Mayrhofer, René; Sigg, Stephan

Adversary Models for Mobile Device Authentication

Published in:
ACM Computing Surveys

DOI:
10.1145/3477601

Published: 01/12/2022

Document Version
Publisher's PDF, also known as Version of record

Please cite the original version:
Mayrhofer, R., & Sigg, S. (2022). Adversary Models for Mobile Device Authentication. *ACM Computing Surveys*, *54*(9), 1-35. Article 198. https://doi.org/10.1145/3477601

Adversary Models for Mobile Device Authentication

RENÉ MAYRHOFER, Google and Johannes Kepler University Linz, Austria
STEPHAN SIGG, Aalto University, Finland

Mobile device authentication has been a highly active research topic for over 10 years, with a vast range of methods proposed and analyzed. In related areas, such as secure channel protocols, remote authentication, or desktop user authentication, strong, systematic, and increasingly formal threat models have been established and are used to qualitatively compare different methods. However, the analysis of mobile device authentication is often based on weak adversary models, suggesting overly optimistic results on their respective security. In this article, we introduce a new classification of adversaries to better analyze and compare mobile device authentication methods. We apply this classification to a systematic literature survey. The survey shows that security is still an afterthought and that most proposed protocols lack a comprehensive security analysis. The proposed classification of adversaries provides a strong and practical adversary model that offers a comparable and transparent classification of security properties in mobile device authentication.

CCS Concepts: • **Security and privacy → Mobile platform security**; Trust frameworks; **Authentication;**

Additional Key Words and Phrases: Mobile device authentication, adversary model, survey

ACM Reference format:
René Mayrhofer and Stephan Sigg. 2021. Adversary Models for Mobile Device Authentication. *ACM Comput. Surv.* 54, 9, Article 198 (October 2021), 35 pages.
https://doi.org/10.1145/3477601

198

1 INTRODUCTION

Mobile devices carry an increasing variety of personal data. For instance, recent proposals to include electronic identities into smartphones to replace classical photo identification such as driver's licenses or passports [124] as well as applications and sensors to more accurately capture the wearer's health status [119], audible interaction,[1, 2, 3] and even emotional state [110, 168] highlight the breath of sensitive data.

[1]https://www.apple.com/ios/siri/.
[2]https://developer.amazon.com/alexa.
[3]https://assistant.google.com/.

R. Mayrhofer and S. Sigg had equal contribution and are listed in alphabetic order.
Later parts of this work have been carried out within the scope of Digidow, the Christian Doppler Laboratory for Private Digital Authentication in the Physical World, funded by the Christian Doppler Forschungsgesellschaft, 3 Banken IT GmbH, Kepler Universitätsklinikum GmbH, NXP Semiconductors Austria GmbH, and Österreichische Staatsdruckerei GmbH and partially been supported by the LIT Secure and Correct Systems Lab funded by the State of Upper Austria.
Authors' addresses: R. Mayrhofer, Google and Johannes Kepler University Linz, Vienna/Linz, Altenbergerstr. 69, 4040 Linz, Austria; email: rm@ins.jku.at; S. Sigg, Aalto University, P.O. Box 1212, 43017-6221 Espoo, Finland; email: stephan.sigg@aalto.fi.

0360-0300/2021/10-ART198
https://doi.org/10.1145/3477601

Mobile devices are therefore becoming a critical component in terms of security and privacy not only in the digital domain but also for interactions in the physical world, with users unlocking their smartphones for short (10–250 s) interactions about 50 times per day on average [80, 121].

In this article, we address **user-to-device (U2D)** authentication, i.e., users authenticating themselves before being able to use certain functionality of a device [211, 267], as well as two other forms of authentication, **device-to-device (D2D)** [50, 94, 183], and **device-to-user (D2U)** [89, 181]. For an excellent discussion and history of adversary models also in other domains, please refer to Reference [78].

U2D authentication can be performed by one or a combination of four *factors*[4] [84, 175]:

(1) something a user knows (passwords, PIN codes, graphical patterns, etc.)
(2) something a user possesses (hardware tokens, keys, etc.)
(3) something a user is (static biometric, e.g., fingerprint, face, iris, hand geometry, vein patterns)
(4) something a user does (dynamic biometric, e.g., gait, handwriting, speech)

Many authentication *methods* have been proposed for mobile devices, however, a canonical U2D authentication did not yet converge. Instead, approaches have their respective advantages and disadvantages [66, 120]. Second factor authentication with something a user possesses often demands D2D authentication through wireless communication. Secure D2D authentication is thus a condition to using wireless devices as hardware token for U2D authentication. In this article, we do the following:

- Survey security analyses in the state of the art and derive their assumptions (which are often not explicitly stated) about attackers of such authentication methods. These so-called *adversary models* are a sub-set of threat models commonly applied to cryptographic protocols.
- Show that existing security evaluations of these methods often lack, with many proposals using an insufficient number of volunteers or missing independent analysis by others.
- Propose a qualitative classification of adversaries to mobile device authentication that enables a more systematic adversary modeling, and use this *scheme* in our review.

We design our classification scheme by studying the requirements for useful adversary models at a meta level, with the aim of applying specific instances of these model classes to individual authentication methods. Our intention is for this scheme to be used for future research, giving authentication methods a concrete security level to aim for and to test against. Finally, this article is also a call for action to improve the state of the art in security testing of mobile device authentication.

2 AUTHENTICATION ON MOBILE DEVICES

General threats for user authentication, which include brute-force, password guessing, installing malware, and hardware-level exploits to bypass authentication, typically also apply to mobile devices. Mobile device security, however, is inferior to security on desktop computers [51, 214]. In mobile device scenarios, additional security threats exist [23] because of usability issues or limitations due to smaller size (e.g., watches), and in some cases even due to computational and storage capabilities, for instance, on implanted, medical or wearable devices (e.g., pacemakers, earables, hearing aids) [35, 125, 220].

2.1 Adversary Models for User Authentication

In a recent meta survey by Ferrag et al. [12], impactful surveys on mobile device authentication are analysed [7, 82, 105, 116, 147, 159, 188, 211, 214, 252, 267]. In total, these articles describe 26

[4] For D2D and D2U authentication, various factors and physical channels have been proposed, but no systematic classification has so far been accepted as common knowledge.

attacks, 5 threat models, and 4 authentication categories. By complementing this work on attacks and countermeasures, we target adversary models.

To describe the security properties of a particular protocol, formal models are employed in the literature. The most famous of these adversary models for communication channels is the Dolev–Yao model.[5] It assumes that communication partners trust their encrypted messages to an adversary for delivery [79]. The adversary may use any information obtained from previous messages in attempts to decrypt the information and is, in particular, not constrained by other assumptions. The Dolev–Yao model is indistinguishable under chosen plaintext attacks, respectively chosen ciphertext attacks (IND-CPA/IND-CCA) for formal cryptographic protocol verification [24].

The existence of such accepted standards is crucial for the field, since it (1) helps to build trust in security mechanisms, (2) generates a common ground on which approaches are comparable, and (3) creates incentives to build stronger security schemes. It is also a necessary requirement for (4) the generation of business models grounded on secure technology.

In mobile device authentication, however, the literature has yet to converge on a common adversary model. While the Dolev–Yao model has been applied also for mobile device authentication [247, 275], this approach has shortcomings as it does not reflect the specific nature of mobile device authentication. For instance, authentication on mobile devices is performed in public spaces, potentially under video surveillance. Furthermore, the user interface is limited, and thus prevents some strong authentication mechanisms.

The landscape of mobile device authentication methods is fragmented and methods are hardly comparable to each other. This creates uncertainty on the security properties and on the appropriateness of any mobile device authentication method. Challenges to selecting appropriate security margins and cryptographic parameters are that (1) real-world applications require different security levels [153] and that (2) the resources (e.g., attention, constrained or absent interfaces) in mobile settings place limitations on the authentication method [44]. Adversaries differ, for instance, in their *capability* (ability, training, knowledge), e.g., typical user, developers, or manufacturers, and in the *effort* (storage, computational, monetary) they invest, e.g., individuals, organizations, or nation states.

Table 1 summarizes recently proposed security models sorted by their year of publication. In particular, the discussion on the best suited modality to condition and build the threat model on, has not yet converged. For instance, Ong et al. and Boyd et al. define security levels based on key size, block size, and type of data [38, 207], while Hager et al. and Burmester et al. consider performance, energy and resource consumption to be most relevant [44, 113]. This relates to Damgard et al. who analyse the tradeoff between complexity and security [58]. Likewise, also Ng et al. and Paise et al. see computational complexity as the relevant measure to distinguish adversarial classes [202, 209]. Instead, Sun et al. suggest the quality of protection to measure the level of security [259], while Ksiezopolski et al. distinguish between types of applications to define the adversary model [153]. An adversary model for mobile settings that is based on a Dolev and Yao–type adversary model has been proposed in Reference [76]. A different approach is taken by Ahmed et al. [4], who identify a least-strong attacker by iteratively testing against decreasing security strength.

A number of further adversary models have been proposed for specialized cases within the larger frame of mobile device settings. Specifically, this regards the adversary model by Gligor, which is specifically targeted toward mobile ad hoc networks [106] as well as a collection of adversary models toward forensic investigations on mobile phones, which were proposed by Azfar et al. [18] and Do et al. [77]. Notably, Do et al. defined their adversary via her goals, assumptions and limitations. This framework was later applied by them also to an app-based adversary model, where the classes were slightly modified to replace limitations with capabilities [78].

[5]Other types of formal definitions for authentication can be found, for instance, in static analysis or type theory [1, 34].

Table 1. Previously Proposed Adversary Models

Paper	Brief summary of the proposed contribution	Year
Ong et al. [207]	Security levels based on key size, block size, and type of data	2003
Hager [113]	Security levels conditioned on performance, energy and resource consumption	2004
Ksiezopolski et al. [153]	Different applications require different security levels	2007
Gligor [106]	Adversary model specifically focused on mobile ad hoc networks	2007
Sun et al. [259]	Evaluation model based on quality of protection	2008
Damgård et al. [58]	Tradeoff between complexity and security in symmetric cryptography	2008
Ng et al. and Paise et al. [202, 209]	Security model with adversarial classes based on computational complexity	2008
Burmester et al. [44]	Mobile device security suffers from limited resources	2009
Ahmed et al. [4]	Model conditioned on iterative testing of security strength	2011
Boyd et al. [38]	Defines security levels conditioned on key size, block size and type of data	2013
Do et al. [77]	For forensic investigation, using adversary goals, assumptions and limitations	2015
Song et al. [251]	Metric to measure the strength of pattern lock systems	2015
Do et al. [76]	Dolev and Yao type of adversary model for mobile covert data exfiltration	2015
Azfar et al. [18]	Adapt an adversary model for forensic investigations on mobile phones	2016
Miettinen et al. [191]	Security levels conditioned on the entropy of the context source	2018
Do et al. [78]	Adversary classified by assumptions, goals and capabilities	2019
Ferrag et al. [84]	Survey on threat models for mobile devices	2020
Hosseinzadeh et al. [126]	Adversary model for RFID; grounded on Gong-Needham-Yahalom logic	2020

Specifically, for pattern lock systems on smartphones, Song at al. conditioned their model on characteristics of the pattern-lock design [251], while Hosseinzadeh et al. focus on strictly resource limited RFID devices and base their scheme on Gong-Needham-Yahalom logic [126]. In particular, similar to Reference [4], their model also includes attackers of various strength [202, 209].

Finally, in recent years, context-based device pairing schemes have been proposed that rely on shared access to common contextual stimuli for device-to-device authentication. For this setting, Miettinen et al. [191] have proposed an adversary model that is conditioned on the entropy of the context source.

A survey on threat models for mobile devices has also been presented by Ferrag et al. [84]. In summary, although recent publications on device authentication bring forward a discussion on potential security threats or attacker studies [47, 136, 151], a single universally accepted model is lacking.

Due to the diversity of mobile devices and applications, a single common adversary model might not be feasible. To be useful in general practical application, a meta model, exploiting a *set* of models that account for different usability requirements is needed to qualitatively assess the security level. Therefore, in Section 4 we introduce a classification scheme for adversary models to support such qualitative comparison.

2.2 Limitations of Traditional Authentication Schemes

Electronic devices are traditionally protected via alphanumerical passwords or PIN codes [99]. Due to restrictions in the user interfaces of mobile devices, passwords generate a tradeoff between usability and security. A frequently employed alternative for authentication are graphical patterns. However, such patterns are vulnerable to shoulder surfing or smudge attacks [15, 28]. In shoulder surfing, the adversary either directly or through video [300] observes the authentication sequence and reproduces it. In smudge attacks, the adversary visualizes smears on the touch interface left behind as a consequence of user authentication. The frequent changing of authentication challenges to counter these attacks again compromises usability [73].

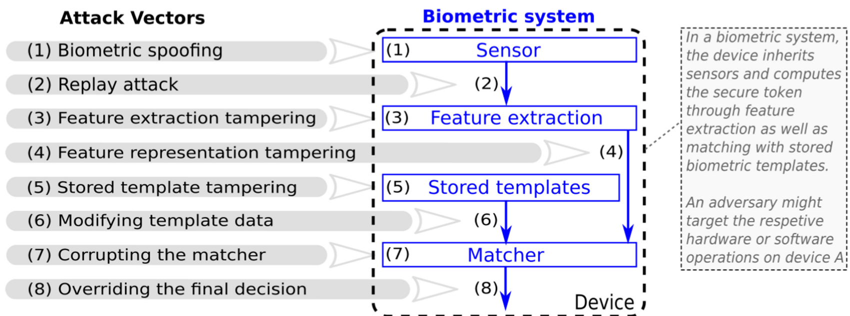

Fig. 1. Visualisation of generic attack vectors in biometric systems (based on Reference [219]). The right side depicts the components of a bU2D authentication system and their interplay while on the left side, various attack vectors on the respective components are exemplified.

Alternatively, biometrics, recognising individuals from behavior and biological characteristics,[6] gained attention for authentication. This is attributed to biometric sensors included in smartphones, such as fingerprint [139] (pore and ridge structure [256]), voice [48] (mel frequency cepstral coding, today deep neural networks [144]), gait (heel-strike ratio [237] or cycle matching [200]), face (features learned in deep neural networks [134]), keystroke dynamics (key-press latencies [195]), or iris [290] (image intensity maps from Hough-transformed Daugman rubber sheet models [281]).

Since biometrics inherit noise, fuzzy pairing is used to account for dissimilarities in the key sequences [140]. Sequences are mapped onto the key-space of an error correcting code (for instance, BCH or Reed Salomon codes), where t bits can be corrected. This process also boosts the success probability of an adversary. Assuming $|c|$ bit long sequences of which t bits are corrected to result in $|c| - t$ bit long keys, the success probability of a single randomly drawn sequence is then only

$$\sum_{i=0}^{t} \binom{|c|}{i} / 2^{|c|} = \frac{\sum_{i=0}^{t} \left(\frac{|c|!}{(|c|-i)! \cdot i!} \right)}{2^{|c|}}. \tag{1}$$

However, biometrics cannot be kept secret and they cannot be revoked [85, 235, 236]. Consequently, they cannot withstand strong attackers under the assumption of targeted spoofing.

Figure 1 shows attack vectors for biometric systems [219]: (1) biometric spoofing [158, 193, 200, 244, 254, 298], (2) replay attacks [112, 230, 268], tampering with (3) feature extraction [167], (4) biometric feature representation, (5) stored templates [102, 255], (6) modifying template data [112, 230], (7) corrupting the matcher, and (8) overriding the final decision. Suggested countermeasures include liveliness detection, supervised enrollment, and securing all stored biometric data [255].

2.3 Adversary Models for Device-to-device Authentication

Device-to-device authentication is used to pair devices under mutual trust. The information relevant for the pairing can be present at the devices, provided by human ineraction, or acquired from the device's software or hardware sensors. Also, for D2D authentication, capabilities and effort of the adversary are of key relevance for adversary models.

Figure 2 summarizes attack vectors for D2D authentication. In particular, devices acquire data (stored, human interaction, or sensed), quantize it to bit strings after pre-processing, apply error

[6] International Organization for Standardization. ISO/IEC 2382-37:2012, Information technology – Vocabulary – Part 37: Biometrics, 2012.

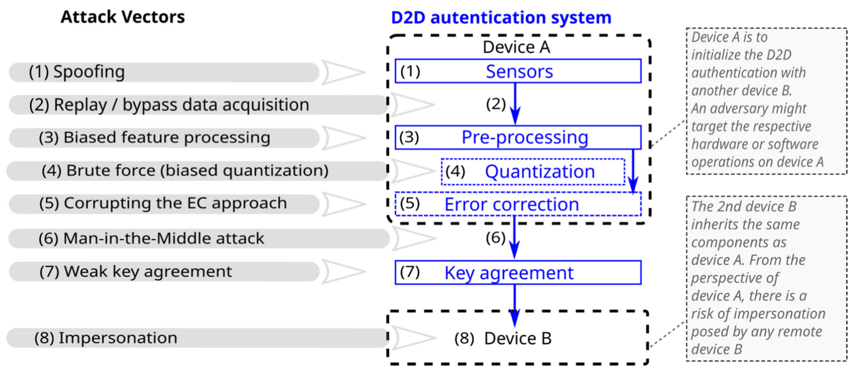

Fig. 2. Visualisation of generic attack vectors in D2D authentication systems (based on Reference [40]). The right side depicts the components of a D2D authentication system and their interplay while on the left side, various attack vectors on the respective components are exemplified.

correction, and agree on a key. Attack vectors are (1) sensors (forcing the device owner to behave in certain ways), (2) bypassing acquisition through replay, and (3) biased feature processing. Some protocols employ communication before the actual key agreement [109, 237, 298] that might (4) potentially leak information; after error correction, which might be (5) corrupted, the key agreement is executed between both devices, thus enabling potential (6) **Man-in-the-Middle (MitM)** (also referred to as Person-in-the-Middle or on-path attacks), (7) exploitation of weak or false assumption-based key agreement, as well as (8) impersonation attacks.

To prevent exhausting the key space, adversaries should be forced into a one-shot model [280]. For instance, **Password Authenticated Key Exchange (PAKE)**, implemented, e.g., by Bluetooth 4.2 **Secure Simple Pairing (SSP)**,[7] IPSec, and ZRTP [143, 262, 303], ensures that the chances of a successful attack depend solely on interactions in the protocol and not on offline computing power [183, 233]. They thus provide sufficient security margin even with short keys K. Most PAKEs allow for multiple parallel protocol runs [280] and threat models that allow implicit error correction choose a relatively high $K = 24$ to still have a negligible attacker success probability even if only 16 out of 24 bits are compared correctly [81]. Similar margins have been chosen in Bluetooth for PIN comparison with $K = 20$ and ZRTP for word comparison with $K = 20$. Modern PAKEs also provide resilience to dictionary, replay, unknown key-share, and Denning-Sacco attacks [274], as well as toward mutual authentication, key control, known-key security, and forward secrecy.

Implicit pairing derives secure secrets from similar patterns, e.g., acceleration [90, 109, 118, 185, 253], audio [238], magnetometer [138], or RF features [179], from devices co-present in the same context.

2.4 Device-to-user Authentication

An adversary able to deceive a user into wrongly trusting the identity of a (malicious) device, can harvest user credentials (biometric or knowledge-based) on a subsequent attempt to log in to the device.[8] Device-to-user authentication attempts to address this issue by establishing a means of authenticating the device to the user. One approach is to visually reveal secret information to establish trust, e.g., by displaying variations of secret images to assure authenticity [225, 226]. However,

[7]Because each Bluetooth pairing uses a new ephemeral passkey, SSP does not provide passkey secrecy [212, 232, 262].
[8]This is similar to the well-known credential phishing problem for websites with users mistaking malicious login forms for genuine ones.

such systems are prone to shoulder surfing. Device-to-User authentication is intended to be used frequently and must therefore mitigate usability drawbacks. Although mutual authentication is well established in D2D authentication (e.g., IPsec [60]), it is rarely used for authentication involving humans. A reason for this is that device-to-user authentication is bandwidth limited due to the limited attention span and cognitive resources for the recognition of patterns by the user [181]. Initial approaches with vibration patterns have been analyzed [89] but seem impractical.

3 ATTACKS AND MODALITIES

For all authentication settings (U2D, D2D, D2U) we distinguish various attack types. An authentication system shall at least prevent *accidental* login from non-authorized users: evaluation against blind guesses (knowledge-based authentication) or samples (biometric) [64, 83, 96, 108].

Any *targeted* attack will be more powerful [240], for instance, biometric spoofing to exploit weaknesses of specific biometric modalities [21, 276], such as using a picture of a target person in an attempt to spoof face recognition.

An *informed* adversary may also attempt to attack the software implementation [217], or to exploit security breaches in the operating system to leak confidential information about the authentication challenge [164], for instance, obtaining extraordinary *privileges* to install a keylogger.

In some cases, historical or other publicly *available data* can be used to elevate chances of a successful attack. For instance, Reference [20] exploits population statistics to launch an attack on a handwriting biometrics system, while Reference [239] leverages a typing-database to attack keystroke authentication.

Adversaries can also *steal* authentication samples to, e.g., replay them [217], to train adversaries to forge patterns [200, 268], or to distort the victim's template and expose it to further attacks [288].

The victim sometimes enables attacks through careless actions that lower the effective security (disabling authentication [96], inadvertently providing access to credentials [19]). Mobile systems can counter this by, e.g., careful choice of images [11] or geometric transformations [234].

Another threat is automated attacks against mobile authentication by *robotic systems* [240].

Finally, *side channels* are a common threat to mobile systems, such as smudge [15] and shoulder surfing attacks [95, 115]. Others are the use of on-device accelerometers to recover a PIN [16] or infering credentials from **channel state information (CSI)**[9] [165]. Countermeasures include input methods that integrate haptic and audio feedback [28], or applying geometric image transformation [234]. Another countermeasure is to lower the number of authentication challenges presented by introducing a limited access safe-mode to access non-critical functions without authentication, while falling back to authentication for other functions [45].

4 CLASSIFYING ADVERSARY MODELS IN MOBILE DEVICE AUTHENTICATION

Our classification of adversary models in mobile device authentication is related to the ISO/IEC 62443 security levels that have been specified in ISA99 [131][10]:

SL0 "No special requirement or protection required"
SL1 "Protection against unintentional or accidental misuse"

[9]Changes in electromagnetic signals at a radio receiver caused by movement of a user or object reflecting the signals are visible in the CSI.

[10]Only a summary document of this standard is available online at the time of this writing, in the form of public slides by Pierre Cobes; Available online at http://isa99.isa.org/Public/Meetings/Committee/201205-Gaithersburg/ISA-99-Security_Levels_Proposal.pdf. In this article, we use the slightly more detailed wording from https://en.wikipedia.org/wiki/IEC_62443.

	Capabilities
C3	Capabilities of **manufacturer, owner, operator** (in-depth knowledge; access to cryptographic keys, instructions, or hardware ports (*insider* [182]).[11]
C2	Capabilities of a **developer** (knowledge about internal structure; no privileged access or possession of cryptographic keys (Kerkhoff's principle)).[12]
C1	Capabilities attributed to an average **user** (benign user of the system, with no additional knowledge).

Effort		
Resources (time, computation, memory, etc.) available to an average **individual** (dependent on culture, country, time, etc.).	Resources available to an **organization** (capture-the-flag teams, organized crime, multinational companies, etc.).	Resources available to a **nation state** (assumed to be able to compel organizations or individuals to assist).
E1	**E2**	**E3**

Fig. 3. Adversaries differ with respect to their capabilities and the effort they are prepared to invest.

- **SL2** "Protection against intentional misuse by simple means with few resources, general skills and low motivation"
- **SL3** "Protection against intentional misuse by sophisticated means with moderate resources, (IACS-specific) knowledge and moderate motivation"
- **SL4** "Protection against intentional misuse using sophisticated means with extensive resources, (IACS-specific) knowledge and high motivation"

We formally classify adversaries in mobile device authentication along the dimensions "capabilities" and "effort" (cf. Figure 3).

In particular, *capabilities* in terms of sophistication of specific attacks on mobile device authentication defines an upper bound on the capability of an adversary and which information and secrets she has access to. This is roughly comparable to the definition of oracles in cryptographic protocol verification.

The *effort* in terms of time, computation, (volatile or non-volatile) memory, and other resources is the upper bound on the amount of energy an adversary is prepared or capable to spend. This limits the number of trials to attack an authentication method (e.g., the number of guesses in a brute-force attack).

Note that effort and capabilities define qualitative (ordinal) aspects in mobile device authentication that are not absolute but vary in their severity with the context in which mobile device authentication is performed. Classifying attacks along these dimensions allows systematic comparison of authentication methods with respect to adversary models. Capabilities and effort are the essential characteristics for adversary classification, which are found prominently in many adversary models in the literature, such as References [25, 78, 208]. They also relate loosely to the terms "skills" and "resources" from the IEC 62443 standard. These two categories are essential and sufficient to describe an adversary model in mobile device authentication. Separating those two dimensions indeed supports a formal classification of adversary models. Practical experience shows an increasing number of attacks with low sophistication (capabilities), but high computational resources (effort), such as cloud-support or networks of compromised machines. A preliminary version of our distinction between adversary classes has appeared in Reference [200].

Using the attack modeling abstractions of "collusion" and "oracles" that is also used to argue on the security of cryptographic protocols, we can compare these two categories to the security levels defined in IEC 62443:

[11]Within the scope of this article, we do not distinguish between an original manufacturer of a system, the current owner, and a technical operator, but assume the superset of all their capabilities. In terms of cryptographic protocol analysis, this class is most similar to a collusion between all parties besides the actual target system of an attack.

[12]We explicitly do not distinguish between original developers and outsiders, as the internal structure can typically be reversed engineered.

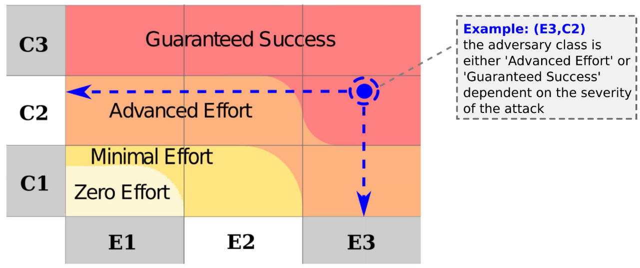

Fig. 4. Summary of adversary classes; The table may be used during the classification and to help for easy identification of adversary classes. Some combinations of capability and effort leave leave freedom to the practitioner with respect to the choice of the most appropriate class and should be decided based on the severity of the attack.

- $\leq$ C1 (*no oracle* access) $\implies$ $\leq$ SL2 ("general skills")
- $\leq$ C2 (access to an *oracle with source code and all other implementation details*, but not to private keys of devices protected with the relevant authentication method) $\implies$ $\leq$ SL3 ("specific knowledge")
- $\leq$ C3 (access to an *oracle with all long-term keys* (explicitly including private keys of individual devices), just not the session keys of past authentication interactions) $\implies$ $\leq$ SL4 ("sophisticated means and specific knowledge")
- $\leq$ E1 (a single adversary, *no collusion* with other parties allowed) $\implies$ $\leq$ SL2 ("few resources")
- $\leq$ E2 (a *group of colluding adversaries*, e.g., multiple angles to observe an authentication event at the same time or multiple tokens correlated for learning something about the internal state) $\implies$ $\leq$ SL3 ("moderate resources")
- $\leq$ E3 (a *collusion of all parties* besides the actual, legitimate user) $\implies$ $\leq$ SL4 ("extensive resources")

These are upper bounds for security levels that can be reached under the assumption of the respective capability and effort classes. Our scheme assumes that all authentication methods can be broken by an adversary with sufficient capabilities and effort. However, the required level of capability and effort to do so differs between authentication methods. We define four classes of adversaries to provide an ordinal scale to compare the security efforts different authentication methods have been tested against (cf. Figure 4).

In particular, we distinguish between zero effort, minimal effort, advanced effort, and guaranteed success attack cases. As can be seen from the figure, in mobile device authentication, the distinction between these attack classes inherits a limited degree of fuzzyness, which stems from the context in which the attack is performed. The same attacker with identical effort and capabilities may conduct attacks of different severity, depending on the context in which the authentication method is situated. For instance, contexts that demand a higher mental load (e.g., due to distraction; higher loudness; impaired vision (e.g., water, smoke, light)) or higher degree of exposedness to public may render attacks of adversaries with same resources and capabilities more significant. Since the context space is infinite, including context means to abandon generality. Therefore, our model tolerates limited degree of fuzzyness in the definition of the attack type.

4.1 Zero Effort Attacks

It is common procedure to measure false-positive and false-negative rates for biometric authentication, and this is also adopted to evaluate authentication schemes such as graphical passwords [8, 223, 263]. Most quantitative evaluations use n subjects with ground truth and compute the confusion matrix of authentication attempts against stored templates. Common measures such as accuracy, precision, recall, true-/false-positive/negative rates, or F-measure are all based on this same principle [31, 42]. We refer to this a zero effort attack, because no malicious adversary other than benign subjects exists (adversaries with basic capabilities (**C1**), and small effort (**E1**)). Zero effort attacks represent the risk of random success and include naïve (non-targeted) brute force attacks. Examples are honest-but-curious office colleagues, or a stranger who chances upon a misplaced device.

In terms of IEC 62443, zero effort attacks can happen in both SL0 and SL1 (random or unintentional misclassification).

4.2 Minimal Effort Attacks

A minimal effort attack is targeted, for instance, mimicking gait, but not with particular sophistication. The adversary has no specific system knowledge (**C1**), but moderate effort (**E1–E2**). Minimal-effort adversaries have the explicit intention of attacking an authentication method and a specific target. Many published approaches used minimal effort attacks in their analysis, typically with students or colleagues from the same research group, with low effort and low to average sophistication.

Minimal effort attacks are possible up to SL2 with a growing spectrum of computational resources available to otherwise unskilled attackers.

4.3 Advanced Effort Attacks

Advanced effort attacks show higher sophistication (**C1 and C2**), such as, e.g., professional actors trained in imitating body motions, and significant effort (**E1–E3**), loosely mapping to SL3. We explicitly exclude the combination of (insider) advanced developer-level sophistication with nation-state effort (**E3, C2**), which would map to SL4. However, it does not seem helpful for evaluating mobile device authentication methods.

4.4 Guaranteed Success Attacks

A guaranteed success attack succeeds in breaking the security of an authentication method. It allows for any system to describe which capabilities or effort are required for a successful attack. Authors of device authentication methods are advised to include this adversary class to define the minimum adversary expected to break the system. An adversary in this class may possess all capability (**C2–C3**) and effort (**E1–E3**). Note that low-effort guaranteed success attacks are possible, for instance through access to cryptographic credentials (**E1, C3**).

Our notion of guaranteed success does not have a correspondence in IEC 62443 security levels; it is one area where we argue that existing standards are lacking in explicitly defining which adversary assumptions are outside the scope of security designs.

5 LITERATURE SURVEY: ADVERSARY MODELS FOR MOBILE AUTHENTICATION

We discuss proposals for mobile authentication and adversary models used, and group the literature according to the adversary class utilized to allow a domain-specific discussion of adversary models. A summary of the publications covered is given in Tables 6 to 9. We recommend to use the survey as a reference and refer the informed reader to the overview in Figure 5 to quickly navigate to the section of her interest. In addition, attack schemes are collected in Tables 2, 3, and 4.

Fig. 5. Overview and structure of the literature survey.

5.1 Biometric User-to-device Authentication (bU2D)

A large body of work has exploited biometric stimuli for mobile authentication [189]. Measures cover, for instance, spoken audio, keystroke dynamics, face biometrics, gaze, application usage, iris, gait, or fingerprints [132].

Most work in this domain show the general feasibility of a working principle (E1, C1; zero effort), by using a small number of subjects distinguished by the modality, but no threat model, attack scenario, or analysis of password space. Table 2 summarizes attacks on biometric authentication.

5.1.1 Speech and Audio. A number of *zero effort* attacks has been considered for biometric systems based on speech and audio. For instance, in speakersense [173], during a voice phone call a person is identified. The system was tested with 17 subjects, achieving over 95% of accuracy.

However, an adversary actively trying to break the system has not been considered (E1, C1; zero effort). For instance, already a *minimal effort* attack using voice impersonation (replay) might trick the system [48]. A protection against such attack is proposed by exploring the magnetic field emitted from loudspeakers to distinguish between playback and live voice. Note that, an informed *advanced adversary*, not using magnetics based loudspeakers with access to respecive resources (advanced microphones) could easily circumvent this protection.

Another example for a system tested only with respect to *minimal effort* attacks is Reference [302]. The authors utilize the audio system of the phone as a doppler radar to obtain further evidence on speaker identity. The authors launched mimicry attacks (adversary with access to video recording and practice) but did not consider advanced (e.g., developer) sophistication.

An example of a comprehensive security discussion in this domain is the usable two-factor authentication based on proximity measured from ambient sound is Reference [142]. Starting from false acceptance and false rejection rates (*zero effort*), *advanced effort* attacks are considered (similar environment, same media) and the analysis further distinguishes remote from co-located attacks, which then includes *definite success* attacks (E3, C3; guaranteed success).

5.1.2 Keystroke and Touch Dynamics. Keystroke and touch dynamics, specifically the usage patterns of keyboard or a touch screen interaction inherits features of a biometric and has thus been considered for means of bU2D authentication. An overview on the use of keystroke-dynamics for mobile devices is provided in Reference [267]. A number of studies consider *zero effort* attacks only, such as Reference [52], to authenticate phone users via keystroke analysis of their PIN input [52]. Authors report equal error rates (E1, C1; zero effort) but ignore active adversaries with access to advanced resources, such as key-press latencies that can be spoofed with a generative keystroke dynamics model [195] via trained replay attacks [217] or utilizing audio [268] or video [300].

Table 2. Attacks on Mobile Biometric Authentication Systems

Paper	Modality	Attack scheme	Year
Gafurov [103]	Gait	Impersonation	2006
Stang [254]	Gait	Continuous visual feedback impostors	2007
Gafurov [102]	Gait	Spoof/various attacks	2007
Ruiz et al. [230]	Iris	Fake images	2008
Derawi et al. [72]	Gait	Active impostor	2010
Mjaland et al. [193]	Gait	Active long-term trained impostors	2010
Rahman et al. [217]	Keystrokes	Snoop-forge-replay attack	2013
Tey et al. [268]	Keystrokes	Imitation through Mimesis technique	2013
Karapanos et al. [142]	Audio	Advanced co-located attackers	2015
Kumar et al. [158]	Gait	Treadmill attack	2015
Liu et al. [170]	Keystrokes	Snooping Keystrokes with mm-Audio	2015
Monaco et al. [195]	Keystrokes	Spoof keypress latencies	2015
Gupta et al. [112]	Iris	Attacks: Masquerade, Replay, Database	2016
Xu et al. [298]	Gait	Passive/active impostor (imitation), MitM	2016
Zhant et al. [302]	Speech	Mimicry	2017
Abdelrahman et al. [2]	Keystrokes	Thermal attacks on mobile user authentication	2017
Muaaz et al. [200]	Gait	Active impostor (imitation)	2017
Trippel et al. [161]	Gait	Poisoning acoustic injection attack	2017
Khan et al. [146]	Keystroke	Real-time mimicry attack guidance system	2018
Tolosana et al. [273]	Signature	Analysis of different spoofing (presentation) attacks	2019
Marcel et al. [176]	Biometrics	Handbook of biometric anti-spoofing	2019
Vyas et al. [285]	bio-sensors	Attack types on body area networks using bio sensors	2020
Tiefenau et al. [270]	Biometrics	Attacks bypassing authentication on mobile devices	2020
Neal et al. [201]	Behaviour	Spoofing (presentation) attacks on various biometrics	2020
Jia et al. [135]	Face	Evaluation of 30 face spoofing attacks	2020
Hagestedt et al. [114]	Eye	Attacks on Classifiers for Eye-based User Modelling	2020

Examples for studies considering *minimal effort* adversaries targeting specific subjects are References [33, 129] or Reference [64] to authenticate from dynamics of using pattern-unlock (E1, C1; minimal effort). However, all these approaches omit investigation on protocol weaknesses or potential bias in the keystroke dynamics patterns due to statistical distributions over a larger set of users [239].

5.1.3 Face. Face features may be used for authentication and are adapted also in commercial hardware[13] [74, 231]. An example for a *zero effort* study is Reference [149] who test their approach using face, teeth (stereo cameras), and voice on a database with 50 subjects to report EER, FAR, and FRR (E1, C1; zero effort), but ignoring targeted attacks using advanced resources such as replay or database attacks.

Examples for *minimal effort* studies are References [57, 74, 88], who consider to break face-based continuous authentication of 24 subjects by an impostor with no specific system insight (E1, C1; minimal effort). These studies were not tested against *advanced attacks*, such as impersonation or dodging via image manipulation [244] or using images from online social networks [167].

5.1.4 Iris. Features from the iris are considered as one of the strongest biometrics, and are, consequently, also employed in bU2D authentication. Iris recognition on mobile phones has, at that time, been constrained by the limited resources of the phone and have been respected in the *zero effort* study in Reference [148]. Without an adversary study, only successful instrumentation has been verified (E1, C1; zero effort). A number of *advanced effort* attacks against iris verification

[13] e.g., Apple FaceID: https://support.apple.com/en-us/HT208108 (an exact adversary model is not publicly documented).

comprise fake images [230], masquerading (dilation and contact lenses), database and template hacking attacks [112].

5.1.5 Application Usage Patterns. Application usage patterns constitute another biometric for mobile device authentication. This has been tested, for instance, in a *zero effort* study in Reference [284] with 50 subjects. However, an attack study is missing (E1, C1, zero effort), as well as monitoring application usage via other apps on the phone [249].

5.1.6 Gait. Gait characterizes the way a person is walking and is believed to be difficult to mimic by adversaries. Despite studies suggesting gait as biometric feature [71, 100, 132, 228], investigations on security features and entropy of gait are lacking, for instance, with respect to impact of natural gait changes over time by clothing, footwear, walking surface, walking speed and emotion [36, 205, 250].

Early studies on gait-based mobile authentication (shoe-mounted [22, 127, 196]; waist-mounted [5, 46, 72, 122, 123, 197, 227]; hand, breast pocket, hip pocket [282]) used *zero effort* adversaries, mainly investigating feasibility (E1, C1; zero effort) and did not consider attacks.

Examples for *minimal effort* studies on gait-authentication are References [101, 103], which consider from pairs of 22 subjects the robustness of gait-authentication against impersonation attacks (E1, C1; minimal effort). In an *advanced effort* study in Reference [200], professional actors were instead employed to mimic the gait of 15 subjects with close physical properties (E2, C2; advanced effort). Other *advanced effort* study comprise control of the speed, step-length, thigh lift, hip movement and width of steps [158] (E2, C2; advanced effort), intensively training individuals over multiple days [193] (E2, C2; advanced effort) or exploiting a 100+ subject database of gait sequences [101, 102] (E1, C2; advanced effort). In addition, the high accuracy of video-based gait recognition systems also empowers an adversary to generate a database of gait information on multiple subjects unnoticed [236].

5.1.7 Fingerprint. Biometric authentication using fingerprints is frequently installed in mobile systems [276]. Typical attack vectors are (1) and (2) in Figure 4, since fingerprint impressions are easily left on surfaces touched [235]. Attacks on fingerprint-based systems are discussed in Reference [139]. An *advanced effort* study providing countermeasures against such attacks presents a system combining biometrics, possession, and continuity features for progressive authentication (switching between different security levels conditioned on the confidence in the authentication) [224]. The study comprises 26 attack attempts using 3 attack scenarios in which the attacker had system knowledge and tried to avoid detection via video and audio sensors (E1, C2; advanced effort).

5.1.8 Body Impedance. Rasmussen et al. propose a pulse-based biometric for two-factor or continuous authentication. In their approach, a metal keyboard sends small electric current through the user's body of which the frequency response is used for authentication [178]. The study investigates usability and disucsses the theoretical password space (E1, C1; minimal effort). However, it lacks a targeted attack study and an investigation on the uniqueness of body impedance in a larger population.

5.2 Usably Secure User-to-Device Authentication

Similarly to biometrics, **usably secure user-to-device authentication (uU2D)** schemes are conditioned on specific patterns have been presented for authentication. Attacks on these authentication schemes, as summarized in Table 3, are either related to traditional attacks on authentication systems or tailored to the respective modality, such as shoulder-surfing or imitation attacks.

Table 3. Attacks and Security Analysis of User-to-Device Authentication Systems

Paper	Modality	Attack scheme	Year
Dhamila et al. [73]	Image	Brute force, observer, intersection attacks	2000
Thorpe et al. [269]	Image	Dictionary attack	2004
Davis et al. [61]	Image	Password distribution	2004
Ku et al. [155]	Image	Dictionary, replay, compromise password file, DoS, predictable *n*, insider	2005
Dirik et al. [75]	Image	Dictionary attack	2007
Hayashi et al. [117]	Image	Brute force, educated guess, observer, intersection	2008
Brostoff et al. [39]	Image	Human bias in password choice	2010
Sun et al. [258]	Multi-touch	Shoulder-surfing (video observation and disclosure of exact password)	2014
Yue et al. [300]	Touch	Technical challenges of blind recognition of touched keys from video	2014
Huhta et al. [128]	Acceleration	Attack on the ZEBRA system [177], discuss improvements	2015
Li et al. [166]	Acceleration	Imitation of head movement	2016
Nguyen et al. [203]	Image recall	Shoulder surfing	2016
Cha et al. [47]	Pattern	Optimal conditions for smudge attacks, protection, mitigation strategies	2017
Zhang et al. [301]	Voice	Dolphin attack: inaudible voice commands	2017
Kraus et al. [151]	Emoji recall	Shoulder surfing	2017
Chen et al. [48]	Audio/Magnetom.	Machine-based voice impersonation	2017
Miettinen et al. [191]	Audio	Impersonation, Man-in-the-Middle	2018
Prange et al. [216]	various	Threats and design flaws of smart home environments	2019
Prange et al. [215]	various	Model of security incidents with personal items in public; survey and stories	2019
Shin et al. [245]	pattern	Attacks on Android pattern lock systems	2020
Alqahtani et al. [9]	image	Attacks on machine learning for image-based captcha	2020
Bhana et al. [27]	Various	Usability and security comparison of authentication schemes	2020
Vyas et al. [285]	Various	Attack prevention schemes for body area networks	2020

5.2.1 Image. In image-based uU2D authentication, the user is presented one or more challenges based on images, such as image content or sorting of images. Image-based authentication has an advantage [261, 292] over password or PIN-based authentication due to improved usability [293], and since it is easier to *recognize* or *recall* an image than a text [62, 73]. However, memorability and security strength of image-based recognition in comparison to PIN and password based solutions when multiple (10–20) of such passwords need to be remembered, has not been considered in the literature. Davis et al. [61] further found that (1) user password selection is biased by race and gender [39], thus lowering password entropy, (2) the need for several rounds to provide a reasonably large password space impairs usability, and (3) recognition-based systems are vulnerable to replay attacks [15, 266]. It is a research challenge to exploit memorability to improve freshness of authentication challenges [203].

Recognition-based. Recognition-based systems condition authentication on the selection of a specific image or groups of images in a partiular order. A commercial example is Passfaces,[14] which uses images of faces for authentication. *Zero-effort* studies proposing implementations of this approach with no security investigation, are, for instance, References [6, 62, 263] (E1, C1; zero effort).

A *minimal effort* study was presented in Reference [73], in which the authors show that failed logins raised to 30–35% for PIN and password based authentication, while it dropped only to 10% and 5% for artwork and photo images. Several attacks are discussed (brute-force, observer, intersection), while other attacks, e.g., on the image database or on the system are disregarded (E1, C1; minimal effort). Another example for a *minimal effort* study is Reference [151] (replace numerical PIN-pads with emojis), which studied memorability and robustness against shoulder surfing (E1, C1; minimal effort) but did not consider any strong adversaries.

Recall-based. These graphical password schemes require that a pattern is recalled, e.g., drawing a shape [133]. Since the precision required to establish a sufficiently large password space is high,

[14] www.realuser.com.

cued recall schemes provide cues that help to achieve sufficient precision [30, 32], such as images to guide the input or distorted and blurred images [117].

Example *zero effort* studies are Reference [69] (pure recall) or References [8, 213] (cued recall), which focus on usability and the risk of observation attacks (E1, C1; zero effort), but lack an attack study or security analysis.

A *minimal effort* study is Reference [150], which calculates the size of the password space and remarks that chosen passwords are clustered [150] (only 10^{-8} of the space is used 25% of the time) (E1, C2; minimal effort). Other attack vectors, such as shoulder surfing or smudge attacks are not exploited.

In their *advanced effort* study, Ku et al. [155] study a variation of this scheme for its reparability [130], resistance against dictionary attacks, replay attacks, compromising the password file, denial-of-service, predictable *n* attack and the insider attack [26, 154, 192, 269] (E2, C2; advanced effort). Another example is Reference [75], who analyze the PassPoints scheme (regions in an image constitute an authentication challenge), originally presented in a zero effort study in Reference [293]. The authors present an evaluation approach for graphical password schemes, in which a password consists of a sequence of click points in an image. For the attack study, the probability of click points was considered as well as attention-related saliency features (luminosity contrast, color contrast, foreground) in a study with more than 100 subjects. For the images used, the observed entropy was derived from the observed FoA map (clicking probability to every grid square) (E2, C2; advanced effort). Definite success cases and nation state adversaries with strong capabilities are not considered.

5.2.2 Multi-touch. The concept of multi-touch has been proposed to increase the password space, to reduce time to input a password and to address security risks through shoulder-surfing and smudge attacks.

In References [206, 223], usability issues are in the focus of their discussion while security threats appear as after-thoughts (E1, C1; zero effort). For instance, References [17, 264, 265] propose finger-tapping for multi-touch pin authentication and investigate only usability in their 30-user case study (E1, C1; zero effort).

In an *advanced effort* study on multi-touch input in Reference [258], the authors recruited 30 volunteers to test rotation-invariant multi-touch free-form passwords. Ten adversaries with access to video recorded password inputs and exact password shapes attacked the system (E2, C1; advanced effort).

5.2.3 Gaze-based. Eye-gaze may be tracked and thus may serve as an input modality for uU2D authentication. Gaze-based password entry exploits the movement of the eye for password input [68].

In *zero-effort* usability studies in References [68, 157, 291], the subjects had to focus on some location on the screen or perform eye gestures (E1, C1; zero effort), without any attacker consideration.

A similar approach was investigated in a *minimal effort* study in Reference [95], where a subject stares for a certain period (the dwell time) at an area on the display to perform an action [289]. The authors evaluated their approach in a study with 18 subjects and achieved an error rate for the password input of 96% (E1, C1; minimal effort). However, an attack study was not conducted.

An *advanced effort* study has been prestented in Reference [41] and authors investigated the security of gaze-based graphical passwords using saliency masks by theoretical estimation of password space and discussion of threat models (E2, C2; advanced effort).

An example of a medium effort and capability *guaranteed success* study is Reference [63]. Password input by 24 subjects was video-recorded so that attackers could break the system in a single

Table 4. Attacks and Security Analysis of Device-to-Device Authentication Systems

Paper	Modality	Attack scheme	Year
Mayrhofer [180]	Arbitrary	Man-in-the-Middle, DoS	2007
Schurmann et al. [238]	Audio	Statistical properties (keys); brute force, DoS, MitM, audio amplification attacks	2013
Truong et al. [275]	Various	Performance of sensor modalities wrt. Dolev–Yao adversary (relay attacks)	2014
Anand et al. [13]	Audio	Extract vibration sequence from audio noise	2016
Kwong et al. [161]	Acceleration	Active adversary emitting acoustic interference at MEMS resonant frequency	2017
Findling et al. [91]	Shaking	Protocol-specific attacks: observatory, cooperative, handshaking	2017
Gong et at. [107]	Audio	Spoofing, replay and zero effort attacks	2017
Schurmann et al. [236]	Gait	Brute-force, gait mimicry, video, adding a malicious device	2018
Bruesch et al. [40]	Gait	Gait-pairing: brute-force, mimicry, video, malicious device, protocol weakness	2019
Focardi et al. [93]	QR	Performance, size and security of cryptographic schemes with respect to usability	2019
Shafi et al. [242]	Spoofing	Attack on the downlink (half-duplex) in cellular communication	2020

try in 96% of the cases while the method was robust against simple shoulder surfing (E2, C2; guaranteed success).

5.2.4 Audio based. It is possible to use auditory stimuli for uU2D authentication. A targeted but unsophisticated attack study (*advanced effort*) over audio-based PIN input has been presented in Reference [28]. Subjects have been instructed and conducted targeted attacks after observing the login process of the target. However, attackers were artificially limited in their access to the recorded material (e.g., no audio, reduced quality) and time (E2, C2; advanced effort). In particular, it was derived in Reference [191] that time is critical in impersonation and Man-in-the-Middle attacks and that otherwise the secure establishing of a shared secret is possible.

A *guaranteed success* study is presented in Reference [142], who propose to use similarity in ambient audio as a second factor to authentication. Weak and strong adversaries are considered up to guaranteed success attacks where the adversary is physically located in the same audio context (E3, C3; guaranteed success).

5.2.5 Acceleration-based. Acceleration sensors are nowadays integrated in a multitude of devices. Consequently, the stimuli that can be utilized for acceleration-based authentication are available across a broad range of devices. An example for a *zero effort* attack is Reference [171], in which gesture-based authentication from acceleration sequences was investigated for its usability with five subjects (E1, C1; zero effort). An attack study has not been conducted though.

A targeted but unsophisticated attack study (*minimal effort*) is, for instance, Reference [166] (authentication utilising head-movement patterns while listening to an audio pattern). The authors provided videos of successful authentication attempts to the non-trained amateur attackers to imitate the authentication movements (E2, C1; advanced effort).

An example of an attack study also covering *guaranteed success* is Reference [14]. An in-air hand gesture authentication system was evaluated through experiments including video-based attacks and allowing to watch the video multiple times, rewind, or to play in slow motion (E2, C2).

5.3 Device-to-device Authentication

Device-to-device authentication, or simply pairing, typically exploits similarity in context or proximity to achieve seamless authentication [180]. Alternatively, device-to-device authentication can also be realized following the principles of zero-interaction authentication [55], in which proximity is exploited to verify identity without explicit input, but relying on contextual cues derived from sensor measurements. In Reference [275], security properties of these schemes is evaluated with respect to different sensor modalities and with respect to a Dolev–Yao adversary. Table 4 depicts several attacks on device-to-device authentication.

Table 5. Selection of Publicly Available Datasets in Mobile Authentication

Paper	Modality	Description	Year
Gafurov et al. [102]	Gait	760 gait sequences from 100 subjects	2007
Liu et al. [171]	Acceleration	>4,000 gesture samples, 8 subjects; over multiple weeks; 8 gesture patterns	2009
Fierrez et at. [86]	Biometrics	Speech, iris, face, signature, text, fingerprint, hand, keystroke from 400 subjects	2010
Findling et al. [74]	Face	600 high quality, colored 2D stereo vision face images	2013
Wang et al. [286]	Face	Web faces database	2013
Galbally et al. [104]	Passwords	KoreLogic dataset of 75,000,000 unique passwords	2014
Truong et al. [275]	co-presence	2,303 samples (co-/non-co-present: 1140/1163); Audio, Bluetooth, GPS, WiFi	2014
Shrestha et al. [247]	co-presence	Phone data (temp., gas, humidity, altitude, orient.); 207 samples; 21 locations	2014
Samangouei et al. [231]	Face	Database of 152 facial images	2015
Kim et al. [148]	Iris	500 iris image sequences from 100 subjects	2016
Costa-Pazo et al. [56]	Face	1,190 video sequences of attack attempts to 40 clients	2016
Patel et al. [210]	Face	9,000 (1000 live/8000 spoof) face images	2016
Ramachandra et al. [218]	Face	Databases to benchmark presentation attack resilience	2017
Tolosana et al. [272]	Handwriting	e-BioSign signature and handwriting from 65 subjects	2017
Boulkenafet et al. [37]	Face	4,950 real access and presentation attack videos of 55 subjects	2017
Shrestha et al. [248]	co-presence	100 audio samples from synchronized audio streams for non-co-present devices	2018
Tolosana et al. [271]	handwriting	e-BioDigit database (on-line handwritten digits) & benchmark results	2020

5.3.1 Acceleration-based. For D2D authentication with acceleration, simultaneous movement during physical co-presence are exploited. Examples for *zero effort* studies exploiting vibration are References [162, 186, 187]. They exploit shared vibration sequences between physically connected smartphones or physical tapping of devices onto each other. The prototypes have been validated for their basic functionality but no attack or user study has been conducted (E1, C1; zero effort).

For this kind of key distribution that utilizes vibration as an out-of-band channel, Anand et al. [13] attack vibration-based pairing schemes by overhearing the audio signature of the vibration pattern (E2, C1; minimal effort).

In an *advanced effort* study, Reference [277] authenticate mobile devices toward a remote server, where the challenges are given by the duration of vibration and responses. A number of security issues is discussed, follwed by a publicly available taxonomy and entropy analysis (E2, C2; advanced effort).

Alternatively, gait acceleration has been exploited for authentication between devices that are carried by the same (walking) subject. Instantaneous and characteristic variations in the acceleration and gait sequences, that can be extracted at different body positions constitute the features to a pairing key [54, 163]. This problem has been considered in the *zero effort* studies [198, 199, 260], which discuss general fasibility, usability such as averse affects of orientation differences as well as cross pocket gait-based authentication (left-to-right) but no adversary study (E1, C1; zero effort).

Advanced effort studies on gait-based D2D authentication are, for instance, References [221, 297, 298], who consider impersonation and man-in-the-middle attacks, passive eavesdropping, impersonation, entropy, randomness, key distribution analysis from a study conducted with 14 subjects analyze the randomness of the resulting key (E1, C2; advanced effort). Examples for *guaranteed success* studies on gait-based D2D authentication are References [40, 236], which concisely compare and evaluate several gait-based D2D authentication protocols, and consider brute-force attacks, gait mimicry, informed attackers that exploit protocol weaknesses, as well as powerful adversaries with access to video or possibility to attach malicious devices unnoticed on the persons body (E3, C2; guaranteed success).

A further attack on acceleration-based D2D authentication is to actively emit modulated acoustic interference at the resonant frequency of materials in MEMS sensors to control or modify measured acceleration, and thus inject changes to acceleration sequences [161].

Finally, *minimal effort* studies have been conducted on shaking-based acceleration-pairing [109, 172, 184, 185], where attacker–victim pairs have been built with the purpose of demonstrating the

Table 6. Summary Classification of Adversary Models—Zero Effort

Modality	Refer.	Performance			#	Type	Remark	Year
Gait	[141]	—	E1	C1	44/25/71	bU2D	Feasibility on 3 gait databases, No attack study	2003
Iris	[148]	Detection rate: 99.4%	E1	C1	100	bU2D	Feasibility and success case. No security analysis	2016
Speech	[222]	Rejection rate: <94.1%	E1	C1	16+44	bU2D	Feasibility study, playback attack resilience, no adversary	2019
Gait	[123]	Accuracy: 94.93%	E1	C1	38	bU2D	Android-based gait authentication. No attack study.	2013
Gait	[122]	FAR: 0%, FRR: 16.18%	E1	C1	38	bU2D	Naive brute-force success probability; no attack study.	2015
Gait	[5]	EER=FAR:6.4%, FRR:5.4%	E1	C1	36	bU2D	Feasibility of gait for authentication. No attack study.	2005
Gait	[228]	EER: 6.7%	E1	C1	35	bU2D	Feasibility study, no security discussion	2007
Gait	[282]	EER: 17.2/14.1/14.8%	E1	C1	31	bU2D	Gait-authentication from hand/hip-pocket/breast-pocket.	2006
Gait	[227]	EER: 5.6%&21.1%	E1	C1	21	bU2D	Feasibility of gait for authentication.	2007
Audio	[173]	Accuracy: >80%	E1	C1	15+17	bU2D	Focus on success cases (speaker-distinction)	2011
Gait	[22, 196]	Accuracy: <97%	E1	C1	15	bU2D	Feasibility of gait (shoe-mounted) for authentication.	2008
Gait	[46]	Accuracy: <98%	E1	C1	10	bU2D	Demonstrate the feasibility of gait for authentication.	2012
Iris	[174]	FAR/FRR: <6%/18%	E1	C1	10	uU2D	Feasibility study, general security discussion, no targeted attack	2019
Gait	[127]	Accuracy: 96.133%	E1	C1	9	bU2D	Feasibility of gait (shoe-mounted) for authentication.	2007
Touch	[70]	accuracy: 100%	E1	C1	—	bU2D	Evaluation details unclear, no adversary study	2019
Gait	[100]	—	E1	C1	—	bU2D	Discuss security challenges, no attack study	2007
Keystroke	[27]	—	E1	C1	112	uU2D	Entropy and failures for login, no attack study	2020
Pattern	[69]	—	E1	C1	86	uU2D	shapes of strokes on touch sceen. Questionnaire: Usability	2007
Pattern	[257]	—	E1	C1	81	uU2D	Analytic metric proposed to classify password strength	2014
Image	[62]	Errors: 2%–10%	E1	C1	66	uU2D	Errors, usability, password completion time; no attack study.	2002
Image	[151]	Accuracy: 97%	E1	C1	53	uU2D	Human bias in password choice; shoulder surfing robustness.	2017
Image	[39]	Accuracy: 97%	E1	C1	53	uU2D	Human bias in password choice; no security analysis.	2010
Gaze	[95]	Success rate: 96%	E1	C1	45	uU2D	Zero-effort random success study. No security analysis	2010
Keystroke	[52]	EER: 12.8%	E1	C1	32	uU2D	4-bit and 11-bit pin input; no attack study.	2007
Touch	[204]	Accuracy: 12%	E1	C1	12	uU2D	Low energy tokens for interacition with capacitive devices	2016
Mult.touch	[223]	—	E1	C1	30	uU2D	Multi-touch image authentication. No attack study.	2013
Image	[223]	—	E1	C1	30	uU2D	Focus on usability and password space	2013
Gaze	[68]	—	E1	C1	21	uU2D	Usability of 3 eye-gaze methods; General security discussion.	2007
Image	[293]	—	E1	C1	20	uU2D	Improved usability of the PassPoints cued recall scheme.	2005
QR	[59]	Accuracy: 88%	E1	C1	20	uU2D	Validation and Usability study, no adversaries	2019
Gaze	[157]	Error rate: 4%	E1	C1	18	uU2D	Limited capability threat model (eyes not captured).	2007
Icons	[294]	Accuracy: 90.35	E1	C1	15	uU2D	Shoulder-surfing robust; focus on usability;	2006
M.touch	[17]	Entropy: 15.6bits	E1	C1	13	uU2D	Multi-touch free-form passwords; theoretical password space	2012
M.touch	[206]	—	E1	C1	10	uU2D	Success cases and feasibility; no security analysis	2012
Shaking	[172]	—	E1	C1	8	uU2D	Attack shaking with random acceleration; no video; no entropy	2014
M.touch	[264, 265]	–	E1	C1	6	uU2D	Success cases, usability (memorability & time); password space	2013
Radio	[53]	TP/FP/FN: <95%/6%/51	E1	C1	3	uU2D	De-authentication method; usability and positive cases	2017
Image	[263]	—	E1	C1	—	uU2D	Self-captured images (conceptual study); no security analysis	2003
Image	[8]	–	E1	C1	—	uU2D	Implicit authentication by clicking on objects in images.	2013
Image	[6]	–	E1	C1	—	uU2D	Images for authentication. Concept; no security analysis	2004
Image	[213]	—	E1	C1	—	uU2D	Image-supported password entry; no security analysis	2003
Image	[292]	Accuracy: >90%	E1	C1	—	uU2D	Acceptance rate up to 5 months after training.	2004
Image	[30]	—	E1	C1	—	uU2D	Image-based cued recall; password space and human bias.	2006
Gesture	[111]	—	E1	C1	—	uU2D	Secure smartwatch authentication; No security study/analysis	2019
Gaze	[291]	Success rate: 83%	E1	C1	—	uU2D	Eye gaze input by clustering gaze points. Only usability	2011
Acceler.	[90]	TPR/TNR: 79%/86%	E1	C1	29	D2D	Non-targeted attacks (random success)	2014
Gait	[237]	—	E1	C1	15	D2D	Quantization for gait-based pairing. Statistical analysis keys	2017
Gesture	[171]	Accuracy: 98.6%	E1	C1	5+5	D2D	Authentication from acceleration (DTW matched); usability	2009
Acceler.	[54]	Accuracy: 85%	E1	C1	7	D2D	Feasibility study (correlation); no adversaries	2011
Gait	[260]	Agreement rate: <89%	E1	C1	5	D2D	Propose quantization method based on inter-pulse-interval	2017
Vibration	[162]	Success rate: <60%	E1	C1	—	D2D	Common secret via vibration signatures; No security analysis	2018
Acceler.	[253]	—	E1	C1	—	D2D	Collocation detection; User study unclear; no adversary	2015
Vibration	[89]	Success rate: 97.5%	E1	C1	12	D2U	D2U authentication via vibration patterns; Usability study	2015
Image/text	[225, 226]	—	E1	C1	—	D2U	D2U authentication via visual cues.	2010

robustness against active attacks (E1, C2; zero to minimal effort). Attacks on shaking-based pairing protocols are, for instance, investigated in Reference [91] (observatory, cooperative, handshaking).

5.3.2 Audio. Correlation in audio-readings from co-located devices may also be utlized for D2D authentication. An *advanced effort* audio-based D2D authentication was proposed in

Table 7. Summary Classification of Adversary Models—Minimal Effort

Modality	Refer.	Performance			#	Type	Remark	Year
Behavior	[145]	—	E2	C1	40-158	bU2D	Non-sophisticated attacks on multiple biometric systems	2014
Keystroke	[287]	EER: 12%	E2	C1	104	bU2D	Exploit adversarial noise; Non-targeted attacks	2019
Keystroke	[10]	EER: 9.9%	E2	C1	100	bU2D	Non-targeted comparison of collected keystroke entries	2019
Voice	[302]	EER: 1%; Accuracy: 99%	E2	C1	21	bU2D	Liveness detection system to protect against replay attacks.	2017
behavior	[194]	—	E2	C1	20	bU2D	Interactive biometric authentication; non-targeted attack	2019
Gait	[254]	EER: 26%	E1	C2	13	bU2D	Targeted attacks; video-recordings; physical characteristics	2007
Face	[231]	Accuracy: >0.72	E1	C1	152	bU2D	Feasibility; database of 152 images; No security analysis	2015
Gait	[72]	EER: 20.1%	E1	C1	51	bU2D	Focus on success cases	2010
Gait	[197]	EER: 22.49%	E1	C1	51	bU2D	No attack cases considered	2013
Face	[149]	Error rates: <9%	E1	C1	50	bU2D	FAR & FRR; no dedicated security study	2010
Handwriting	[271]	Mean EER: 14%	E1	C1	50	bU2D	Non-targeted attack from database of samples	2020
Keystroke	[64]	Accuracy: <57%	E1	C1	48	bU2D	Intensive but untargeted (non-sophisticated) attacks	2012
Gait	[123]	Accuracy: 94.93%	E1	C1	38	bU2D	No dedicated attack cases; FAR & FRR	2013
Gait	[198]	EER: 18.965	E1	C1	35	bU2D	EER for orientation-independent gait authentication.	2014
Gait/Face	[87]	EER: 11.4 & 5.4	E2	C1	35	bU2D	Non-targeted blind matching of patterns between subjects.	2018
Gait	[122]	FAR: 0; FRR: 16.18%	E1	C1	34	bU2D	No dedicated attack cases; FAR & FRR	2015
Face	[74]	TP: 0.9781; TN: 0.9998	E1	C1	30	bU2D	Focus on positive case	2013
Keystroke	[129]	EER: 13%	E1	C1	25	bU2D	Limited capability attackers: Password provided; pattern not	2009
Face	[57]	TP: 65%; FP: 35%	E1	C1	24	bU2D	Victims first interacted with device before handing to impostor	2015
Gait	[103]	EER: 16%	E1	C1	22	bU2D	Active impostor; no matching person height, no actors	2006
PPG	[243]	acc: 96.31%	E1	C1	12	bU2D	Limited capability adversary; brute-force, shoulder surfing	2019
Face	[88]	TP: 93.89; TN: 99.95	E1	C1	9	bU2D	Positive cases	2013
Accelerat.	[177]	Accuracy: 85%	E1	C2	20	uU2D	Bracelet: verify typing of legitimate user; weak attacks.	2014
Environm.	[248]	FNR: <14.5%	E1	C2	2	uU2D	Relay attacks; system knowledge assumed	2018
Audio	[48]	FAR/EER/FRR: 0/0/<41%	E1	C2	—	uU2D	Magnetic field from loudspeakers; No tailored attacks.	2017
Magnet.	[137, 138]	Accuracy: 92%	E1	C2	—	uU2D	Comparison: password space PIN-based login	2016
Image	[133]	—	E1	C2	—	uU2D	'Draw a Secret' scheme; theoretical password space; human bias	1999
Image	[269]	—	E1	C2	—	uU2D	Dictionary attacks against graphical password schemes	2004
Image	[117]	—	E1	C1	99	uU2D	Usability; Brute force, educated guess, observer, intersection A.	2008
App-use	[284]	—	E1	C1	50	uU2D	Study positive case with professionals	2016
Headmove	[166]	EER: <7%, FAR: <5%	E2	C1	37	uU2D	Reduced capability video analysis (no audio)	2016
Image	[73]	Success rate: 90%	E1	C1	20	uU2D	Discuss possible attacks and countermeasures	2000
object	[98]	—	E2	C1	15	uU2D	HMD auth.; limited capab. attacks, brute force, shoulder surfing	2019
Impedance	[178]	Accuracy: >87%	E1	C1	10	uU2D	User study and theoretical consideration of the password space.	2017
Drawing	[241]	—	E1	C1	6	uU2D	Threat model; no attacks; no Entropy; no statistical analysis	2014
Keystroke	[33]	Accuracy: 99%	E1	C1	5	uU2D	Random correlation attacks; no sophisticated or active attacker	2013
Shaking	[109]	Success rate: <95%	E1	C1	—	uU2D	Entropy & security analysis; no trained, informed adversary	2012
Shaking	[29]	Success rate: 80%	E1	C1	—	uU2D	Entropy analysis of the generated keys	2007
Pattern	[266]	—	E1	C1	20	uU2D	Shoulder-surfing robust; low capability, non-trained attack.	2006
Pin	[229]	—	E1	C1	8	uU2D	Shoulder-surfing robust; complexity analysis; weak attack.	2004
Audio	[13]	—	E2	C1	—	D2D	Vibration of devices in contact; extract key from vibration noise.	2016
Shaking	[184]	FN: 10.24%; FP: 0	E1	C2	8/30/51	D2D	Competition among limited capability attackers	2007
Gait	[199]	FMR/FNMR: <0.09/0.47	E1	C1	25	D2D	No attack cases; false non match rate / false match rate (FMR)	2015
Vibration	[186, 187]	FN=FP=EER: 9.99%	E1	C1	23	D2D	Synchronized vibration through device-tapping. No attacks.	2014
Context	[191]	—	E2	C1	—	D2D	Impersonation, MitM, no guaranteed success (same context)	2018

Reference [107] in which devices in proximity (round-trip audio signals) are automatically paired. Non-sophisticated replay and spoofing attacks were identified but no attack study conducted (E2, C2; advanced effort).

A *guaranteed success* study is Reference [238], in which authentication is conditioned on ambient audio. Statistical properties of the keys are discussed, as well as limitations of the approach and a number of cases in various environments with different noise conditions is considered, also covering definite success attack scenarios where the attacker establishes the same audio context

Table 8. Summary Classification of Adversary Models – Advanced Effort

Modality	Refer.	Performance			#	Type	Remark	Year
Gait	[193]	EER: 6.2%	E2	C2	50	bU2D	Targeted attacks; trained non-professionals; EER: 6.2%	2010
Gait	[158]	FAR: 70% (attack)	E2	C2	18	bU2D	Developer insight (features) & exploiting treadmill; FAR: 46.66%	2015
Behavior	[156]	EER/FAR: <5.9%/3.3%	E2	C1	30	bU2D	Public lock pattern, strong attacker with video	2019
Face	[135]	Classification Error rate	E2	C1	55/40/40	bU2D	Presentation attacks, targeted from database	2020
Gait	[102]	EER: 13%	E1	C2	100	bU2D	Mimicry, non-trained amateurs; non-matching characteristics	2007
Behavior	[43]	TAR: 99.35%	E2	C1	85+6	bU2D	Targeted attack; attacker strength unclear	2019
Fingerprint	[295]	Acc/FAR/FRR: <99/2/3	E2	C1	90	bU2D	Puppet attack resilience, limited capability (targeted) adversary	2020
Biometric	[224]	Precision = Recall < 93%	E1	C2	20	bU2D	System knowledge, audio/video support; 26 attempts; # unclear	2012
Image	[75]	TPR: >0.79, TNR: >0.68	E2	C2	100	uU2D	Automated attack; 70-80% password points correctly predicted	2007
Force	[152]	—	E2	C1	50+10	uU2D	Targeted attacks, video support	2017
Pattern	[65]	—	E2	C2	32	uU2D	Targeted attacks, video support, shoulder surfing	2014
Pattern	[67]	Accuracy: 44%	E2	C2	24	uU2D	Developer insight & video analysis (incl. playback)	2013
Gaze	[97]	TPR/FPR: 81%/12%	E2	C1	29	uU2D	Targeted spoofing attacks on free-form gaze-passwords	2019
Image	[49]	Success rate: >83%	E2	C2	24	uU2D	Cued Click Points; shoulder surfing and dictionary attacks	2007
Gaze/gesture	[3]	—	E2	C2	16	uU2D	Unlimited video access. schoulder surfing resistant	2019
Gaze	[41]	Success. attacks: <25%	E2	C2	4+12	uU2D	Password space; threat models; Attackers with videos	2012
Pattern	[47]	FAR: 74%	E2	C2	12	uU2D	Smudge attacks: optimal conditions, protection, mitigation	2017
Audio	[28]	—	E2	C2	12	uU2D	Threat: audio-visual recording; Low detail security evaluation	2011
Radio	[179, 278]	FPR: <0.3	E2	C2	—	uU2D	Access to historical information; MitM; powerful adversary	2011
Image	[155]	—	E2	C2	—	uU2D	dictionary, replay, pass compromise, DoS, predictable n, insider	2005
Accel.	[277]	TPR/FPR: 0.7444/0.0978%	E2	C2	—	uU2D	Security issues; public taxonomy; entropy	2016
Gaze	[92]		E2	C1	15+25	uU2D	EOG-based, observation-attack resistant, targeted attacks	2019
Pattern	[234]	success rate: >70%	E2	C1	20	uU2D	Smudge protection; Limited capability attackers: 3 attempts	2014
Multi-touch	[258]	TPR: 97.5%, FPR: 2.3%	E2	C1	30	uU2D	Adversary with video & multi-touch password; FPR: 2.2%	2014
Image	[203]	—	E1	C2	10	uU2D	Always-fresh auth., Random & targeted attacks, non-trained,	2016
Environm.	[247]	FPR: 16.25%, FNR: 8.57%	E1	C2	—	uU2D	Adversary with technical understanding of the system	2014
Multi-factor	[175]	—	E1	C2	—	uU2D	Replay and MitM; finite automata as adversaries	2020
Gait	[200]	—	E2	C2	35	D2D	Trained, matched actors, 15 victims; EER: 13%	2017
Accelerat.	[246]	Prec/recall: >0.94, 0.97	E2	C2	20	D2D	Tap-based pairing via NFC	2016
Audio	[107]	FRR: 1–12%; FAR: <0.8%	E2	C2	-	D2D	Co-presence via acoustic signals; spoofing, replay	2017
Gait	[298]	Agreement rate: <73%	E1	C2	20	D2D	Impersonation, MitM; analyze randomness of keys	2016
Gait	[297]	Agreement rate: <73%	E1	C2	20	D2D	Impersonation, MitM; analyze randomness of keys	2017
Gait	[221]	—	E1	C2	14	D2D	Eavesdrop, impersonate, entropy, key randomness/distribution	2017

Table 9. Summary Classification of Adversary Models – Guaranteed Success

Modality	Refer.	Performance			#	Type	Remark	Year
Audio	[142]	FAR=FRR=<0.01	E3	C3	32	uU2D	Incl. attakcer in same context (guaranteed success).	2015
Generic	[296]	—	E3	C3	—	uU2D	Theoretical study: protocol security, various attacks	1998
Gaze	[63]	FAR: 42% (attack)	E2	C2	24	uU2D	Shapes with gaze. video breaks system, shoulder surfing not	2009
Pattern	[160]	—	E2	C1	24	uU2D	Smudge protection; image analysis to detect smudge patterns	2014
Magnet.	[14]	EER: 96.6%	E2	C2	10-15	uU2D	sophisticated attackers, video analysis, (slow motion, rewind)	2014
Pattern	[15]	—	E2	C1	—	uU2D	Smudge protection; Case study needs further detail	2010
Pattern	[283]	Error rate: 9.5%	E1	C2	24	uU2D	Smudge protection; Single security expert attacker	2013
Gait	[40]	—	E3	C3	15+482	D2D	Brute-force, mimicry, video, malicious device, protocol flaws	2019
Vibration	[169]	Accu/FPR: >95%/<3%	E3	C3	15	D2D	Implicit vibration an surface. Different attacker classes	2017
Audio, light	[248]	—	E3	C3	—	D2D	Proximity detection; active adversaries; 538 audio samples	2018
Gait	[236]	—	E3	C2	15+482	D2D	Brute-force, mimicry, video, malicious device	2018
EMG	[299]	Bit mismatch rate: <0.4	E3	C2	10	D2D	EMG signals for device pairing	2016
Various	[275]	FPR: <27%	E3	C2	—	D2D	Co-presence: WiFi, GPS, Bluetooth, audio; strong adversary	2014
Audio, light	[190]	—	E2	C2	—	D2D	Context-based pairing; replay, same-context definite success	2014
Shaking	[180]	—	E2	C2	—	D2D	MitM, DoS, incl. definite success (low noise channel)	2007
Shaking	[91]	EER: 0.1293	E1	C2	29	D2D	Observatory, cooperative, handshaking. No video or entropy	2017
Audio	[238]	—	E1	C2	2	D2D	Statistical key properties; attacks incl. guaranteed success	2013

at two distinct places as well as silent cases that would cause the protocol to fail (E1, C2; guaranteed success). An entropy estimation or adversaries with advanced technical support such as directional antennas have been postponed to later work though.

5.3.3 Token-based. The authors in Reference [204] propose a token-based system to verify user authentication at the time of touch interaction with the capacitive screen of the mobile device. A *zero effort* usability study is conducted with 12 participants (E1, C1; zero effort). An example of a *minimal effort* study is References [137, 138] who exploiting magnetic interaction through a touch screen for token-based implicit two-factor authentication. Technical feasibility and theoretical security in comparison to PIN based login are discussed (E1, C2; minimal effort). An advanced and targeted attack study was omitted.

The *advanced effort* study [91] proposes token-based mobile-device unlocking over a pre-estaglished secure channel through conjoint shaking. Protocol-specific attacks, assuming accelerated knowledge of the adversary were considered (E1, C2; advanced effort).

5.3.4 Electromagnetic Signals (RF). In recent years, the radio interface has been increasingly exploiting for sensing purposes. Consequently, the entropy of reciprocal characteristics of a wireless channel between two devices has been exploited to independently compute a key pair for D2D authentication. Exploiting similarity in physical radio channel characteristics, References [179, 278] consider *advanced effort* attacks using only few subjects. They consider strong adversaries that might control the radio channel and induce channel fluctuation to bias correlation for devices in proximity (E2, C2; advanced effort). The adversary has access to historical channel information. Other advanced attack types, such as beam-tracing simulations are disregarded.

5.4 Device-to-user Authentication

As described in Reference [181], an adversary might attempt to exploit that a device or app is mistaken by a user for another, trusted device or app. In this manner, credential information might be derived by the adversary. This is especially critical when some devices in the usage chain of a mobile service are not physically exposed to the user such as, for instance, pointed out for 5G small cell installations in Reference [279]. To protect against such cases, the author of References [225, 226] proposes for a user interface to present a known secret for authentication toward the user. This document merely sketches the idea. An attack study or even a theoretical analysis of the attack surfaces has not been conducted (E1, C1; zero effort)

A device-to-user authentication approach exploiting vibration patterns has been proposed in Reference [89]. The authors propose to define specific vibration patterns specifically for a device to allow device-to-user authentication. The usability has been tested in a study with 12 subjects that targeted on the acceptance of the system. Patterns have been recognized with 97% accuracy; however, an attack scenario or adversaries with access to the device or audio in proximity (to potentially reveal the pattern) have not been considered (C1, E1; zero effort).

5.5 Discussion on Applied Adversary Classes

The proposed classification of adversary classes has proven useful to distinguish between various approaches in the literature, as summarized in Tables 6 to 9. It is striking that more than half of the literature considered falls into low security classes (*zero effort* or *minimal effort*). One reason for this is that authors focus on the usability of their approach solely and disregard security. We suggest that this lax habit need to be broken, to develop better authentication approaches. An insecure authentication might be convenient to use, but its usability is low. Security is also an aspect of usability and must not be taken lightly. We should refrain from stressing mostly convenience of usable security approaches.

This picture calls for a need of re-thinking and strengthening attacker models in mobile authentication schemes, and for further research in this direction. Similarly, benchmark datasets are needed to comprehensively compare mobile authentication approaches [118]. In Table 5, we provide a selection of open datasets in mobile authentication.

6 CONCLUSIONS

Too many publications use weak adversary models, which is comparable to the early work on cryptography, notably symmetric ciphers. In cryptography, nowadays, new cipher proposals are only considered secure candidates[15] after many other, typically more capable, cryptographers have tried to break it.

We recommend to adopt this attitude for research on authentication methods and, in particular, in the domain of mobile/ubiquitous/wearable/embedded devices. Studies often mix usability and security concerns, which is commendable, because security is an important aspect of usability. However, security is often considered as an after-thought and employing non-security experts as participants can only provide an estimate for false negatives, but have little validity for the false positives of an authentication system. To estimate these false positives, a class of significantly stronger attackers is required.

Authors should use realistic attacker models of adversaries who have a real motivation in breaking the system and who are potentially either more skilled than the average user of the system and/or willing to spend significantly more effort than a legitimate user (i.e., false matches are allowed much more effort than true matches). For a comprehensive discussion of a new model—and new authentication papers should go this far in their own evaluation—authors should use additional attacker models that will indeed break that authentication method.

The boundary of what security a system can achieve lies between *advanced effort* and *guaranteed success* categories, i.e., how far it is capable of providing protection against targeted attacks. Good authentication methods should define this security level as precisely as possible.

ACKNOWLEDGMENTS

Our particular thanks go to Vishwath Mohan, who has contributed directly to the discussion of biometric user authentication methods.

We also thank three anonymous reviewers for their insightful, diligent, and highly detailed comments on a previous revision of this article. They have all contributed valuable pointers to additional papers to include in the survey part and helped us shape and focus our main arguments.

REFERENCES

[1] Martín Abadi. 1999. Secrecy by typing in security protocols. *J. ACM* 46, 5 (1999), 749–786.

[2] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay cool!: Understanding thermal attacks on mobile-based user authentication. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 3751–3763.

[3] Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismail, and Amrl Elmougy. 2019. Just gaze and wave: Exploring the use of gaze and gestures for shoulder-surfing resilient authentication. In *Proceedings of the 11th ACM Symposium on Eye Tracking Research & Applications*. 1–10.

[4] Naveed Ahmed and Christian Damsgaard Jensen. 2011. Adaptable authentication model: Exploring security with weaker attacker models. In *Proceedings of the International Conference on Engineering Secure Software and Systems (ESSoS'11)*. Springer, 234–247.

[15] They will never be more than candidates. After all, there is typically no formal proof of security, only the absence of specific attacks that mark a "secure" cipher even to this day.

[5] Heikki J. Ailisto, Mikko Lindholm, Jani Mantyjarvi, Elena Vildjiounaite, and Satu-Marja Makela. 2005. Identifying people from gait pattern with accelerometers. In *Defense and Security.* International Society for Optics and Photonics, 7–14.

[6] Srinath Akula and Veerabhadram Devisetty. 2004. Image based registration and authentication system. In *Proceedings of the Midwest Instruction and Computing Symposium*, Vol. 4. 5.

[7] Mojtaba Alizadeh, Saeid Abolfazli, Mazdak Zamani, Sabariah Baaaharun, and Kouichi Sakurai. 2016. Authentication in mobile cloud computing: A survey. *J. Netw. Comput. Appl.* 61, 1 2 (2016), 59–80. https://doi.org/10.1016/j.jnca.2015.10.005

[8] Sadiq Almuairfi, Prakash Veeraraghavan, and Naveen Chilamkurti. 2013. A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. *Math. Comput. Model.* 58, 1 (2013), 108–116. https://www.sciencedirect.com/science/article/pii/S0895717712001719.

[9] Fatmah H. Alqahtani and Fawaz A. Alsulaiman. 2020. Is image-based CAPTCHA secure against attacks based on machine learning? an experimental study. *Comput. Secur.* 88 (2020), 101635.

[10] Faisal Alshanketi, Issa Traoré, and Ahmed Awad. 2019. Multimodal mobile keystroke dynamics biometrics combining fixed and variable passwords. *Secur. Priv.* 2, 1 (2019), e48. https://onlinelibrary.wiley.com/doi/10.1002/spy2.48.

[11] Florian Alt, Stefan Schneegass, Alireza Sahami Shirazi, Mariam Hassib, and Andreas Bulling. 2015. Graphical passwords in the wild: Understanding how users choose pictures and passwords in image-based authentication schemes. In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services.* ACM, 316–322.

[12] M. Amine Ferrag, L. Maglaras, A. Derhab, A. V. Vasilakos, S. Rallis, and H. Janicke. 2018. authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. arXiv:1803.10281. Retrieved from https://arxiv.org/abs/1803.10281.

[13] S. Abhishek Anand and Nitesh Saxena. 2016. Vibreaker: Securing vibrational pairing with deliberate acoustic noise. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks.* ACM, 103–108.

[14] Md Tanvir Islam Aumi and Sven Kratz. 2014. Airauth: Evaluating in-air hand gestures for authentication. In *Proceedings of the 16th International Conference on Human-computer Interaction With Mobile Devices & Services.* ACM, 309–318.

[15] Adam J. Aviv, Katherine L. Gibson, Evan Mossop, Matt Blaze, and Jonathan M. Smith. 2010. Smudge attacks on smartphone touch screens. In *Proceedings of the IEEE Workshop on Offensive Technologies (WOOT'10)*, 1–7.

[16] Adam J. Aviv, Benjamin Sapp, Matt Blaze, and Jonathan M. Smith. 2012. Practicality of accelerometer side channels on smartphones. In *Proceedings of the 28th Annual Computer Security Applications Conference.* ACM, 41–50.

[17] Shiri Azenkot, Kyle Rector, Richard Ladner, and Jacob Wobbrock. 2012. Passchords: Secure multi-touch authentication for blind people. In *Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility.* ACM, 159–166.

[18] Abdullah Azfar, Kim-Kwang Raymond Choo, and Lin Liu. 2016. An android social app forensics adversary model. In *2016 Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS'16).* IEEE, 5597–5606.

[19] Lucas Ballard, Seny Kamara, Fabian Monrose, and Michael K. Reiter. 2008. Towards practical biometric key generation with randomized biometric templates. In *Proceedings of the 15th ACM Conference on Computer and Communications Security.* ACM, 235–244.

[20] Lucas Ballard, Daniel Lopresti, and Fabian Monrose. 2007. Forgery quality and its implications for behavioral biometric security. *IEEE Trans. Syst. Man Cybernet. B (Cybernet.)* 37, 5 (2007), 1107–1118.

[21] Lucas Ballard, Fabian Monrose, and Daniel P. Lopresti. 2006. Biometric authentication revisited: Understanding the impact of wolves in sheep's clothing. In *Proceedings of the USENIX Security Symposium.*

[22] Stacy J. Morris Bamberg, Ari Y. Benbasat, Donna Moxley Scarborough, David E. Krebs, and Joseph A. Paradiso. 2008. Gait analysis using a shoe-integrated wireless sensor system. *IEEE Trans. Inf. Technol. Biomed.* 12, 4 (2008), 413–423.

[23] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf. 2011. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *Proceedings of the IEEE Symposium on Security and Privacy.* 96–111.

[24] Mihir Bellare, Anand Desai, David Pointcheval, and Phillip Rogaway. 1998. Relations among notions of security for public-key encryption schemes. In *Advances in Cryptology.* Springer, 26–45.

[25] Mihir Bellare and Phillip Rogaway. 1995. Provably secure session key distribution: The three party case. In *Proceedings of the 27th Annual ACM Symposium on Theory of Computing.* 57–66.

[26] Steven M Bellovin and Michael Merritt. 1993. Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise. In *Proceedings of the 1st ACM Conference on Computer and Communications Security.* ACM, 244–250.

[27] Bhaveer Bhana and Stephen Flowerday. 2020. Passphrase and keystroke dynamics authentication: Usable security. *Comput. Secur.* (2020), 101925.

[28] Andrea Bianchi, Ian Oakley, Vassilis Kostakos, and Dong Soo Kwon. 2011. The phone lock: Audio and haptic shoulder-surfing resistant PIN entry methods for mobile devices. In *Proceedings of the 5th International Conference on Tangible, Embedded, and Embodied Interaction*. ACM, 197–200.

[29] Daniel Bichler, Guido Stromberg, Mario Huemer, and Manuel Löw. 2007. Key generation based on acceleration data of shaking processes. In *Proceedings of the International Conference on Ubiquitous Computing*. Springer, 304–317.

[30] J.-C. Birget, Dawei Hong, and Nasir Memon. 2006. Graphical passwords based on robust discretization. *IEEE Trans. Inf. Forens. Secur.* 1, 3 (2006), 395–399.

[31] Christopher M. Bishop. 2006. *Pattern Recognition and Machine Learning*.

[32] Greg E. Blonder. 1996. Graphical password. (Sept. 24 1996). US Patent 5,559,961.

[33] Cheng Bo, Lan Zhang, Xiang-Yang Li, Qiuyuan Huang, and Yu Wang. 2013. Silentsense: Silent user identification via touch and movement behavioral biometrics. In *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*. ACM, 187–190.

[34] Chiara Bodei, Mikael Buchholtz, Pierpaolo Degano, Flemming Nielson, and H. Riis Nielson. 2003. Automatic validation of protocol narration. In *Proceedings of the IEEE Computer Security Foundations Workshop*. IEEE, 126–140.

[35] Reinhardt A. Botha, Steven M. Furnell, and Nathan L. Clarke. 2009. From desktop to mobile: Examining the security experience. *Comput. Secur.* 28, 3–4 (2009), 130–137.

[36] Nikolaos V. Boulgouris, Dimitrios Hatzinakos, and Konstantinos N. Plataniotis. 2005. gait recognition: A challenging signal processing technology for biometric identification. *IEEE Sign. Process. Mag.* 22, 6 (2005), 78–90.

[37] Z. Boulkenafet, J. Komulainen, Lei. Li, X. Feng, and A. Hadid. 2017. OULU-NPU: A mobile face presentation attack database with real-world variations. In *Proceedings of the IEEE International Conference on Automatic Face and Gesture Recognition*.

[38] Colin Boyd and Anish Mathuria. 2013. *Protocols for Authentication and Key Establishment*. Springer Science & Business Media.

[39] Sacha Brostoff, Philip Inglesant, and M. Angela Sasse. 2010. Evaluating the usability and security of a graphical one-time PIN system. In *Proceedings of the 24th BCS Interaction Specialist Group Conference*. British Computer Society, 88–97.

[40] Arne Bruesch, Le Nguyen, Dominik Schürmann, Stephan Sigg, and Lars C. Wolf. 2019. Security properties of gait for mobile device pairing. *IEEE Trans. Mobile Comput.* (2019).

[41] Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2012. Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 3011–3020.

[42] Andreas Bulling, Ulf Blanke, and Bernt Schiele. 2014. A tutorial on human activity recognition using body-worn inertial sensors. *ACM Comput. Surv.* 46, 3 (2014), 33.

[43] Attaullah Buriro, Bruno Crispo, and Mauro Conti. 2019. Answerauth: A bimodal behavioral biometric-based user authentication scheme for smartphones. *J. Inf. Secur. Appl.* 44 (2019), 89–103.

[44] Mike Burmester and Jorge Munilla. 2009. A flyweight RFID authentication protocol. *IACR Cryptology Eprint Archive* 2009 (2009), 212.

[45] Daniel Buschek, Fabian Hartmann, Emanuel Von Zezschwitz, Alexander De Luca, and Florian Alt. 2016. Snapapp: Reducing authentication overhead with a time-constrained fast unlock option. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. ACM, 3736–3747.

[46] Pierluigi Casale, Oriol Pujol, and Petia Radeva. 2012. Personalization and user verification in wearable systems using biometric walking patterns. *Pers. Ubiq. Comput.* 16, 5 (2012), 563–580.

[47] Seunghun Cha, Sungsu Kwag, Hyoungshick Kim, and Jun Ho Huh. 2017. Boosting the guessing attack performance on android lock patterns with smudge attacks. In *Proceedings of the ACM on Asia Conference on Computer and Communications Security*. ACM, 313–326.

[48] Si Chen, Kui Ren, Sixu Piao, Cong Wang, Qian Wang, Jian Weng, Lu Su, and Aziz Mohaisen. 2017. You can hear but you cannot steal: Defending against voice impersonation attacks on smartphones. In *Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS'17)*. IEEE, 183–195.

[49] Sonia Chiasson, Paul C. Van Oorschot, and Robert Biddle. 2007. Graphical password authentication using cued click points. In *Proceedings of the European Symposium on Research in Computer Security*. Springer, 359–374.

[50] Ming Ki Chong, René Mayrhofer, and Hans Gellersen. 2014. A survey of user interaction for spontaneous device association. *Comput. Surv.* (2014).

[51] Nathan L. Clarke and Steven M. Furnell. 2005. Authentication of users on mobile telephones–a survey of attitudes and practices. *Comput. Secur.* 24, 7 (2005), 519–527.

[52] Nathan L. Clarke and Steven M. Furnell. 2007. Authenticating mobile phone users using keystroke analysis. *Int. J. Inf. Secur.* 6, 1 (2007), 1–14.

[53] Mauro Conti, Giulio Lovisotto, Ivan Martinovic, and Gene Tsudik. 2017. Fadewich: Fast deauthentication over the wireless channel. In *Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS'17)*. IEEE, 2294–2301.
[54] Cory Cornelius and David Kotz. 2011. Recognizing whether sensors are on the same body. In *Proceedings of the International Conference on Pervasive Computing (Pervasive'11)*. Springer-Verlag, Berlin, 332–349.
[55] Mark D. Corner and Brian D. Noble. 2002. Zero-interaction authentication. In *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking*. ACM, 1–11.
[56] Artur Costa-Pazo, Sushil Bhattacharjee, Esteban Vazquez-Fernandez, and Sébastien Marcel. 2016. The REPLAY-MOBILE face presentation-attack database. In *Proceedings of the International Conference on Biometrics Special Interests Group (BioSIG'16)*.
[57] David Crouse, Hu Han, Deepak Chandra, Brandon Barbello, and Anil K. Jain. 2015. Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data. In *Proceedings of the International Conference on Biometrics (ICB'15)*. IEEE, 135–142.
[58] Ivan Damgård and Michael Pedersen. 2008. RFID security: Tradeoffs between security and efficiency. In *Cryptographers' Track at the RSA Conference: Topics in Cryptology (CT-RSA'08)* , 318–332.
[59] Dimitrios Damopoulos and Georgios Kambourakis. 2019. Hands-free one-time and continuous authentication using glass wearable devices. *J. Inf. Secur. Appl.* 46 (2019), 138–150.
[60] Carlton R. Davis. 2001. *IPSec: Securing VPNs*. McGraw–Hill Professional.
[61] Darren Davis, Fabian Monrose, and Michael K. Reiter. 2004. On user choice in graphical password schemes. In *Proceedings of the USENIX Security Symposium*, Vol. 13. 11–11.
[62] Antonella De Angeli, Mike Coutts, Lynne Coventry, Graham I. Johnson, David Cameron, and Martin H. Fischer. 2002. VIP: A visual approach to user authentication. In *Proceedings of the Working Conference on Advanced Visual Interfaces*. ACM, 316–323.
[63] Alexander De Luca, Martin Denzel, and Heinrich Hussmann. 2009. Look into my eyes!: Can you guess my password? In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS'09)*.
[64] Alexander De Luca, Alina Hang, Frederik Brudy, Christian Lindner, and Heinrich Hussmann. 2012. Touch me once and I know it's you!: Implicit authentication based on touch screen patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 987–996.
[65] Alexander De Luca, Marian Harbach, Emanuel von Zezschwitz, Max-Emanuel Maurer, Bernhard Ewald Slawik, Heinrich Hussmann, and Matthew Smith. 2014. Now you see me, now you don't: Protecting smartphone authentication from shoulder surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'14)*. Association for Computing Machinery, New York, NY, USA, 2937–2946. https://doi.org/10.1145/2556288.2557097
[66] Alexander De Luca and Janne Lindqvist. 2015. Is secure and usable smartphone authentication asking too much? *Computer* 48, 5 (2015), 64–68.
[67] Alexander De Luca, Emanuel Von Zezschwitz, Ngo Dieu Huong Nguyen, Max-Emanuel Maurer, Elisa Rubegni, Marcello Paolo Scipioni, and Marc Langheinrich. 2013. Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2389–2398.
[68] Alexander De Luca, Roman Weiss, and Heiko Drewes. 2007. Evaluation of eye-gaze interaction methods for security enhanced PIN-entry. In *Proceedings of the 19th Australasian Conference on Computer-human Interaction: Entertaining User Interfaces*. ACM, 199–202.
[69] Alexander De Luca, Roman Weiss, and Heinrich Hussmann. 2007. Passshape: Stroke based shape passwords. In *Proceedings of the 19th Australasian Conference on Computer-human Interaction: Entertaining User Interfaces*. ACM, 239–240.
[70] Timothy Dee, Ian Richardson, and Akhilesh Tyagi. 2019. Continuous transparent mobile device touchscreen soft keyboard biometric authentication. In *Proceedings of the 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID'19)*. IEEE, 539–540.
[71] Mohammad Omar Derawi. 2012. Smartphones and biometrics: Gait and activity recognition. (2012).
[72] Mohammad Omar Derawi, Claudia Nickel, Patrick Bours, and Christoph Busch. 2010. Unobtrusive user-authentication on mobile phones using biometric gait recognition. In *Proceedings of the 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'10)*. IEEE, 306–311.
[73] Rachna Dhamija and Adrian Perrig. 2000. Deja vu-a user study: Using images for authentication. In *Proceedings of the USENIX Security Symposium*, Vol. 9. 4–4.
[74] Rainhard Dieter Findling and Rene Mayrhofer. 2013. Towards pan shot face unlock: Using biometric face information from different perspectives to unlock mobile devices. *Int. J. Perv. Comput. Commun.* 9, 3 (2013), 190–208.
[75] Ahmet Emir Dirik, Nasir Memon, and Jean-Camille Birget. 2007. Modeling user choice in the passpoints graphical password scheme. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*. ACM, 20–28.

[76] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. 2015. Exfiltrating data from android devices. *Comput. Secur.* 48 (2015), 74–91.
[77] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. 2015. A forensically sound adversary model for mobile devices. *PLoS One* 10, 9 (2015), e0138449.
[78] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. 2019. The role of the adversary model in applied security research. *Comput. Secur.* 81 (2019), 156–181.
[79] Danny Dolev and Andrew Yao. 1983. On the security of public key protocols. *IEEE Trans. Inf. Theory* 29, 2 (1983), 198–208.
[80] Hossein Falaki, Ratul Mahajan, Srikanth Kandula, Dimitrios Lymberopoulos, Ramesh Govindan, and Deborah Estrin. 2010. Diversity in smartphone usage. In *Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services (MobiSys'10)*. ACM, New York, NY, 179–194. https://doi.org/10.1145/1814433.1814453
[81] Michael Farb, Yue-Hsun Lin, Tiffany Hyun-Jin Kim, Jonathan McCune, and Adrian Perrig. 2013. Safeslinger: Easy-to-use and secure public-key exchange. In *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*. ACM, 417–428.
[82] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M. S. Gaur, M. Conti, and M. Rajarajan. 2015. Android security: A survey of issues, malware penetration, and defenses. *IEEE Commun. Surv. Tutor.* 17, 2 (Secondquarter 2015), 998–1022. https://doi.org/10.1109/COMST.2014.2386139
[83] Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Shi, Bogdan Carbunar, Yifei Jiang, and Nhung Nguyen. 2012. Continuous mobile authentication using touchscreen gestures. In *Proceedings of the IEEE Conference on Technologies for Homeland Security (HST'12)*. IEEE, 451–456.
[84] Mohamed Amine Ferrag, Leandros Maglaras, Abdelouahid Derhab, and Helge Janicke. 2020. Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. *Telecommun. Syst.* 73, 2 (2020), 317–348.
[85] Tobias Fiebig, Jan Krissler, and Ronny Hänsch. 2014. Security impact of high resolution smartphone cameras. In *Proceedings of the IEEE Workshop on Offensive Technologies (WOOT'14)*.
[86] Julian Fierrez, Javier Galbally, Javier Ortega-Garcia, Manuel R. Freire, Fernando Alonso-Fernandez, Daniel Ramos, Doroteo Torre Toledano, Joaquin Gonzalez-Rodriguez, Juan A. Siguenza, and Javier Garrido-Salas. 2010. BiosecurID: A multimodal biometric database. *Pattern Anal. Appl.* 13, 2 (2010), 235–246.
[87] Rainhard Dieter Findling, Michael Hölzl, and René Mayrhofer. 2018. Mobile match-on-card authentication using offline-simplified models with gait and face biometrics. *IEEE Trans. Mobile Comput.* 17, 11 (2018), 2578–2590.
[88] Rainhard D. Findling and Rene Mayrhofer. 2013. Towards secure personal device unlock using stereo camera pan shots. In *Proceedings of the International Conference on Computer Aided Systems Theory*. Springer, 417–425.
[89] Rainhard Dieter Findling and René Mayrhofer. 2015. Towards device-to-user authentication: Protecting against phishing hardware by ensuring mobile device authenticity using vibration patterns. In *Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia (MUM'15)*. ACM, 131–136. https://doi.org/10.1145/2836041.2836053
[90] Rainhard Dieter Findling, Muhammad Muaaz, Daniel Hintze, and René Mayrhofer. 2014. shakeunlock: Securely unlock mobile devices by shaking them together. In *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia*. ACM, 165–174.
[91] Rainhard Dieter Findling, Muhammad Muaaz, Daniel Hintze, and Rene Mayrhofer. 2017. shakeunlock: Securely transfer authentication states between mobile devices. *IEEE Trans. Mobile Comput.* 16, 4 (2017), 1163–1175.
[92] Rainhard Dieter Findling, Tahmid Quddus, and Stephan Sigg. 2019. Hide my gaze with EOG! towards closed-eye gaze gesture passwords that resist observation-attacks with electrooculography in smart glasses. In *Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia (MoMM'19)*. Association for Computing Machinery, New York, NY, 107116. https://doi.org/10.1145/3365921.3365922
[93] Riccardo Focardi, Flaminia L. Luccio, and Heider A. M. Wahsheh. 2019. Usable security for QR code. *J. Inf. Secur. Appl.* 48 (2019), 102369.
[94] Mikhail Fomichev, Flor Alvarez, Daniel Steinmetzer, Paul Gardner-Stephen, and Matthias Hollick. 2017. Survey and systematization of secure device pairing. *IEEE Commun. Surv. Tutor.* (Sep. 2017). https://doi.org/10.1109/COMST.2017.2748278
[95] Alain Forget, Sonia Chiasson, and Robert Biddle. 2010. Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1107–1110.
[96] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2013. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. *IEEE Trans. Inf. Forens. Secur.* 8, 1 (2013), 136–148.
[97] Eira Friström, Elias Lius, Niki Ulmanen, Paavo Hietala, Pauliina Kärkkäinen, Tommi Mäkinen, Stephan Sigg, and Rainhard Dieter Findling. 2019. Free-form gaze passwords from cameras embedded in smart glasses. In *Proceedings of the 17th International Conference on Advances in Mobile Computing & Multimedia*. 136–144.

[98] Markus Funk, Karola Marky, Iori Mizutani, Mareike Kritzler, Simon Mayer, and Florian Michahelles. 2019. Lookunlock: Using spatial-targets for user-authentication on hmds. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–6.
[99] Steven Furnell, Nathan Clarke, and Sevasti Karatzouni. 2008. Beyond the PIN: Enhancing user authentication for mobile devices. *Comput. Fraud Secur.* 2008, 8 (2008), 12–17.
[100] Davrondzhon Gafurov. 2007. A survey of biometric gait recognition: Approaches, security and challenges. In *Proceedings of the Annual Norwegian Computer Science Conference*. 19–21.
[101] Davrondzhon Gafurov. 2008. *Performance and Security Analysis of Gait-based User Authentication*. Ph.D. Dissertation. University of Oslo.
[102] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. 2007. Spoof attacks on gait authentication system. *IEEE Trans. Inf. Forens. Secur.* 2, 3 (2007), 491–502.
[103] Davrondzhon Gafurov, Einar Snekkenes, and Tor Erik Buvarp. 2006. Robustness of biometric gait authentication against impersonation attack. In *Proceedings of the OTM Confederated International Conferences "on the Move to Meaningful Internet Systems."* Springer, 479–488.
[104] Javier Galbally, Iwen Coisel, and Ignacio Sanchez. 2014. A probabilistic framework for improved password strength metrics. In *Proceedings of the International Carnahan Conference on Security Technology (ICCST'14)*. IEEE, 1–6.
[105] Pimmy Gandotra, Rakesh Kumar Jha, and Sanjeev Jain. 2016. A survey on device-to-device (D2D) communication: Architecture and security issues. *J. Netw. Comput. Appl.* 78 (11 2016). https://doi.org/10.1016/j.jnca.2016.11.002
[106] Virgil D. Gligor. 2007. *Handling New Adversaries in Secure Mobile Ad-hoc Networks*. Technical Report. Department of Electrical and Computer Engineering, University of Maryland, College Park.
[107] Neil Zhenqiang Gong, Altay Ozen, Yu Wu, Xiaoyu Cao, Richard Shin, Dawn Song, Hongxia Jin, and Xuan Bao. 2017. PIANO: Proximity-based user authentication on voice-powered internet-of-things devices. In *Proceedings of the IEEE 37th International Conference on Distributed Computing Systems (ICDCS'17)*. IEEE, 2212–2219.
[108] Sathya Govindarajan, Paolo Gasti, and Kiran S. Balagani. 2013. Secure privacy-preserving protocols for outsourcing continuous authentication of smartphone users with touch data. In *Proceedings of the IEEE 6th International Conference on Biometrics: Theory, Applications and Systems (BTAS'13)*. IEEE, 1–8.
[109] Bogdan Groza and Rene Mayrhofer. 2012. SAPHE: Simple accelerometer based wireless pairing with heuristic trees. In *Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia*. ACM, 161–168.
[110] Agnes Grünerbl, Amir Muaremi, Venet Osmani, Gernot Bahle, Stefan Oehler, Gerhard Tröster, Oscar Mayora, Christian Haring, and Paul Lukowicz. 2015. Smartphone-based recognition of states and state changes in bipolar disorder patients. *IEEE J. Biomed. Health Inf.* 19, 1 (2015), 140–148.
[111] Meriem Guerar, Luca Verderame, Mauro Migliardi, and Alessio Merlo. 2019. 2GesturePIN: Securing PIN-Based authentication on smartwatches. In *Proceedings of the IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'19)*. IEEE, 327–333.
[112] Richa Gupta and Priti Sehgal. 2016. A survey of attacks on iris biometric systems. *Int. J. Biometr.* 8, 2 (2016), 145–178.
[113] Creighton Tsuan-Ren Hager. 2004. *Context Aware and Adaptive Security for Wireless Networks*. Ph.D. Dissertation.
[114] Inken Hagestedt, Michael Backes, and Andreas Bulling. 2020. Adversarial attacks on classifiers for eye-based user modelling. In *Proceedings of the ACM Symposium on Eye Tracking Research and Applications*. 1–3.
[115] Marian Harbach, Emanuel Von Zezschwitz, Andreas Fichtner, Alexander De Luca, and Matthew Smith. 2014. It'sa hard lock life: A field study of smartphone (un) locking behavior and risk perception. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS'14)*. 213–230.
[116] Mark A. Harris and Karen P. Patten. 2014. Mobile device security considerations for small- and medium-sized enterprise business mobility. *Inf. Manage. Comput. Secur.* 22, 1 (2014), 97–114. https://doi.org/10.1108/IMCS-03-2013-0019
[117] Eiji Hayashi, Rachna Dhamija, Nicolas Christin, and Adrian Perrig. 2008. Use your illusion: Secure authentication usable anywhere. In *Proceedings of the 4th Symposium on Usable Privacy and Security*. ACM, 35–45.
[118] Ernst A. Heinz, Kai S. Kunze, Stefan Sulistyo, Holger Junker, Paul Lukowicz, and Gerhard Tröster. 2003. experimental evaluation of variations in primary features used for accelerometric context recognition. In *Proceedings of the European Symposium on Ambient Intelligence*. Springer, 252–263.
[119] Javier Hernandez, Daniel J. McDuff, and Rosalind W. Picard. 2015. Biophone: Physiology monitoring from peripheral smartphone motions. In *Proceedings of the 37th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC'15)*. IEEE, 7180–7183.
[120] Daniel Hintze, Rainhard Dieter Findling, Muhammad Muaaz, Eckhard Koch, and René Mayrhofer. 2015. CORMORANT: Towards continuous risk-aware multi-modal cross-device authentication. In *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication (UbiComp'15)*. ACM, 169–172. https://doi.org/10.1145/2800835.2800906

[121] Daniel Hintze, Philipp Hintze, Rainhard Dieter Findling, and René Mayrhofer. 2017. A large-scale, long-term analysis of mobile device usage characteristics. *Proc. ACM Interact. Mob. Wear. Ubiq. Technol.* 1, 2, Article 13 (Jun. 2017), 21 pages. https://doi.org/10.1145/3090078

[122] Thang Hoang, Deokjai Choi, and Thuc Nguyen. 2015. gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. *Int. J. Inf. Secur.* 14, 6 (2015), 549–560.

[123] Thang Hoang, Deokjai Choi, Viet Vo, Anh Nguyen, and Thuc Nguyen. 2013. A lightweight gait authentication on mobile phone regardless of installation error. In *Proceedings of the IFIP International Information Security Conference.* Springer, 83–101.

[124] Michael Hoelzl, Michael Roland, and René Mayrhofer. 2017. Real-world identification for an extensible and privacy-preserving mobile eID. In *The Proceedings of the 12th IFIP Smart World Revolution Conference on Privacy and Identity Management.* Springer International Publishing, Ispra, Italy.

[125] Ann-Marie Horcher. 2018. *Conservation of Limited Resources: Design Principles for Security and Usability on Mobile Devices.* Ph.D. Dissertation. Nova Southesastern University.

[126] Mehdi Hosseinzadeh, Jan Lansky, Amir Masoud Rahman, Cuong Trinh, Masoumeh Safkhani, Nasour Bagheri, and Bao Huynh. 2020. A new strong adversary model for RFID authentication protocols. *IEEE Access* (2020).

[127] Bufu Huang, Meng Chen, Panfeng Huang, and Yangsheng Xu. 2007. Gait modeling for human identification. In *Proceedings of the IEEE International Conference on Robotics and Automation.* IEEE, 4833–4838.

[128] Otto Huhta, Prakash Shrestha, Swapnil Udar, Mika Juuti, Nitesh Saxena, and N. Asokan. 2015. Pitfalls in designing zero-effort deauthentication: Opportunistic human observation attacks. arXiv:1505.05779. Retrieved from https://arxiv.org/abs/1505.05779.

[129] Seong-seob Hwang, Sungzoon Cho, and Sunghoon Park. 2009. Keystroke dynamics-based authentication for mobile devices. *Comput. Secur.* 28, 1 (2009), 85–93.

[130] Tzonelih Hwang and Wei-Chi Ku. 1995. Reparable key distribution protocols for internet environments. *IEEE Trans. Commun.* 43, 5 (1995), 1947–1949.

[131] ISA99 Committee and IEC Technical Committee 65 Working Group 10 (TC65WG10). 2016. The 62443 Series of standards: Industrial Automation and Control Systems Security.

[132] Anil Jain, Patrick Flynn, and Arun A. Ross. 2007. *Handbook of Biometrics.* Springer Science & Business Media.

[133] I. H. Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. 1999. *The Design and Analysis of Graphical Passwords.* USENIX Association.

[134] Shan Jia, Guodong Guo, and Zhengquan Xu. 2020. A survey on 3D mask presentation attack detection and countermeasures. *Pattern Recogn.* 98 (2020), 107032.

[135] Shan Jia, Guodong Guo, Zhengquan Xu, and Qiangchang Wang. 2020. Face presentation attack detection in mobile scenarios: A comprehensive evaluation. *Image Vision Comput.* 93 (2020), 103826.

[136] Lijun Jiang and Weizhi Meng. 2017. Smartphone user authentication using touch dynamics in the big data era: Challenges and opportunities. In *Biometric Security and Privacy.* Springer, 163–178.

[137] Rong Jin, Liu Shi, Kai Zeng, Amit Pande, and Prasant Mohapatra. 2014. Magpairing: Exploiting magnetometers for pairing smartphones in close proximity. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS'14).* IEEE, 445–453.

[138] Rong Jin, Liu Shi, Kai Zeng, Amit Pande, and Prasant Mohapatra. 2016. Magpairing: Pairing smartphones in close proximity using magnetometers. *IEEE Trans. Inf. Forens. Secur.* 11, 6 (2016), 1306–1320.

[139] Young-Hoo Jo, Seong-Yun Jeon, Jong-Hyuk Im, and Mun-Kyu Lee. 2016. Security analysis and improvement of fingerprint authentication for smartphones. *Mobile Inf. Syst.* 2016 (2016).

[140] Ari Juels and Martin Wattenberg. 1999. A fuzzy commitment scheme. In *Proceedings of the 6th ACM Conference on Computer and Communications Security.* ACM, 28–36.

[141] Amir Kale, Naresh Cuntoor, B. Yegnanarayana, A. N. Rajagopalan, and Rama Chellappa. 2003. Gait analysis for human identification. In *Proceedings of the International Conference on Audio-and Video-based Biometric Person Authentication.* Springer, 706–714.

[142] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. 2015. Sound-proof: Usable two-factor authentication based on ambient sound. In *Proceedings of the USENIX Security Symposium.* 483–498.

[143] Charlie Kaufman, Paul Hoffman, Yoav Nir, Parsi Eronen, and Tero Kivinen. 2014. *Internet Key Exchange Protocol Version 2 (IKEv2).* Technical Report.

[144] Jaspreet Kaur, Amitoj Singh, and Virender Kadyan. 2020. Automatic speech recognition system for tonal languages: State-of-the-art survey. *Arch. Comput. Methods Eng.* (2020), 1–30.

[145] Hassan Khan, Aaron Atwater, and Urs Hengartner. 2014. A comparative evaluation of implicit authentication schemes. In *Proceedings of the International Workshop on Recent Advances in Intrusion Detection.* Springer, 255–275.

[146] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2018. Augmented reality-based mimicry attacks on behaviour-based smartphone authentication. In *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services.* 41–53.

[147] W. Z. Khan, Y. Xiang, M. Y. Aalsalem, and Q. Arshad. 2013. Mobile phone sensing systems: A survey. *IEEE Commun. Surv. Tutor.* 15, 1 (First 2013), 402–427. https://doi.org/10.1109/SURV.2012.031412.00077

[148] Dongik Kim, Yujin Jung, Kar-Ann Toh, Byungjun Son, and Jaihie Kim. 2016. An empirical study on iris recognition in a mobile phone. *Expert Syst. Appl.* 54 (2016), 328–339.

[149] Dong-Ju Kim, Kwang-Woo Chung, and Kwang-Seok Hong. 2010. Person authentication using face, teeth and voice modalities for mobile device security. *IEEE Trans. Consum. Electr.* 56, 4 (2010).

[150] Daniel V. Klein. 1990. Foiling the cracker: A survey of, and improvements to, password security. In *Proceedings of the 2nd USENIX Security Workshop*. 5–14.

[151] Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, and Sebastian Möller. 2017. On the use of emojis in mobile authentication. In *ICT Systems Security and Privacy Protection*, Sabrina De Capitani di Vimercati and Fabio Martinelli (Eds.).

[152] Katharina Krombholz, Thomas Hupperich, and Thorsten Holz. 2017. May the force be with you: The future of force-sensitive authentication. *IEEE Internet Comput.* 21, 3 (2017), 64–69.

[153] Bogdan Ksiezopolski and Zbigniew Kotulski. 2007. adaptable security mechanism for dynamic environments. *Comput. Secur.* 26, 3 (2007), 246–255. https://doi.org/10.1016/j.cose.2006.11.002

[154] Wei-Chi Ku, Chien-Ming Chen, and Hui-Lung Lee. 2003. Cryptanalysis of a variant of peyravian-zunic's password authentication scheme. *IEICE Trans. Commun.* 86, 5 (2003), 1682–1684.

[155] Wei-Chi Ku and Maw-Jinn Tsaur. 2005. A remote user authentication scheme using strong graphical passwords. In *Proceedings of the IEEE Conference on Local Computer Networks*. IEEE, 351–357.

[156] Yeeun Ku, Leo Hyun Park, Sooyeon Shin, and Taekyoung Kwon. 2019. Draw it as shown: Behavioral pattern lock for mobile user authentication. *IEEE Access* 7 (2019), 69363–69378.

[157] Manu Kumar, Tal Garfinkel, Dan Boneh, and Terry Winograd. 2007. Reducing shoulder-surfing by using gaze-based password entry. In *Proceedings of the 3rd Symposium on Usable Privacy and Security*. ACM, 13–19.

[158] R. Kumar, V. V. Phoha, and A. Jain. 2015. Treadmill attack on gait-based authentication systems. In *2015 Proceedings of the IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS'15).*

[159] Douglas Kunda and Mumbi Chishimba. 2018. A survey of android mobile phone authentication schemes. *Mobile Netw. Appl.* (09 Aug. 2018). https://doi.org/10.1007/s11036-018-1099-7

[160] Taekyoung Kwon and Sarang Na. 2014. Tinylock: Affordable defense against smudge attacks on smartphone pattern lock systems. *Comput. Secur.* 42 (2014), 137–150.

[161] Andrew Kwong, Connor Bolton, Timothy Trippel, Wenyuan Xu, and Kevin Fu. 2017. Why Do You Trust Sensors? Analog Cybersecurity Attack Demos. https://ieeexplore.ieee.org/document/8615693.

[162] Kyuin Lee, Vijay Raghunathan, Anand Raghunathan, and Younghyun Kim. 2018. SYNCVIBE: Fast and secure device pairing through physical vibration on commodity smartphones. In *Proceedings of the IEEE 36th International Conference on Computer Design (ICCD'18).* IEEE, 234–241.

[163] Jonathan Lester, Blake Hannaford, and Gaetano Borriello. 2004. Are you with me?—Using accelerometers to determine if two devices are carried by the same person. In *Proceedings of the International Conference on Pervasive Computing*. Springer, 33–50.

[164] Lingjun Li, Xinxin Zhao, and Guoliang Xue. 2013. Unobservable re-authentication for smartphones. In *Proceedings of the Network and Distributed System Security Symposium (NDSS'13).*

[165] Mengyuan Li, Yan Meng, Junyi Liu, Haojin Zhu, Xiaohui Liang, Yao Liu, and Na Ruan. 2016. When CSI meets public wifi: Inferring your mobile phone password via wifi signals. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS'16).* ACM, New York, NY, 1068–1079. https://doi.org/10.1145/2976749.2978397

[166] Sugang Li, Ashwin Ashok, Yanyong Zhang, Chenren Xu, Janne Lindqvist, and Macro Gruteser. 2016. Whose move is it anyway? authenticating smart wearable devices using unique head movement patterns. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom'16).* IEEE, 1–9.

[167] Yan Li, Yingjiu Li, Ke Xu, Qiang Yan, and Robert H. Deng. 2018. Empirical study of face authentication systems under OSNFD attacks. *IEEE Trans. Depend. Secure Comput.* 15, 2 (2018), 231–245.

[168] Robert LiKamWa, Yunxin Liu, Nicholas D. Lane, and Lin Zhong. 2013. Moodscope: Building a mood sensor from smartphone usage patterns. In *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services.* ACM, 389–402.

[169] Jian Liu, Chen Wang, Yingying Chen, and Nitesh Saxena. 2017. Vibwrite: Towards finger-input authentication on ubiquitous surfaces via physical vibration. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. ACM, 73–87.

[170] Jian Liu, Yan Wang, Gorkem Kar, Yingying Chen, Jie Yang, and Marco Gruteser. 2015. Snooping keystrokes with mm-level audio ranging on a single phone. In *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking*. ACM, 142–154.

[171] Jiayang Liu, Lin Zhong, Jehan Wickramasuriya, and Venu Vasudevan. 2009. Uwave: Accelerometer-based personalized gesture recognition and its applications. *Perv. Mobile Comput.* 5, 6 (2009), 657–675.

[172] Yu Liu and Jianwei Niu. 2014. Overlapped-shaking: A local authentication method for mobile applications. In *Proceedings of the Computing, Communications and IT Applications Conference (ComComAp'14)*. IEEE, 93–97.

[173] Hong Lu, A. J. Bernheim Brush, Bodhi Priyantha, Amy K. Karlson, and Jie Liu. 2011. Speakersense: Energy efficient unobtrusive speaker identification on mobile phones. In *Proceedings of the International Conference on Pervasive Computing*. Springer, 188–205.

[174] Nemanja Maček, Saša Adamović, Milan Milosavljević, Miloš Jovanović, Milan Gnjatović, and Branimir Trenkić. 2019. Mobile banking authentication based on cryptographically secured iris biometrics. *Acta Polytechn. Hung.* 16, 1 (2019).

[175] Bartłomiejczyk Maciej and Mirosław Kurkowski. 2019. Multifactor authentication protocol in a mobile environment. *IEEE Access* 7 (2019), 157185–157199.

[176] Sébastien Marcel, Mark S. Nixon, Julian Fierrez, and Nicholas Evans. 2019. *Handbook of Biometric Anti-spoofing: Presentation Attack Detection.* Springer.

[177] Shrirang Mare, Andrés Molina Markham, Cory Cornelius, Ronald Peterson, and David Kotz. 2014. Zebra: Zero-effort bilateral recurring authentication. In *Proceedings of the IEEE Symposium on Security and Privacy (SP'14)*. IEEE, 705–720.

[178] Ivan Martinovic, Kasper Rasmussen, Marc Roeschlin, and Gene Tsudik. 2017. Authentication using pulse-response biometrics. *Commun. ACM* 60, 2 (2017), 108–115.

[179] Suhas Mathur, Robert Miller, Alexander Varshavsky, Wade Trappe, and Narayan Mandayam. 2011. Proximate: Proximity-based secure pairing using ambient wireless signals. In *Proceedings of the 9th International Conference on Mobile Systems, Applications, and Services.* ACM, 211–224.

[180] Rene Mayrhofer. 2007. The candidate key protocol for generating secret shared keys from similar sensor data streams. In *Proceedings of the European Workshop on Security in Ad-hoc and Sensor Networks.* Springer, 1–15.

[181] René Mayrhofer. 2014. An architecture for secure mobile devices. *Secur. Commun. Netw.* 8 (07/2014 2014), 1958–1970. https://doi.org/10.1002/sec.1028

[182] René Mayrhofer. 2019. Insider attack resistance in the android ecosystem. In *Proceedings of Enigma 2019.* USENIX Association.

[183] René Mayrhofer, Jürgen Fuss, and Iulia Ion. 2013. UACAP: A unified auxiliary channel authentication protocol. *IEEE Trans. Mobile Comput.* 12 (Apr. 2013), 710–721. https://doi.org/10.1109/TMC.2012.43

[184] Rene Mayrhofer and Hans Gellersen. 2007. Shake well before use: Authentication based on accelerometer data. In *Proceedings of the International Conference on Pervasive Computing*. Springer, 144–161.

[185] Rene Mayrhofer and Hans Gellersen. 2009. Shake well before use: Intuitive and secure pairing of mobile devices. *IEEE Trans. Mobile Comput.* 8, 6 (Jun. 2009), 792–806.

[186] Maryam Mehrnezhad, Feng Hao, and Siamak F. Shahandashti. 2014. Tap-Tap and Pay (TTP): Preventing man-in-the-middle attacks in NFC payment using mobile sensors. In *Proceedings of the 2nd International Conference on Research in Security Standardisation (SSR'15).*

[187] Maryam Mehrnezhad, Feng Hao, and Siamak F. Shahandashti. 2015. Tap-tap and pay (TTP): Preventing the mafia attack in NFC payment. In *Proceedings of the International Conference on Research in Security Standardisation.* Springer, 21–39.

[188] W. Meng, D. S. Wong, S. Furnell, and J. Zhou. 2015. Surveying the development of biometric user authentication on mobile phones. *IEEE Commun. Surv. Tutor.* 17, 3 (thirdquarter 2015), 1268–1293. https://doi.org/10.1109/COMST.2014.2386915

[189] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou. 2015. Surveying the development of biometric user authentication on mobile phones. *IEEE Commun. Surv. Tutor.* 17, 3 (2015), 1268–1293.

[190] Markus Miettinen, N. Asokan, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and Majid Sobhani. 2014. Context-based zero-interaction pairing and key evolution for advanced personal devices. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security.* ACM, 880–891.

[191] Markus Miettinen, Thien Duc Nguyen, Ahmad-Reza Sadeghi, and N. Asokan. 2018. Revisiting context-based authentication in iot. In *Proceedings of the 55th Annual Design Automation Conference.* ACM, 32.

[192] Chris J. Mitchell and Liqun Chen. 1996. Comments on the S/KEY user authentication scheme. *ACM SIGOPS Operat. Syst. Rev.* 30, 4 (1996), 12–16.

[193] Bendik B. Mjaaland, Patrick Bours, and Danilo Gligoroski. 2010. Walk the walk: Attacking gait biometrics by imitation. In *Proceedings of the International Conference on Information Security.* Springer, 361–380.

[194] Manar Mohamed, Prakash Shrestha, and Nitesh Saxena. 2019. Challenge-response behavioral mobile authentication: A comparative study of graphical patterns and cognitive games. In *Proceedings of the 35th Annual Computer Security Applications Conference.* 355–365.

[195] John V. Monaco, Md Liakat Ali, and Charles C. Tappert. 2015. Spoofing key-press latencies with a generative keystroke dynamics model. In *Proceedings of the IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS'15)*. IEEE, 1–8.

[196] Stacy J. Morris. 2004. *A Shoe-integrated Sensor System for Wireless Gait Analysis and Real-time Therapeutic Feedback*. Ph.D. Dissertation. Massachusetts Institute of Technology.

[197] Muhammad Muaaz and René Mayrhofer. 2013. An analysis of different approaches to gait recognition using cell phone based accelerometers. In *Proceedings of the International Conference on Advances in Mobile Computing & Multimedia*. ACM, 293.

[198] Muhammad Muaaz and René Mayrhofer. 2014. Orientation independent cell phone based gait authentication. In *Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia*. ACM, 161–164.

[199] Muhammad Muaaz and René Mayrhofer. 2015. Cross pocket gait authentication using mobile phone based accelerometer sensor. In *Proceedings of the International Conference on Computer Aided Systems Theory*. Springer, 731–738.

[200] Muhammad Muaaz and René Mayrhofer. 2017. Smartphone-based gait recognition: From authentication to imitation. *IEEE Trans. Mobile Comput*. https://doi.org/10.1109/TMC.2017.2686855

[201] Tempestt Neal and Damon Woodard. 2020. Presentation attacks in mobile and continuous behavioral biometric systems. In *Securing Social Identity in Mobile Platforms*. Springer, 21–40.

[202] Ching Yu Ng, Willy Susilo, Yi Mu, and Reihaneh Safavi-Naini. 2008. RFID privacy models revisited. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS'08)*, Vol. 5283. Springer, 251–266.

[203] Le Ngu Nguyen and Stephan Sigg. 2016. Personalized image-based user authentication using wearable cameras. arXiv:1612.06209. Retrieved from https://arxiv.org/abs/1612.06209.

[204] Phuc Nguyen, Ufuk Muncuk, Ashwin Ashok, Kaushik R. Chowdhury, Marco Gruteser, and Tam Vu. 2016. Battery-free identification token for touch sensing devices. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*. ACM, 109–122.

[205] Mark Nixon, John Carter, D. Cunado, Ping Huang, and S. V. Stevenage. 1996. Automatic gait recognition. In *Biometrics*. Springer, 231–249.

[206] Ian Oakley and Andrea Bianchi. 2012. Multi-touch passwords for mobile device access. In *Proceedings of the ACM Conference on Ubiquitous Computing*. ACM, 611–612.

[207] Chui Sian Ong, Klara Nahrstedt, and Wanghong Yuan. 2003. Quality of protection for mobile multimedia applications. In *Proceedings of the 2003 International Conference on Multimedia and Expo (ICME'03)*, Vol. 2. IEEE, II–137.

[208] Rolf Oppliger. 2011. *Contemporary Cryptography*. Artech House.

[209] Radu-Ioan Paise and Serge Vaudenay. 2008. Mutual authentication in RFID: Security and privacy. In *Proceedings of the ACM Symposium on Information, Computer and Communications Security*. ACM, 292–299.

[210] Keyurkumar Patel, Hu Han, and A. K. Jain. 2016. Secure face unlock: Spoof detection on smartphones. *IEEE Trans. Inf. Forens. Secur.* (Jun. 2016).

[211] Vishal M. Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello. 2016. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Sign. Process. Mag.* 33, 4 (2016), 49–61.

[212] Raphael C.-W. Phan and Patrick Mingard. 2012. Analyzing the secure simple pairing in bluetooth v4. 0. *Wireless Pers. Commun.* 64, 4 (2012), 719–737.

[213] Justin D. Pierce, Jason G. Wells, Matthew J. Warren, and David R. Mackay. 2003. A conceptual model for graphical authentication. In *Proceedings of the 1st Australian Information Security Management Conference*, Vol. 24. 347–351.

[214] M. La Polla, F. Martinelli, and D. Sgandurra. 2013. A survey on security for mobile devices. *IEEE Commun. Surv. Tutor.* 15, 1 (2013), 446–471.

[215] Sarah Prange, Lukas Mecke, Michael Stadler, Maximilian Balluff, Mohamed Khamis, and Florian Alt. 2019. Securing personal items in public space: Stories of attacks and threats. In *Proceedings of the 18th International Conference on Mobile and Ubiquitous Multimedia*. 1–8.

[216] Sarah Prange, Emanuel von Zezschwitz, and Florian Alt. 2019. Vision: Exploring challenges and opportunities for usable authentication in the smart home. In *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW'19)*. IEEE, 154–158.

[217] Khandaker A. Rahman, Kiran S. Balagani, and Vir V. Phoha. 2013. Snoop-forge-replay attacks on continuous verification with keystrokes. *IEEE Trans. Inf. Forens. Secur.* 8, 3 (2013), 528–541.

[218] Raghavendra Ramachandra and Christoph Busch. 2017. Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Comput. Surv.* 50, 1 (2017), 1–37.

[219] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle. 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst. J.* 40, 3 (2001), 614–634.

[220] S. Ray and J. Bhadra. 2016. Security challenges in mobile and iot systems. In *Proceedings of the 29th IEEE International System-on-chip Conference (SOCC'16)*. 356–361.

[221] Girish Revadigar, Chitra Javali, Weitao Xu, Athanasios V. Vasilakos, Wen Hu, and Sanjay Jha. 2017. Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables. *IEEE Trans. Inf. Forens. Secur.* 12, 10 (2017), 2467–2482.

[222] A. Revathi, C. Jeyalakshmi, and Karuppusamy Thenmozhi. 2019. Person authentication using speech as a biometric against play back attacks. *Multimedia Tools Appl.* 78, 2 (2019), 1569–1582.

[223] Daniel Ritter, Florian Schaub, Marcel Walch, and Michael Weber. 2013. MIBA: Multitouch image-based authentication on smartphones. In *CHI'13 Extended Abstracts on Human Factors in Computing Systems*. ACM, 787–792.

[224] Oriana Riva, Chuan Qin, Karin Strauss, and Dimitrios Lymberopoulos. 2012. Progressive authentication: Deciding when to authenticate on mobile phones. In *Proceedings of the USENIX Security Symposium*. 301–316.

[225] Paul Cador Roberts, Laura Posey Benofsky, William Gifford Holt, Leslie Helena Johnson, Madeline Jinx Bryant, and Nicholas I. Nussbaum. 2009. Systems and methods for demonstrating authenticity of a virtual machine using a security image. https://patents.google.com/patent/US20060253706A1/en.

[226] Paul Cador Roberts, Laura Posey Benofsky, William Gifford Holt, Leslie Helena Johnson, Bryan Mark Willman, and Madeline Jinx Bryant. 2010. Systems and methods for determining if applications executing on a computer system are trusted. https://www.freepatentsonline.com/y2006/0253705.

[227] Liu Rong, Zhou Jianzhong, Liu Ming, and Hou Xiangfeng. 2007. A wearable acceleration sensor system for gait recognition. In *Proceedings of the IEEE Conference on Industrial Electronics and Applications*. 2654–2659.

[228] Liu Rong, Duan Zhiguo, Zhou Jianzhong, and Liu Ming. 2007. identification of individual walking patterns using gait acceleration. In *Proceedings of the International Conference on Bioinformatics and Biomedical Engineering*. 543–546.

[229] Volker Roth, Kai Richter, and Rene Freidinger. 2004. A PIN-entry method resilient against shoulder surfing. In *Proceedings of the 11th ACM Conference on Computer and Communications Security*. ACM, 236–245.

[230] Virginia Ruiz-Albacete, Pedro Tome-Gonzalez, Fernando Alonso-Fernandez, Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia. 2008. Direct attacks using fake images in iris verification. In *Proceedings of the European Workshop on Biometrics and Identity Management*. Springer, 181–190.

[231] Pouya Samangouei, Vishal M. Patel, and Rama Chellappa. 2015. Attribute-based continuous user authentication on mobile devices. In *Proceedings of the IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS'15)*. IEEE, 1–8.

[232] S. Sandhya and K. A. S. Devi. 2012. Analysis of bluetooth threats and v4.0 security features. In *Proceedings of the International Conference on Computing, Communication and Applications*.

[233] J. Schmidt. 2017. *Requirements for Password-authenticated Key Agreement (PAKE) Schemes*. Technical Report.

[234] Stefan Schneegass, Frank Steimle, Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2014. Smudgesafe: Geometric image transformations for smudge-resistant user authentication. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*. ACM, 775–786.

[235] Bruce Schneier. 1999. The uses and abuses of biometrics. *Commun. ACM* 42, 8 (1999), 136–136.

[236] Dominik Schürmann, Arne Brüsch, Ngu Nguyen, Stephan Sigg, and Lars Wolf. 2018. Moves like jagger: Exploiting variations in instantaneous gait for spontaneous device pairing. *Perv. Mobile Comput.* 47 (2018), 1–12.

[237] Dominik Schürmann, Arne Brüsch, Stephan Sigg, and Lars Wolf. 2017. BANDANA—Body area network device-to-device authentication using natural gait. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom'17)*. 190–196.

[238] Dominik Schürmann and Stephan Sigg. 2013. Secure communication based on ambient audio. *IEEE Trans. Mobile Comput.* 12, 2 (2013), 358–370.

[239] Abdul Serwadda and Vir V. Phoha. 2013. Examining a large keystroke biometrics dataset for statistical-attack openings. *ACM Trans. Inf. Syst. Secur.* 16, 2 (2013), 8.

[240] Abdul Serwadda, Vir V. Phoha, Zibo Wang, Rajesh Kumar, and Diksha Shukla. 2016. Toward robotic robbery on the touch screen. *ACM Trans. Inf. Syst. Secur.* 18, 4 (2016), 14.

[241] Mohit Sethi, Markku Antikainen, and Tuomas Aura. 2014. Commitment-based device pairing with synchronized drawing. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom'14)*. IEEE, 181–189.

[242] Misbah Shafi and Rakesh Kumar Jha. 2020. Half-duplex attack: An effectual attack modelling in D2D communication. In *Proceedings of the International Conference on Communication Systems & Networks (COMSNETS'20)*. IEEE, 879–881.

[243] Jiacheng Shang and Jie Wu. 2019. A usable authentication system using wrist-worn photoplethysmography sensors on smartwatches. In *Proceedings of the IEEE Conference on Communications and Network Security (CNS'19)*. IEEE, 1–9.

[244] Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer, and Michael K. Reiter. 2016. Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1528–1540.

[245] Sang-Yun Shin, Yong-Won Kang, and Yong-Guk Kim. 2020. Android-GAN: Defending against android pattern attacks using multi-modal generative network as anomaly detector. *Expert Syst. Appl.* 141 (2020), 112–964.

[246] Babins Shrestha, Manar Mohamed, Sandeep Tamrakar, and Nitesh Saxena. 2016. Theft-resilient mobile wallets: Transparently authenticating NFC users with tapping gesture biometrics. In *Proceedings of the 32nd Annual Conference on Computer Security Applications*. ACM, 265–276.

[247] Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, and N. Asokan. 2014. Drone to the rescue: Relay-resilient authentication using ambient multi-sensing. In *Proceedings of the International Conference on Financial Cryptography and Data Security*. Springer, 349–364.

[248] Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, and N. Asokan. 2018. Sensor-based proximity detection in the face of active adversaries. *IEEE Trans. Mobile Comput.* (2018).

[249] Stephan Sigg, Eemil Lagerspetz, Ella Peltonen, Petteri Nurmi, and Sasu Tarkoma. 2016. Sovereignty of the apps: There's more to relevance than downloads. arXiv:1611.10161. Retrieved from https://arxiv.org/abs/1611.10161.

[250] Leon Sloman, Mavis Berridge, S. Homatidis, D. Hunter, and T. Duck. 1982. Gait patterns of depressed patients and normal subjects. *Am. J. Psychiatr.* (1982).

[251] Youngbae Song, Geumhwan Cho, Seongyeol Oh, Hyoungshick Kim, and Jun Ho Huh. 2015. On the effectiveness of pattern lock strength meters: Measuring the strength of real world pattern locks. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. 2343–2352.

[252] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard. 2018. Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE Commun. Surv. Tutor.* 20, 1 (Firstquarter 2018), 465–488. https://doi.org/10.1109/COMST.2017.2779824

[253] Animesh Srivastava, Jeremy Gummeson, Mary Baker, and Kyu-Han Kim. 2015. step-by-step detection of personally collocated mobile devices. In *Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications*. ACM, 93–98.

[254] Øyvind Stang. 2007. *Gait Analysis: Is It Easy to Learn to Walk Like Someone Else?* Master's thesis.

[255] Martin Stokkenes, Raghavendra Ramachandra, and Christoph Busch. 2016. Biometric authentication protocols on smartphones: An overview. In *Proceedings of the 9th International Conference on Security of Information and Networks*. ACM, 136–140.

[256] Jonathan D. Stosz and Lisa A. Alyea. 1994. Automated system for fingerprint authentication using pores and ridge structure. In *Automatic Systems for the Identification and Inspection of Humans*, Vol. 2277. International Society for Optics and Photonics, 210–224.

[257] Chen Sun, Yang Wang, and Jun Zheng. 2014. Dissecting pattern unlock: The effect of pattern strength meter on pattern selection. *J. Inf. Secur. Appl.* 19, 4 (2014), 308–320.

[258] Jingchao Sun, Rui Zhang, Jinxue Zhang, and Yanchao Zhang. 2014. Touchin: Sightless two-factor authentication on multi-touch mobile devices. In *Proceedings of the IEEE Conference on Communications and Network Security*. IEEE, 436–444.

[259] Yan Sun and Anup Kumar. 2008. Quality-of-protection (QoP): a quantitative methodology to grade security services. In *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops (ICDCS'08)*. IEEE, 394–399.

[260] Yingnan Sun, Charence Wong, Guang-Zhong Yang, and Benny Lo. 2017. Secure key generation using gait features for body sensor networks. In *Proceedings of the IEEE 14th International Conference on Wearable and Implantable Body Sensor Networks (BSN'17)*. IEEE, 206–210.

[261] Xiaoyuan Suo, Ying Zhu, and G. Scott Owen. 2005. Graphical passwords: A survey. In *Proceedings of the 21st Annual Computer Security Applications Conference*. IEEE.

[262] Jani Suomalainen, Jukka Valkonen, and N. Asokan. 2007. *Security Associations in Personal Networks: A Comparative Analysis*. 43–57.

[263] Tetsuji Takada and Hideki Koike. 2003. Awase-e: Image-based authentication for mobile phones using users favorite images. *Hum.-Comput. Interact. Mobile Dev. Serv.* (2003), 347–351.

[264] Tetsuji Takada and Yuki Kokubun. 2013. Extended pin authentication scheme allowing multi-touch key input. In *Proceedings of the International Conference on Advances in Mobile Computing & Multimedia*. ACM, 307.

[265] Tetsuji Takada and Yuki Kokubun. 2014. MTAPIN: Multi-touch key input enhances security of PIN authentication while keeping usability. *Int. J. Perv. Comput. Commun.* 10, 3 (2014), 276–290.

[266] Furkan Tari, Ant Ozok, and Stephen H. Holden. 2006. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In *Proceedings of the 2nd Symposium on Usable Privacy and Security*. ACM, 56–66.

[267] Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen. 2016. A survey on touch dynamics authentication in mobile devices. *Comput. Secur.* 59 (2016), 210–235.

[268] Chee Meng Tey, Payas Gupta, and Debin Gao. 2013. I can be you: Questioning the use of keystroke dynamics as biometrics.(2013). In *Proceedings of the 20th Annual Network and Distributed System Security Symposium (NDSS'13)*. 1–16.

[269] Julie Thorpe and Paul C. Van Oorschot. 2004. Towards secure design choices for implementing graphical passwords. In *Proceedings of the 20th Annual Computer Security Applications Conference*. IEEE, 50–60.

[270] Christian Tiefenau, Maximilian Häring, Mohamed Khamis, and Emanuel von Zezschwitz. 2019. "Please enter your PIN"—On the risk of bypass attacks on biometric authentication on mobile devices. arXiv:1911.07692. Retrieved from https://arxiv.org/abs/1911.07692.

[271] Ruben Tolosana, Ruben Vera-Rodriguez, and Julian Fierrez. 2019. Biotouchpass: Handwritten passwords for touchscreen biometrics. *IEEE Trans. Mobile Comput.* (2019).

[272] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales, and Javier Ortega-Garcia. 2017. Benchmarking desktop and mobile handwriting across COTS devices: The e-biosign biometric database. *PLoS One* 12, 5 (2017), e0176792.

[273] Ruben Tolosana, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. 2019. Presentation attacks in signature biometrics: Types and introduction to attack detection. In *Handbook of Biometric Anti-spoofing*. Springer, 439–453.

[274] Mohsen Toorani. 2014. Security analysis of J-PAKE. In *Proceedings of the IEEE Symposium on Computers and Communication (ISCC'14)*. IEEE, 1–6.

[275] Hien Thi Thu Truong, Xiang Gao, Babins Shrestha, Nitesh Saxena, N. Asokan, and Petteri Nurmi. 2014. Comparing and fusing different sensor modalities for relay attack resistance in zero-interaction authentication. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom'14)*. IEEE, 163–171.

[276] Umut Uludag and Anil K. Jain. 2004. Attacks on biometric systems: A case study in fingerprints. In *Security, Steganography, and Watermarking of Multimedia Contents VI*, Vol. 5306. International Society for Optics and Photonics, 622–634.

[277] Tom Van Goethem, Wout Scheepers, Davy Preuveneers, and Wouter Joosen. 2016. Accelerometer-based device fingerprinting for multi-factor mobile authentication. In *Proceedings of the International Symposium on Engineering Secure Software and Systems*. Springer, 106–121.

[278] Alex Varshavsky, Adin Scannell, Anthony LaMarca, and Eyal De Lara. 2007. Amigo: Proximity-based authentication of mobile devices. In *Proceedings of the International Conference on Ubiquitous Computing*. Springer, 253–270.

[279] Vassilios Vassilakis, Emmanouil Panaousis, and Haralambos Mouratidis. 2016. Security challenges of small cell as a service in virtualized mobile edge, computing environments. In *Proceedings of the IFIP International Conference on Information Security Theory and Practice*. Springer, 70–84.

[280] Serge Vaudenay. 2005. Secure communications over insecure channels based on short authenticated strings. In *Crypto*, Vol. 3621. Springer, 309–326.

[281] Prateek Verma, Maheedhar Dubey, Somak Basu, and Praveen Verma. 2012. Hough transform method for iris recognition-a biometric approach. *Int. J. Eng. Innov. Technol.* 1, 6 (2012), 43–48.

[282] Elena Vildjiounaite, Satu-Marja Mäkelä, Mikko Lindholm, Reima Riihimäki, Vesa Kyllönen, Jani Mäntyjärvi, and Heikki Ailisto. 2006. unobtrusive multimodal biometrics for ensuring privacy and information security with personal devices. In *Proceedings of the International Conference on Pervasive Computing*. Springer, 187–201.

[283] Emanuel Von Zezschwitz, Anton Koslow, Alexander De Luca, and Heinrich Hussmann. 2013. Making graphic-based authentication secure against smudge attacks. In *Proceedings of the 2013 International Conference on Intelligent User Interfaces*. ACM, 277–286.

[284] Jonathan Voris, Yingbo Song, Malek Ben Salem, and Salvatore Stolfo. 2016. You are what you use: An initial study of authenticating mobile users via application usage. In *Proceedings of the 8th EAI International Conference on Mobile Computing, Applications and Services*. Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, 51–61.

[285] Avani Vyas and Sujata Pal. 2020. Preventing security and privacy attacks in WBANs. In *Handbook of Computer Networks and Cyber Security*. Springer, 201–225.

[286] Dayong Wang, Steven C. H. Hoi, Ying He, Jianke Zhu, Tao Mei, and Jiebo Luo. 2013. Retrieval-based face annotation by weak label regularized local coordinate coding. *IEEE Trans. Pattern Anal. Mach. Intelligence* 36, 3 (2013), 550–563.

[287] Yuhua Wang, Chunhua Wu, Kangfeng Zheng, and Xiujuan Wang. 2019. Improving reliability: User authentication on smartphones using keystroke biometrics. *IEEE Access* 7 (2019), 26218–26228.

[288] Zibo Wang, Abdul Serwadda, Kiran S Balagani, and Vir V. Phoha. 2012. Transforming animals in a cyber-behavioral biometric menagerie with frog-boiling attacks. In *Proceedings of the IEEE 5th International Conference on Biometrics: Theory, Applications and Systems (BTAS'12)*. IEEE, 289–296.

[289] Colin Ware and Harutune H. Mikaelian. 1987. An evaluation of an eye tracker as a device for computer input2. *ACM SIGCHI Bull.* 18, 4 (1987), 183–188.

[290] James Wayman, Anil Jain, Davide Maltoni, and Dario Maio. 2005. An introduction to biometric authentication systems. *Biometr. Syst.* (2005), 1–20.

[291] Justin Weaver, Kenrick Mock, and Bogdan Hoanca. 2011. Gaze-based password authentication through automatic clustering of gaze points. In *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC'11)*. IEEE, 2749–2754.

[292] Daphna Weinshall and Scott Kirkpatrick. 2004. Passwords you'll never forget, but can't recall. In *CHI'04 Extended Abstracts on Human Factors in Computing Systems*. ACM, 1399–1402.

[293] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. 2005. Passpoints: Design and longitudinal evaluation of a graphical password system. *Int. J. Hum.-Comput. Stud.* 63, 1–2 (2005), 102–127.

[294] Susan Wiedenbeck, Jim Waters, Leonardo Sobrado, and Jean-Camille Birget. 2006. Design and evaluation of a shoulder-surfing resistant graphical password scheme. In *Proceedings of the Working Conference on Advanced Visual Interfaces*. ACM, 177–184.

[295] Cong Wu, Kun He, Jing Chen, Ziming Zhao, and Ruiying Du. 2020. Liveness is not enough: Enhancing fingerprint authentication with behavioral biometrics to defeat puppet attacks. In *Proceedings of the 29th USENIX Security Symposium (USENIX Security'20)*.

[296] Thomas D. Wu. 1998. The secure remote password protocol. In *Proceedings of the Network and Distributed System Security Symposium (NDSS'98)*, Vol. 98. 97–111.

[297] Weitao Xu, Chitra Javali, Girish Revadigar, Chengwen Luo, Neil Bergmann, and Wen Hu. 2017. Gait-key: A gait-based shared secret key generation protocol for wearable devices. *ACM Trans. Sens. Netw.* 13, 1 (2017), 6.

[298] W. Xu, G. Revadigar, C. Luo, N. Bergmann, and W. Hu. 2016. Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication. In *Proceedings of the 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN'16)*.

[299] Lin Yang, Wei Wang, and Qian Zhang. 2016. Secret from muscle: Enabling secure pairing with electromyography. In *Proceedings of the 14th ACM Conference on Embedded Network Sensor Systems CD-ROM*. ACM, 28–41.

[300] Qinggang Yue, Zhen Ling, Xinwen Fu, Benyuan Liu, Kui Ren, and Wei Zhao. 2014. Blind recognition of touched keys on mobile devices. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1403–1414.

[301] Guoming Zhang, Chen Yan, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. 2017. Dolphinattack: Inaudible voice commands. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. ACM, 103–117.

[302] Linghan Zhang, Sheng Tan, and Jie Yang. 2017. Hearing your voice is not enough: An articulatory gesture based liveness detection for voice authentication. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. ACM, 57–71.

[303] Philip Zimmermann, Alan Johnston, and Jon Callas. 2011. *ZRTP: Media Path Key Agreement for Unicast Secure RTP*. Technical Report.

Received August 2020; revised May 2021; accepted July 2021