

A Context-Driven Modelling Framework for Dynamic Authentication Decisions

Anne Bumiller, Olivier Barais, Stéphanie Challita, Benoit Combemale, Nicolas Aillery, Gael Le Lan

▶ **To cite this version:**

Anne Bumiller, Olivier Barais, Stéphanie Challita, Benoit Combemale, Nicolas Aillery, et al.. A Context-Driven Modelling Framework for Dynamic Authentication Decisions. SEAA 2022 - Euromicro Conference Series on Software Engineering and Advanced Applications, Aug 2022, Maspalomas, Spain. pp.1-8. hal-03729080

HAL Id: hal-03729080
https://inria.hal.science/hal-03729080

Submitted on 20 Jul 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Context-Driven Modelling Framework for Dynamic Authentication Decisions

Anne Bumiller
University of Rennes 1/INRIA/IRISA
Rennes, France
Email: anne.bumiller@inria.fr

Olivier Barais
University of Rennes 1/INRIA/IRISA
Rennes, France
Email: olivier.barais@inria.fr

Stéphanie Challita
University of Rennes 1/INRIA/IRISA
Rennes, France
Email: stephanie.challita@inria.fr

Benoit Combemale
University of Rennes 1/INRIA/IRISA
Rennes, France
Email: benoit.combemale@inria.fr

Nicolas Aillery
Orange Labs
Rennes, France
Email: nicolas.aillery@orange.com

Gael Le Lan
Orange Labs
Rennes, France
Email: gael.lelan@orange.com

***Abstract*—Nowadays, many mechanisms exist to perform authentication, such as text passwords and biometrics. However, reasoning about their relevance (*e.g.,* the appropriateness for security and usability) regarding the contextual situation is challenging for authentication system designers. In this paper, we present a Context-driven Modelling Framework for dynamic Authentication decisions (COFRA), where the context information specifies the relevance of authentication mechanisms. COFRA is based on a precise metamodel that reveals framework abstractions and a set of constraints that specify their meaning. Therefore, it provides a language to determine the relevant authentication mechanisms (characterized by properties that ensure their appropriateness) in a given context. The framework supports the adaptive authentication system designers in the complex trade-off analysis between context information, risks and authentication mechanisms, according to usability, deployability, security, and privacy. We validate the proposed framework through case studies and extensive exchanges with authentication and modelling experts. We show that model instances describing real-world use cases and authentication approaches proposed in the literature can be instantiated validly according to our metamodel. This validation highlights the necessity, sufficiency, and soundness of our framework.**

***Index Terms*—Authentication, Meta-Modelling, Context-Awareness**

I. INTRODUCTION

Authentication technique weaknesses, like password-based authentication, are known [27], and service operators often implement additional authentication mechanisms to limit the restraints of the individual techniques [18], [25]. Contextually available features are used to calculate an impersonation risk score during password entry. Such risk scores are typically classified into three categories: low, medium, and high [8], [11], [13], [14], [17]. Additional authentication mechanisms are usually required if a high-risk is detected [27]. So-called risk-based authentication approaches, aiming to strengthen security while maintaining usability by monitoring how risky a login attempt is, have the potential to provide secure authentication with good usability [6], [11]. Hence, taking into account the context[1] for authentication is not a new concept. However, until now, it is primarily used to continuously calculate risk scores, which estimate the probability of impersonation [11], [22]. Nonetheless, the question of which authentication mechanisms are relevant (*e.g.,* appropriate for security and usability) in the given context is often disregarded. The relevance of an authentication mechanism can not simply be measured by a one-dimensional score because there are different types of risks behind the risk of impersonation. Also, for usability, there is no one-fit-all solution. For example, the authentication mechanism "face recognition" is not usable in the dark, and the authentication mechanism "voice recognition" is not usable in a noisy environment. According to [2], "adaptive authentication allows a system to dynamically select the relevant mechanism(s) to authenticate a user depending on contextual factors, such as location, proximity to devices, and other attributes." If the selection is based only on a continuous risk score, then the selected authentication mechanism(s) may not be relevant in the context. The probability of impersonation expressed in the score can contain various risks (*e.g.*, password theft, device theft), for which different countermeasures need to be provided. In addition, the selected authentication mechanism(s) may not be usable in a specific context. Hence, considering only the security aspect is not enough to reason about the relevance of an authentication mechanism. Also, an authentication mechanism is not relevant when it is not deployable in a context (*e.g.,* high implementation costs, not browser compatible, the user has not registered the biometric data) or when it requests information that is too private. Scores are insufficient to select the best authentication mechanisms concerning two main points. First, the fusion of the contextually available features in a one-dimensional risk score reduces the comprehensibility and explainability of risks (1). Second, context information not only influences the risk of an unexpected or suspicious login attempt but also concerns other properties of authentication mechanisms (*e.g.*, usability) (2).

To tackle these restrictions and to support authentication system designers, this paper proposes a Context-driven Modelling Framework for dynamic Authentication decisions (COFRA). This framework is not based on calculating a risk score but on a complex and fine-grained mapping of context information to

[1]Defined as information that can be used to characterise an authentication attempt (*e.g.,* IP address, device, browser).

authentication mechanisms. The main objective is to abstract domain knowledge about context modelling for adaptive authentication systems gathered from the literature and experience in the industry in a modelling framework. The framework is useful to support authentication system designers to take full advantage of context information beyond a risk score. For that, context information, threat situations and risks specify the relevance of authentication mechanisms, along with four required concerns:

- **Usability**, which is the condition of being able to be used (*e.g.,* the authentication mechanism is easy to understand for a user)
- **Deployability**, which is the condition of being able to be deployed (*e.g.,* the user's smartphone is equipped with a camera to perform face recognition, the implementation costs of the authentication mechanisms are not too high)
- **Security**, which is the capability to protect the major system aspects along the authentication process (*e.g.* by minimising the likelihood of an attack)
- **Privacy**, which is the ability to protect private context information (*e.g.,* by avoiding the request for personal identifiable information)

These concerns are in line with the seven laws of identity proposed by Kim Cameron in 2005 [5], which are known as essential laws that explain the successes and failures of digital identity systems.

The remaining of this paper is organised as follows. To motivate our work, we first present some motivational scenarios in section II and the results of an expert survey in section III. The framework CoFrA, its concepts and relationships are presented in section IV. In section V, we explain the implementation and the usage of CoFrA. Our validation is described in section VI. In section VII, we present related works, and we conclude our work in section VIII.

II. Motivational Scenarios

In order to determine the suitable authentication mechanism for a particular context, it is crucial to represent context information with appropriate and well-designed models. The relevance of authentication mechanisms cannot simply be determined by a one-dimensional risk score, as different types of risks need to be differentiated in a model. We illustrate this in the following scenarios.

a) Scenario 1: Let us assume a legitimate user who authenticates regularly with username, password, and an *One Time Password* (OTP). An attacker was able to get the user credentials through a phishing attack. Using social engineering, the attacker calls the user and convinces him to give away an OTP. Then, the attacker enters the credentials and types in the OTP, getting access to the protected resource.

b) Scenario 2: Another possible scenario is a user who authenticates regularly with username, password, and push-authentication[2]. The attacker hacked the phone, and malware ended up being installed by an attacker, giving him complete control of the user's phone. Push is not protected by a PIN or biometric. The attacker would use stolen credentials to authenticate, while monitoring the user's phone. When the push arrives, the attacker will use the control of the phone to approve the push and get access to the resource.

The two scenarios illustrate that for high-risk authentication attempts, there are different types of attacks. These differences are not considered when the context information is exclusively used to calculate a one-dimensional risk score. Therefore, there is a need for a modelling framework that enables a complex and fine-grained mapping between context information and authentication mechanisms.

The following example further illustrates the importance of taking into account context information for authenticating legitimate users in different contexts and not only denying access in the case of high-risk.

c) Scenario 3: Let us consider Bob, a German traveler in Spain. He checks his e-mails at 2:00 am in a poorly lit room. He enters the username and password correctly. His e-mail provider can acquire contextual information: geolocation, luminosity, time, and typing speed. Bob's e-mail provider determines some threats: Bob is not located in Germany as usual, he is checking his e-mails at an unusual time, it is dark around him, and he is typing slower than usual. All these threats make the e-mail provider assume that there is a risk that an intruder who has Bob's password might try to access Bob's e-mails. Bob has registered facial recognition and fingerprint as authentication mechanisms. Password-based authentication can be bypassed by the intruder who has stolen Bob's password. Face recognition is not efficient to use in the dark. Bob needs to be authenticated with his fingerprint.

The three presented scenarios would all have led to a high score in a risk-score-based approach. However, we see that to properly fend off attackers and allow legitimate users access, a more fine-grained and complex mapping of contextual information and authentication methods is needed.

III. Expert Survey

a) Objectives: We aim to identify the needs in industry regarding adaptive authentication. Therefore, we design a survey to uncover experts' thoughts on the relationship between context information and authentication mechanisms. Our questions fall into three categories: the **use of context information for authentication** (1), **impersonation risks and frauds** (2) and **desired properties of authentication mechanisms** (3). The totality of the questions and anonymous answers are available on our homepage [3].

b) The Expert Panel: The expert panel consists of eleven people working on identity management, authentication, and system security. They come from a multinational telecommunications corporation (Orange), a multinational aerospace corporation (Airbus), two European university research institutes (University of Hohenheim, Chouaïb Doukkali University El Jadida), and a medium-sized family-owned company for smart

[2]A mobile-centric authentication mechanism whereby the service provider sends the user a notification and the user responds to the challenge by performing an action (*e.g.,*"OK" button)

[3]Cf. https://github.com/BumillerAnne/CoFrA

sensor and image processing technologies (Wenglor Sensoric). We targeted people aware of the opportunity to use context information for authentication. It is not possible to identify and survey this entire population. Hence, we have chosen people from our professional network. All those people are potential adaptive authentication system designers and, therefore, users of our framework. Table I shows the job titles of the experts.

TABLE I
EXPERTS JOB TITLES

	Job Title
Expert 1	Identity Transverse Architect
Expert 2	Architect for Access Platforms
Expert 3	PhD Student: Behavioural Biometrics
Expert 4	Project Manager: Adaptive Authentication
Expert 5	System Architect of the Digital Identity Train
Expert 6	Direction of the Identity and Trust Research Program
Expert 7	Architect for Projects for Identity Anticipation and Research
Expert 8	Head Of Identity and Access Management for Users
Expert 9	Professor (Chair of Information Systems)
Expert 10	Master student of Big Data Analytics and Biometrics
Expert 11	Team Leader IT-Infrastructure

c) The Survey Procedure: In the first stage, the main idea of using context information (defined as any information that can be used to characterise an authentication attempt) for authentication was presented to the expert panel, followed by instructions on answering our online survey[4]. We invited them to contact us in the case of any questions or if they are interested in having an in-depth discussion. In the second stage, the experts answered our three question types. Three of the experts contacted us to discuss the topic further.

d) Analysis of the Responses: Most of the experts claim that **context information is not sufficiently used for authentication**. Nine out of eleven experts agree that context information is used for authentication, but eight of them claim that it is not sufficiently used. The two experts claiming that context information is not used mention the reason that there is a "lack of knowledge about how to use it". Hence, experts need more support to use contextual information for authentication. Furthermore, the great diversity of answers to the question of which context information is used (*e.g.,* device, risk score, localisation, browser fingerprint) shows that needs and perceptions vary greatly. This also points to the need for more support.

Most of the experts claim that **impersonation risks and frauds are not addressed during the authentication process**. Seven out of eleven experts agree that no risks are addressed during the authentication process. Eight out of eleven experts are aware of these risks. The results show that the risks are a concern for the experts but they are not addressed during the authentication process. To take full advantage of risks, experts need more support. We observed a great diversity of answers to the question of which risks are considered (*e.g.*, fraud, attack, the user is not whom he claims to be, stolen password, fast location change). Nevertheless, most of the terms can be traced back to the same risk (*e.g.,* fraud and attack). This shows that the experts do consider risks at different levels and that notions of risks are not unified in the domain. Support for using contextual information to identify risks and distinguish between different risk types is necessary to take full advantage of risks for authentication.

Finally, ten out of eleven experts claim that **not enough authentication mechanisms are used**. At least five experts consider each of the properties: security (9), deployability (5), usability (10), and privacy (9) essential to evaluate authentication mechanisms.

e) Results: Our survey results show that the experts need support to take full advantage of context information for authentication. We show that the experts are interested in **using contextual information** and do not yet make sufficient use of it. **Taking into account risks** for authentication decisions also interests the experts, and they find that this is not yet being done sufficiently. The **evaluation of authentication mechanisms** regarding the context and along with the properties **security**, **usability**, **deployability**, and **privacy** is considered necessary by the experts. Our framework helps adaptive authentication practitioners to determine the relevant authentication mechanisms characterized by properties using the available context information and according to identified risks. The results of our expert survey point out its usefulness.

IV. COFRA

The COFRA framework has been generated based on knowledge obtained through a literature review, together with the experience from industry experts gathered through extensive exchanges with authentication, security, and identity experts. First framework proposals have been discussed with experts and confronted with use cases. Then, we modified the initial proposals within an iterative feedback loop before proposing our final framework, detailed in the following section.

The structure of COFRA is represented in Figure 1[5] and captures the core domain concepts and relationships. We created the abstract syntax as an Ecore model. We use sufficient generalization (inheritance) to group common elements from different classes sharing abstract definitions. Considering the difficulty of expressing some information in a diagrammatic way, we specify 15 textual constraints in *Object Constraint Language* (OCL) to restrict the scope of some defined concepts. In [7], the authors investigate metamodel inaccurate structures that are often completed with OCL constraints. Based on their analysis, we assume having sufficient constraints to avoid such inaccuracies. In that way, the metamodel covers the intended domain while providing a good balance between the syntactical and static semantic parts. The defined constraints restrict how the structural elements can be instantiated and assembled to form a valid model with respect to the domain semantics.

A. Concepts and Relationships

Figure 1 shows the main concepts of COFRA in an Ecore-based metamodel. A CONTEXTINFORMATION defines any context information that can be used for adaptive authentication, *e.g.*, the geolocation of an entity. CONTEXTINFORMATION can

[4]https://msurvey.orange.com/AA_ENG

[5]For visibility reasons we do not show the root class MODELLINGFRAMEWORK

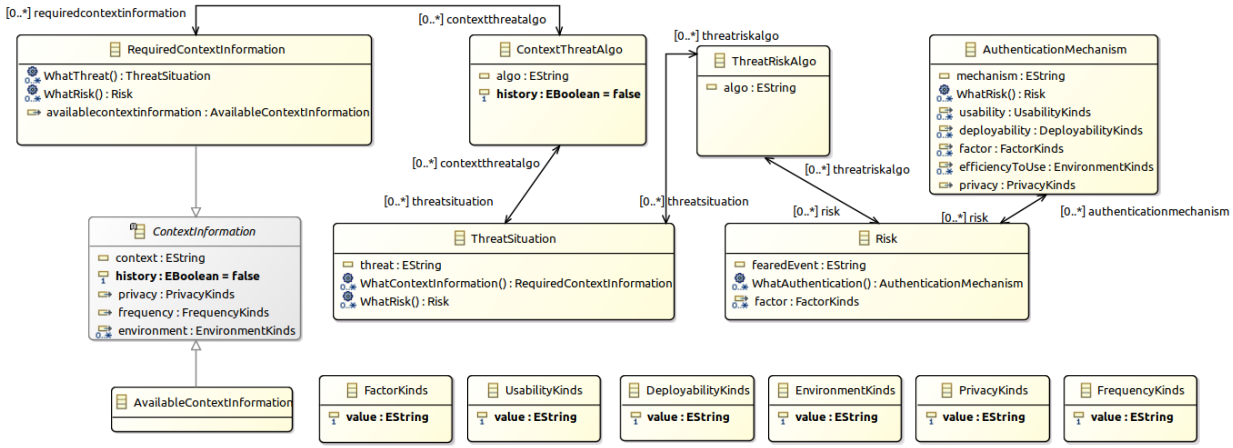


Fig. 1. Ecore Diagram of the CoFRA Metamodel

be either REQUIREDCONTEXTINFORMATION that represents any context information required in the authentication system, or AVAILABLECONTEXTINFORMATION that represents any context information actually available in the authentication system. Available and required context information are aligned as soon as the required information is available and the formats of the available and required information match (the attribute values of the available information must match those of the required information). The question of availability also arises when users use both mobile and static devices, as is common today. Context information acquirement with mobile devices (*e.g.,* smartphones) is often easier (more integrated sensors) than with non-mobile devices. Anyway, non-mobile devices must not be neglected, and therefore, the question of availability must be considered. The *context* of a CONTEXTINFORMATION instance uniquely describes the context information (*e.g.*, "geolocation"), and the *history* describes whether the history of the context information is available or required, for AVAILABLECONTEXTINFORMATION or REQUIREDCONTEXTINFORMATION respectively. For example, the history of the context information "geolocation" is required to detect derivations from geolocation patterns. The *privacy* attribute describes the context information privacy-sensitivity (*e.g.,* "luminosity" is not privacy sensitive while the user's "geolocation" is). The *environment* (*e.g., darkness*, *noise*, *activity*, *surrounded*) describes the environmental circumstances influenced by the context information. For example, the "luminosity" influences the "darkness" circumstance. Finally, the *frequency* describes the frequency at which the context information is available. For example, to determine fast location changes of users, which are suspicious, the "geolocation" needs to be used at a high frequency. A set of values for *EnvironmentKinds*, *PrivacyKinds* and *FrequencyKinds* are provided within a standard library included in the modeling framework (see Section subsection IV-C).

A REQUIREDCONTEXTINFORMATION is related to a CONTEXTTHREATALGO that determines threats from the context information, *i.e.,* defines any algorithm that can be used to determine THREATSITUATIONs from required context information (*e.g.,* an anomaly detection algorithm determining derivations from a user's usual "geolocation"). The *threat* describes uniquely the threat (*e.g.*, "newLocation").

A THREATSITUATION is related to a THREATRISKALGO that characterises RISKs from THREATSITUATIONs. For example, the risk of a stolen password can be characterised by a derivation of a user's habits regarding the geolocation, because it may be an intruder who is using the legitimate user's password from another geolocation. The *algo* describes uniquely the actual algorithm (*e.g.*, "StolenPWCharacterization"). Any RISK is characterized by the *fearedEvent* (*e.g.*, "StolenPW") and the *factor*s (*i.e.,* a list of possible secrets owned by the intruder (*e.g.,* knowledge)).

Finally, any RISK is related to AUTHENTICATIONMECHANISM(s) (*e.g.*, "username password") describing which authentication mechanisms can be applied to provide countermeasures against the risk. The *mechanism* describes uniquely the mechanism (*e.g.*, "username password"). The *usability* is a list of usability benefits (*e.g.*, nothing to carry, memory-wise effortless), and the *deployability* is a list of deployability benefits (*e.g.*, negligible costs per user, browser compatible). The *factor* describes the credential exchanged between the entity to be authenticated and the authenticating entity used by the authentication mechanism (*e.g., knowledge*, *possession*, *being*). The *efficiencyToUse* describes the environmental circumstances in which the authentication mechanism is efficient to use (*e.g., darkness*, *noise*, *activity*, *surrounded*). The *privacy* describes the privacy level of the authentication mechanism. A set of values for *FactorKinds*, *UsabilityKinds* and *DeployabilityKinds* are provided within a standard library included in the modeling framework (see Section subsection IV-C).

B. Required Concerns on Authentication Mechanisms

With the help of our framework, the relevance of authentication mechanisms can be evaluated according to multi-criteria optimizations of four required concerns as identified in our literature review and expert interviews: *security*, *usability*, *deployability* and *privacy*. In many works, the **security** evaluation of authentication mechanisms is based on their resilience against different attack types [9], [23], [24]. Our framework

focuses on the resilience against risks behind the attacks (*e.g.*, the risk of stolen memorial credentials behind a credential leak attack). We assume a mechanism to be resilient when an attacker does not own the authentication *factor* that the authentication mechanism is based on. We take into account desirable **usability** benefits of authentication mechanisms that are put forward in the literature to date (see subsection IV-C). The authentication mechanism class owns the attribute *usability* which describes the usability of the mechanism. We take into account desirable **deployability** benefits of authentication mechanisms that are put forward in the literature to date (see subsection IV-C). The authentication mechanism class owns the attribute *deployability* which describes deployability benefits. **Privacy** challenges regarding authentication are discussed in the literature to date [24], [28]. The context information class and the authentication mechanism class own the attribute *privacy* which describes the privacy level of the context information or the authentication mechanism, respectively.

C. A Standard Library for CoFrA

Associated with the metamodel, we deliver a standard library. We built the library based on reviewed scientific literature ([3], [9], [23], [24], [26]), as well as interviews with domain experts. The goal is to obtain a thorough overview of existing authentication credentials (*FactorKinds*), as well as usability (*UsabilityKinds*) and deployability (*DeployabilityKinds*) benefits of authentication mechanisms. For the privacy levels (*PrivacyKinds*) and the frequency at which context information is required or available (*FrequencyKinds*), our standard library provides a possible abstraction of the reality. Our standard library consists of the following lists of common values:

- ***FactorKinds***: Knowledge, Possession, Being, Doing, Human, Personal, Location
- ***UsabilityKinds***: Memorywise Effortless, Nothing to Carry, No Additional Network Access, Frictionless Setup, Affinity to User, Ease to Use, Ease of Learning, Ease of Recovery, Reliability, User Choice, Scalable for Users, Physically Effortless, Infrequent Errors, Not too Complex, Efficient to Use
- ***DeployabilityKinds***: Accessible, Negligible Cost per User, Server Compatible, Browser Compatible, Mature, Non-Proprietary, Negligible Implementation Costs, Computationally-Unrestricted, Multiple Channel
- ***PrivacyKinds***: High, Medium, Low
- ***FrequencyKindsKinds***: High, Medium, Low

The standard library is extendable so that an authentication system designer can adapt the metamodel to its specific needs. The *privacy* and *frequency* enumerations simplify the reality by using three levels. An authentication system designer can extend them (*e.g.,* to have more than three privacy levels, to use numeric values for the frequency). The authentication system designer can also add or remove usability and deployability benefits from the standard library. Within the standard library, we also introduce a set of template fragments for some literature authentication mechanisms to facilitate their reuse.

D. Structural Constraints Over the Metamodel

In this section, we present two examples of the 15 OCL invariants that we used to complete our metamodel's structure. In this way we ensure that we address the required concerns of security, usability, deployability, and privacy. The totality of all OCL invariants is available on the companion webpage[3].

a) Invariant 1: This invariant concerns the usability property. When context information impacts the environmental circumstances, the authentication mechanisms applied to provide countermeasures against risks that are characterised by this context information need to be efficient to use within the environmental circumstances. For example, when context information impacts the luminosity in a room so that it is dark around the user, we can not use the authentication mechanism "face recognition". In times of pandemic, a relevant example of the need to use contextual information to determine the efficiency of authentication mechanisms in environmental circumstances is the non-efficiency of face recognition when face masks are worn. The OCL invariant *EnvironmentCheck* ensures the efficiency of authentication mechanisms within the environmental circumstances.

```
class RequiredContextInformation
    invariant EnvironmentCheck:
        self.contextthreatalgo.threatsituation.
             threatriskalgo.risk.authenticationmechanism.
             efficiencyToUse
            -> includesAll(self.environment);
```

b) Invariant 2: This invariant concerns the security property. The risks are characterised by the authentication factors that the intruders are in possession of. Authentication mechanisms applied to provide countermeasures against the risks must not be based on the factors that the intruder is in possession of. For example, in the case of a stolen password, the intruder owns the "knowledge" factor, and the authentication mechanism "password" based on the "knowledge" factor must not be used. The OCL invariant *FactorCheck* makes sure that the intruder does not own an authentication mechanism's factor.

```
class Risk
    invariant FactorCheck:
        self.authenticationmechanism.factor
            ->excludesAll(self.factor));
```

V. Framework Implementation and Usage

In this section, we describe how CoFrA is implemented and how it can be used by adaptive authentication designers.

A. Framework Implementation

Our precise metamodel to reason about the relevance of authentication mechanisms regarding context information is based on the de-facto standard *Model Driven Engineering* (MDE) framework ***Eclipse Modelling Framework (EMF)***. As illustrated in Figure 1, for the structural part, we use the **Ecore** language, which provides structural modeling capabilities similar to the *Unified Modeling Language* (UML) class diagram. We have chosen the *Eclipse Modelling Framework* (EMF) as this is the leading metamodelling framework, offering several metamodelling technologies such as Ecore to encode the structure of metamodels, and ***Object Constraint Language***

(OCL) to encode the static semantics of metamodels. We benefit from the EMF ecosystem to provide an integrated no-code environment on top of our modeling framework.

B. Framework Usage

The framework supports the adaptive authentication system designer in the complex trade-off analysis between context information, risks, and authentication mechanisms, according to usability, deployability, security, and privacy. This enables the use of context information for authentication decisions not only to calculate a risk score but to reason about the relevance of authentication mechanisms according to the contextual situation and identified risks. In Figure 2 we show the main functionality of CoFrA in contrast to score-based approaches (*e.g.,* [27]). Instead of using the context information to calculate a risk score and to choose the authentication mechanism based only on this score, CoFrA enables a more complex mapping of context information to authentication mechanisms with the help of multiple threat situations and risks. The final goal is to obtain a context-aware authentication system design model: which context information to use, which threat situations to determine, which risks to identify, and which authentication methods to use.

VI. Framework Evaluation - Case Studies

In this section, we present the evaluation of our approach. We illustrate how the proposed framework can be used for context modelling of various authentication applications. For each application, we create a dynamic modelling instance of our metamodel and run a OCL validation. The totality of the created model instances is available on the companion webpage[3]. The experimental protocol consists of selecting hypothetical cases, cases from the literature, and real-world cases to validate our framework. We show that the amount of abstraction covers all domain concepts (**sufficiency**) without specifying unnecessary, too many details (**necessity**). We prove that our approach can handle all the cases and allows us to present them in a clear manner (**soundness**). Finally, we demonstrate that our approach can design, validate and deploy the adaptive authentication system design for all the chosen cases.

A. Experimental Setup

The goal of the CoFrA framework is to provide constructs for authentication system designers to reason about authentication mechanisms according to the context. To validate the relevance of the abstraction provided, we propose to discuss

1) The domain concepts coverage of our framework's abstraction (sufficiency)
2) The amount of details required to specify most contexts (necessity)
3) The framework's ability to correctly handle concrete example cases and to present them in a clear manner (soundness)

We selected hypothetical cases, cases from the literature, and real-world cases to support the discussion.

B. Results

We present the results of our experimentation to validate a) the sufficiency, b) the necessity, and c) the soundness of our framework.

a) ***Sufficiency****:* To highlight the sufficiency of our framework, we create model instances of existing context modelling approaches for context-aware authentication proposed in the literature from the last ten years. We searched for relevant approaches based on a search clause consisting of a conjunction of the term "authentication system", "context modelling" and a disjunction of terms expressing the adaptation capability of the authentication system for conducting a systematic literature review[6]. We classified the identified works into five different types of authentication approaches for which the context is modelled (biometric recognition methods (*e.g.,* [19]), approaches for mobile devices (*e.g.,* [16]), behaviour based authentication (*e.g.,* [15]), approaches for ubiquitous services (*e.g.,* [12]), approaches for digital identity management (*e.g.,* [10])). For each category, we modelled at least one approach and successfully built the model conforming to CoFrA. We can abstract all the notions of the approaches within the classes of our metamodel. We model our motivational example introduced in section II (Bob - The Traveler), a second hypothetical case (paragraph VI-B0b) and a real-world adaptive authentication application (paragraph VI-B0c). Also, for these cases, all the notions can be abstracted within our metamodel's classes, highlighting our model's sufficiency.

b) ***Necessity****:* To model the cases from the literature (paragraph VI-B0a), we make use of all the meta-classes and all our OCL constraints for at least one of the model instances. We prove that we do not specify unnecessary, too complex details in our metamodel. The model instance of our motivational example introduced in section II consists of four ContextInformation instances, four ContextThreatAlgo instances, four ThreatSituation instances, one ThreatRiskAlgo instance, one Risk instance and three AuthenticationMechanism instances. We make use of all our metamodel's classes and all OCL constraints to create this model instance. This also highlights necessity of our approach. We also model a real-world application described in paragraph VI-B0c, which consists of three ContextInformation instances, five instances of the class ContextThreatAlgo, five ThreatSituation instances, three instances of the class ThreatRiskAlgo, three Risk instances, and four AuthenticationMechanism instances. To model this real-world application, we use all our metamodel's classes.

c) ***Soundness****:* We aim to conduct a case study based on a hypothetical application whose contextual situation considers a standard case in contrast to our motivational example introduced in section II whose contextual situation considers an extreme case (*i.e.,* many derivations from the user's patterns). Therefore, we take the example of Alice, an employee who accesses her e-mails on a Monday at 09:03 AM as usual. She is in her usual workplace, and she is using her device.

[6]The publication process of our *Systematic Literature Review on Understanding Context Modelling for Adaptive Authentication Systems* is ongoing.

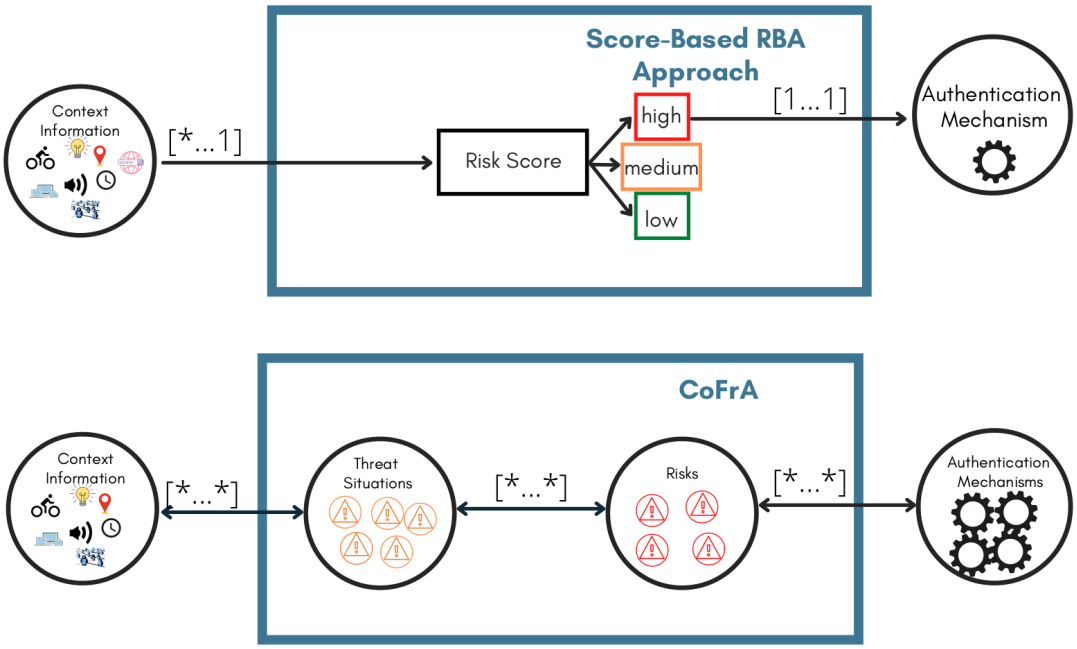


Fig. 2. Illustration of our CoFrA Framework in Contrast to Score-Based *Risk Based Authentication* (RBA) Approaches

Her e-mail provider can acquire contextual information: IP address, user agent, and time, and determines that there is no threat concerning these features. This makes the e-mail provider assume that there is no risk. Therefore, the authentication can be done with any method from a security point of view. We can choose the method which is the easiest to use for Alice or even just grant access without asking for any authentication. We can successfully create a model instance of this hypothetical case. This shows soundness of our metamodel in the presence of standard and extreme features. To prove the soundness of our framework in real-world applications, we analyse a company's project towards user notifications. The project's origins come from the need to notify the user in the case of changes in the device or the country. The notifications are created based on successful authentication events containing the ContextInformation date (time), the IP address (country), and the user agent (device). Based on this information, indicators that the user needs to be notified (new IP address, new location, new device, fast location change, and robot suspected) are calculated. The indicators can be classified according to three Risks: stolen memorial credentials, stolen devices, and robots. We can successfully model the project conform to our metamodel, which shows soundness of our metamodel in presence of real-world cases.

Through the conducted case studies, we show that the amount of complexity allows covering all domain concepts (**sufficiency**) without specifying unnecessary, too complex details (**necessity**). Also, we show **soundness** of our model for standard and extreme cases as well as for real-world applications.

VII. Related Work

In the current state of the art, as stated in the introduction, we observe a trend of separating the risk analysis from the actual authentication decision. Typically risk engines determine risk levels, which are sent to an authentication engine without using information about the risk to make authentication decisions. Several modeling techniques have been introduced in the past decades for supporting such an approach [4], [21].

Instead, we demonstrate in this paper the need for managing complex mappings between the contextual information and the possible authentication mechanisms, according to identified threads and related risks. DeepAuth is an example of a generic framework with mappings for re-authenticating users in a mobile app [1].

For supporting domain experts in the definition of such complex mappings, we introduce in this paper a dedicated framework and discuss the benefits of using modeling techniques. While model-driven engineering have been widely considered for authentication configuration [20], this is from the best of our knowledge the first modeling framework dedicated to dynamic authentication decisions, introducing key abstractions (e.g., *Threat*, *Risk*) and an associated approach.

VIII. Conclusion and Future Work

This article aims to cover an existing gap in the literature: the lack of a method for reasoning about the relevance of authentication mechanisms according to the context and four desired properties of the mechanisms: security, usability, deployability, and privacy. We propose a modelling framework to realize this, which covers the shortcomings of existing works based on risk scores. Both the knowledge from literature and the experience from industry were gathered through this work to learn the needs of both sides and obtain an added value

to the proposals given by this article. The model's validity in terms of sufficiency, necessity, and soundness is ascertained through three case studies. Our main contribution is creating a precise modelling framework based on the academy and the industry, which allows authentication system designers to use context information efficiently for authentication. Several tasks can be performed as future work of our research. To show the usability of our framework, we plan an evaluation by experts using the framework. Therefore, we are currently working on a fully functional recommendation tool. Some of the framework's abstractions (*e.g.*, the privacy levels) can be developed in greater detail. It would also be interesting to introduce a quantification of the properties security usability, privacy and deployability, enabling the authentication system designers to meet their needs and find their trade-offs between the properties. Future work will also include the development of the concrete syntax to enable user-friendly modelling for the designers. We are also planning to further develop our homepage so that the use of CoFrA is explained with the help of tutorials and sample scenarios.For the users of our framework, it can be of interest not only to get a context information model but that the framework provides them with the implementation of their adaptive authentication system design. Also, the context information acquirement needs further investigation.

References

[1] Amini, S., Noroozi, V., Pande, A., Gupte, S., Yu, P.S., Kanich, C.: Deepauth: A framework for continuous user re-authentication in mobile apps. In: Proceedings of the 27th ACM International Conference on Information and Knowledge Management. p. 2027–2035. CIKM '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3269206.3272034, https://doi.org/10.1145/3269206.3272034

[2] Arias-Cabarcos, P., Krupitzer, C., Becker, C.: A survey on adaptive authentication. ACM Computing Surveys (CSUR) **52**(4), 1–30 (2019)

[3] Bonneau, J., Herley, C., Van Oorschot, P.C., Stajano, F.: The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: 2012 IEEE Symposium on Security and Privacy. pp. 553–567. IEEE (2012)

[4] Calvo, M., Beltrán, M.: A model for risk-based adaptive security controls. Computers & Security **115**, 102612 (2022). https://doi.org/https://doi.org/10.1016/j.cose.2022.102612, https://www.sciencedirect.com/science/article/pii/S0167404822000116

[5] Cameron, K.: The laws of identity, microsoft corp (2005)

[6] Campobasso, M., Allodi, L.: Impersonation-as-a-service: Characterizing the emerging criminal infrastructure for user impersonation at scale. In: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. pp. 1665–1680 (2020)

[7] Cherfa, E., Kesraoui, S., Tibermacine, C., Fleurquin, R., Sadou, S.: On investigating metamodel inaccurate structures. In: Proceedings of the 35th Annual ACM Symposium on Applied Computing. pp. 1642–1649 (2020)

[8] Daud, N.I., Haron, G.R., Othman, S.S.S.: Adaptive authentication: Implementing random canvas fingerprinting as user attributes factor. In: 2017 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE). pp. 152–156. IEEE (2017)

[9] Doerfler, P., Thomas, K., Marincenko, M., Ranieri, J., Jiang, Y., Moscicki, A., McCoy, D.: Evaluating login challenges as adefense against account takeover. In: The World Wide Web Conference. pp. 372–382 (2019)

[10] En-Nasry, B., El Kettani, M.D.E.C.: Towards an open framework for mobile digital identity management through strong authentication methods. In: FTRA International Conference on Secure and Trust Computing, Data Management, and Application. pp. 56–63. Springer, na (2011)

[11] Freeman, D., Jain, S., Dürmuth, M., Biggio, B., Giacinto, G.: Who are you? a statistical approach to measuring user authenticity. In: NDSS. vol. 16, pp. 21–24 (2016)

[12] GH, S.G., Swamy, S.C.: A security approach to build a trustworthy ubiquitous learning system. In: 2020 IEEE Bangalore Humanitarian Technology Conference (B-HTC). pp. 1–6. IEEE, Karnataka, India (2020)

[13] Herley, C., Schechter, S.E.: Distinguishing attacks from legitimate authentication traffic at scale. In: NDSS (2019)

[14] Hurkała, A., Hurkała, J.: Architecture of context-risk-aware authentication system for web environments. The Third International Conference on Informatics Engineering and Information Science (2014)

[15] Lima, J.C.D., Rocha, C.C., Augustin, I., et al.: A context-aware recommendation system to behavioral based authentication in mobile and pervasive environments. In: 2011 IFIP 9th International Conference on Embedded and Ubiquitous Computing. pp. 312–319. IEEE, Melbourne, Australia (2011)

[16] Miraoui, M., El-etriby, S.: A context-aware authentication approach for smartphones. In: 2019 International Conference on Computer and Information Sciences (ICCIS). pp. 1–5. IEEE, Aljouf, Kingdom of Saudi Arabia (2019)

[17] Molloy, I., Dickens, L., Morisset, C., Cheng, P.C., Lobo, J., Russo, A.: Risk-based security decisions under uncertainty. In: Proceedings of the second ACM conference on Data and Application Security and Privacy. pp. 157–168 (2012)

[18] Morris, R., Thompson, K.: Password security: A case history. Communications of the ACM **22**(11), 594–597 (1979)

[19] Saedi, S., Charkari, N.M.: Characterization of palmprint using discrete orthonormal s-transform. In: 2011 International Conference on Hand-Based Biometrics. pp. 1–6. IEEE, na (2011)

[20] Satoh, F., Nakamura, Y., Ono, K.: Adding authentication to model driven security. In: 2006 IEEE International Conference on Web Services (ICWS'06). pp. 585–594 (2006). https://doi.org/10.1109/ICWS.2006.25

[21] Sepczuk, M., Kotulski, Z.: A new risk-based authentication management model oriented on user's experience. Computers & Security **73**, 17–33 (2018). https://doi.org/https://doi.org/10.1016/j.cose.2017.10.002, https://www.sciencedirect.com/science/article/pii/S0167404817302079

[22] Traore, I., Woungang, I., Obaidat, M.S., Nakkabi, Y., Lai, I.: Combining mouse and keystroke dynamics biometrics for risk-based authentication in web environments. In: 2012 fourth international conference on digital home. pp. 138–145. IEEE (2012)

[23] Velásquez, I., Caro, A., Rodríguez, A.: Kontun: A framework for recommendation of authentication schemes and methods. Information and Software Technology **96**, 27–37 (2018)

[24] Wang, D., Gu, Q., Cheng, H., Wang, P.: The request for better measurement: A comparative evaluation of two-factor authentication schemes. In: Proceedings of the 11th ACM on Asia conference on computer and communications security. pp. 475–486 (2016)

[25] Weber, J.E., Guster, D., Safonov, P., Schmidt, M.B.: Weak password security: An empirical study. Information Security Journal: A Global Perspective **17**(1), 45–54 (2008)

[26] Wiefling, S., Dürmuth, M., Lo Iacono, L.: More than just good passwords? a study on usability and security perceptions of risk-based authentication. In: Annual Computer Security Applications Conference. pp. 203–218 (2020)

[27] Wiefling, S., Iacono, L.L., Dürmuth, M.: Is this really you? an empirical study on risk-based authentication applied in the wild. In: IFIP International Conference on ICT Systems Security and Privacy Protection. pp. 134–148. Springer (2019)

[28] Wiefling, S., Tolsdorf, J., Iacono, L.L.: Privacy considerations for risk-based authentication systems. In: 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). pp. 320–327. IEEE (2021)