A Survey on Adaptive Authentication

PATRICIA ARIAS-CABARCOS, University of Mannheim, Germany
CHRISTIAN KRUPITZER, University of Würzburg, Germany
CHRISTIAN BECKER, University of Mannheim, Germany

Adaptive Authentication allows a system to dynamically select the best mechanism(s) for authenticating a user depending on contextual factors, such as location, proximity to devices, and other attributes. Though this technology has the potential to change the current password-dominated authentication landscape, research to date has not led to practical solutions that transcend to our daily lives. Motivated to find out how to improve adaptive authentication design, we provide a structured survey of the existing literature to date and analyze it to identify and discuss current research challenges and future directions.

CCS Concepts: • **Computer systems organization → Self-organizing autonomic computing**; • **Security and privacy → Usability in security and privacy**; *Distributed systems security*; *Software and application security*;

Additional Key Words and Phrases: Adaptive authentication, usable security, systematic literature review

ACM Reference format:
Patricia Arias-Cabarcos, Christian Krupitzer, and Christian Becker. 2019. A Survey on Adaptive Authentication. *ACM Comput. Surv.* 52, 4, Article 80 (September 2019), 30 pages.
https://doi.org/10.1145/3336117

1 INTRODUCTION

Research on the authentication area has been intense, demonstrating over more than 40 years that, despite being dominant, passwords are flawed, insecure, and openly hated by users [1, 73]. For these reasons, there have been many academic initiatives to find alternatives to replace passwords, as well as proposals to alleviate the complexities of managing them [19, 20, 68, 97, 99, 108].

However, all this research knowledge has not yet been materialized into radically better authentication solutions. We believe that, to make progress, the focus should be placed not on finding a replacement, but on smart technologies that are able to combine multiple heterogeneous authentication mechanisms, adapting its usage to the situation.

Adaptive authentication is not a new concept; we can find initial proposals already in the early 2000s, tied to the appearance of the first ubiquitous computing systems [2]. Subsequent works delved into adaptation for smartphones and web authentication and explored the inclusion of

The work of P. Arias-Cabarcos has been supported through an Alexander von Humboldt Post-Doctoral Fellowship.
Authors' addresses: P. Arias-Cabarcos (corresponding author) and C. Becker, University of Mannheim, L15, 1-6, Mannheim, 69161, Germany; emails: pariasca@mail.uni-mannheim.de, christian.becker@uni-mannheim.de; C. Krupitzer, University of Würzburg, Am Hubland, Würzburg, 97074, Germany; email: christian.krupitzer@uni-wuerzburg.de.

0360-0300/2019/09-ART80 $15.00
https://doi.org/10.1145/3336117

emerging implicit [96] and continuous authenticators [78]. In this sense, the integration of biometrics, especially those that are behavioral-based (e.g., typing patterns [92], gait [81], or brainwaves [104]), is key to favor a less obtrusive, more usable interaction.

Though there are recent in-depth studies of password alternatives [19] as well as surveys that extensively analyze biometrics [71] and their usage for implicit authentication [4], no work has yet provided a comprehensive overview of the combined use of different authentication mechanisms within adaptive systems. Existing surveys are either limited, covering just a few adaptation examples [8], or have a more general focus on the broader field of adaptive security [32, 34, 107, 117]. To fill this gap, we set out to systematically review the literature on adaptive authentication.

Our approach is to formalize the findings of state-of-the-art adaptive authentication systems through the lens of the extensively studied self-adaptive systems discipline and its design principles [24, 61]. Surprisingly, all the reviewed works have neglected such a huge body of research. As we will discuss later, their focus has been put on demonstrating feasibility and basic usability improvements in specific scenarios rather than on design, which hinders faster advance on research. In fact, our analysis uncovers a significant fundamental challenge: adaptive authentication systems to date are difficult to extend or reuse (e.g., to include new authenticators, adaptation strategies, or contexts) and, therefore, it is hard to easily deploy new solutions and fairly compare them with each other.

First, we outline how to apply the structured modelling principles well-known in self-adaptive systems to the authentication domain; second, we survey how the literature to date covers each design dimension. Our primary goal is to identify where the design problems lie, what is missing, and to elicit a roadmap for the research community to help move forward. The main contributions are:

(1) establishing a common definition of adaptive authentication systems, explaining their main architectural components,
(2) survey, systematization, and analysis of adaptive authentication approaches in the academic literature to date through the lens of self-adaptive systems design, and
(3) identification and discussion of current research challenges and future directions.

We start by introducing the related surveys in Section 2. Next, we present relevant adaptive systems concepts in Section 3, needed to understand the survey methodology described in Section 4. Section 5 introduces the building blocks of adaptive authentication systems: their authenticators. After that, we analyze adaptive authentication approaches under different design dimensions (Sections 6–9), thoroughly dissecting the state-of-the-art on the topic. Section 10 offers a consolidated overview of the surveyed works and provides a critical discussion about open challenges, from which a roadmap for future research is elicited. The article closes with a set of concluding remarks in Section 11.

2 RELATED SURVEYS

Most of the surveys related to our work fall in the category of adaptive security, analyzing systems that change their behavior to adjust security defenses at runtime. In 2007, Elkhodary and Whittle [32] conducted a review of four generic approaches for adaptive security, which was updated by Evesti and Ovaska [34] with five more approaches in 2013. Both surveys look into generic solutions for self-adaptive security systems at an abstract level that does not include specificities related to authentication. Furthermore, since these reviews are not systematic, but based on papers considered significant, the literature coverage is rather limited. In their evaluation frameworks, besides the type of security mechanisms in use and the supported self-adaptation properties, they introduce other general considerations, such as extensibility, flexibility, or reusability, which served as a basis to frame the discussion of challenges in our survey. More recently, the literature

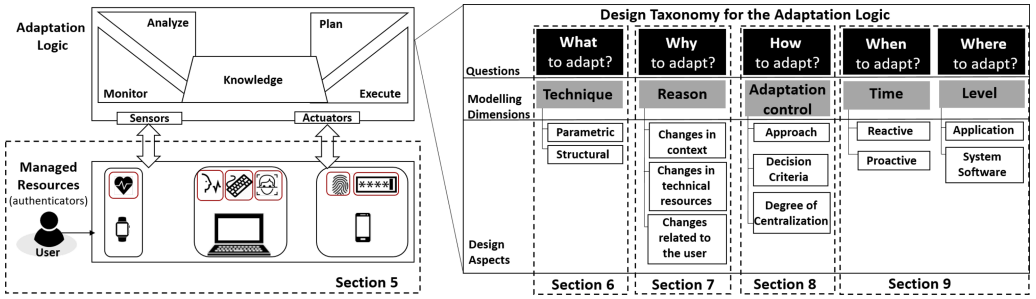

Fig. 1. The left side of the image shows a generic MAPE-K architecture for distributed adaptive authentication systems. The right side depicts the taxonomy of design dimensions for developing the adaptation logic, according to Reference [61]. As a whole, this picture provides a roadmap for the article, indicating which aspects are covered in the literature survey of adaptive authentication works, and which sections discuss each aspect.

on adaptive security has been surveyed following systematic approaches in References [107, 117]. On the one hand, Yuan et al. [117] reviewed 107 articles and compared them based on a multilevel taxonomy including security and adaptation aspects. However, this taxonomy covers the security goals of confidentiality, integrity and availability, but not authentication. On the other hand, Tziakouris et al. [107] have a slightly different and specific focus for their survey. They reviewed the literature on adaptive security looking at how the underlying architectures of the reported research are applicable to open and ultra-large environments.

While these works provide detailed analyses and valuable insights on self-adaptive security systems, they are not concerned with the design challenges that arise in the specific domain of authentication. Looking at this concrete aspect of security, though there are extensive literature reviews covering authentication subtopics such as behavioral biometrics [71] or implicit authentication [4], we have found just one survey at the intersection between adaptation and authentication [8]. In this work, Bakar and Haron describe and identify issues in four representative adaptive authentication proposals, as a basis to present their own system. In our article, we go beyond by systematically covering research works on adaptive authentication, using the methodological design principles of self-adaptive systems to analyze their architectures. We further discuss specific challenges for adaptive authentication systems and establish a research roadmap intended to foster advance on the topic and influence real-world implementations.

3 SELF-ADAPTIVE SYSTEMS IN A NUTSHELL

The research field of *self-adaptive systems* was born in the late '90s driven by the need to deal with the ever-increasing complexity and dynamism of software systems, a situation that still holds true today. With this goal in mind, the self-adaptation approach envisions the development of *"systems that are able to modify their behavior and/or structure in response to their perception of the environment and the system itself"* [24]. This approach has been widely recognized as effective not only to manage complexity but also to design more versatile, flexible, resilient, dependable, energy-efficient, recoverable, customizable, configurable, and self-optimizing software [24, 30, 55, 59, 76].

Research on the field of adaptive systems has converged to a reference architectural model for adaptation, whose main components are depicted in Figure 1. Accordingly, an adaptive system comprises two parts: a set of *managed resources* and the *adaptation logic*. For adaptation to happen, the adaptation logic incorporates a control structure. The most well-known structure is the MAPE-K cycle [55], which includes components to: *monitor* the environment and managed

resources (M), *analyze* the data for changes (A), *plan* adaptation (P), and control its *execution* (E), based on a shared *knowledge* repository (K). To model what should be done in the adaptation logic, there is a well-known procedure [61, 89], which consists of answering five basic questions,[1] namely: *What?*, *Why?*, *How?*, *When?*, and *Where?* to adapt. Each question targets a modeling dimension and the answers give insights on the design aspects to consider when prototyping an adaptive system. The taxonomy in Reference [61] (see Figure 1) summarizes this design procedure and complements it with different design dimensions.

Self-adaptation has become an important research topic with applicability to many diverse domains [67], such as, e.g., autonomous driving [15], adaptive smart homes [52], or dynamic web service composition [98]. In the authentication domain, which is the focus of this article, though there are proposals to automatically adapt authentication mechanisms to the user environment, they have not been defined or studied considering the bigger picture and existing research on self-adaptation.

Therefore, though there is no formal definition of adaptive authentication, it can be easily rewritten from the definition of general adaptive systems [24, 61] as follows:

> *"An **adaptive authentication system** is able to automatically modify its behavior and/or structure in response to changes in its operating environment."*

Mapping the architectural model of adaptive systems to the authentication domain, the managed resources are the authenticators (available in user devices and applications), and the adaptation logic is the software layer in charge of orchestrating their usage according to the sensed situation. Furthermore, the adaptation logic can run on the same device as the application that wants to use the authenticators, or on another device, enabling different use cases.

According to the above definition and concepts, an example of adaptive authentication with on-device logic could be a smartphone that detects when the user is at home (change in the operating environment) and deactivates password protection (automatic behavior modification) until she moves out to a different place [46]. Or, if the adaptation logic is distributed, then we can have a system where a user authenticates with the smartphone fingerprint scanner to access her laptop, when both devices are nearby.

In Figure 1, we visually summarize the discussed elements that compose an adaptive authentication system, together with the applicable design dimensions of self-adaptive systems. This image works as a roadmap for the literature survey presented in this article, following the methodology described in the next section.

4 METHODOLOGY

By transferring the concepts from the taxonomy of self-adaptive systems design [61] to adaptive authentication, it is possible to confront the development of systems where the managed resources are devices and applications with heterogeneous authenticators. However, this kind of methodological approach to design has never been applied to the authentication domain [6]. Our goal here is to use the taxonomy to analyze how the literature covers the different design dimensions, what can we learn from that, and what is missing to advance research.

In line with related literature [40], we narrow the scope of this survey to research approaches. While commercial solutions—such as iPhone X Face ID—are interesting examples of adaptive authentication systems, the availability of the details on their implementation is limited. Hence, comparability is not given.

[1] We omit the *Who* dimension (*"Who has to perform the adaptation?"*) mentioned in Reference [89], because we consider that a self-adaptive system should adapt automatically without user involvement, as in Reference [61].

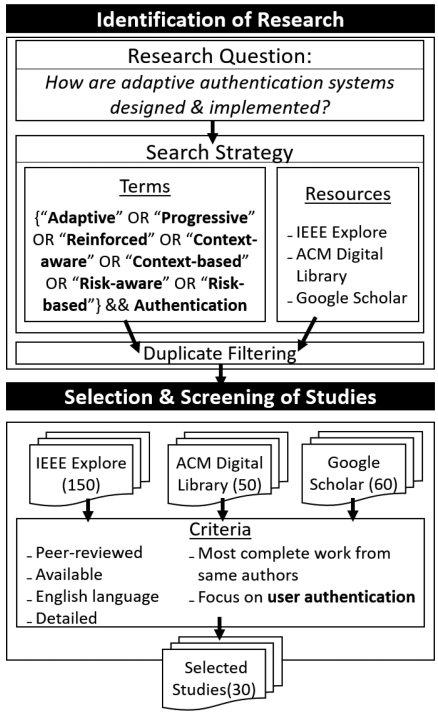

Fig. 2. Summary of the procedure for identifying and selecting relevant studies on adaptive authentication. We first analyzed the literature in top security conferences and derived key terms. We then used those key terms as shown in the diagram to extend the search to other publication venues, following Kitchenham's guidelines for systematic literature reviews [58].

We performed a systematic literature review following Kitchenham's [58] guidelines to identify relevant studies on adaptive authentication , as it is depicted in Figure 2.

Our guiding research question was *"How are adaptive authentication systems designed and implemented?"* Starting from there, we used the search keywords *"adaptive authentication"* and the semantically similar terms: *"context-aware/context-based authentication," "risk-aware/risk-based authentication," "progressive authentication,"* and *"reinforced authentication,"* elicited after an initial scan of the literature published in top security conferences.[2] Based on these search terms, we compiled works with no constraints on publication date, obtaining a set of 260 papers spanning from 2003 to 2018, after filtering duplicates. The down-selection of studies considered the following criteria. Documents were excluded if:

(1) The publication format was other than peer-reviewed academic journal or conference paper.
(2) The paper could not be retrieved using IEEE Explore, ACM Digital Library or Google Scholar.
(3) The publication language was not English.
(4) Another paper by the same authors superseded the work, in which case the most complete work was considered.

[2]ACM Computer Communications and Security, IEEE Security and Privacy, USENIX Security, Symposium on Usable Privacy and Security, and Network and Distributed System Security Symposium.

(5) The focus was not put on the design of an adaptive authentication[3] system, or the subject of authentication was not the end-user.
(6) The approach is described at a high level and not enough details are provided to address the research question.

The search and selection protocol yielded a final corpus of 30 peer-reviewed works on adaptive authentication. This corpus was sub-categorized in five clusters, depending on the scope of the adaptation: (1) authentication to smart spaces, (2) authentication to smartphones, (3) authentication to websites, (4) authentication to applications/services, and (5) other types of authentication. This division will allow the reader to better extract design commonalities per scenario.

After selection and clustering, we reviewed each paper analyzing their use of managed resources (Section 5) and their adaptation logic (Sections 6–9), with regard to the five taxonomical dimensions in Figure 1 to facilitate the understanding of the involved design aspects and classify the existing work. We then examined the literature in a consolidated way, identifying gaps and future challenges.

5 AUTHENTICATORS IN ADAPTIVE SYSTEMS

Authenticators, as discussed in Section 3, are the *managed resources* of adaptive authentication systems, the elements that need to be adapted. Table 1 shows the authentication mechanisms covered in the adaptive authentication literature, divided according to the widely used three-dimensional categorization [75] as: biometric (*"something you are"*), knowledge-based (*"something you know"*), and token-based (*"something you have"*).

Next, we further discuss the usage of authenticators implemented across the surveyed works according to three key aspects: *diversity*, *continuity*, and *pluggability*.

Authenticator diversity. The inclusion of diverse sets of authenticators improves the flexibility of the adaptive system, favoring their applicability to different scenarios. Looking at the literature, it can be observed that passwords and/or PINs are supported by most of the works and, on the opposite side, tokens are the less common authenticators. Biometrics and behaviorals in particular, are included more frequently than tokens as an alternative or complement to knowledge-based authenticators. The reason for these choices is that the majority of approaches focus on improving usability through adaptation, for which behavioral biometrics are good candidates, since the user can be implicitly "sensed" without requiring explicit interaction. In general, the range of supported authenticators is limited (2-authenticator systems are the most common configuration) and normally not covering the three *"something-you-*"* categories. Gupta et al. [45] offer the most comprehensive solution, including 15 different authenticators.

Authenticator Continuity. Authenticators can be used on a *one-shot* basis to log the user in at a particular instant, or they can be used to continuously monitor in real time that the legitimate person is using the service during the whole duration of the session. A plethora of continuous authentication mechanisms has been proposed and analyzed in the literature [78], but only a subset of them is covered in the studied adaptive systems: gait, trajectory, face, voice, behavior-based multimodal profiling, and token presence. It can be observed that there is no single recipe for multimodal profiling, but different behavioral features are selected based on the specific scenario. Table 2 details the features and Machine-learning (ML) techniques used in the profiling mechanisms across the different works.

[3]We do not explore literature on authorization. This procedure (checking user's permissions) is orthogonal to authentication (checking user's identity) and normally takes place after it. Therefore, existing authorization approaches can be integrated with adaptive authentication systems.

Table 1. Overview of Authenticators Used in Adaptive Systems

	Work, Year	Something You Are: Behavioral: Multimodal	Gait	Trajectory	Signature, Text	Mouse	Keystrokes	Something You Are: Physiological: Iris, Periocular	Face	Voice	Fingerprint	Hand	Something You Know: Password	PIN	Pattern	OTP, SMS, TAN	Questions, CAPTCHA	Something You Have: User Device	RFID, NFC, BT Tokens	USB Keys	Digital Certificates
Smart Space	Cerberus [2], 2003										●		●					●	◪	●	
	[11], 2003												●						●		
	[62], 2008												●					●	●		
	[42], 2009												●								
	UC-TBAS [109], 2011	○									○		●			●					
	CARS-AD [63], 2011	◪											●				●				
Smartphone	[45], 2012												●		●						
	CASA [46], 2013												●	●							
	ConXsense [72], 2014												○								
	[81], 2014		◪																		
	[54], 2014	◪											○								
	[116], 2014			◪							●		●								
	[115], 2016								●	●	●										
	[28], 2017		◪																		
Websites	SmartAuth [80], 2015	◪											○								
	CYOA [38], 2015												●								
	[29], 2016		●		●	●	●	●	●	●	●	●	●			●	●				
	Reinforced AuthN [40], 2016	●											●			●	●				
	[69], 2016				●				●	●	●										
	ASSO [64], 2016	●									○		○						○		
Apps/Services	TreasurePhone [94], 2010													●					●		
	Progressive AuthN [84], 2011								●	●				●							
	[113], 2013	◪		●		●	●	●													
	UAP [9], 2014												●	●	●						●
	i/k-Contact [7], 2014										○		●								
	PRISM [82], 2015												○								
	UFSA [35], 2015	◪							●	●			●			●	●		●		
Other	PICO [101], 2011																		◪		
	CORMORANT [48], 2015		◪						●												
	[114], 2017								●		●			●							

Legend: "●" = includes the authentication mechanism; "○"= includes an unspecified mechanism in this *something-you-** category (the most popular mechanism is selected). If the background follows a hatched pattern, the mechanism can be used for continuous authentication. **BT** = Bluetooth; **NFC**= Near Field Communication; **RFID** = Radio Frequency Identification; **TAN** = Transaction Identification Number; **CAPTCHA** = Completely Automated Public Turing test to tell Humans and Computers Apart.

Table 2. Behavior-based Multimodal Profiling Authenticators Used in the Surveyed Adaptive Authentication Systems

Work	Behavioral-based profiling features	ML Algorithm
CARS-AD [63]	Device, application, application constraints	Vector Space Model (VSM) [90]
[54]	Application, wifi, cell, cpu load, light, noise, magnetic field, rotation	Kernel density estimators (KDE) [95]
SmartAuth [80]	Browser, user agent, SW version, device model, language, color depth, screen resolution, plugins (on client side); IP address, time of access, geolocation, request headers (on server side)	Hoeffding trees [79]
Reinforced AuthN [40]	IP address, User agent	Logistic Regresion [49]
ASSO [64]	Time, location data from GPS, cellular network information, and WLAN access points	Support Vector Machines (SVM) [47]
[113]	Location, accelerometer, magnetic field, microphone, light, battery, screen state, shutdown/boot time, calls	SVM [47]
UFSA [35]	Time, geolocation, application, browser, OS	SVM [47]

The selected behavioral features are tailored to the application scenario.

In the case of tokens as continuous authenticators, there are two operational approaches: (1) sending beacons with information that identifies the user [2]; or (2) implementing more complex cryptographic protocols, where multiple tokens need to be co-present and contribute to compute a shared secret that unlocks the system [101]. Furthermore, to facilitate token adoption, PICO [101] also explores the conversion of everyday objects into tokens by attaching RFID tags or similar components with signal emission/transmission capability to them. However, though this "tokenization" idea potentially helps in achieving more natural ways of authentication, studies show that users still feel anxious about the possibility of losing these objects and the responsibility of carrying them [105].

Authenticator Pluggability. A desirable aspect of adaptive authentication systems is flexibility. The system should not remain static serving the user with the same authentication options she enrolled in at registration time, but should evolve and provide new alternatives as new enhanced authenticators appear in the market or new devices are acquired. This extensibility is positive both for enhancing user experience and for administrators, who do not need to migrate to a completely new adaptive authentication solution every time there are changes.

One of the pillars for extensibility is pluggability, i.e., the usage of well-defined interfaces that allow developers to programmatically add new authenticators in a straightforward fashion, without re-coding the system. In the analyzed literature, just four works clearly consider pluggability [2, 38, 48, 113]. They all propose architectures where authenticators are viewed as plugins that conform to an interface, in some cases standardized; in others, self-defined. In the first category, Cerberus [2] uses the Pluggable Authentication Modules abstraction (PAM) [91] to develop two types of authenticators: device-independent (e.g., passwords), and device-dependent (e.g., fingerprint scanners). Similarly, the system proposed by Witte et al. [113] complies to the BioAPI standard [18], which enables the integration of biometric authentication modules provided by different vendors. On the other side, though not based on standard libraries or interfaces, both

CORMORANT [48] and CYOA [38] do consider their own means for authenticator pluggability. For instance, CORMORANT's authors [48] state that, though not yet formalized, they expect authentication plugins *"to feature only a minimal interface that enables their integration into the framework."* As for CYOA [38], the proposed system implements adaptation among four different authentication schemes: passwords, persuasive text passwords [39], object pass tiles [102], and persuasive cued click points [25]. Since all of these authenticators compare a hashed secret string with the one previously stored at registration time, the authors approached their integration as pluggable modules able to perform this operation, acknowledging that further work would be required to incorporate other categories of authenticators, such as biometrics.

6 WHAT TO ADAPT?—THE TECHNIQUE

Now that we have seen the managed resources (authenticators), we can start analyzing the adaptation logic with regard to the different design dimensions in Figure 1. Accordingly, the first question to answer is "*What* to adapt?" In this regard, there are two types of adaptation techniques that can be applied to authenticators [61]:

- **Parametric adaptation** achieves a modified system behavior by adjusting system parameters. An example can be tuning internal elements of specific authenticators, such as the number of features in face recognition, or the use of feature-level, score level or fusion-level algorithms in multi-modal authentication [85].
- **Structural adaptation** subsumes changes in the structure of the system, such as the exchange of components, a new composition, or the removal/addition of components. For example, it can be used to activate or deactivate an authenticator, switch between them, or require multiple authentication factors depending on the adaptation reason.

Using the supported authenticators as building blocks, the surveyed works create different adaptation scenarios by applying parametric and/or structural adjustments. The majority of the approaches for adaptive authentication are based on structural techniques (see Table 5, Section 10), possibly because this type of adaptation does not require low-level access to the authenticators and so implementation is easier. In this case, the interaction between adaptation logic and authenticator consists of simple calls to activate the authentication procedure and get the result (continuously or not). Instead, to perform parametric adaptation, the logic component needs to know which settings of the authenticators can be adapted and implement mechanisms to execute the changes.

To give a clearer idea of the kind of low-level parameters to adjust, Table 3 summarizes those works exploring parametric adaptation. A type of authentication that is commonly adapted by adjusting parameters is behavioral biometrics, since behavioral features are less stable than physiological features [75] and their accuracy varies more due to changes in external conditions. For example, keystroke patterns are different when the user is moving or not, and gait changes if the user is injured. Because of this, it is useful to have different *templates* that allow for accurate identification under each condition. Template switching is a parametric adjustment considered in References [28, 81]. Another parameter that is used for adapting behaviorals is the set of selected *features* used in the comparison. In Reference [80], users select which identifying features are collected to build their fingerprint depending on the context, e.g., deciding not to send location data when the user is not at work. Though the idea behind this adaptation is to improve privacy, it also increases authentication accuracy by introducing diversity in the fingerprints.

Bardram et al. [11] adjust the number of explicit inputs requested to the user depending on the context: nothing if the user location and that of her token coincide, just the password if the location difference is small, and both *username* and password in case the location differs significantly.

Table 3. Authenticator Parameters in Adaptive Systems

Authenticator Category	Authenticator	Parameter	In works
Something You Are	Multimodal Behavioral	Template	CARS-AD [63]
		Features	SmartAuth [80]
	Gait	Template	[81]
	Keystroke	Template	[28]
	Face, Voice, Fingerprint	User Interaction	[115]
Something You Know	Password	Username	[11]
		Time to lock	[45]
	Pattern	Time to lock	[45]
Something You Have	RFID, NFC, and Bluetooth Tokens	Number and importance of tokens	PICO [101]

Apart from adjusting the internal settings of the authentication mechanisms, it is also possible to adapt the *interaction* method to inform the user about the selected authenticator and ask for input data. This parameter is explored in Reference [115], where three methods are considered: screen interaction (text message, touch reaction), voice interaction (voice sentences or signals and voice reaction), and vibration interaction (different kinds of vibrations and shaking reaction). For example, authentication interaction can be voice-based when a speakerphone is connected, because the user is supposedly unable to use her hands on a screen. Furthermore, when authentication is *one-shot* instead of continuous, there is a risk that a user change during the session goes undetected. To avoid session theft in this case, the *time-to-lock* can be used as an adaptation parameter, as in Reference [45]. This way, when the user inactivity period is longer than a threshold, re-authentication is required.

In the case of parametric adaptation applied to tokens, PICO [101] contemplates the adjustment of the *number and weight or "importance" of tokens*, so that objects contribute in different ways to the user authentication.

Finally, looking at the nature of the adaptation techniques and their usage in the analyzed works, we observe that the adaptive authentication use-cases that can be implemented based on each technique are diverse and therefore more richness could stem from combining both techniques.

Structural adaptation includes support to:

- Offer a list of suitable authenticators for the user to select one or more[4] of them.
- Automatically activate one or more suitable authentication mechanism(s) to login into a service.
- Alternate between no authentication required and authentication required.
- Run a continuous authenticator to get constant implicit access to the most frequently accessed low-security services and activate additional explicit mechanisms only when higher security is required.
- Use the output of implicit authenticators to modulate the required strength of *one-shot* explicit authenticators. In this way, if the probability that the user is authentic sensed through non-intrusive means is high, no further explicit input would be required; otherwise, an

[4]The strategy of using two or more authenticators is called Multifactor Authentication (MFA) and it is employed to strengthen security.

additional mechanism would be chosen that complements this probability to achieve the desired level of assurance.

Parametric adaptation includes support to:

- Change the type of interaction to communicate the user that authentication is required (audio, visual notification).
- Change the number of features or the template used in behavioral authenticators to adjust performance.
- Change the number of times a password is requested after failed authentication, the *time-to-lock*, or the amount of required explicit input data. These parameters help to adjust the relationship convenience-security.
- Change the decision algorithm of a multimodal biometric authentication (e.g., average, minimum).

7 WHY TO ADAPT?—THE REASON

The adaptation reason is the source of change that influences the system reaction, i.e., *Why* should an authenticator be triggered, modified, or deactivated? We examine the reasons underlying adaptive authentication proposals, structuring them within the three categories of change in adaptive systems (see Figure 1), namely: *context* (further divided into *security context* and *usability context*), *technical resources*, and *users*. Results are summarized in Table 4.

7.1 Changes in the Security Context

The most common adaptation reason is a contextual change that impacts security. The specific set of security contexts in the literature is shown in Table 4 and includes: *Time*, *Location*, *Device Proximity/Placement*, *Device and SW Fingerprinting*, *Activity*, *Physical Trust Relationship*, and *Data Sensitivity*. Among them, *Location* and *Data Sensitivity* are the most widely used, so we start this section by discussing their usage before explaining the usage of the others.

Location is highly present as adaptation reason in works targeting adaptive authentication inside a smart space [2, 11, 42, 62, 109], because it is required to position the user in the proximity of the smart service to use or correlate her history of transactions to a specific place. But location is also used in works focused on other authentication scenarios. Typically, they consider a subset of locations where the user frequently spends time—the most common are Home, Work, and Other—and adapt the authentication to the safety level at each of these places [45, 46, 48, 72, 94]. Alternatively, some works learn the expected user behavior at different locations and adapt authentication when there is an anomaly [9, 82].

Data sensitivity is covered in all the works oriented to provide granular adaptation depending on which application or service the user is trying to access [35, 61, 82, 84, 94, 113]. In this kind of implementation, applications and services are categorized according to the value of the information they handle. The adaptation logic uses these categories in the decision-making process to select authenticators. The most common values for sensitivity are confidence score ranges, which represent the required level of trust in the authentication performed by the authenticator. Another way of defining sensitivity in the analyzed works is by directly assigning rules of the type *"data X are safe for context Y"* (see Section 8).

Device and Software Fingerprinting are used as security context in References [9, 29, 109]. In all the three cases, data such as OS, browser, device in use, or network type serve to adjust the required authentication level when there is a divergence from common behavior.

Device Proximity, sensed through Bluetooth beacons, is the basis to assess location familiarity in References [45, 72]. The more familiar (already known) devices are concentrated in a particular

Table 4. Adaptation Reasons

	Work, Year	Security Context: Time	Location	Device Proximity/Placement	SW/Device Fingerprinting	Activity	Physical Trust Relationship	Data Sensitivity	Usability Context: Time	Location	Device Fingerprint	User/Device Position	Activity	Ambient: Light, Noise	Battery	TR	User: Role	Preferences
Smart Space	Cerberus [2], 2003		●			●										●	●	
	[11], 2003		●													●		
	[62], 2008		●													●		
	[42], 2009		●			●											●	
	UC-TBAS [109], 2011	●	●		●	●	●											
	CARS-AD [63], 2011							●	●	●						●		
Smartphone	[45], 2012		●	●														
	CASA [46], 2013		●															
	ConXsense [72], 2014		●	●														
	[81], 2014											●						
	[54], 2014															●		
	[116], 2014															●		
	[115], 2016												●					●
	[28], 2017											●						
Websites	SmartAuth [80], 2015															●		●
	CYOA [38], 2015																	●
	[29], 2016				●							●		●				
	Reinforced AuthN [40], 2016															●		
	[69], 2016								●	●	●							
	ASSO[64], 2016															●		
Apps/Services	TreasurePhone [94], 2010		●					●										
	Progressive AuthN [84], 2011			●				●							●	●		
	[113], 2013							●								●		
	UAP [9], 2014	●	●		●			●										
	i/k-Contact [7], 2014						●	●										
	PRISM [82], 2015		●			●		●										
	UFSA [35], 2015							●								●		●
Other	PICO [101], 2011															●		
	CORMORANT [48], 2015		●													●		
	[114], 2017					●								●		●		●

Location and sensitivity are the most used security contexts; usability is rarely considered.
Legend: "●" = includes the adaptation reason; **TR** = Technical Resources.

place, the safest the place is considered. Furthermore, Progressive Authentication [84] considers *Phone Placement* as a security context that aids in predicting the confidence on user authentication using a machine-learning model (see Section 8 for details on model-based adaptation).

Activity is considered as a security context in References [2, 42, 82, 109, 114], with the difference that References [2, 42] get user activity information from calendar-like applications filled by the user themselves or by administrators of the smart space (e.g., *"meeting in room X at 5pm"*), while References [82, 109, 114] infer activities through sensing user devices. In the pre-configured calendar-based works, the activity is combined with the user role to adapt the required authentication level. The system in Reference [109] logs the user purchase transactions to determine if the activity is normal or not and adapt authentication accordingly. Similarly, the approach in Reference [114] is to infer if a transaction at the Point of Sales can be considered routine or not based on its features, and select an appropriate authenticator for each case. Furthermore, Reference [82] captures information from smartphone sensors to detect activities, such as *"user is running,"* and then applies adaptation rules based on this information.

Finally, there is one work, i/k-Contact [7], considering *Physical Trust Relationship* as security context. When a user wants to access a device or application, other users in the visual range are queried to provide confirmation that the user is correct. Then, a trust score about the user identity is computed and the authentication mechanism is adapted based both on this score and the application sensitivity.

7.2 Changes in the Usability Context

Looking now at usability, we find that very few studies [28, 29, 63, 69, 81, 84, 114, 115] consider this type of context as a reason for adaptation, and only four of them [29, 63, 84, 114] combine both usability and security contexts within the adaptive authentication system.

One option for usability-driven adaptation is to rely on objective empirical measurements of authenticators' performance in relation to external conditions. For example, the authenticators in Reference [29] whose performance is impacted by the surrounding light level, such as face or iris recognition, are discarded from selection if a constraint on the luminance is not fulfilled (i.e., *"luminance <= value"*). The value of the constraint is adjusted to guarantee an adequate performance of the authenticator in terms of the desired False Acceptance Rate (FAR) and False Rejection Rate (FRR). The same approach is used in Reference [29] for authenticators affected by user position and background noise, through restrictions on the range of motion and dB range, respectively. Similarly, References [28, 81] perform experimental analyses on the performance of behavioral-based authentication with regard to the user and device position. Grounded on these measurements, when the user is detected to be sitting, standing, or walking [28] or the device is identified as being in the user's hand or in her pocket [81], the parameters of the authenticator are adjusted for better performance (see Section 6). Along the same lines, CARS-AD [63] also implements template switching to improve the performance of a behavioral algorithm. Furthermore, another relevant measurement to consider as usability context is battery consumption. Though mentioned as an important factor to consider in several studies, it is only included in Progressive Authentication [84]. In this approach, depending on whether the device is plugged or not, authenticator-related computations are performed locally or offloaded to the cloud or to another device, to provide the best trade-off between performance and delay.

Another option is to build rules that directly map the usability context to the selected authenticator. These rules can be learnt dynamically from the user as in Reference [69] or they can be statically configured based on common knowledge. This is the case in Reference [115], where available authenticators are discarded if the contextual information about user activity suggests they are not appropriate. This adaptation logic is encoded in rules of the type "*if sound is disabled,*

avoid voice authentication," because this violates the silence requirement, or "*if the user is walking, avoid face recognition,*" because it would not work properly. A similar methodology is followed in Reference [114], where rules are put in place to rank the convenience of authenticators based on usability contextual factors. More details about rules are given in Section 8.

7.3 Changes in Technical Resources

In the domain of adaptive authentication, the technical resources are the different devices and authenticators available for the user. In this dimension, we identify two types of changes: changes related to the *availability*, and changes related to the *output*. Changes in the availability of technical resources occur when devices are present or not, when new authenticators are installed/removed, or when there is a defect in a hardware or software component that impacts an authenticator's operation or availability. The second type of change refers to the variation in the output value of probabilistic authenticators operating in continuous mode. An example on the importance of monitoring technical resources for adaptation, is that if the system detects a user-owned fixed computer in the proximity of her smartphone (i.e., a new resource), authentication to the latter can be based on periodic face scans realized by the computer camera, instead of activating a password or other locking mechanism in the phone. Within the 30 surveyed papers, half of the approaches cover adaptation based on technical resources.

On the one hand, the approaches in References [2, 11, 62, 101] describe systems that sense the availability of devices and authenticators. Cerberus [2] monitors the presence of users' smart badges. If present, then automatic login to low sensitive applications is allowed, whereas the user is requested to provide additional authentication factors to access higher security applications. Similarly, in the smart health space envisioned in Reference [11], authentication is made stricter only when a contact-less user identity card is not detected in the same location as the user. Finally, both [62] and PICO [101] sense the subset of pre-registered user devices that are co-present (via RFID, Bluetooth, or WiFi connections), with the difference that the first approach builds an aggregated trust score based on them, while the second establishes the condition that k out of n tokens must be present to authenticate the user.

On the other hand, the approaches in References [35, 40, 48, 54, 63, 64, 80, 84, 113, 114, 116] present systems that sense the output of an authenticator (often continuous) as a basis for adaptation. This authenticator operates in the background, calculating the probability that the user is correct or not, which is used for hardening authentication if required. Among these solutions, Progressive Authentication [84] and CORMORANT [48] are special cases, because they sense and fuse the output of several authenticators, which can even be distributed across different devices, as the basis for decision making.

7.4 Changes Caused by the User

With regard to user-related changes, important aspects to consider are: (1) user role; (2) authentication preferences, e.g., personal interaction preferences or those related to user disabilities; and (3) changes on the user itself, e.g., when a different user takes over the system.

In the surveyed literature, user-related reasons are considered in References [2, 35, 38, 42, 80, 114, 115]. More specifically, Cerberus [2] and Reference [42], which adapt authentication inside an academic smart space, monitor changes in the roles ("student," "visitor," "faculty") to determine the required authenticators. In Reference [115], UFSA [35], and Reference [114], once the system decides the list of suitable authenticators based on the context or on the output of an implicit authenticator, the final selection is made considering user preferences. SmartAuth [80] uses a behavioral authenticator based on the deviation from the normal device fingerprint pattern. This authenticator is adapted internally by allowing the user to tune her privacy preferences, i.e., which

fingerprint features to collect at different times and locations. Last, also on the preferences-based kind of adaptation, CYOA [38] presents website users with four authentication alternatives (together with information regarding their strength and usability), allowing them to choose the most preferred one. This work is the only one completely based on user-defined preferences, which leads to a system where adaptation is "manual" instead of automatic: the user chooses her authenticator once and the selection remains fixed unless she wants to change it again.

8 HOW TO ADAPT?—THE ADAPTATION CONTROL

The *"How"* modelling dimension refers to the implementation of the adaptation logic. There are three important aspects to consider: *criteria*, *approach*, and *degree of centralization* [61]. We discuss these aspects in detail and analyze their realization in the adaptive authentication literature.

8.1 Adaptation Criteria

The adaptation logic takes as inputs the sensed data that describe adaptation reasons (i.e., context, user, and technical resources data), as well as the list of available authenticators and their features. Then, it combines this information to output a decision. Developers can implement the logic for processing the inputs and generating the output decision based on the following criteria or combinations of them: *rules/policies*, *goals*, *utility functions*, and *models*.

Rules/Policies. Is the most widely used approach in adaptive authentication. Rules or policies determine how the system should react in different situations and how to adapt. In the surveyed literature, rules are used to:

- Map authentication mechanisms to authentication security strength values.
- Map adaptation reasons to required authentication mechanisms or to required authentication strength/usability.
- Map adaptation reasons to the required modifications of authenticators' parameters.
- Introduce constraints, e.g., filtering out authentication mechanisms under specific conditions.

Rules can be defined at design time, which leads to static approaches, or learned through system operation, which requires cooperation of the users to verify if the learned rules ar correct.

Goals. Goal-based approaches aim at fulfilling specific system goals, which influence how the system should perform and might be conflicting. In the case of adaptive authentication, the observed goals are usability and security. Only two proposals within the surveyed literature are centered around goals, Reference [29] and UFSA [35]. In Reference [29], the authors develop an algorithm for selecting an optimal multifactor authentication mechanism. The selected authenticator must fulfill two goals: (1) its aggregated security level is maximized and (2) the number of factors is minimized (for better usability). The approach is formulated as an optimization problem and solved through non-linear programming [66]. UFSA [29] defines an optimization algorithm that explores all possible combinations of authentication mechanisms and chooses the set of factors that, apart from fulfilling the required security level, is perceived as more usable by the user, based on the aggregation of pre-assigned usability metrics.

Utility functions. In utility-based approaches, *utility* is a function of the system value for the user and the involved costs. The adaptation logic's goal is to maximize the overall system utility by evaluating the utility values of different strategies and selecting the one with the highest utility. In the case of adaptive authentication, utilities could be used to express, e.g., the preference value of each authenticator depending on the battery level, which is specially relevant for continuous mechanisms. The main disadvantage of utility-based adaptation is the difficulty of defining suitable utility functions, which can be a reason why none of the analyzed proposals use this approach.

Models. In model-based approaches, models are used to represent the system state and the environment. Through analysis of the models, suitable adaptation plans are worked out. In the surveyed literature, models are used to:

- Classify the global context as safe or unsafe.
- Represent and infer high-level context from combinations of multiple sensors.
- Predict the global confidence level on user authentication based on context factors and on previous outputs of authentication mechanisms.
- Describe how authenticator's strength varies with context.
- Characterize and predict the relationship between context and user authentication preferences.
- Characterize the relationship between application sensitivity and context.
- Describe system behavior.

Models can be constructed in different ways. Starting with the case of context classification as safe or unsafe, Reference [45] proposes an heuristic model that defines equations to calculate the familiarity of devices and places based on how often and recently they are observed. Then, a mapping from familiarity metrics to safety levels is defined and translated into rules, which are executed by the adaptation logic to select a suitable smartphone lock mechanism. The foundation for such a model is the assumption that familiar places are safer than unfamiliar ones, backed by previous studies on the correlation of risk perception and familiarity [12, 118]. Alternatively, Reference [72] classifies context as safe or unsafe using a machine-learning model trained with user feedback to provide ground truth. They root the model on a sociological survey examining the perceptions and concerns of users, where familiarity of places and persons are deemed relevant factors.

Models for context inference are used by References [28, 81]. Building on machine-learning techniques, both works implement a context inference model to determine the different categories of user or device position, based on measurements from gyroscope and accelerometer sensors. The inferred position data value is later used to change the template for behavioral recognition. Another related approach is Reference [115], where a context situation is modeled as a vector containing discretized values that categorize the readings obtained by the different sensors in the smartphone. Vectors are then fed as inputs to a rule-based engine that completes the adaptation process.

The model in Progressive Authentication [84] uses face and voice recognition, PIN, device placement, and device proximity data as input; then outputs the "User Authenticity Level," a metric that represents the confidence on user authentication. The final selection is based on rules that associate application sensitivity levels to user authenticity level, defaulting to explicit authentication if requirements are not met.

CASA [46] defines a probabilistic model to express the authenticator strength as a combination of the conditional probability that the user is legitimate given her location and the conditional probability that the user is illegitimate given her location. The model uses three location contexts (Home, Work, Other), identified as the most common in a user study conducted before the design, and assumes that the probability of being attacked in a particular location is proportional to the number of people who can physically come into the location (but no empirical data supports this estimation).

PRISM [82] and Reference [69] use models to learn user authentication preferences and later base the adaptation on these preferences, improving usability. Both approaches use associative classification algorithms [57] to establish the correlations and derive also confidence metrics on the significance of the mined rules for further refining the adaptation process.

Last, Treasurephone [94] and PICO [101] build the core of the adaptation logic on system behavior models. In Treasurephone [94], the relationship between privacy requirements and context

is modeled through the concept of *spheres*. A *sphere* is configured by the user as the set of applications in her smartphone that are available without authentication in a particular location context. Transitions between the spheres are triggered by location changes and the required authentication mechanisms are adapted accordingly. This sphere-centered model is grounded on the psychological concept of "faces" described by Goffman [43], which refers to the fact that privacy is highly individual and people show different faces in different contexts, i.e., reveal different information to different audiences. In the case of PICO [101], the system adaptation behavior is modeled through a state machine that describes the transitions of a device from locked to unlocked depending on contextual factors, which in this case are the nearby presence of other user owned devices. Accordingly, the device will "feel safe" and unlock itself when in the company of other known devices, but defensively lock itself up otherwise. This model is based on the "resurrecting duckling" security policy [100].

8.2 Adaptation Approach and Degree of Centralization

The literature on adaptive system distinguishes two approaches regarding the interplay of the adaptation logic and the managed resources: *internal* and *external* [36].

Internal approaches intertwine the application logic and the managed resources, which offers fast and optimized decision making. However, these approaches are individualized for a specific system, resulting in scalability and maintainability issues [61]. In turn, *external* approaches separate the adaptation logic from the managed resources, connecting them via sensors and effectors/actuators [61] to solve the drawbacks of the internal implementations: responsibilities are divided and can be maintained separately so the same logic can be used to manage various resources. Furthermore, externalizing the logic facilitates the achievement of a global view of the system, making testing easier [36]. Another aspect of the adaptation logic is the locus of control, i.e., the distribution of the MAPE-K components, which can be *centralized*, *decentralized*, or *hybrid*.

Looking at the surveyed works and analyzing them regarding the approach and degree of centralization (see Table 5), we find the following. A third of the approaches utilize an internal adaptation logic, despite the external approach is clearly superior from a maintainability and scalability point of view. Even if there are approaches offering external adaptation logics that interconnect multiple devices to adapt the required authentication mechanisms, just three of them [2, 48, 84] permit *distributed authentication*, i.e., using the authentication mechanisms available in one device/application to get access to a different device/application. Centralization of the adaptation logic is the most common strategy. Hybrid proposals perform the monitoring of context, state of technical resources, and user changes in a decentralized way. CORMORANT [48] is the only work envisioning a fully decentralized architecture, acknowledging the need for a new communication protocol to exchange adaptation information. In general, the surveyed works present a basic architecture (if any), but concentrate on the design and tests of a specific functionality, e.g., context detection and classification, or authentication selection.

9 WHEN AND WHERE TO ADAPT?—THE OPERATIONAL NUANCES

The *"When"* and *"Where"* design dimensions , as detailed in Reference [61], refer to the adaptation *time* and the different system *levels* in which changes have to be implemented, respectively. Here, we analyze how these aspects are covered in the surveyed works.

9.1 Adaptation Time

The *time* dimension refers to *When* should the system start the adaptation. In this sense, a system is *reactive* if it triggers adaptation after an event occurs and *proactive* if the adaptation logic is able to anticipate events that would trigger adaptation and prepare accordingly. In the domain of

Table 5. Overview of Adaptation Approaches in the Surveyed Works

	Work, Year	Time	Reason	Level	Tec	Adaptation Control		
						Appr	DC	DDec
Smart Space	Cerberus [2], 2003	R, P	Ctx, TR, U	App	Str	Ext	Policies	Cen
	Bardram [11], 2003	R, P	Ctx, TR	Sys	Par, Str	Int	Rules	Hyb
	[62], 2008	R, P	Ctx, TR	App	Str	Ext	Policies	Cen
	[42], 2009	R	Ctx, U	App	Str	Ext	Policies	Hyb
	UC-TBAS [109], 2011	R, P	Ctx	App	Str	Ext	Rules	Hyb
	CARS-AD [63], 2011	R, P	Ctx, TR	App	Par, Str	Ext	Rules	Hyb
Smartphone	Gupta [45], 2012	P	Ctx	Sys	Par, Str	Int	Model, Rules	Cen
	CASA [46], 2013	P	Ctx	Sys	Str	Int	Model	Cen
	ConXsense [72], 2014	P	Ctx	Sys	Str	Int	Model, Rules	Cen
	[81], 2014	P	Ctx	Sys	Par	-	Model, Rules	-
	[54], 2014	R, P	TR	Sys	Str	-	Rules	-
	[116], 2014	R, P	TR	Sys	Str	Int	Rules	Cen
	[115], 2016	-	Ctx, U	Sys	Par, Str	-	Model, Rules	-
	[28], 2017	P	Ctx	Sys	Par	-	Model, Rules	-
Websites	SmartAuth [80], 2015	P	Ctx, TR, U	App	Par, Str	Ext	Rules	Hyb
	CYOA [38], 2015	R	U	App	Str	Ext	-	Cen
	[29], 2016	R	Ctx, TR	App	Str	Ext	Goal, Rules	Cen
	Reinforced AuthN [40], 2016	R	TR	App	Str	Int	Rules	Cen
	[69], 2016	R	Ctx	App	Str	Ext	Model, Rules	Cen
	ASSO[64], 2016	R	TR	App	Str	-	-	-
Apps/Services	TreasurePhone [94], 2010	P	Ctx	App	Str	Int	Model	Cen
	Progressive AuthN [84], 2011	R, P	Ctx, TR	App	Str	Int	Model, Rules	Hyb
	[113], 2013	R, P	Ctx, TR	App, Sys	Str	Int	Rules	Cen
	UAP [9], 2014	R	Ctx	App	Str	Ext	Rules	Cen
	i/k-Contact [7], 2014	R	Ctx	App, Sys	Str	Ext	Rules	Hyb
	PRISM [82], 2015	P	Ctx	App, Sys	Str	Ext	Model, Policies	Cen
	UFSA [35], 2015	R, P	Ctx, TR, U	App	Str	Ext	Rules, Goal	Cen
Other	PICO [101], 2011	P	TR	App	Par	Int	Model	Cen
	CORMORANT [48], 2015	R, P	Ctx, TR	App, Sys	Str	Ext	-	Dec
	[114], 2017	R	Ctx, TR, U	App	Str	Ext	Rules	Hyb

Legend: **R** = Reactive; **P** = Proactive; **Ctx** = Context; **TR** = Technical resources; **U** = User(s); **App** = Application; **Sys** = System; **Tec** = Technique; **Par** = Parameter; **Str** = Structure; **Appr** = Approach; **Ext** = External; **Int** = Internal; **DC** = Decision Criteria; **DDec** = Degree of Decentralization; **Hyb** = Hybrid; **Dec** = Decentralized; **Cen** = Centralized. If a cell is marked with "-," then no further information is given.

authentication, reactiveness means that the selected authenticator is chosen when the user tries to access an application or device. In the proactive case, we have systems that automatically change the authenticator for device lock/unlock depending on the context, being ready for the time of authentication. This makes the process faster and more seamless.

Architecturally, this distinction between reactive and proactive adaptation impacts the design of algorithms for analyzing the monitored data. Reactive approaches just need to monitor user access events, at which point additional context information is acquired and analyzed *on-the-fly* to select the authenticator. In turn, proactive approaches need to continuously monitor and analyze more data for anticipated pre-selection.

In the surveyed works (see Table 5), the dominant approach is combining both proactive and reactive features. Typically, if the monitored context and technical resources are enough to have the user implicitly authenticated, then this is done proactively. Then, in the event of accessing a service that requires a higher level of authentication, the new method is selected reactively.

9.2 Adaptation Level

The adaptation logic must be aware of the relevant levels for adaptation in a specific system. In the authentication domain, applicable levels are *system* and *application*.

System-level adaptation implies that the selected authenticator gives access to the whole system, while *application-level adaptation* means that authenticator selection is performed per application. Solutions covering the application level are desirable, because they provide room for more granular adaptation strategies. That is, when adapting for a whole system, the security level of the selected authenticator must fit the highest level of sensitivity of all the applications in the system and so its usability might be worse than that of lower strength authenticators required for most applications. The counterpart of application-level adaptation is the need for configuration of adequate policies mapping sensitivity to authentication levels.

Table 5 provides an overview of the adaptation levels covered in the surveyed literature on adaptive authentication. For those works covering application-level adaptation, the logic determines the required authenticator either per application name or per application sensitivity. The latter case is more flexible, because when a new application is to be added to the system, the developer or administrator just needs to classify it with regard to the sensitivity level without the necessity of knowing all the specific authentication mechanisms and defining a one-to-one matching.

When integrating the adaptive authentication logic with different applications, a natural straightforward way to make it flexible and build on existing knowledge, would be the connection with Identity Management (IdM) protocols and standard architectures, such as the widely deployed SAML [65] and OpenID Connect [88]. These protocols provide standardized support for applications to send authentication requests with specific requirements (e.g., security level) and reuse authentication results across domains, providing single sign-on functionalities. Nevertheless, despite their suitability, just four works in the analyzed literature [2, 9, 64, 80] considered this type of integration.

10 DISCUSSION

Table 5 provides a consolidated overview of the surveyed works and their features with regard to the five dimensions in the design taxonomy of self-adaptive systems: technique, reason, adaptation control, time, and level.

In the following, apart from reflecting on the open research challenges related to each of these dimensions, we also elaborate on two additional (cross-dimensional) aspects that must be considered when designing adaptive authentication systems: *usability* and *security*. Based on our findings, a research roadmap summarizing open issues in adaptive authentication is depicted in Figure 3. We envision adaptive authentication as an emerging interdisciplinary research field that can be built from the combined efforts of four communities: security and privacy, machine learning, identity management, and adaptive systems.

10.1 Technique-related Challenges

After analyzing the adaptive authentication literature under the *"Technique"* design dimension, we observe limitations with regard to diversity and extensibility. Research to address these limitations should focus on new authenticators, and on the definition of abstractions to easily integrate and manage them within adaptive authentication systems.

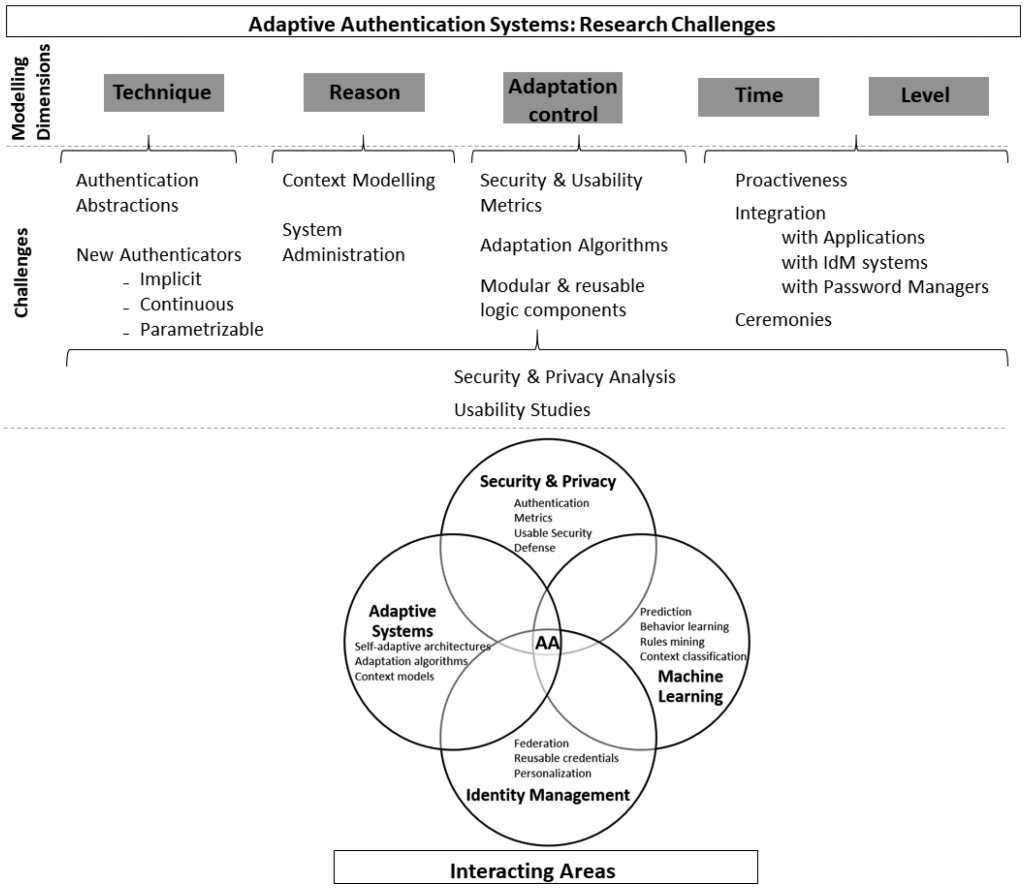

Fig. 3. Overview of challenges in the design of Adaptive Authentication (AA) systems (top); and venn diagram visualizing the interdisciplinary research areas whose interaction can tackle those challenges (bottom).

Authenticators. For adaptive authentication systems to be accepted, it is key to minimize the number of explicit interactions with the user, to improve usability. This way, security will be no longer perceived as an interfering task [93]. Therefore, research is required on new implicit authenticators that are energy efficient and privacy-aware, two dimensions currently in conflict with each other [78]. Implicit mechanisms running continuously require complex computations, maintenance and infrastructure, and so they are often outsourced to third parties. To deal with the privacy issues that arise from this situation, methods for securely outsourcing continuous implicit authentication systems are needed. Additional challenges posed by continuous authentication are related to their usage of machine learning, e.g., determining when to switch from training to deployment, when to retrain, or how to set the detection thresholds. All these decisions impact authentication performance and need to be optimized. Furthermore, as pointed out in References [21, 31], traditional FAR and FRR metrics are not adequate and further research is required to establish performance metrics to evaluate continuous authenticators.

We have also seen that parametric adaptation can provide fine-grained levels of adjustments that benefit the overall system performance. A comprehensive study of authentication parameters is required. Results will shed light on what aspects are relevant to consider when integrating a

particular mechanism in an adaptive system and most important, on how to design abstractions to model any kind of authenticator, which is a key enabler for flexibility and extensibility.

Abstractions. None of the abstractions used in the surveyed works is complete enough to deal with adaptive authentication: PAM is tied to Unix systems, and BioAPI only integrates biometric authenticators.

To the best of our knowledge, the only other standard abstraction is WebAuthN [10], recently proposed by the World Wide Web Consortium (W3C). WebAuthN defines an interface for public-key-based user authentication. Diverse authenticators, such as face or fingerprint, can be utilized to unlock user credentials, ensuring that no transaction is performed without consent. However, its operation is limited to web applications and authenticators can not be parametrized.

Consequently, research is needed on how to evolve or combine current abstractions so they are applicable independently of the operating system and type of applications for which an adaptive system is designed. Furthermore, it is required that abstractions are able to provide secure authenticator discovery, fine-grained access to parameters, and to deal with the emerging continuous authentication mechanisms, where the communication app-authenticator is not "one time" but constant. Research on abstractions will enable the creation of more diverse (any authenticator, any app, any system), flexible (parametrizable), and extensible (able to accommodate a growing number of authenticators) adaptive authentication systems.

10.2 Reason-related Challenges

The main challenges with regard to the *"Why"* dimension are context modelling and system administration.

Context modelling. There is a vast literature on context modelling for context-aware systems, covering information gathering, design tools, data structures, and comparatively evaluating them [17, 103]. However, context modelling for security applications has not been deeply studied [53]. Most of the works surveyed in this article show a limited usage of context, with vague descriptions and grounds. To improve adaptive authentication design, efforts need to be conducted to define and evaluate context models that are suitable for the field. Research should be done toward answering the question: *"How can we identify, collect, and manage relevant information that impacts the security and usability of authentication mechanisms?"* Methodologies to identify relevant contextual factors and to actually measure and evaluate the changes on security and usability are fundamental to advance the design of adaptive authentication systems. Based on this, standardized means for context representation and gathering are also required to make context available to programmers of authentication systems. Efforts like the recent Generic Sensor API [111], which provides interfaces for exposing sensor data to web applications, as well as other sensor APIs for different operating systems, contribute to fulfill this requirement, but it is still necessary to investigate how to enable their interoperability within adaptive systems that will potentially include different sensors, devices and platforms.

Another aspect of context modelling to be considered is *Quality of Context* (QoC) [22]. In adaptive authentication systems, because security decisions depend on the context, methods should be defined to guarantee that context information is provided at the right time, in the right quality, guaranteeing adequate levels of precision, probability of correctness, trustworthiness, resolution, and up-to-dateness.

System administration. Adaptive authentication systems include heterogeneous authenticators, and the removal and addition of new ones should be done easily. Similarly, administrators should be able to make changes on the supported contexts and algorithms, modifying the behavior of the system. Current systems either do not offer these capacities, or they require manual modification of complex policies, for which the administrator needs to know all the details of the

system. Therefore, new administrative interfaces are necessary that provide: information about the state of the system, assistance to configure the different components, and insights on how the system would work under each configuration. Usability studies on these interfaces are crucial to arrive to acceptable designs where the management overhead does not deter acceptance.

10.3 Adaptation Control-related Challenges

The main research challenges related to the *"How"* dimension are: comprehensive studies on adaptation algorithms, the definition of adequate metrics for adaptation, and the development of modular reusable components for the logic.

Adaptation algorithms. Current works explored mostly rule-based adaptation, and the use of other approaches is scarce. There are many alternatives for authenticator selection, such as optimization algorithms [70], utility functions [83], structured decision-making techniques coming from the field of operations research [87, 106], different machine-learning algorithms, and so on. It is crucial to research and test these alternatives to understand their advantages and shortcomings, which of them are more suitable for the adaptive authentication domain, what is their performance, and how they can be incorporated in a modular way within the architecture.

Metrics. Adaptation algorithms depend on metrics that measure the security strength and usability level of authenticators. Security strength metrics appear under different names in the surveyed works, such as *"confidence value," "credential confidence," "authentication level," "authentication strength,"* or *"trustworthiness."* These values are introduced in the system by the administrator, defined for the application scenario. It is worthy to note that very few approaches [29, 46] are explicitly based on standard authentication metrics, such as NIST's assurance levels [44] or FAR metrics. In the case of usability, metrics are less common. CYOA [38] is the only surveyed work considering authenticator quantitative usability metrics, namely *"memorability"* and *"login speed,"* which are built on previous empirical studies [26, 102].

Therefore, open challenges in this area are: analyzing the applicability of standard metrics to adaptive authentication systems, defining new security and usability metrics studying their relation with adaptation reasons, and testing the actual validity of these metrics.

Modular logic components. Together with the need for abstractions to plug heterogeneous authenticators identified in Section 10.1, it is important to design a generic architecture with reusable components for the adaptation logic. This blueprint would help in faster prototyping and deployment, contributing to break *"Authentication Silos."* Instead of authenticators that require proprietary server technology, a reference architecture for adaptive authentication will allow for flexible, and re-configurable systems, favoring market competition, and facilitating that companies break inertia to adopt new technologies [6].

Additionally, a modular reference architecture will enable collaborative research. Different system components can be subject of research by different specialized communities. For example, research on context definition, adaptation algorithms, usability, metrics, or new implicit authenticators, can be carried out in isolation and contributed to the architecture by following the defined standard interfaces and protocols, rewriting new modules accordingly. Furthermore, different instances of the reference system would be directly comparable and could be evaluated under the eyes of both usable security and adaptive systems experts.

The adaptive systems community is a good starting point not only for confronting the design of adaptive authentication, but to consult engineering tools, such as FESAS [60] or Genie [16]. These tools provide support for developing adaptive system's software and can be the foundation to define similar tools including the particularities of the authentication domain.

10.4 Operation-related Challenges

The analysis of adaptive authentication systems under the *"When"* and *"Where"* dimensions reveals open challenges with regard to proactiveness, integration and "ceremonies,"[5] which we further describe below.

Proactiveness. Proactive adaptation allows the system to select which authenticator(s) to trigger before the user needs to authenticate. When combined with automated decision making (see Section 8.1), it would lead to theoretically good solutions from a usability perspective, because the system is fast and avoids security-related interruptions in the user's workflow. However, time and battery consumption may be an issue due to the intensive monitoring and analysis and the associated frequent changes of authenticators. Ideally, the system could predict the intention of the user to authenticate and change the mechanism only in that case, but the complexity of prediction algorithms of that kind would be presumably high. Furthermore, usability studies have shown in the past that users need to feel they have some degree of control over the system to perceive it as secure [3]. Thus, important questions that need to be explored regarding the time dimension are:

- *Is it possible to efficiently predict the user's intent to access an application?*
- *Would a fully automated proactive approach be perceived as more or less usable?* or *Would the time and battery consumption be unacceptable for user adoption?*
- *Would such automatic inferences lead to the system appearing more trustworthy or the contrary?*
- *Would a reactive approach imply unacceptable delays and fatigue for the extra user interaction required in the authentication process?*
- *Could we use hybrid approaches for better trade-offs between seamlessness-performance?*

Additionally, the different response times depending on the context and available authenticators, and the varying automation levels, imply different user experiences and levels of explicit interaction. These variations, added to the integration of the adaptive authentication system with heterogeneous devices, operating systems and applications, will impact the creation of usable *"ceremonies"* [33], an open challenge discussed later.

Integration. Adaptive authentication systems, to provide value, need to be integrated with the current applications ecosystem (native, web, distributed, etc.). They should ideally provide smart authentication to any service that the user needs to access [5]. Therefore, research efforts need to be placed on integration requiring no or minimal changes in the applications.

Adaptive authentication systems to date were conceived and implemented without considering the already existing IdM infrastructures and protocols, such as SAML [65] or OpenID Connect [88]. It is an open challenge to integrate intelligent authentication selection within IdM, leveraging current deployments and fostering easier adoption. This integration will be beneficial to allow additional adaptive features, such as dynamically changing between different user accounts or identities, depending on the context.

Furthermore, since adaptive authentication systems will still have to manage passwords, it would be interesting to explore their integration with recent APIs [112] that enable to programatically access user passwords stored in password managers to ease the sign-in process.

Ceremonies. In the domain of authentication and IdM, it is important that ceremonies are well defined, so they become predictable and unambiguous enough to allow for informed decisions: the user knows exactly what to expect, so errors and confusion that might lead to security problems

[5]The concept of a *"ceremony"* [33] is an extension of the concept of a network protocol, but with human nodes alongside computer nodes. In these ceremonies, the communication links include user interface(s), human-to-human communication, and transfers of physical objects that carry data.

are reduced [23]. Predictability in the exchange of authentication data enables a consistent user experience, favoring reliability. However, this predictability conflicts with the dynamic nature of adaptive systems; so the question is: *How can we design secure ceremonies for adaptive authentication systems?*

10.5 Cross-dimensional Challenges

10.5.1 Usability. Usability is a key aspect of secure system design, as it can reduce friction and favor acceptance. However, despite its importance, few works on adaptive authentication include usability studies [11, 29, 38, 46, 72, 80, 82, 84, 94, 101, 114], and they are generally limited to testing if there is some improvement with respect to using passwords. More specifically, the conducted studies were focused on:

- Proving that users understand the benefits of adaptive authentication.
- Testing if adaptive authentication systems are perceived positively.
- Measuring performance in two dimensions: reduction in the number of times the user is required to type a password, and authentication delay.

Results showed that, in average, adaptive authentication systems are easy to understand, and perceived as useful despite the additional required configuration. Users of the studied systems show willingness to adopt them, though the type of authenticators in the system might have negative effects. For example, the idea of carrying multiple tokens was proved to increase perceived personal responsibility for secure authentication, making the risks and inconvenience associated with loss and theft salient for participants [101].

Regarding performance, despite many works include metrics for single architectural components (e.g., classification accuracy of a behavioral authenticator), just four papers provide quantitative measurements of overall performance. Here, we discuss these general metrics instead of covering single-component performance metrics, as the latter do not establish a common ground for comparing the surveyed works. Accordingly, PRISM [82] and Progressive Authentication [84] report average authentication delays below 200ms,[6] while the prototype in Reference [114] reports an average delay of 20s, which users pointed out as an aspect to improve. As for the overhead, both Progressive Authentication [84] and CASA [46] measure similar reductions in password overhead (42% and 47% less password requests, respectively). However, the number of participants in the studies is generally too small to extract meaningful results. The concrete numbers range from 4 to 100 participants, with almost half of the studies being performed with less than 20 users.[7]

Additionally, some works performed pre-studies to justify if an adaptive system would fit users' interests and how [11, 84], and to support the selection of relevant contextual factors [46, 72, 94].

Our research shows a fundamental problem: current poor designs of adaptive authentication systems cannot foster easy deployment, fast integration of diverse components, and flexible reconfiguration. For this reason, the number and scope of usability studies is so far limited. No comparative studies of different configurations exist, e.g., varying the number and type of authenticators, or changing the selection techniques. This kind of research is necessary to improve design and understand acceptance. Therefore, solving the design problems should be a priority, since it will provide the foundation to further investigate usability and security issues.

[6]It is generally accepted that response times below 1 second make users satisfactorily experience interaction as a continuous flow [74].

[7]Though it was long believed that 5 participants were enough to test usability [110], more recent studies suggest numbers bigger than 10 to achieve better results [51]. Twenty participants is the average sample size used in security usability studies [86].

10.5.2 Security. The realization of authentication systems that react to environmental changes opens new vulnerabilities and avenues for attack. Half of the surveyed works [11, 28, 38, 40, 42, 45, 48, 54, 72, 80, 82, 101, 109, 116] mentioned potential security threats. The identified issues are:

- Context manipulation, to make the system believe that the situation is secure so it can be more easily attacked.
- Device theft and secure pairing when using tokens as authenticators.
- Mimicry attacks [41, 56], which can be used to impersonate a legitimate user by imitating her observed behavior.
- Privacy of data used for behavioral authentication, specially if these data are not locally stored or if computations are outsourced to a third party.
- Privacy of contextual data, which can reveal very sensitive information about the user, such as location or activity.
- Metric reliability, which is crucial, because selection algorithms choose authentication mechanisms based on these metrics.
- Attacks directed to system components that are based on machine-learning techniques [13, 14, 50], for instance, to force the miss-classification of an illegitimate user as authentic.

The above aspects are worthy of further investigation, not only from a theoretical point of view but also experimentally. Existing advanced cryptographic techniques, such as homomorphic encryption [37] or multi-party computation [27], need to be also analyzed in the context of adaptive systems to understand their applicability to efficiently protect sensitive biometrics. Another related issue, which derives from the need to comply with privacy regulations like the *General Data Protection Regulation* [77], is the incorporation of user consent for the authentication-related transactions without decreasing the overall usability.

Finally, a key challenge that remains unsolved is the comprehensive analysis of the attack surface of adaptive authentication systems and its implications, considering diversity, i.e., varying number of authenticators, contexts, and selection algorithms. However, as it occurs with usability research, it is first required to solve the problem of designing flexible, easy-to-deploy adaptive authentication systems to subsequently address security challenges.

11 CONCLUDING REMARKS

We deserve better authentication mechanisms [92] to move on from the current password-dominated scene. However, since there is *no one-size-fits-all* in security, no new mechanism is going to replace all the others and be accepted as the universal solution. Adaptive authentication systems that dynamically select the best (most usable, most secure) authenticator depending on the situation are a viable path to take the most of authentication heterogeneity. We observed that adaptive authentication systems to date have not been designed using methodological approaches, which might be one of the reasons hindering their progress. Here, we have analyzed the literature on adaptive authentication under the design principles well-known in the adaptive systems discipline, to identify the main open challenges. We expect this work can serve as a starting point to better understand adaptive authentication and to foster research advance on the topic.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (Dec. 1999), 40–46.

[2] Jalal Al-Muhtadi, Anand Ranganathan, Roy Campbell, and M. Dennis Mickunas. 2003. Cerberus: A context-aware security scheme for smart spaces. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom'03).* 489–496.

[3] Nora Alkaldi and Karen Renaud. 2016. Why do people adopt, or reject, smartphone password managers? In *Proceedings of the IEEE European Symposium on Security and Privacy (EuroUSEC'16).*

[4] Abdulaziz Alzubaidi and Jugal Kalita. 2016. Authentication of smartphone users using behavioral biometrics. *IEEE Commun. Sur. Tut.* 18, 3 (2016), 1998–2026.

[5] Patricia Arias-Cabarcos, Florina Almenarez, Ruben Trapero, Daniel Diaz-Sanchez, and Andres Marin. 2015. Blended identity: Pervasive IdM for continuous authentication. *IEEE Secur. Privacy* 13, 3 (2015), 32–39.

[6] Patricia Arias-Cabarcos and Christian Krupitzer. 2017. On the design of distributed adaptive authentication systems. In *Proceedings of the WAY Symposium on Usable Privacy and Security (SOUPS'17)*.

[7] Shiori Arimura, Masahiro Fujita, Shinya Kobayashi, Junya Kani, Masakatsu Nishigaki, and Akira Shiba. 2014. i/k-Contact: A context-aware user authentication using physical social trust. In *Proceedings of the 12th IEEE Annual Conference on Privacy, Security, and Trust (PST'14)*. 407–413.

[8] Khairul Azmi Abu Bakar and Galoh Rashidah Haron. 2013. Adaptive authentication: Issues and challenges. In *Proceedings of the World Congress on Computer and Information Technology (WCCIT'13)*. IEEE, 1–6.

[9] Khairul Azmi Abu Bakar and Galoh Rashidah Haron. 2014. Adaptive authentication based on analysis of user behavior. In *Proceedings of the IEEE Science and Information Conference (SAI'14)*. 601–606.

[10] Dirk Balfanz, Alexei Czeskis, Jeff Hodges, J. C. Jones, Michael B. Jones, Akshay Kumar, Angelo Liao, Rolf Lindemann, and Emil Lundberg. 2018. Web Authentication: An API for accessing Public Key Credentials Level 1. W3C Candidate Recommendation.

[11] Jakob E. Bardram, Rasmus E. Kjær, and Michael Ø. Pedersen. 2003. Context-aware user authentication–supporting proximity-based login in pervasive computing. In *Proceedings of the International Conference on Ubiquitous Computing*. 107–123.

[12] Abigail Barr. 1999. Familiarity and trust: An experimental investigation. *The Centre for the Study of African Economies Working Paper Series*. 107.

[13] Marco Barreno, Blaine Nelson, Anthony D. Joseph, and J. Doug Tygar. 2010. The security of machine learning. *Mach. Learn.* 81, 2 (2010), 121–148.

[14] Marco Barreno, Blaine Nelson, Russell Sears, Anthony D. Joseph, and J. Doug Tygar. 2006. Can machine learning be secure? In *Proceedings of the ACM Symposium on Information, Computer, and Communications Security*. ACM, 16–25.

[15] Sagar Behere and Martin Törngren. 2016. A functional reference architecture for autonomous driving. *Info. Software Technol.* 73 (2016), 136–150.

[16] Nelly Bencomo, Paul Grace, Carlos Flores, Danny Hughes, and Gordon Blair. 2008. Genie: Supporting the model driven development of reflective, component-based adaptive systems. In *Proceedings of the ACM International Conference on Software Engineering (ICSE'08)*. 811–814.

[17] Claudio Bettini, Oliver Brdiczka, Karen Henricksen, Jadwiga Indulska, Daniela Nicklas, Anand Ranganathan, and Daniele Riboni. 2010. A survey of context modelling and reasoning techniques. *Pervas. Mobile Comput.* 6, 2 (2010), 161–180.

[18] Technical Committee: ISO/IEC JTC 1/SC 37 Biometrics. 2018. ISO/IEC 19784-1:2018 Information technology—Biometric application programming interface—Part 1: BioAPI specification. Retrieved from https://www.iso.org/standard/70866.html.

[19] Joseph Bonneau, Cormac Herley, Paul C. Van Oorschot, and Frank Stajano. 2012. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Proceedings of the IEEE Symposium on Security and Privacy*. 553–567.

[20] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2015. Passwords and the evolution of imperfect authentication. *Commun. ACM* 58, 7 (June 2015), 78–87.

[21] Patrick Bours and Soumik Mondal. 2015. Performance evaluation of continuous authentication systems. *IET Biometrics* 4, 4 (2015), 220–226.

[22] Thomas Buchholz and Michael Schiffers. 2003. Quality of context: What it is and why we need it. In *Proceedings of the 10th Workshop of the OpenView University Association (OVUA'03)*.

[23] Kim Cameron. 2005. The laws of identity. *Microsoft Corp.*

[24] Betty H. C. Cheng, Rogerio De Lemos, Holger Giese, Paola Inverardi, Jeff Magee, Jesper Andersson, Basil Becker, Nelly Bencomo, Yuriy Brun, Bojan Cukic et al. 2009. Software engineering for self-adaptive systems: A research roadmap. In *Software Engineering for Self-adaptive Systems*. Springer, 1–26.

[25] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C. Van Oorschot. 2012. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Trans. Depend. Secure Comput.* 9, 2 (2012), 222–235.

[26] Sonia Chiasson, Elizabeth Stobert, Alain Forget, Robert Biddle, and Paul C. Van Oorschot. 2012. Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Trans. Depend. Secure Comput.* 9, 2 (2012), 222–235.

[27] Ronald Cramer, Ivan Bjerre Damgård, et al. 2015. *Secure Multiparty Computation*. Cambridge University Press.

[28] Heather Crawford and Ebad Ahmadzadeh. 2017. Authentication on the go: Assessing the effect of movement on mobile device keystroke dynamics. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS'17)*. 163–173.

[29] Dipankar Dasgupta, Arunava Roy, and Abhijit Nag. 2016. Toward the design of adaptive selection strategies for multi-factor authentication. *Comput. Secur.* 63 (2016), 85–116.

[30] Rogério De Lemos, Holger Giese, Hausi A Müller, Mary Shaw, Jesper Andersson, Marin Litoiu, Bradley Schmerl, Gabriel Tamura, Norha M Villegas, Thomas Vogel et al. 2013. Software engineering for self-adaptive systems: A second research roadmap. In *Software Engineering for Self-Adaptive Systems II*. Springer, 1–32.

[31] Simon Eberz, Kasper B. Rasmussen, Vincent Lenders, and Ivan Martinovic. 2017. Evaluating behavioral biometrics for continuous authentication: Challenges and metrics. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS'17)*. 386–399.

[32] Ahmed Elkhodary and Jon Whittle. 2007. A survey of approaches to adaptive application security. In *Proceedings of the International Workshop on Software Engineering for Adaptive and Self-Managing Systems (SEAMS'07)*. IEEE, 16–16.

[33] Carl M. Ellison. 2007. Ceremony design and analysis. *IACR Cryptol. ePrint Arch.* (2007), 399. Retrieved from https://pdfs.semanticscholar.org/8b6a/22b53e9ab50d29c804311e9151f09a8e7243.pdf.

[34] Antti Evesti and Eila Ovaska. 2013. Comparison of adaptive information security approaches. *ISRN Artific. Intell.* 2013, Article 482949 (2013), 18 pages. https://doi.org/10.1155/2013/482949

[35] Reza Fathi, Mohsen Amini Salehi, and Ernst L. Leiss. 2015. User-friendly and secure architecture (UFSA) for authentication of cloud services. In *Proceedings of the IEEE International Conference on Cloud Computing (CLOUD'15)*. 516–523.

[36] Jacqueline Floch, Svein Hallsteinsen, Erlend Stav, Frank Eliassen, Ketil Lund, and Eli Gjorven. 2006. Using architecture models for runtime adaptability. *IEEE Software* 23, 2 (2006), 62–70.

[37] Caroline Fontaine and Fabien Galand. 2007. A survey of homomorphic encryption for nonspecialists. *EURASIP J. Info. Secur.* 2007, 1 (2007), 15.

[38] Alain Forget, Sonia Chiasson, and Robert Biddle. 2015. Choose your own authentication. In *Proceedings of the New Security Paradigms Workshop*. 1–15.

[39] Alain Forget, Sonia Chiasson, Paul C. van Oorschot, and Robert Biddle. 2008. Improving text passwords through persuasion. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS'08)*. 1–12.

[40] David Freeman, Sakshi Jain, Markus Dürmuth, Battista Biggio, and Giorgio Giacinto. 2016. Who are you? A statistical approach to measuring user authenticity. In *Proceedings of the Network and Distributed System Security Symposium (NDSS'16)*. 1–15.

[41] Davrondzhon Gafurov, Einar Snekkenes, and Patrick Bours. 2007. Spoof attacks on gait authentication system. *IEEE T. Inf. Foren. Sec.* 2, 3 (2007), 491–502.

[42] Diwakar Goel, Eisha Kher, Shriya Joag, Veda Mujumdar, Martin Griss, and Anind K. Dey. 2009. Context-aware authentication framework. In *Proceedings of the International Conference on Mobile Computing, Applications, and Services (MobiCASE'09)*. 26–41.

[43] Erving Goffman. 1959. *The Presentation of Self in Everyday Life*. Doubleday Anchor Books, Doubleday, Garden City.

[44] P. A. Grassi, M. E. Garcia, and J. L. Fenton. 2017. NIST special publication 800–63-3: Digital identity guidelines. Retrieved from https://pages.nist.gov/800-63-3/.

[45] Aditi Gupta, Markus Miettinen, N. Asokan, and Marcin Nagy. 2012. Intuitive security policy configuration in mobile devices using context profiling. In *Proceedings of the International Conference on Privacy, Security, Risk and Trust (PASSAT'12) and the International Confernece on Social Computing (SocialCom'12)*. IEEE, 471–480.

[46] Eiji Hayashi, Sauvik Das, Shahriyar Amini, Jason Hong, and Ian Oakley. 2013. CASA: Context-aware scalable authentication. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS'13)*. 3:1–3:10.

[47] Marti A. Hearst, Susan T Dumais, Edgar Osuna, John Platt, and Bernhard Scholkopf. 1998. Support vector machines. *IEEE Intell. Syst. Appl.* 13, 4 (1998), 18–28.

[48] Daniel Hintze, Rainhard D. Findling, Muhammad Muaaz, Eckhard Koch, and René Mayrhofer. 2015. Cormorant: Towards continuous risk-aware multi-modal cross-device authentication. In *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing and ACM International Symposium on Wearable Computers*. 169–172.

[49] David W. Hosmer Jr., Stanley Lemeshow, and Rodney X. Sturdivant. 2013. *Applied Logistic Regression*, Vol. 398. John Wiley & Sons.

[50] Ling Huang, Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, and J. D. Tygar. 2011. Adversarial machine learning. In *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*. ACM, 43–58.

[51] Wonil Hwang and Gavriel Salvendy. 2010. Number of people required for usability evaluation: The 10±2 rule. *Commun. ACM* 53, 5 (2010), 130–133.

[52] Didac Gil De La Iglesia and Danny Weyns. 2015. MAPE-K formal templates to rigorously design behaviors for self-adaptive systems. *ACM Trans. Auton. Adapt. Syst.* 10, 3 (2015), 15.
[53] Gleneesha M. Johnson. 2009. Towards shrink-wrapped security: A taxonomy of security-relevant context. In *Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PERCOM'09)*. 1–2.
[54] Hilmi Gunes Kayacik, Mike Just, Lynne Baillie, David Aspinall, and Nicholas Micallef. 2014. Data driven authentication: On the effectiveness of user behaviour modelling with mobile device sensors. *arXiv preprint arXiv:1410.7743*.
[55] Jeffrey O. Kephart and David M. Chess. 2003. The vision of autonomic computing. *IEEE Comput.* 36, 1 (2003), 41–50.
[56] Hassan Khan, Urs Hengartner, and Daniel Vogel. 2016. Targeted mimicry attacks on touch input-based implicit authentication schemes. In *Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services (MobySys'16)*. 387–398.
[57] Arun Kishore Ramakrishnan, Davy Preuveneers, and Yolande Berbers. 2014. Enabling self-learning in dynamic and open IoT environments. *Comput. Sci.* 32 (2014), 207–214.
[58] Barbara Kitchenham. 2004. *Procedures for Performing Systematic Reviews*. Technical Report TR/SE-0401. Keele University, Keele, UK.
[59] Jeff Kramer and Jeff Magee. 2007. Self-managed systems: An architectural challenge. In *Future of Software Engineering*. IEEE Computer Society, 259–268.
[60] Christian Krupitzer, Felix Maximilian Roth, Christian Becker, Markus Weckesser, Malte Lochau, and Andy Schürr. 2016. FESAS IDE: An integrated development environment for autonomic computing. In *Proceedings of the IEEE International Conference on Autonomic Computing (ICAC'16)*. 15–24.
[61] Christian Krupitzer, Felix Maximilian Roth, Sebastian VanSyckel, Gregor Schiele, and Christian Becker. 2015. A survey on engineering approaches for self-adaptive systems. *Pervas. Mobile Comput.* 17 (2015), 184–206.
[62] Gabriele Lenzini, Mortaza S. Bargh, and Bob Hulsebosch. 2008. Trust-enhanced security in location-based adaptive authentication. *Electron. Notes Theoret. Comput. Sci.* 197, 2 (2008), 105–119.
[63] João Carlos D. Lima, Cristiano C. Rocha, Matheus A. Vieira, Iara Augustin, and Mario A. R. Dantas. 2011. CARS-AD: A context-aware recommender system to decide about implicit or explicit authentication in ubihealth. In *Proceedings of the 9th ACM International Symposium on Mobility Management and Wireless Access (MobiWac'11)*. ACM, New York, NY, 83–92. DOI: https://doi.org/10.1145/2069131.2069146
[64] Zhan Liu, Riccardo Bonazzi, and Yves Pigneur. 2016. Privacy-based adaptive context-aware authentication system for personal mobile devices. *J. Mob. Multimed.* 12, 1–2 (Apr. 2016), 159–180. Retrieved from http://dl.acm.org/citation.cfm?id=3177177.3177187.
[65] Hal Lockhart and B. Campbell. 2008. Security assertion markup language (SAML) V2. 0 technical overview. *OASIS Committee Draft* 2 (2008), 94–106.
[66] David G. Luenberger, Yinyu Ye et al. 1984. *Linear and Nonlinear Programming*, Vol. 2. Springer.
[67] Frank D. Macías-Escrivá, Rodolfo Haber, Raul Del Toro, and Vicente Hernandez. 2013. Self-adaptive systems: A survey of current approaches, research challenges and applications. *Expert Syst. Appl.* 40, 18 (2013), 7267–7279.
[68] Eve Maler and Drummond Reed. 2008. The venn of identity: Options and issues in federated identity management. *IEEE Secur. Priv.* 6, 2 (2008), 16–23.
[69] Abdeljebar Mansour, Mohamed Sadik, Essaïd Sabir, and Mohamed Azmi. 2016. A context-aware multimodal biometric authentication for cloud-empowered systems. In *Proceedings of the IEEE International Conference on Wireless Networks and Mobile Communications (WINCOM'16)*. 278–285.
[70] R. Timothy Marler and Jasbir S. Arora. 2004. Survey of multi-objective optimization methods for engineering. *Struct. Multidisc. Optimiz.* 26, 6 (2004), 369–395.
[71] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou. 2015. Surveying the development of biometric user authentication on mobile phones. *IEEE Commun. Surv. Tut.* 17, 3 (2015), 1268–1293.
[72] Markus Miettinen, Stephan Heuser, Wiebke Kronz, Ahmad-Reza Sadeghi, and N. Asokan. 2014. ConXsense: Automated context classification for context-aware access control. In *Proceedings of the ACM ASIA Conference on Computer and Communications Security (ASIACCS'14)*. 293–304.
[73] Robert Morris and Ken Thompson. 1979. Password security: A case history. *Commun. ACM* 22, 11 (1979), 594–597.
[74] Jakob Nielsen. 1994. *Usability Engineering*. Elsevier.
[75] Lawrence O'Gorman. 2003. Comparing passwords, tokens, and biometrics for user authentication. *P. IEEE* 91, 12 (2003), 2021–2040.
[76] P. Oreizy, M. M. Gorlick, R. N. Taylor, D. Heimhigner, G. Johnson, N. Medvidovic, A. Quilici, D. S. Rosenblum, and A. L. Wolf. 1999. An architecture-based approach to self-adaptive software. *IEEE Intell. Syst. App.* 14, 3 (1999), 54–62.
[77] EU Parliament and the Council of the EU. 2016. General Data Protection Regulation. Retrieved from http://eur-lex.europa.eu/legal-content/EN/TXT/.
[78] Vishal M. Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello. 2016. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal. Proc. Mag.* 33, 4 (2016), 49–61.

[79] Bernhard Pfahringer, Geoffrey Holmes, and Richard Kirkby. 2007. New options for hoeffding trees. In *Proceedings of the Australasian Joint Conference on Artificial Intelligence*. 90–99.
[80] Davy Preuveneers and Wouter Joosen. 2015. SmartAuth: Dynamic context fingerprinting for continuous user authentication. In *Proceedings of the ACM Special Interest Group on Applied Computing (SIGAPP'15)*. 2185–2191.
[81] Abena Primo, Vir V. Phoha, Rajesh Kumar, and Abdul Serwadda. 2014. Context-aware active authentication using smartphone accelerometer measurements. In *Proceedings of the IEEE Conference Computer Vision and Pattern Recognition Workshops*. 98–105.
[82] Arun Ramakrishnan, Jochen Tombal, Davy Preuveneers, and Yolande Berbers. 2015. PRISM: Policy-driven risk-based implicit locking for improving the security of mobile end-user devices. In *Proceedings of the ACM International Conference on Advances in Mobile Computing & Multimedia (MoMM'15)*. 365–374.
[83] Peter Reichert, Nele Schuwirth, and Simone Langhans. 2013. Constructing, evaluating and visualizing value and utility functions for decision support. *Environ. Model. Software* 46 (2013), 283–291.
[84] 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.
[85] Arun Ross and Anil K. Jain. 2004. Multimodal biometrics: An overview. In *Proceedings of the 12th IEEE European Signal Processing Conference*. 1221–1224.
[86] Scott Ruoti, Brent Roberts, and Kent Seamons. 2015. Authentication melee: A usability analysis of seven web authentication systems. In *Proceedings of the 24th International Conference on World Wide Web*. International World Wide Web Conferences Steering Committee, 916–926.
[87] Thomas L. Saaty. 1990. How to make a decision: The analytic hierarchy process. *Eur. J. Operation. Res.* 48, 1 (1990), 9–26.
[88] Nat Sakimura, John Bradley, Mike Jones, Breno de Medeiros, and Chuck Mortimore. 2014. OpenID connect core 1.0 incorporating errata set 1. *OpenID Found., Specific.* (2014). Retrieved from https://openid.net/specs/openid-connect-core-1_0.html.
[89] Mazeiar Salehie and Ladan Tahvildari. 2009. Self-adaptive software: Landscape and research challenges. *ACM Trans. Auton. Adapt. Syst.* 4, 2 (2009), 14:1–14:42.
[90] Gerard Salton, Anita Wong, and Chung-Shu Yang. 1975. A vector space model for automatic indexing. *Commun. ACM* 18, 11 (1975), 613–620.
[91] Vipin Samar. 1996. Unified login with pluggable authentication modules (PAM). In *Proceedings of the ACM Conference on Computer and Communications Security (CCS'96)*. 1–10.
[92] M. Angela Sasse. 2013. Technology should be smarter than this!: A vision for overcoming the great authentication fatigue. In *Proceedings of the Workshop on Secure Data Management*. 33–36.
[93] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. 2001. Transforming the "weakest link" human/computer interaction approach to usable and effective security. *BT Technol. J.* 19, 3 (2001), 122–131.
[94] Julian Seifert, Alexander De Luca, Bettina Conradi, and Heinrich Hussmann. 2010. Treasurephone: Context-sensitive user data protection on mobile phones. In *Proceedings of the International Conference on Pervasive Computing*. 130–137.
[95] Simon J. Sheather and Michael C. Jones. 1991. A reliable data-based bandwidth selection method for kernel density estimation. *J. Roy. Stat. Soc. Ser. B (Methodological)* (1991), 683–690.
[96] Elaine Shi, Yuan Niu, Markus Jakobsson, and Richard Chow. 2010. Implicit authentication through learning user behavior. In *Proceedings of the International Conference on Information Security*. Springer, 99–113.
[97] David Silver, Suman Jana, Dan Boneh, Eric Yawei Chen, and Collin Jackson. 2014. Password managers: Attacks and defenses. In *Proceedings of the USENIX Security Symposium*. 449–464.
[98] Bogdan Solomon, Dan Ionescu, Marin Litoiu, and Gabriel Iszlai. 2010. Autonomic computing control of composed web services. In *Proceedings of the ICSE Workshop on Software Engineering for Adaptive and Self-Managing Systems*. ACM, 94–103.
[99] Sampath Srinivas, John Kemp, and FIDO Alliance. 2013. FIDO UAF architectural overview. Retrieved from https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-overview-v1.0-ps-20141208.html.
[100] Frank Stajano. 1999. The resurrecting duckling. In *Proceedings of the International Workshop Security Protocols*. 183–194.
[101] Frank Stajano. 2011. Pico: No more passwords!. In *Proceedings of the International Workshop on Security Protocols*. 49–81.
[102] Elizabeth Stobert and Robert Biddle. 2013. Memory retrieval and graphical passwords. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS'13)*. 15:1–15:14.
[103] Thomas Strang and Claudia Linnhoff-Popien. 2004. A context modeling survey. In *Proceedings of the Workshop Advanced Context Modelling, Reasoning and Management (UbiComp'04)*, Vol. 4. 34–41.

[104] Julie Thorpe, Paul C. van Oorschot, and Anil Somayaji. 2005. Pass-thoughts: Authenticating with our minds. In *Proceedings of the Workshop New Security Paradigms*. ACM, 45–56.
[105] C. Toader and Frank Stajano. 2014. User authentication for Pico: When to unlock a security token. *Master's Thesis, University of Cambridge*.
[106] Evangelos Triantaphyllou. 2000. Multi-criteria decision making methods. In *Multi-criteria Decision Making Methods: A Comparative Study*. Springer, 5–21.
[107] Giannis Tziakouris, Rami Bahsoon, and Muhammad Ali Babar. 2018. A survey on self-adaptive security for large-scale open environments. *ACM Comput. Surveys* 51, 5 (2018).
[108] Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib et al. 2017. Design and evaluation of a data-driven password meter. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'17)*. 3775–3786.
[109] Pallapa Venkataram and B. Sathish Babu. 2008. An authentication scheme for ubiquitous commerce: A cognitive agents-based approach. In *Proceedings of the IEEE Network Operations and Management Symposium (NOMS'08)*. 248–256.
[110] Robert A. Virzi. 1992. Refining the test phase of usability evaluation: How many subjects is enough? *Hum. Fact.* 34, 4 (1992), 457–468.
[111] Rick Waldron, Mikhail Pozdnyakov, and Alexander Shalamov. 2018. Generic Sensor API, W3C Candidate Recommendation.
[112] Mike West. 2017. Credential Management Level 1. W3C Working Draft.
[113] Heiko Witte, Christian Rathgeb, and Christoph Busch. 2013. Context-aware mobile biometric authentication based on support vector machines. In *Proceedings of the 4th IEEE International Conference on Emerging Security Technologies (EST'13)*. 29–32.
[114] Adam Wójtowicz and Jacek Chmielewski. 2017. Technical feasibility of context-aware passive payment authorization for physical points of sale. *Person. Ubiq. Comput.* 21, 6 (2017), 1113–1125.
[115] Adam Wójtowicz and Krzysztof Joachimiak. 2016. Model for adaptable context-based biometric authentication for mobile devices. *Person. Ubiq. Comput.* 20, 2 (2016), 195–207.
[116] Jeffrey Xiong, John Xiong, and Christophe Claramunt. 2014. A spatial entropy-based approach to improve mobile risk-based authentication. In *Proceedings of the 1st ACM SIGSPATIAL International Workshop on Privacy in Geographic Information Collection and Analysis*. 3.
[117] Eric Yuan, Naeem Esfahani, and Sam Malek. 2014. A systematic survey of self-protecting software systems. *ACM Trans. Auton. Adapt. Syst.* 8, 4 (2014).
[118] Jie Zhang, Ali A. Ghorbani et al. 2004. Familiarity and trust: Measuring familiarity with a web site. In *Proceedings of the International Conference on Privacy, Security, and Trust (PST'04)*. 23–28.

Received December 2018; revised May 2019; accepted May 2019