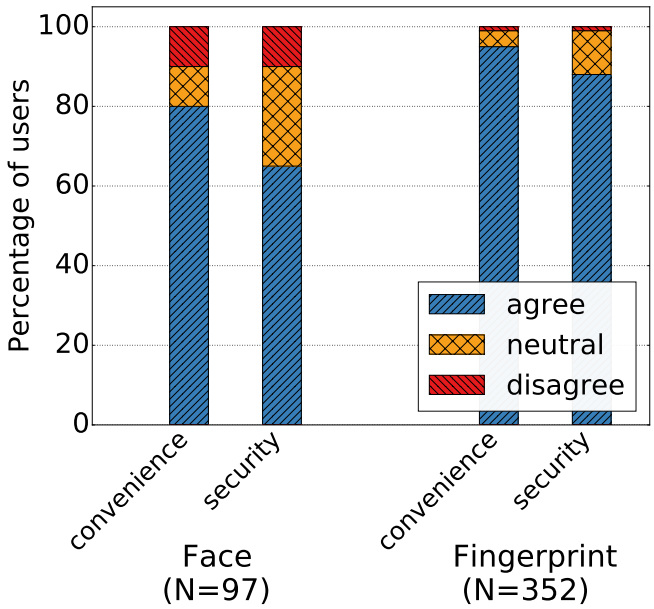
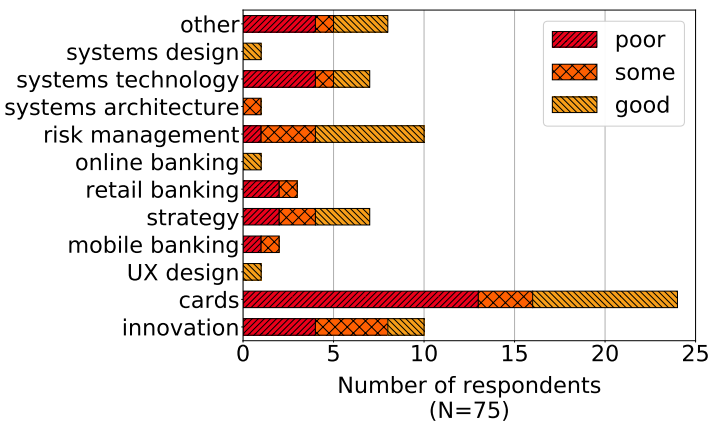


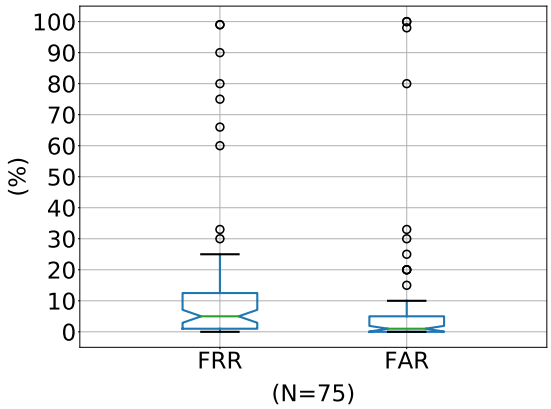
Fig. 5: Comparison between biometric authentication and password-based approaches. Users' agreement with the statements *"biometric authentication is more [convenient|secure] than passwords"*.

Figure 2 shows the timeline of the user study. Spanning over 4 months, the study began in August 2015, when 1,203 participants entered the study and completed a *pre-trial* survey. In the following three months, users were able to use either their fingerprints or faces to authenticate online payments. Each user was assigned only one biometric modality based on their mobile phone capabilities. The trial period ended in November 2015, when 449 of the initial participants completed a *post-trial* survey. Out of the final group of 449 users, 352 used fingerprint recognition, while 97 used face recognition. In both surveys, we used both qualitative and quantitative methods to collect users' perceptions. To understand changes in perceptions, we linked user responses across measurements of the two surveys.

Results. We report in Figure 4 prominent results of the study. Most of the study participants fit the profile of early adopters,



(a) Industry professionals job department, and self-reported previous experience with biometrics: either *poor*, *some*, or *good* experience.



(b) Value of false accept (FAR) and false reject (FRR) rates that respondents reported as "appropriate" for biometric authentication in financial services.

Fig. 6: Results of the industry survey.

showing an high degree of knowledge about emerging technologies. Figure 4a shows the age and gender distribution of the participants (34 users did not disclose this information). During the three months trial, ***92% of the participants used the biometric system at least once***, and ***43% used it more than five times***, shown in Figure 4b. The pre-trial survey shows that 85% of users already had an positive attitude about using biometrics. Nonetheless, after the trial, ***the amount of participants with "very positive" attutitude increased: 9% and 27% for fingerprint and face***, respectively (Figure 4c). We asked users to compare security and convenience of biometric authentication with traditional password/PIN-based methods, we report the results in Figure 5. Overall, ***users believe that biometric authentication is more secure (83%) and more convenient (92%) than passwords***. Fingerprint recognition obtained marginally better results compared to face recognition, for both security and convenience.

Discussion. Results show that users react more positively to fingerprint compared to face recognition. This is likely due to the fact that fingerprint is an older and better known modality. Qualitative analysis revealed that face recognition users sometimes struggled finding proper lightning and/or angle to take a good quality picture of their face during the trial. Altogether, the study shows that users are eager to move to biometrics-based solutions, and their perception is that these solutions would be more secure and convenient than password-based methods.

IV. Industry Survey

To understand industry perspectives on biometric authentication in financial services, we conducted a survey of 75 industry professionals.

Motivation. This survey aims to collect opinions of financial services professionals regarding the deployment of biometric systems for authentication. When implementing a biometric system in this context, these individuals need to account for several aspects of its deployment.

Reviewing the current industry standards, regulations, academic literature, and using Mastercard's experience with authentication in financial services, we identified five key aspects of biometric systems: (1) biometric modality performance, (2) usability, (3) interoperability, (4) security, (5) privacy. We believe these aspects (or *factors*) are the most important topics to consider deploying a biometric system in financial services. Our survey uses quantitative and qualitative methods to investigate the opinions of industry professionals regarding these factors: how these factors affect decision making, and what the perceptions and opinions of these factors are in the industry.

Structure. We used Mastercard's network of relationships to reach relevant financial services professionals. The survey consisted of a demographics part, and for the rest was structured into separate sections, each of them regarding one of the five aspects of biometric systems mentioned above. In each section, we measured participants' perceptions on the topic with a 5-point scale. The survey was carried out in August 2016, a total of 75 individuals completed the survey. The majority of respondents were mid- to senior-level managers in banks with more than 500 employees, mainly based in Western Europe and North America.

Results. The participants were asked to report their job departments and self-assess previous experience with biometrics. As Figure 6a shows, most participants were involved in either *cards*, *innovation* or *risk management*, and only ***36% of them claimed to have good experience with biometrics***. This is compared to the ***88% who expect themselves to be involved in decision-making regarding biometric deployments***. The lack of experience seems to also translate into high optimism about the potential of biometric systems: ***(96%) of inexperienced individuals believe biometrics will improve the security of mobile banking and payments, compared to 61% of experienced professionals*** that agree with this proposition.

This result is also confirmed in Figure 6b, which reports the respondents' idea of "appropriate" false accept and false reject rates for financial services use cases. Figure 6b shows

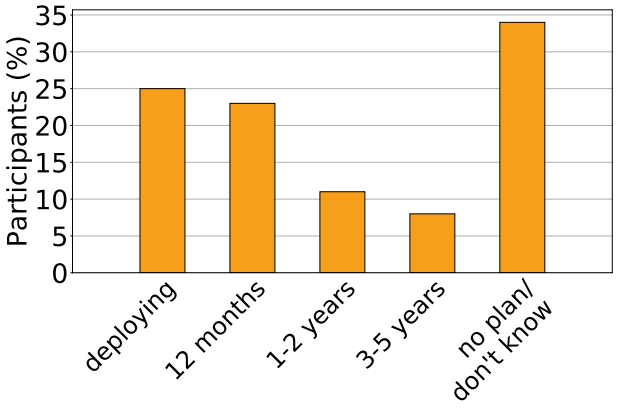


Fig. 7: Expected time to deployment of biometric systems in participants' organisations.

that participants are not familiar or misunderstood the meaning of these rates: lots of responses reported ***as appropriate error rates over 20%***, which do not seem reasonable in the context of financial services.

The survey highlighted significant differences in opinions when segmenting the industry professionals based on their background and department, either more involved in the *technical*-side, or in the *business*-side. Table I reports meaningful differences in these opinions. As an example, we found that 67% of the technical subgroup agreed with the need for a 2nd factor for authentication, compared to only 35% of agreement in the business subgroup. Similarly, there is a difference in the seriousness of phone theft: 76% and 37% of individuals consider phone theft as a serious threat, for the technical and business subgroup, respectively.

	Technical	**Business**
2nd factor is necessary for user authentication	**67**	**35**
Identity theft is a serious threat	53	33
Phone theft is a serious threat	**76**	**37**
Consumers will adopt voice recognition	52	29

TABLE I: Percentage of agreement with different statements regarding biometric recognition systems, segmenting the respondents into technical and business subgroups. Significant differences highlighted in bold

Most participants expect their companies to be deploying biometric systems in short time, shown in Figure 7. Results indicate that more than ***50% of the financial services companies surveyed plan to implement biometric solutions within 2 years*** of the date of the survey.

Discussion. Industry professionals recognise that biometrics have the potential to improve security against fraud and convenience for users. However, there is a wide gap: individuals that are supposed to be taking decisions in deployment of biometrics often do not have sufficient knowledge and experience to make well-informed choices. This gap is mainly due to biometrics being a technology that has not been used by businesses for authentication on large-scale, but also to the fact that industry professionals have different backgrounds. Technical professionals are more focused on mitigating risk of fraud or compromise and are therefore more supportive of 2nd factors being used. On the other hand, business professionals appear to be less concerned about the risk of phone theft. While phone theft is certainly a major concern for the victim's biometric, physically stealing phones is not a scalable threat (compared to others) and therefore represents low overall business risk. This is discussed further in Section Factor 4: Security.

Our results confirm that the financial services industry intends to move quickly towards the adoption of biometrics. Nonetheless, industry professionals are growing more wary of the drawbacks of biometrics. For instance, qualitative analysis shows that the regulatory aspect is becoming more concerning: respondents reported that regulation *"delays the design, makes decision making very slow due to higher risks"*. Therefore, it is fundamental that different stakeholders collaborate to identify best practices to ensure the success of biometric systems.

V. Five Factor Framework

The decision to deploy a biometric solution requires a deep understanding of its implications. These implications are multidimensional and include, security, privacy, and usability, and they should all be taken into account. Our research and the surveys we conducted highlight that the stakeholders of a biometric system (i.e., companies, users, industry groups) do not have a clear picture of its implications, and might have contrasting opinions on different factors and their importance.

In order to address the knowledge gaps and inconsistencies in prioritization of various aspects, we designed the Five Factor Framework. The framework is based on the structure of the industry survey, and is composed of five major factors, that thoroughly describe the capabilities of a biometric authentication system. The factors are the following:

- Modality Performance;
- Usability;
- Interoperability;
- Security;
- Privacy.

In the following sections, we provide a brief description of each factor, outline the respective key concepts, relevant challenges and trends to be aware of when deploying mobile biometrics in financial services. By presenting the factors in this manner, we draw into focus the need to be more cognizant of the roles that each of the factors plays in ensuring a successful and responsible biometric deployment.

Factor 1: Modality Performance

In this section, we describe how biometrics performance can be evaluated.

Performance Metrics. With biometric modalities we refer to traits that can be measured to perform biometric recognition. In the past years, a multitude of modalities have been investigated, both physiological characteristics (e.g., iris, fingerprint, face), and behavioural characteristics (e.g., keystroke dynamics, gait). Due to the growing number of modalities, the need for their evaluation brought the biometrics community to adopt common metrics to measure their performance. The

TABLE II: Usability goals and metrics, Usability and Biometrics: Ensuring Successful Biometric Systems [26].

Usability Goal	Description	Metric
Effectiveness	How well can a user perform a task	*Success rates:* can users provide an high-quality sample?
Efficiency	How quickly can a user perform work, and what are the error rate in doing so	*Time on task*: can users quickly use the system?
Satisfaction	What are the user attitudes, perceptions, feelings and opinions of the system	*Users satisfaction level*: are users comfortable using the system?
Learnability	How rapidly can a user become productive	*Time to learn a task*: how long does it take users to learn how to use the system?
Memorability	How well a returning user forms a mental model of the system and remembers how to use it	*Number of errors made over time*: can users remember how to use the system?

following are the most used metrics [27] (also reported in ISO/IEC 19795 [28]):

- *False Accept Rate* (FAR): proportion of false acceptances divided by the total number of biometric claims that ought to have been rejected,
- *False Reject Rate* (FRR): proportion of false rejections divided by the total number of biometric claims that ought to have been accepted,
- *Receiver Operating Curve* (ROC): curve that shows the relation between the FAR, the FRR and the system detection threshold,
- *Equal Error Rate* (EER): error rate obtained by setting the detection threshold of the system such that FAR and FRR are equal.

Although these metrics are widely accepted as the benchmark comparison between different biometric technologies, they fail to describe a biometric system thoroughly (Eberz et al. [27]). This is particularly true for continuous authentication with behavioural biometrics, that suffers from errors that are not captured by traditional metrics (*systematic errors* [27]). Additionally, false acceptances are sometimes calculated under the assumption of *zero-effort* attacks (adversary simply presents their own biometric trait in an attempt to impersonate the user), which do not typically address realistic threat models. Furthermore, since the error rates are database-dependent (i.e., they depend on the size/content of a specific biometric database), the value of these errors could not generalise when the population size increases significantly, or if the biometric characteristic changes (e.g., with ageing).

Templates Distinctiveness. In theory, one could use the entropy of biometric templates given the user's identity to estimate the intrinsic distinctiveness of a biometric trait. ISO/IEC 30107 [29] defines entropy as the "measure of the amount of uncertainty that an attacker faces to determine the value of a secret". The greater the entropy the easier it is to discriminate between different templates, and the harder it is to guess them for an adversary. Similarly to passwords entropy, which is impractical to estimate in real-world applications (due, for example to password re-use [5]), biometric entropy is also a challenging topic. We lack robust statistical models to describe the multidimensional distributions of template features, therefore entropy estimation requires several assumptions [30].

Integrated Solutions. Even though biometrics represent a desirable alternative to passwords, a simple replacement of passwords with stand-alone biometrics is generally not recommended [11]. Such implementations would be comparably vulnerable to compromises under realistic threat models. Integrated solutions such as *multi-factor* and *multi-layer* should be adopted (as acknowledged by ***67% of industry professionals in our survey***). Multi-factor approaches require users to respond to two or more explicit authentication challenges (e.g., multi-modal biometrics). Multi-layer approaches combine a single explicit factor with other data element that are typically invisible to users (e.g., device fingerprinting, geofencing, risk scoring).

FACTOR 2: USABILITY

This section gives a brief background on the notion of usability with a focus on the biometrics field, and examines user perceptions that emerged from our surveys in more detail.

Designing for Usability. Analysis of usability is usually broken down into simpler concepts (or *goals*) that can be evaluated separately, through user studies [31]. NIST provided a summary of these goals in their Usability and Biometrics handbook [26], which proposes a user-centric design process for the development of biometric systems. Table II shows usability goals and measurable metrics to assess the usability of a biometric system. As an example, Table II shows that *efficiency* can be indicatively quantified by measuring the *time on task*, i.e., the time users take to use the system. Even if usability of biometric solutions has been studied in controlled settings, analysis in the unsupervised environments of mobile biometrics where user-base numbers are much higher, could have different outcomes. Interestingly, we found that neither of current industry standards, FIDO UAF and BOPS, address usability in depth. We refer the reader to Dix et al. [32] for a deeper overview on the subject of usability in human-computer interaction systems.

Users' Perceptions. Perception of biometrics plays a fundamental role in their adoption, as it influences the propensity of users to adopt these technologies (Technology Readiness [33]). We investigated the perceptions of both end-users and industry professionals, as they represent direct and indirect stakeholders of a biometric system, respectively. Analysing perceptions helps understand the rate of adoption, its obstacles, and how

TABLE III: Perceptions of aspects of biometric systems, results from both industry survey and user study.

Perception of	Key Findings
Convenience	• 94% of industry professionals believe users value convenience in authentication systems • 92% of users find biometrics more convenient than passwords • Many users choose to enrol with IDCM to avoid passwords and PINs
Security	• 76% of industry professionals believe biometrics are more secure than passwords • 83% of users believe biometrics are more secure than passwords • 73% of users believe biometrics will reduce fraud • 93% and 77% of users believe fingerprint and face recognition are secure, respectively
Purchasing Behaviour	• Many industry professionals believe biometrics reduce friction, decrease cart abandonment and simplify shopping • Users report an increased inclination towards mobile commerce during the IDCM trial
Adoption	• 93% of users state they will adopt biometric solutions • 65% of industry professionals believe users will adopt biometric solutions (face or fingerprint recognition) • positive perception of biometrics improved from 85% before trial to 93% after trial

these can be addressed. In Table III we report key findings of our surveys, regarding perceptions on four core aspects of biometric systems in financial services: convenience, security, purchasing behaviour, and adoption. Surveys highlight discrepancies in the perceptions of adoption: ***93% of end users compared to 65% of industry professionals believe users will adopt biometrics***. We also found differences in the perception of security: for ***fingerprint and face recognition, 93% and 77% of users considered them secure, respectively***. These results highlights the importance of users' familiarity with the technology: willingness to adoption and perception of security both increased after trial. In addition, these metrics scored higher for fingerprints compared to face recognition, as fingerprinting has a longer history of being used as a security tool by authorities (e.g., border control, governments, police). Users took longer to get used to facial recognition, as it required the learning of specific behaviours (e.g., camera distance and angle, lighting).

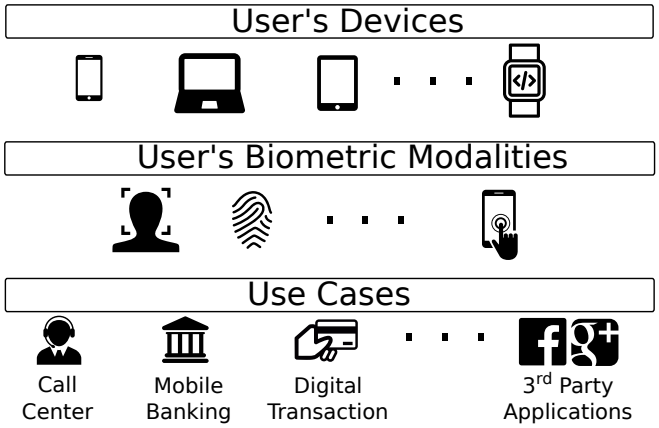


Fig. 8: Types of interoperability. Ideally, biometric systems authenticate users across multiple modalities, different user devices, and in different use cases.

FACTOR 3: INTEROPERABILITY

Interoperability refers to the ability of a system's components to work with other components or with other systems.

Types of Interoperability. We identify three types of interoperability that are relevant to the context of biometric systems, these are presented in Figure 8:

- across *devices*: the system can authenticate users via biometric measured by different devices (e.g., mobile phone, laptop, wearable).
- across *use cases*: the system can authenticate users across different applications (e.g., mobile banking login, payment verification).
- across *modalities*: the system can authenticate users using different biometric traits interchangeably (e.g., fingerprint, facial recognition).

Our survey reveals that industry professionals strongly believe interoperability is important, with a ***preference for device interoperability*** (82%, 68% and 66%, for device, use case, and modality interoperability, respectively).

Template Storage. Mobile biometric solutions can either store templates on users' devices, or on central servers. This architectural choice has significant impact on the interoperability properties of the system and on security and privacy as discussed in Section Factor 4: Security and Factor 5: Privacy. Figure 9 shows an overview of a distributed and a centralised model. In distributed models, user devices capture, match and store biometric data of the individual owner, authentication occurs locally, and communication with the server is authenticated. In centralised models, a server stores and matches biometric data for all users, while user devices collect and transmit biometric samples. Recently, hybrid architectures have been proposed (such as *visual cryptography* Ross et al. [34]) where the template is partially stored on the device and partially on a central server. In financial services, distributed models are preferred, as they minimise the risks of related to data protection (confirmed by FIDO UAF and BOPS being distributed architectures).

Achieving Device Interoperability. In distributed models, interoperability across devices is not straight-forward to achieve. In fact, in the case of distributed template storage, only the device where the user previously enrolled is able to recognise the user, since that device is the only one that can access the user's stored biometric template (as in FIDO UAF and BOPS). Therefore, solutions such as higher level identity architectures that support *house-holding* of devices are required to achieve device interoperability. On the other hand, with central template storage the interoperability among

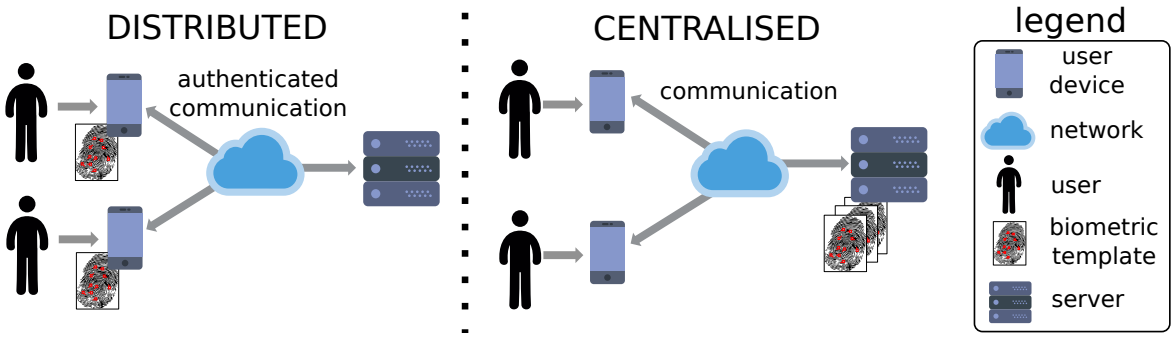


Fig. 9: Distributed and centralised models of template storage.

different sensors needs to be addressed: biometric sensors are manufactured by different OEM, and could have different data formats and quality. With the average number of user-owned devices (e.g., laptops, mobile phones, tablets) at 3.64 and growing rapidly [35], interoperability across devices is an important challenge for future research.

FACTOR 4: SECURITY

Definition of threat models is one of the most important tasks when designing the security of a biometric system. Since the classification of threat models anticipates the likely forms of attacks, it assists in the identification and prioritisation of valuable assets to protect, and provides additional focus to assess and prevent such attacks. To model threats, system designers also need to take into account how architectural choices of deployment affect possible attack vectors.

In this section we present the main threats to biometric systems, and outline the challenges in evaluation and assessment of biometric system security.

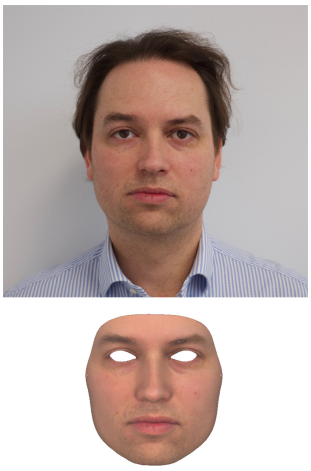
Zero-effort Attacks. In *zero-effort* attacks, the adversary presents their own biometric trait claiming another user's identity, and makes no effort to impersonate that user. If the adversary is enrolled in the biometric system, the effectiveness of zero-effort attacks can be measured with the false accept rate. For this reason, FAR can usually be associated with the level of security against impostors. However, this is an imperfect view in real-world scenarios, for two main reasons. First, it is hard to measure how the system will react to unseen biometric samples: false accepts may not generalise to larger populations. Second, in modern biometric systems, multiple parties are involved in the security of the system. Threats can target client devices, device manufacturers, third-party applications, and authentication servers.

Presentation Attacks. In *presentation attacks*, the adversary attempts to construct an artifact that reproduces the biometric trait of a user. The adversary can then present such artifact to the biometric sensor, claiming the user's identity. Presentation attacks have been proved feasible for several modalities, as shown in Figure 10. Faces can be reconstructed with 3D printers from simple photographs, shown in Figure 10a. Similarly, fingerprints can be reconstructed with silicone, even from photographs of the hands [37], shown in Figure 10b. Recently, presentation attacks have been carried out even with ECG biometrics [36], showing that a laptop with an audio card is sufficient to recreate ECG signals, shown in Figure 10c.

The countermeasure for PA is *presentation attack detection* (PAD) [38] (addressed by ISO/IEC 30107-3 [29]). PAD techniques can be classified into three subgroups: (i) measuring physiological properties of the individual (e.g., blood pulse or pressure, spectral or optical properties of the skin), (ii) identifying human behavioural responses (e.g., blinking, pupil or head movement), and (iii) challenge-response protocols [39]. Some detection approaches are based on software (e.g., spoof and live fingerprint images present different textural properties such as morphology, smoothness, and orientation [40]), while others might require additional hardware (e.g., using an additional sensor to measure the warmth of a finger). Some examples of challenge-response mechanisms are to require users to read a randomly generated phrase for voice recognition or nod their heads for face recognition.

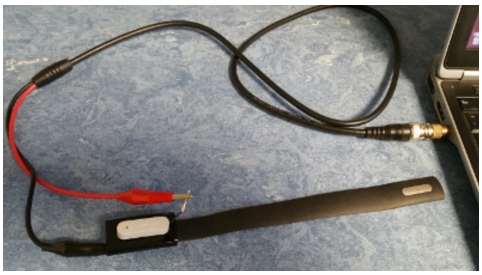
Scalable Attacks. Although research has focused primarily on presentation attacks, PAD is an arms race. Once attackers become aware of a new PAD technique, they will try to improve their artifacts to replicate the required characteristics. When approaching adoption of biometrics at scale, organisations (and fraudsters too) must consider corresponding scalability of attacks. In particular, zero-effort and presentation attacks are not easily scalable, as they require physical access to the biometric sensor. To conduct such attacks at scale, an adversary needs to be able to access several of these devices (e.g., by stealing them), which is impractical in realistic settings.

In modern mobile biometric systems, malware results in a more profitable attack vector. Malware could intercept and alter biometric measurements, or other information while it is being processed on the device, or potentially even steal user templates. Furthermore, an adversary that controls another legitimate application on user's device might be able to use different side-channels, such as gyroscope or battery usage to infer information about the user. Recent examples of real-world attacks confirm the importance of considering such attack vectors. Michalevsky et al. [41], have shown that mobile phone gyroscopes can be used to reconstruct speech. Another study [42] reports that most malware is used to steal user credentials (e.g., email/bank accounts), that are later sold on the black market. Since malware infections grant to the adversaries the possibility to reach a very large pool of devices



(a) Reconstructing a user's face using photographs and 3D printing technology.

(b) Spoofing fingerprints with silicon reconstructions.



(c) Spoofing ECG biometrics for a fitness tracker (Nymi Band[a]), using a laptop and an audio cable [36].

[a]http://nymi.com/

Fig. 10: Examples of presentation attacks on biometric systems.

(up to millions [43]), they represent a scalable threat, and a lucrative opportunity for criminals.

Integrity of Enrolment. One problem that is not being addressed yet is the malicious enrolment with identity attributes of another individual, and related risks of identity theft. In this case, an adversary is able to obtain the credentials required for enrolment (i.e. by stealing someone else's credentials), and use these to enrol their own biometrics as belonging to the individual whose credentials have been stolen. In the US, financial losses caused by identity theft totalled up to $15 billion in 2014, targeting more than 17 million citizens [44].

The identity assurance provided by the biometric system relies on the assurance provided by the identity proofing procedures at enrolment. Even though organisations such as NIST [45] and CESG [46] have started addressing the problem of identity proofing, ensuring an appropriate level of assurance of the user identity is challenging and depends on the intended use cases of the biometric system. In financial services, many banks are under regulatory requirements to collect and validate information about consumers – Know Your Customer (KYC) – prior to opening accounts [47]. These "rooted" forms of identity are often established by governments at a specific moment in time, and usually involve in-person interaction between an identity authority and the user. Hence, the basis for strong identity assertion within the industry is already present, but is difficult from an operational standpoint, due to the discrepancy between digital/mobile biometric enrolment processes and physical/manual KYC procedures.

Governments are also attempting to define policies for establishing unique identities, and a variety of government ID digitisation initiatives are taking place (e.g., e-Identification[6], UIDAI[7], GOV.UK Verify[8], BankID[9]). Secure assertion of user identity and related authentication are fundamental ways to mitigate the threats of identity theft, and should be accounted for during the design of a biometric system.

Discussion. In Table IV, we summarise how FIDO UAF and BOPS approach security analysis in their specifications. Table IV shows a comparison of the security objectives they identified, and the measures adopted to achieve them. Table IV shows that the main focus of the industry is on the network communication rather than the protection from attacks at the sensor. This shows that the standards correctly invested more effort in protection from scalable attacks. On the other hand, guidelines for attacks at the sensor are lacking, partly due to the fact that they are hard to evaluate in a quantifiable way.

As distributed architectures become the predominant deployment model for biometric authentication in financial services, threat analyses should focus more on the client application, which becomes more likely to be the target of an attack [50]. We summarise in the following a list of security insights that resulted from our research, and that we believe will be significant in future deployments of biometric systems:

- *Monitoring of authentication requests*. In both centralised and distributed models, monitoring of accesses (both at the server and in the client) can help for blocking adversaries sending multiple authentication attempts (as in brute-force attacks).
- *Access control*. Standard tools such as intrusion detection and firewalls should be obligatory on servers, as these machines represent the most profitable point of attack (in particular in centralised models).
- *Protection from malware*. Particularly in distributed models, client software should contain malware and rooting detection capabilities. Deployment of mechanism for the protection of the integrity and confidentiality of data storage and code execution will be fundamental for the security of biometric systems (i.e., Trusted Execution Environments [48] and Secure Elements [49]).
- *Integrated solutions*. Security threats can and should be

[6]http://ec.europa.eu/digital-single-market/en/e-identification
[7]http://uidai.gov.in
[8]http://gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify
[9]http://bankid.com/en/

TABLE IV: Measures adopted by the FIDO UAF and BOPS standards to obtain the security objectives.

Objective	FIDO UAF	BOPS
Presentation attack detection	Liveness detection suggested in the security guidelines	Liveness detection required. Level of detection decided by the organisation.
Secure communication (pre-enrolment)	Pre-loaded TLS certificate	Pre-loaded TLS certificate
Secure communication (post-enrolment)	One-way TLS communication	Two-way TLS communication
Secure enrolment	-	Based on pre-existing identities of external services
Client Data Protection	File encryption suggested for protection of keys and templates	File encryption suggested for protection of keys and templates
Client side tamper protection	Trusted Execution Environment [48] and Secure Element [49] suggested in the security guidelines	-
Biometric sensor DoS/replay resistance	Nonces in enrolment and authentication protocol	Nonces in enrolment protocol, intrusion detection afterwards

mitigated with deployment of multi-factor or multi-layer solutions, that considerably improve the confidence in the authentication.

Systematic evaluation of biometric systems remains a very challenging task. Despite the growing body of research on the topic, further improvements and standardisation is needed in the future, both from industry and academia.

FACTOR 5: PRIVACY

With biometrics becoming more widespread, protection and privacy of biometric data has become an increasingly important subject of discussion across academia, industry and governments. Countermeasures for password leaks are straightforward, as passwords/accounts can be revoked or changed. However, in the case of a comparable theft of biometric data, the implications on the privacy of individuals are far more significant, due to the permanence of the underlying biometric characteristics (i.e., an individual's face, finger or iris). Since biometric templates are generally linked to users' personally identifiable information, which increases the threat to user privacy.

In this section, we analyse how privacy issues related to biometrics have been addressed by academia and industry groups and also share perspectives from financial services professionals and users.

Protection of Biometric Data. Protection of biometric template privacy is a very different issue than protection of a password. In fact, even if biometrics are permanent, when measuring a biometric characteristic, each measurement suffers from a noise component (e.g., ageing, environment, sensor quality), that causes slight fluctuations from each other (*intra-subject* variations). These differences are dealt with at an algorithmic level, in such a way that sufficiently similar samples can be matched together. Differently from passwords, these fluctuations in the biometric measurements imply that data protection cannot be addressed by traditional cryptographic methods (i.e., hashing and salting). Measures known as biometric template protection attempt to solve this issue by

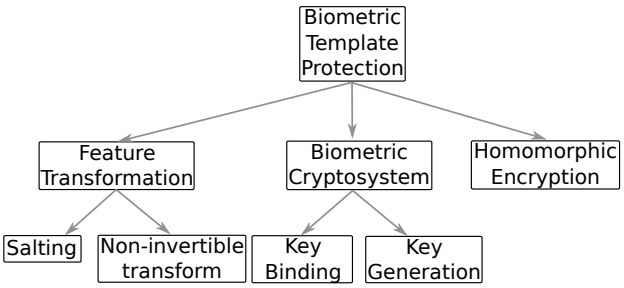


Fig. 11: Overview of biometric template protection schemes.

applying transformations to the biometric template before it is stored during enrolment. These protection measures ensure that an adversary cannot easily retrieve the original biometric template from its protected reference (*noninvertibility*), cannot obtain the original biometric template from multiple-instances of protected biometric reference derived from the same individual (*revocability*), and cannot discover whether two or more instances of the protected biometric template were derived from the same biometric trait of a user (*nonlinkability*) [51].

Two main methods for biometric template protection have been investigated: (i) feature transformation and (ii) biometric cryptosystems, we report in Figure 11 a taxonomy of such approaches. The principle behind feature transformation approaches is that the transformation on the template should behave like a hash function that can accept noise in its input data. Biometrics cryptosystems use error correcting codes to transform the original template into a *secure sketch*. The secure sketch is not sufficient to reconstruct the original template, but is used in combination with the biometric features provided by the user during recognition to perform the matching. In both approaches, usually a secret (e.g. keys [52], transformation parameters [53]) grants the noninvertibility. Disclosure of the secret can compromise the biometric data of the user, as adversaries can (to some extent) reconstruct the original template if they obtains the secret [52]. Nowadays, template protection schemes involve a degradation of recognition accuracy, since these schemes need to add tolerance to the

discriminatory information present in biometric templates. An emerging approach is homomorphic encryption, which allows arithmetic operations to be performed on encrypted data, without the need to ever uncover the plain biometric template. An implementation of homomorphic encryption for biometric templates is presented by Gomez Barrero et al. [54]. Unfortunately, homomorphic encryption comes at the cost of increased computation time which might not be presently suitable in real-world mobile scenarios.

Industry Protocols and Regulations. Recently, ISO addressed protection of biometric information with ISO/IEC 24745 [55]. However, FIDO UAF and BOPS do not mention any template protection requirement. In these standards, biometric authentication takes place locally on users' devices, and unlocks a stronger secret (*key*) that is used to authenticate users to the third-party application. Privacy is additionally supported by the choice to not assign unique device identifiers within the protocols, ensuring that third-parties cannot collaborate on identifying a user's device.

Analysing the regulatory scenario we identified two main trends in laws and regulations around biometrics in financial services. The first regulatory trend is to support authentication and data security in the context of online payments (e.g., Revised Payment Services Directive, PSD2 [56]). The European Banking Authority supports biometrics as a factor for authentication in their proposed regulatory technical standard [57] implementing PSD2. The second trend consists in regulating biometric data as personal identifiable or sensitive information under a country's data privacy or data protection laws. Sensitive data regulations, such as the General Data Protection Regulation [58], require user's express consent for the use of their biometric data, making sure that it is transparent to the user what rights they are granting. A concern that industry needs to take into account is that data protection laws governing biometrics are not uniform globally. Several data protection laws have varying levels of requirements surrounding user consent, storage and retention of biometric data, and security of the technologies that maintain such data.

Industry Perceptions. Our survey highlighted that, industry professionals identify as primary concerns both data breach risks and user/regulator privacy considerations. Most of them ***identified reputational damage as the main concern (75%)***, and a similar portion believes that ***biometric data leaks could stop the users from using the system (72%)***. Many respondents reported distributed models as an architectural choice that would mitigate these concerns. Regarding the regulatory environment, respondents confirmed their concerns. ***81% of industry professionals in our survey believe that regulatory environment influences design of biometric solutions*** (although 62% reported that the changing regulations will not harm long-term investments), and ***57% believe that privacy concerns will become more pronounced as biometrics gain popularity***. Overall, respondents seemed comfortable with current biometric regulations. However, conformance to and assessment of privacy by design/data protection laws remains ambiguous, and should be addressed in more detail in the future to drive wider adoption of biometrics in the industry.

VI. Conclusion

Financial services are slowly moving towards the adoption of biometrics for authentication. Years of biometric research highlighted the advantages of biometrics and their potential to improve convenience and security for users. However, the deployment process needs to be performed in a thoughtful and comprehensive manner. In this paper, we review and systematise knowledge on the current state of mobile biometric recognition systems in the financial services industry. We gather opinions and perceptions from a variety of stakeholders with two user studies: one spanning three months and including 449 users of a real-world deployed biometrics system, and the other which included financial services industry professionals. In addition, we review the related academic literature and analyse industry standards and regulations.

Our analysis shows that there are discrepancies in the opinions of different stakeholders regarding various aspects of biometric systems. Some of the reasons for the gaps include inexperience (familiarity with biometrics) and background (user- or fraud prevention-oriented). These gaps cause a slowdown in deployment of biometric systems, as confirmed by our survey: 88% of individuals will take decisions regarding biometric implementations, compared to 36% with knowledge of biometrics. This becomes even more important when considering that 66% of the surveyed companies plan to deploy a biometric system within 5 years.

In order to help stakeholders fill these gaps, we organise the information into the Five Factor Framework, that should be used when deploying mobile-based biometric systems for financial services use cases. For each factor, we outline the current trends and main challenges that should be addressed to ensure a successful deployment of the biometric system. We encourage industry professionals to leverage our framework to analyse and support decisions about the biometric systems they are deploying. This will enable decision makers with competing priorities to have a clear view of how one priority may support or conflict with another. We hope our framework will promote more effective collaboration, as it provides the structure necessary to engage with the complex topic of mobile biometric system deployment.

References

[1] CapGemini, *World payments report*, http://worldpaymentsreport.com/download, [online; accessed 19-July-2016], 2014.

[2] Federal Reserve Board of Governors, *Consumers and mobile financial services*, http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201603.pdf, [online; accessed 12-March-2017], 2016.

[3] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *IEEE Symposium on Security and Privacy (S&P)*, 2012.

[4] Dashlane, *Online overload: It's worse than you thought*, http://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/, [online; accessed 17-November-2016], 2014.

[5] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. F. Wang, "The tangled web of password reuse," in *Network and Distributed System Security Symposium (NDSS)*, 2014, pp. 23–26.

[6] B. Ur, S. M. Segreti, L. Bauer, N. Christin, L. F. Cranor, S. Komanduri, D. Kurilova, M. L. Mazurek, W. Melicher, and R. Shay, "Measuring real-world accuracies and biases in modeling password guessability," in *USENIX Security Symposium (USENIX)*, 2015, pp. 463–481.

[7] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, "Does my password go up to eleven? the impact of password meters on password selection.," in *ACM Conference on Human Factors in Computing Systems (CHI)*, 2013, pp. 2379–2388.

[8] Centrify, *Centrify survey results*, http://centrify.com/downloads/public/Centrify-Password-Survey-Summary.pdf, [online; accessed 17-November-2016], 2015.

[9] B. Stock and M. Johns, "Protecting users against xss-based password manager abuse," in *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2014.

[10] Z. Li, W. He, D. Akhawe, and D. Song, "The emperors new password manager: Security analysis of web-based password managers," in *USENIX Security Symposium (USENIX)*, 2014.

[11] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2015.

[12] D. An, *Find out how you stack up to new industry benchmarks for mobile page speed*, http://thinkwithgoogle.com/articles/mobile-page-speed-new-industry-benchmarks.html, [online; accessed 12-March-2017], 2017.

[13] Mastercard, *Mastercard identity check to simplify and strengthen online shopping*, http://newsroom.mastercard.com/press-releases/mastercard-identity-check-to-simplify-and-strengthen-online-shopping/, [online; accessed 17-November-2016], 2015.

[14] LexisNexis, *True cost of fraud study*, http://lexisnexis.com/risk/downloads/assets/true-cost-fraud-2016.pdf, [online; accessed 17-November-2016], 2016.

[15] World Economic Forum, *A blueprint for digital identity*, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf, [online; accessed 17-November-2016], 2016.

[16] A. K. Jain, A. Ross, and K. Nandakumar, *Introduction to biometrics*. Springer Science & Business Media, 2011.

[17] *Information technology – vocabulary – part 37: Biometrics*, ISO/IEC 2382-37, 2012.

[18] EMVCo, *3-D Secure - protocol and core functions specification*, http://emvco.com/specifications.aspx?id=299, [online; accessed 12-March-2017], 2016.

[19] J. Bonneau and S. Preibusch, "The password thicket: Technical and market failures in human authentication on the web," in *Workshop on the Economics of Information Security (WEIS)*, 2010.

[20] D. Arp, M. Spreitzenbarth, M. Hübner, H. Gascon, and K. Rieck, "Drebin: Effective and explainable detection of android malware in your pocket," *Symposium on Network and Distributed System Security (NDSS)*, 2014.

[21] *Draft NIST digital identity guidelines - authentication and lifecycle management*, NIST Special Publication 800-63B, 2016.

[22] S. J. Murdoch and R. Anderson, "Verified by Visa and Mastercard Securecode: or, how not to design authentication," in *International Conference on Financial Cryptography and Data Security*, 2010, pp. 336–342.

[23] HSBC, *HSBC targets faster customer enrolment with "selfie" verification technology*, http://about.hsbc.co.uk/~/media/uk/en/news-and-media/cmb/160906-hsbc-news-release-hsbc-targets-faster-customer-enrolment-with-selfie-verification-technology.pdf, [online; accessed 12-March-2017], 2016.

[24] FIDO Alliance, *Uaf v1.1 specifications*, http://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202.zip, [online; accessed 12-March-2017], 2017.

[25] *Standard for Biometric Open Protocol*, IEEE Std. 2410, 2015.

[26] NIST, *Usability and biometrics: Ensuring successful biometric systems*, http://nist.gov/sites/default/files/usability_and_biometrics_final2.pdf, [online; accessed 12-March-2017], 2008.

[27] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, "Evaluating behavioral biometrics for continuous authentication: Challenges and metrics," in *ACM Asia Conference on Computer and Communications Security (ASIACCS)*, 2017.

[28] *Information technology - biometric performance testing and reporting*, ISO/IEC 19795, 2006.

[29] *Information technology - biometric presentation attack detection - part 3: Testing and reporting*, ISO/IEC DIS 30107-3, 2016.

[30] M.-H. Lim and P. C. Yuen, "Entropy measurement for biometric verification systems," *IEEE Transactions on Cybernetics*, vol. 46, no. 5, pp. 1065–1077, 2016.

[31] A. Seffah, M. Donyaee, R. B. Kline, and H. K. Padda, "Usability measurement and metrics: A consolidated model," *Software Quality Journal*, vol. 14, no. 2, pp. 159–178, 2006.

[32] A. Dix, *Human-computer interaction*. Springer, 2009.

[33] A. P. Parasuraman, "Technology readiness index (TRI)," *Journal of Service Research*, vol. 2, no. 4, pp. 307–320, 2000.

[34] A. Ross and A. Othman, "Visual cryptography for biometric privacy," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 70–81, 2011.

[35] Global Web Index, *Digital consumers own 3.64 connected devices*, http://globalwebindex.net/blog/digital-consumers - own - 3 . 64 - connected - devices, [online; accessed 12-March-2017], 2016.

[36] S. Eberz, A. Patané, N. Paoletti, M. Kwiatkowska, M. Roeschlin, and I. Martinovic, "Broken hearted: How to attack ecg biometrics," in *Network and Distributed System Security Symposium (NDSS)*, 2017.

[37] The Guardian, *Hacker fakes german minister's fingerprints using photos of her hands*, https : / / www . theguardian.com/technology/2014/dec/30/hacker-fakes-german - ministers - fingerprints - using - photos - of - her - hands, [online; accessed 12-March-2017], 2014.

[38] N. Evans, S. Z. Li, S. Marcel, and A. Ross, "Guest editorial: Special issue on biometric spoofing and countermeasures," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 4, pp. 699–702, 2015.

[39] I. Sluganovic, M. Roeschlin, K. B. Rasmussen, and I. Martinovic, "Using reflexive eye movements for fast challenge-response authentication," in *ACM Conference on Computer and Communications Security (CCS)*, 2016.

[40] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, pp. 1–36, 2014.

[41] Y. Michalevsky, D. Boneh, and G. Nakibly, "Gyrophone: Recognizing speech from gyroscope signals," in *USENIX Security Symposium (USENIX)*, 2014, pp. 1053–1067.

[42] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *First ACM Workshop on Security and Privacy in Smartphones and Mobile Devices (SPSM)*, 2011, pp. 3–14.

[43] Check Point Software Technologies, *Hummingbad case study*, http://blog.checkpoint.com/wp-content/uploads/2016 / 07 / HummingBad - Research - report_FINAL - 62916.pdf, [online; accessed 12-March-2017], 2016.

[44] US Department of Justice, *Victims of identity theft*, http://bjs.gov/content/pub/pdf/vit14.pdf, [online; accessed 12-March-2017], 2015.

[45] *Draft NIST digital identity guidelines*, NIST Special Publication 800-63-3, 2016.

[46] CESG, *Identity proofing and verification of an individual*, http : / / gov . uk / government / uploads / system / uploads / attachment_data / file / 370033 / GPG_45_identity_proofing_v2_3_July_2014.pdf, [online; accessed 12-March-2017], 2014.

[47] PWC, *Know your customer: Quick reference guide*, http://pwc.com/gx/en/financial - services/publications/assets/pwc - anti - money - laundering - 2016.pdf, [online; accessed 12-March-2017], 2016.

[48] J.-E. Ekberg, K. Kostiainen, and N. Asokan, "Trusted execution environments on mobile devices," in *ACM Conference on Computer and Communications Security (CCS)*, ACM, 2013, pp. 1497–1498.

[49] M. Reveilhac and M. Pasquet, "Promising secure element alternatives for nfc technology," in *First International Workshop on Near Field Communication*, 2009, pp. 75–80.

[50] Verizon, *Data breach investigation report*, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/, [online; accessed 12-March-2017], 2016.

[51] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 88–100, 2015.

[52] M. Roeschlin, I. Sluganovic, I. Martinovic, G. Tsudik, and K. B. Rasmmussen, "Generating secret keys from biometric body impedance measurements," in *ACM CCS Workshop on Privacy in Electronic Society (WPES)*, 2016.

[53] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 744–757, 2007.

[54] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on homomorphic encryption," *Pattern Recognition*, vol. 67, pp. 149–163, 2017.

[55] *Information technology - security techniques - biometric information protection*, ISO/IEC 24745, 2011.

[56] European Parliament, *Directive 2015/2366 on payment services in the internal market*, 2015.

[57] European Banking Association, *Draft regulatory technical standards on strong customer authentication and common and secure communication*, http://eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+\%28EBA-RTS-2017-02\%29.pdf, [online; accessed 12-March-2017], 2017.

[58] European Parliament, *Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, 2016.