Karlsruhe Institute of Technology

Hewlett Packard Enterprise

HECTOR SCHOOL
Technology Business School of the KIT

Towards a Unified Qualitative Usable Security Assessment Framework for Cloud Computing

Master's Thesis of

Oliver Rudzinski

at the HECTOR School of Engineering and Management
Information Systems Engineering and Management

for the Institute for Program Structures and Data Organization (IPD)

in collaboration with Hewlett Packard Enterprise

Reviewer:	Prof. Dr. Ralf Reussner
Second reviewer:	Dr. Robert Heinrich

01. October 2022 – 31. March 2023

HECTOR School of Engineering and & Management
℅ International Department of the KIT gGmbH
Schlossplatz 19
76131 Karlsruhe

Table of Contents

List of Acronyms

API	Application Programming Interface
CC	Cloud Computing
CLI	Command Line Interface
HCD	Human-Centered Design
HPE	Hewlett Packard Enterprise
IaaS	Infrastructure as a Service
IAM	Identity & Access Management
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
SaaS	Software as a Service
UI	User Interface

1 Introduction

1.1 Motivation

Cybersecurity has been and still remains *the* most crucial discipline in the domain of Information Technology (IT): According to Mordor Intelligence, the global cybersecurity market was valued at approx. $150 billion in 2021. This trend is expected to continue, rising up to approx. $317 billion by the year of 2027 with a constant annual growth rate of 13.4% [11]. This can be linked to the average cost of a single data breach equaling $4.24 million in the same year and describing the highest value on record so far, as per IBM [10]. These rises are proportional to the increase in cyber attacks: Malware attacks increased by 358% in 2020, Ransomeware attacks rose by 435% [24].The current landscape of cybersecurity can be summarized as an arms race between the attackers of valuable resources and their protectors.

Looking at the domain of Cloud Computing (CC), 27% of organizations report having experienced security incidents within one year [36]. Overall, the fear of security challenges is the main concern why some businesses do not introduce CC at all [1, 2].

Businesses investing in sophisticated security technology and services might not be enough, as 95% of cybersecurity issues can be linked to human error [26]. One reason for this might be the increased complexity of security systems and settings, leading to misconfigurations that in turn lead to security vulnerabilities. In CC, misconfiguration in the cloud infrastructure accounted for 23% of security incidents [36]. It can be assumed that the increased complexity of IT security features reduces its usability, resulting in a decrease of their efficiency.

The research discipline of *usable security* has recognized this issue and aims at bringing effective IT security together with information system usability [19]. Considered separately, there exist several design and assessment frameworks for security aspects within information systems, e.g., the Security Design Principles by Saltzer and Schröder (1975) [35], the Security By Design Principles according to the Open Web Application Security Project (OWASP), or the Cybersecurity Framework by the National Institute of Standards and Technology (NIST) [18]. On the other hand, usability assessments, e.g., the Usability Heuristics by Nielsen (1994) [30], or usability principles and guidelines support the evaluation of the user friendliness of User Interfaces (UIs) [28]. These existing frameworks will hereinafter be referred to as *current frameworks*.

However, usable security research as a whole is considered complicated due to interdisciplinary factors, technological velocity, etc. [19]. That is why it is currently conducted based on individual definition and execution of experiments rather than supported by guidelines or frameworks. This can lead to slower examination of the problems at hand, consequently leading to fewer insights on how to potentially address them.

This is where this proposed Master's thesis ties in: It suggests a unified framework for qualitative usable security assessment that will be developed and evaluated experimentally within the security-crucial domain of CC. This will hereinafter be referred to as the *unified framework*.

1.2 Problem Statements

The previous motivation to the topic (cf. Section 1.1) as well as further demonstration of current research in that area (cf. Chapter 3) recognize the following problems:

P1 Usable security research is currently conducted on a case-by-case basis which limits efficiency and quantity of insights in order to address problems within that domain.

P2 In terms of CC, security configuration aspects are currently complicated to consider in terms of usable security, which visibly leads to a significant amount of security incidents.

1.3 Contribution

The problems stated in Section 1.2 are aimed at being addressed through the following aspired contributions. While these contributions are build on one another, they are also designed to individually undertake issues within current usable security research.

C1 Evaluate the applicability of present usability and security design frameworks to usable security individually to the domain of CC in order to deduct limitations and improvements.

This contribution will partly address P1, as there is limited research present regarding the explicit applicability of usability and security design frameworks to usable security. Thus, it cannot be justified that these frameworks are not applicable per se. This contribution's output will generate the input for C2 in order to have a foundation for the design of the unified framework. As this assessment will be pracitically performed within a CC environment, this contribution also partly covers P2.

C2 Design a unified qualitative usable security assessment framework based on the findings from C1.

This contribution will mainly address P1 by applying the findings from C1 in order to develop a unified framework for usable security evaluation. It is expected that certain aspects of the frameworks under test in C1 will appear in the unified framework, while others might be refined or newly introduced.

C3 Validate the unified framework regarding improvements in terms of applicability, conclusivity, and efficiency compared to C1.

This contribution, again, addresses P1 and P2 in that the actual benefit of the new framework needs to be validated within a CC security feature scope.

All in all, P2 will be addressed across all contributions as each practical application will be done in terms of CC security features. The actual methodology for the achievement of the contributions will be outlined in Chapter 4.

1.4 Proposal Structure

This Introduction chapter introduced the motivation to the topic as well as outlined problems and corresponding contributions to the matter. Chapter 2 provides necessary background information to the domains of information and cyber security, security design, usability evaluation, usable security research, as well as Cloud Computing. Chapter 3 discusses the current research in the area and derives its limitations that are addressed by the contributions of this thesis. Chapter 4 describes the methodology and process of achieving the aspired contributions. Chapter 6 outlines the research stakeholders, Master's thesis artefacts as well as the project plan of this work.

2 Foundations

This chapter aims at providing an overview on the necessary background information and technical foundations required to perform the desired research. It is expected that these foundations will be elaborated in the actual thesis as certain examined aspects of the research might require additional background. The design of this chapter is not meant to be exhaustive to each area but shall only provide the information that is strictly required for the sake of this work.

2.1 Information Security

The U.S. National Institute of Standards and Technology (NIST) defines information security as "the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability" [29]. The last three characteristics can be further defined:

Confidentiality Unauthorized entities are restricted from access and disclosure of information for the purpose of protecting personal privacy and proprietary information [29].

Integrity Improper modification or destruction of information, including the compromitation of data non-repudiation and authenticity, is protected against. Furthermore, *data integrity* means that data has not been improperly altered, whereas *system integrity* goes beyond unautorized manipulation, defining system function quality when performing as intended and unimpaired [29].

Availability Accessibility and usability of information is reliable and timely [29]. This also includes the prevention of intended, unauthorized withholding of data [17, p. 36].

This *CIA triad* can be extended by additional characteristics, e.g. *accountability* (user actions can be traced back to them), *functionality* (system's behavior is as intended and expected) and *reliability* (system always performs under equal conditions) [17, p. 36 sq.].

2.1.1 Distinction from Cyber Security

The terms *information security* and *cyber security* (i.a.), are often used interchangeably in literature. However, this work requires a specific distinction between those terms. As defined by the NIST Cybersecurity Framework, cyber security means "the ability to protect or defend the use of cyberspace from cyber attacks" [18]. By that, cyber security is a disciplinary subset of information security that especially considers the electronic protection of data and resources within its technical perimeter. Consequently, this excludes activities like physical access or compliance control that are inherent information security disciplines. Nevertheless, both areas focus on achieving the goal of the information security definition by ensuring the application of the CIA tiad.

2.1.2 Security Design

As motivated in Chapter 1, cyberattacks are still on the rise, which leads to assume that the current state of the art of security design and implementation cannot systematically exclude security flaws. This has already been recognized by Saltzer and Schröder (1975) who summarized general security design guidelines that address general security problems during the design of information systems [35]. They include best practices that aim at considering the CIA triad from the software perspective.

It appears to support security design aspects during the actual design and implementation. There exist similar design frameworks in that domain, e.g., the OWASP Security By Design Principles.

Finally, there exist distinct security assessment and improvement frameworks for information systems that are already in place, such as the NIST Cybersecurity Framework. It defines a process model for the evaluation of the current state, a tiered readiness assessment, as well as transition profiles to reach a desired state of cybersecurity [18].

2.2 Usability of Information Systems

Information system usability is part of ergonomics of human-system interaction, standardized by the International Organization for Standardization (ISO) [12]. It defines *usability* as the "extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [12].

The interaction between the user and the system is done through a User Interface (UI), defined by ISO as the "set of all the components of an interactive system that provide information and controls for the user to accomplish specific tasks with the interactive system" [12].

While usability design and evaluation are often applied to UIs, these processes could also apply to less end-user-focussed interfaces, e.g., Application Programming Interfaces (APIs) or Command Line Interfaces (CLIs).

2.2.1 Usability Design Guidelines

The process of providing *good* system usability to users is aided by several guidelines and frameworks: The ISO defines the Human-Centered Design (HCD) process, which describes an "approach to systems design and development that aims to make interactive systems more usable by focusing on the use of the system and applying human factors/ergonomics and usability knowledge and techniques" [13].

HCD is an iterative approach and includes the understanding and requirement of the context, as well as the cooperative development and evaluation of design solutions [13]. The latter steps are aided by potential users of the system under design.

HCD is particularized through further guidelines developed by notable researchers that define general principles on usability design. These include, but are not limited to, Shneiderman's Eight Golden Rules of Interface Design [38], Norman's Seven Design Principles [31], and Nielsen's Ten Usability Heuristics for User Interface Design [30]. All of those frameworks follow a similar structure in that they specifically ask for the existence or absence of characteristics within the interface, e.g., visibility of things, consistency of design, etc.

2.2.2 Usability Evaluation

The evaluation of usability is often referred to *usability testing* [28]. Its goals are to identify problems, uncover opportunities as well as learn about the target user's behavior and preferences [28]. Elements of usability testing include participants (i.e., realistic users of the system), specific tasks or activities performed by the participant, as well as a facilitator (i.e., moderator and creator of the specific activity) [28]. After performing the activities, the participants are expected to provide feedback to the moderator, whereas the moderator notes insights to the behavior of the participant and the system.

Usability evaluation can be either qualitative (i.e., focussing on distinct insights and findings with regards to user behavior) or quantitative (i.e., focussing on benchmarks, e.g., task success or elapsed time). They are usually conducted in a remote setting, however there also exists in-person usability testing. Finally, it can be performed in a moderated (i.e., interactive) or unmoderated manner (i.e., no interaction between the participant and the facilitator) [28].

The definition of tasks for a usability evaluation highly depends on the specific area under test. However, it can be expected that the usability design guidelines (cf. Subsection 2.2.1) can be taken into account.

2.3 Usable Security

Bringing it all together, *usable security* deals with the design, implementation, and evaluation of the usability of security features and aspects within information systems [34]. Chronologically, it originates from the already mentioned Security Design Principles by Saltzer and Schröder (1975), specifically the final one considering the "psychological acceptability" of the mechanisms [34, 35]. Later, Zurko and Simon (1996) novelly suggested to apply usability aspects of software design to security features [43]. Shortly after, Adams and Sasse (1999) researched usability flaws in terms of password protection from a user perspective and provided recommendations on remedial measures [4]. Since then, the majority of usable security research is focussed on end-user security in terms of password protection and email encryption [34, 41]. More recently, this field also started to consider developers and IT professionals as their usability issues in terms of security can lead to severe security vulnerabilities [8].

Other than with security *or* usability evaluation, there do not exist established unified frameworks or guidelines for usable security assessment. Some more recent studies suggest certain approaches that will be discussed in Chapter 3. Other than that, usable security is currently performed by means of individual experiments [19].

2.4 Cloud Computing

The NIST defines CC as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (...) that can be rapidly provisioned and released with minimal management effort (...)" [27]. It can be seen as the latest form of infrastructure consolidation after the introduction of client-server computing and the rise of datacenter hardware virtualization [37, p. 1].

In general, CC is described by a vendor-consumer relationship, with the vendor being the provider of the IT resources, and the consumer being the receiver and user of those resources. Depending on the deployment model of the CC infrastructure at hand, the vendor can be

- internal to an organization or providing isolated resources exclusively to that organization (i.e., *private cloud*),
- external, providing resources to multiple entities (i.e., *public cloud*),
- or a mix of both [27].

The service level defines the level of abstraction of the resources to the consumer and which party is responsible for which layer of application provisioning and deployment. Typically, this includes Infrastructure as a Service (IaaS) (vendor provides virtualized infrastructure), Platform as a Service (PaaS) (vendor provides virtualized infrastructure as well as the specific operating system, runtime environment, etc. to that platform), and Software as a Service (SaaS) (vendor provides infrastructure, platform, and specific software deployment) [27].

The NIST laid out several aspects that further define CC characteristics, service, and deployment models.

On-demand self-service Provisioning of (more) computing, storage, network resources, etc. is done by the consumer without interaction with the CC service provider [27]. This implies a form of automation on the CC vendor's end as well as the existence of control and monitoring interfaces for the consumer [37, p. 51].

Broad network access The CC vendor's services and capabilities are accessible over the network and can be accessed via mechanisms that are already in place for consuming clients [27, 37, p. 45].

Resource pooling Resource pooling allows CC vendor's to introduce the concept of *multi-tenancy*, where the physical infrastructure that is made available is virtualized and dynamically assigned to distinct consumers, or *tenants*, based on demand or contractual agreements [27, 37, p. 45]. In other words, a *pool* of total resources present is made available to multiple consumers based on their *current* needs and re-evaluated over the course of the usage.

Rapid elasticity The consumer can dynamically scale their resource capacity up or down as needed. The consumer is not aware of any global resource limitations which make the CC resources appear unlimited [27].

Measured service The consumed services are quantitatively measured by the CC vendor for billing, controlling and optimization purposes. This is based on appropriate forms of metering with regard to the service (e.g., number of terabytes of storage consumed within a month). Thus, billing of utilized services is often done on a pay-per-use basis [27]. Consequently, the more resources are utilized by the vendor, the higher the cost. This process is transparent to both vendor and consumer, allowing for consumption and billing monitoring, control, and reporting [27].

3 Related Work

As mentioned in Section 2.3, the discipline of usable security has recently gained in importance. Therefore, it is of interest, which aspects of this underlying work are already present in current research, and which aspects of interest have currently not been addressed. The discussion of related work will prove valuable for the identification of current research limitations that need to be addressed by the contributions of this work. As with Chapter 2, it is expected that the consideration of related work might be enlarged during the actual research.

3.1 Present Research

3.1.1 General Research on Usable Security

Starting with a critical look at usable security research, Theofanos (2020) points out that, even though this discipline has been around for a quarter of a decade, there have been little to no achievements to the underlying problem of so-called *security fatigue* observed in user behavior. She points out the major areas where usable security might make a difference (e.g., authentication, encryption, user dialogs, etc.) and appeals to developers and researchers to make this field of study more applicable and practical [40]. The arguments and appeals support this proposed work.

More concretely, Acar et al. (2016) recognize the problem of this research field being almost entirely end-user-centric up until now. They suggest specific measures and key research questions in order to consider developers' and IT professionals' points of view in that domain. This includes the evaluation of interfaces outside of end user scope, introducing secure usability research towards APIs, as well as providing relevant security resources for the development process [3]. Similar claims are made by Green and Smith (2016). They, again, demand more emphasis on secure and usable APIs [20]. These claims support the validity of this work's research topic and will be of great guidance pursuing the goal of developing a qualitative usable security assessment framework.

Chiasson et al. (2007) furthermore propose general design principles to make administrator interfaces more psychologically graspable [9]. These were not validated by the authors during research, but can be used as knowledgable input to the design of this work's assessment framework.

Finally, Lennartsson et al. (2020) analyzed current research directions of usable security more thorougly than possible in this work. Apart from other findings, they recognized the urge of "developing concrete guidelines for implementation of user-centric security" [23], which, again, validates this work's purpose.

3.1.2 Towards Usable Security Frameworks

Parkin et al. (2010) recognized the psychological distance between technology-driven password policies in contrast to their users and what negative effect this could have on businesses' security. They essentially suggest an HCD-driven approach that includes users of the security mechanism and their feedback throughout its entire design phase [32]. However, this approach ties in with how usable security design and evaluation is currently conducted in terms of individual experiments. Plus, the evaluation and enhancement of features potentially in place is missing here.

Similarly, Feth et al. (2017) extended the individual steps of the HCD process to include security awareness from the start. They applied their model exemplarily to a smart home use case. Apart from mentioning the models abstractness, they realize their uncertainty regarding the model's applicability to other use case domains [16]. Furthermore, the research appears to combine security and privacy-related aspects. It also leads to assume that it is rather end-user-focussed which ties in with the majority of current usable security research.

This looks differently when considering research performed by Caputo et al. (2016) who manufactured interview questionnaires for different stages of security feature development and introduction (i.e., development, product, and management level). They then performed three case studies validating the applicability of their methodology and falsified some hypotheses from the beginning (e.g., that complicated security measures are *always* more secure, that usability is common sense, and that there *must be* a tradeoff between usability and security) [7]. Although very valuable for further research, the questionnaires provided are very abstract in that their development does not appear to be based on specific domains nor on current usability or security evaluation frameworks. It also puts a large emphasis on management perception as well as benchmarks in the *process* of development and introduction, rather than on the development or evaluation itself.

Conversely, Ambore et al. (2021) present an evaluation approach that is inspired by usability evaluation heuristics. Specifically, they derive heuristics from general usability assessment and refine as well as apply them to the domain of financial technology. They validate their approach by performing usable security assessment in financial organizations and conclude that such evaluation, in fact, improved usable security of the evaluated applications [6]. This research can be considered as a starting point for the development of this work's unified framework for the different application domain of cloud computing.

Another approach of usable security evaluation is presented by Hausawi and Allen (2015). They introduce a general quantitative evaluation approach in terms of a risk assessment for usable security. The output of the assessment is a numerical value that aims at classifying the overall risk of present or non-present usable security in terms of an application under test [22]. While this approach appears very general and thus applicable to various domains of interest, it might add an additional burden to the process as it is solely quantitative and does not take individual aspects of usable security into account.

3.1.3 Research on Cloud Security

Understanding current security-related CC research and its underlying or discovered problems might aid in moving this work's practical approach in a relevant direction.

A variety of researchers claims that the aspects of multi-tenancy [21, 39, 33, 25], extensive virtualization [15, 21], and Identity & Access Management (IAM) [5] present the most critical security concerns across CC infrastructure management, regardless of their deployment of service models [25]. This leads to assume that general features implementing inherent characteristics of CC are generally implemented similarly. Consequently, they also share similar security issues.

In slight contrast, Yandong and Yongsheng (2012) mention that public cloud vendors might be more susceptible to cyberattacks as it is known that they store a vast amount of data that could be leveraged for malicious activities [42]. While it can be argued, that many cloud security issues cannot solely be tackled by improving their security feature usability, an understanding of the criticality of those features can support prioritization of validation criteria when designing a unified usable security assessment framework.

3.1.4 Towards Usable Security in the Cloud

Research on usable security in the domain of CC is strongly limited. However, Fahl et al. (2012) propose a way to introduce usable security in terms of CC management. They argue that the current way of securing CC resources is done via public key infrastructures that are perceived to be very complicated from an end-users point of view. They propose a novel form of user-friendly security mechanism that removes the perceived burden in the form of a distinct security service [14]. While it appears valuable that entirely new mechanisms are researched and developed with the primary goal of usability, this research does not consider the improvement of current established systems by enhancing their usability. The reinvention of security mechanisms should be the last resort, as it merely shifts responsibility from one end to another. This, in turn, might lead to entirely new security concerns.

3.2 Achievements & Limitations

Based on the findings of the evaluation of the related work to that topic, it can be seen that a lot of effort has been put into discussing and partially solving usable security issues. Specifically, the following general research achievements can be summarized:

A1 Recognition of the need for more usable security consideration across all human-facing security features, especially outside of end-user applications.

A2 Following from A1, the specific usable security consideration under the domain of CC.

A3 Recognition of prime security issues within the domain of CC outside of the scope of usable security.

A4 Recognition of more efficient usable security assessment.

A5 Following from A3, initial development and partial evaluation of such frameworks under limited scope and generalization.

Following a process of exclusion, the following limitations to that research can be derived:

L1 Despite A1, there is currently little effort to focus on developers and IT professionals in terms of usable security enablement.

L2 Despite A2 and A3, the efforts in terms of usable security in the domain of CC are limited to reinventing security features rather than assessing and improving them from a usable security point of view.

L3 Despite of A4 and A5, there currently does not exist a unified, qualitative usable security assessment framework that CC could benefit from.

With that, the derived limitations can be linked to the problem statements (cf. Section 1.2) and proposed contributions (cf. Section 1.3) of this work, which will be done in the following section.

3.3 Application of Contributions

The following relationship of problems, contributions, as well as current research's achievements and limitations shall finally justify the direction and scope of this work:

- **P1** [tedious usable security evaluation] might benefit from addressing
  L3 [lack of unified assessment framework],
  which will be achieved by sequentially performing
  C1 [applicability evaluation of current frameworks],
  C2 [design of unified framework], and
  C3 [validation of unified framework], aided by input given by
  A5 [suggested frameworks from current research].

- **P2** [CC security incidents due to misconfiguration] might benefit from addressing
  L2 [lack of usable security assessment of CC security features], and inherently
  L1 [little consideration of IT professionals within usable security research],
  which will be achieved by the CC scope inside
  C1 [see above] and
  C3 [see above], aided by input given by
  A2 [initial consideration of CC usable security] and
  A3 [prime security challenges within CC].

The specific approach of solving the mentioned problems through the aspired contributions will be outlined in Chapter 4.

4 Approach

This chapter outlines the necessary steps and methodology that is applied in order to achieve the aspired contributions in terms of the desired research goal of this work (Section 4.1). This approach definition is not meant to be final and makes no claim to be exhaustive. This is because the practical application of this approach is expected to yield results that either not fit the approach or require extension.

Apart from that, this chapter also identifies underlying assumptions required to perform the work (Section 4.2) as well as potential risks to the research and their appropriate countermeasures (Section 4.3)

4.1 Research Structure & Methodology

In essence, the underlying research methodology will follow an experimental and empirical approach that aims to (i) find limitations and challenges in current frameworks, (ii) develop a unified framework that addresses these issues, and finally (iii) validate its applicability and overall benefit after the fact. The specific measures to be undertaken are outlined in the following.

4.1.1 Preparation of Research Environment & Scope

Before pursuing the first contribution of this work, the research environment and scope need to be prepared. Chapters 1 and 3 already established the overall domain under this research will take place, which is Cloud Computing. For that matter, appropriate candidate CC offerings and services must be derived in order to have a finite scope of consideration (referred to as $C_{CC_{ofr}}$ and $C_{CC_{svc}}$, respectively). Similarly, this is also the case for the choice of currently used frameworks that solely consider *either* usability *or* security design or evaluation (referred to as $C_{FW_{use}}$ and $C_{FW_{sec}}$, respectively). Due to limitations in time and scope that come with a Master's thesis, the goal is to have

- three CC offerings (denoted as A, B, and C),
- five CC services (denoted as 1, 2, 3, 4, and 5), as well as
- two current usability, and
- two current security evaluation or design frameworks.

To allow for an independent assessment of the current framework as well as a controllable validation of the unified framework, the following split is suggested, such that

- $A_{CC_{ofr}} \coloneqq \{A, B\} \supset C_{CC_{ofr}}$ defines the assessment set of CC offerings,
- $A_{CC_{svc}} \coloneqq \{1, 2, 3\} \supset C_{CC_{svc}}$ defines the assessment set of CC services,
- $V_{CC_{ofr}} \coloneqq \{B, C\} \supset C_{CC_{ofr}}$ defines the validation set of CC offerings,
- $V_{CC_{svc}} \coloneqq \{2, 3, 4, 5\} \supset C_{CC_{svc}}$ defines the validation set of CC services,
- $K_{CC_{ofr}} \coloneqq A_{CC_{ofr}} \cap V_{CC_{ofr}} = \{B\}$ defines the control set of CC offerings, and
- $K_{CC_{svc}} \coloneqq A_{CC_{svc}} \cap V_{CC_{svc}} = \{2, 3\}$ defines the control set of CC service. Consequently,
- $A_{CC} \coloneqq A_{CC_{ofr}} \times A_{CC_{svc}} = \{A, B\} \times \{1, 2, 3\} = \{A1, A2, A3, B1, B2, B3\}$ defines the CC assessment combination,
- $V_{CC} \coloneqq V_{CC_{ofr}} \times V_{CC_{svc}} = \{B, C\} \times \{2, 3, 4, 5\} = \{B2, B3, \ldots, C4, C5\}$ defines the CC validation combination, and finally
- $K_{CC} \coloneqq K_{CC_{ofr}} \times K_{CC_{svc}} = \{B\} \times \{2, 3\} = \{B2, B3\}$ defines the CC control combination.

The total number and setup of the individual candidates is open to discussion and is merely to support the presentation of the upcoming contributions. The concrete candidate choice criteria will be set up during the actual research phase of this work. However, general choice criteria are briefly outlined in the following:

The choice of offerings will be aided by quantitative indicators (e.g., market share). To allow for comparability, the choice of CC services must be done such that each service is similarly implemented and presented across all CC offerings. These candidates will then, again, be validated through quantitative indicators (e.g., relevance or popularity).

The choice of current frameworks will solely be done based on its degree of establishment in the corresponding area of application, that is, the most-used design or evaluation frameworks used in either the usability or security domain.

The corresponding CC environments will then be set up. These sets of candidates will then serve as the required input for achieving the first contribution C1.

4.1.2 C1: Assessment of Current Framework Applicability

In order to evaluate the applicability of current usability and security design and evaluation frameworks, the candidate sets $C_{FW_{sec}}$ and $C_{FW_{use}}$ will be applied on the CC assessment set A_{CC}. Specifically, every element of A_{CC} will be individually evaluated by means of all frameworks $C_{FW_{sec}}$ and $C_{FW_{use}}$. This yields the following mapping:

$$\mathcal{A} \coloneqq A_{CC} \times (C_{FW_{sec}} \cup C_{FW_{use}}) = \\ \{FW_{sec_1}(A1), \ldots, FW_{sec_1}(B3), FW_{sec_2}(A1), \ldots, FW_{use_1}(A1), \ldots, FW_{use_2}(B3)\}$$

with $\mathcal{A}$ being the entire set of assessments and its elements being individual assessments mappings of offering service candidates and current frameworks. This yields a total of 24 assessments. Each assessment will be performed manually, noting findings in terms of the usable security applicability for the particular case. It is expected to have the following categories of findings:

- pure usability aspects directly related to the application of a usability framework,
- pure usability aspects derived from applying a security framework,
- pure security aspects directly related to the application of a security framework,
- pure security aspects derived from applying a usability framework,
- usable security aspects derived from a usability framework, and
- usable security aspects derived from a security framework.

These categories then yield three applicability degrees:

1. aspects that are applicable without change,
2. aspects that are applicable with change, and
3. aspects that are not applicable at all.

Furthermore, each assessment is expected to aid the subsequent design process of the unified framework (cf. C2) such that relevant aspects that are missing from the current framework can be derived by justified assumption. After performing each evaluation, the findings and insights can be prioritized in terms of their relevance, how often they appeared, etc.

The results from the control group evaluation will be most thoroughly documented as they will serve as additional input to the validation process of the unified framework (cf. C3).

It is expected that certain cloud services' interfaces do not solely include security aspects, which is why the evaluation will only focus on aspects within the usability that is mostly or entirely security-related.

The ultimate design of this proposed assessment will be revised after deciding on the specific CC offerings, services, as well as current frameworks, if necessary. In any case, the output of the total assessment will be subsequently used in the next contribution C2.

4.1.3 C2: Design of Unified Qualitative Usable Security Assessment Framework

The findings from C1 are now applied in order to design the unified qualitative usable security assessment framework, as part of the second contribution.

The design will consider the following findings in order:

1. High-priority aspects from current frameworks that can be taken over without change.
2. High-priority aspects from current frameworks that can be taken over with change.
3. Low-priority aspects from current frameworks that can be taken over without change.

4. Low-priority aspects from current frameworks that can be taken over with change.
5. High-priority aspects derived by justified assumption.
6. Low-priority aspects derived by justified assumption.

After each step, it is validated that the included steps are not redundant to the previously undertaken step. Finally, after performing all steps based on all findings from C1, all aspects are considered in total in terms of consolidation or generalization, if applicable.

Again, the ultimate design of this proposed framework development process will be revised after having the actual assessment of the current frameworks. In any case, this contribution is expected to yield a unified framework that is similar to the mode of application to the previously chosen, current frameworks. This framework is now subject to validation in terms of the third and last contribution C3, outlined in its separate Chapter 5.

4.2 Assumptions & Limitations

As certain limitations might not be clear until the start of the actual Master's thesis development, this list of assumptions and limitations makes no claim to be exhaustive.

Lack of Budget At the time of creating this research proposal, it is expected that the research to-be-conducted will not receive any financial support which might be beneficial to the evaluation of paid services or offerings. This limits the choice of CC offerings and services to free-tier availability.

Positioning of HPE This research is conducted in cooperation with the author's employer and requires that their CC offering is taken into account. Therefore, one of the supposedly three CC offerings must be covered by *HPE GreenLake*.

Operational Correctness & Integrity As this research does not aim at revealing operational issues of the chosen CC offerings or services, it is expected that the deployments perform as intended by the provider.

Agnostic Implementation In order to allow for general applicability across CC offerings, this research does not differentiate between CC deployment models for the assessment, development, and validation of the framework(s). Thus, it assumes that the implementation of service configuration interfaces as well as of underlying security features is generally similar.

Framework Design The choice of current frameworks is limited to heuristics, guidelines, or principles that do not explicitly define the approach on how they are applied. The goal is to create a unified framework that can be applied on various application approaches and settings (e.g., both moderated *and* unmoderated). This leads to the research not being validated by actual users as the design of application scenarios of the unified framework lies outside the scope of this work.

Overall, further limitations to the scope and complexity of this proposed research are expected as for the given nature of Master's thesis, that is, a limited working time frame of six months, a generally limited amount of content pages (approx. 60-80 pages), and the fact that the work is conducted in a cooperative study manner next to a full-time employment as given by the study program of the HECTOR School.

4.3 Risk to the Research & Mitigation

As certain risks to this proposed work might not be clear until the start of the actual Master's thesis development, this list of risks and risk mitigations makes no claim to be exhaustive. It does also not contain superior risks outside of the scope of the research and outside the control of the stakeholders (e.g., sickness, emergency situations, etc.).

Misrepresentation of Research Novelty The analysis of the related work (cf. Chapter 3) has been and will be done to the best of the author's knowledge and belief, especially in terms of describing the present research's limitations. However, it is possible that relevant work is disregarded (e.g., due to unavailability, etc.) that might render this research's contributions less novel than they were expected. In that case, this will be remedied through scope readjustment.

Misinterpretation of Complexity During the practical application of the research approach (cf. Section 4.1), it is possible that intermediate results yield (i.a.) the unexpected applicability of current frameworks in terms usable security, or, in contrast, their absolute inapplicability, which could distort the expected value of this research. Again, this will be remedied by means of research scope readjustment.

5 Evaluation (C3)

The validation of the unified framework is expected to assess its validity and benefits compared to current frameworks as well as overall evaluate the success of this research. It also defines the final contribution C3 of this work. This will be done in two steps; (i) the validation by means of the control set K_{CC} as well as by means of the remaining feature set V_{CC}.

As the control set features have already been assessed by means of the current frameworks, this form of validation can evaluate efficiency, conclusivity, and applicability in comparison to those frameworks. Since these features have been used to design the framework, there is the risk that it is rather tailored to the particular feature set rather than generally applicable (i.e., *overfitting*). For that, the remaining validation set is used. Even though it cannot compare its outcome with current frameworks, it can validate if the unified framework is generally applicable, efficient and conclusive outside of its design space (i.e., specific cloud offerings *and* services. In short:

Comparison of Operation $\mathcal{K}_c := K_{CC} \times (C_{FW_{sec}} \cup C_{FW_{use}}) = \{FW_{sec_1}(B2), \ldots, FW_{use_2}(B3)\}$ compared with $\mathcal{K}_u := K_{CC} \times FW_u = \{FW_u(B2), FW_u(B3)\}$

Validation of General Applicability $\mathcal{V} := (V_{CC} \backslash K_{CC}) \times FW_u = \{FW_u(B4), FW_u(B5), FW_u(C2), FW_u(C3), FW_u(C4), FW_u(C5)\}$,

with $\mathcal{K}_c$ being the control set assessment of current frameworks, $\mathcal{K}_u$ being the control set assessment of the unified framework, and FW_u being the unified framework application.

Again, as with previous contributions, the ultimate design of this proposed evaluation process will be revised after having the actual framework design in place. This is because the nature of a qualitative framework complicates performing a quantifiable evaluation. In any case, this evaluation will conclude the work by answering whether this unified framework actually solves (or, at least, partially addresses) the underlying problems of this thesis (i.e., slow case-by-case approach for usable security research as well as little consideration of non-end-users), critically consider shortcomings of the developed framework, and finally suggest further research in that particular area.

6 Organization

6.1 Research Stakeholders

The Master's thesis will be conducted by **Oliver Rudzinski** (oliver.rudzinski@hpe.com).

KIT affiliation M.Sc. Candidate for Information Systems Engineering and Management at the HECTOR School of Engineering and Management (Technology Business School of the KIT)

HPE affiliation Infrastructure Technology Architect for the *Value Solutions* department at the Hewlett Packard Enterprise Sales Center GmbH in Berlin, Germany.

The following stakeholders affiliated with the Karlsruhe Institute of Technology are identified.

Reviewer Prof. Dr. Ralf Reussner (ralf.reussner@kit.edu)

Second Reviewer Dr. Robert Heinrich (robert.heinrich@kit.edu)

Additionally, as the Master's thesis will be conducted in cooperation with the author's employer, the following stakeholder(s) affiliated with HPE are identified.

Manager Markus Leitzgen | Inside Sales Manager *Value Solutions* (markus.leitzgen@hpe.com)

It shall be noted that additional subject-matter experts, closely related to the HPE GreenLake business unit, might be brought in for supporting purposes, or out of interest to their business.

6.2 Artefacts

This section outlines the artefacts that are expected to be developed during the process of the Master's thesis. This research proposal document serves as the first artefact. The Master's thesis documentation itself will contain the following artefacts:

- description of foundational background to this work (as prepared in Chapter 2)
- analysis and discussion of related work in the underlying research area (as prepared in Chapter 3)
- definition of research scope by means of CC offerings, services, usability, and security frameworks as well as their classification into assessment, control, and validation sets (as described in Subsection 4.1.1)

- quantified assessment documentation of current frameworks (coinciding with C1, as described in Subsection 4.1.3)
- unified framework definition (coinciding with C2, as described in Subsection 4.1.3)
- evaluation of framework and total research approach (coinciding with C3, as described in Chapter 5)

The preliminary versions of these artefacts will be summarized in a presentation that will be held during the thesis' colloquium 4-6 weeks prior to submission. The corresponding presentation slides serve as another artefact to this research.

In case any source code or configuration files are created during the evaluation process of this research, they will be included in adequate manner.

Furthermore, it is expected that the findings of this research will also be presented to an interested audience at HPE, which lies outside of the scope of the formal valuation of the thesis.

6.3 Work Schedule

According to the Master's thesis information sheet issued by the HECTOR School, the extent of the Master's thesis for the study program *Information Systems Engineering and Management* is described by 20 ECTS points that correspond to a workload of 600 hours and a development time frame of six months. At the time of this proposal, the official starting date is not yet confirmed. In any case, for the first five months of the thesis development, a rough work capacity of 25 hours per week is expected, which will be increased to 50 hours per week in the last month, excluding the time frames of the remaining HECTOR school modules. This is taken into account for the specific planning of the milestones.

The desired starting date of the thesis development corresponds to the **1st of October 2022**, which yields the submission date of the **31st of March 2023**.

It is highly desired to have regular update and mentoring sessions with the reviewers and remaining stakeholders of this research.

6.3.1 Work Packages

The work packages of this research roughly coincide with the proposed research approach (cf. Chapter 4) and evaluation (cf. Chapter 5).

The preparation work phase (phase 1, cf. Subsection 4.1.1) aims at developing criteria for choosing appropriate CC offerings and services, followed by deciding on the corresponding elements for this research. Subsequently, this is also done to current security and usability assessment frameworks. Finally, the assessment, validation, and control sets are defined as well as the corresponding CC environments prepared. Phase 1 is overlapped by the permanent documentation phase in that the preparatory work is documented as well as the Foundations chapter refined.

Phase 1 flows into the assessment phase of current frameworks (phase 2, cf. Subsection 4.1.2). Before starting with the actual assessment, its proposed approach is refined as well as relevant assessment KPIs defined. Then, the assessments are performed. Findings are derived in parallel to the assessments, and finalized by means of a total assessment insight priorization. As before, the documentation phase overlaps in that the entire process is documented. Related Work refinement is also done in that phase.

Phase 2 then flows into the design phase of the unified framework (phase 3, cf. Subsection 4.1.3) with the evaluation of the total findings from phase 2. With that, the framework design approach can be refined, if necessary, that is subsequently used for the actual development of the unified framework. Upon finalizing the framework, it is thoroughly examined in terms of redundancy, possibility of abstraction, etc. Again, the documentation phase runs in parallel by documenting the design approach refinement as well as the actual process of framework development. Further potential Foundations and Related Work refinement is also done in that phase.

Phase 3 flows into the last practical work phase of evaluating the new framework as well as the entire approach (phase 4, cf. Chapter 5). This, again, starts with a potential refinement of the evaluation strategy, followed by the comparative evaluation by means of the control set as well as the validation of general applicability via the validation set. Again, the evaluation is documented in parallel.

Phase 4 finally flows into the now solely present documentation phase. Here, the preliminary documentation is refined in terms of structure, wording, conciseness, etc., resulting in a first completed draft that will be presented during this thesis' colloquium. The feedback received during the presentation will finally be applied to the work, before final proof reading and formatting takes place. Finally, the thesis is completed, printed, and submitted for grading.

6.3.2 Milestones

The milestones of this work generally coincide with the end of each major work phase and work artefacts, which are defined as follows:

Phase 1 completed choice of CC offerings, services, and current framework candidates and corresponding mappings into assessment, validation, and control sets

Phase 2 derived findings and insights on current framework assessment in terms of usable security

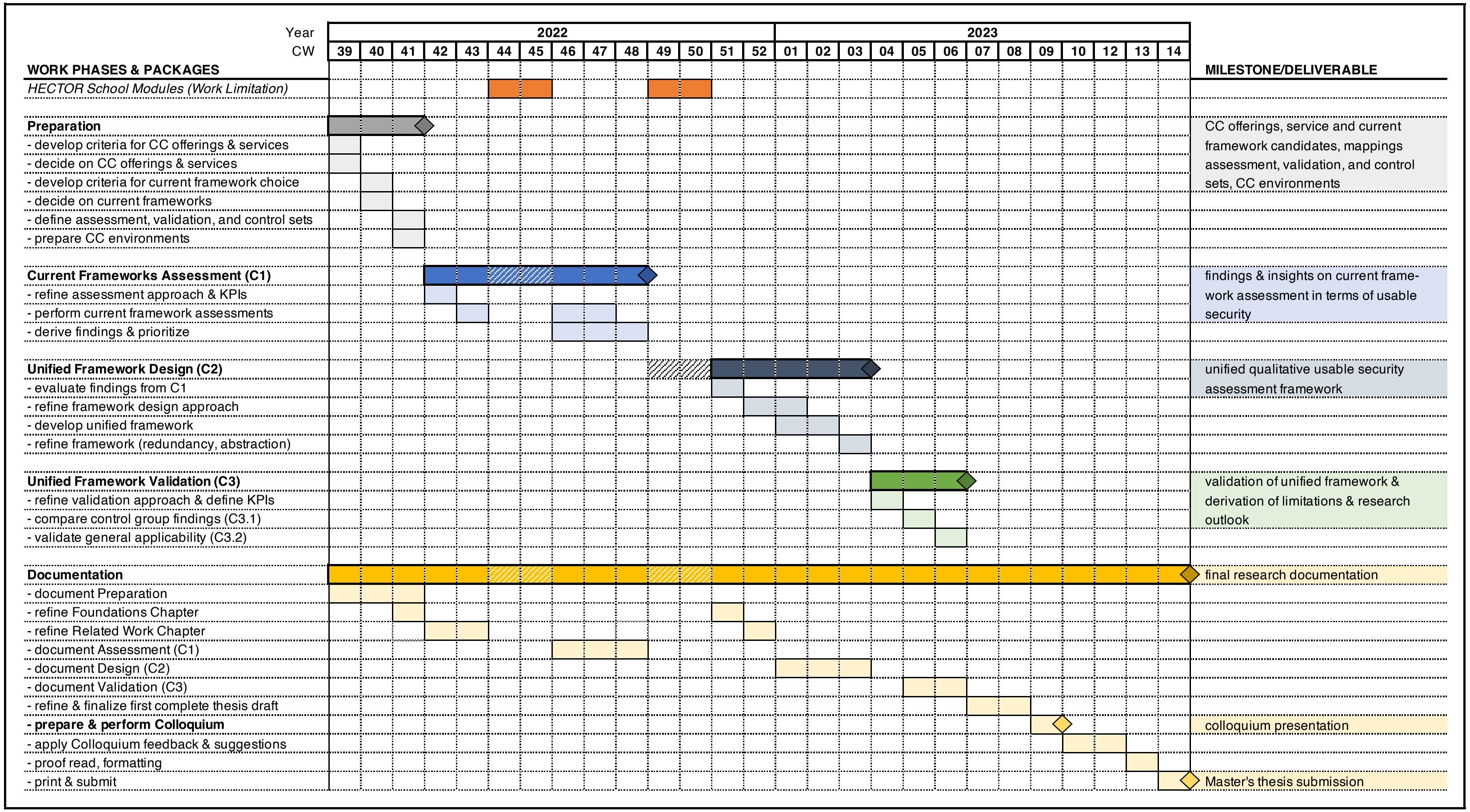
Phase 3 final definition of unified qualitative usable security assessment framework

Phase 4 final findings of unified framework and total research evaluation, as well as final derivation of limitations and research outlook

Documentation Phase divided into two milestones: (i) perform colloquium presentation, as well as (ii) submission of Master's thesis

In Subsection 6.3.3 on the next page, a GANTT chart represents the described work phases and corresponding milestones of the Master's thesis development.
This concludes the research proposal.

6.3.3 GANTT Chart



Year	2022														2023													
CW	39	40	41	42	43	44	45	46	47	48	49	50	51	52	01	02	03	04	05	06	07	08	09	10	12	13	14	
WORK PHASES & PACKAGES																												**MILESTONE/DELIVERABLE**
HECTOR School Modules (Work Limitation)						■	■				■	■																
Preparation	■	■	■◆																									CC offerings, service and current framework candidates, mappings assessment, validation, and control sets, CC environments
- develop criteria for CC offerings & services	■																											
- decide on CC offerings & services	■																											
- develop criteria for current framework choice		■																										
- decide on current frameworks		■																										
- define assessment, validation, and control sets			■																									
- prepare CC environments			■																									
Current Frameworks Assessment (C1)				■	■	▨	▨	■	■	■◆																		findings & insights on current framework assessment in terms of usable security
- refine assessment approach & KPIs				■																								
- perform current framework assessments					■			■	■																			
- derive findings & prioritize								■	■	■																		
Unified Framework Design (C2)											▨	▨	■	■	■	■	■◆											unified qualitative usable security assessment framework
- evaluate findings from C1													■															
- refine framework design approach														■	■													
- develop unified framework															■	■												
- refine framework (redundancy, abstraction)																	■											
Unified Framework Validation (C3)																		■	■	■◆								validation of unified framework & derivation of limitations & research outlook
- refine validation approach & define KPIs																		■										
- compare control group findings (C3.1)																			■									
- validate general applicability (C3.2)																				■								
Documentation	■	■	■	■	■	▨	▨	■	■	■	▨	▨	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■◆	final research documentation
- document Preparation	■	■	■																									
- refine Foundations Chapter			■										■															
- refine Related Work Chapter				■	■									■														
- document Assessment (C1)								■	■	■																		
- document Design (C2)															■	■	■											
- document Validation (C3)																			■	■								
- refine & finalize first complete thesis draft																					■	■						
- prepare & perform Colloquium																							■◆					colloquium presentation
- apply Colloquium feedback & suggestions																								■	■			
- proof read, formatting																										■		
- print & submit																											■◆	Master's thesis submission

Bibliography

[1] *2021 State of the Cloud Report.* Tech. rep. Flexera, 2021. URL: https://resources.flexera.com/web/pdf/report-cm-state-of-the-cloud-2021.pdf (visited on 09/24/2022).

[2] *2022 Cloud Security Report.* Tech. rep. ISC2, 2022. (Visited on 09/24/2022).

[3] Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. “You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users”. In: *2016 IEEE Cybersecurity Development (SecDev).* Nov. 2016, pp. 3–8. DOI: 10.1109/SecDev.2016.013.

[4] Anne Adams and Martina Angela Sasse. “Users are not the enemy”. In: *Communications of the ACM* 42.12 (Dec. 1999), pp. 40–46. ISSN: 0001-0782. DOI: 10.1145/322796.322806. (Visited on 09/23/2022).

[5] Sameera Abdulrahman Almulla and Chan Yeob Yeun. “Cloud computing security management”. In: *2010 Second International Conference on Engineering System Management and Applications.* Mar. 2010, pp. 1–7.

[6] Stephen Ambore, Huseyin Zekeriya Dogan, and Edward Apeh. “Development of Usable Security Heuristics for Fintech”. In: (July 2021). Publisher: BCS Learning & Development. DOI: 10.14236/ewic/HCI2021.12. URL: https://www.scienceopen.com/hosted-document?doi=10.14236/ewic/HCI2021.12 (visited on 09/23/2022).

[7] Deanna D. Caputo et al. “Barriers to Usable Security? Three Organizational Case Studies”. In: *IEEE Security & Privacy* 14.5 (Sept. 2016). Conference Name: IEEE Security & Privacy, pp. 22–32. ISSN: 1558-4046. DOI: 10.1109/MSP.2016.95.

[8] Sonia Chiasson, Robert Biddle, and Anil Somayaji. “Even experts deserve usable security: Design guidelines for security management systems”. In: *In SOUPS Workshop on Usable IT Security Management (USM.* 2007.

[9] Sonia Chiasson, Robert Biddle, and Anil Somayaji. “Even experts deserve usable security: Design guidelines for security management systems”. In: *SOUPS Workshop on Usable IT Security Management (USM).* 2007. URL: https://cups.cs.cmu.edu/soups/2007/workshop/Design_Guidelines.pdf (visited on 09/26/2022).

[10] *Cost of a Data Breach. Report 2022.* Tech. rep. Armonk, NY: IBM Corporation, July 2022. URL: https://www.ibm.com/security/data-breach (visited on 09/24/2022).

[11] *Cybersecurity Market - Growth, Trends, Covid-19 Impact, and Forecasts (2022 - 2027).* Tech. rep. Mordor Intelligence, 2022. URL: https://www.mordorintelligence.com/industry-reports/cyber-security-market (visited on 09/24/2022).

[12] *Ergonomics of human-system interaction — Part 110: Interaction principles.* Tech. rep. ISO 9241-110:2020(en). International Organization for Standardization, 2020. URL: `https://www.iso.org/obp/ui/#iso:std:iso:9241:-110:ed-2:v1:en` (visited on 09/25/2022).

[13] *Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems.* Tech. rep. ISO 9241-210:2019(en). International Organization for Standardization, 2019. URL: `https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-2:v1:en` (visited on 09/25/2022).

[14] Sascha Fahl et al. "Confidentiality as a Service – Usable Security for the Cloud". In: *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.* ISSN: 2324-9013. June 2012, pp. 153–162. DOI: `10.1109/TrustCom.2012.112`.

[15] Dennis Felsch et al. "How Private is Your Private Cloud? Security Analysis of Cloud Control Interfaces". In: *Proceedings of the 2015 ACM Workshop on Cloud Computing Security Workshop.* CCSW '15. New York, NY: Association for Computing Machinery, Oct. 2015, pp. 5–16. ISBN: 978-1-4503-3825-7. DOI: `10.1145/2808425.2808432`. URL: `https://doi.org/10.1145/2808425.2808432` (visited on 09/26/2022).

[16] Denis Feth, Andreas Maier, and Svenja Polst. "A User-Centered Model for Usable Security and Privacy". In: *Human Aspects of Information Security, Privacy and Trust.* Ed. by Theo Tryfonas. Lecture Notes in Computer Science. Cham, CH: Springer International Publishing, 2017, pp. 74–89. ISBN: 978-3-319-58460-7. DOI: `10.1007/978-3-319-58460-7_6`.

[17] Simone Fischer-Hübner. *IT-Security and Privacy.* Lecture Notes in Computer Science 1958. Berlin, DE. Heidelberg, DE. New York, NY.: Springer, 2001. ISBN: 3-540-42142-4.

[18] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.* Tech. rep. NIST CSWP 04162018. Gaithersburg, MD: National Institute of Standards and Technology, Apr. 2018. DOI: `10.6028/NIST.CSWP.04162018`. URL: `http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf` (visited on 09/25/2022).

[19] Simson Garfinkel and Heather Richter Lipford. *Usable Security: History, Themes, and Challenges.* Cham, CH: Springer International Publishing, 2014. ISBN: 978-3-031-01215-0 978-3-031-02343-9. DOI: `10.1007/978-3-031-02343-9`. URL: `https://link.springer.com/10.1007/978-3-031-02343-9` (visited on 09/24/2022).

[20] Matthew Green and Matthew Smith. "Developers are Not the Enemy!: The Need for Usable Security APIs". In: *IEEE Security & Privacy* 14.5 (Sept. 2016). Conference Name: IEEE Security & Privacy, pp. 40–46. ISSN: 1558-4046. DOI: `10.1109/MSP.2016.111`.

[21] Keiko Hashizume et al. "An analysis of security issues for cloud computing". In: *Journal of Internet Services and Applications* 4.1 (Feb. 2013), p. 5. ISSN: 1869-0238. DOI: `10.1186/1869-0238-4-5`. URL: `https://doi.org/10.1186/1869-0238-4-5` (visited on 09/26/2022).

[22] Yasser M. Hausawi and William H. Allen. “Usable-Security Evaluation”. In: *Human Aspects of Information Security, Privacy, and Trust.* Ed. by Theo Tryfonas and Ioannis Askoxylakis. Vol. 9190. Series Title: Lecture Notes in Computer Science. Cham, CH: Springer International Publishing, 2015, pp. 335–346. ISBN: 978-3-319-20375-1 978-3-319-20376-8. DOI: `10.1007/978-3-319-20376-8_30`. URL: `http://link.springer.com/10.1007/978-3-319-20376-8_30` (visited on 09/25/2022).

[23] Markus Lennartsson, Joakim Kävrestad, and Marcus Nohlberg. “Exploring the Meaning of “Usable Security””. In: *Human Aspects of Information Security and Assurance.* Ed. by Nathan Clarke and Steven Furnell. IFIP Advances in Information and Communication Technology. Cham, CH: Springer International Publishing, 2020, pp. 247–258. ISBN: 978-3-030-57404-8. DOI: `10.1007/978-3-030-57404-8_19`.

[24] *Malware increased by 358% in 2020.* Help Net Security. Feb. 2021. URL: `https://www.helpnetsecurity.com/2021/02/17/malware-2020/` (visited on 09/24/2022).

[25] Sheeja Shaji Manakattu, Shivakumar Murugesh, and Rajashekhar Ningappa Hirekurabar. “Security Landscape for Private Cloud”. In: *Inventive Computation Technologies.* Ed. by S. Smys, Robert Bestak, and Álvaro Rocha. Lecture Notes in Networks and Systems. Cham, CH: Springer International Publishing, 2020, pp. 67–78. ISBN: 978-3-030-33846-6. DOI: `10.1007/978-3-030-33846-6_8`.

[26] Paul Mee and Rico Brandenburg. *After reading, writing and arithmetic, the 4th ’r’ of literacy is cyber-risk.* World Economic Forum. Dec. 2020. URL: `https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education/` (visited on 09/24/2022).

[27] Peter Mell and Timothy Grance. *The NIST Definition of Cloud Computing.* Tech. rep. NIST SP 800-145. Gaithersburg, MD: National Institute of Standards and Technology, Sept. 2011, p. 7.

[28] Kate Moran. *Usability Testing 101.* Nielsen Norman Group. Dec. 2019. URL: `https://www.nngroup.com/articles/usability-testing-101/` (visited on 09/24/2022).

[29] Michael Nieles, Kelley Dempsey, and Victoria Yan Pillitteri. *An introduction to information security.* Tech. rep. NIST SP 800-12r1. Gaithersburg, MD: National Institute of Standards and Technology, June 2017. DOI: `10.6028/NIST.SP.800-12r1`. URL: `https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf` (visited on 09/25/2022).

[30] Jakob Nielsen. *10 Usability Heuristics for User Interface Design.* en. Apr. 1994. URL: `https://www.nngroup.com/articles/ten-usability-heuristics/` (visited on 09/24/2022).

[31] Donald A. Norman. *The design of everyday things.* 3rd ed. Philadelphia, PA: Basic Books, 2013. ISBN: 978-0-465-05065-9.

[32] Simon Parkin et al. “A stealth approach to usable security: helping IT security managers to identify workable security solutions”. In: *Proceedings of the 2010 New Security Paradigms Workshop.* NSPW ’10. New York, NY: Association for Computing Machinery, Sept. 2010, pp. 33–50. ISBN: 978-1-4503-0415-3. DOI: `10.1145/1900546.1900553`. URL: `https://doi.org/10.1145/1900546.1900553` (visited on 09/23/2022).

[33] Napoleon C. Paxton. “Cloud Security: A Review of Current Issues and Proposed Solutions”. In: *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*. Nov. 2016, pp. 452–455. DOI: `10.1109/CIC.2016.066`.

[34] Christian Reuter, Luigi Lo Iacono, and Alexander Benlian. “A quarter century of usable security and privacy research: transparency, tailorability, and the road ahead”. In: *Behaviour & Information Technology* 41.10 (July 2022), pp. 2035–2048. ISSN: 0144-929X, 1362-3001. DOI: `10.1080/0144929X.2022.2080908`. URL: `https://www.tandfonline.com/doi/full/10.1080/0144929X.2022.2080908` (visited on 09/25/2022).

[35] J.H. Saltzer and M.D. Schroeder. “The protection of information in computer systems”. In: *Proceedings of the IEEE* 63.9 (Sept. 1975). Conference Name: Proceedings of the IEEE, pp. 1278–1308. ISSN: 1558-2256. DOI: `10.1109/PROC.1975.9939`.

[36] Holger Schulze. *Cloud Security Report 2022*. Tech. rep. Cybersecurity Insiders, 2022. URL: `https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/the-biggest-cloud-security-challenges-in-2022/` (visited on 09/24/2022).

[37] Naresh Kumar Sehgal and Pramod Chandra P. Bhatt. *Cloud Computing: Concepts and Practices*. Cham, CH: Springer International Publishing, 2018. ISBN: 978-3-319-77838-9 978-3-319-77839-6. DOI: `10.1007/978-3-319-77839-6`. URL: `https://link.springer.com/10.1007/978-3-319-77839-6` (visited on 09/25/2022).

[38] Ben Shneiderman et al. *Designing the user interface: strategies for effective human-computer interaction*. 6th ed. Boston, MA: Pearson, 2018. ISBN: 978-1-292-15391-9.

[39] Ashish Singh and Kakali Chatterjee. “Cloud security issues and challenges: A survey”. In: *Journal of Network and Computer Applications* 79 (Feb. 2017), pp. 88–115. ISSN: 1084-8045. DOI: `10.1016/j.jnca.2016.11.027`. URL: `https://www.sciencedirect.com/science/article/pii/S1084804516302983` (visited on 09/26/2022).

[40] Mary Theofanos. “Is Usable Security an Oxymoron?” In: *Computer* 53.2 (Feb. 2020), pp. 71–74. ISSN: 1558-0814. DOI: `10.1109/MC.2019.2954075`. (Visited on 09/25/2022).

[41] Alma Whitten and J. D. Tygar. “Why Johnny Can’t Encrypt: A Usability Evaluation of {PGP} 5.0”. en. In: 1999. URL: `https://www.usenix.org/conference/8th-usenix-security-symposium/why-johnny-cant-encrypt-usability-evaluation-pgp-50` (visited on 09/23/2022).

[42] Zhang Yandong and Zhang Yongsheng. “Cloud computing and cloud security challenges”. In: *2012 International Symposium on Information Technologies in Medicine and Education*. Vol. 2. Aug. 2012, pp. 1084–1088. DOI: `10.1109/ITiME.2012.6291488`.

[43] Mary Ellen Zurko and Richard T. Simon. “User-centered security”. In: *1996 workshop on New security paradigms - NSPW ’96*. Lake Arrowhead, CA: ACM Press, 1996, pp. 27–33. ISBN: 978-0-89791-944-9. DOI: `10.1145/304851.304859`. URL: `http://portal.acm.org/citation.cfm?doid=304851.304859` (visited on 09/23/2022).