Cyber Security for Europe

D3.4

Analysis of key research challenges for adaptive security

Document Identification	
Due date	31st January 2020
Submission date	31st January 2020
Revision	2.00 (20 July 2020)

Related WP	WP3	Dissemination Level	PU
Lead Participant	UCD/Lero	Lead Author	Liliana Pasquale (UCD)
Contributing Beneficiaries	KUL, ATOS, UPRC, UM, UPS-IRIT, CNR, VTT, UniTN	Related Deliverables	D5.1

Abstract: This task will explore the development of flexible security solutions that can quickly adapt security controls in response to security changes such as new attacks or changes in security requirements. To improve the modelling and analysis of dynamic systems, we will provide tools and techniques to support elicitation and representation of assets, security requirements and threats, focusing on interconnected systems in various domains (e.g., cloud systems and Internet of Things). This task will also provide scalable architectures supporting security situation computation and risk assessment, and also selection and deployment of security controls that could satisfy security requirements and policies, also enabling awareness of the current system status. Finally, the acceptance of adaptive systems by stakeholders will be addressed developing techniques to provide explanations (assurances) about why certain security controls should be adapted.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

In this deliverable we aim to identify key research challenges for adaptive security. To achieve this aim we performed a systematic literature review surveying existing research on adaptive security. We used the maritime transport use cases described in deliverable D5.1 to elicit the research questions of this survey.

This survey poses three types of research questions related to the role of the application domain, the stakeholders, and the requirements in adaptive security. First, we investigate the application domains where adaptive security systems have been deployed. Second, we identify all involved stakeholders of adaptive security systems, their role in the development and use of such systems, and the types of artifacts/information they receive to explain system decisions. Finally, we assess whether and how adaptive security objectives influence the design and implementation of an adaptive security system.

The literature review allowed us to identify trends, patterns and gaps in existing research and provide a set of recommendations for future research directions for adaptive security systems.

Document information

Contributors

Name	Partner
Liliana Pasquale	UCD
Dimitri Van Landuyt	KUL
Manuel Cheminod, Luca Durante	CNR
Abdelmalek Benzekri	UPS-IRIT
Panayotis Kotzanikolaou, Spyros Papastergiou	UPRC
Rodrigo Diaz, Susana Gonzalez Zarzosa	ATOS
Marko Kompara	UM

Reviewers

Name	Partner
Ivan Pashchenko	UniTN
Kimmo Halunen	VTT
Ahad Niknia (High-level review)	GUF

History

0.01	2019-08-01	Liliana Pasquale	1st Draft
0.02	2019-10-18	Liliana Pasquale, Dimitri Van Landuyt, Manuel Cheminod, Luca Durante, Abdelmalek Benzekri, Panayotis Kotzanikolaou, Spyros Papastergiou, Rodrigo Diaz, Marko Kompara	2nd Draft – Research Questions
0.03	2019-11-15	Liliana Pasquale, Dimitri Van Landuyt, Manuel Cheminod, Luca Durante, Abdelmalek Benzekri, Panayotis Kotzanikolaou, Spyros Papastergiou, Rodrigo Diaz, Marko Kompara	3rd Draft – Motivating Case Study
0.1	2020-01-07	Liliana Pasquale	4th Draft –Literature review
0.2	2020-01-17	Liliana Pasquale	5th Draft –Literature review results
0.3	2020-01-24	Liliana Pasquale	6th Draft – Recommendations
1.0	2020-01-29	Liliana Pasquale, Dimitri Van Landuyt, Manuel Cheminod, Luca Durante, Abdelmalek Benzekri, Panayotis Kotzanikolaou, Spyros Papastergiou, Rodrigo Diaz, Marko Kompara	7th Draft - Revision
2.0	2020-07-20	Liliana Pasquale	Improved conclusion with future work including survey with industry practitioners. Fixed typos, broken links and formatting issues.

List of Contents

List of Figures

1 Introduction

1.1 Motivation

In the last years we have seen an increasing amount of large-scale, severe breaches, such as the Equifax breach in 2017 [1] or the Marriot breach in 2018 [2]. Such events pose huge costs to organizations and governments. For example, the average cost of cybercrime by consequence of the attack in 2018 was estimated to amount to $13 million [4]. Cyber attacks can also threaten critical infrastructure and disrupt individual's lives [5]. For example, in October 2016, the Mirai botnet caused disruptions of major sites such as Etsy and Twitter [3]. Although security has been considered a critical concern during the design and development of modern software systems, the number and severity of cyber security incidents is expected to increase in the next years [6].

One of the reasons behind this is that software systems are traditionally developed by enacting static security controls. However, unanticipated changes can occur in the environment where the system operates (e.g., new assets require to be protected), in the system itself (previously unknown vulnerabilities are discovered) and/or in the security properties (i.e. confidentiality, integrity, availability and accountability (CIAA) [11]) that a system must satisfy. These changes may render ineffective the security controls deployed, making the system more vulnerable to potential attacks. Note that although security controls support the satisfaction of security properties, they can negatively affect other requirements, such as usability and performance. Thus, different approaches have been proposed in previous research to build *adaptive security systems* [7], which can *self-protect* [8] from the varying risk of harm by adjusting their security controls, in a way that minimally impacts other system requirements.

Surveys [9][10][15] about adaptive security systems demonstrate that existing research in this domain has been fairly recent. Existing surveys have mainly focused on how adaptive security systems are designed and implemented, without considering other important dimensions such as the *who* and *why* dimensions. The "who" dimension covers the interactions that an adaptive security system has with its stakeholders who design, build, use, and certify it. While, the "why" dimension covers the objectives that an adaptation of security controls should achieve. Also, existing surveys focus on adaptive security systems proposed for purely software and large-scale systems, without considering the application domains where adaptive security systems have been adopted.

1.2 Assumptions and General Objective

In this deliverable we aim to identify the gaps in engineering adaptive security systems more systematically. The objective of this deliverable is three-fold. First, we aim to clearly identify all involved stakeholders of adaptive security systems, their role in the development and use of such systems, and the types of artifacts/information they receive to explain system decisions. Second, we aim to assess whether and how adaptive security objectives influence the design and implementation of an adaptive security system. Finally, we aim to investigate the application domains where adaptive security systems have been deployed. This deliverable has the main contribution of surveying adaptive security systems from a "requirements engineering" perspective where stakeholders, adaptive security objectives, and application domains are considered explicitly. We also identify trends, patterns and gaps in existing research and provide a set of recommendations for future research directions for adaptive security systems. To perform our survey, we have followed a systematic literature review process, similar to the one proposed by Kitchenham [13] .

1.3 Participants

The deliverable was led by Liliana Pasquale (UCD) and was collaboratively edited by Dimitri Van Landuyt (KUL), Manuel Cheminod and Luca Durante (CNR), Abdelmalek Benzekri (UPS-IRIT), Panayotis Kotzanikolaou, and Spyros Papastergiou (UPRC), Rodrigo Diaz and Susana Gonzalez Zarzosa (ATOS), and Marko Kompara (UM).

1.4 Organization of the Deliverable

The rest of the deliverable is organized as follows. Section 2 provides a motivating example to introduce the research questions investigated in the survey. Section 3 illustrates the systematic literature review protocol adopted for the survey. Section 4 describes the application domains where adaptive security research has been applied. Section 5 characterizes how stakeholders have been involved in the engineering and execution of an adaptive security system. Section 6 explains the role of adaptive security objectives with respect to the techniques and approaches that have been adopted to engineer decision-making activities of an adaptive security system. Section 7 provides recommendations for future research in the domain of adaptive security. Section 8 concludes.

2 Motivating Example, Reference Architecture, and Research Questions

This section provides a motivating example for adaptive security and describes a reference architecture for adaptive security systems that is used to introduce the research questions that are investigated in this deliverable.

2.1 The Maritime Transport Example

Our motivating example is inspired by the maritime transport use cases and demonstrator that are being developed in Task 5.5. For reasons of simplicity, here we just provide a version of the use cases that is simplified specifically to elicit the research questions of this survey. Figure 1 represents some of the components that are part of the maritime transport use cases and demonstrator considered in this deliverable. Modern vessels include various software-controlled and interconnected systems that are critical for proper vessel operation. The vessel crew accesses the Internet at ports or via satellite connectivity to use a variety of services, such as medical and navigation services. The vessel is also equipped with sensors such as cameras, water temperature and depth sensors to obtain and transmit meteorological and hydrological information over the network. Availability of Internet connectivity via satellite and/or other wireless communication increases the vulnerability of the ship. For example, vulnerabilities in the network can be exploited by malicious individuals in nearby vessels and/or ports, for example, to tamper with the sensors readings or provide incorrect navigation information. This can ultimately harm the integrity of not only the vessel, the safety of crew and the passengers, but also at the larger scale the integrity of the overall management and communication systems between vessels and ports. Therefore, proximity to other vessels and/or the port may increase the risk of harm and may require, for example, to adopt stronger encryption techniques to transmit sensors' information and/or verify authenticity of received information.

Passenger servicing and management systems are software systems used for passengers' limited (for example, only during boarding). Moreover, such information should not be stored in tablets and digital devices used by the crew. Stronger authentication and access control to passenger information should be implemented, especially when the vessel is close to the port and/or other vessels, or there are passengers onboard with a profile that can suggest illegal, criminal and/or terrorist intent [16]. Finally, access to different areas of the vessel can be monitored to ensure physical security of the vessel and its cargo. Malicious passengers can exploit vulnerabilities in the onboard computer network or passengers' management systems to disable the access control system, in order to reach restricted areas unnoticed or cause physical damage to the ship and/ or its cargo. To mitigate these threats, it may be possible to temporarily enact default access control policies when, for example passengers are discovered to roam in restricted areas.

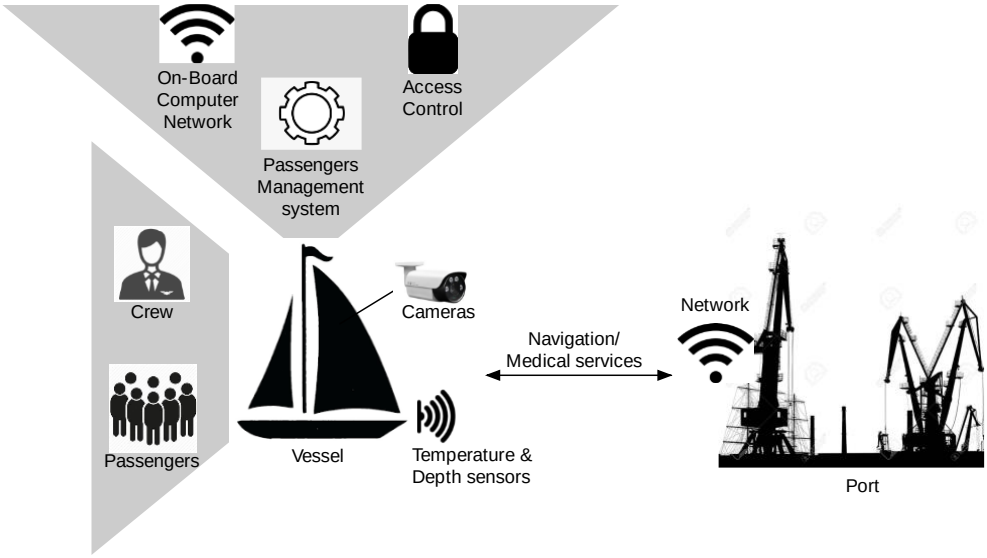

Figure 1: Components of the Maritime Transport Use Cases and Demonstrator.

In the above scenarios different changes in the system operating environment require to modify the set of security controls applied to the vessel, in order to protect a variety of assets. Changes can occur in the cyberspace where the system operates. Examples of such changes include discovery of previously unknown vulnerabilities and transmission of passengers' sensitive information over the network. Changes can also occur in the physical space where the vessel operates. Examples of such changes include proximity to other vessels or ports, presence of passengers with a suspicious profile onboard, or movement of passengers. Security goals to be satisfied include the availability of these systems (resilience against deliberate attacks), the integrity of the vessel and the transported passengers and cargo, integrity of navigation services, and confidentiality of passengers' information. Different security controls are adopted to achieve different adaptive security objectives, such as *preventing* harm to the system, the vessel and the passenger information, and *mitigating* situations in which the vessel and/or its cargo can be subjected to physical damage.

2.2 A Reference Architecture for Adaptive Security

As shown with the maritime transportation example, it is often not possible to anticipate how security threats can materialize and thus appropriate security countermeasures to prevent them cannot be selected at design time. In contrast, software systems such as these that face unanticipated security threats have to be designed and architected in such a way that they can fundamentally adapt their security countermeasures dynamically, to continue to satisfy some security goals at runtime, i.e. during execution.

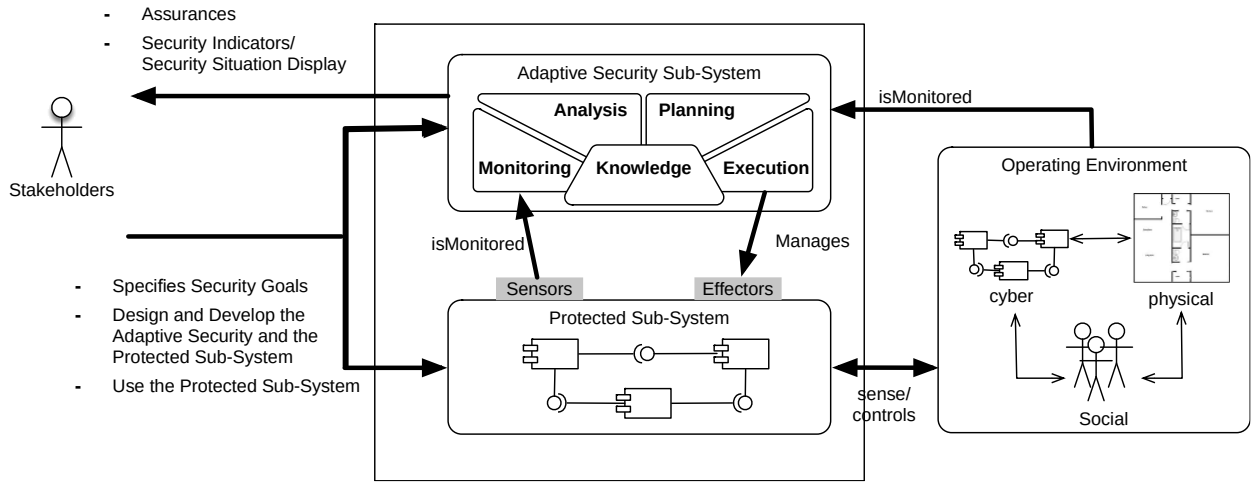

Figure 2: Adaptive Security Reference Architecture.

Adaptive security systems [9] are a class of self-adaptive systems able to detect and counteract security threats at runtime. Figure 2 shows a reference architecture for adaptive security systems. Similarly to other adaptive systems – this architecture generally comprises two sub-systems: an *adaptive security sub-system* is concerned with satisfaction of security goals and manages a *protected sub-system* concerned with the domain functionality.

The adaptive security sub-system is structured in accordance with the MAPE (Monitor-Analyze-Plan-Execute) loop architecture [8]. This is traditionally considered to be the reference architecture to engineer adaptive systems [12]. It *monitors* (M) the protected sub-system and its operating environment and maintains an updated representation of the protected sub-system and its operating environment at runtime (*knowledge* - K). The protecting sub-system uses this representation to *analyze* (A) security threats and assess security risks, and *plan* (P) and *execute* (E) countermeasures aimed to prevent or thwart the threats discovered during analysis. The protected subsystem (e.g., maritime transport system) is the system to be protected, which interacts with the cyber, physical and social spaces characterizing its operating environment.

A variety of stakeholders [14] are generally involved in the design and use of an (adaptive) security system. For example, software engineers and system operators are those who may need to assess the security posture of the system and decide which security controls are effective to satisfy some security goals. They can elicit security requirements, perform risk assessment, and design, implement, and release security controls that should be enforced. Software users/end users (e.g., passengers and crew operators) directly use and interact with the system to be protected (the protected sub-system). Business units may contribute to the elicitation of security goals in the form of security policies, whereas legal/regulatory units (e.g., port and custom authorities) may impose security and related regulations (e.g., the GDPR privacy regulation) and standards (e.g., ISO27001) that the system must comply with.

Although different surveys have been provided to describe related research on adaptive security systems, they have mainly focused on the design and implementation aspects of such systems. Elkhodary and Whittle [10] classify only four existing adaptive security approaches along two main perspectives: adaptive security service and adaptation method. The adaptive security service dimension identifies a set of security controls (authentication, authorization and tolerance) that should be implemented to satisfy security properties. The

adaptation methods examine the reconfiguration mechanisms employed by the adaptive security system. These include the computational paradigm adopted to enact self-protection (e.g., parameterization, component-based composition, reflection, aspect orientation), the re-configuration scale (single unit, inter-unit, or system wide) and the capability to handle conflicts between units and requirements. Yuan et al. [9] provide a more comprehensive classification of adaptive security systems along the "What" and the "How" dimensions. The "What" dimension includes the objectives and the intent of self-protection research and the security goals to be satisfied, while the "How" dimension is concerned with classifying how self-protection is implemented (e.g., the theoretical model adopted for decision making, the strategy adopted to perform decision making). Finally, the survey also considers various approaches adopted to evaluate research on adaptive security systems, in terms of intrinsic qualities of the research outcome, such as the validation method, repeatability of the approach, and generalizability of the results. Tziakouris et al. [15] extends previous taxonomies by providing architectural patterns and methodologies that can be re-used to design large-scale adaptive security systems. The authors provide guidelines to select an appropriate architectural pattern depending on the dynamism of the operating environment and the problem setting.

From the analysis of existing surveys on adaptive security we noticed that a few essential aspects have not been examined. First, **stakeholders** are rarely considered as part of an adaptive security system. They may not just be involved in the design of an adaptive security system, but they may also be involved directly in the execution of the activities of the MAPE loop. Security engineers may be involved during decision-making when there are multiple alternative sets of security controls that can be enacted in the same situation. System administrators responsible for deployment aspects may provide information about the levels of physical security in the different networking environments of relevance and may decide upon deployment-level mitigations (e.g. firewall configurations). End users can also serve as monitors and actuators. For example, passengers can monitor other passengers' movement and/or inform crew operators in case of an increased risk that a passenger may damage the cargo and/or the vessel. Adaptive security systems should also provide capabilities to increase confidence in their security controls decisions among their stakeholders. For example, they can provide formally-grounded assurances that demonstrate that the system satisfies a set of security goals and complies with regulations and/or standards. However, the adaptive security system can also provide less formal explanations (e.g., in the form of arguments), which can justify system decisions or describe the current security situation. As with current generations of AI-driven systems, the *explainability* of automated decisions is a key impediment to trust and adoptions and limited explainability, to the relevant stakeholders, in many cases hinders the application of these techniques in practice.

Another aspect is the interplay between adaptive security objectives (e.g., prevent, detect, and mitigate attacks) and the design and implementation of adaptive security systems. More precisely, we aim to identify objectives that existing research in adaptive security aimed to achieve and identify the link between such requirements and how adaptive security capabilities are designed and implemented. Finally adaptive security systems have mainly been considered for purely software systems and have rarely addressed cyber-physical and socio-technical systems.

2.3 Research Questions

Taking into account the gaps described in the previous subsection, this survey is grounded on the following research questions:

Domain-related questions

- For what types of systems and application domains have adaptive security systems been developed?

Stakeholders-related questions

- What are the categories of stakeholders considered in adaptive security systems?
- In what ways have stakeholders been involved in the activities of the adaptive security MAPE loop?
- What types of artifacts (e.g., assurances/explanations) do adaptive security systems produce and for what types of stakeholders?

Requirements-related questions

- Have adaptive security objectives (e.g., detect, prevent, mitigate attacks) been considered in existing research?
- What types of design and implementation solutions are adopted to satisfy a specific adaptive security objectives?

3 Systematic Literature Review Protocol

For this survey the following protocol was adopted. We searched for research papers in the most complete research databases (IEEE Explore, ACM Digital Library, Springer Digital Library, Elsevier ScienceDirect - Computer Science collection, and Google Scholar). To identify papers on adaptive security, we considered the following keywords: “Software Self-Protection”, “Self-Protecting Software”, “Self-Securing Software”, “Adaptive Security”, “Self-Adaptive Security and Autonomous Security”.

We only selected refereed and conference publications and excluded patents. Position papers or research proposal not yet implemented or evaluated were excluded. When reviewing a candidate paper, we have in many occasions further extended the collection with additional papers that appear in its citations or those that are citing it (backward and forward citation search). We reviewed papers published between 2012 and 2020. A total of 5950 papers matched the search criteria. After reading title and abstract of the papers matching the search criteria, only 63 papers were in scope (addressed the topic of engineering adaptive security systems). Among these 63 papers 13 were ruled out because they were position papers and/or did not provide an evaluation section.

4 The Role of the Application Domain in Adaptive Security

In this Section we position the role of the application domain in the development of adaptive security systems. To achieve this aim, we answer the application domain related questions mentioned in Section 2.3. We highlight our main findings in a bold type face.

4.1 For what types of systems and application domains have adaptive security systems been developed?

Figure 3 provides a chart describing the application domains where adaptive security approaches have been developed and deployed. The majority of the surveyed papers were aimed to securing communications in IoT systems (33%), mobile devices (15%) virtual and private networks (12%), cloud and web services (12%) and autonomous vehicles (9%). A central problem in these

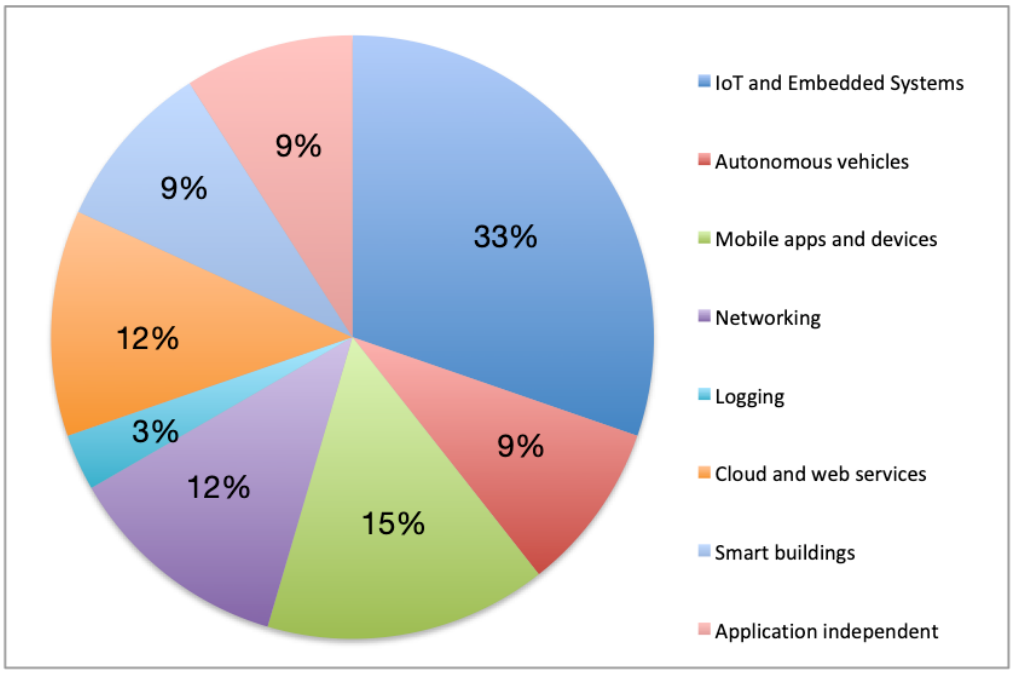

Figure 3: Adaptive Security Application Domains.

domains are to balance the tradeoff between secure communication, performance and energy consumption. Other approaches have been applied to prevent security threats and hazards in smart buildings (9%), or are application-independent. One of the papers that was surveyed considered securing blockchain-based logs. An interesting finding is that user authentication did not emerged as an application domain. This is surprising considering emerging research on continuous authentication and current "zero-trust" approach.

However, only a few approaches [29-30] have considered systems (in this case, smart buildings) where threats do not just arise from network communication but also from the structure of the physical space (e.g., physical location of assets) and the roles of human actors using the system. For such types of systems, analysis and planning activities require to take into account heterogeneous models involving both cyber and physical system components and users, and their interaction. **As cyber-physical systems are becoming**

more ubiquitous more holistic adaptive security solutions able to analyze the extended attack surface of cyber-physical systems should be provided. These solution should be capable to enact and coordinate security controls in both the cyber and physical spaces where the system operates.

5 The Role of Stakeholders in Adaptive Security

In this Section we position the role of the stakeholders in the engineering and use of adaptive security systems. To achieve this aim, we answer the stakeholder-related questions mentioned in Section 2.3.

5.1 What are the categories of stakeholders considered in adaptive security systems and what types of output do stakeholders receive?

Stakeholders are rarely considered in existing adaptive security approaches. We grouped the stakeholders that were mentioned explicitly in existing research on adaptive security in three main categories: *system users*, *software engineers*, and *security engineers/operators*.

System users is the category of stakeholders that has been considered the most in the body of literature on adaptive security. Users are often considered in approaches aimed to secure mobile devices and applications [17-18, 26-28], cloud applications [19, 25], distributed systems [23], IoT systems [20-21, 24], and smart buildings [22, 29-30]. Adaptive security approaches aimed to secure mobile devices require to adapt to changes in users' contextual information (e.g., changes in network and location [17, 27-28]) and/or security preferences [26,28]. These changes can modify the security requirements (e.g., new assets to be protected), or bring new vulnerabilities (e.g., a mobile phone uses an unprotected network). Similarly involvement of IoT system users has been briefly considered, because they may host a body area network [20-21] and/or they may trigger events (changes) generated by the various networked devices (things) in a monitored IoT environment [24]. In the context of smart buildings [29-30] changes in user locations may leave certain assets unattended requiring to adapt access control policies. **Despite the predominant role of users in triggering a change in the security controls, existing research has not posed much emphasis on how to inform users about what personal data require to be collected, in order to select appropriate security controls.** This becomes important especially considering emerging personal data protection regulations world-wide (e.g., the GDPR in Europe, the California Consumer Privacy Act, the LGPD in Brazil).

In other situations, adaptation decisions can affect the user interaction with the system. For example, an adaptation may disallow execution of an application [18, 23] or a required functionality [25], or access to certain areas of a building [22, 29-30]. Thus, adaptive security systems should also explain how and why security controls have changed at runtime. This is particularly important, considering that users may lose trust in the system when its behavior deviates from their expectations [25]. Only two of the approaches that were surveyed provide a contribution in this direction. For example, Mukhin et al. [23] suggest sending a warning message to system administrators or the users before shutting down a suspected software application. Nhlabatsi et al. [25] inform users about whether a cloud application functionality can be executed in a specific context, why, and what actions should be performed instead in order to satisfy a security policy.

Software engineers is the category of stakeholders tasked to design and develop an adaptive security system. They can specify relevant security concerns (e.g., security requirements, threats, attacks), the adaptive behavior of the system (e.g., possible security controls) and the properties and behavior of the environment in which the adaptive security system executes [28-30]. Adaptation decisions can also affect how an application should be implemented, for example, depending on the personal information about a

user that can be disclosed [19]. Despite a few exceptions [31-32], **previous research has not really addressed the problem of how to facilitate software engineers in specifying and implementing the behavior of an adaptive security system**. Tun et al. [31] provide a language to specify adaptive security requirements in the presence of incomplete knowledge about the environment. Aman and Snekkenes [32] provide software engineers a specification of the adaptive security system in the form of scenarios.
Security engineers/operators is the category of stakeholders tasked to specify the security requirements and relevant security concerns (e.g., security requirements, threats, attacks). They may also be required to take some actions when an anomaly is discovered. For example, LSC [33] performs automatic online log analysis in blockchain-enabled log systems using smart contracts. When anomalies in the logs are discovered a smart contract is provided to the security operator to demonstrate the type of anomaly. **However, none of existing approaches provides techniques to support security operators in the decision making**.

We identified three types of stakeholders: users, software engineers and security engineers/human operators. Users can trigger changes in the security controls. Thus, their (personal) data may need to be monitored during the adaptation loop to select security controls. Also, enactment of security controls can affect the user's interaction with the system. However, existing work on adaptive security has not focused on how to inform users about what personal data are required to be collected for adaptive security purposes. Existing research has provided information and explanations about enacted security controls in the form of warning messages [23] or arguments [25], generated by exploiting traceability links between security policies, requirements and domain assumptions. Software engineers are responsible for designing and implementing the adaptive security behavior of the system. To support software engineers, previous work has considered providing them with scenarios [32] and formal languages [31] to specify adaptive security requirements. Finally, security engineers and operators can provide insights about effectiveness of security controls during decision making. However, no artifact has been proposed to encourage their involvement in the analysis and planning activities of the adaptive security loop.

5.2 In what ways have stakeholders been involved in the activities of the adaptive security MAPE loop?

Stakeholders have been involved very sporadically in the execution of the activities of the adaptive security MAPE loop. However, security- and safety-critical systems can greatly benefit from human involvement. Humans can act as sophisticated sensors by complementing the knowledge base of the adaptive system with information that is difficult to monitor or analyze automatically. Humans can also provide input into the decision-making process, to have a better insight about the best way of adapting a system. Humans can also be employed as system-level effectors, to execute security controls in case their execution cannot be automated [34].

Only few approaches [18, 22] address the role of the users in the monitoring, decision making and execution of security controls. For example, Ahmad et al. [18] allow users to select hardware and software resources that are security-critical. When access to one of these critical resources is performed, the user is asked whether s/he would like to allow or block access (temporarily or permanently) to such resources. In the domain of smart buildings [22, 29-30] the user's conditions or activities can be actively monitored, like working with a hammer or a very high heartbeat. Adaptation actions can also require human involvement.

For example a security guard may be asked to reach a location or a human operator may be required to turn on the ventilation system.

Existing research has not taken into account the fact that the correct execution of a task allocated to humans can be affected by human factors external to the system (e.g., training level, stress, fatigue, dissatisfaction). Thus, appropriate models and techniques should be provided to determine the likelihood of stakeholders in performing a given task, whether they are willing to perform in the first place, or whether they may act as potential offenders.

5.3 What types of artifacts (assurances/explanations) do adaptive security systems produce and for what types of stakeholders?

Existing research on adaptive security has mainly aimed to provide assurances to security engineers and operators about effectiveness of security controls. For example, Asaithambi et al. [33] demonstrate from an algorithmic point of view that the approach selects the maximum security level possible for a mobile device, while still ensuring that the energy does not exceed a given budget. Lin et al. [35] demonstrate that an adaptive security data collector can reduce the amount of monitored data, while ensuring accuracy of information collected. Teimourikia et al. [36] demonstrate that adaptive security decisions are conflict-free. Tsigkanos et al. [30] adopt formal methods (explicit state model checking) to ensure that selected security controls satisfy a set of security requirements. Cheminod et al. [54] also uses state model checking to verify that a system configuration is correct with respect to a set of defined access-control policies. Vo et al. [19] proves that access to users' personal information is revoked when the ciphertext or tokens adopted during network communication were expired. Beer et al. [40] demonstrate compliance with the OWASP recommendations provided for web applications.

Provisioning of explanations about why security controls selected at runtime are effective is important to increase trust and facilitate involvement of stakeholders in the execution of the activities of the MAPE adaptation loop. The work by Nhlabatsi et al. [25] represents the only approach aimed to help users understand security decisions made by an adaptive application. It provides explanation to the users justifying why certain actions can/cannot be performed, by establishing traceability relationships between requirements and security concerns.

Because adaptation decisions can change dynamically, provided assurances and explanations have to be regenerated and revised at runtime. Among the work we surveyed, only Shao et al. [33] update smart contracts dynamically based on self-renewal anomaly detection algorithms in order to certify absence of anomalies in blockchain-based logs. **To introduce adaptive security systems into production, more systematic approaches are necessary to generate assurances demonstrating compliance with existing security standards and regulations, even in the presence of adaptation.** Moreover, personalized assurances and explanations should be provided depending on the type of role of stakeholders in the execution of the activities of the MAPE adaptive security loop.

6 The Role of Requirements in Adaptive Security

In this Section we position the role of the adaptive security objectives (e.g., detect, prevent, mitigate a violation of security requirements) in the engineering of adaptive security systems. To achieve this aim, we answer the requirements related questions mentioned in Section 2.3.

6.1 How adaptive security objectives have been considered in the engineering of adaptive security systems?

Adaptive security objectives can be classified in the following main categories: *detection*, *prevention* and *mitigation* of security threats and attacks, and management of trade-offs between security and other system requirements.

Detection. Previous research on adaptive security has tackled the problem of security threats and attack detection rather sporadically. Existing approaches on adaptive security aim to continuously detect potential violations of security requirements when the strategies of attackers [33] or the system operating environment change [35]. For example, Shao et al. [33] allow updating the notion of *anomaly* in blockchain-based logs dynamically, to reflect changes in strategies of attackers. Lin et al. [35] adapt the activities of a data collector depending on the operating context in heterogeneous networks. They also aim to reduce the amount of collected data, while maintaining accuracy of collected information.
However, there are other factors that may affect adaptation of data collection strategies for detection purposes. In recent years we have observed the rise of stealthy attacks [37-38]. For example, advanced persistent threats are posed by stealthy computer network attackers, which gain unauthorized access to a computer network and remain undetected for extended periods of time. Advanced persistent threats often target cyber-physical systems, where physical characteristics of the control process and knowledge of the anomaly detector are used by an attacker to remain undetected until actual harm is caused. For this type of threats, it is necessary to continue to perform data collection activities to gather as much information as possible about the attacker. Data collection activities should also adapt dynamically to avoid detection by attackers, who, would change their strategy otherwise. However, data collection cannot continue when the risk of harm exceeds a threshold. Security strategies aimed to prevent or mitigate attacks should be enacted dynamically, instead, in such situation.

Prevention. The majority of existing approaches proposed to support adaptive security are aimed to prevent security threats and attacks. For example, IoT systems [39, 42], cloud based applications [19] and mobile devices [26] are highly vulnerable to attacks aiming to harm confidentiality and integrity of information transmitted between nodes in the network. For this reason, security controls commonly adopted select forms of authentication and encryption, depending on the level of trust associated with the communicating nodes. For example, trust-based monitoring schemes [39][42] have been proposed to enable authentication depending on the trust level associated with a message sender. This trust level is computed over time by external intelligent agents [39] or can be established cooperatively by the various nodes belonging to the IoT network [42]. Similarly, in cloud based applications [19] an important objective is to avoid disclosure of users' personal information. To achieve this aim, a trust model among service components is created and used to provide a platform-specific security infrastructure.

Also a purpose-based encryption is proposed to protect disclosure of personal information to intermediary entities in a business transaction and from untrusted hosts. Other work [22, 29, 30, 36, 41] has aimed to prevent security risks and hazards in smart buildings. Some of them [29-30] express threats to be prevented in terms of undesired structures of the building (connectivity/containment relationships to be avoided), for example representing unauthorized network connectivity, exfiltration of confidential information, or unauthorized access to areas of the building.

Mitigation. Surprisingly, very little work has focused on adaptive security strategies that could adaptively support harm containment after an attack occurs. Important considerations to be made in this space are related to the time necessary to adapt [52]. Indeed, adaptation objectives should aim to minimize the time to compute and perform an adaptation in order to reduce harm. An aspect that stroked our attention was the absence of a more complete adaptive security approach that could modify adaptation objectives (e.g., detection vs prevention vs mitigation) depending on the likelihood and time necessary for an attack to materialize.

Management of Trade-offs between Security and other System requirements. Management of the tradeoff between security and other requirements of the systems has been considered in various application domains. For example tradeoffs between security and network performance are mainly considered in wireless sensor networks [17, 21, 32, 43-46], where more reliable network mechanisms have a high impact over the already limited computational capacity of network nodes. Application of encryption can increase computation and packet transmission time [44], signature verification can increase the time necessary to process packets from nearby nodes, increasing the packet loss rate [47]. These types of trade-offs are also important in real time storage applications [50,54], where CPU utilization used to support security mechanisms can impact on the overall throughput. Implementation of security mechanisms can also increase energy consumption in wireless networks [20, 48, 49, 51] that should be minimized. Finally, other domain-independent approaches aim to minimize security risks [24] or maximize the trade-off between security and, more generally, other requirements of the system [28].
Adaptive security objectives have been mainly addressed separately in existing approaches. The majority of work has focused on prevention of security attacks. Tradeoffs between security, energy consumption and performance has been a predominant objective in approaches deployed in the wireless sensor networks domain. A gap in research is represented by the lack of a holistic approach integrating different adaptive security objectives and switching objectives depending on the likelihood of an attack to materialize.

6.2 What types of design and implementation solutions are adopted to satisfy adaptive security objectives?

We observed that the techniques adopted to support analysis and planning activities of adaptive security systems do not vary depending on the adaptive security objectives, but mainly depend on the application domain where they have been applied. These techniques are based on the computation of *mathematical functions*, on formal *logic-based reasoning*, *game theory* and *control theory*. They also use machine learning techniques to improve accuracy of analysis.

Mathematical functions have been often used to represent and measure trust of messages' senders in wireless sensor networks [39, 42, 44-45] and cloud services [19], in order to identify an appropriate authentication and encryption mechanism to be adopted. The measure of trust can be computed depending on attributes of physical signals (e.g., signal strength) of communicating nodes [44, 39] or depending on the cryptographic loss rate. Computation of trust may depend on direct observations of the network traffic [45] and also on recommendations sent by other neighbor nodes [42]. In vehicular networks a computation of the cryptographic packet loss is performed to prioritize packet signature verification [47].
In other work [28] a utility function is used to compute analytically effectiveness of various configurations of security controls. The utility function expresses the tradeoff between satisfaction of security and other system requirements and the cost of applying the security controls. A configuration of security controls that maximizes this utility function is selected during planning. Asaithambi et al [17] adopt the online multi-choice knapsack algorithm to identify an optimal compromise between selection of a security level and energy consumption in mobile device applications. Modafi et al. [26] use Analytic Hierarchy Process (AHP) to decide whether a mobile app should be granted secure or insecure network access depending on the users' context information (e.g., location, time and network) and also on the security settings of their mobile device.

Rule-based approaches [22, 24, 32] have been proposed to guide decision making. For example, Fugini et al. [22] adopt Event-Condition-Action (ECA) meta-rules, which in turn trigger modification of access control policies in smart buildings depending on the security risks and hazards computed in smart buildings [36]. Aman and Snekkenes [24, 32] propose to correlate and analyze events coming from wearable devices and the network to identify security risks. They create a rule base to select appropriate security controls depending on the risks. Rules based on transition probability have also been adopted to change the cryptographic algorithms, the key sizes and the hash functions used during vehicle-to-vehicle communication, depending on the vehicles energy level, sensor memory and processing capacity and the position of the charging station [43].
Approaches based on formal **logic-based reasoning** have been adopted to model the dynamic behavior of a system and speculate on its future evolution in order to identify security threats. To achieve this aim, solutions have been based on Answer Set Programming [41] and model checking [30].

Stochastic games have been used to balance the tradeoff between conflicting requirements (e.g., security vs performance [20-21, 51]) in IoT systems. For example, Hamdi and Abie [51] define two functions: one representing the efficiency of a security policy in mitigating an intrusion and the other representing the impact of security controls on the lifetime of the network. A Nash bargaining model is used to determine an equilibrium, allowing both security and performance to be maximized.
Although these approaches have demonstrated to be effective in their own application domain, they have not considered uncertainties which can be introduced by imprecision of the monitoring infrastructure or information that is not known accurately about the operating environment (e.g., effectiveness of security controls). To take into account these uncertainties during analysis and planning, existing approaches [44, 21] have used Markov Decision Processes, for example, to represent the impact of security controls on energy depletion and performance degradation. Approaches based on machine learning have also been proposed to improve accuracy of the analysis. For example, the k-means clustering algorithm [44] has been used to better identify distance of a vehicle from a sender's node, in order to prioritize packet signature verification. Neural networks [23] and Naïve Bayes classifiers [46] have been adopted to improve accuracy

in the identification of security risks. One of the problems of approaches based on machine learning is that they require to be trained in advance and their performance can be affected over time if models are not re-trained. Only very recently existing research [33] has proposed to combine anomaly detection models with the capability of self-adaptive learning [51], in order to face evolving adversarial attacks. However, while current adaptive security approaches are able to model and reason about the uncertainty associated with a system and its environment, they do not consider explicitly ways to reduce uncertainty [53].

Finally, only one of the work [50] that was surveyed adopts PID (proportional integral derivative) adaptive control to control system vulnerability and utilization in flash memories. These are monitored at runtime and their value is compared with the corresponding desired value to compute an offset that is used to adjust the number of pages that the memory shall encrypt. However, work based on control theory cannot allow reasoning about disruptive changes in the structure and/or behavior of the system and its operating environment in a scalable way.

7 Recommendations

This section elicits a list of recommendations for future research on adaptive security systems, which emerged from the gaps in research identified in this survey.

7.1 A holistic approach to adaptive security

It is necessary to design and develop adaptive security solutions that can be applied to heterogeneous cyber-physical systems composed of cyber, physical and human components. This means that security threats can arise from an extended attack surface covering cyber and physical spaces and human factors. Cyber-physical systems are characterized by a large number of software components and individual computation nodes. Thus, it is necessary to focus future research on more modular and decentralized analysis and planning techniques that can reduce the reasoning complexity.

7.2 Integration between adaptive security objectives

Adaptive security systems should be designed with the capability to enact and adapt their adaptive security objectives (detect, prevent and mitigate). This would allow an adaptive security system to mimic and reflect the strategies of an attacker, especially for advanced persistent threats. For example, at the early stages of an attack, an adaptive security system may favor monitoring rather than blocking an attack, because the risk of harm is rather low and there is not sufficient evidence that an attack is occurring. When the risk of harm is higher an adaptive security system can opt for a strategy preventing an attack from happening or for reducing/containing harm. To achieve this aim, some form of hierarchical planning should be designed allowing not only to adapt security controls but also adaptive security objectives.

7.3 Explicit consideration of the stakeholders

Existing adaptive security systems should be designed assuming that their stakeholders can be involved in the execution of some of the activities of the MAPE loop. To achieve this aim it is necessary to explicitly represent stakeholders' capabilities. For example, certain users can monitor a set of properties of the operating environment or execute security controls. Security engineers can provide additional information during security risk analysis and/or be involved in the decision-making. End users may be involved in an explicit *mediation* process in which they can make or contribute to essential trade-off decisions through direct interaction with the self-adaptive systems (e.g., [55]).

Allocation of tasks to humans also requires reasoning about the factors that may affect the successful execution of the task (stakeholders' capabilities and knowledge, time when a stakeholder is required to perform a task) and provide a runtime models to update such success factors. Correct task execution by humans can also depend on the type of explanations provided to the stakeholder. Thus, explanations should be customized depending on the stakeholder's role.

7.4 Perpetual security assurances

Existing adaptive security approaches have used formal techniques to support decision making. However, they do not use the results of analysis and planning to provide assurances to a) either demonstrate that a sufficient level of security has been achieved or b) suggest and prioritize to software architects mitigation techniques that can be used to remove identified vulnerabilities, if those cannot be mitigated automatically. Providing such assurances is fundamental also to demonstrate compliance with existing security standards.

Goal Structuring Notation (GSN) can be used to model assurances, because this notation has been used successfully to represent assurance cases in the safety domain. Flexible approaches should also be provided to generate assurances incrementally only modifying parts of the assurance case associated with the parts of the system that were affected by a change.

7.5 Reducing security uncertainties

Existing adaptive security approaches operate under the assumption that the possible set of security controls is pre-determined and do not evaluate effectiveness of security controls at runtime. However, at design time it is not possible to foresee all possible changes that can affect a system and the security threats and vulnerabilities. Therefore it is necessary to design mechanisms to detect uncertainties, i.e. situations where the system is characterized by unknown threats and vulnerabilities that have not been taken into account at design time. Such situations can be monitored by identifying anomalies and/or situations when security control are no longer effective.

8 Conclusions

This deliverable has the main contribution of surveying adaptive security research from a "requirements engineering" perspective where stakeholders, adaptive security objectives, and application domains are considered explicitly.

We noticed that existing solutions do not take into account application of security controls in both the cyber and physical spaces where the system operates. We also noticed that very limited research was performed to encourage stakeholder's involvement in the MAPE adaptation loop. More systematic approaches are necessary to generate assurances and explanations demonstrating compliance with existing security standards and regulations, even in the presence of adaptation. Moreover, adaptive security approaches are mainly focused on prevention of security threats and do not consider other objectives, such as detection and mitigation of security threats. Finally, while current adaptive security approaches are able to model and reason about the uncertainty associated with a system and its environment, they do not consider explicitly ways to reduce uncertainty.

We recommend future research to focus on a) considering the cyber and physical spaces were modern systems operate during monitoring and execution of security controls; b) integrating multiple security objectives during decision-making; c) considering the stakeholders during design and development of the activities of the adaptive security MAPE loop; d) provisioning of perpetual security assurances that can be re-generated after adaptation; e) reducing security uncertainties.

We acknowledge the need to gather an industrial view regarding the challenges of adaptive security in practice. We will conduct a survey involving practitioners to validate the gaps and future research directions that emerged from the literature review. The survey will also be aimed to identify new research challenges that were not identified from previous work on adaptive security. The survey participants will be practitioners who are already part of the CyberSec4Europe consortium, as well as practitioners who have a collaboration relationship with the partners of the project.

9 References

[1] Bomey, N., A. A. Dastagir, A. Shell, K. McCoy, and R. Yu. "Equifax data breach: What you need to know about hacking crisis." *USA Today, September* 15 (2017).

[2] Forbes. "Marriott Breach: Starwood Hacker Gains Access to 500 Million Customer Records." 2018.

[3] Antonakakis, Manos, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric et al. "Understanding the mirai botnet." In *26th {USENIX} Security Symposium ({USENIX} Security 17)*, pp. 1093-1110. 2017.

[4] Bissell, Kelly, and Larry Ponemon. "The Cost of Cybercrime – Accenture." 2019.

[5] Zimmermann, Verena, and Karen Renaud. "Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset." *International Journal of Human-Computer Studies* (2019).

[6] Varonis. "60 Must-Know Cybersecurity Statistics for 2019." 2019.

[7] Salehie, Mazeiar, Liliana Pasquale, Inah Omoronyia, Raian Ali, and Bashar Nuseibeh. "Requirements-driven adaptive security: Protecting variable assets at runtime." In *2012 20th IEEE International Requirements Engineering Conference (RE)*, pp. 111-120. IEEE, 2012.

[8] Kephart, Jeffrey O., and David M. Chess. "The vision of autonomic computing." *Computer* 1 (2003): 41-50.

[9] Yuan, Eric, Naeem Esfahani, and Sam Malek. "A systematic survey of self-protecting software systems." *ACM Transactions on Autonomous and Adaptive Systems (TAAS)* 8, no. 4 (2014): 17.

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

[11] Pfleeger, Charles P., and Shari Lawrence Pfleeger. *Security in computing*. Prentice Hall Professional Technical Reference, 2002.

[12] Brun, Yuriy, Giovanna Di Marzo Serugendo, Cristina Gacek, Holger Giese, Holger Kienle, Marin Litoiu, Hausi Müller, Mauro Pezzè, and Mary Shaw. "Engineering self-adaptive systems through feedback loops." In *Software engineering for self-adaptive systems*, pp. 48-70. Springer, Berlin, Heidelberg, 2009.

[13] Kitchenham, B. 2004. Procedures for Performing Systematic Reviews. Keele University, Keele, UK.

[14] Maynard, S. B., A. B. Ruighaver, and A. Ahmad. "Stakeholders in security policy development." (2011).

[15] Tziakouris, Giannis, Rami Bahsoon, and Muhammad Ali Babar. "A Survey on Self-Adaptive Security for Large-scale Open Environments." *ACM Computing Surveys (CSUR)* 51, no. 5 (2018): 100.

[16] Leather, Anthony. "Passenger Profiling: cases for and against." Aviation Security International Magazine, https://www.asi-mag.com/passenger-profiling-cases-for-and-against/, Last Retrieved: Jan 2020.

[17] Asaithambi, Asai, Ayan Dutta, Chandrika Rao, and Swapnoneel Roy. "Online Context-Adaptive Energy-Aware Security Allocation in Mobile Devices: A Tale of Two Algorithms." In *International Conference on Distributed Computing and Internet Technology*, pp. 281-295. Springer, Cham, 2020.

[18] Ahmad, Aakash, Asad Waqar Malik, Abdulrahman Alreshidi, Wilayat Khan, and Maryam Sajjad. "Adaptive Security for Self-Protection of Mobile Computing Devices." *Mobile Networks and Applications* (2019): 1-20.

[19] Vo, Tri Hoang, Woldemar Fuhrmann, Klaus-Peter Fischer-Hellmann, and Steven Furnell. "Identity-as-a-Service: An Adaptive Security Infrastructure and Privacy-Preserving User Identity for the Cloud Environment." *Future Internet* 11, no. 5 (2019): 116.

[20] Arfaoui, Amel, Asma ben Letaifa, Ali Kribeche, Sidi Mohammed Senouci, and Mohamed Hamdi. "A stochastic game for adaptive security in constrained wireless body area networks." In *2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1-7. IEEE, 2018.

[21] Arfaoui, Amel, Ali Kribeche, Sidi Mohammed Senouci, and Mohamed Hamdi. "Game-Based Adaptive Risk Management in Wireless Body Area Networks." In *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 1087-1093. IEEE, 2018.

[22] Fugini, Mariagrazia, Mahsa Teimourikia, and George Hadjichristofi. "A web-based cooperative tool for risk management with adaptive security." *Future Generation Computer Systems* 54 (2016): 409-422.

[23] Mukhin, Vadym, Yaroslav Kornaga, Viktor Steshyn, and Yevgeniy Mostovoy. "Adaptive security system based on intelligent agents for distributed computer systems." In *2016 International Conference on Development and Application Systems (DAS)*, pp. 320-325. IEEE, 2016.

[24] Aman, Waqas, and Einar Snekkenes. "Managing security trade-offs in the internet of things using adaptive security." In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 362-368. IEEE, 2015.

[25] Nhlabatsi, Armstrong, Thein Tun, Niamul Khan, Yijun Yu, Arosha Bandara, Khaled M. Khan, and Bashar Nuseibeh. "“Why can’t I do that?”: tracing adaptive security decisions." *EAI Endorsed Transactions on Self-Adaptive Systems* 1, no. 1 (2015).

[26] Mowafi, Yaser, I. Dhiah el Diehn, Tareq Al-Aqarbeh, Marat Abilov, Viktor Dmitriyev, and Jorge Marx Gomez. "A Context-aware Adaptive Security Framework for Mobile Applications." *ICCASA* 14 (2014): 147-153ICST.

[27] Halunen, Kimmo, and Antti Evesti. "Context-aware systems and adaptive user authentication." In *International Joint Conference on Ambient Intelligence*, pp. 240-251. Springer, Cham, 2013.

[28] Salehie, Mazeiar, Liliana Pasquale, Inah Omoronyia, Raian Ali, and Bashar Nuseibeh. "Requirements-driven adaptive security: Protecting variable assets at runtime." In *2012 20th IEEE international requirements engineering conference (RE)*, pp. 111-120. IEEE, 2012.

[29] Tsigkanos, Christos, Liliana Pasquale, Carlo Ghezzi, and Bashar Nuseibeh. "On the interplay between cyber and physical spaces for adaptive security." *IEEE Transactions on Dependable and Secure Computing* 15, no. 3 (2016): 466-480.

[30] Tsigkanos, Christos, Liliana Pasquale, Claudio Menghi, Carlo Ghezzi, and Bashar Nuseibeh. "Engineering topology aware adaptive security: Preventing requirements violations at runtime." In *2014 IEEE 22nd International Requirements Engineering Conference (RE)*, pp. 203-212. IEEE, 2014.

[31] Tun, Thein Than, Mu Yang, Arosha K. Bandara, Yijun Yu, Armstrong Nhlabatsi, Niamul Khan, Khaled M. Khan, and Bashar Nuseibeh. "Requirements and specifications for adaptive security: concepts and analysis." In *2018 IEEE/ACM 13th International Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS)*, pp. 161-171. IEEE, 2018.

[32] Aman, Waqas, and Einar Snekkenes. "Managing security trade-offs in the internet of things using adaptive security." In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pp. 362-368. IEEE, 2015.

[33] Shao, Wei, Zhi Wang, Xiaolu Wang, Kefan Qiu, Chunfu Jia, and Chong Jiang. "LSC: Online auto-update smart contracts for fortifying blockchain-based log systems." *Information Sciences* 512 (2020): 506-517.

[34] Cámara, Javier, Gabriel Moreno, and David Garlan. "Reasoning about human participation in self-adaptive systems." In *2015 IEEE/ACM 10th International Symposium on Software Engineering for Adaptive and Self-Managing Systems*, pp. 146-156. IEEE, 2015.

[35] Lin, Huaqing, Zheng Yan, and Yulong Fu. "Adaptive security-related data collection with context awareness." *Journal of Network and Computer Applications* 126 (2019): 88-103.

[36] Teimourikia, Mahsa, Guido Marilli, and Mariagrazia Fugini. "Context-based risk-adaptive security model and conflict management." In *International Conference on Database and Expert Systems Applications*, pp. 121-135. Springer, Cham, 2016.

[37] Urbina, David I., Jairo A. Giraldo, Alvaro A. Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, and Henrik Sandberg. "Limiting the impact of stealthy attacks on industrial control systems." In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1092-1105. 2016.

[38] Khalil, Issa, and Saurabh Bagchi. "Stealthy attacks in wireless ad hoc networks: detection and countermeasure." *IEEE Transactions on Mobile Computing* 10, no. 8 (2010): 1096-1112.

[39] Alqahtani, Fayez, Zafer Al-Makhadmeh, Amr Tolba, and Omar Said. "TBM: A trust-based monitoring security scheme to improve the service authentication in the Internet of Things communications." *Computer Communications* 150 (2020): 216-225.

[40] Beer, Mohamed Ibrahim, and Mohd Fadzil Hassan. "Adaptive security architecture for protecting RESTful web services in enterprise computing environment." *Service Oriented Computing and Applications* 12, no. 2 (2018): 111-121.

[41] Sartoli, Sara, and Akbar Siami Namin. "A semantic model for action-based adaptive security." In *Proceedings of the Symposium on Applied Computing*, pp. 1130-1135. 2017.

[42] Hellaoui, Hamed, Abdelmadjid Bouabdallah, and Mouloud Koudil. "Tas-iot: trust-based adaptive security in the iot." In *2016 IEEE 41st Conference on Local Computer Networks (LCN)*, pp. 599-602. IEEE, 2016.

[43] Fraiji, Yosra, Lamia ben Azzouz, Wassim Trojet, Leila Azouz Saidane, and Ghaled Hoblos. "Adaptive Security for the Intra-Electric Vehicular Wireless Networks." In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*, pp. 1215-1220. IEEE, 2019.

[44] Javed, Muhammad Awais, Elyes Ben Hamida, Ala Al-Fuqaha, and Bharat Bhargava. "Adaptive security for intelligent transport system applications." *IEEE Intelligent Transportation Systems Magazine* 10, no. 2 (2018): 110-120.

[45] Bahnasse, Ayoub, Fatima Ezzahraa Louhab, Mohamed Talea, Hafsa Ait Oulahyane, Adel Harbi, and Azeddine Khiat. "Towards a new approach for adaptive security management in new generation virtual private networks." In *2017 International Conference on Wireless Networks and Mobile Communications (WINCOM)*, pp. 1-6. IEEE, 2017.

[46] Gebrie, Mattias T., and Habtamu Abie. "Risk-based adaptive authentication for Internet of things in smart home eHealth." In *Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings*, pp. 102-108. 2017.

[47] Javed, Muhammad Awais, and Elyes Ben Hamida. "Adaptive security mechanisms for safety applications in internet of vehicles." In *2016 IEEE 12th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 1-6. IEEE, 2016.

[48] Ferrera, Enrico, Rosaria Rossini, Davide Conzon, Sandro Tassone, and Claudio Pastrone. "Adaptive security framework for resource-constrained internet-of-things platforms." In *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1-5. IEEE, 2016.

[49] Di Mauro, Alessio, Xenofon Fafoutis, and Nicola Dragoni. "Adaptive security in odmac for multihop energy harvesting wireless sensor networks." *International Journal of Distributed Sensor Networks* 11, no. 4 (2015): 760302.

[50] Jiang, Wei, Yue Ma, Xia Zhang, Xupeng Wang, and Zili Shao. "Adaptive security management of real-time storage applications over NAND based storage systems." *Journal of Network and Computer Applications* 52 (2015): 139-153.

[51] Xie, Xueshuo, Zhi Wang, Xuhang Xiao, Lei Yang, Shenwei Huang, and Tao Li. "A Pvalue-guided Anomaly Detection Approach Combining Multiple Heterogeneous Log Parser Algorithms on IIoT Systems." *arXiv preprint arXiv:1907.02765* (2019).

[52] Moreno, Gabriel A., Javier Cámara, David Garlan, and Bradley Schmerl. "Flexible and efficient decision-making for proactive latency-aware self-adaptation." *ACM Transactions on Autonomous and Adaptive Systems (TAAS)* 13, no. 1 (2018): 1-36.

[53] Moreno, Gabriel A., Javier Cámara, David Garlan, and Mark Klein. "Uncertainty reduction in self-adaptive systems." In *Proceedings of the 13th International Conference on Software Engineering for Adaptive and Self-Managing Systems*, pp. 51-57. 2018.

[54] Cheminod, Manuel, Luca Durante, Lucia Seno, and Adriano Valenzano, “Semiautomated Verification of Access Control Implementation in Industrial Networked Systems,” in *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1388-1399, Dec. 2015