Assessment of Remote Biometric Authentication Systems: Another Take on the Quest to Replace Passwords

Daniel Köhler
Faculty of Digital Engineering
Hasso-Plattner-Institute
Potsdam, Germany
daniel.koehler@hpi.de

Eric Klieme
Faculty of Digital Engineering
Hasso-Plattner-Institute
Potsdam, Germany
eric.klieme@hpi.de

Matthias Kreuseler
Faculty of Engineering
University Wismar
Wismar, Germany

Feng Cheng
Faculty of Digital Engineering
Hasso-Plattner-Institute
Potsdam, Germany

Christoph Meinel
Faculty of Digital Engineering
Hasso-Plattner-Institute
Potsdam, Germany

***Abstract*—Passwords are often criticized due to being prone to misuses such as bad password creation and management practices. Experts usually advise using other forms of authentication. While there are plenty of alternative authentication methods available, an overall assessment often proves to be challenging. This is because of aspects such as differences in security techniques, different applicability of the system, or varying difficulties of implementation. To tackle the issue of comparing different authentication systems, unified criteria are needed. Bonneau et al. proposed a framework for comparing authentication schemes in their "*The Quest to Replace Passwords*". We contribute to the quest by providing information and assessment on the previously unassessed Remote Biometric Authentication Systems, thus increasing the variety of analyzed systems. We achieve this by analyzing six exemplary implementations. To enable proper evaluation of the details of that new category of authentication schemes, this work furthermore expands the framework by the two aspects *Resilient-to-Biometric-Loss* and *No-Trusted-Execution-Environments*.**

***Index Terms*—authentication, smartphones, biometric, remote**

I. Introduction

The hassle of authentication is one of the problems that are still prominent in the security industry [1]. Even though passwords can be used in a secure way, actually pursuing password best-practices such as using complex passwords is often too much effort for the everyday user. Thus, many problems deriving from insecure passwords still remain [2]. For years, new authentication principles have been developed. Be it based on *knowledge*, *possession*, or *biometry*. The *perfect one* has not yet been found. While this paper does not attempt to create or identify the perfect authentication mechanism, it provides insights into the assessment of a - previously unassessed - group of authentication systems, the systems for remote biometric authentication. Remote biometric authentication refers to the attempt of using biometric authentication for distant, remote applications such as web applications. Section II-A elaborates on Remote Biometric Authentication (*RBA*) Systems and the underlying concepts.

For many years, one main drawback of biometric authentication systems was the fact that biometric sensors were not broadly available. With the successes and innovations surrounding modern smartphones, it has been achieved that almost every person carries around their personal biometric sensors, built directly into their smartphones.

How can those sensors be used to simplify the average user's life? This question is answered by well-known companies such as Google or Microsoft with their applications for passwordless authentication. Are those systems a valuable and secure alternative to the ancient password though?

One approach to compare and evaluate authentication systems has been made in 2012 with a framework proposed by Bonneau et al. in their paper *The Quest to Replace Passwords* [3]. Since the framework has been revisited in various valuable contributions [4] [5] [6]. The different contributions have refined the framework and expanded the number of evaluated authentication schemes. In 2016, Mayer et al. have transformed the literature-version of the original framework into an online application, *ACCESS* [6]. The *Authentication ChoiCE Support System* leverages the potential of performed analysis on the different authentication systems into a valuable source of information for decision-makers. While ACCESS features plenty different authentication principles and their various ratings, ranging from *Associative Questions* [6] or *passwords* [3] up to *Yubikey* [3], it currently lacks the availability of information on systems for remote biometric authentication. To tackle this issue, this work provides a threefold contribution:

- Proposal of two new sub-features to the framework especially required for (remote) biometric authentication principles in Section III: *Resilient-to-Biometric-Loss* and *No-Trusted-Execution-Environment*. Alongside this work,

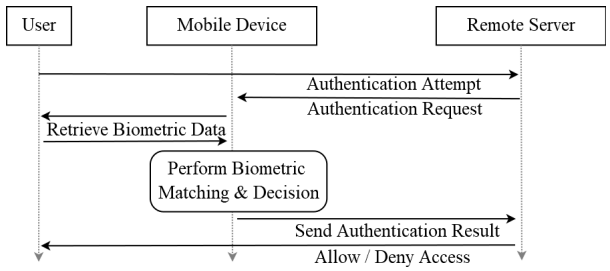

Fig. 1. Overview of the authentication process for RBA with the biometric matching being performed on the mobile device.

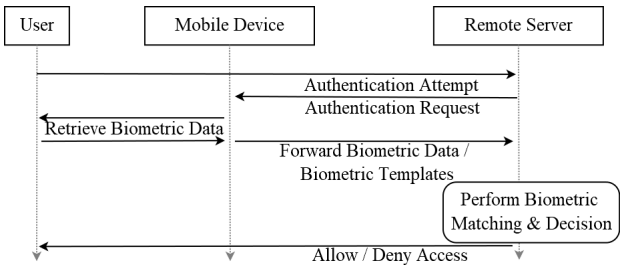

Fig. 2. Overview of the authentication process for RBA with the biometric matching being performed on the server.

the features are proposed to be added into the ACCESS platform [1].

- Analysis of six practical implementations of remote biometric authentication systems, thus increasing the diversity and variety of analyzed authentication schemes along the *Quest to replace Passwords* in Section IV.
- Integration of the assessment and results into to the aforementioned *ACCESS* Database.

II. Background

To ensure a proper understanding of the underlying principles and the target systems, Section II-A introduces the core concepts of Remote Biometric Authentication while Section II-B introduces the underlying framework from related work, used to analyze the systems.

A. Remote Biometric Authentication Systems

This work considers remote biometric authentication as those authentication attempts that work passwordless between a user and a remote server. Upon an authentication attempt, the authentication system requires biometric data that are input by a user into their mobile device. For the specified approach, there are multiple architecture models in which remote biometric authentication systems could be deployed.

The processes outlined in Figures 1 & 2 show the two core architectures of remote biometric authentication systems. The authentication is performed between the user, their mobile device, and a remote server. The main differences separating both architectures are, where the biometric matching is performed. Either it is performed on the mobile device in which case the server will only receive the authentication result: *Successful* or *Failed*. In the opposite case, the server is provided the biometric data and performs the biometric assessment itself. However, with this scenario, the (secured) biometric data has to be transferred via the Internet in one way or another. Besides the two basic implementations, there are sophisticated authentication architectures which we have though not yet seen in practice.

In contrast to the RBA, one example for *local* biometric authentication could be considered a person using their fingerprint to unlock their smartphone. In that case, the system that is being accessed is the same one that has full control over the authentication attempt and the connected biometric matching and decision-making.

Important is, to keep in mind, that - in contrast to e.g. password authentication - biometric authentication is always a question of probability [7]. The retrieved biometric data during the current authentication attempt is compared against the biometric templates from the system's storage. The similarity of both sets of data is measured. Should the similarity be higher than a threshold value, the authentication attempt is rated successful and the user is authenticated. The sovereignty for said biometric matching should lie within the backend server. The main reason for this is that a server that is performing the biometric matching and decision-making itself would be able to determine the system's security by adjusting the thresholds for the biometric decision. If the biometric decision is performed on a mobile device, the server cannot judge on the security of that device.

B. Comparing Authentication Systems

In their 2012 work *The Quest to Replace Passwords*, Bonneau et al. proposed a framework to assess authentication schemes [8]. The proposed criteria, so-called benefits, are used to rate the schemes in three different categories: *Usability*, *Security* and *Deployability*. Inside those categories, they defined 25 benefits (Usability: 8, Security: 11, Deployability: 6). The evaluated system would then be rated on whether the scheme was *Offering the benefit*, *Not offering the Benefit* or *Almost Offering the Benefit* (*Quasi-Offering the Benefit*). For the original 36 rated authentication schemes, Bonneau et al. presented the results in a comprehensive table. Some of the examples of the systems originally compared by Bonneau et al. in the original work were the traditional *Password* [9], *Password Managers* (e.g. Firefox [2]) or even Hardware Tokens such as *Yubikey* [3].

Based on this original work, Renaud et al. have suggested *ACCESS* (*Authentication ChoiCE Support System*), an abstract framework based on the original criteria by Bonneau et al. Following, Mayer et al. have presented their first realization of the *ACCESS* system in their work *Supporting Decision Makers in Choosing Suitable Authentication Schemes* [6]. Thereby,

[1] *ACCESS Platform*: https://access.secuso.org/

[2] Firefox Browser: https://www.mozilla.org/de/firefox/

[3] *Yubikey, 2015, "The YubiKey Manual", https://www.yubico.com/wp-content/uploads/2015/03/YubiKeyManual_v3.4.pdf, Retrieved: June 11th 2020*

the authors have created an online version of the framework. With that version, the authors have further chosen to step back from the original differentiation of *Almost- (Quasi-) Offering the Benefits*. Instead, they proposed to introduce multiple sub-criteria for those aspects. One example is the benefit of *Nothing-to-Carry* from the original framework. In the ACCESS platform it has been refined to feature sub-benefits which can be rewarded individually such as *No-Object-to-Carry*, *Phone-to-Carry*, *SmartCard-to-Carry*, *Document-to-Carry* or *Device-to-Carry*. This way, the assessment - and in turn the retrieved results - can be investigated in higher detail compared to the original framework.

In further work, the authors improved on the platform, developing the newer version *ACCESSv2* [5]. The new platform contains three modules: (1) *Information Module*, which allows anybody to retrieve the information stored within the platform. (2) *Collaboration Module*, which allows people to contribute to the knowledge base. (3) *Decision Support Module*, which helps decision-makers in choosing the most suitable authentication scheme.

III. Extending the ACCESS Framework

While the original work already features the analysis of basic biometric authentication principles such as *Fingerprint, Iris* and *Voice*, that analysis is not entirely applicable to remote biometric authentication principles. This is due to the fact that with remote biometric authentication systems - as explained in Section II-A - more parties are involved in the authentication attempt. Which in turn brings up questions in regard to data security, or control about the authentication attempt. Therefore, this work proposes improvement on the framework in the areas of the criterions *No-Trusted-Third-Party* [3] and *Resilient-to-Internal-Observation* [3]. *Resilient-to-Internal-Observation* consists of the sub-features *Resilient-to-Eavesdropping* [5] and *Resilient-to-Malware* [5].

Within the *ACCESS* platform[4], the features are currently described as:

No-Trusted-Third-Party The scheme does not involve third parties, which might compromise the prover's security or privacy when being attacked or becoming untrustworthy for any other reason.

Resilient-to-Internal-Observation This feature pertains to all observation of the user's input through the device itself. This includes malware, (e.g. keyloggers) and intercepting/analyzing the communication between prover and verifier.

Resilient-to-Eavesdropping The attacker is not able to intercept the communication between the client and server to obtain sensitive information that will enable him to identify the identity of the user before the verifier. For this feature, it is assumed that the attacker is able to bypass Transport Layer Security (TLS). For example, through the certification authority or through Man-in-the-Middle attacks and can thus access the plain-text communication of both communication partners.

Resilient-to-Malware Even if the attacker uses malware to record inputs and outputs from the device of the user and evaluates it, they do not manage to obtain the required credentials of the user. We assume that the attacker is able to infect devices that we use in our everyday life such as, personal computers and smartphones with malicious software, but they are not able to modify closed systems such as hardware tokens.

To enable the assessment of a remote biometric authentication application, this work proposes to add two new features. *No-Trusted-Execution-Modules* (c.f. section III-A) is supposed to expand on the interpretation of Third-Party-Systems. From the server's point of view, a mobile device should be considered as a Third-Party. Further, *Resilient-to-Biometric-Loss* should be considered as an expansion of the classifiers for Internal-Observation. (c.f. section III-B)

No-Trusted-Execution-Modules This feature requires that all tasks to perform the authentication are performed in the sovereignty of the server.

Resilient-to-Biometric-Loss This feature requires the authentication scheme to be free of transfer of biometric data - even in an encrypted or templated form - through potentially unsecured channels such as the internet.

A. No-Trusted-Execution-Modules

With authentication systems such as e.g. *OpenID* [3] or *FacebookConnect* [3], it is entirely obvious that a third party is integrated into the authentication process. Therefore, the feature of *No-Trusted-Third-Party* is not assigned. However, for some Remote Biometric Authentication Systems, the existence of a third-party can not be as clearly defined. As described in Section II-A, an authentication in fact happens between three parties: *User*, *Mobile Device* and *Server*.

From the server's point of view, the mobile device in charge of the biometric matching should be considered a Third-Party. As the current definition of Third-Party differs from the above scenario, this work proposes the integration of the new sub-classifier *No-Trusted-Execution-Modules* for the group of *Resilient-To-Third-Party*. By proposing the feature as described above, the same feature can similarly be used for authentication schemes where Trusted-Execution-Environments of other systems might be used.

The applicability of this classifier is to be rated on whether the server in its role as data-owner is performing the actual process of authentication by itself. If - for that crucial assessment - trust has to be shared with a user's device, or any other *trusted* environment, the specific authentication system is not awarded the classifier.

[4] *ACCESS Platform*: https://access.secuso.org/

This feature differs from the former *No-Trusted-Third-Party*: Previously, only a third entity in the authentication process would be considered a *Third-Party*. However, *No-Trusted-Execution-Environment* opens up for the identification of Third-Party-Like entities in-between a communication affecting only the user and the service provider. Taken the exemplary password-login from a user's mobile device, the mobile device itself is not providing an impact in the authentication. In that case, the authentication is featuring *No-Trusted-Third-Party* as well as *No-Trusted-Execution-Environment*. If a user was to perform their authentication to a third-party service such as e.g. Facebook-Connect, the authentication was obviously not rated *No-Trusted-Third-Party*. However, if a user was to perform a biometric authentication attempt in-between their mobile device and a remote server, their mobile device might perform the biometric authentication and only send the authentication result to the server. In that way, a *Trusted-Execution-Environment* other than the server itself decides about whether the user is actually authenticated.

B. Resilient-to-Biometric-Loss

Security of the biometric data is one of the most important aspects during the analysis of biometric authentication systems [10]. Contrasting to authentication mechanisms using e.g. passwords, the results of potential data loss are far worse. If a password happens to be compromised due to whichever reason, the user can easily issue a new password. However, with biometric data, a compromise of the transferred data will lead to a user potentially never being able to use those biometric treats again. Hence, with biometric systems, not only shall they be *Resilient-To-Eavesdropping*, but they shall rather be rated with a feature such as *Resilient-to-Biometric-Loss*.

The major reason for the proposal of a new feature especially for biometric systems is the following: Currently, features such as *Resilient-to-Eavesdropping* primarily take into account whether the current authentication attempt could be broken. If the only chance to break the security was to crack proper encryption in 10-20 years, the system is regarded as resilient. Handling biometric data however, this assumption is required to change. Whenever using biometric data, administrators should be aware that once (raw) biometric data is compromised, it is most probably compromised for the user's entire life.

Therefore, one important aspect to note when considering whether a system fulfills the feature of biometric secrecy is the following: In many cases, data will be considered *secure* if e.g. the transmission method is properly secured and can not be broken with current knowledge/technology. One example would be a situation in which one communication partner would send (his) biometric data encrypted using the recipient's 8192-bit RSA key. This communication is currently considered *secure* because most probably there will be no method to break the used encryption in the upcoming years. However, for years computers have improved their computation strength and whenever that computational power would come close to impacting the currently used security mechanisms, one's reaction was to increase the key length. This works for secure information that is likely to have changed in e.g. 20 years. Whichever e.g. encrypted password gets intercepted today and cracked in the future is most likely already outdated once the encryption is cracked. However, as previously outlined, biometric data does not share the same (short) life-span. Instead, a (currently) secure transmission of biometric data might be intercepted today, cracked in the future, and still prove to be useful for the attacker [11], [12]. Therefore one main goal of biometric authentication systems should be to transfer no biometric data via a network. If that is given, the feature of *Resilient-to-Biometric-Loss* shall be assigned.

Biometric Security is an area of research that is strongly populated. Many approaches offer advanced security mechanisms for biometric authentication systems: **non-revertible, revokable Templates** offer the possibility to create templates from the biometric data which can not be used to forge the original biometric data from them. Further, those templates can be revoked once they might have been compromised [13]. One main goal should, therefore, be to design secure biometric applications that do not allow an attacker to recreate the original biometric data from any communication he can compromise [14].

IV. Analysis and Results

This section presents the performed analysis and the retrieved results on the exemplary implementations of remote biometric authentication schemes. We performed our analysis on six different systems, both proprietary and Open Source.

- **Microsoft Authenticator** [5] A wide-spread commercial product implementing FIDO-like principles. Fast Identity Online (FIDO) and in particular the standardized FIDO2[6]
- **ThumbSignIn** [7] ThumbSignIn is a commercial product, similarly implementing FIDO-like principles.
- **Gluu Server** [8] Gluu is an Open-Source software which Similarly to Microsoft Authenticator and ThumbSignIn implements FIDO-like principles.
- **Viridium** [9] Viridium offers Identity Solutions that enable FIDO-Certified passwordless authentication.
- **BioID** [10] Contrasting the previous systems, in their proprietary product, BioID does not implement the FIDO-Specification.
- **LastPass** [11] LastPass offers proprietary software that enables password-safe like applications on all of a users device. However, LastPass further offers support for passwordless biometric authentication.

While the full results of the analysis are to be available within the *ACCESS* platform, this work focuses on some of

[5]Webpage: https://www.microsoft.com/authenticator

[6]Webpage: https://fidoalliance.org/fido2/ specification aim at allowing easier authentication in the web.

[7]Webpage: https://thumbsignin.com/

[8]Webpage: https://www.gluu.org/

[9]Webpage: https://veridiumid.com/why-veridium/

[10]Webpage: https://www.bioid.com/

[11]Webpage: https://www.lastpass.com/de

the major aspects, especially highlighting the analysis based on the newly proposed criteria. Many other of the to-be-evaluated features are identical to the already evaluated biometric authentication methods from the ACCESS platform. One example of this is the criterion of *No-Secret-To-Remember*, which is similarly present with remote biometric authentication systems as it is with classic biometric authentication systems. The following Subchapter IV-A presents the results as Table IV-A, while the detailed analysis can be found in the Subsections succeeding the table.

A. Rating Results

The following graphical representation (Table IV-A) allows the identification of similarities and differences in-between the authentication schemes. In the original work by Bonneau et al. much more information was to be found in the table. However, for the sake of solely comparing different schemes amongst each other, the table representation has been streamlined. One of the aspects that are no longer contained is the depiction of whether a scheme or the feature of a scheme is considered *Better than Passwords*. The proposed representation is supposed to be as simple as possible to allow an easy overview.

The following sub-sections start by providing an in-depth analysis of the *Microsoft Authenticator* System. The following sections for the analysis of the other systems only provide a shorter analysis as a major amount of the analyzed benefits is equally applicable.

1) Analysis in-Depth: Microsoft Authenticator: When performing password-less login using biometric authentication with Microsoft Authenticator, a login attempt will trigger an authentication request to the user's phone. The user has to unlock their phone and approve the authentication attempt using their biometric authentication method of choice. This authentication falls back on the phone's built-in authentication mechanism which could - in theory - be a PIN instead of a biometric factor. However, as this work pursues the analysis of biometric systems, it is assumed that a biometric trait is used to use the mobile device's internal authentication [15]. The following paragraphs describe the analysis of Microsoft's Authenticator based on the criteria from the assessment framework.

The thorough, step-by-step analysis is omitted in this print due to space constrictions. The details of the analyzed criteria can be found in the *ACCESS* database. This section identifies some of the specific criteria for RBA-Systems using the example of Microsoft's Authenticator. Starting with the analysis of a few exemplary features which are already available in the database and meaningful for biometric authentication, *Scalable for Users* and *No Secret to Remember* are both assigned to the system. Those features are defined by the nature of password-less login systems using biometric authentication. Regarding the feature of *Physically Effortless*, most biometric authentication systems will not be considered as such. Specifically, this is because while working on a computer and using a mobile device to perform the biometric authentication, the process of performing the actual biometric assessment interrupts the user's workflow. Instead, the mechanism is rated the difficulty of *Type-to-Enter*. This is chosen as it depicts the effort that it takes to enter something into a device that requires some pressure to operate, which should correspond to the effort it takes to use a biometric authentication with a phone.

One specialty of biometric authentication is that errors will always be present. This is due to the biometric systems nature of matching for similarity [16]. Hence, biometric authentication schemes, in general, Cannot be rated *Not-Susceptible-to-Input-Errors*.

To rate the aspect of *No-Trusted-Third-Party* and the connected *No-Trusted-execution-Modules*, the authentication system and in particular the process of authentication has to be evaluated in detail. Microsoft's Authenticator adheres to the process proposed in the FIDO(2) authentication framework. During the *Registration Phase*, the authenticating device (e.g. the smartphone) creates a set of cryptographic keys. The public key is sent to the identity system (e.g. Azure Active Directory) and is stored in the user's profile at the identity provider. The private key is securely locked on the device, secured by the authentication factor of choice (e.g. biometrics). The process of an authentication attempt is hence similar to the abstract process described earlier in Figure 1 in Section II-A. During an *Authentication Attempt*, the identity system requests authentication and thus sends an authentication prompt to the user's device (e.g. the smartphone). The authentication prompt contains a cryptographic *nonce*. Upon receiving the authentication attempts, the device requests the user to authenticate himself e.g. by the means of biometric authentication. This local authentication unlocks the locally stored and secured private key that had initially been created. The provided *nonce* is being encrypted with the private key of the user and send back to the identity system where the user can be verified. [12]

In the outlined process, the assessment of the biometric treats provided by the suspected user happens solely on the device itself. Therefore, the connected servers and systems have to hand over the sovereignty of authentication to the third-party device. The security of the local biometric authentication on the device highly depends on the device itself. The availability of core security features such as liveness detection therefore cannot be guaranteed. Further, settings such as the threshold for the biometric decision making cannot be influenced by the server. The system relies on the authenticating module in the mobile device and is thus rated as **not** offering the *No-Trusted-Execution-Modules* benefit. Similarly, as no biometric data is transferred over any network, the scheme is rated as offering the feature of *Resilient-to-Biometric-Loss*.

2) ThumbSignIn: ThumbSignIn provides FIDO-based authentication services. This leads to many similarities to Microsoft Authenticator, especially in the registration and authentication progress. With ThumbSignIn relying on the use of built-in authentication mechanisms of the user's smartphones,

[12] *FIDO-Alliance, 2018, "Microsoft's Path to Passwordless", https://fidoalliance.org/Microsofts-path-to-passwordless-fido-authentication-for-windows-azure-active-directory/, Retrieved: April 30th 2020*

TABLE I
RESULTS FROM THE ANALYSIS OF THE PROPOSED APPLICATIONS. THE IN-DEPTH RESULTS ARE TO BE FOUND IN THE ACCESS DATABASE.

		Benefits	*Analyzed Systems*					
			MS Authenticator	*ThumbSignIn*	*Gluu*	*Viridium*	*BioID*	*LastPass*
Deployability	Accessible	Accessible-with-Read-Write-Impairments	x	x	x	x	x	x
		Accessible-with-Visual-Impairments	x	x	x	x		x
		Accessible-with-Physical-Impairments	x	x	x	x	x	x
		Negligible-Cost-per-User	x	x	x	x	x	x
		Server-Compatible						x
	Browser-Compatible	Compatible-to-Native-Browser	x	x	x	x	x	x
		Compatible-to-Extended-Browser	x	x	x	x	x	x
	Mature	Adopted-beyond-Academics	x	x	x	x	x	x
		Adopted-Repeatedly	x		x	x		x
		Adopted-in-Academics	x	x	x	x	x	x
		Non-Proprietary			x			
Security	Resilient-to-Physical-Oberservation	Resilient-to-Visual-Recording	x	x	x	x	x	x
		Resilient-to-Shoulder-Surfing	x	x	x	x	x	x
		Resilient-to-Residual-Traces-Recording	x	x	x	x	x	x
		Resilient-to-Sound-Recording	x	x	x	x	x	x
		Resilient-to-Targeted-Impersonation	x	x	x	x	x	x
		Resilient-to-Throttled-Guessing	x	x	x	x	x	x
		Resilient-to-Unthrottled-Guessing						
	Resilient-to-Internal-Observation	Resilient-to-Eavesdropping	x	x	x	x	x	
		Resilient-to-Biometric-Loss	**x**	**x**	**x**	**x**		x
		Resilient-to-Malware					x	
		Resilient-to-Leaks-from-Other-Verifiers	x	x	x	x	x	
		Resilient-to-Phishing	x	x	x	x	x	
		Resilient-to-Theft	x	x	x	x	x	x
	Resilient-to-Third-Party	No-Trusted-Third-Party	x		x	x	x	
		No-Trusted-Execution-Modules					**x**	
		Requiring-Explicit-Consent	x	x	x	x	x	x
		Unlinkable	x	x	x	x	x	x
Usability	Memorywise-Effortless	No-Secret-to-Remember	x	x	x	x	x	x
		One-Secret-to-Remember						
		More-than-One-Secret-to-Remember						
		Scalable-for-Users	x	x	x	x	x	x
	Nothing-to-Carry	No-Object-to-Carry						
		Phone-to-Carry	x	x	x	x	x	x
		SmartCard-to-Carry						
		Document-to-Carry						
		Device-to-Carry						
	Physically-Effortless	No-Physical-Effort						
		Speak-to-Enter						
		Type-to-Enter	x	x	x	x		x
		Scribble-to-Enter						
		Gesticulate-to-Enter					x	
		Easy-to-Learn	x	x	x	x		x
	Efficient-to-Use	No-Obstructive-Latency	x	x	x	x		x
		No-Fiddling-Tasks						
		No-Secret-to-Transcribe	x	x	x	x	x	x
	Infrequent-Errors	Not-Susceptible-to-Input-Errors						
		Not-Susceptible-to-Assignment-Errors						
		Not-Susceptible-to-Transmission-Errors	x	x	x	x		x
		Easy-Recovery-from-Loss	x	x	x	x	x	x

it is very similar to the internal process of Microsoft Authenticator. The major contrast between both, MS Authenticator and ThumbSignIn is that the ThumbSignIn products appear to be available only as Software-As-A-Service (SaaS), thus rendering the system furthermore dependent on another third-party service. Similarly to Microsoft's Authenticator, all biometric operations are performed on the mobile device itself, thus the scheme is rated as providing the feature of *Resilient-to-Biometric-Loss* however the scheme can hence not be rated *No-Trusted-Execution-Modules*.

3) Gluu Server: Gluu offers an Open-Source Identity and Access Management (IAM) solution, which provides all kinds of services to operate enterprise-grade architectures. Similarly to Microsoft's Authenticator, Gluu's passwordless authentication processes rely on the FIDO framework and principles. With that, they implement features such as e.g. cryptographic nonces or private and public key principles. Due to the close resemblance of Gluu's authentication process to Microsoft's

nearly all criteria are similarly assigned. The only difference lies in the fact that Gluu as an Open-Source Software is rated *Non-Proprietary* and *Adopted-Repeadetly*. Finally, as Gluu offers the full solution to be deployed on-premise and managed within a company, Gluu provides the benefit of *No-Trusted-Third-Party* [17]..

4) Viridium: As Viridium is FIDO2 specified, it shares a multitude of the criteria of the previously discussed schemes. Such is that no biometric data is transferred via the network (*Resilient-to-Biometric-Loss*) but also that they cannot be assigned *No-Trusted-Execution-Modules*. Similar to Microsoft and Gluu, Viridium offers on-premise installations thus applying the criterion *No-Trusted-Third-Party*. Further, as Viridium has been properly certified by the FIDO-Alliance, we rate it as *Adopted-Repeatedly*.

5) BioID: BioID is a german company offering authentication solutions either as Biometrics-as-a-Service or as on-premise systems. BioID's authentication is relying on the underlying biometric principle of face recognition [18].

BioID proves to be the outlier from the other assessed systems. Mainly because it does not rely on the usage of FIDO-like principles to perform the authentication. With BioID, a video feed from the user's webcam is sent to the server, where then the face recognition is performed. The authentication process hence follows process two from the previously described RBA processes in Figure 2. The data is evaluated on the corresponding server. Therefore the authenticating platform itself has the sovereignty over any authentication and is therefore assigned the feature *No-Trusted-Execution-Modules*. However, there are drawbacks to said solution as well. As authentication is performed on the server, the server needs to be provided with the corresponding biometric data. As far as was identified, the biometric data (pictures) is sent over an encrypted connection to the server. Once on the server, the data is being transformed into the irreversible biometric templates. Therefore, if an attacker was to eavesdrop on that connection and was to eventually crack the encryption (or even perform Man-In-The-Middle attacks), he was able to get hold of the original biometric data. Hence the feature of *Resilient-to-Biometric-Loss* is not assigned. However, as the server itself is performing the biometric matching, no user device is to be trusted and hence the system is rated *Resilient-to-Malware*.

Further, as BioID provides its schema as an on-premise solution, it can be set-up without having any third-party dependencies, thus *No-Trusted-Third-Party* is assigned. Besides that, we rate BioID as not *Accessible-with-Visual-Impairments* as the use of a Face-Camera depends on being able to see the image of oneself properly.

To ensure resilience against replay or eavesdropping attacks, BioID implements a challenge-and-response-like paradigm that requires the user to turn his head in a specific way to ensure liveness. However, this paradigm introduces complexity. Therefore the system Cannot be rated *Easy-to-Learn*. The effort for an authentication attempt similarly increases to *Gesticulate-to-Enter*. Finally, due to the principle relying on a video being sent to the authenticating servers, BioID is *Susceptible-to-Transmission-Errors*.

6) LastPass: LastPass is essentially a password manager with additional features such as IAM solutions built on top of it. Recently, the company has started to offer passwordless authentication with their products. While many of the discussed features are identical to the other solutions assessed, there are a couple of differences. LastPass claims that their definition of passwordless is the passwordless login procedure for a user [19]. Their solution uses the biometric authentication from the user to then log in with the stored password from the password safe. Therefore their solution is to be interpreted as a representative for all biometrically secured password safes, such as the Apple iCloud Keychain. Concretely the biometric assessment is performed solely on the device (*Resilient-to-Biometric-Loss*). The criterion of *No-Trusted-Execution-Modules* is hence not assigned. Similarly, LastPass appears not to be available on-premise, thus rendering it reliant on a *Trusted-Third-Party*. Finally, as LastPass is essentially a biometrically secured password manager, it is *Server-Compatible*. However, this brings with it the classic threats of passwords such as in the case of e.g. a successful Man-In-The-Middle-Attack.

V. Discussion

With the results of the analysis, a discussion on the benefits or shortcomings of the specific authentication schemes can be performed. Specifically interesting aspects could be benefits that either none of the biometric schemes offers or benefits where the different remote biometric authentication schemes differ.

A. General Interpretation of the Results

The analysis and comparison of different authentication methods, their weaknesses, and advantages, is primarily an architecture-comparison. Therefore, the assessment between many of the systems is not as differentiated as we have expected. We would expect many more differences to be found in e.g. a code analysis where advantages of high-quality product development standards, e.g. *Pair Programming* or *Reviews* might come into play [20].

B. Resilient to Malware

Recalling from the original framework description, systems are not considered resilient against *Malware* attacks when the capturing of data from inside the device might lead to a compromise of the system's security. All kinds of smartphone-based biometric authentication systems are possibly prone to malware that is capable of modifying, altering, and/or compromising raw biometric data as soon as it is captured by the sensor. If a system was supposed to be resilient to malware, it would be required to still be secure even if an attacker had full control over the device itself. Excluded from that assumption might be the control over possible Trusted Execution Environments (TEE) within the device. This is due to the TEE's core concept relying on those being still secure even if the device itself was compromised.

Considering an attacker was able to completely compromise the device's security but for the secure enclave, he would be able to capture all network traffic potentially to be sent from the device to an authenticating party. Thus, he might be able to capture either biometric data or the secured biometric templates as soon as they are sent out from the secure enclave on the device. If such data is not specifically signed or secured from within the secure enclave, the attacker might be able to leverage previously recorded samples for future authentication attempts with the device. Therefore, if a service had methods such as challenge-response principles implemented, those might keep an attacker from using the pre-recorded data to perform the authentication attempt. BioID has implemented a similar mechanism in its Challenge-Response-Principle requiring user interaction before authentication. In the case of BioID, such interaction would be e.g. nodding the head up and down. By enforcing those principles, attackers might be kept off of using prerecorded data. Another alternative could be a challenge-response-system which requires to cryptographically sign nonces with a secret key only available in the TEE on the system. For similar cases which prevent the attacker to authenticate even in a case in which he has had previous control over the device and had the possibility to record previous authentication attempts, the feature of *Resilient-To-Malware* would be assigned.

Currently, of the analyzed systems, only BioID offers that feature. The other systems are relying on the integrated authentication principles of the phone. However, research has already shown that those principles currently do not live up to the attacks that they are being confronted with [21].

C. No Trusted Execution Module

Many mobile authentication systems use the authentication methods provided by the device. Those may be the Face/TouchID of Apple, fingerprint sensors of Samsung, or any other authentication method provided by mobile phone manufacturers. This is the proposed way by the FIDO(2) standard. The framework proposes the authentication in the following process: An authentication request is sent to the user from the web application that requires authentication. The user unlocks their phone using the local (biometric) authentication which in turn unlocks the secret credentials and uses those to cryptographically sign a nonce which is used to authenticate against the server. However, by using those systems, the remote application is required to trust the user's device. Even in a case in which the mobile device might not be compromised, the security requirements for the biometric authentication system might be severely lower than the security requirements for the web application. One such factor could be e.g. a fingerprint sensor that does not perform a proper *liveness* detection and is hence easily foolable. Further, the thresholds for the authentication which are used by the phone might provide a high *False-Match-Rate*. I.e. many impostors would be granted access. To overcome the drawbacks of performing biometric authentication on the mobile phone directly, the system architecture should rather consider the server's backend to perform the matching and decision-making process. That way, it is ensured that the remote system has the sovereignty of allowing or denying access according to principles that are defined in the backend. As explained previously, BioID performs such assessment where images are sent to the server and analyzed (fraud detection, matching, decision making...) in the system's backend.

D. Resilient-To-Biometric-Loss

The analysis shows that the question of Resilience-to-Biometric-Loss is not as clear as it might be expected. The FIDO-Framework superimposed the quasi-requirement to be **Resilient-to-Biometric-Loss** because the authentication is performed on the mobile devices themselves. In turn, no biometric data is sent across unsecured channels. Only BioID, which does not follow the FIDO-standards is not offering this benefit.

E. The Agony Of Choice on the Security Drawbacks

As previously outlined, *Resilient-to-Biometric-Loss* should be one of the core considerations in regard to biometric authentication applications. Judging from the analysis, applications seem to offer only one of the two main benefits: Either *Resilient-To-Biometric-Loss* or *No-Trusted-Execution-Modules*. Most often, both of the two approaches appear to be mutually exclusive.

Hence, it is in the responsibility of a system administrator to take both aspects into close consideration. This work proposes to choose a fitting authentication method based on the use and the expected potential for dangers from either of the two drawbacks. This boils down to the question of whether the importance and security of the application which is supposed to be accessed make up for the higher risk on the security of the user's biometric data. Administrators should similarly take into account, in which frequency the application is supposed to be used. One example might be securing access to a user's E-Mail account. This is an authentication which is performed on a regular basis and where a compromise of the system's security might have *minor* consequences. Therefore, in such a case, an administrator should consider accepting a lower security level for the E-Mail account itself in favor of the security of the user's biometric data. Contrasting this, however, the CEO of a company might use a business-critical password manager which is accessed on a seldom basis and only from the specifically secured company devices. That specific access is supposed to be biometrically secured now. In such a case, the security of the application might be regarded as more important than the security of the user's biometric data. [13]

VI. Outlook

While this work proposed the improvement of the framework around the *Quest to replace passwords* especially for (remote) biometric authentication methods, the quest is not

[13]This is a fictional example. This work does not propose putting every CEO's biometric data at risk. Decisions like outlined above have to be performed on a case-to-case basis and the potential risks for the biometric data should be explained to the users.

completed and will very likely not be in the near future. However, improvements in the knowledge-base for decision-makers have been achieved. This work opens up new questions for research. Some of those questions are shortly explained below.

A. Fuzzy Extactors

Fuzzy extractors have been closely evaluated and improved over the last years. Their principled take on the problems of deriving the same cryptographic values from similar input data. One such example might be the derivation of a cryptographic key from a fingerprint. Due to the challenges with biometric data which has been outlined before such as that there are seldomly identical biometric samples for the same user, the algorithms have to deal with a certain amount of random noise.

Potentially, approaches such as Fuzzy Extractors might be starting points to investigate solutions in which biometric samples are collected on the phone, then some data is derived from them and that data is sent to the server. On the server-side, a sort-of biometric matching can be performed assessing the data derived from the biometric samples. Depending on the results, a server would be able to decide on whether to grant or deny access to the user.

B. Zero-Knowledge-Proofs

Similarly, to the described Fuzzy Extractors, In 2009, Kikuchi et al. presented an approach to enable zero-knowledge proofs to be biometric data-compatible [22]. Approaches like the ones presented by Kikuchi et al. would allow us to take on the problem of either *Resiliency-Against-Biometric-Loss* or *No-Trusted-Execution-Modules*. In theory, an authentication attempt might potentially be started on the mobile device, which in turn captures biometric samples to initiate a ZKP-like authentication with the server. The mobile device might send information on the biometric samples which does not contain insights on the biometric data itself to the server. Depending on the received information, the server can then calculate the trust values for the authenticating user and their authentication attempt. If such a system might be imaginable it might effectively allow shifting the trust to the server-side while not interfering with the principle of *Biometric-Data-Secrecy*.

C. Evaluation of Importance of Frameworks

As previously outlined, frameworks and the connected requirements to systems implementing those are superimposing certain criteria on the final authentication systems. A proper analysis of available frameworks and the criteria that such ideas define for implementing authentication systems might show certain aspects that require specific investigation. Further, such an assessment would in turn not only help the decision-makers in their decision which authentication mechanism to implement but might further help developers in assessing which difference the choice of a certain framework to adhere to makes.

VII. Related Work

In Section II we described the improvements and research alongside the *Quest to Replace Passwords*. One main aspect to keep in mind is that the Framework proposed by *Bonneau et al.* is mainly assessing the different authentication systems based on their architecture. This refers to the fact that aspects such as flaws in the code or other vulnerabilities that might be introduced by an imperfect implementation of the system are not assessed. However, the above focus enables us to assess the different authentication systems on a general level. As an indicator of the quality of the application in terms of. e.g. Software Vulnerabilities one can only merely choose the benefit of *Maturity*.

Another line of research in the area of remote biometric authentication has been started by *Li* and *Hwang* in 2010 when they proposed an efficient biometric-based remote authentication scheme [23]. Since, many researcher such as *Das A.* [24], *An, Y.* [25] as well as *Park et al.* [26] and lately *Boonkrong, S.* [27] have started to analyze and enhance the system at hand. While doing so, they often focussed on evaluating the actual system in detail by aspects such as computational cost or few security features such as *Session Key Agreement* or *Replay Attack Resistance* [27]. However, they have not yet assessed the biometric systems in contrast to other authentication systems and with a specified set of criteria. An in-depth analysis like performed in the mentioned work is essential for advancement in the different fields or improvements of certain frameworks but is incapable of setting the system into an overall perspective in comparison to alternative systems or methods.

Similar to the above, plenty of other researchers have assessed biometric authentication systems or proposed new (biometric) authentication systems. However, an overall comparison to other systems is seldom done. This work clearly differentiates between *(1)* in-depth system assessment which analyzes the resiliency against potential sophisticated attacks or analyzes the code quality of a certain implementation of a system and *(2)* the overall assessment as performed by *Bonneau et al.* and continued by the other researchers. The later *(2)* assessment allows us to evaluate whether and for which instances a certain group of authentication schemes might be beneficial. In-between a specific group, a more in-depth assessment such as *(1)* should prove valuable.

VIII. Conclusion

The hassle of authentication is one of the problems that are still prominent in the security industry. Therefore this work follows-up on *Bonneau et al.'s* work on the *Quest to Replace Passwords* which introduced a framework for rating and comparing authentication schemes. Since the framework has been expanded by various other authors in terms of expanding the variety of schemes analyzed with the framework as well as enhancing the framework itself by introducing new criteria and developing it into the *ACCESS* web application.

This work expands the variety of analyzed schemes inside the framework by the first analysis of six systems for remote

biometric authentication. Remote Biometric Authentication refers to the process of using biometric treats to authenticate against a remote party such as a web application. To perform the assessment, we propose two new criteria to be added to the framework: *No-Trusted-Execution-Environment* and *Biometric Data Secrecy*.

With the assessment of *Microsoft Authenticator*, *Thumb-SignIn*, *Gluu*, *Viridium*, *BioID*, and *LastPass*, we have identified a central aspect of those remote biometric authentication systems in their current state: Either, the server has to transfer its trust in the biometric assessment to a mobile device, or the system has to transfer the user's biometric data across open networks. We see neither of the two options as a perfect solution and hence shortly describe possible starting points for future work.

REFERENCES

[1] L. Bosnjak and B. Brumen, "Rejecting the death of passwords: Advice for the future," *Computer Science and Information Systems*, vol. 16, no. 1, pp. 313–332, 2019. [Online]. Available: http://www.doiserbia.nb.rs/Article.aspx?ID=1820-02141800016B

[2] D. Jaeger, C. Pelchen, H. Graupner, F. Cheng, and C. Meinel, "Analysis of Publicly Leaked Credentials and the Long Story of Password (Re-) use," in *PASSWORDS'16*, 2016. [Online]. Available: https://pdfs.semanticscholar.org/b480/ccf4e396c63567a0bdb3f372993c691799b7.pdf

[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 *2012 IEEE Symposium on Security and Privacy*. San Francisco, CA, USA: IEEE, May 2012, pp. 553–567. [Online]. Available: http://ieeexplore.ieee.org/document/6234436/

[4] V. Zimmermann, N. Gerber, M. Kleboth, A. von Preuschen, K. Schmidt, and P. Mayer, "The Quest to Replace Passwords Revisited – Rating Authentication Schemes," in *Twelth International Proceedings of the Twelfth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2018)*, N. L. Clarke and S. M. Furnell, Eds. Plymouth, UK: University of Plymouth, Aug. 2018, pp. 38–48. [Online]. Available: https://tubiblio.ulb.tu-darmstadt.de/111860/

[5] P. Mayer, P. Stumpf, T. Weber, and M. Volkamer, "ACCESSv2: A Collaborative Authentication Research and Decision Support Platform," in *Who Are You? Adventures in Authentication Workshop 2018*}, Aug. 2018. [Online]. Available: https://www.researchgate.net/publication/340661321_ACCESSv2_A_Collaborative_Authentication_Research_and_Decision_Support_Platform

[6] P. Mayer, S. Neumann, D. Storck, and M. Volkamer, "Supporting Decision Makers in Choosing Suitable Authentication Schemes," in *Tenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2016)*, Frankfurt, Germany, 2016, p. 67. [Online]. Available: https://publikationen.bibliothek.kit.edu/1000081972

[7] P. Ambalakat, "Security of Biometric Authentication Systems," in *21st Computer Science Seminar*, 2005, p. 7. [Online]. Available: https://pdfs.semanticscholar.org/e1d7/7b951c55d7d1f322d1f96942daa77ec6c4ee.pdf

[8] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "Technical Report: The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," University of Cambridge, Computer Laboratory, San Francisco, CA, USA, Tech. Rep. UCAM-CL-TR-817, May 2012. [Online]. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

[9] J. Bonneau and S. Preibusch, "The password thicket: Technical and market failures in human authentication on the web," in *WEIS 2010, The Ninth Workshop on the Economics of Information Security*, 2010, p. 49.

[10] V. Matyáš and Z. Říha, "Biometric Authentication — Security and Usability," in *Advanced Communications and Multimedia Security*, B. Jerman-Blažič and T. Klobučar, Eds. Boston, MA: Springer US, 2002, vol. 100, pp. 227–239. [Online]. Available: http://link.springer.com/10.1007/978-0-387-35612-9_17

[11] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on Post-Quantum Cryptography," National Institute of Standards and Technology, Tech. Rep. NIST IR 8105, Apr. 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf

[12] F. Wilhelm, R. Steinwandt, B. Langenberg, P. Liebermann, A. Messinger, and P. Schuhmacher, "Entwicklungsstand Quantencomputer," Bundesamt für Sicherheit in der Informationstechnik, Tech. Rep. Projektnummer 283, 2019. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie-V_1_1.pdf

[13] N. Ratha, J. Connell, R. Bolle, and S. Chikkerur, "Cancelable Biometrics: A Case Study in Fingerprints," in *18th International Conference on Pattern Recognition (ICPR'06)*. Hong Kong, China: IEEE, 2006, pp. 370–373. [Online]. Available: http://ieeexplore.ieee.org/document/1699857/

[14] Y. Sutcu, Q. Li, and N. Memon, "Secure Biometric Templates from Fingerprint-Face Features," in *2007 IEEE Conference on Computer Vision and Pattern Recognition*, Jun. 2007, pp. 1–6.

[15] iainfoulds, "Passwordless sign-in with the Microsoft Authenticator app - Azure Active Directory." [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phone

[16] P. Jonathon Phillips, A. Martin, C. Wilson, and M. Przybocki, "An Introduction to Evaluating Biometric Systems," *National Institute of Standards and Technology*, p. 8, 2000. [Online]. Available: https://marathon.cse.usf.edu/~sarkar/biometrics/papers/BiometricEvaluation.pdf

[17] Gluu, "Gluu Server 4.1 Docs," 2020. [Online]. Available: https://gluu.org/docs/gluu-server/

[18] BioID, "Securing privacy by design — Biometric services," 2019. [Online]. Available: https://www.bioid.com/securing-privacy-by-design/

[19] Y. Masoudnia, "Is Passwordless Really Possible?" Jan. 2020. [Online]. Available: https://blog.lastpass.com/2020/01/is-passwordless-really-possible/

[20] M. M. Müller, "Are Reviews an Alternative to Pair Programming?" *Empirical Software Engineering*, vol. 9, no. 4, pp. 335–351, Dec. 2004. [Online]. Available: http://link.springer.com/10.1023/B:EMSE.0000039883.47173.39

[21] K. Cao and A. K. Jain, "Hacking Mobile Phones Using 2D Printed Fingerprints," Michigan State University, Tech. Rep. MSU-CSE-16-2, 2016.

[22] H. Kikuchi, K. Nagai, W. Ogata, and M. Nishigaki, "Privacy-preserving similarity evaluation and application to remote biometrics authentication," *Soft Computing*, vol. 14, no. 5, pp. 529–536, Mar. 2010.

[23] C.-T. Li and M.-S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1–5, Jan. 2010. [Online]. Available: https://linkinghub.elsevier.com/retrieve/pii/S1084804509001192

[24] A. Das, "Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards," *IET Information Security*, vol. 5, no. 3, p. 145, 2011. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2010.0125

[25] Y. An, "Security Analysis and Enhancements of an Effective Biometric-Based Remote User Authentication Scheme Using Smart Cards," p. e519723, Jul. 2012. [Online]. Available: https://www.hindawi.com/journals/bmri/2012/519723/

[26] Y. Park, K. Park, K. Lee, H. Song, and Y. Park, "Security analysis and enhancements of an improved multi-factor biometric authentication scheme," *International Journal of Distributed Sensor Networks*, vol. 13, no. 8, p. 1550147717724308, Aug. 2017.

[27] S. Boonkrong, "Security Analysis and Improvement of aMulti-Factor Biometric-Based RemoteAuthentication Scheme," in *IAENG International Journal of Computer Science*, 2019. [Online]. Available: http://www.iaeng.org/IJCS/issues_v46/issue_4/IJCS_46_4_22.pdf