User Authentication and Authorization for Next Generation Mobile Passenger ID Devices for Land and Sea Border Control

Maria Papaioannou
Instituto de Telecomunicações
Aveiro, Portugal
m.papaioannou@av.it.pt

Georgios Mantas
Instituto de Telecomunicações
Aveiro, Portugal
University of Greenwich
London, UK
gimantas@av.it.pt

Dimitrios Lymberopoulos
University of Patras
Patras, Greece
dlympero@upatras.gr

Jonathan Rodriguez
Instituto de Telecomunicações
Aveiro, Portugal
jonathan@av.it.pt

***Abstract*—Despite the significant economic benefits derived from the continuously increasing number of visitors entering the European Union through land-border crossing points or sea ports, novel solutions, such as next generation mobile devices for passenger identification for land and sea border control, are required to promote the comfort of passengers. However, the highly sensitive information handled by these devices makes them an attractive target for attackers. Therefore, strong user authentication and authorization mechanisms are required. Towards this direction, we provide an overview of user authentication and authorization requirements for this new type of devices based on the NIST Special Publication 500-280v2.1.**

Keywords—border control security, mobile passenger ID devices, user authentication and authorization

I. INTRODUCTION

Transport is a fundamental sector for and of the world economy. According to the European Commission [1], transport services encompass a diverse and complex network comprising around 1.2 million private and public enterprises across the EU, employing approximately 11 million people and delivering products and services to EU residents, companies and its trading partners. Efficient transport services and infrastructure are a cornerstone component to exploiting the economic strengths of the European Union, and to empowering cohesion both at economic and social level. While airports are of an acceptable standard transport services and infrastructure, land border crossing points and sea ports require more research and investment for novel efficient solutions, such as next generation mobile devices for passenger identification for land and sea border control.

The next generation mobile devices for passenger identification for land and sea border control comprise a promising and innovative solution for accurate passenger identification "on the fly" while ensuring passenger´s comfort. However, the highly sensitive and confidential information handled by these devices makes them susceptible to data loss, data theft and data misuse. In order to ensure high level of device security to protect sensitive data handled by these devices, strong user authentication and authorization mechanisms are required [2]. Towards this direction, we provide an overview of user authentication and authorization requirements for this new type of devices based on the NIST Special Publication 500-280v2.1 [3]. Besides that, we also present a set of use cases in order to give researchers a better understanding of this new type of devices and of their requirements in terms of user authentication and authorization. Moreover, an overview of existing user authentication and authorization mechanisms for smartphone devices is given in order to provide a foundation for organizing research efforts towards the design and development of proper user authentication and authorization mechanisms for next generation mobile passenger ID devices for land and sea border control. We focus on user authentication and authorization mechanisms for smartphone devices since it is anticipated that the next generation mobile passenger ID devices will be devices with capabilities similar to those of smartphone devices.

Following the Introduction, the rest of the paper is organized as follows. Section II presents a set of use cases for next generation mobile passenger ID devices for land and sea border control. User authentication and authorization requirements for this new type of devices are described in Section III, while an overview of existing user authentication and authorization mechanisms for smartphone devices is provided in Section IV. Finally, the paper is concluded in Section V.

II. USE CASES FOR NEXT GENERATION MOBILE PASSENGER ID DEVICES FOR LAND AND SEA BORDER CONTROL

The purpose of this section is to present a set of use cases as part of a foundation for understanding the necessary security requirements for next generation mobile passenger ID devices for land and sea border control. To develop these use cases, we relied on NISTIR 8196 "Security Analysis of First Responder Mobile and Wearable Devices", where several cases from reputable public safety organizations were identified, surveyed, and analyzed [4].

A. Mobile Information Collection and Sharing

While in the land or sea border control, an officer is utilizing the next generation mobile passenger ID device to record and capture relevant identification information, but not biometric information covered in II.C, for a passenger. This information may be stored on the officer's mobile device or relayed to the backend platform where the information is processed or analysed further by specific algorithms, stored in backend databases, and/or reviewed by investigators, supervisors, and other command staff. Nevertheless, the data stored on the officer's mobile device

The research work leading to this publication has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement H2020-MSCA-RISE-2019-eBORDER-872878.

or transmitted to the backend platform may be unencrypted, allowing easy access of information by unauthorized users.

B. Shared Equipment with Multiple Users

A border control officer selects a device from a charging station. Although this device is different from the device the officer used before, the officer logs into the device. After login, the device is automatically configured with the officer's profile settings. However, the officer may have unauthorized access to sensitive information that was authorized for a previous user in this mobile device. For instance, collected and stored, on the device, passenger identification data may be exposed to unauthorized users. Furthermore, it is possible that the default device settings may be incorrectly assigned (e.g., higher access level user incorrectly assigned to a lower access level user). In addition, location data and officer information may also be incorrectly associated with the previous user.

C. Gathering and Processing Biometric Information

The capability of the next generation mobile passenger ID device to capture and validate accurately the passenger´s biometric information is a cornerstone component for efficient land and sea border control applications. A border control officer makes use of biometric sensors to capture biometrics to facilitate the identification of the passenger. Similar to the captured relevant identification information, considered in II.A, the biometric information is transmitted to the backend platform for processing and storage. Then, the officer receives the processing results that lead to improved situational awareness and enable an informed action. Thefore, data in transit and data at rest protection for the biometric information is important and can be achieved by encrypting the transmitted or stored data, respectively. Data encryption can protect against unauthorized extraction or modification of the data in transit or at rest.

D. Lost or Stolen Device

There is the possibility that an officer loses his/her mobile passenger ID device (e.g., during a break of his/her duty) or an individual steals the device intentionally. In the case that the officer loses the mobile passenger ID device, thereafter an unauthorized user may find the device and try to login and access the stored information and applications on the mobile passenger ID device. Similar to the lost device case, when an individual steals the mobile passenger ID device of the officer, the individual may be able to access critical information stored on it. In both cases, the level of ease to obtain unauthorized access to sensitive information significantly depends on the authentication and authorization mechanisms supported by the mobile passenger ID device.

III. User Authentication and Authorization Requirements

In this section, we provide an overview of the user (i.e., officer) authentication and authorization requirements for this new type of devices based on the NIST Special Publication 500-280v2.1 [3].

A. Officer Authentication & Authorization

The next generation mobile passenger ID device should provide the means for an officer to authenticate his/her identity and enable authorization levels for that person depending on a two-factor authentication.

- *Two-factor Authentication*: The next generation mobile passenger ID device should provide the means for a two-factor authentication. The one should be a biometric, while the other may be a strong password, e.g. of minimum length with alphabetical/ numeric/ special characters.
- *Officer Re-Authentication*: The next generation mobile passenger ID device should provide the means for an officer to re-authenticate his/her identity after a default time of using the mobile device or device inactivity, or after a shut-off.
- *Failed Officer Authentication Attempts or Unknown Device Location*: The next generation mobile passenger ID device should have the capability to lock itself or to render itself inoperable and/or erase selective or all data stored on the device (e.g., a remote data "wiping" capability) as a result of a maximum limit of failed authentication attempts or an unknown device location. In these cases, the device should require unlock only by an IT administrator.

B. Device Authentication & Authorization:

The next generation mobile passenger ID device should be authenticated and authorized by the backend platform right after the completion of the officer authentication and authorization process as well as before establishing any communication with the platform for data transmission. The device identification should be firstly verified against a registered list, stored on the platform, of specified devices (e.g., lost or stolen) before being authorized. A device with a matching identification to one of the list should not be authenticated and an alert should be generated...

IV. Related Work on User Authentication and Authorization for Smartphone Devices

User authentication and authorization are fundamental security objectives for the security of the the next generation mobile passenger ID devices. As these devices comprise a novel solution for accurate "on the fly" passenger identification, no specific user authentication and authorization mechanisms for this kind of devices have been developed so far. However, it is anticipated that the next generation mobile passenger ID devices will be devices with similar capabilities to those of smartphone devices. Therefore, in this section, we give an overview of existing user authentication and authorization mechanisms for smartphone devices in order to provide a foundation for organizing research efforts towards the design and development of proper user authentication and authorization mechanisms for next generation mobile passenger ID devices for land and sea border control.

A. Means of Authentication

In this section, we review the recent literature emphasizing on the commonly used user authentication mechanisms on smartphones, and that, potentially, could be a basis for designing and developing proper user authentication mechanisms for the next generation mobile passenger ID devices for land and sea border control applications. User authentication techniques may be divided into three main categories, depending on which of the following the security is based: something known, something possessed, and something inherent [5].

1) Something known. Examples of this category include standard passwords, Personal Identification Numbers (PINs), graphical patterns, and the secret or private keys whose knowledge is demonstrated in challenge-response protocols [5]. Gupta et al. [6] presented the commonly used ways and classified numerous types to achieve authentication in smartphones. According to their review article, knowledge-based schemes are generally used as one-shot, periodic, single sign-on (SSO) and static authentication mechanism types. More specifically, one-shot authentication is a type of authentication mechanism in which the user authentication is proceed only at the beginning of the session. Once user authentication is established, the user has unlimited access to the device and the authentication remains valid until the user signs off or closes the session. This mechanism type could violate the requirement of Officer Re-Authentication that is described in Section III. On the other hand, periodic authentication mechanism is simply the variant of ``one-shot authentication´´ with the addition of a default timeout duration, after which the user has to re-authenticate himself. Additionally, the SSO authentication mechanism type permits the user to remain signed on using valid login credentials until the session is terminated or the user revoked. In case, if the system detects any abnormality with respect to fix set of attributes, e.g. the user location or the network connection, the session is closed or user re-authentications is requested [6]. For instance, Google provides G Suite apps with SSO mechanisms for Android devices which can be achieved by pairing smartphones with wearable devices such as smartwatches [7]. Finally, the static authentication mechanism type requests a fixed set of challenges to authenticate the users.

According to the recent studies [8], the aforementioned conventional user authentication techniques are no more considered secure and convinient for the user. First of all, these techniques are not able to distinguish the users, rather they authenticate everyone with the valid credentials. Despite this, they require users to memorize their passwords to unlock the device every time that is needed. At [9], Zhang at al. describe the difficulties of the users in memorizing and correctly recalling the several passwords. As a consequence, the users set easy or simple passwords to remember making the mobile devices vulnerable to numerous attacks, e.g. guessing. Alternatively, Android users tend to set graphical patterns for device unlocking. Nevertheless, this approach requires users to memorize them too, and thus, users choose simple patterns and an attacker could possible guess or observe the pattern. Researchers collected unique graphical patterns from 215 users, and cracked the 95% of those patterns within just five attempts [10].

2) Something possesed. This is typically a physical accessory, resembling a passport in function. Examples include magnetic-striped cards, chipcards or smart cards, hand-held customized calculators (password generators) which provide time-variant passwords and tokens [5]. For instance, smartphone applications (e.g., e-banking and e-wallet) that handle sensitive information enable two-factor authentication techniques such as one-time passcodes (OTPs) along with the usual username and password authentication. For the passcodes generation, the service providers often supply a small security device to each user, or the passcode could be sent via SMS on the user´s smartphone [6]. OTP scheme could be easily implemented on mobile devices. Additionally, the user is able to generate even offline the passcode using the mobile app provided by the service provider, or with the pairing of another (often wearable) device, such as smartwatches or smartglasses [6]. Secure device pairing schemes allow access to the smartphones by pairing it with a trusted Bluetooth device and use the same to unlock the phone. However, OTP solutions do not ensure the confidentiality of the generated passcodes as they are vulnerable to Man-In-The-Middle attacks (MITM) and Man-In-The-PC/Phone (MITPC/P) attacks. As per the Verizon Data Breach Investigations Report [11], NIST stopped recommending the two-factor user authentication via SMS, as malicious code infesting mobile endpoints could surreptitiously capture second factors delivered by SMS or offline OTP generated using apps. On top of that, in-depth security and usability studies [12], [13], [14], [15] mentioned that OTP schemes result more cost to the user and are comparatively slower, as they may require an additional hardware for the only purpose of authentication. Regarding those studies, users consider the OTP-based authentication not a convenient for the user solution. The analysis [16] shows that the users are facing several problems due to mistyped passcodes for example.

Gupta et al. [6] mention that token-based authentication schemes are used in the type of risk-based authentication mechanism. According to review article [6], risk-based authentication schemes are mostly based on a continuous decision to accept or reject user authentication. This decision depends on the comparison of a risk score computed in real-time with the stored risk profiles of the users, and then the system challenges the users for authentication, accordingly. For instance, when an officer is using the next generation mobile ID device from a verified secure location (land or sea border control workplace), re-authentication should not be required. While in case of an unknown or nonverified location, the service may require additional evidence about the identity of the user and thus asking for re-authentication. Nowadays, risk-based authentication schemes tend to offer frictionless user authentication while enhancing security and promoting user´s comfort [6], [16], [17], [18].

3) Something inherent. This category includes methods which make use of human physical characteristics and involuntary actions (biometrics), such as handwritten signatures, fingerprints, voice, retinal patterns, hand geometries, and dynamic keyboarding characteristics [5]. Gupta et al. [6] have further classified this category as physiological and behavioral biometrics.

a) Physiological Biometrics. Regarding the physiological biometrics, for example, face, fingerprint and iris recognition, the mobile device manufacturers have started embedding the corresponding biosensors in order to capture them and utilize them for accurate and convenient user authentication. For instance, Apple, Huawei, Samsung, Nokia have already developed iris scanners and fingerprint sensors in some of their recently launched smartphones. Despite that the physiological biometrics are considered secure due to the fact that they are unique, they have shown

to be vulnerable to different types of attacks such a impersonation. More specifically, the face of a user, nowadays, could be easily found on social media websites, while the fingerprint could be extracted from the gestures on some photos. Recent researchers has shown that these physiological biometric schemes can be hacked easily with a cheap equipment and not very sophisticated algorithms. For instance, iPhone X Face ID was hacked with a 3D printed mask of its owner face costing around 150 dollars [19], while with a simple photo of the owner, researches unlocked the Samsung S8 [20]. Similarly, the German Chaos Computer Club hacked the iPhone 5S fingerprint scanner by photographing the glass surface with the user´s fingerprint, and then creating a thin film with a fake one within two days after Apple launched iPhone 5S worldwide [21]. Additionally, the researcher Isao Echizen from Japan´s National Institute of Informatics (NII) shown that fake fingerprints can be easily created from a simple photo with the peace sign taken just from three meters away, and they can unlock the device without any sophisticated process [22]. This is a proof that there is a need for novel solutions and more sophisticated algorithms to exploit the advantages of uniqueness of the physiological biometrics.

For instance, it is worthwhile to mention the Face ID advanced technology that is already applied in some recent iPhone models (e.g., iPhone XR, iPhone 11) and iPad models (e.g., iPad Pro) [23]. Face ID revolutionizes user authentication by means of facial recognition providing secure authentication enabled by the state-of-the-art TrueDepth camera system with advanced machine learning technologies to accurately map the geometry of the face of the user. More precisely, the TrueDepth projects and analyzes over 30.000 invisible dots in order to create a depth map of user´s face. Consequently, the camera captures accurate face data together with an infrared image of the face. Then, advanced software transforms the depth map and the infrared image into a mathematical representation. Every time that the user attempts to login, the software compares that representation to the enrolled facial data. Additionally, Face ID automatically adapts to changes in user´s appearance, such as growing facial hair. If there is a more significant change, before it updates the face data, Face ID is able to authenticate the user by using a set passcode. Face ID is designed to work with numerous accessories like hats, scarves, glasses, contact lenses, and many sunglasses. Furthermore, it's designed to work indoors, outdoors, and even in total darkness. On top of that, all Face ID data - including mathematical representations of the face - is encrypted and protected. According to statistics [23], the probability that a random individual could fool the Face ID and unlock it is approximately 1 in 1,000,000 with a single enrolled appearance. As an additional security protection, Face ID requires the passcode after five unsuccessful match attempts. Finally, Face ID matches against depth information, and so it cannot be fooled from a print or 2D digital photographs. It's designed to protect against spoofing by masks or other techniques by using sophisticated anti-spoofing neural networks. Face ID is even attention-aware and can identify if the eyes are open and the attention is focused on the smartphone device..

b) Behavioral Biometrics. User authentication based on behavioral biometrics is considered as the future of user authentication for sensitive applications performed with mobile devices [24]. For instance, for the next generation mobile passenger ID devices for land and sea border control, behavioral biometric-based solutions are very promising. Although the behavioral biometrics are not considered unique enough for ensuring user identification, they have proved efficient for user authentication. Additionally, combining two or more modalities can improve the accuracy and enhance the security. These schemes can work as an additional transparent authentication layer, that enhance the existing authentication mechanisms without affecting the usage of the device [5], [24], [25], [26]. Research efforts have been already started in gait recognition, keystroke or touch dynamics and voice recognition behavioral biometric modalities [5], [25].

- Gait recognition is the process of authenticating the user based on his/her walking style [6]. Recently, smartphones and wearable devices have started developing schemes for user authentication by means of gait recognition. Most of the researchers [27], [28], [29] presented gait-based solution that they are implemented together with a wearable sensor. The results are promising, although more testing is required to ensure robustness against impersonation attacks. However, for the next generation mobile passenger ID devices for land and sea border control, the gait-based solution with a wearable device is not so convenient, considering that the officer may move long distances, and also regarding the large number of the officers working (e.g., cost of many sensors). On the other hand, a gait-based solution implemented by some in-built sensors, such as the accelerometer or the gyroscope, could possible fit better in the land and sea border control application.
- Keystroke or touch dynamics refers to the user´s characteristics while typing due to timing differences or different pressure. Researchers consider them efficient, and since they do not require a special hardware, they have been widely evaluated [6], [30], [31], [32]. Most of the proposed schemes examine the way of typing while users entering their credentials in order to sign into their online banking apps. This modality potentially could be integrated for the user authentication for the next generation mobile passenger ID devices for land and sea border control as an additional authentication level when for instance the face recognition fails, and the system asks for the passcode.
- Research efforts have been addressed to voice recognition experimented on public databases [33]. They digitalized the voice of the user, and then compute the Mel Frequency Cepstral Coefficients (MFCCs) and the Euclidean distance. The results could potentially enhance the performance of the traditional biometric systems and broaden the landscape of the continuous user authentication.

To sum up, considering a smartphone device, the face physiological biometric can be collected by using the camera of the device, while the fingerprint and iris recognition need special equipment. On the other hand, the behavioral biometrics, such as gait, touch, swipe and voice can be collected all by the sensors of the mobile device, namely, accelerometer, gyroscope, touch screen and microphone [34]. The behavioral biometrics are starting to get attention as they are cost-effective; they do not need any additional hardware equipment, and they are lightweight in the implementation [30]. For instance, the touch-based solution e.g. swipe or keystroke, manage to authenticate the users unobtrusively based on their interactions with the device. Additionally, both physiological and behavioral biometrics authentication mechanisms are considered secure and accurate as they are unique and they cannot be shared, copied, lost or stolen [6]. Furthermore, they can be combined with another authentication means (e.g., username and password) for establishing multifactor authentication in order to enhance the security of the mobile device.. As such, security experts are focusing on developing such mechanisms as they seem that they will restructure the authentication landscape in the following years [6], [35], [36].

B. Means of Authorization

Authorization is a term which is used (and often abused) in a very broad sense [5]. It conveys the idea that some means has been provided to ensure the process of granting or denying specific requests to obtain and use specific information or applications [37]. The process of permitting or restricting the access can happen at a granular level, such as per-user, per-group, and per-resources [37]. Although, authorization can be considered as a security objective, it is very often intrinsically connected to authentication. More precisely, one of the primary purposes of authentication is to facilitate access control to a resource, when an access privilege is linked to a particular user. For instance, a username-password authentication scheme that give access to a user's smartphone may be viewed as the simplest example of an access control matrix. In the access control matrix, each resource has a list of users associated with it and successful corroboration of a user allows access to the authorized resources as listed for that user [5]. The most obvious approach is for the system to store user passwords cleartext in a read- and write-protected system password file. When the user enters the password, the system compares the entered password to the password file entry for the corresponding userid. A drawback of this method is that it provides no protection against privileged insiders or superusers (special userids which have full access privileges to system files and resources). Storage of the password file on backup media is also a security concern, since the file contains cleartext passwords [5].

According to the handbook of NIST about access control [38],,when implementing a secure and accurate access control system we should consider three abstractions: access control policies, models, and mechanisms. Firstly, access control policies are high-level requirements that specify in general how access is managed, for instance, who may access which information under what circumstances. At a high level, access control policies are applied through a mechanism that translates an access request of the user often in terms of a structure required by the system. A common example of an access control mechanism is an access control list. Finally, access control models bridge the gap in abstraction between policy and mechanism.

V. CONCLUSIONS

The next generation mobile devices for passenger identification for land and sea border control comprises a promising and innovative solution for accurate passenger identification "on the fly" while ensuring passenger´s comfort. However, the highly sensitive information handled by these devices makes them an attractive target for attackers. Therefore, strong user authentication and authorization mechanisms are required. Towards this direction, the objective of this work is two-fold: a) to give researchers a better understanding of this new type of devices through a series of use cases and provide an overview of the user authentication and authorization requirements, and b) to provide a foundation for organizing research efforts towards the design and development of proper user authentication and authorization mechanisms for next generation mobile passenger ID devices for land and sea border control.

ACKNOWLEDGMENT

The research work leading to this publication has received funding from the European Union's Horizon 2020 Research and Innovation programme under grant agreement H2020-MSCA-RISE-2019-eBORDER-872878.

REFERENCES

[1] European Commission, "Mobility and Transport Transport in the European Union Current Trends and Issues BACKGROUND INFORMATION," *Eur. Comm.*, no. April, p. 144, 2018.

[2] G. Mantas, N. Komninos, J. Rodriguez, E. Logota, and H. Marques, "Security for 5G Communications," in *Fundamentals of 5G Mobile Networks, J. Rodriguez*, L. Eds., John Wiley & Sons, Ed. Chichester, UK, 2015, pp. 207–220.

[3] R. M. Mccabe, "Mobile ID Device Best Practice Recommendation Mobile ID Device Best Practice Recommendation," *Nist Spec. Publ.*, vol. 2, no. July, pp. 1–55, 2009.

[4] J. M. Franklin, G. Howell, S. Ledgerwood, and J. L. Griffith, "Draft NISTIR 8196, Security Analysis of First Responder Mobile and Wearable Devices."

[5] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "APPLIED CRYPTOGRAPHY."

[6] S. Gupta, A. Buriro, and B. Crispo, "Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access," *Mob. Inf. Syst.*, vol. 2018, 2018.

[7] Google, "'G suite: single sign-on on an android device,'" 2016. [Online]. Available: https://support.google.com/a/users/answer/2758865?hl=en.

[8] M. Harbach, E. von Zezschwitz, A. Fichtner, A. De Luca, and M. Smith, "It's a Hard Lock Life: A Field Study of Smartphone (Un)Locking Behavior and Risk Perception," *SOUPS '14 Proc. Tenth Symp. Usable Priv. Secur.*, pp. 213–230, 2016.

[9] J. Zhang, X. Luo, S. Akkaladevi, and J. Ziegelmayer, "Improving multiple-password recall: An empirical study," *Eur. J. Inf. Syst.*,

vol. 18, no. 2, pp. 165–176, 2009.

[10] G. Ye *et al.*, “Cracking Android Pattern Lock in Five Attempts,” 2017.

[11] Verizon, “‘How long since you took a hard look at your cybersecurity?,’” 2017.

[12] C. Braz and J. M. Robert, “Security and usability: The case of the user authentication methods,” *ACM Int. Conf. Proceeding Ser.*, vol. 133, pp. 199–203, 2006.

[13] S. G. Belk M., Germanakos P., Fidas C., “A Personalization Method Based on Human Factors for Improving Usability of User Authentication Tasks,” *Springer, Cham*, vol. 8538, no. User Modeling, Adaptation, and Personalization. UMAP 2014. Lecture Notes in Computer Science, 2014.

[14] K. Krol, E. Philippou, E. De Cristofaro, and M. A. Sasse, “‘They brought in the horrible key ring thing!’ Analysing the Usability of Two-Factor Authentication in UK Online Banking,” 2015.

[15] T. Zink and M. Waldvogel, “X.509 user certificate-based two-factor authentication for web applications,” *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, vol. 271, 2017.

[16] I. Traore, I. Woungang, M. S. Obaidat, Y. Nakkabi, and I. Lai, “Online risk-based authentication using behavioral biometrics,” *Multimed. Tools Appl.*, vol. 71, no. 2, pp. 575–605, 2014.

[17] A. J. Harris and D. C. Yen, “Biometric authentication: Assuring access to information,” *Inf. Manag. Comput. Secur.*, vol. 10, no. 1, pp. 12–19, 2002.

[18] B. Causey, “‘Adaptive authentication: an introduction to riskbased authentication,’” 2013. .

[19] J. Titcomb, “‘Hackers claim to beat iPhone X’s face id in one week with 115 mask,’” *2017*. .

[20] S. Kovach, “‘Business insider-Samsung’s Galaxy S8 facial recognition feature can be fooled with a photo,’” 2017.

[21] A. Charles, “‘The guardian-iPhone 5S fingerprint sensor hacked by Germany’s Chaos Computer Club,’” 2013. .

[22] D. McGoogan, C., & Demetriou, “Peace sign selfies could let hackers copy your fingerprints,” 2017. .

[23] Apple, “About Face ID advanced technology,” 2020. [Online]. Available: https://support.apple.com/en-us/HT208108.

[24] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, and R. A. Abd-Alhameed, “HIDROID: Prototyping a Behavioral Host-based Intrusion Detection and Prevention System for Android,” *IEEE Access*.

[25] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, “An Autonomous Host-Based Intrusion Detection System for Android Mobile Devices,” *Mob. Networks Appl.*, vol. 25, no. 1, pp. 164–172, 2020.

[26] J. Ribeiro, G. Mantas, F. B. Saghezchi, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, “Towards an Autonomous Host-based Intrusion Detection System for Android Mobile Devices,” in *9th EAI International Conference on Broadband Communications, Networks, and Systems (BROADNETS2018)*, pp. 139–148.

[27] M. Muaaz and R. Mayrhofer, “Smartphone-Based Gait Recognition: From Authentication to Imitation,” *IEEE Trans. Mob. Comput.*, vol. 16, no. 11, pp. 3209–3221, 2017.

[28] M. R. Hestbek, C. Nickel, and C. Busch, “Biometric gait recognition for mobile devices using wavelet transform and support vector machines,” *2012 19th Int. Conf. Syst. Signals Image Process. IWSSIP 2012*, no. April, pp. 205–210, 2012.

[29] T. Murao, K., Tobise, H., Terada, T., Iso, T., Tsukamoto, M. and Horikoshi, “‘Mobile phone user authentication with grip gestures using pressure sensors,’” *Int. J. Pervasive Comput. Commun.*, vol. 11, no. 3, pp. 288–301, 2015.

[30] A. Buriro, B. Crispo, F. DelFrari, and K. Wrona, “Hold and Sign: A Novel Behavioral Biometrics for Smartphone User Authentication,” *Proc. - 2016 IEEE Symp. Secur. Priv. Work. SPW 2016*, pp. 276–285, 2016.

[31] B. Attaullah, S. Gupta, and B. Crispo, “Evaluation of Motion-based Touch-typing Biometrics in Online Financial Environments,” pp. 219–226, 2017.

[32] A. Buriro, S. Gupta, and B. Crispo, “Evaluation of Motion-Based Touch-Typing Biometrics for Online Banking,” *Lect. Notes Informatics (LNI), Proc. - Ser. Gesellschaft fur Inform.*, 2017.

[33] Y. Obuchi, “‘PDA speech database,’” 2006. .

[34] N. Forsblom, “‘Were you aware of all these sensors in your smartphone?,’” 2015. [Online]. Available: https://blog.adtile.me/2015/11/12/wereyou-%0Aaware-of-all-these-sensors-in-your-smartphone/.

[35] A. De Luca, A. Hang, E. Von Zezschwitz, and H. Hussmann, “I feel like i’m taking selfies all day! towards understanding biometric authentication on smartphones,” *Conf. Hum. Factors Comput. Syst. - Proc.*, vol. 2015-April, pp. 1411–1414, 2015.

[36] T. Sloane, “‘Behavioral biometrics: the restructuring of the authentication landscape,’” 2017. .

[37] NIST - National Institute of Standards and Technology, “Glossary | CSRC.” [Online]. Available: https://csrc.nist.gov/glossary/term/access-control.

[38] V. C. V. Hu, D. F. Ferraiolo, and D. R. Kuhn, “Assessment of access control systems,” *Nistir 7316*, p. 60, 2006.