*Article*

# Systematic Literature Review of Security Pattern Research

**Hironori Washizaki[1]** , **Tian Xia[1]** , **Natsumi Kamata[1], Yoshiaki Fukazawa[1]** , **Hideyuki Kanuka[2]** , **Takehisa Kato[2]** , **Masayuki Yoshino[2], Takao Okubo[3]** , **Shinpei Ogata[4]** , **Haruhiko Kaiya[5]** , **Atsuo Hazeyama[6]** , **Takafumi Tanaka[7], Nobukazu Yoshioka[8]** **and G Priyalakshmi[9]**

[1]Waseda University; washizaki@waseda.jp
[2]Hitachi, Ltd.; hideyuki.kanuka.dv@hitachi.com
[3]Institute of Information Security; okubo@iisec.ac.jp
[4]Shinshu University; ogata@cs.shinshu-u.ac.jp
[5]Kanagawa University; kaiya@kanagawa-u.ac.jp
[6]Tokyo Gakugei University; hazeyama@u-gakugei.ac.jp
[7]Tamagawa University; tanaka_t@eng.tamagawa.ac.jp
[8]National Institute of Informatics; nobukazu@nii.ac.jp
[9]PSG College of Technology; priya.venky2001@gmail.com
* Correspondence: washizaki@waseda.jp

1 **Abstract:** Security patterns encompass security-related issues in secure software system development
2 and operations that often appear in certain contexts. Since the late 1990s about 500 security patterns
3 have been proposed. Although the technical components are well investigated, the direction, overall
4 picture, and barriers to implementation are not. Here, a systematic literature review of 240 papers is
5 used to devise a taxonomy for security pattern research. Our taxonomy and the survey results should
6 improve communications among practitioners and researchers, standardize the terminology, and
7 increase the effectiveness of security patterns.

8 **Keywords:** Security patterns, software patterns, systematic literature review (SLR)

---

9 ## 1. Introduction

10 A pattern is a solution to a problem that arises within a specific context [1]. Security patterns
11 are patterns specific to security problems and solutions. Security patterns describe security-related
12 problems and corresponding solutions as best practices that recur under specific contexts in secure
13 developments and operations [2]. There are concrete security patterns and abstract ones that capture
14 successful secure analysis, designs, and implementations. Security patterns provide guidelines to
15 improve security characteristics such as confidentiality, integrity, and availability since security patterns
16 incorporate the knowledge of security experts [3]. To reveal the overall picture and directions of security
17 pattern research, we employ a systematic literature review of 240 papers [4–243] and devise a taxonomy
18 in this paper.

19 The number of security patterns has recently grown; however, they are still challenging to apply
20 appropriately. Although there are ongoing researches and practices about various topics such as the
21 discovery, documentation, formalization application of security patterns [244], the current trends
22 and prospects of security patterns research are uncertain due to the diversity in the research results
23 themselves. Most studies have focused on technical aspects and implementation, but few have
24 examined the overall picture and significant technical challenges. To elucidate the current trends
25 and prospects, it is necessary to have a scheme to categorize and analyze research papers on security
26 patterns.

Several surveys such as [245] have been conducted on specific security patterns and related patterns to classify and analyze them. Moreover, there are some existing works such as [3,246] on studying different research techniques and approaches for security patterns. However, the survey and analysis are limited to specific security patterns or a small number of research papers. None of these related works is a rigorous survey targeting many research papers on security patterns in general.

It is clear that only considering limited security characteristics triad (i.e., CIA standing for confidentiality, integrity, and availability) is not enough to accomplish the complexity of secure software systems properly. Thus, it is crucial to have a resource for characterizing available security pattern research concerning various characteristics, not only CIA but also others such as suitable development methodologies and phases, to support practitioners select existing security pattern methods and tools, and to help systems and software security community communicate and conduct further research in security pattern methods and tools.

This paper proposes a taxonomy for characterizing and classifying security pattern research through a systematic literature review (SLR) [247]. Based on the taxonomy, we categorize and analyze 240 papers to clarify state-of-the-art and future directions of security pattern research in terms of 13 facets including topics and security characteristics. Our taxonomy and the survey results should improve communications among practitioners and researchers, standardize the terminology, and increase the effectiveness of security patterns. We summarize our contributions as follows:

- Using an SLR to identify necessary facets, we created a comprehensive taxonomy. Our taxonomy characterizes security pattern research to help practitioners choose existing security pattern methods as well as tools. Besides, our taxonomy serves as a resource for the software security community to support communication and research in security pattern methods and tools.
- We surveyed and classified existing security pattern research and clarified state-of-the-art and future directions of security pattern research based on our taxonomy. These findings should stimulate and improve security pattern research, resulting in the improvement of the effectiveness of security patterns.

The rest of this paper is organized as follows. Section 2 summarizes related work. Section 3 overviews our SLR and taxonomy construction process. Section 4 outlines our taxonomy. Sections 5 shows the survey results of the facets in the taxonomy. Section 6 shows the validation and use case of the taxonomy. Section 7 describes limitations of the taxonomy and the SLR. Finally, section 8 provides the conclusion and future work.

## 2. Related Work

Several surveys have been conducted on specific security patterns and related patterns to classify and analyze them. Nobukazu et al. [242] conducted a survey of security patterns in general; however, the number of patterns studied is limited since it was an early survey in 2008. Uzunov et al. [30] conducted a comprehensive survey of security solutions including patterns for distributed publish/subscribe systems. Washizaki et al. [245] conducted a survey of IoT patterns including security patterns for IoT systems. Laverdiere et al. [155] conducted another comprehensive survey of security patterns useful at the design phase. These surveys are not intended to reveal characteristics of security patterns in general at all phases in the software system lifecycle. Besides, none of them is a comprehensive survey of security pattern research.

Apart from the surveys of specific or general security patterns, there are some existing works on studying different research techniques and approaches for security patterns. Alvi et al. [5] conducted a study to compare various classification schemes of security patterns; in the study, other research approaches such as application and formalization are out of scope. Rajmohan et al. [246] systematically analyzed around 20 research papers that have been published around patterns and architectures for IoT security and privacy; the analysis is limited to IoT security and privacy patterns only. Ito et al. [3] conducted a systematic mapping study targeting security pattern research; however, the number
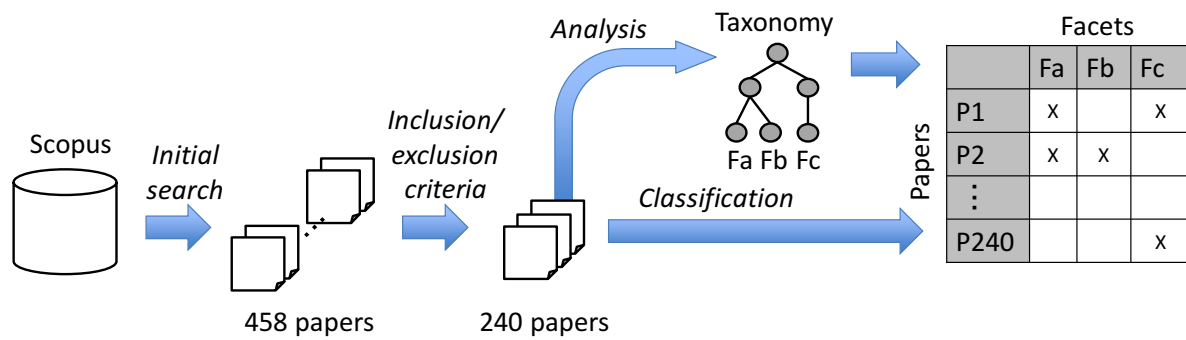
**Figure 1.** Taxonomy construction process

of research papers surveyed is limited to only 30, and it is a brief summarization of pattern research without in-depth analysis.

None of those mentioned above related works is a rigorous survey targeting many research papers on security patterns in general. In our preliminary conference paper, we reported a result of an SLR targeting more than 200 papers [248]. Since the set of papers to be analyzed was limited to those published from 1992 to early August 2016, we expanded the SLR target to include more papers published from August 2016 to 2017 in this paper. Also, we added an in-depth analysis based on the survey (such as security measurements in detail) and related works. Besides, we revised the taxonomy by removing two subfeatures "User" and "Type of pattern." We removed the former since it is quite similar to "Phase" under the same feature "Purpose." We removed the latter since it is redundant to hold in addition to "Security pattern" and "Attack pattern" under the same feature "Pattern." Also, we added a new subfeature "Pattern modeling" to the feature "Method" since it was additionally identified as an essential and independent feature in addition to "Methodology" and "Relationship between pattern."

### 3. Taxonomy Construction

The development of a taxonomy can be approached in two different ways: top-down and bottom-up [249,250]. In the top-down approach, the taxonomy is built upon existing knowledge structures, allowing established definitions and categorizations to be reused, increasing the probability of achieving an objective classification procedure [249]. Existing works have classified and analyzed security pattern research, but none have provided a comprehensive guide that takes major characteristics into account. Therefore, we adopt a top-down approach to design our taxonomy.

Figure 1 outlines how various characteristics are identified to distinguish existing security pattern studies to realize a comprehensive taxonomy, which classifies security pattern research as feature diagrams. A top-down approach is used by having four steps: determining the scope, conducting an SLR, analyzing the results, and validating the results.

1. To determine the scope, we first defined our purpose and goals. The purpose is to support the classification, comparison, reuse, and extension of security pattern research. Our goals are to improve communications about security software stakeholders such as researchers, developers, and users and improve the research achievements' availability. Thus, we aimed to develop a taxonomy to classify security patterns and standard terminology.

2. Next, we conducted an SLR aiming to aggregate existing evidence to achieve the research goal and support the construction of evidence-based guidelines for practitioners and researchers [251].

107 The SLR used Scopus [1], which is citation and abstract database provided by Elsevier, to search
108 for papers about security pattern research. The search query was the following.

109 ```
TITLE-ABS-KEY(''security pattern") AND
```
110 ```
( LIMIT-TO(SUBJAREA,''COMP") OR LIMIT-TO(SUBJAREA,''ENGI") )
```

111 Scopus was chosen because its effectiveness as a software engineering SLR has been demonstrated
112 [245,252–254]. In addition, the results can be easily exported. On October 23, 2018, our query
113 returned 484 papers published between 1992–2017. The following inclusion and exclusion criteria
114 were subsequently used to compile research on security patterns:

115 **Inclusion criteria:**

116 • Studies published in conference proceedings or journals in the form of papers employing
117 security patterns for systems and software systems engineering.

118 **Exclusion criteria:**

119 • Studies that do not employ any security pattern.
120 • Studies that introduce or propose security patterns without any further engineering
121 activities such as application of patterns.

122 Each paper was initially read by one author to determine if it was within the scope of this study.
123 If it fitted within the scope, the author analyzed it against known features used in [3], and
124 identified additional characteristics. Then another author confirmed the assessment. If these
125 classifications conflicted, all authors discussed to reach a consensus. This procedure returned 240
126 papers and their initial classification results[2].
127 3. Afterward, the identified characteristics were merged using existing methods such as CWE
128 (Common Weakness Enumeration) [255] and CVSS (Common Vulnerability Scoring System)
129 [256] as well as critical concepts clarified in the Security and Privacy Metamodel [257] to form a
130 feature diagram [258]. A feature diagram is a tree to visualize four types of relationships between
131 a parent feature and its child features (subfeatures): The first is "Mandatory," which indicates a
132 required subfeature. The second is "Optional," which denotes a voluntary feature. The third is
133 "Or," which requires at least one of the subfeatures. The fourth is "Alternative," which means only
134 one subfeature is selected among all possible subfeatures. Since a feature diagram essentially
135 defines a taxonomy, feature diagrams have been used for defining taxonomies to classify papers
136 and documents in literature reviews [259,260].
137 4. Finally, the taxonomy was validated by classifying existing security pattern research identified in
138 the SLR. Each subfeature was assigned to one of the authors to check initial classification results
139 in terms of the assigned subfeature. If the author identified classification conflicts in terms of the
140 assigned subfeature, all authors discussed to reach a consensus modify the taxonomy and/or
141 classification results.

142 **4. Constructed taxonomy**

143 Figure 2 shows our taxonomy, which includes five features as facets for characterizing and
144 classifying security pattern research.
145 The first feature is "Purpose," which includes topics addressed by security pattern research, and
146 phases of the systems and software lifecycle. These are particularly important to help practitioners
147 choose appropriate methods and tools against their needs, such as necessary supports (e.g., application

---

1 https://www.scopus.com/
2 The list of 240 papers and their analysis details are available at http://www.washi.cs.waseda.ac.jp/security/ .
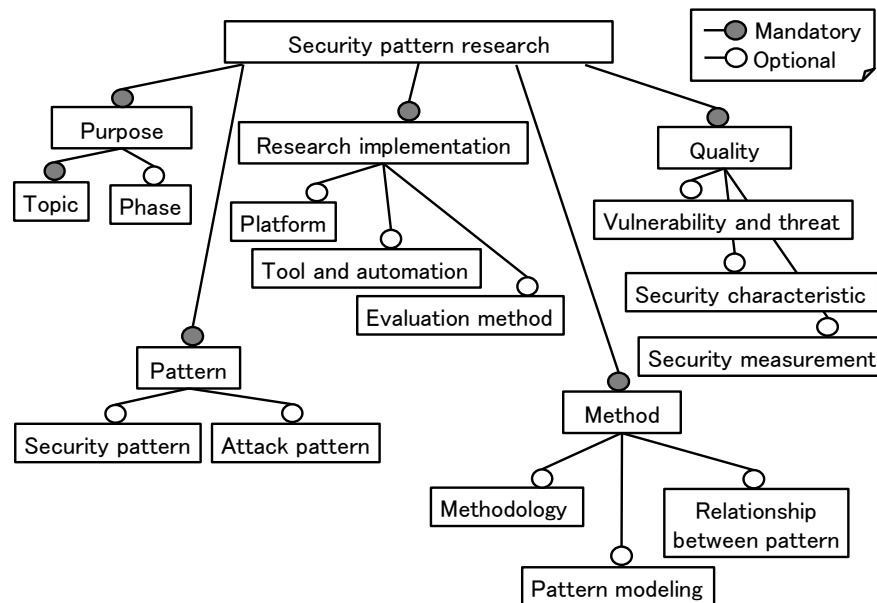
**Figure 2.** Feature diagram of the taxonomy (adopted from [248] with reduction of several features for simplification)

of security patterns) and phases necessary to be secured (e.g., secure design) by utilizing security pattern research. These are also helpful for researchers to identify each topic's and phase's maturity and envision necessary future efforts.

The second is "Research Implementation," which consists of the platform to realize the pattern research results, whether the results are encapsulated or (semi-)automated as a tool, and whether experiments or case studies are performed to evaluate the results relevant to the original research purpose. These are important to help practitioners choose easy-to-use or empirically validated methods on targeted platforms. These are also helpful for researchers to identify each research area's maturity and envision necessary future efforts.

The third is "Quality," which consists of items related to quality characteristics: Threats and vulnerabilities toward a specific security problem; security characteristics in detail such as privacy, integrity, and availability; and whether a security measurement system is incorporated in order to detect changes in security by introducing or applying the research results. These are useful for choosing and carefully using specific methods and tools by understanding their impact on quality characteristics. These are also helpful for researchers to envision necessary future efforts concerning quality aspects, including security and privacy.

The fourth is "Pattern," which includes the types of patterns employed or addressed in the pattern research. Patterns that address security concerns can be classified into two types: security patterns and attack patterns. The former addresses both recurring security problems and corresponding solutions from the viewpoint of defenders to security risks, while the latter addresses only security problems from the viewpoint of malicious attackers by detailing security risks. These are useful for choosing specific methods and tools against intended patterns, especially when practitioners examine specific patterns for use. These are also helpful for researchers to envision necessary future efforts in terms of each specific pattern.

The fifth is "Method," which includes the methodology, pattern modeling notations, and pattern relationships. These are useful for considering the adaptability of specific methods and tools to ongoing or intended development contexts, including development methodologies, modeling notations, and patterns considered to be used. These are also helpful for researchers to envision necessary future efforts concerning development contexts and security pattern combinations.
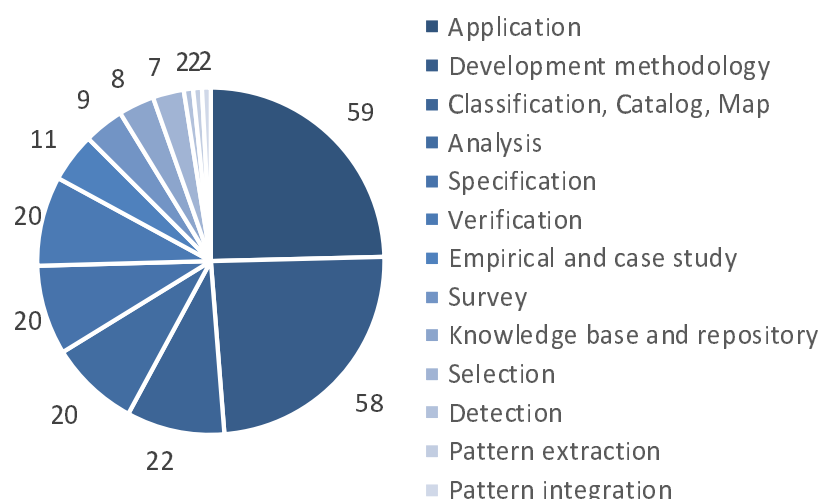
**Figure 3.** Breakdown of topics (adopted from [248] with updates of numbers)

## 5. Survey results

The 240 papers identified in the SLR are classified by the 13 facets defined in the taxonomy to clarify state-of-the-art approaches and future research directions. Below, we summarize how the taxonomy helps characterization and classification of papers on security pattern research.

*5.1. Purpose*

5.1.1. Topic

Figure 3 divides the 240 papers by research topic. Most papers propose or report applications of patterns during systems and software development, certain development methodologies, and pattern classification. Empirical and case study reports are limited, indicating that future research should consider case studies, methodologies, and applied experiments.

Although security patterns have been documented and reported at conferences such as PLoP [3] since the late 1990s, patterns are still manually identified and extracted. Pattern extraction is rarely reported (i.e., 1%) [11,13] in research papers. Mechanisms for identifying and extracting security patterns are highly anticipated, but in reality, research is not being conducted on this topic. Similarly, automatically identifying critical attack and security patterns is desired to determine coding requirements and design, but these topics are not extensively researched as only 8% of papers report pattern specifications and verification. Hence, more research on these topics should be conducted in the future.

5.1.2. Phase of lifecycle

As shown in table 1, we categorized the papers into 16 phases. Each paper is categorized into zero or more phases. Numerous phases from "Analysis" to "Evolution" can be research targets. Besides, if target phases are not clearly specified in a paper, the paper is categorized as "Any"; each paper should be classified into more concrete phases as possible.

The most commonly investigated phases are "Design" followed by "Analysis" and "Implementation." Hence, research targets are skewed towards the earlier phases. Few report post-implementation phases including "Evolution" and "Maintenance," suggesting that security

---

[3] https://www.hillside.net/plop/

**Table 1.** Phases targeted by security pattern research

| Phase | Number of papers |
|---|---|
| Design | 123 |
| Analysis | 68 |
| Implementation | 37 |
| Any | 18 |
| Development | 14 |
| Test | 7 |
| Operation | 6 |
| Maintenance | 5 |
| Modeling | 5 |
| Run | 4 |
| Deployment | 3 |
| Evolution | 3 |
| Verification | 2 |
| Evaluation | 1 |
| Integration | 1 |
| Disposal | 1 |

pattern research in later phases may be a frontier field. Cutting-edge topics include multi-dimensional classification of patterns [16], detection of patterns from the program source code [41], improvement of existing legacy software systems using patterns [10], and security patterns for operational dynamics [181]. Classifying security patterns for the system lifecycle, defining and formalizing patterns that address dynamic behaviors, and utilizing defined patterns in existing software systems are topics that should be further examined.

*5.2. Research implementation*

5.2.1. Platform

Among the 240 papers, 25% (61) are platform specific (Fig. 4), including Ambient Intelligence Environments, Business Process Management (BPM), and Multi-Agent Systems (MAS). Most reports use general platforms like the web, cloud, and distributed system.

A few papers address Cyber Physical Systems (CPS) and the Internet of Things (IoT) [227,233], and 75% do not refer to a specific computing platform. Since various IoT security patterns are emerging, active research on platforms involving IoT, cloud, and their applications is desirable.

5.2.2. Tool and automation

As shown in figure 5, about 34% (82 papers) mention tools or automation. Many use tools and approaches that involve modeling. A few also include aspect-oriented approaches, formal verification, and code generation. Because the majority of reports create a unique tool, there are many tools for modeling, analysis, design, and implementation. However, few studies propose testing tools (such as model-based testing [179,209]) and operating tools (such a runtime framework [40,171,173,199]).

Tools should span the entire lifecycle because security issues appear in all phases. Hence, future studies should develop tools that directly incorporate security patterns in the testing and operation phases.

5.2.3. Evaluation method

About half (51.6%, 124 papers) incorporate an evaluation by implementing a case study (19.5%), referencing examples (15%), and conducting experiments (4.1%). Additionally, 12.9% report using an evaluation without specifying the method.
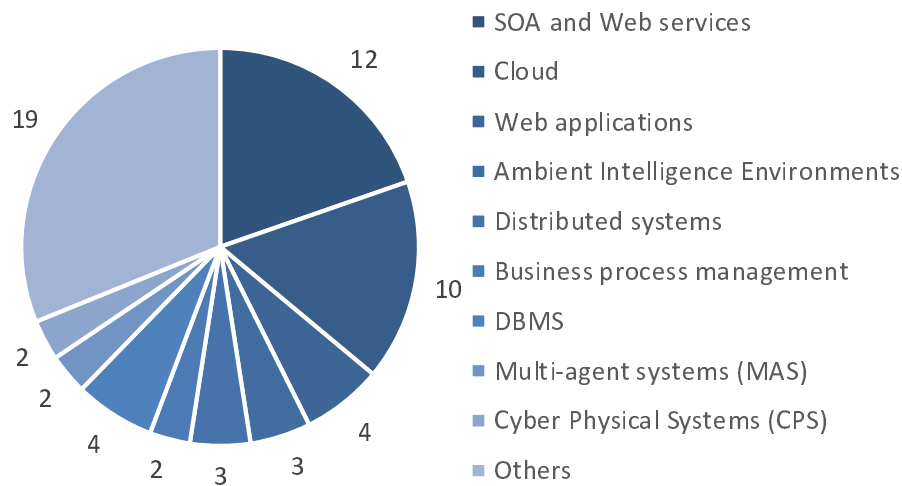
**Figure 4.** Breakdown of computing platforms (adopted from [248] with updates of numbers)
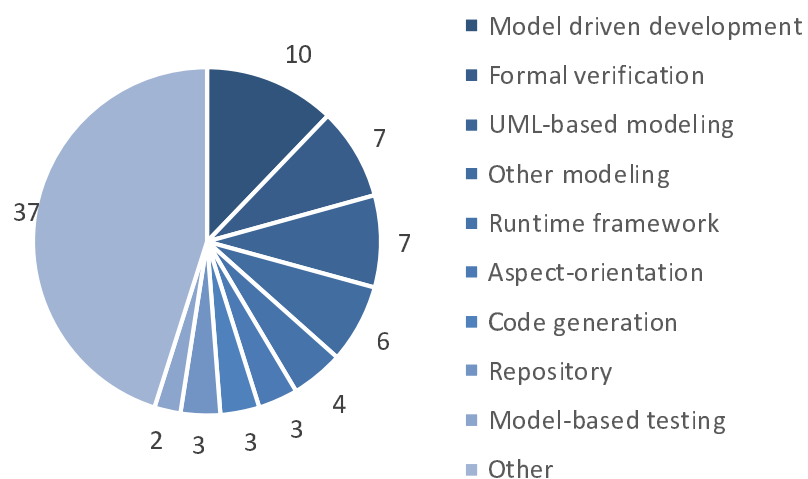


**Figure 5.** Breakdown of tools and automation (adopted from [248] with updates of numbers)

The findings indicate that evaluations of security pattern usage are an immature research area. Even if an evaluation is conducted, it is often limited to a case study or referencing an example. Stricter evaluation methods (e.g., a control experiment) are almost non-existent. More rigorous evaluation methods are expected in the future to improve the maturity, usefulness, and validity of security pattern research.

*5.3. Quality*

5.3.1. Vulnerability and threat

Vulnerabilities or threats are mentioned in 29.6% (71) of the papers. Only 1.2% (3 [50,189,219])[4] refer to STRIDE [261], which is advocated by Microsoft, while another 2.5% (6) refer to other publicly available information in terms of vulnerabilities and threats. Among these six papers, one [10] references CVSS [256], which summarizes risk information. Four papers reference more tangible vulnerability information such as CWE [255] and CVE (Common Vulnerability and Exposures) [262]. Furthermore, one paper [214] refers to CAPEC (Common Attack Pattern Enumeration and Classification) [263], which categorizes known attacks employed by adversaries.

Security patterns should clearly explain how to deal with security measures that involve addressing system vulnerabilities and threats. Thus, the fact that more than 70% of the papers do not mention vulnerabilities or threats is troublesome. Future research should collect both the theoretical and actual relationships on vulnerabilities and threats to achieve practical uses of security patterns. Currently, few papers refer to publicly available information on known vulnerabilities and threats. Consequently, future research should investigate how to utilize such publicly available information and increase the awareness of security patterns.

5.3.2. Security characteristic

Over half (58.8%, 141) mention security characteristics. Of the 141 papers, 91.5% (129) refer CIA characteristics. In these papers, there are 109, 84, and 71 references to confidentiality, integrity, and availability, respectively (Fig. 7).

Another 37 papers reference non-CIA security characteristics such as accountability, authenticity, authentication, authorization, and nonrepudiation. 25 of these mention both CIA and non-CIA characteristics, while 12 mention non-CIA characteristics only.

We confirmed that many studies examine security characteristics, especially those based on CIA. Confidentiality, which allows only individuals with granted permission to access information, is essential and the most mentioned characteristic. One example involving privacy and confidentiality is Role-Based Access Control (RBAC).

5.3.3. Security measurement

Only a few papers (10.8%, 26) adopted security measurements to evaluate patterns. Two used STRIDE [261]. [57] evaluated the handling of potential threats via a graph and indicated STRIDE's attack categories against secure and non-secure systems. [141] evaluated the system against security attacks by using STRIDE. Their evaluation based on fuzzy logic defined five levels for the five main events, where the levels correspond to a STRIDE's category.

The following list summarizes other measurements in the literature. The numbers of levels and categories are different, and each level and category are defined differently. The majority of

---

[4] Although more papers refer to STRIDE, most do not incorporate STRIDE into their proposed techniques or achievements. For example, in [45], STRIDE is not handled in the proposed security testing technique; STRIDE is mentioned just in its case study in terms of threat identification without detailed explanations [45]. By excluding such papers, we finally identified that three papers [50,189,219] incorporate STRIDE into their research techniques or achievements in terms of threat identification modeling and classification.
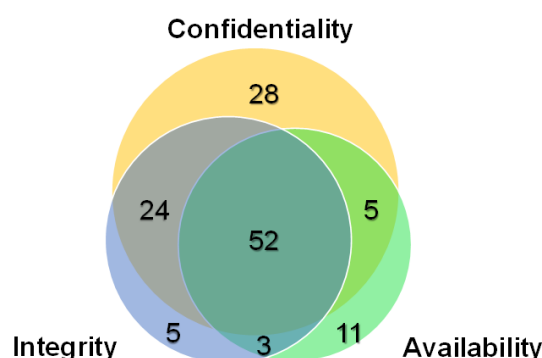
**Figure 6.** Breakdown of the security characteristics (adopted from [248] with updates of numbers)

them employ an approach to evaluate three to five discrete levels for the likelihood of exposing vulnerabilities and their effects on the system associated with security patterns.

- In [5], security patterns found in 23 papers are grouped into 14 categories. Then the categories are evaluated using nine levels of quality standard classifications.
- In [26], forces and Solution are used to evaluate attribute, risk reduction frequency, risk reduction consequence, annual number of attacks, cost per attack, and cost solution. Furthermore, XSS (Cross Site Scripting) is evaluated as a case study.
- In [29], seven levels of security criteria are used to compare and evaluate nine security patterns. In addition, performance gain and loss is compared. The implementation cost and degree of security are also evaluated in three levels.
- In [37], the following three categories are used for evaluating security pattern description elements (problem and forces, structure description, structure image, behavior description, behavior image, consequences, and example): not provided, minimal, and satisfactory.
- In [39], measures against possible threats are evaluated using a graph.
- In [59], resource access restrictions granted to different roles are evaluated in terms of four operations: C (create), R (retrieve), U (update), and D (delete).
- [76] supports an aspect-oriented approach and proposes an evaluation using Object Constraint Language (OCL) for Account Lockout with Selective Logging (ALSEL) and IMAP system.
- In [[116], nine levels of quality are used to evaluate nine concerns such as threats and attacks to be avoided, an attack pattern to be applied, threats to be passed, and security requirements.
- In [125], security patterns of eight categories such as accountability, confidentiality, and integrity are evaluated.
- In [152], security patterns of a distributed system are categorized and five quality indicators are evaluated.
- In [155], using the $6\sigma$ approach, 12 security patterns are evaluated by 6 categories of undesirable properties.
- In [200], using its own unique evaluation formula, the applicability of patterns is calculated as rate.
- In [202], three indices (completeness, isolation, and verifiability) are used as the engineering principles of security kernel.
- [203] is related to security patterns of a grid system. Password and digital signature are expressed as graphic extension of Backus normal form (a.k.a. Backus–Naur form) in the authentication pattern.
- In [204], using an example of an ATM terminal, security objects, and patterns are described and evaluated in eight matrices.
- [205] categorizes patterns into three layers and evaluates them.

Because each research paper used its own evaluation categories, assessing the evaluation results' applicability is challenging. In the future, a standard index such as STRIDE should be used to evaluate results to have comparable security pattern research.

**Table 2.** Major security patterns mentioned in at least ten papers (adopted from [248] with updates of numbers and descriptions)

| Security pattern | Number of appearances |
| --- | --- |
| Role-Based Access Control (RBAC) | 49 |
| Authorization | 34 |
| Authentication | 23 |
| Access control | 21 |
| Authenticator | 21 |
| Secure logger | 19 |
| Check point | 17 |
| Reference monitor | 15 |
| Secure pipe | 14 |
| Single access point | 13 |
| Authentication enforcer | 11 |
| Attribute-Based Access Control (ABAC) | 10 |
| Encrypted Storage | 10 |
| Firewall | 10 |
| Replicated system | 10 |

*5.4. Security related patterns*

5.4.1. Security pattern

Most papers (77.9%, 187) mention a specific security pattern by name. On average, each paper mentions 4.9 patterns. Although there are 1179 references to a pattern name, only 558 are unique patterns. Of these, 31.5% (176 patterns) are mentioned in at least two papers. By the definition of the word "pattern," a software pattern should be used by many practitioners. However, this study reveals that the majority of patterns ( 70%) are not actually shared. As shown in table 2, only 16 patterns are mentioned in 10+ papers. These patterns are related to authentication, authorization, and access control.

Ironically, over 22% of the papers on security patterns do not mention a certain pattern by name. Without a pattern name, it is difficult to explain a new idea or method. Our results reveal about one-third of the patterns are common; using easy-to-use directed graph representations such as UML class diagrams would contribute to their high reusability. Although many research papers express patterns without specific names, this will become more challenging in the future as research expands to include concepts that are often hard to describe by a structural description such as availability.

5.4.2. Attack pattern

Attack patterns are much less prevalent than security patterns. Only 17.0% (41) papers mention attack patterns. Many patterns are mentioned in only one paper. Table 3 summarizes patterns mentioned in multiple papers.

Moreover, the abstraction varies widely. Some refer to abstract attack patterns in STRIDE, which is a categorization of attack patterns. Others discuss CIA security characteristics. One is specific to illegal money transfers in a certain application. Although attack patterns and security characteristics are common, specific examples are rare.
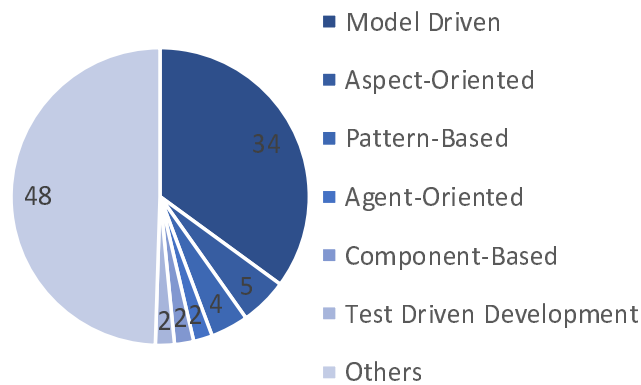
*5.5. Method*

5.5.1. Methodology

97 papers (40.4%) describe a development methodology (Fig. 7). Some discuss a methodology related to a model-driven development approach (14.2%) or an aspect-oriented development approach

**Table 3.** Appearances of attack patterns in at least two papers (adopted from [248] with updates of numbers and descriptions)

| Attack pattern | Number of appearances |
|---|---|
| Spoofing | 6 |
| Denial-of-service (DoS) | 5 |
| Misuse | 5 |
| Information disclosure | 4 |
| Injection | 4 |
| Tampering | 4 |
| Malicious Virtual Machine Migration | 3 |
| Elevation of privilege | 2 |
| Integrity | 2 |
| Message secrecy violation | 2 |
| Repudiation | 2 |
| Resource usage monitoring | 2 |
| Session state poisoning | 2 |
| Theft of services | 2 |



**Figure 7.** Papers referencing the intended development methodology (adopted from [248] with updates of numbers)

(2.1%). Although many development methodologies are reported, few examine security-focused methodologies. As IoT becomes ubiquitous, studies on the methodology should intentionally focus on security by design.

5.5.2. Pattern modeling notation

The types of modeling notations used in security-pattern research are examined. About two-third of the papers represent the notations of security patterns, which can be categorized into six groups. Table 4 shows the groupings, where multiple groups indicate papers using multiple notations. The "UML" group includes UML diagrams and UML based notations. The "Goal-oriented," "Formal," and "Natural language" groups include models used in goal-oriented methods, formal notations, and natural language notations, respectively.

Security patterns are mostly UML, which is reasonable since UML is generally accepted for modeling software and systems. In papers that address specific development methods or tools, formal, goal-oriented, and natural language notations are used in 13, 12, and 12 papers, respectively. Moreover, about one-third of papers do not describe the notations of security patterns. In the future, the notation should be described to clarify security patterns.

**Table 4.** Pattern modeling notation

| Group | Example | Number of papers |
|---|---|---|
| UML | Class/Activity diagram | 104 (43.3%) |
| Goal oriented | i*, KAOS, threat tree | 13 (5.4%) |
| Formal | Z notation, formula | 12 (5.0%) |
| Natural language | Text, structured document | 12 (5.0%) |
| Original | Original notations | 6 (2.5%) |
| Others | Process model, XML, OWL | 65 (27.1%) |
| Not specified | | 77 (32.1%) |

5.5.3. Relationship between patterns

Because security patterns are often used and applied as combinations, their relationships must be clarified. Relationships between patterns can be classified into two types: between security patterns (relationship A) to enhance described security methods by combination, and between an attack pattern and a corresponding security pattern to reduce security risks (relationship B).

Of the 240 papers, 98 papers (40.8%) focus on relationship A. Only 5.8% (14) mention relationship B. These results demonstrate that security pattern combinations are often not considered. In the future, more research needs to be conducted with an emphasis on relationship B. Such research is expected to reveal how security patterns reduce risks imposed by attack patterns in specific development processes.

## 6. Validation and Use case of Taxonomy

There are multiple methods to validate a taxonomy. Examples include demonstrating the orthogonality of its classification features, benchmarking against existing classification schemes, or confirming its utility to classify existing knowledge [264]. Herein orthogonality means that a paper can be classified as only one category of possible combinations of concrete features. We validated our taxonomy by classifying the research papers identified in the SLR. Because fitting of each characteristic gave only one classification category shown in the survey results in section 5, the classification features are orthogonal.

Besides, we validated our taxonomy by classifying the four latest popular papers[5] that are not included in the SLR. Tables 5, 6, 7, and 8 show the classification results of these papers using our taxonomy.

We summarized the results aligned with classification features as follows.

- Purpose: Three-quarters of the papers report security pattern applications targeting the earlier phases, including analysis and design.
- Research Implementation: Half of the papers use cloud as their application platform. Half mention tools. Evaluations of security patterns are limited to an example or a case study.
- Quality: Half of the papers mention vulnerabilities or threats. Only one paper refers to publicly available information regarding vulnerabilities and threats (i.e., STRIDE). All studies examine security characteristics based on the CIA. Only one paper adopts security measurements.
- Pattern: All papers focus on security patterns only.
- Method: Half of the papers describe some development methodologies. Three-quarters represent the pattern modeling notations, including UML as the most major one. None of the papers explicitly handle security pattern combinations.

---

[5] On December 30th, 2020, we applied the same search query for papers published in or after 2018 at Scopus. Our query returned 129 papers. By applying the inclusion and exclusion criteria to them, we confirmed that 66 papers fit within our study's scope. Among 66, we selected the top four mostly-cited papers that meet the inclusion criteria. The list of these latest 129 papers is available at http://www.washi.cs.waseda.ac.jp/security/ .

**Table 5.** Classification of latest papers: Purpose and Research implementation

| Paper | Topic | Phase | Platform | Tool | Evaluation |
|---|---|---|---|---|---|
| [265] | Application | Design | Cloud | Model-driven development | Example |
| [266] | Survey | Design | Cloud | – | – |
| [267] | Application | Design | IoT | – | – |
| [268] | Application | Analysis | – | Goal-oriented modeling | Case study |

**Table 6.** Classification of latest papers: Quality

| Paper | Vulnerability | Characteristic | Measurement |
|---|---|---|---|
| [265] | – | Integrity, Availability | Security level |
| [266] | Vulnerabilities, threats | Confidentiality, Integrity, Availability | – |
| [267] | – | Confidentiality | – |
| [268] | STRIDE, threats | Confidentiality, Integrity, Availability | – |

Since these trends are quite similar to those of our SLR for 240 papers published in 1992-2017, we believe our taxonomy and SLR results are still applicable to the latest situation and useful. Moreover, we confirmed that we successfully classified the latest popular papers according to the characteristics defined in our taxonomy and show how it can help classify security pattern research papers.

Based on the classification capability, our taxonomy should guide practitioners and researchers in the two use cases (UCs).

- **UC1** is to help practitioners select appropriate security pattern methods and tools. When practitioners want to reuse and eventually extend existing methods and tools, these must be compared prior to selecting the most appropriate one for the scenario. Selection should be based on how the methods and tools meet the intended objectives. The taxonomy helps compare criteria to assess methods and tools according to their characteristics.
- **UC2** is to communicate and research methods and tools. researchers. By incorporating the characteristics of security pattern research into a single structure, the taxonomy can serve as a framework to guide future communications and research on security pattern methods and the corresponding tools. For example, the taxonomy can serve as the basis to build an open repository of information of existing methods and tools. Moreover, the taxonomy should stimulate and improve security pattern research, resulting in improvement of the effectiveness of security patterns.

## 7. Limitation

Since papers (such as [6,11,45]) dealing with attack patterns often mention them together with related security patterns, we used the term "security pattern" only for the search query. Nevertheless,

**Table 7.** Classification of latest papers: Pattern

| Paper | Security pattern | Attack pattern |
|---|---|---|
| [265] | Protection Reverse Proxy | – |
| [266] | Authorization, Authentication, Logging/Auditing | – |
| [267] | Reference Monitor, Role Based Access Control (RBAC), Remote Authenticator/Authorizer, Matrix Authentication, File Authentication | – |
| [268] | Alternative service, Client Checking, Separation of Duty, Certification authority, Supervision Relation, Access Control, Auditing, Input Guard, Server sandbox, Firewall, Replicated System, Load Balancer, Limited View, Full View with Errors, Secure Access Layer, Secure Pipe, Storage Encryption, Equipment siting and protection, Supporting Utility, Physical Entry Control, Cabling security | – |

**Table 8.** Classification of latest papers: Method

| Paper | Methodology | Modeling | Relationship |
|-------|-------------|----------|--------------|
| [265] | Model-driven | UML, Operational Flow Language | – |
| [266] | – | UML | – |
| [267] | – | – | – |
| [268] | Goal-oriented requirements engineering | Goal-oriented model | – |

we may miss research papers that deal with attack papers only without mentioning security patterns. To address this issue, we plan to extend the search query to include the term "attack pattern."

Research papers are often published in conference proceedings first and refereed journals second, and later rarely books. To narrow down the survey scope to a specific range of targets, we limit the target publication to a paper in a journal or conference proceeding. Nevertheless, we may miss some books or book chapters describing the latest security pattern research achievements that are not published in conference proceedings or journals. We plan to extend the survey's target scope to include books and book chapters to address this issue.

We chose Scopus as the search engine since it is effectively used in SLRs of software engineering, and the search results can be exported. The database covers many major publishers, including IEEE, ACM, Springer Nature, Wiley Blackwell, Taylor & Francis, and Elsevier. Furthermore, the database provides a mechanism to perform keyword searches. Although many other SLRs have adopted it, relevant papers may have been missed. To mitigate this issue, we plan to use other databases, extend our SLR, and elicit a public review of the results.

Our SLR's targets are papers published in 1992-2017. And, we confirmed that the results are still applicable to the latest situation by examining the top four mostly-cited papers out of 66 latest papers published in 2018-2021. Since these four papers are the most cited ones, we believe that these can represent the latest 66 papers' trend to some extent. Nevertheless, we still need to continue validating the trends by enhancing our SLR to include the latest publications since other less-cited 62 papers may indicate different directions.

## 8. Conclusion and Future Work

It is crucial to have a resource for characterizing available security pattern research concerning various characteristics, not only CIA but also others such as suitable development methodologies and phases, to help practitioners select appropriate security pattern methods and tools, and to help systems and software security community to communicate and research in methods and tools.

To respond to the necessity, we devised a new comprehensive taxonomy for security pattern research via an SLR. Herein 13 facets are used to define the taxonomy. To clarify the state-of-the-art and future directions of security pattern research from various facets, including topics and security characteristics, this taxonomy analyzed the contents of 240 security pattern research papers identified through an SLR, demonstrating its usefulness. This taxonomy should also support communications among researchers, practitioners, and stakeholders. Hence, it should improve not only the quality of security pattern research but also the effectiveness of security patterns.

The analysis results are summarized along with five features as follows.

- Purpose: Most papers report applications of security patterns, development methodologies, and pattern classification. Research targets are skewed towards the earlier phases, including analysis and design.
- Research Implementation: Most papers use general platforms like the web, cloud, and distributed systems. Only around one third mention tools or automation. Evaluations of security pattern usage are an immature research area since it is often limited to a case study or referencing an example even if an evaluation is conducted.

- Quality: Vulnerabilities or threats are mentioned in only less than one-third of the papers. Many studies examine security characteristics, especially those based on the CIA. Only a few papers adopted security measurements to evaluate patterns.
- Pattern: There are attack patterns and security patterns, but most focus on security patterns and not attack patterns. Most papers mention a specific security pattern by name. There are more than 230 unique security patterns mentioned.
- Method: Around two-fifths describe some development methodologies, in which the model-driven approach is the most major one. About two-thirds represent the pattern modeling notations, including UML as the most major one. Security pattern combinations are often not considered.

Future efforts include experimentally verifying our taxonomy using the two use cases (UC1 and UC2) in section 6. We will implement a collaborative Wiki so that the community can refine and modify the taxonomy online. Besides, we intend to enhance our SLR to include the latest publications that have been published in or after 2018 to confirm the identified research trends and gaps in this paper still exist. Also, we will extend our SLR using additional databases and additional categories. Our findings will be shared with the public so that our taxonomy can be validated and revised by the community, and standard terminology can be defined.

**Author Contributions:** Conceptualization and methodology, Hironori Washizaki.; literature review and analysis, all authors. All authors have read and agreed to the published version of the manuscript.

## References

1. Schumacher, M.; Fernández-Buglioni, E.B.; Hybertson, D.; Buschmann, F.; Sommerlad, P. *Security Patterns - Integrating Security and Systems Engineering*; Wiley, 2005.
2. Yoshioka, N.; Washizaki, H.; Maruyama, K. A survey on security patterns. *Progress in Informatics* **2008**, pp. 35–48.
3. Ito, Y.; Washizaki, H.; Yoshizawa, M.; Fukazawa, Y.; Okubo, T.; Kaiya, H.; Hazeyama, A.; Yoshioka, N.; Fernandez, E. Systematic Mapping of Security Patterns Research. 22nd Conference on Pattern Languages of Programs Conference (PLoP), 2015, pp. 1–7.
4. Bouaziz, R.; Kallel, S.; Coulette, B. A Collaborative Process for Developing Secure Component Based Applications. 2014 IEEE 23rd International WETICE Conference, WETICE 2014, Parma, Italy, 23-25 June, 2014; Reddy, S., Ed. IEEE Computer Society, 2014, pp. 306–311.
5. Alvi, A.K.; Zulkernine, M. A Comparative Study of Software Security Pattern Classifications. Seventh International Conference on Availability, Reliability and Security, Prague, ARES 2012, Czech Republic, August 20-24, 2012. IEEE Computer Society, 2012, pp. 582–589.
6. Uzunov, A.V.; Fernández, E.B.; Falkner, K. A Comprehensive Pattern-Driven Security Methodology for Distributed Systems. 23rd Australian Software Engineering Conference, ASWEC 2014, Milsons Point, Sydney, NSW, Australia, April 7-10, 2014. IEEE Computer Society, 2014, pp. 142–151.
7. Uzunov, A.V.; Falkner, K.E.; Fernández, E.B. A comprehensive pattern-oriented approach to engineering security methodologies. *Inf. Softw. Technol.* **2015**, *57*, 217–247.
8. Bouaziz, R.; Kammoun, S. A Decision Support Map for Security Patterns Application. Computational Science and Its Applications - ICCSA 2015 - 15th International Conference, Banff, AB, Canada, June 22-25, 2015, Proceedings, Part IV; Gervasi, O.; Murgante, B.; Misra, S.; Gavrilova, M.L.; Rocha, A.M.A.C.; Torre, C.M.; Taniar, D.; Apduhan, B.O., Eds. Springer, 2015, Vol. 9158, *Lecture Notes in Computer Science*, pp. 750–759.
9. Balopoulos, T.; Gymnopoulos, L.; Karyda, M.; Kokolakis, S.; Gritzalis, S.; Katsikas, S.K. A Framework for Exploiting Security Expertise in Application Development. Trust and Privacy in Digital Business,

Third International Conference, TrustBus 2006, Krakow, Poland, September 4-8, 2006, Proceedings; Fischer-Hübner, S.; Furnell, S.; Lambrinoudakis, C., Eds. Springer, 2006, Vol. 4083, *Lecture Notes in Computer Science*, pp. 62–70.

10. Guan, H.; Wang, X.; Yang, H. A framework for security driven software evolution. 20th International Conference on Automation and Computing, ICAC 2014, Cranfield, Bedfordshire, United Kingdom, September 12-13, 2014; Luo, X.; Cao, Y.; Tong, Z., Eds. IEEE, 2014, pp. 194–199.

11. Singpant, P.; Prompoon, N. A Method for Web Security Context Patterns Development from User Interface Guidelines Based on Structural and Textual Analysis. Information Science and Applications; Kim, K., Ed. Springer, 2015, Vol. 339, *Lecture Notes in Electrical Engineering*, pp. 541–550.

12. Abramov, J.; Anson, O.; Dahan, M.; Shoval, P.; Sturm, A. A methodology for integrating access control policies within database development. *Comput. Secur.* **2012**, *31*, 299–314.

13. Ryoo, J.; Laplante, P.A.; Kazman, R. A Methodology for Mining Security Tactics from Security Patterns. 43rd Hawaii International International Conference on Systems Science (HICSS-43 2010), Proceedings, 5-8 January 2010, Koloa, Kauai, HI, USA. IEEE Computer Society, 2010, pp. 1–5.

14. Fernandez, E.B.; Larrondo-Petrie, M.M.; Sorgente, T.; Vanhilst, M., A methodology to develop secure systems using patterns; Integrating Security and Software Engineering: Advances and Future Visions, 2006; pp. 107–126.

15. Hamid, B.; Percebois, C. A Modeling and Formal Approach for the Precise Specification of Security Patterns. Engineering Secure Software and Systems - 6th International Symposium, ESSoS 2014, Munich, Germany, February 26-28, 2014, Proceedings; Jürjens, J.; Piessens, F.; Bielova, N., Eds. Springer, 2014, Vol. 8364, *Lecture Notes in Computer Science*, pp. 95–112.

16. VanHilst, M.; Fernández, E.B.; Braz, F.A. A Multi-Dimensional Classification for Users of Security Patterns. *J. Res. Pract. Inf. Technol.* **2009**, *41*, 87–118.

17. Alvi, A.K.; Zulkernine, M. A Natural Classification Scheme for Software Security Patterns. IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, DASC 2011, 12-14 December 2011, Sydney, Australia. IEEE Computer Society, 2011, pp. 113–120.

18. Mourad, A.; Otrok, H.; Baajour, L. A Novel Approach for the Development and Deployment of Security Patterns. Proceedings of the 2010 IEEE Second International Conference on Social Computing, SocialCom / IEEE International Conference on Privacy, Security, Risk and Trust, PASSAT 2010, Minneapolis, Minnesota, USA, August 20-22, 2010; Elmagarmid, A.K.; Agrawal, D., Eds. IEEE Computer Society, 2010, pp. 914–919.

19. Abramov, J.; Sturm, A.; Shoval, P. A Pattern Based Approach for Secure Database Design. Advanced Information Systems Engineering Workshops - CAiSE 2011 International Workshops, London, UK, June 20-24, 2011. Proceedings; Salinesi, C.; Pastor, O., Eds. Springer, 2011, Vol. 83, *Lecture Notes in Business Information Processing*, pp. 637–651.

20. Benameur, A.; Fenet, S.; Saïdane, A.; Sinha, S.K. A Pattern-Based General Security Framework: An eBusiness Case Study. 11th IEEE International Conference on High Performance Computing and Communications, HPCC 2009, 25-27 June 2009, Seoul, Korea. IEEE, 2009, pp. 339–346.

21. Schnjakin, M.; Menzel, M.; Meinel, C. A pattern-driven security advisor for service-oriented architectures. Proceedings of the 6th ACM Workshop On Secure Web Services, SWS 2009, Chicago, Illinois, USA, November 13, 2009; Damiani, E.; Proctor, S.; Singhal, A., Eds. ACM, 2009, pp. 13–20.

22. Delessy, N.A.; Fernández, E.B. A Pattern-Driven Security Process for SOA Applications. Proceedings of the The Third International Conference on Availability, Reliability and Security, ARES 2008, March 4-7, 2008, Technical University of Catalonia, Barcelona , Spain. IEEE Computer Society, 2008, pp. 416–421.

23. Ratchakom, M.; Prompoon, N. A process model design and tool support for information assets access control using security patterns. *2011 Eighth International Joint Conference on Computer Science and Software Engineering (JCSSE)* **2011**, pp. 307–312.

24. Halkidis, S.T.; Chatzigeorgiou, A.; Stephanides, G. A qualitative analysis of software security patterns. *Comput. Secur.* **2006**, *25*, 379–392.

25. Ruiz, J.F.; Rudolph, C.; Maña, A.; Arjona, M. A security engineering process for systems of systems using security patterns. IEEE International Systems Conference, SysCon 2014, Proceedings, Ottawa, ON, Canada, March 31 - April 3, 2014. IEEE, 2014, pp. 8–11.

26. Varela-Vaca, A.J.; Warschofsky, R.; Gasca, R.M.; Pozo, S.; Meinel, C. A Security Pattern-Driven Approach toward the Automation of Risk Treatment in Business Processes. International Joint Conference

CISIS'12-ICEUTE'12-SOCO'12 Special Sessions, Ostrava, Czech Republic, September 5th-7th, 2012; Herrero, Á.; Snásel, V.; Abraham, A.; Zelinka, I.; Baruque, B.; Quintián-Pardo, H.; Calvo-Rolle, J.L.; Sedano, J.; Corchado, E., Eds. Springer, 2012, Vol. 189, *Advances in Intelligent Systems and Computing*, pp. 13–23.

27. Fernández, E.B.; Monge, R. A security reference architecture for cloud systems. Proceedings of the WICSA 2014 Companion Volume, Sydney, NSW, Australia, April 7-11, 2014; Liu, A.; Klein, J.; Tang, A., Eds. ACM, 2014, pp. 3:1–3:5.

28. Tekbacak, F.; Tuglular, T.; Dikenelli, O. A Semantic Based Certification and Access Control Approach Using Security Patterns on SEAGENT. Proceedings of the Twentieth International Conference on Software Engineering & Knowledge Engineering (SEKE'2008), San Francisco, CA, USA, July 1-3, 2008. Knowledge Systems Institute Graduate School, 2008, pp. 741–744.

29. Rosado, D.G.; Fernández-Medina, E.; Piattini, M.; Gutiérrez, C. A Study of Security Architectural Patterns. Proceedings of the The First International Conference on Availability, Reliability and Security, ARES 2006, The International Dependability Conference - Bridging Theory and Practice, April 20-22 2006, Vienna University of Technology, Austria. IEEE Computer Society, 2006, pp. 358–365.

30. Uzunov, A.V. A survey of security solutions for distributed publish/subscribe systems. *Comput. Secur.* **2016**, *61*, 94–129.

31. Ahmed, N.; Matulevicius, R. A taxonomy for assessing security in business process modelling. IEEE 7th International Conference on Research Challenges in Information Science, RCIS 2013, Paris, France, May 29-31, 2013; Wieringa, R.J.; Nurcan, S.; Rolland, C.; Cavarero, J., Eds. IEEE, 2013, pp. 1–10.

32. Bergmann, G.; Massacci, F.; Paci, F.; Tun, T.T.; Varró, D.; Yu, Y. A Tool for Managing Evolving Security Requirements. IS Olympics: Information Systems in a Diverse World - CAiSE Forum 2011, London, UK, June 20-24, 2011, Selected Extended Papers; Nurcan, S., Ed. Springer, 2011, Vol. 107, *Lecture Notes in Business Information Processing*, pp. 110–125.

33. Fernández, E.B.; Sorgente, T.; Larrondo-Petrie, M.M. A UML-Based Methodology for Secure Systems: The Design Stage. Security in Information Systems, Proceedings of the 3rd International Workshop on Security in Information Systems, WOSIS 2005, In conjunction with ICEIS2005, Miami, USA, May 2005; Fernández-Medina, E.; Castro, J.C.H.; Castro, L.J.G., Eds. INSTICC Press, 2005, pp. 207–216.

34. Fernandez, E.B.; Washizaki, H.; Yoshioka, N. Abstract Security Patterns. Proceedings of the 15th Conference on Pattern Languages of Programs; Association for Computing Machinery: New York, NY, USA, 2008; PLoP '08.

35. Fernández, E.B.; Yoshioka, N.; Washizaki, H.; Yoder, J.W. Abstract security patterns for requirements specification and analysis of secure systems. Anais do WER14 - Workshop em Engenharia de Requisitos, Pucón, Chile, April 23, 24 and 25, 2014; Giachetti, G.; Lucena, M., Eds., 2014.

36. Busnel, P.; Khoury, P.E.; Giroux, S.; Li, K. Achieving Socio-technical Confidentiality Using Security Pattern in Smart Homes. The Second International Conference on Future Generation Communication and Networking, FGCN 2008, Volume 2, Workshops, Hainan Island, China, December 13-15, 2008. IEEE Computer Society, 2008, pp. 447–452.

37. Heyman, T.; Yskout, K.; Scandariato, R.; Joosen, W. An Analysis of the Security Patterns Landscape. Third International Workshop on Software Engineering for Secure Systems, SESS 2007, Minneapolis, MN, USA, May 20-26, 2007. IEEE Computer Society, 2007, p. 3.

38. Bouaziz, R.; Kallel, S.; Coulette, B. An Approach for Security Patterns Application in Component Based Models. Computational Science and Its Applications - ICCSA 2014 - 14th International Conference, Guimarães, Portugal, June 30 - July 3, 2014, Proceedings, Part V; Murgante, B.; Misra, S.; Rocha, A.M.A.C.; Torre, C.M.; Rocha, J.G.; Falcão, M.I.; Taniar, D.; Apduhan, B.O.; Gervasi, O., Eds. Springer, 2014, Vol. 8583, *Lecture Notes in Computer Science*, pp. 283–296.

39. Fernández, E.B.; Washizaki, H.; Yoshioka, N.; VanHilst, M. An Approach to Model-based Development of Secure and Reliable Systems. Sixth International Conference on Availability, Reliability and Security, ARES 2011, Vienna, Austria, August 22-26, 2011. IEEE Computer Society, 2011, pp. 260–265.

40. Serrano, D.; na, A.M.; Soria-Rodríguez, P.; nuela, A.P.; Sotirious, A.D. An Architecture for secure ambient intelligence environments. Juan M. Corbacho; Dante I. Tapia y José Bravo (Eds.). 3rd. Symposium of Ubiquitous Computing and Ambient Intelligence 2008. Advances in Soft Computing; 51; Springer-Verlag: Berlin-Heidelberg, 2009; pp. 21–29.

41. Bunke, M.; Sohr, K. An Architecture-Centric Approach to Detecting Security Patterns in Software. Engineering Secure Software and Systems - Third International Symposium, ESSoS 2011, Madrid, Spain, February 9-10, 2011. Proceedings; Erlingsson, Ú.; Wieringa, R.J.; Zannone, N., Eds. Springer, 2011, Vol. 6542, *Lecture Notes in Computer Science*, pp. 156–166.

42. Mouheb, D.; Talhi, C.; Mourad, A.; Lima, V.; Debbabi, M.; Wang, L.; Pourzandi, M. An Aspect-Oriented Approach for Software Security Hardening: from Design to Implementation. New Trends in Software Methodologies, Tools and Techniques - Proceedings of the Eighth SoMeT 2009, September 23-25, 2009, Prague, Czech Republic; Fujita, H.; Marík, V., Eds. IOS Press, 2009, Vol. 199, *Frontiers in Artificial Intelligence and Applications*, pp. 203–222.

43. Mourad, A.; Laverdière, M.; Debbabi, M. An aspect-oriented approach for the systematic security hardening of code. *Comput. Secur.* **2008**, *27*, 101–114.

44. Alebrahim, A.; Tun, T.T.; Yu, Y.; Heisel, M.; Nuseibeh, B. An Aspect-Oriented Approach to Relating Security Requirements and Access Control. Proceedings of the CAiSE'12 Forum at the 24th International Conference on Advanced Information Systems Engineering (CAiSE), Gdansk, Poland, June 28, 2012; Kirikova, M.; Stirna, J., Eds. CEUR-WS.org, 2012, Vol. 855, *CEUR Workshop Proceedings*, pp. 15–22.

45. He, K.; Feng, Z.; Li, X. An Attack Scenario Based Approach for Software Security Testing at Design Stage. 2008 International Symposium on Computer Science and Computational Technology, ISCSCT 2008, 20-22 December 2008, Shanghai, China, 2 Volumes. IEEE Computer Society, 2008, pp. 782–787.

46. Bouaziz, R.; Kallel, S.; Coulette, B. An Engineering Process for Security Patterns Application in Component Based Models. 2013 Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, Hammamet, Tunisia, June 17-20, 2013; Reddy, S.; Jmaiel, M., Eds. IEEE Computer Society, 2013, pp. 231–236.

47. Alaküla, M.; Matulevicius, R. An Experience Report of Improving Business Process Compliance Using Security Risk-Oriented Patterns. The Practice of Enterprise Modeling - 8th IFIP WG 8.1. Working Conference, PoEM 2015, Valencia, Spain, November 10-12, 2015, Proceedings; Ralyté, J.; España, S.; Pastor, O., Eds. Springer, 2015, Vol. 235, *Lecture Notes in Business Information Processing*, pp. 271–285.

48. Noël, R.; Pedraza-Garcia, G.; Astudillo, H.; Fernández, E.B. An exploratory comparison of security patterns and tactics to harden systems. Proceedings of the XVII Iberoamerican Conference on Software Engineering, CIbSE 2014, Pucon, Chile, April 23-25, 2014; Castro, J.; Ayala, C.P.; Giachetti, G.; Lucena, M.; Cares, C.; Franch, X.; Barcellos, M.P.; Lencastre, M.; Marín, B.; Gacitua, R., Eds. Curran Associates, 2014, pp. 378–391.

49. Khoury, P.E.; Mokhtari, A.; Coquery, E.; Hacid, M. An Ontological Interface for Software Developers to Select Security Patterns. 19th International Workshop on Database and Expert Systems Applications (DEXA 2008), 1-5 September 2008, Turin, Italy. IEEE Computer Society, 2008, pp. 297–301.

50. Guan, H.; Yang, H.; Wang, J. An ontology-based approach to security pattern selection. *Int. J. Autom. Comput.* **2016**, *13*, 168–182.

51. Hwang, G.; Chang, T. An operational model and language support for securing XML documents. *Comput. Secur.* **2004**, *23*, 498–529.

52. Ortiz, R.; Garzás, J.; Fernández-Medina, E. Analysis of Application of Security Patterns to Build Secure Systems. Advanced Information Systems Engineering Workshops - CAiSE 2011 International Workshops, London, UK, June 20-24, 2011. Proceedings; Salinesi, C.; Pastor, O., Eds. Springer, 2011, Vol. 83, *Lecture Notes in Business Information Processing*, pp. 652–659.

53. Li, T.; Horkoff, J.; Mylopoulos, J. Analyzing and Enforcing Security Mechanisms on Requirements Specifications. Requirements Engineering: Foundation for Software Quality - 21st International Working Conference, REFSQ 2015, Essen, Germany, March 23-26, 2015. Proceedings; Fricker, S.A.; Schneider, K., Eds. Springer, 2015, Vol. 9013, *Lecture Notes in Computer Science*, pp. 115–131.

54. Ortiz, R.; Moral-García, S.; Moral-Rubio, S.; Vela, B.; Garzás, J.; Fernández-Medina, E. Applicability of Security Patterns. On the Move to Meaningful Internet Systems: OTM 2010 - Confederated International Conferences: CoopIS, IS, DOA and ODBASE, Hersonissos, Crete, Greece, October 25-29, 2010, Proceedings, Part I; Meersman, R.; Dillon, T.S.; Herrero, P., Eds. Springer, 2010, Vol. 6426, *Lecture Notes in Computer Science*, pp. 672–684.

55. Changadwech, C.; Prompoon, N. Applying information retrieval technique for security requirements verification based on security patterns. Lecture Notes in Engineering and Computer Science, 2016, Vol. 1, pp. 467–472.

56. Bouaziz, R.; Coulette, B. Applying Security Patterns for Component Based Applications Using UML Profile. 15th IEEE International Conference on Computational Science and Engineering, CSE 2012, Paphos, Cyprus, December 5-7, 2012. IEEE Computer Society, 2012, pp. 186–193.

57. Halkidis, S.T.; Tsantalis, N.; Chatzigeorgiou, A.; Stephanides, G. Architectural Risk Analysis of Software Systems Based on Security Patterns. *IEEE Trans. Dependable Secur. Comput.* **2008**, *5*, 129–142.

58. Uzunov, A.V.; Fernández, E.B.; Falkner, K.E. ASE: A comprehensive pattern-driven security methodology for distributed systems. *Comput. Stand. Interfaces* **2015**, *41*, 112–137.

59. Steinegger, R.; Schäfer, J.; Vogler, M.; Abeck, S. Attack surface reduction for web services based on authorization patterns. SECURWARE 2014 - 8th International Conference on Emerging Security Information, Systems and Technologies, 2014, pp. 194–201.

60. Warschofsky, R.; Menzel, M.; Meinel, C. Automated Security Service Orchestration for the Identity Management in Web Service Based Systems. IEEE International Conference on Web Services, ICWS 2011, Washington, DC, USA, July 4-9, 2011. IEEE Computer Society, 2011, pp. 596–603.

61. Dong, J.; Peng, T.; Zhao, Y. Automated verification of security pattern compositions. *Inf. Softw. Technol.* **2010**, *52*, 274–295.

62. Gunawan, L.A.; Kraemer, F.A.; Herrmann, P. Behavioral Singletons to Consistently Handle Global States of Security Patterns. Distributed Applications and Interoperable Systems - 12th IFIP WG 6.1 International Conference, DAIS 2012, Stockholm, Sweden, June 13-16, 2012. Proceedings; Göschka, K.M.; Haridi, S., Eds. Springer, 2012, Vol. 7272, *Lecture Notes in Computer Science*, pp. 73–86.

63. Tatsubori, M.; Imamura, T.; Nakamura, Y. Best-Practice Patterns and Tool Support for Configuring Secure Web Services Messaging. Proceedings of the IEEE International Conference on Web Services (ICWS'04), June 6-9, 2004, San Diego, California, USA. IEEE Computer Society, 2004, pp. 244–251.

64. Fernández, E.B.; Monge, R.; Hashizume, K. Building a security reference architecture for cloud systems. *Requir. Eng.* **2016**, *21*, 225–249.

65. Rimba, P. Building high assurance secure applications using security patterns for capability-based platforms. 35th International Conference on Software Engineering, ICSE '13, San Francisco, CA, USA, May 18-26, 2013; Notkin, D.; Cheng, B.H.C.; Pohl, K., Eds. IEEE Computer Society, 2013, pp. 1401–1404.

66. Fernández, E.B.; Mujica, S. Building Secure Systems: From Threats to Security Patterns. SCCC 2010, Proceedings of the XXIX International Conference of the Chilean Computer Science Society, Antofagasta, Chile, 15-19 November 2010; Ochoa, S.F.; Meza, F.; Mery, D.; Cubillos, C., Eds. IEEE Computer Society, 2010, pp. 66–70.

67. Bayley, I. Challenges for a Formal Framework for Patterns. In *Cyberpatterns, Unifying Design Patterns with Security and Attack Patterns*; Blackwell, C.; Zhu, H., Eds.; Springer, 2014; pp. 47–55.

68. Slavin, R.; Shen, H.; Niu, J. Characterizations and boundaries of security requirements patterns. Second IEEE International Workshop on Requirements Patterns, RePa 2012, Chicago, IL, USA, September 24, 2012. IEEE Computer Society, 2012, pp. 48–53.

69. Fernández, E.B.; Washizaki, H.; Yoshioka, N.; Kubo, A.; Fukazawa, Y. Classifying Security Patterns. Progress in WWW Research and Development, 10th Asia-Pacific Web Conference, APWeb 2008, Shenyang, China, April 26-28, 2008. Proceedings; Zhang, Y.; Yu, G.; Bertino, E.; Xu, G., Eds. Springer, 2008, Vol. 4976, *Lecture Notes in Computer Science*, pp. 342–347.

70. Rimba, P.; Zhu, L.; Bass, L.; Kuz, I.; Reeves, S. Composing Patterns to Construct Secure Systems. 11th European Dependable Computing Conference, EDCC 2015, Paris, France, September 7-11, 2015. IEEE Computer Society, 2015, pp. 213–224.

71. Alzahrani, A.A.H.; Eden, A.H.; Yafi, M.Z. Conformance checking of single access point pattern in JAAS using codecharts. 2015 World Congress on Information Technology and Computer Applications, WCITCA 2015, 2015.

72. Schmidt, H.; Jürjens, J. Connecting Security Requirements Analysis and Secure Design Using Patterns and UMLsec. Advanced Information Systems Engineering - 23rd International Conference, CAiSE 2011, London, UK, June 20-24, 2011. Proceedings; Mouratidis, H.; Rolland, C., Eds. Springer, 2011, Vol. 6741, *Lecture Notes in Computer Science*, pp. 367–382.

73. Ouedraogo, W.F.; Biennier, F.; Silva, C.F.D.; Ghodous, P. Context-aware Security@run.time Deployment. CLOSER 2015 - Proceedings of the 5th International Conference on Cloud Computing and Services Science,

Lisbon, Portugal, 20-22 May, 2015; Helfert, M.; Ferguson, D.; Muñoz, V.M., Eds. SciTePress, 2015, pp. 276–283.

74. Bouaziz, R.; Krichen, F.; Coulette, B. C-SCRIP: Collaborative Security Pattern Integration Process. *Int. J. Inf. Technol. Web Eng.* **2015**, *10*, 31–46.

75. Li, T.; Horkoff, J. Dealing with Security Requirements for Socio-Technical Systems: A Holistic Approach. Advanced Information Systems Engineering - 26th International Conference, CAiSE 2014, Thessaloniki, Greece, June 16-20, 2014. Proceedings; Jarke, M.; Mylopoulos, J.; Quix, C.; Rolland, C.; Manolopoulos, Y.; Mouratidis, H.; Horkoff, J., Eds. Springer, 2014, Vol. 8484, *Lecture Notes in Computer Science*, pp. 285–300.

76. Tian, K.; Cooper, K.M.L.; Feng, K.; Tang, Y. Defining Re-usable Composite Aspect Patterns: An FDAF Based Approach. On the Move to Meaningful Internet Systems: OTM 2008 Workshops, OTM Confederated International Workshops and Posters, ADI, AWeSoMe, COMBEK, EI2N, IWSSA, MONET, OnToContent + QSI, ORM, PerSys, RDDS, SEMELS, and SWWS 2008, Monterrey, Mexico, November 9-14, 2008. Proceedings; Meersman, R.; Tari, Z.; Herrero, P., Eds. Springer, 2008, Vol. 5333, *Lecture Notes in Computer Science*, pp. 384–395.

77. Rosado, D.G.; Gutiérrez, C.; Fernández-Medina, E.; Piattini, M. Defining Security Architectural Patterns Based on Viewpoints. Computational Science and Its Applications - ICCSA 2007, International Conference, Kuala Lumpur, Malaysia, August 26-29, 2007. Proceedings. Part III; Gervasi, O.; Gavrilova, M.L., Eds. Springer, 2007, Vol. 4707, *Lecture Notes in Computer Science*, pp. 262–272.

78. Rosado, D.G.; Gutiérrez, C.; Fernández-Medina, E.; Piattini, M. Defining Viewpoints for Security Architectural Patterns. SECRYPT 2006, Proceedings of the International Conference on Security and Cryptography, Setúbal, Portugal, August 7-10, 2006, SECRYPT is part of ICETE - The International Joint Conference on e-Business and Telecommunications; Malek, M.; Fernández-Medina, E.; Hernando, J., Eds. INSTICC Press, 2006, pp. 419–424.

79. Fernández, E.B.; Larrondo-Petrie, M.M. Designing Secure SCADA Systems Using Security Patterns. 43rd Hawaii International International Conference on Systems Science (HICSS-43 2010), Proceedings, 5-8 January 2010, Koloa, Kauai, HI, USA. IEEE Computer Society, 2010, pp. 1–8.

80. Gymnopoulos, L.; Karyda, M.; Balopoulos, T.; Dritsas, S.; Kokolakis, S.; Lambrinoudakis, C.; Gritzalis, S. Developing a security patterns repository for secure applications design. 5th European Conference on Information Warfare and Security 2006, ECIW 2006, 2006, pp. 51–60.

81. Serrano, D.; Ruíz, J.F.; Muñoz, A.; Maña, A.; Armenteros, A.; Crespo, B.G.. Development of applications based on security patterns. Proceedings - 2009 2nd International Conference on Dependability, DEPEND 2009, 2009, pp. 111–116.

82. Yskout, K.; Scandariato, R.; Joosen, W. Do Security Patterns Really Help Designers? 37th IEEE/ACM International Conference on Software Engineering, ICSE 2015, Florence, Italy, May 16-24, 2015, Volume 1; Bertolino, A.; Canfora, G.; Elbaum, S.G., Eds. IEEE Computer Society, 2015, pp. 292–302.

83. Yskout, K.; Scandariato, R.; Joosen, W. Does organizing security patterns focus architectural choices? 34th International Conference on Software Engineering, ICSE 2012, June 2-9, 2012, Zurich, Switzerland; Glinz, M.; Murphy, G.C.; Pezzè, M., Eds. IEEE Computer Society, 2012, pp. 617–627.

84. Gandhi, R.A.; Rahmani, M. Early security patterns: A collection of constraints to describe regulatory security requirements. Second IEEE International Workshop on Requirements Patterns, RePa 2012, Chicago, IL, USA, September 24, 2012. IEEE Computer Society, 2012, pp. 17–22.

85. Okubo, T.; Kaiya, H.; Yoshioka, N. Effective Security Impact Analysis with Patterns for Software Enhancement. Sixth International Conference on Availability, Reliability and Security, ARES 2011, Vienna, Austria, August 22-26, 2011. IEEE Computer Society, 2011, pp. 527–534.

86. Mathew, G. Elements of application security in the cloud computing environment. 2012 IEEE Conference on Open Systems, ICOS 2012, 2012.

87. Braz, F.A.; Fernández, E.B.; VanHilst, M. Eliciting Security Requirements through Misuse Activities. 19th International Workshop on Database and Expert Systems Applications (DEXA 2008), 1-5 September 2008, Turin, Italy. IEEE Computer Society, 2008, pp. 328–333.

88. Solinas, M.; Fernández, E.B.; Antonelli, L. Embedding Security Patterns into a Domain Model. Database and Expert Systems Applications, DEXA, International Workshops, Linz, Austria, August 31-September 4, 2009, Proceedings; Tjoa, A.M.; Wagner, R.R., Eds. IEEE Computer Society, 2009, pp. 176–180.

89. Yu, Y.; Kaiya, H.; Washizaki, H.; Xiong, Y.; Hu, Z.; Yoshioka, N. Enforcing a security pattern in stakeholder goal models. Proceedings of the 4th ACM Workshop on Quality of Protection, QoP 2008, Alexandria, VA, USA, October 27, 2008; Ozment, A.; Stølen, K., Eds. ACM, 2008, pp. 9–14.

90. Khoury, P.; Busnel, P.; Giroux, S. Enforcing security in smart homes using security patterns. *International Journal of Smart Home* **2009**, *3*, 57–70.

91. Uzunov, A.V.; Fernández, E.B.; Falkner, K. Engineering Security into Distributed Systems: A Survey of Methodologies. *J. Univers. Comput. Sci.* **2012**, *18*, 2920–3006.

92. Katt, B.; Gander, M.; Breu, R.; Felderer, M. Enhancing Model Driven Security through Pattern Refinement Techniques. Formal Methods for Components and Objects, 10th International Symposium, FMCO 2011, Turin, Italy, October 3-5, 2011, Revised Selected Papers; Beckert, B.; Damiani, F.; de Boer, F.S.; Bonsangue, M.M., Eds. Springer, 2011, Vol. 7542, *Lecture Notes in Computer Science*, pp. 169–183.

93. Supaporn, K.; Prompoon, N.; Rojkangsadan, T. Enterprise Assets Security Requirements Construction from ESRMG Grammar based on Security Patterns. 14th Asia-Pacific Software Engineering Conference (APSEC 2007), 5-7 December 2007, Nagoya, Japan. IEEE Computer Society, 2007, pp. 112–119.

94. Moral-García, S.; Moral-Rubio, S.; Fernández, E.B.; Fernández-Medina, E. Enterprise security pattern: A model-driven architecture instance. *Comput. Stand. Interfaces* **2014**, *36*, 748–758.

95. Moral-García, S.; Moral-Rubio, S.; Rosado, D.G.; Fernández, E.B.; Fernández-Medina, E. Enterprise security pattern: a new type of security pattern. *Secur. Commun. Networks* **2014**, *7*, 1670–1690.

96. Faily, S.; Parkin, S.; Lyle, J. Evaluating the Implications of Attack and Security Patterns with Premortems. In *Cyberpatterns, Unifying Design Patterns with Security and Attack Patterns*; Blackwell, C.; Zhu, H., Eds.; Springer, 2014; pp. 199–209.

97. Abramov, J.; Sturm, A.; Shoval, P. Evaluation of the Pattern-based method for Secure Development (PbSD): A controlled experiment. *Inf. Softw. Technol.* **2012**, *54*, 1029–1043.

98. Dalai, A.K.; Jena, S.K. Evaluation of web application security risks and secure design patterns. Proceedings of the 2011 International Conference on Communication, Computing & Security, ICCCS 2011, Odisha, India, February 12-14, 2011; Jena, S.K.; Kumar, R.; Turuk, A.K.; Dash, M., Eds. ACM, 2011, pp. 565–568.

99. Hafiz, M.; Johnson, R.E. Evolution of the MTA architecture: the impact of security. *Softw. Pract. Exp.* **2008**, *38*, 1569–1599.

100. van Veenstra, A.F.; Ramilli, M. Exploring Information Security Issues in Public Sector Inter-organizational Collaboration. Electronic Government - 10th IFIP WG 8.5 International Conference, EGOV 2011, Delft, The Netherlands, August 28 - September 2, 2011. Proceedings; Janssen, M.; Scholl, H.J.; Wimmer, M.A.; Tan, Y., Eds. Springer, 2011, Vol. 6846, *Lecture Notes in Computer Science*, pp. 355–366.

101. Savic, D.; Simic, D.; Vlajic, S. Extended Software Architecture Based on Security Patterns. *Informatica* **2010**, *21*, 229–246.

102. Robinson, P. Extensible Security Patterns. 18th International Workshop on Database and Expert Systems Applications (DEXA 2007), 3-7 September 2007, Regensburg, Germany. IEEE Computer Society, 2007, pp. 729–733.

103. Muñoz, A.; Maña, A. Facilitating the Use of TPM Technologies Using the Serenity Framework. Autonomic and Trusted Computing - 8th International Conference, ATC 2011, Banff, Canada, September 2-4, 2011. Proceedings; Calero, J.M.A.; Yang, L.T.; Mármol, F.G.; García-Villalba, L.J.; Li, X.A.; Wang, Y., Eds. Springer, 2011, Vol. 6906, *Lecture Notes in Computer Science*, pp. 164–174.

104. Near, J.P.; Jackson, D. Finding security bugs in web applications using a catalog of access control patterns. Proceedings of the 38th International Conference on Software Engineering, ICSE 2016, Austin, TX, USA, May 14-22, 2016; Dillon, L.K.; Visser, W.; Williams, L.A., Eds. ACM, 2016, pp. 947–958.

105. Ruamjinda, P.; Prompoon, N. Framwork for information security standards storage and retrieval using security patterns. Proceedings of the IEEE International Conference on Software Engineering and Service Sciences, ICSESS, 2013, pp. 296–300.

106. Horvath, V.; Dörges, T. From security patterns to implementation using petri nets. Proceedings of the Fourth International Workshop on Software Engineering for Secure Systems, SESS 2008, Leipzig, Germany, May 17-18, 2008; Win, B.D.; Lee, S.; Monga, M., Eds. ACM, 2008, pp. 17–24.

107. Hafiz, M.; Adamczyk, P.; Johnson, R.E. Growing a pattern language (for security). ACM Symposium on New Ideas in Programming and Reflections on Software, Onward! 2012, part of SPLASH '12, Tucson, AZ, USA, October 21-26, 2012; Leavens, G.T.; Edwards, J., Eds. ACM, 2012, pp. 139–158.

108. Dikanski, A.; Steinegger, R.; Abeck, S. Identification and implementation of authentication and authorization patterns in the spring security framework. SECURWARE 2012 - 6th International Conference on Emerging Security Information, Systems and Technologies, 2012, pp. 14–20.

109. Patu, V.; Yamamoto, S. Identifying and Implementing Security Patterns for a Dependable Security Case - From Security Patterns to D-Case. 16th IEEE International Conference on Computational Science and Engineering, CSE 2013, December 3-5, 2013, Sydney, Australia. IEEE Computer Society, 2013, pp. 138–142.

110. Yoshizawa, M.; Washizaki, H.; Fukazawa, Y.; Okubo, T.; Kaiya, H.; Yoshioka, N. Implementation Support of Security Design Patterns Using Test Templates. *Inf.* **2016**, *7*, 34.

111. Edge, C.; Mitropoulos, F. Improving security design patterns with aspect-oriented strategies. Proceedings of the 50th Annual Southeast Regional Conference, 2012, Tuscaloosa, AL, USA, March 29-31, 2012; Smith, R.K.; Vrbsky, S.V., Eds. ACM, 2012, pp. 24–29.

112. Washizaki, H.; Fernández, E.B.; Maruyama, K.; Kubo, A.; Yoshioka, N. Improving the Classification of Security Patterns. Database and Expert Systems Applications, DEXA, International Workshops, Linz, Austria, August 31-September 4, 2009, Proceedings; Tjoa, A.M.; Wagner, R.R., Eds. IEEE Computer Society, 2009, pp. 165–170.

113. Netter, M.; Pernul, G. Integrating Security Patterns into the Electronic Invoicing Process. Database and Expert Systems Applications, DEXA, International Workshops, Linz, Austria, August 31-September 4, 2009, Proceedings; Tjoa, A.M.; Wagner, R.R., Eds. IEEE Computer Society, 2009, pp. 150–154.

114. Li, T.; Horkoff, J.; Mylopoulos, J. Integrating Security Patterns with Security Requirements Analysis Using Contextual Goal Models. The Practice of Enterprise Modeling - 7th IFIP WG 8.1 Working Conference, PoEM 2014, Manchester, UK, November 12-13, 2014. Proceedings; Frank, U.; Loucopoulos, P.; Pastor, O.; Petrounias, I., Eds. Springer, 2014, Vol. 197, *Lecture Notes in Business Information Processing*, pp. 208–223.

115. Filho, A.E.S.; Smith, P.; Mauthe, A.; Hutchison, D. Management Patterns for Network Resilience: Design and Verification of Policy Configurations. In *Cyberpatterns, Unifying Design Patterns with Security and Attack Patterns*; Blackwell, C.; Zhu, H., Eds.; Springer, 2014; pp. 85–95.

116. Fernández, E.B.; Yoshioka, N.; Washizaki, H.; VanHilst, M. Measuring the Level of Security Introduced by Security Patterns. ARES 2010, Fifth International Conference on Availability, Reliability and Security, 15-18 February 2010, Krakow, Poland. IEEE Computer Society, 2010, pp. 565–568.

117. Dong, J.; Peng, T.; Zhao, Y. Model Checking Security Pattern Compositions. Seventh International Conference on Quality Software (QSIC 2007), 11-12 October 2007, Portland, Oregon, USA. IEEE Computer Society, 2007, pp. 80–89.

118. Shiroma, Y.; Washizaki, H.; Fukazawa, Y.; Kubo, A.; Yoshioka, N. Model-Driven Security Patterns Application Based on Dependences among Patterns. ARES 2010, Fifth International Conference on Availability, Reliability and Security, 15-18 February 2010, Krakow, Poland. IEEE Computer Society, 2010, pp. 555–559.

119. Nguyen, P.H.; Klein, J.; Traon, Y.L. Model-Driven Security with A System of Aspect-Oriented Security Design Patterns. Proceedings of the 2nd Workshop on View-Based, Aspect-Oriented and Orthographic Software Modelling, VAO@STAF 2014, York, United Kingdom, July 22, 2014; Atkinson, C.; Burger, E.; Goldschmidt, T.; Reussner, R.H., Eds. ACM, 2014, pp. 51–54.

120. Li, T.; Mylopoulos, J. Modeling and Applying Security Patterns Using Contextual Goal Models. Proceedings of the Seventh International i* Workshop co-located with the 26th International Conference on Advanced Information Systems Engineering (CAiSE 2014), Thessaloniki, Greece, June 16-17, 2014; Dalpiaz, F.; Horkoff, J., Eds. CEUR-WS.org, 2014, Vol. 1157, *CEUR Workshop Proceedings*.

121. Dai, L.; Cooper, K.M.L. Modeling and performance analysis for security aspects. *Sci. Comput. Program.* **2006**, *61*, 58–71.

122. Asnar, Y.; Paja, E.; Mylopoulos, J. Modeling Design Patterns with Description Logics: A Case Study. Advanced Information Systems Engineering - 23rd International Conference, CAiSE 2011, London, UK, June 20-24, 2011. Proceedings; Mouratidis, H.; Rolland, C., Eds. Springer, 2011, Vol. 6741, *Lecture Notes in Computer Science*, pp. 169–183.

123. Fernández, E.B.; Yoshioka, N.; Washizaki, H. Modeling Misuse Patterns. Proceedings of the The Forth International Conference on Availability, Reliability and Security, ARES 2009, March 16-19, 2009, Fukuoka, Japan. IEEE Computer Society, 2009, pp. 566–571.

124. Mouratidis, H.; Weiss, M.; Giorgini, P. Modeling Secure Systems Using an Agent-oriented Approach and Security Patterns. *Int. J. Softw. Eng. Knowl. Eng.* **2006**, *16*, 471.

125. Weiss, M., Modelling security patterns using NFR analysis; Integrating Security and Software Engineering: Advances and Future Visions, 2006; pp. 127–141.

126. Halkidis, S.T.; Chatzigeorgiou, A.; Stephanides, G. Moving from Requirements to Design Confronting Security Issues: A Case Study. On the Move to Meaningful Internet Systems: OTM 2009, Confederated International Conferences, CoopIS, DOA, IS, and ODBASE 2009, Vilamoura, Portugal, November 1-6, 2009, Proceedings, Part II; Meersman, R.; Dillon, T.S.; Herrero, P., Eds. Springer, 2009, Vol. 5871, *Lecture Notes in Computer Science*, pp. 798–814.

127. Mourad, A.; Otrok, H.; Baajour, L. New Approach Targeting Security Patterns Development and Deployment. *Inf. Secur. J. A Glob. Perspect.* **2011**, *20*, 231–244.

128. Fernández, E.B; Wu, J.; Larrondo-Petrie, M.M.; Shao, Y. On building secure SCADA systems using security patterns. Fifth Cyber Security and Information Intelligence Research Workshop, CSIIRW '09, Knoxville, TN, USA, April 13-15, 2009; Sheldon, F.T.; Peterson, G.; Krings, A.W.; Abercrombie, R.K.; Mili, A., Eds. ACM, 2009, p. 17.

129. Bunke, M. On the description of software security patterns. Proceedings of the 19th European Conference on Pattern Languages of Programs, EuroPLoP 2014, Irsee, Germany, July 9-13, 2014; Eloranta, V.; van Heesch, U., Eds. ACM, 2014, pp. 34:1–34:10.

130. Hafiz, M.; Adamczyk, P.; Johnson, R.E. Organizing Security Patterns. *IEEE Softw.* **2007**, *24*, 52–60.

131. Dove, R. Pattern qualifications and examples of next-generation agile system-security strategies. Proceedings - International Carnahan Conference on Security Technology, 2010, pp. 71–80.

132. Rrenja, A.; Matulevicius, R. Pattern-Based Security Requirements Derivation from Secure Tropos Models. The Practice of Enterprise Modeling - 8th IFIP WG 8.1. Working Conference, PoEM 2015, Valencia, Spain, November 10-12, 2015, Proceedings; Ralyté, J.; España, S.; Pastor, O., Eds. Springer, 2015, Vol. 235, *Lecture Notes in Business Information Processing*, pp. 59–74.

133. Fernández, E.B.; Pernul, G.; Larrondo-Petrie, M.M. Patterns and Pattern Diagrams for Access Control. Trust, Privacy and Security in Digital Business, 5th International Conference, TrustBus 2008, Turin, Italy, September 4-5, 2008, Proceedings; Furnell, S.; Katsikas, S.K.; Lioy, A., Eds. Springer, 2008, Vol. 5185, *Lecture Notes in Computer Science*, pp. 38–47.

134. Fernández, E.B.; Yoshioka, N.; Washizaki, H. Patterns for security and privacy in cloud ecosystems. 2nd IEEE Workshop on Evolving Security and Privacy Requirements Engineering, ESPRE 2015, Ottawa, ON, Canada, August 25, 2015. IEEE Computer Society, 2015, pp. 13–18.

135. Hafiz, M.; Adamczyk, P.; Johnson, R.E. Patterns Transform Architectures. 9th Working IEEE/IFIP Conference on Software Architecture, WICSA 2011, Boulder, Colorado, USA, June 20-24, 2011. IEEE Computer Society, 2011, pp. 242–251.

136. Thomsen, D. Practical policy patterns. First ACM Conference on Data and Application Security and Privacy, CODASPY 2011, San Antonio, TX, USA, February 21-23, 2011, Proceedings; Sandhu, R.S.; Bertino, E., Eds. ACM, 2011, pp. 225–230. doi:10.1145/1943513.1943543.

137. Hazeyama, A.; Saito, M. Preliminary Evaluation of a Software Security Learning Environment. *Int. J. Softw. Innov.* **2014**, *2*, 26–39.

138. Fernández, E.B. Preventing and unifying threats in cyberphysical systems. 17th IEEE International Symposium on High Assurance Systems Engineering, HASE 2016, Orlando, FL, USA, January 7-9, 2016; Babiceanu, R.F.; Waeselynck, H.; Paul, R.A.; Cukic, B.; Xu, J., Eds. IEEE Computer Society, 2016, pp. 292–293.

139. Romanosky, S.; Acquisti, A.; Hong, J.; Cranor, L.F.; Friedman, B. Privacy patterns for online interactions. PLoP 2006 - PLoP Pattern Languages of Programs 2006 Conference Proceedings, 2006.

140. Alebrahim, A.; Heisel, M. Problem-oriented security patterns for requirements engineering. Proceedings of the 19th European Conference on Pattern Languages of Programs, EuroPLoP 2014, Irsee, Germany, July 9-13, 2014; Eloranta, V.; van Heesch, U., Eds. ACM, 2014, pp. 9:1–9:17.

141. Halkidis, S.T.; Chatzigeorgiou, A.; Stephanides, G. Quantitative Evaluation of Systems with Security Patterns Using a Fuzzy Approach. On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, OTM Confederated International Workshops and Posters, AWeSOMe, CAMS, COMINF, IS, KSinBIT, MIOS-CIAO, MONET, OnToContent, ORM, PerSys, OTM Academy Doctoral Consortium,

RDDS, SWWS, and SeBGIS 2006, Montpellier, France, October 29 - November 3, 2006. Proceedings, Part I; Meersman, R.; Tari, Z.; Herrero, P., Eds. Springer, 2006, Vol. 4277, *Lecture Notes in Computer Science*, pp. 554–564.

142. Hafner, M.; Breu, R. Realizing Model Driven Security for Inter-organizational Workflows with WS-CDL and UML 2.0. Model Driven Engineering Languages and Systems, 8th International Conference, MoDELS 2005, Montego Bay, Jamaica, October 2-7, 2005, Proceedings; Briand, L.C.; Williams, C., Eds. Springer, 2005, Vol. 3713, *Lecture Notes in Computer Science*, pp. 39–53.

143. Netter, M.; Fernández, E.B.; Pernul, G. Refining the Pattern-Based Reference Model for Electronic Invoices by Incorporating Threats. ARES 2010, Fifth International Conference on Availability, Reliability and Security, 15-18 February 2010, Krakow, Poland. IEEE Computer Society, 2010, pp. 560–564.

144. Heyman, T.; Scandariato, R.; Joosen, W. Reusable Formal Models for Secure Software Architectures. 2012 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture, WICSA/ECSA 2012, Helsinki, Finland, August 20-24, 2012. IEEE, 2012, pp. 41–50.

145. Fernández, E.B.; Astudillo, H.; Pedraza-Garcia, G. Revisiting Architectural Tactics for Security. Software Architecture - 9th European Conference, ECSA 2015, Dubrovnik/Cavtat, Croatia, September 7-11, 2015, Proceedings; Weyns, D.; Mirandola, R.; Crnkovic, I., Eds. Springer, 2015, Vol. 9278, *Lecture Notes in Computer Science*, pp. 55–69.

146. Bouaziz, R.; Kammoun, S. SCRIStUDIO: A security pattern integration tool. 2016 International Conference on Information Technology for Organizations Development, IT4OD 2016, 2016.

147. Bergmann, G.; Massacci, F.; Paci, F.; Tun, T.T.; Varró, D.; Yu, Y. SeCMER: A Tool to Gain Control of Security Requirements Evolution. Towards a Service-Based Internet - 4th European Conference, ServiceWave 2011, Poznan, Poland, October 26-28, 2011. Proceedings; Abramowicz, W.; Llorente, I.M.; Surridge, M.; Zisman, A.; Vayssière, J., Eds. Springer, 2011, Vol. 6994, *Lecture Notes in Computer Science*, pp. 321–322.

148. Hafner, M.; Breu, R.; Agreiter, B.; Nowak, A. Sectet: an extensible framework for the realization of secure inter-organizational workflows. *Internet Res.* **2006**, *16*, 491–506.

149. Bouaziz, R.; Coulette, B. Secure Component Based Applications through Security Patterns. 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing, GreenCom/iThings/CPSCom 2012, Besancon, France, November 20-23, 2012. IEEE Computer Society, 2012, pp. 749–754.

150. Ruiz, J.F.; Arjona, M.; Mana, A.; Carstens, N. Secure Engineering and Modelling of a Metering Devices System. 2013 International Conference on Availability, Reliability and Security, ARES 2013, Regensburg, Germany, September 2-6, 2013. IEEE Computer Society, 2013, pp. 418–427.

151. Fernández, E.B.; Yuan, X. Securing analysis patterns. Proceedings of the 45th Annual Southeast Regional Conference, 2007, Winston-Salem, North Carolina, USA, March 23-24, 2007; John, D.; Kerr, S.N., Eds. ACM, 2007, pp. 288–293.

152. Uzunov, A.V.; Fernández, E.B.; Falkner, K. Securing distributed systems using patterns: A survey. *Comput. Secur.* **2012**, *31*, 681–703.

153. Sohn, J.; Ryoo, J. Securing Web Applications with Better "Patches": An Architectural Approach for Systematic Input Validation with Security Patterns. 10th International Conference on Availability, Reliability and Security, ARES 2015, Toulouse, France, August 24-27, 2015. IEEE Computer Society, 2015, pp. 486–492.

154. Armenteros, Á.; Muñoz, A.; Maña, A.; Serrano, D. Security and Dependability in Ambient Intelligence Scenarios - The Communication Prototype. ICEIS 2009 - Proceedings of the 11th International Conference on Enterprise Information Systems, Volume ISAS, Milan, Italy, May 6-10, 2009; Cordeiro, J.; Filipe, J., Eds., 2009, pp. 49–56.

155. Laverdière, M.; Mourad, A.; Hanna, A.; Debbabi, M. Security Design Patterns: Survey and Evaluation. Proceedings of the Canadian Conference on Electrical and Computer Engineering, CCECE 2006, May 7-10, 2006, Ottawa Congress Centre, Ottawa, Canada. IEEE, 2006, pp. 1605–1608.

156. Memon, M.; Menghwar, G.D.; Depar, M.H.; Jalbani, A.A.; Mashwani, W.M. Security modeling for service-oriented systems using security pattern refinement approach. *Softw. Syst. Model.* **2014**, *13*, 549–572.

157. Duncan, I.; de Muijnck-Hughes, J. Security Pattern Evaluation. 8th IEEE International Symposium on Service Oriented System Engineering, SOSE 2014, Oxford, United Kingdom, April 7-11, 2014. IEEE Computer Society, 2014, pp. 428–429.

158. Sarmah, A.; Hazarika, S.M.; Sinha, S.K. Security Pattern Lattice: A Formal Model to Organize Security Patterns. 19th International Workshop on Database and Expert Systems Applications (DEXA 2008), 1-5 September 2008, Turin, Italy. IEEE Computer Society, 2008, pp. 292–296.

159. Moral-García, S.; Moral-Rubio, S.; Fernández-Medina, E. Security Pattern Mining: Systematic Review and Proposal. WOSIS 2011 - Proceedings of the 8th International Workshop on Security in Information Systems, In conjunction with ICEIS 2011, Beijing, China, 8-9 June, 2011; Rosado, D.G.; Sanchez, L.E.; Jürjens, J., Eds. SciTePress, 2011, pp. 13–24.

160. Fernández, E.B. Security Patterns and A Methodology to Apply them. In *Security and Dependability for Ambient Intelligence*; Kokolakis, S.; Gómez, A.M.; Spanoudakis, G., Eds.; Springer, 2009; Vol. 45, *Advances in Information Security*, pp. 37–46.

161. Rosado, D.G.; Gutiérrez, C.; Fernández-Medina, E.; Piattini, M. Security patterns and requirements for internet-based applications. *Internet Res.* **2006**, *16*, 519–536.

162. Fernández, E.B. Security Patterns and Secure Systems Design. Dependable Computing, Third Latin-American Symposium, LADC 2007, Morella, Mexico, September 26-28, 2007, Proceedings; Bondavalli, A.; Brasileiro, F.V.; Rajsbaum, S., Eds. Springer, 2007, Vol. 4746, *Lecture Notes in Computer Science*, pp. 233–234.

163. Cuevas, Á.; Khoury, P.E.; Gomez, L.; Laube, A. Security Patterns for Capturing Encryption-Based Access Control to Sensor Data. Proceedings of the Second International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2008, August 25-31, 2008, Cap Esterel, France; Cotton, A.; Dini, O.; Gómez-Skarmeta, A.F.; Ion, M.; Popescu, M.; Takesue, M., Eds. IEEE Computer Society, 2008, pp. 62–67.

164. Mouratidis, H.; Weiss, M.; Giorgini, P. Security Patterns Meet Agent Oriented Software Engineering: A Complementary Solution for Developing Secure Information Systems. Conceptual Modeling - ER 2005, 24th International Conference on Conceptual Modeling, Klagenfurt, Austria, October 24-28, 2005, Proceedings; Delcambre, L.M.L.; Kop, C.; Mayr, H.C.; Mylopoulos, J.; Pastor, O., Eds. Springer, 2005, Vol. 3716, *Lecture Notes in Computer Science*, pp. 225–240.

165. Hamid, B.; Gürgens, S.; Fuchs, A. Security patterns modeling and formalization for pattern-based development of secure software systems. *Innov. Syst. Softw. Eng.* **2016**, *12*, 109–140.

166. Yoshioka, N.; Honiden, S.; Finkelstein, A. Security Patterns: A Method for Constructing Secure and Efficient Inter-Company Coordination Systems. 8th International Enterprise Distributed Object Computing Conference (EDOC 2004), 20-24 September 2004, Monterey, California, USA, Proceedings. IEEE Computer Society, 2004, pp. 84–97.

167. Bandara, A.; Shinpei, H.; Jurjens, J.; Kaiya, H.; Kubo, A.; Laney, R.; Mouratidis, H.; Nhlabatsi, A.; Nuseibeh, B.; Tahara, Y.; Tun, T.; Washizaki, H.; Yoshioka, N.; Yu, Y. Security patterns: comparing modeling approaches. In *Software Engineering for Secure Systems: Industrial and Research Perspectives*; Mouratidis, H., Ed.; IGI Global: Hershey, PA, 2010; pp. 75–111.

168. Menzel, M.; Thomas, I.; Meinel, C. Security Requirements Specification in Service-Oriented Business Process Management. Proceedings of the The Forth International Conference on Availability, Reliability and Security, ARES 2009, March 16-19, 2009, Fukuoka, Japan. IEEE Computer Society, 2009, pp. 41–48.

169. Uzunov, A.V.; Fernández, E.B.; Falkner, K. Security solution frames and security patterns for authorization in distributed, collaborative systems. *Comput. Secur.* **2015**, *55*, 193–234.

170. Hasheminejad, S.M.H.; Jalili, S. Selecting proper security patterns using text classification. Proceedings - 2009 International Conference on Computational Intelligence and Software Engineering, CiSE 2009, 2009.

171. Serrano, D.; Maña, A.; Llarena, R.; Crespo, B.G.; Li, K. SERENITY Aware System Development Process. In *Security and Dependability for Ambient Intelligence*; Kokolakis, S.; Gómez, A.M.; Spanoudakis, G., Eds.; Springer, 2009; Vol. 45, *Advances in Information Security*, pp. 165–179.

172. Sánchez-Cid, F.; Maña, A. SERENITY Pattern-Based Software Development Life-Cycle. 19th International Workshop on Database and Expert Systems Applications (DEXA 2008), 1-5 September 2008, Turin, Italy. IEEE Computer Society, 2008, pp. 305–309.

173. Sánchez-Cid, F.; Muñoz, A.; Serrano, D.; Gago, M.C. Software engineering techniques applied to AmI: Security patterns. Developing Ambient Intelligence - Proceedings of the First International Conference on Ambient Intelligence Developments, AmID 2006, 2006, pp. 108–123.

174. Tryfonas, T.; Kearney, B. Standardising business application security assessments with pattern-driven audit automations. *Computer Standards & Interfaces* **2008**, *30*, 262 – 270.

175. Alzahrani, A.A.H.; Eden, A.H.; Yafi, M.Z. Structural Analysis of the Check Point Pattern. 8th IEEE International Symposium on Service Oriented System Engineering, SOSE 2014, Oxford, United Kingdom, April 7-11, 2014. IEEE Computer Society, 2014, pp. 404–408.

176. Babar, M.A.; Wang, X.; Gorton, I. Supporting Security Sensitive Architecture Design. Quality of Software Architectures and Software Quality, First International Conference on the Quality of Software Architectures, QoSA 2005 and Second International Workshop on Software Quality, SOQUA 2005, Erfurt, Germany, September 20-22, 2005, Proceedings; Reussner, R.H.; Mayer, J.; Stafford, J.A.; Overhage, S.; Becker, S.; Schroeder, P.J., Eds. Springer, 2005, Vol. 3712, *Lecture Notes in Computer Science*, pp. 140–154.

177. Hazeyama, A. Survey on Body of Knowledge Regarding Software Security. 13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, SNPD 2012, Kyoto, Japan, August 8-10, 2012; Hochin, T.; Lee, R.Y., Eds. IEEE Computer Society, 2012, pp. 536–541.

178. Porekar, J.; Saljic, S.; Klobucar, T.; Jerman-Blazic, A. Technical Patterns for Long Term Trusted Archiving. Third International Conference on the Digital Society (ICDS 2009), February 1-7, 2009, Cancun, Mexico. IEEE Computer Society, 2009, pp. 241–246.

179. Kobashi, T.; Yoshizawa, M.; Washizaki, H.; Fukazawa, Y.; Yoshioka, N.; Okubo, T.; Kaiya, H. TESEM: A Tool for Verifying Security Design Pattern Applications by Model Testing. 8th IEEE International Conference on Software Testing, Verification and Validation, ICST 2015, Graz, Austria, April 13-17, 2015. IEEE Computer Society, 2015, pp. 1–8.

180. Morrison, P.; Fernandez, E.B. The credentials pattern. PLoP 2006 - PLoP Pattern Languages of Programs 2006 Conference Proceedings, 2006.

181. Ciria, J.C.; Domínguez, E.; Escario, I.; Francés, A.R.; Lapeña, M.J.; Zapata, M.A. The *history-based authentication* pattern. Proceedings of the 19th European Conference on Pattern Languages of Programs, EuroPLoP 2014, Irsee, Germany, July 9-13, 2014; Eloranta, V.; van Heesch, U., Eds. ACM, 2014, pp. 30:1–30:9.

182. Alkussayer, A.; Allen, W.H. *The ISDF framework: Integrating security patterns and best practices*; Vol. 36, *Communications in Computer and Information Science*, 2009; pp. 17–28.

183. Hafiz, M.; Adamczyk, P. The nature of order: from security patterns to a pattern language. Conference on Systems, Programming, and Applications: Software for Humanity, SPLASH '12, Tucson, AZ, USA, October 21-25, 2012; Leavens, G.T., Ed. ACM, 2012, pp. 75–76.

184. Gutiérrez, C.; Rosado, D.G.; Fernández-Medina, E. The practical application of a process for eliciting and designing security in web service systems. *Inf. Softw. Technol.* **2009**, *51*, 1712–1738.

185. Shahzad, A.; Musa, S.; Aborujilah, A.; Irfan, M. The Security Survey and Anaylsis on supervisory control and Data Acquisition Communication. *J. Comput. Sci.* **2014**, *10*, 2006–2019.

186. Heyman, T.; Yskout, K.; Scandariato, R.; Schmidt, H.; Yu, Y. The Security Twin Peaks. Engineering Secure Software and Systems - Third International Symposium, ESSoS 2011, Madrid, Spain, February 9-10, 2011. Proceedings; Erlingsson, Ú.; Wieringa, R.J.; Zannone, N., Eds. Springer, 2011, Vol. 6542, *Lecture Notes in Computer Science*, pp. 167–180.

187. de Muijnck-Hughes, J.; Duncan, I. Thinking Towards a Pattern Language for Predicate Based Encryption Crypto-Systems. Sixth International Conference on Software Security and Reliability, SERE 2012, Gaithersburg, Maryland, USA, 20-22 June 2012 - Companion Volume. IEEE, 2012, pp. 27–32.

188. Okubo, T.; Wataguchi, Y.; Kanaya, N. Threat and countermeasure patterns for cloud computing. 4th IEEE International Workshop on Requirements Patterns, RePa 2014, Karlskrona, Sweden, August 26, 2014; Zhao, L.; do Prado Leite, J.C.S.; Supakkul, S.; Chung, L.; Wang, Y., Eds. IEEE Computer Society, 2014, pp. 43–46.

189. Anand, P.; Ryoo, J.; Kim, H.; Kim, E. Threat Assessment in the Cloud Environment: A Quantitative Approach for Security Pattern Selection. Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication, IMCOM 2016, Danang, Vietnam, January 4-6, 2016. ACM, 2016, pp. 5:1–5:8.

190. Bouaziz, R.; Hamid, B.; Desnos, N. Towards a Better Integration of Patterns in Secure Component-Based Systems Design. Computational Science and Its Applications - ICCSA 2011 - International Conference,

Santander, Spain, June 20-23, 2011. Proceedings, Part V; Murgante, B.; Gervasi, O.; Iglesias, A.; Taniar, D.; Apduhan, B.O., Eds. Springer, 2011, Vol. 6786, *Lecture Notes in Computer Science*, pp. 607–621.

191. Graziano, A.; Dearden, A.; Seaton, J.W.; Williams, L.A. Towards a classification framework for security patterns. Proceedings of the 6th International Network Conference, INC 2006, 2006, pp. 237–244.

192. Blackwell, C. Towards a Conceptual Framework for Security Patterns. In *Cyberpatterns, Unifying Design Patterns with Security and Attack Patterns*; Blackwell, C.; Zhu, H., Eds.; Springer, 2014; pp. 17–34.

193. Fuchs, A.; Gürgens, S.; Rudolph, C. Towards a Generic Process for Security Pattern Integration. Database and Expert Systems Applications, DEXA, International Workshops, Linz, Austria, August 31-September 4, 2009, Proceedings; Tjoa, A.M.; Wagner, R.R., Eds. IEEE Computer Society, 2009, pp. 171–175. doi:10.1109/DEXA.2009.51.

194. Hafner, M.; Alam, M.; Breu, R. Towards a MOF/QVT-Based Domain Architecture for Model Driven Security. Model Driven Engineering Languages and Systems, 9th International Conference, MoDELS 2006, Genova, Italy, October 1-6, 2006, Proceedings; Nierstrasz, O.; Whittle, J.; Harel, D.; Reggio, G., Eds. Springer, 2006, Vol. 4199, *Lecture Notes in Computer Science*, pp. 275–290.

195. Ortiz, R.; Moral-Rubio, S.; Garzás, J.; Fernández-Medina, E. Towards a Pattern-based Security Methodology to Build Secure Information Systems. WOSIS 2011 - Proceedings of the 8th International Workshop on Security in Information Systems, In conjunction with ICEIS 2011, Beijing, China, 8-9 June, 2011; Rosado, D.G.; Sanchez, L.E.; Jürjens, J., Eds. SciTePress, 2011, pp. 59–69.

196. Fernández, E.B.; Yimam, D. Towards Compliant Reference Architectures by Finding Analogies and Overlaps in Compliance Regulations. SECRYPT 2015 - Proceedings of the 12th International Conference on Security and Cryptography, Colmar, Alsace, France, 20-22 July, 2015; Obaidat, M.S.; Lorenz, P.; Samarati, P., Eds. SciTePress, 2015, pp. 435–440.

197. Kozlovs, D.; Cjaputa, K.; Kirikova, M. Towards Continuous Information Security Audit. Joint Proceedings of REFSQ-2016 Workshops, Doctoral Symposium, Research Method Track, and Poster Track co-located with the 22nd International Conference on Requirements Engineering: Foundation for Software Quality (REFSQ 2016), Gothenburg, Sweden, March 14, 2016; Bjarnason, E.; Borg, M.; Daun, M.; Dieste, O.; España, S.; Felderer, M.; Forbrig, P.; Franch, X.; Gay, G.; Herrmann, A.; Horkoff, J.; Kirikova, M.; Morandini, M.; Opdahl, A.L.; Paech, B.; Palomares, C.; Petersen, K.; Seffah, A.; Tenbergen, B.; Unterkalmsteiner, M., Eds. CEUR-WS.org, 2016, Vol. 1564, *CEUR Workshop Proceedings*.

198. Alebrahim, A.; Heisel, M. Towards Developing Secure Software Using Problem-Oriented Security Patterns. Availability, Reliability, and Security in Information Systems - IFIP WG 8.4, 8.9, TC 5 International Cross-Domain Conference, CD-ARES 2014 and 4th International Workshop on Security and Cognitive Informatics for Homeland Defense, SeCIHD 2014, Fribourg, Switzerland, September 8-12, 2014. Proceedings; Teufel, S.; Tjoa, A.M.; You, I.; Weippl, E.R., Eds. Springer, 2014, Vol. 8708, *Lecture Notes in Computer Science*, pp. 45–62.

199. Serrano, D.; Maña, A.; Sotirious, A. Towards Precise Security Patterns. 19th International Workshop on Database and Expert Systems Applications (DEXA 2008), 1-5 September 2008, Turin, Italy. IEEE Computer Society, 2008, pp. 287–291.

200. Ferreira, A.; Rusu, C.; Roncagliolo, S. Usability and Security Patterns. Second International Conference on Advances in Computer-Human Interaction, ACHI 2009, February 1-7, 2009, Cancun, Mexico. IEEE, 2009, pp. 301–305.

201. Fernández, E.B.; Delessy, N.A. Using Patterns to Understand and Compare Web Services Security Products and Standards. Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT/ICIW 2006), 19-25 February 2006, Guadeloupe, French Caribbean. IEEE Computer Society, 2006, p. 157.

202. Heckman, M.R.; Schell, R.R. Using Proven Reference Monitor Patterns for Security Evaluation. *Inf.* **2016**, 7, 23.

203. Aziz, B.; Blackwell, C. Using Security Patterns for Modelling Security Capabilities in Grid Systems. 8th IEEE International Symposium on Service Oriented System Engineering, SOSE 2014, Oxford, United Kingdom, April 7-11, 2014. IEEE Computer Society, 2014, pp. 422–427.

204. Heyman, T.; Scandariato, R.; Huygens, C.; Joosen, W. Using Security Patterns to Combine Security Metrics. Proceedings of the The Third International Conference on Availability, Reliability and Security, ARES 2008,

March 4-7, 2008, Technical University of Catalonia, Barcelona , Spain. IEEE Computer Society, 2008, pp. 1156–1163.

205.    Fernandez, E.B.; Yoshioka, N.; Washizaki, H.; Jurjens, J.; VanHilst, M.; Pernu, G. Using security patterns to develop secure systems. In *Software Engineering for Secure Systems: Industrial and Research Perspectives*; Mouratidis, H., Ed.; IGI Global: Hershey, PA, 2010; pp. 16–31.

206.    Wagner, R.; Fontoura, L.M.; Fontoura, A.B. Using Security Patterns to Tailor Software Process. Proceedings of the 23rd International Conference on Software Engineering & Knowledge Engineering (SEKE'2011), Eden Roc Renaissance, Miami Beach, USA, July 7-9, 2011. Knowledge Systems Institute Graduate School, 2011, pp. 672–677.

207.    Fernandez, E.B.; Petrie, M.M.L. Using UML and security patterns to teach secure systems design. ASEE Annual Conference and Exposition, Conference Proceedings, 2005, pp. 15511–15520.

208.    Kobashi, T.; Yoshioka, N.; Okubo, T.; Kaiya, H.; Washizaki, H.; Fukazawa, Y. Validating Security Design Patterns Application Using Model Testing. 2013 International Conference on Availability, Reliability and Security, ARES 2013, Regensburg, Germany, September 2-6, 2013. IEEE Computer Society, 2013, pp. 62–71.

209.    Yoshizawa, M.; Kobashi, T.; Washizaki, H.; Fukazawa, Y.; Okubo, T.; Kaiya, H.; Yoshioka, N. Verifying Implementation of Security Design Patterns Using a Test Template. Ninth International Conference on Availability, Reliability and Security, ARES 2014, Fribourg, Switzerland, September 8-12, 2014. IEEE Computer Society, 2014, pp. 178–183.

210.    Anand, P.; Ryoo, J.; Kazman, R. Vulnerability-Based Security Pattern Categorization in Search of Missing Patterns. Ninth International Conference on Availability, Reliability and Security, ARES 2014, Fribourg, Switzerland, September 8-12, 2014. IEEE Computer Society, 2014, pp. 476–483.

211.    Okubo, T.; Tanaka, H. Web security patterns for analysis and design. PLoP08 - 15th Conference on Pattern Languages of Programs, Proceedings, 2008.

212.    King, A.C.; Subramanian, K.; Kanhaa, V. Wireless Information security system via role based access control pattern use case design. Proceedings of the 2008 International Conference on Computing, Communication and Networking, ICCCN 2008, 2008.

213.    Barhoom, T.S.; Shen-Sheng, Z. Using Proven Reference Monitor Patterns for Security Evaluation. *Information Technology Journal* **2007**, *6*, 996–1004.

214.    Regainia, L.; Salva, S.; Ecuhcurs, C. A classification methodology for security patterns to help fix software weaknesses. 13th IEEE/ACS International Conference of Computer Systems and Applications, AICCSA 2016, Agadir, Morocco, November 29 - December 2, 2016. IEEE Computer Society, 2016, pp. 1–8.

215.    Trubiani, C.; Ghabi, A.; Egyed, A. Exploiting traceability uncertainty between software architectural models and extra-functional results. *J. Syst. Softw.* **2017**, *125*, 15–34.

216.    Motii, A.; Hamid, B.; Lanusse, A.; Bruel, J. Guiding the Selection of Security Patterns for Real-Time Systems. 21st International Conference on Engineering of Complex Computer Systems, ICECCS 2016, Dubai, United Arab Emirates, November 6-8, 2016; Wang, H.; Mokhtari, M., Eds. IEEE Computer Society, 2016, pp. 155–164.

217.    Anand, P.; Ryoo, J.; Kim, H. Addressing Security Challenges in Cloud Computing - A Pattern-Based Approach. 1st International Conference on Software Security and Assurance, ICSSA 2015, Suwon, South Korea, July 27, 2015. IEEE, 2015, pp. 13–18.

218.    Regainia, L.; Salva, S. A Methodology of Security Pattern Classification and of Attack-Defense Tree Generation. Proceedings of the 3rd International Conference on Information Systems Security and Privacy, ICISSP 2017, Porto, Portugal, February 19-21, 2017; Mori, P.; Furnell, S.; Camp, O., Eds. SciTePress, 2017, pp. 136–146.

219.    Amorim, T.; Martin, H.; Ma, Z.; Schmittner, C.; Schneider, D.; Macher, G.; Winkler, B.; Krammer, M.; Kreiner, C. Systematic Pattern Approach for Safety and Security Co-engineering in the Automotive Domain. Computer Safety, Reliability, and Security - 36th International Conference, SAFECOMP 2017, Trento, Italy, September 13-15, 2017, Proceedings; Tonetta, S.; Schoitsch, E.; Bitsch, F., Eds. Springer, 2017, Vol. 10488, *Lecture Notes in Computer Science*, pp. 329–342.

220.    Nafees, T.; Coull, N.; Ferguson, R.I.; Sampson, A.T. Idea-Caution Before Exploitation: The Use of Cybersecurity Domain Knowledge to Educate Software Engineers Against Software Vulnerabilities. Engineering Secure Software and Systems - 9th International Symposium, ESSoS 2017, Bonn, Germany,

July 3-5, 2017, Proceedings; Bodden, E.; Payer, M.; Athanasopoulos, E., Eds. Springer, 2017, Vol. 10379, *Lecture Notes in Computer Science*, pp. 133–142.

221. Shin, M.E.; Gomaa, H.; Pathirage, D. Model-based Design of Reusable Secure Connectors. Proceedings of MODELS 2017 Satellite Event: Workshops (ModComp, ME, EXE, COMMitMDE, MRT, MULTI, GEMOC, MoDeVVa, MDETools, FlexMDE, MDEbug), Posters, Doctoral Symposium, Educator Symposium, ACM Student Research Competition, and Tools and Demonstrations co-located with ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS 2017), Austin, TX, USA, September, 17, 2017; Burgueño, L.; Corley, J.; Bencomo, N.; Clarke, P.J.; Collet, P.; Famelis, M.; Ghosh, S.; Gogolla, M.; Greenyer, J.; Guerra, E.; Kokaly, S.; Pierantonio, A.; Rubin, J.; Ruscio, D.D., Eds. CEUR-WS.org, 2017, Vol. 2019, *CEUR Workshop Proceedings*, pp. 3–9.

222. Salva, S.; Regainia, L. Using Data Integration for Security Testing. Testing Software and Systems - 29th IFIP WG 6.1 International Conference, ICTSS 2017, St. Petersburg, Russia, October 9-11, 2017, Proceedings; Yevtushenko, N.; Cavalli, A.R.; Yenigün, H., Eds. Springer, 2017, Vol. 10533, *Lecture Notes in Computer Science*, pp. 178–194.

223. Argyropoulos, N.; Mouratidis, H.; Fish, A. Supporting Secure Business Process Design via Security Process Patterns. Enterprise, Business-Process and Information Systems Modeling - 18th International Conference, BPMDS 2017, 22nd International Conference, EMMSAD 2017, Held at CAiSE 2017, Essen, Germany, June 12-13, 2017, Proceedings; Reinhartz-Berger, I.; Gulden, J.; Nurcan, S.; Guédria, W.; Bera, P., Eds. Springer, 2017, Vol. 287, *Lecture Notes in Business Information Processing*, pp. 19–33.

224. Ruiz, J.F.; Arjona, M.; Maña, A.; Rudolph, C. Security knowledge representation artifacts for creating secure IT systems. *Comput. Secur.* **2017**, *64*, 69–91.

225. Sheta, M.A.; El Salam El Hadad, K.A.; AboelseoudM, H.; Zaki, M. Anti-spyware security design patterns. Proceedings - 2016 6th International Conference on Instrumentation and Measurement, Computer, Communication and Control, IMCCC 2016, 2016, pp. 465–470.

226. Mazo, R.; Feltus, C. Framework for Engineering Complex Security Requirements Patterns. 6th International Conference on IT Convergence and Security, ICITCS 2016, Prague, Czech Republic, September 26, 2016. IEEE Computer Society, 2016, pp. 1–5.

227. Fernandez, E.B. Threat Modeling in Cyber-Physical Systems. Proceedings - 2016 IEEE 14th International Conference on Dependable, Autonomic and Secure Computing, DASC 2016, 2016 IEEE 14th International Conference on Pervasive Intelligence and Computing, PICom 2016, 2016 IEEE 2nd International Conference on Big Data Intelligence and Computing, DataCom 2016 and 2016 IEEE Cyber Science and Technology Congress, CyberSciTech 2016, DASC-PICom-DataCom-CyberSciTech 2016, 2016, pp. 448–453.

228. ur Rehman, O.; Zivic, N. Secure Design Patterns for Security in Smart Metering Systems. 2015 IEEE European Modelling Symposium, EMS 2015, Madrid, Spain, October 6-8, 2015. IEEE, 2015, pp. 278–283.

229. Washizaki, H.; Fukumoto, S.; Yamamoto, M.; Yoshizawa, M.; Fukazawa, Y.; Kato, T.; Ogata, S.; Kaiya, H.; Fernández, E.B.; Kanuka, H.; Kondo, Y.; Yoshioka, N.; Okubo, T.; Hazeyama, A. A Metamodel for Security and Privacy Knowledge in Cloud Services. IEEE World Congress on Services, SERVICES 2016, San Francisco, CA, USA, June 27 - July 2, 2016; Bahsoon, R.; Zhang, L., Eds. IEEE Computer Society, 2016, pp. 142–143.

230. Fernández, E.B. Building Secure Cloud Architectures Using Patterns. 2016 IEEE International Conference on Cloud Engineering Workshop, IC2E Workshops, Berlin, Germany, April 4-8, 2016. IEEE Computer Society, 2016, p. 194.

231. Ponde, P.; Shirwaikar, S.; Kreiner, C. An analytical study of security patterns. Proceedings of the 21st European Conference on Pattern Languages of Programs, EuroPLoP 2016, Kaufbeuren, Germany, July 6-10, 2016; Preschern, C.; Eloranta, V., Eds. ACM, 2016, p. 33.

232. Fernández, E.B.; Yoshioka, N.; Washizaki, H.; Syed, M.H. Modeling and Security in Cloud Ecosystems. *Future Internet* **2016**, *8*, 1–15.

233. He, X.; Fu, Y. Modeling and Analyzing Security Patterns Using High Level Petri Nets. The 28th International Conference on Software Engineering and Knowledge Engineering, SEKE 2016, Redwood City, San Francisco Bay, USA, July 1-3, 2016; Gou, J., Ed. KSI Research Inc. and Knowledge Systems Institute Graduate School, 2016, pp. 623–627.

234. Motii, A.; Hamid, B.; Lanusse, A.; Bruel, J. Towards the integration of security patterns in UML component-based applications. Joint Proceedings of the Second International Workshop on Patterns

in Model Engineering and the Fifth International Workshop on the Verification of Model Transformation, PAME/VOLT 2016, co-located with ACM/IEEE 19th International Conference on Model Driven Engineering Languages and Systems (MoDELS 2016), Saint-Malo, France, October 2-3, 2016; Ergin, H.; Paige, R.F.; Syriani, E.; Zschaler, S.; Amrani, M., Eds. CEUR-WS.org, 2016, Vol. 1693, *CEUR Workshop Proceedings*, pp. 2–6.

235. Motii, A.; Lanusse, A.; Hamid, B.; Bruel, J. Model-Based Real-Time Evaluation of Security Patterns: A SCADA System Case Study. Computer Safety, Reliability, and Security - SAFECOMP 2016 Workshops, ASSURE, DECSoS, SASSUR, and TIPS, Trondheim, Norway, September 20, 2016, Proceedings; Skavhaug, A.; Guiochet, J.; Schoitsch, E.; Bitsch, F., Eds. Springer, 2016, Vol. 9923, *Lecture Notes in Computer Science*, pp. 375–389.

236. Horcas, J.; Pinto, M.; Fuentes, L. Automatic Enforcement of Security Properties. Trust, Privacy and Security in Digital Business - 13th International Conference, TrustBus 2016, Porto, Portugal, September 7-8, 2016, Proceedings; Katsikas, S.K.; Lambrinoudakis, C.; Furnell, S., Eds. Springer, 2016, Vol. 9830, *Lecture Notes in Computer Science*, pp. 19–31.

237. Lee, K.H.; Park, Y.B. Adaption of integrated secure guide for secure software development lifecycle. *International Journal of Security and its Applications* **2016**, *10*, 145–154.

238. Bunke, M. Software-security patterns: degree of maturity. Proceedings of the 20th European Conference on Pattern Languages of Programs, EuroPLoP 2015, Kaufbeuren, Germany, July 8-12, 2015; Link, C.; Eloranta, V., Eds. ACM, 2015, pp. 42:1–42:17.

239. Motii, A.; Hamid, B.; Lanusse, A.; Bruel, J. Guiding the selection of security patterns based on security requirements and pattern classification. Proceedings of the 20th European Conference on Pattern Languages of Programs, EuroPLoP 2015, Kaufbeuren, Germany, July 8-12, 2015; Link, C.; Eloranta, V., Eds. ACM, 2015, pp. 10:1–10:17.

240. Atymtayeva, L.; Abdel-Aty, M. Improvement of security patterns strategy for information security audit applications. BMSD 2015 - Proceedings of the 5th International Symposium on Business Modeling and Software Design, 2015, pp. 199–204.

241. Rimba, P.; Zhu, L.; Xu, X.; Sun, D. Building Secure Applications Using Pattern-Based Design Fragments. 34th IEEE Symposium on Reliable Distributed Systems Workshop, SRDS 2015 Workshop, Montreal, QC, Canada, September 28 - October 1, 2015. IEEE Computer Society, 2015, pp. 19–24.

242. Yoshioka, N.; Washizaki, H.; Maruyama, K. A survey on security patterns. *Progress in Informatics* **2008**, pp. 35–47.

243. Kearney, B.; Tryfonas, T. Security Patterns for Automated Continuous Auditing. *Inf. Secur. J. A Glob. Perspect.* **2008**, *17*, 13–25. doi:10.1080/10658980701784594.

244. Washizaki, H. Security patterns: Research direction, metamodel, application and verification. International Workshop on Big Data and Information Security, IWBIS 2017, Jakarta, Indonesia, September 23-24, 2017. IEEE, 2017, pp. 1–4.

245. Washizaki, H.; Ogata, S.; Hazeyama, A.; Okubo, T.; Fernandez, E.B.; Yoshioka, N. Landscape of Architecture and Design Patterns for IoT Systems. *IEEE Internet Things J.* **2020**, *7*, 10091–10101.

246. Rajmohan, T.; Nguyen, P.H.; Ferry, N. Research Landscape of Patterns and Architectures for IoT Security: A Systematic Review. 46th Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2020, Portoroz, Slovenia, August 26-28, 2020. IEEE, 2020, pp. 463–470.

247. Babar, M.; Zhang, H. Systematic literature reviews in software engineering: Preliminary results from interviews with researchers. Third International Symposium on Empirical Software Engineering and Measurement (ESEM), 2009, pp. 346–355.

248. Washizaki, H.; Xia, T.; Kamata, N.; Fukazawa, Y.; Ogata, S.; Kaiya, H.; Tanaka, T.; Kanuka, H.; Yamaoto, D.; Yoshino, M.; Okubo, T.; Kato, T.; Hazeyama, A.; Yoshioka, N.; Priyalakshmi, G. Taxonomy and literature survey of security pattern research. 2018 IEEE Conference on Application, Information and Network Security, AINS 2018, 2018, pp. 87–92.

249. Unterkalmsteiner, M.; Feldt, R.; Gorschek, T. A Taxonomy for Requirements Engineering and Software Test Alignment. *ACM Transactions on Software Engineering and Methodology* **2014**, *23*, 16:1–16:38.

250. Glass, R.L. Sorting Out Software Complexity. *Communications of the ACM* **2002**, *45*, 19–21.

251. Kitchenham, B.; Brereton, O.P.; Budgen, D.; Turner, M.; Bailey, J.; Linkman, S. Systematic Literature Reviews in Software Engineering - A Systematic Literature Review. *Information and Software Technology* **2009**, *51*, 7–15.

252. dos Santos Marques, A.B.; Rodrigues, R.; Conte, T. Systematic Literature Reviews in Distributed Software Development: A Tertiary Study. 2012 IEEE Seventh International Conference on Global Software Engineering, Porto Alegre, Rio Grande do Sul, Brazil, August 27-30, 2012. IEEE Computer Society, 2012, pp. 134–143.

253. Dadwal, A.; Washizaki, H.; Fukazawa, Y.; Iida, T.; Mizoguchi, M.; Yoshimura, K. Prioritization in Automotive Software Testing: Systematic Literature Review. Proceedings of the 6th International Workshop on Quantitative Approaches to Software Quality co-located with 25th Asia-Pacific Software Engineering Conference (APSEC 2018), Nara, Japan, December 4, 2018, pp. 52–58.

254. Washizaki, H.; Uchida, H.; Khomh, F.; Guéhéneuc, Y. Studying Software Engineering Patterns for Designing Machine Learning Systems. 10th International Workshop on Empirical Software Engineering in Practice, IWESEP 2019, Tokyo, Japan, December 13-14, 2019. IEEE, 2019, pp. 49–54.

255. The MITRE Corporation. Common Weakness Enumeration Version 3.1. https://cwe.mitre.org/, 2018.

256. FIRST.Org. Common Vulnerability Scoring System v3.0: Specification Document. https://www.first.org/cvss/, 2015.

257. Xia, T.; Washizaki, H.; Kato, T.; Kaiya, H.; Ogata, S.; Fernández, E.B.; Kanuka, H.; Yoshino, M.; Yamamoto, D.; Okubo, T.; Yoshioka, N.; Hazeyama, A. Cloud Security and Privacy Metamodel - Metamodel for Security and Privacy Knowledge in Cloud Services. Proceedings of the 6th International Conference on Model-Driven Engineering and Software Development, MODELSWARD 2018, Funchal, Madeira - Portugal, January 22-24, 2018; Hammoudi, S.; Pires, L.F.; Selic, B., Eds. SciTePress, 2018, pp. 379–386.

258. Kang, K.C.; Cohen, S.G.; Hess, J.A.; Novak, W.E.; Peterson, A.S. Feature-Oriented Domain Analysis (FODA) Feasibility Study. *Technical Report CMU/SEI-90-TR-21* **1990**, pp. 1–148.

259. Czarnecki, K.; Helsen, S. Classification of Model Transformation Approaches. OOPSLA Workshop on Generative Techniques in the Context of Model-Driven Architecture, 2003, pp. 1–17.

260. Washizaki, H.; Guéhéneuc, Y.; Khomh, F. ProMeTA: a taxonomy for program metamodels in program reverse engineering. *Empir. Softw. Eng.* **2018**, *23*, 2323–2358.

261. Shostack, A., Ed. *Threat Modeling: Designing for Security*, 1 ed.; Wiley, 2014.

262. The MITRE Corporation. Common Vulnerability and Exposures. https://cve.mitre.org/, 2018.

263. The MITRE Corporation. Common Attack Pattern Enumeration and Classification. https://capec.mitre.org/, 2018.

264. Smite, D.; Wohlin, C.; Galvina, Z.; Prikladnicki, R. An Empirically Based Terminology and Taxonomy for Global Software Engineering. *Empirical Software Engineering* **2014**, *19*, 105–153.

265. Amato, F.; Mazzocca, N.; Moscato, F. Model driven design and evaluation of security level in orchestrated cloud services. *J. Netw. Comput. Appl.* **2018**, *106*, 78–89.

266. Alwakeel, A.M.; Alnaim, A.K.; Fernandez, E.B. A Survey of Network Function Virtualization Security. Conference Proceedings - IEEE SOUTHEASTCON, 2018, Vol. 2018-April.

267. Ali, I.; Asif, M. Applying security patterns for authorization of users in IoT based applications. 2018 International Conference on Engineering and Emerging Technologies, ICEET 2018, 2018, Vol. 2018-January, pp. 1–5.

268. Li, T.; Horkoff, J.; Mylopoulos, J. Holistic security requirements analysis for socio-technical systems. *Softw. Syst. Model.* **2018**, *17*, 1253–1285.