Systematic Mapping of Security Patterns Research

YURINA ITO, Waseda University
HIRONORI WASHIZAKI, Waseda University
MASATOSHI YOSHIZAWA, Waseda University
YOSHIAKI FUKAZAWA, Waseda University
TAKAO OKUBO, Institute of Information Security
HARUHIKO KAIYA, Kanagawa University
ATSUO HAZEYAMA, Tokyo Gakugei University
NOBUKAZU YOSHIOKA, National Institute of Informatics
EDUARDO B. FERNANDEZ, Florida Atlantic University

Security patterns (SPs) are reusable solutions to security problems. We study here research papers that use security patterns to build secure systems or analyze the nature of security patterns. The goal of this paper is neither listing nor direct mapping of existing over 200 SPs but finding about how SPs are being investigated within research works to guide future research targeting SPs. Although the number of SPs has recently grown, the current trends and future prospects of SP research (e.g., research content and their modeling methods of SPs) are uncertain due to the diversity in the research results themselves. To elucidate the current trends and future prospects, herein we classify 30 works on SPs using a technique called systematic mapping (SM), which addresses the following three research questions with nine facets for classification: RQ1. Is SP research an active field? RQ2. What are the current trends of SP research? RQ3: What are the future prospects of SP research? Obtained answers are: A1. SP research has been conducted constantly in the past decade, confirming that the field is active. A2. The most common research topic is the SP application, demonstrating that efficient and reliable techniques to apply SPs are necessary to guarantee security. A3. There could be several future prospects aligned with the facets. For example, Access Control is a common concrete SP in current SP research and is likely in actual development; however, it needs to be further examined for other SPs in addition to access control to handle various threats. These answers are expected to improve further SP research and the effectiveness of SPs.

Categories and Subject Descriptors: D.2.11 **[Software Architectures]**: Patterns

General Terms: Security

Additional Key Words and Phrases: Security patterns, systematic mapping, software pattern

ACM Reference Format:

Ito, I., Washizaki, H., Yoshizawa, M., Fukazawa, Y., Okubo, T., Kaiya, H., Hazeyama, A., Yoshioka, N. and Fernandez, E.B. 2015. Systematic Mapping of Security Patterns Research. HILLSIDE Proc. of Conf. on Pattern Lang. of Prog. 22 (October 2015), 10 pages.

1. INTRODUCTION

Patterns, which are encapsulated reusable solutions to recurrent problems under specific contexts, are important tools in software engineering. Software patterns include design patterns, analysis patterns, and security patterns (SPs). For example, the appearance of design patterns has been one of the most important developments in software engineering (Fernandez et al. 2008a). Developers are expected to achieve efficient and effective software development by reusing patterns (Kubo et al. 2005). SPs including concrete security patterns and abstract ones (Fernandez et al. 2008b) capture successful secure designs in a generic form that can be applied or instantiated to produce solutions with well-defined properties (Uzunov et al. 2012) to stop threats or correct vulnerabilities. Because SPs incorporate the knowledge of security experts, they provide guidelines to improve confidentiality, integrity, and availability of software development. Descriptions of software patterns including SPs usually contain several common items such as Context, Problem, Solution, and Consequences (Yoshioka et al. 2008).

SPs are used to realize security features, leading to a more secure system than a functionally equivalent system without patterns (Halkidis et al. 2006), and are intended for use by developers who are not security

This work was supported by IISF SSR Forum 2015. This work was also supported by JSPS KAKENHI Grant Number 25330091 and "Research Initiative on Advanced Software Engineering in 2015" supported by Reliability Enhancement Center (SEC), Information Technology Promotion Agency Japan (IPA).
Author's address: 3-4-1 Shinokubo, Nakano-ku, Tokyo, 1698555 Japan; email: washizaki@waseda.jp

professionals (Schumaher et al. 2005)(Fernandez 2013). They enable developers and engineers to recognize, with relative ease, known vulnerabilities in their design and potential solutions (Heyman et al. 2007). Several security patterns have been reported by practitioners and researchers, and there are lively and ongoing discussions about the discovery, documentation and application of security patterns (Bandara 2010).

Although the number of SPs has considerably increased (Rosado et al. 2006), the current trends and future prospects of SP research (e.g., research content and their modeling methods of SPs) are uncertain due to the diversity in the research results themselves. To elucidate the current trends and future prospects, we study here research papers that use security patterns to build secure systems or analyze the nature of security patterns. The goal of this paper is neither listing nor direct mapping of existing over 200 SPs but finding about how SPs are being investigated within research works to guide future research targeting SPs.

Because security is involved with almost all aspects, technical elements, and stages of systems and software, numerous organizations are investigating SPs from different perspectives. Thus, the research results and how the results on SPs are shared (e.g., software conferences and journals, system conference, quality conference, etc.) vary tremendously, which makes it challenging for developers and operators to determine the most suitable techniques. To ensure security, it is desirable that every stage of development and operation accurately consider and use SPs. In practice, identifying areas where research on SPs is lacking is problematic, which makes studies beyond elementary technology and the research stage, such as SP groups, extremely difficult. Thus, SP research must be analyzed.

Herein we classify 30 papers[1] on SPs using Systematic Mapping (SM) to analyze the trends, where SP research indicates papers that use existing SPs but excludes papers that propose a specific SP as a new concept because they have been already studied (see Section 2. Related Work). Therefore, these 30 papers include a kind of experience reports of SP applications. The contribution of this paper is that the results should guide future SP research as well as assist engineers in applying or utilizing SPs by referring to the research classification results.

This paper is organized as follows. Section 2 describes related work. Section 3 explains the mapping process. Section 4 provides the mapping results and discussion. Finally, Section 5 summarizes this paper.

2. RELATED WORK

Although previous works have focused on SP classification, they differ from our study, which classifies SP research. One study classified SPs as quality analysis and coverage analysis after screening the literature (Heyman et al. 2007). Another, which aimed to identify the root causes of security violations, based the classification on security flaws along with other parameters to provide easy-to-use SPs (Alvi et al. 2011). In addition, a different study surveyed existing SP classifications (Alvi et al. 2012).

3. MAPPING PROCESS

SM is an existing classification method (Petersen et al. 2008) used to quickly and easily identify the coverage area of a research topic by preparing a visual summary. SM involves six steps: defining research questions, reviewing the scope, conducting a search, screening papers, keywording using abstracts, and data extraction and the mapping process.

We use SM to analyze the trends in SP research. Below each mapping step is described.

3.1 Defining Research Questions (RQs)

In SM, RQs narrow the topic of interest. SPs are used to implement security features and lead to a more secure system than a functionally equivalent system without patterns (Halkidis et al. 2006). Recently, the number of SPs has increased (Rosado et al. 2006). However, to facilitate use of SPs, more SP research and a better understanding of the research trends are desirable. This study poses three RQs.

RQ1: Is SP research an active field?
RQ2: What are the current trends of SP research?
RQ3: What are the future prospects of SP research?

[1] We did not try to select papers based on quality; we just followed the SM process and exclusion criteria described in Section 2. Moreover we were not trying to be comprehensive since the number of papers reviewed is limited to 100. We intend to enlarge the scope of the paper in a subsequent version.

3.2 Reviewing the Scope

In SM, review scope specifies the number of potential targets (hits) used in the mapping. Here the review scope is limited to the top 50 results for a keyword search using two different search engines where the results are sorted by relevance. Because the results are not necessarily related to security patterns, we actually read the papers in the hits. Hence, we reviewed 100 papers on November 2014.

3.3 Conducting a Search

In SM, conduct search sets the parameters in the mapping. Here we define our search engines as ACM Digital Library (ACM DL http://dl.acm.org/) and IEEE Xplore (http://ieeexplore.ieee.org/Xplore/home.js) because these are famous search engines, and "security pattern" is the keyword. We retrieved 50 papers by ACM DL and another 50 by IEEE Xplore. As a result, there was one paper hit in both search engines.

3.4 Screening Papers

In SM, screening allows the results to be roughly evaluated and those inconsistent with the RQs posed in the first step to be excluded. Here we employ four exclusion conditions:

1. Papers that cannot be referenced from the search engines (3 papers)
2. Papers not related to security patterns (32 papers)
3. Papers proposing a specific SP after reading them (34 papers)
4. Papers that were a hit in both search engines (1 paper)

Hence, a total of 30 papers are analyzed in SM. We attached the list of these papers as Table 1. We believe that 30 papers could be enough to grasp the current trends; in the future we have a plan to investigate more papers to clarify detailed trends.

3.5 Keywording Using Abstracts

In SM, facets are defined as the evaluation axes by reading abstracts and identifying keywords in the 30 papers. The facets aim to answer the RQs. Here we define nine facets due to the features of SP research:

(1) F1: Year published

Because the number of SPs has grown recently (Rosado et al. 2006), the number of SP research papers may have also grown. Confirming this speculation will provide insight on SP research.

(2) F2: Research content

Research on SPs covers diverse topics (Uunov et al. 2012). Hence, revealing what topics have been studied will provide insight on SP research.

(3) F3: SP modeling methods

Because various SP modeling methods exist (Bandara et al. 2010), revealing the most common ones might provide a new direction for SP research, such as unification and selection of appropriate modeling method according to objectives (and SPs).

(4) F4: SPs to be dealt with

Because there are various SPs (Rosado et al. 2006), revealing the most common SPs to be dealt with will provide insight on SP research and the applicability to actual problems.

(5) F5: Experimental evaluations

For practical implementation, SP research should not only propose but also conduct experimental evaluations (e.g., case study according to an example). Thus, whether a work includes experiments is crucial for practical applications.

(6) F6: Number of SPs in a paper

As the number of SPs has increased (Rosado et al. 2006), SP research should not only deal with single SP but also investigate multiple SPs although some conferences could have paper size limitation[2].

(7) F7: Relationships between SPs

Because related patterns can solve large problems (Washizaki et al. 2014), whether a paper considers the relationships between SPs is crucial information.

(8) F8: Phases that SPs are applied

Because security must be considered for all phases of the lifecycle (Devanbu et al. 2000), the phase that the SP is applied is crucial information.

(9) F9: Tooling

[2] PLoP conferences usually do not have paper size limitation.

If tooling is fully implemented, the results will be independent of the individuals conducting the research, allowing the maturity to be evaluated. However, tooling implementation can be difficult when SPs or SP research is abstract. Thus, it is important to clarify how much tooling is actually implemented.

Table 1 Entire classification results of SP researches

Ref.	F1	F2	F3	F4	F5	F6	F7	F8	F9
A1	2009	application	UML	RBAC, Authentication, Logger, Firewall, Authorization, IDS	yes	6	yes	(iv)	no
A2	2014	application	UML	SoSpa (System of aspect-oriented Security design Patterns)	no	1 (set)	yes	(ii)	no
A3	2008	modeling	Petri nets	Sandbox and Message Secrecy	no	2	no	(iii)	no
A4	2005	case study	NL	Compartmentalization, Distributed Delegation pattern , Trust Partitioning, Unique Atomic Chunks, Secure Pre-forking, Chroot Jail	no	6	no	(ii)	no
A5	2011	detection	UML	Single Access Point	yes	1	-	(iii)	no
A6	2012	validation	NL	Authentication, Logger, Firewall, Authorization, Single Access etc. (details are in (E. B. Fernandez et al. 2013))	yes	35	yes	(ii)	no
A7	2013	application	SAM	Logger, Authorization	yes	2	no	(vi)	no
A8	2008	case study	UML	ReferenceMonitor, Authorization, Authentication, Firewall etc. (details are in (N. Delessy et al. 2008))	no	18	yes	(vi)	no
A9	2005	modeling	HL7, JAHIS	RBAC	yes	1	-	unknown	no
A10	2010	other	UML	RBAC, Authentication, Authorization, Reference Monitor	yes	4	yes	(v)	no
A11	2013	validation	UML	RBAC, Password Design and Use, Prevent SQL Injection	yes	3	no	(v)	no
A12	2009	application	UML	Property Certification, Secure Match, Mutual Key PoK	no	3	no	unknown	no
A13	2013	application	UML	RBAC	yes	1	-	(iv)	yes
A14	2009	other	UML	Authorization	no	1	-	(i)	no
A15	2012	application	UML	Active Replication	yes	1	-	(iii)	no
A16	2007	detection	UML	Authentication, Secure Pipe	yes	2	yes	unknown	no
A17	2008	case study	XACML	Authorization	yes	1	-	(iv)	no
A18	2008	selection	GRL, Prolog	RBAC, Single Access Point, Checkpoint	no	4	yes	(v)	yes
A19	2011	other	NL	Payment, Anti Cross Site Request Forgery (CSRF)	yes	2	yes	(v)	no
A20	2008	application	NL	Sensor Encryption, Data Decryption, Grant-Based Access Control	no	3	yes	(iii)	no
A21	2009	selection	NL	patterns described in (M. Schumacher et al. 2005)	yes	46	yes	unknown	no
A22	2013	application	unknown	patterns described in (M. Schumacher et al. 2006)	yes	46	yes	(ii)	no
A23	2011	application	UML	Authorization, RBAC, Multilevel Security, Reference Monitor, Password Design And Use	no	5	no	(ii)	yes
A24	2012	application	UML	Authorizationzation, RBAC	yes	2	no	(vi)	no
A25	2010	application	unknown	Authorization, Reference Monitor, Log/Audit	no	3	yes	(v)	no
A26	2012	case study	unknown	Input Validation Vulnerability Tests, Force Exposure Tests, Malicious File Tests, Malicious Use of Security Functions Tests, Dangerous URL Tests, Audit Tests	no	6	no	(vii)	yes
A27	2014	application	unknown	Computer-Oriented Security Patterns (COSPs)	no	1	-	(vi)	no
A28	2010	application	DLS	Authentication	no	1	-	unknown	no
A29	2010	other	NL	Authentication, ServiceAccessControl	no	2	no	(vi)	no
A30	2008	application	unknown	Audit Interceptor, Secure Logger, Authentication	yes	3	no	unknown	no

3.6 Data Extraction and the Mapping Process

This step of SM visualizes the results for further analysis. Firstly we reviewed each paper in detail, classified it into a certain category for each facet and documented the classification result into a data table. Secondly we calculated the frequencies of papers in each category on the data table and created several systematic maps. The results of this study are discussed in the next section.

4. RESULTS AND DISCUSSION

Using SM, we collected 30 papers (denoted as A1-A30) on SPs and analyzed the trends. Table 1 depicts the classification results of the papers.

4.1 Results from a Single Facet

(1) F1: Year published

SP research has been conducted in the past most decade (Fig. 1). For 2014, the number of papers is as of Nov. 2014. Moreover, search engines may need some extra time to index published papers so that the number for

2014 is incomplete. In Fig 1, many researches appeared in 2008, and later constant numbers of researches appeared 2009-2013. The reason could be that 2-3 years were necessary to proceed with solid SP researches after the well-organized set of SPs (M. Schumacher et al. 2005) have been firstly published in 2005.

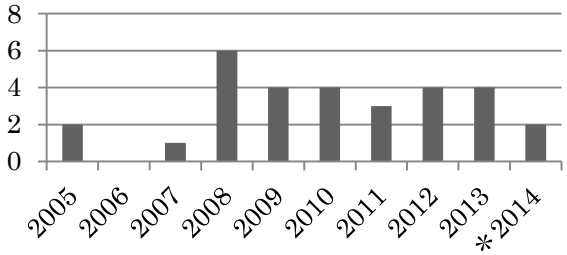

Fig. 1. Number of papers by year (F1)

(2) F2: Research contents

Based on a survey of SPs (Yoshioka et al. 2008), we divided the research content into seven categories. The results are as follows: 46% (14 papers) apply SPs, 13% (four papers) conduct case studies, 7% (two papers) provide specific models for SPs, 7% (two papers) detect SPs, 7% (two papers) validate SPs, 7% (two papers) select SPs, and 13% (four papers) focus on other topics. It should be noted that a case study indicates implementation of SPs in certain scenarios. The most common category is applying SP, suggesting that there could be a large demand for efficient and reliable techniques to apply and implement SPs.

(3) F3: SP modeling methods

We divided the modeling methods into four categories. The results are as follows: 43% (13 papers) use UML, 20% (six papers) use a natural language ("NL"), 20% (six papers) use another language ("others"), and the modeling method is difficult to identify in the remaining 17% (5 papers). The most common modeling method is UML, while "others" is the second most common. Others include Petri Nets (Horvath et al. 2008), SAM (Serscis Access Modeller) notation (Rimba 2013), HL7 and JAHIS (Fernandez et al. 2005), XACML (eXtensible Access Control Markup Language) (Busnel et al. 2008), GRL (goal-oriented requirement language) (Weiss et al. 2008), and DSL (domain specific languages) (Menzel et al. 2010), where each method has a specific purpose. Although modeling using a natural language mainly describes pattern characteristics, it is difficult to convert it into design and code. These findings demonstrate the importance of modeling methods complementing each other.

(4) F4: Concrete SPs to be dealt with

Figure 2 plots the values when at least two papers examine the same SP. The three most common SPs are Authorization, Role-Based Access Control (RBAC), and Authentication. Access control is a common concrete SP in SP research and is likely in actual development. However, it needs to be further examined for other SPs in addition to access control to handle various threats. This may become a more common topic in the future. For example, access control could denote the combination of authorization and enforcement done by the reference monitor.

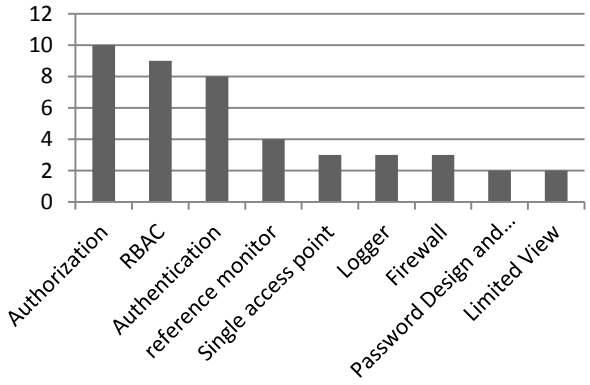

Fig. 2. Number of papers per each SP (F4)

(5) F5: Experimental evaluations

Over half of the papers (53%) involve experimental evaluations. However, the other half only propose an approach; hence, the effectiveness and validity of half are untested. To strengthen the effectiveness and validity, researchers should conduct more experimental evaluations in the future.

(6) F6: Number of SPs in a paper

Although some research uses more than 30 SPs, 47% use only one or two patterns. According to the facet F6 (Section 3.5), future research could consider to address more SPs to handle various specific threats in a uniform way.

(7) F7: Relationships between SPs

Only 40% of the papers consider relationships between SPs. According to the facet F7 (Section 3.5), future research should consider relationships between SPs to handle larger problems.

(8) F8: Phase where SPs are applied

We divided the development phases into categories: (i) analysis/requirement (one paper), (ii) design (five papers), (iii) implementation (four papers), (iv) analysis/requirement, design, and implementation (three papers), (v) analysis/requirement and design (five papers), (vi) design and implementation (five papers), and (vii) testing (one paper). The phases in the remaining six papers are unknown. Although there are fewer papers on the analysis/requirement and testing phases, the remaining phases are almost equally investigated.

(9) F9: Tooling

Only 13% of the papers (Bouziz et al 2013)(Weiss et al. 2008)(Ratchakom et al. 2011)(Smith et al. 2012) involve tooling. Since SPs are know-how and knowledge, their handling is largely by human hands. To promote a convenient treatment, tooling should increase and even be automated. This result indicates that SP research is still in its infancy in terms of automation.

4.2 Results from Facet Relations

The relationships between two or more facets are considered as bubble plots. We show only the characteristic results below where the number in the bubble denotes the number of papers.

(1) F3 and F5

Figure 3 plots the relationship between F3 and F5. The variation in the plot indicates that whether an experimental evaluation is conducted (F5) is independent of the modeling method (F3). It could be because it is not always necessary to have formal and/or specific models for experimental evaluations; experiments could be conducted for SPs modeled even in natural language.

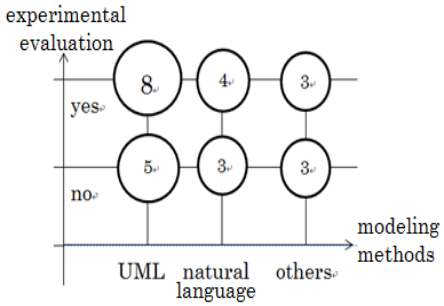

Fig. 3. Modeling methods (F3) and experimental evaluations (F5)

(2) F6 and F7

Figure 4 shows the relationship between F6 and F7. Papers with a large number of SPs (F6) tend to consider relationships between SPs (F7). It seems quite natural since such papers focusing on SP relationships are likely to handle many SPs for explaining motivations and evaluations.

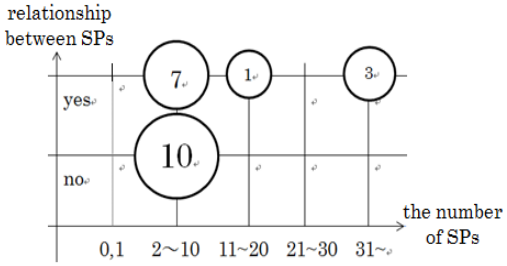

Fig. 4. Number of SPs (F6) and relationships between SPs (F7)

(3) F3, F4 and F5

Figure 5 shows the relations between F3, F4, and F5. On the F4 axis, papers with four or more SPs are arranged in descending order from left. As shown in the upper part of Fig. 5 (F3 and F4), most SP research uses UML for modeling (F3) regardless of SPs to be dealt with (F4). It could be because UML is the most widely accepted formalism for the analysis and design of software (Berardi 2002). Therefore, UML could be considered as SP modeling method first in further researches if there is no specific requirement for models. As shown in the lower part of Fig. 5 (F4 and F5), research on less common patterns (right of F4 axis, e.g., reference monitor) is less likely to include an experimental evaluation (F5). It could be because the more patterns become popular, the more researchers are likely to pay attention to practical aspects of the patterns; and maybe vice versa. According to the facet F5 (Section 3.5), whether experimental evaluations are part of the research is crucial to apply SPs in practice; encouraging researchers conduct experimental evaluations for less common SPs might result in more applications of these SPs.

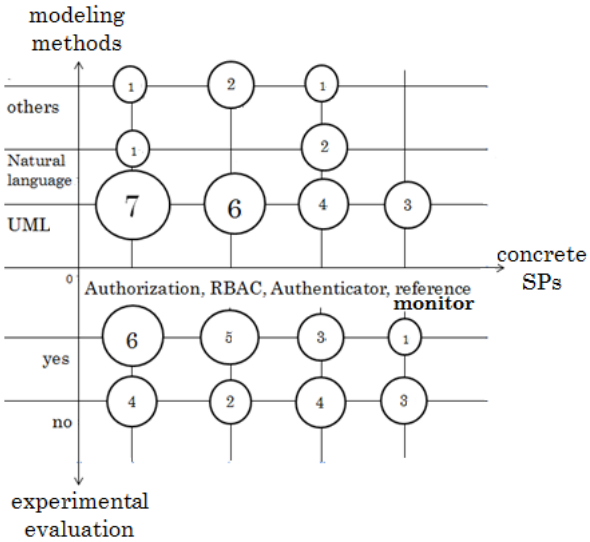

Fig. 5. Modeling methods (F3), concrete SPs to be dealt with (F4), and experimental evaluations (F5)

(4) F1 and F5

Figure 6 plots the relation between F1 and F5. For 2014, the number of papers is as of Nov. 2014. So the number for 2014 is incomplete. The number of experimental evaluations (F5) has increased recently (F1), indicating that research is shifting towards strengthening the effectiveness and validation of SPs.

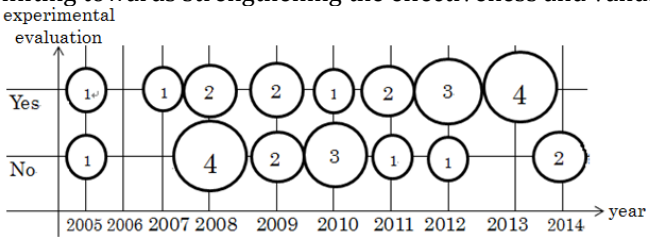

Fig. 6. Year published (F1) and experimental evaluations (F5)

(5) F3 and F6

Figure 7 shows the relation between F3 and F6. Studies that contain many SPs (F6) tend to use a natural language (F3) because it is difficult to precisely model many SPs due to lack of sharing reported results. Hence, accumulating knowledge should increase research requiring precise modeling.

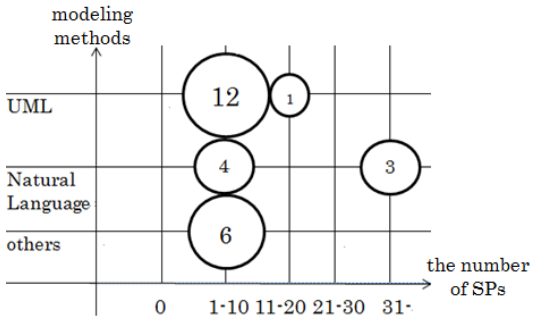

Fig. 7. Modeling methods (F3) and number of SPs (F6)

4.3 Summary of Findings and Future Perspectives

Our findings and future perspectives are as follows.

RQ1: Is SP research an active field?

F1. SP research has been conducted constantly in the past decade, confirming that the field is active.

RQ2: What are the current trends of SP research?

- F2. The most common research topic is application of SPs.
- F3. The most common modeling method is UML; "Others" where each method has a specific purpose is the second most common.
- F4. Access control is a common concrete SP in SP research and is likely in actual development.
- F5. About half of SP research involves experimental evaluations.
- F6. Similarly about half (47%) of SP research uses only one or two patterns.
- F7. Although the facet F7 (Section 3.5) states that future research should consider the relationships between SPs to handle larger problems, only 40% of research considers relationships.
- F8. There are fewer reports on the analysis/requirement and test phases, but the other phases have a similar number of papers, suggesting that SPs are used in all phases.
- F9. To date, only 13% of the papers involve tooling. Tooling and automation promote the reasonable treatment of SPs. The lack of tooling indicates that SP research is in its infancy in terms of automation.

The relationships between the facets are important in determining the direction of SP research. This study reveals many interesting relationships.

- F3 and F5. Whether an experimental evaluation is conducted is independent of the modeling method. It could be because it is not always necessary to have formal and/or specific models for experimental evaluations.
- F6 and F7. Papers with numerous SPs tend to consider their relationships. It seems quite natural since such papers focusing on SP relationships are likely to handle many SPs for explaining motivations and evaluations.
- F3 and F4. Most research on SPs employs UML for modeling regardless of SPs to be dealt with. It could be because UML is the most widely accepted formalism for the analysis and design of software.
- F4 and F5. Research on more common patterns is more likely to include experimental evaluations. It could be because the more patterns become popular, the more researchers likely to pay attention to practical aspects of the patterns; and maybe vice versa.
- F1 and F5. Research involving experimental evaluations has increased recently, indicating that research is strengthening the effectiveness and validation of SPs.
- F3 and F6. Studies using many SPs tend to use modeling methods in natural languages (F3 and F6) because modeling SPs precisely is difficult.

RQ3: What are the future prospects of SP research?

According to the answer of RQ2, there could be several future prospects aligned with the above-mentioned facets.

- F2. The most common research topic is application of SPs, demonstrating that efficient and reliable techniques to apply SPs are necessary to guarantee security.
- F3. Although UML is the most widely accepted formalism, it could be better that modeling methods complement each other to fully utilize each modeling method. Moreover, accumulated knowledge on SPs should improve research requiring precise modeling.
- F4. Encouraging researchers conduct experimental evaluations for less common SPs (e.g., reference monitor) might result in more applications of the SPs. It needs to be further examined for other SPs in addition to access control to handle various threats. For example, access control could denote the combination of authorization and enforcement done by the reference monitor.
- F5. Because the effectiveness and validity of SPs are often untested, the amount of experimental evaluations should increase in the future.
- F6. To handle various threats in a uniform way, future research could consider to incorporate multiple SPs.
- F7. There are only 40% of researches considering relationships among SPs; future research should consider the relationships to handle larger problems. For example, pattern diagrams for describing SPs and relationships could be important.
- F8. SP research on analysis/requirement and test phases should increase.
- F3 and F4. UML could be considered as SP modeling method first in further researches if there is no specific requirement for models.
- F4 and F5. Encouraging researchers conduct experimental evaluations for less common SPs might result in more applications of the SPs.
- F3 and F6. As knowledge on SPs is accumulated, precise modeling should become easier, increasing the amount of research requiring precise models.

5. CONCLUSION

Herein SP research is classified using SM to analyze trends. The results provide various insights on the future direction of SP research as we summarized in Section 4.3. Our results should improve SP research and the effectiveness of SPs.

In the future, we plan to investigate detailed trends by adding more security-specific facets (such as threats and vulnerability addressed by the target research) and general ones (such as the number of citations of the target paper), by conducting statistical analysis if applicable, and by having deeper discussions on each facet. In addition, we plan to investigate more papers and incorporate other sources as the targets because there are many sources for SP research in addition to the ACM digital library and IEEE explore (e.g., papers from conferences and other search engines).

ACKNOWLEDGEMENT

Our thanks go to our shepherd Prof. Rosana Teresinha Vaccare Braga, PLoP 2015 Writer's Workshop group discussions lead Prof. Filipe Correia and participants for their valuable comments and guides to improve our paper significantly.

REFERENCES

A. K. Alvi et al. 2011. A natural classification scheme for software security patterns. DASC

A. K. Alvi et al. 2012. A Comparative Study of Software Security Pattern Classifications, ARES

A. Bandara, H. Shinpei, J. Jurjens, H. Kaiya, A. Kubo, R. Laney, H. Mouratidis, A. Nhlabatsi, B. Nuseibeh, Y. Tahara, T. Tun, H. Washizaki, N. Yoshioka, Y. Yu. 2010. Security patterns: Comparing modeling approaches, in Software Engineering for Secure Systems, pp.75-111, IGI Global

D. Berardi, 2002. Using DLs to reason on UML class diagrams, Workshop on Applications of Description Logic

R. Bouaziz et al. 2012. Applying security patterns for component based applications using UML profile, CSE **(A15)**

R. Bouaziz et al. 2012. Secure component based applications through security patterns, GreenCom **(A24)**

R. Bouaziz et al. 2013. An engineering process for security patterns application in component based models, WETICE **(A13)**

M. Bunke et al. 2011. An architecture-centric approach to detecting security patterns in software, ESSoS **(A5)**

P. Busnel et al. 2008. Achieving socio-technical confidentiality using security pattern in smart homes. FGCN **(A17)**

A. Cuevas et al. 2008. Security patterns for capturing encryption-based access control to sensor data, SECURWARE **(A20)**

A. Cuevas et al. 2009. A security pattern for untraceable secret handshakes, SECURWARE **(A12)**

N. Delessy et al. 2008. A pattern-driven security process for SOA applications, ARES **(A8)**

P. T. Devanbu et al. 2000. Software engineering for security: A roadmap, ICSE
J. Dong et al. 2007. Model checking security pattern compositions. QSIC **(A16)**
E. B. Fernandez et al. 2013. Security Patterns in Practice: Designing Secure Architectures Using Software Patterns, John Wiley & Sons
E. B. Fernandez, H. Washizaki, N. Yoshioka, A. Kubo, Y. Fukazawa. 2008a. Classifying security patterns, The 10th Asia Pacific Web Conference (APWeb2008), Shenyang, China, April 26-28
E. B. Fernandez, H. Washizaki, N. Yoshioka. 2008b. Abstract security patterns, 15th Conference on Pattern Languages of Programs (PLoP 2008)
E. B. Fernandez et al. 2009. On building secure SCADA systems using security patterns, CSIIRW **(A1)**
E. B. Fernandez et al. 2010. Building secure systems: From threats to security patterns, SCCC **(A25)**
E. Fernandez et al. 2005. An analysis of modeling flaws in HL7 and JAHIS, SAC **(A9)**
M. Hafiz. 2005. Security patterns and evolution of MTA architecture, OOPSLA
S. T. Halkidis et al. 2006. Quantitative evaluation of systems with security patterns using a fuzzy approach, OTM **(A4)**
S. Hasheminejad et al. 2009. Selecting proper security patterns using text classification, CiSE **(A21)**
T. Heyman et al. 2007. An Analysis of the Security Patterns Landscape, SESS
T. Heyman et al. 2008. Using security patterns to combine security metrics, ARES **(A30)**
V. Horvath et al. 2008. From security patterns to implementation using petri nets, SESS **(A3)**
T. Kobashi, N. Yoshioka, T. Okubo, H. Kaiya, H. Washizaki, and Y. Fukazawa. 2013. Validating security design patterns application using model testing, ARES **(A11)**
A. Kubo, H. Washizaki, A. Takasu, Y. Fukazawa. 2005. Analyzing relations among software patterns based on document similarity, International Conference on Information Technology: Coding and Computing (ITCC 2005)
M. Menzel et al. 2010. A pattern-driven generation of security policies for service-oriented architectures, ICWS **(A28)**
A. Mourad et al. 2010. A novel approach for the development and deployment of security patterns, SocialCom **(A29)**
P. H. Nguyen et al. 2014. Model-driven security with a system of aspect-oriented security design patterns, VAO **(A2)**
T. Okubo, H. Kaiya, and N. Yoshioka. 2011. Effective security impact analysis with patterns for software enhancement, ARES **(A19)**
K. Petersen et al. 2008. Systematic mapping studies in software engineering, EASE
M. Ratchakom et al. 2011. A process model design and tool support for information assets access control using security patterns, JCSSE **(A23)**
P. Rimba, 2013. Building high assurance secure applications using security patterns for capability-based platforms, ICSE **(A7)**
D. G. Rosado et al. 2006. Comparison of security patterns, IJCSNS 6(2)
P. Ruamjinda et al. 2013. Framework for information security standards storage and retrieval using security patterns, ICSESS **(A22)**
J. Ruiz et al. 2014. A security engineering process for systems of systems using security patterns, SysCon **(A27)**
M. Schumacher et al. 2005. Security Patterns: Integrating security and systems engineering. John Wiley & Sons
Y. Shiroma, H. Washizaki, Y. Fukazawa, A. Kubo, and N. Yoshioka. 2010. Model-driven security patterns application based on dependences among patterns, ARES **(A10)**
B. Smith et al. 2012. On the effective use of security test patterns, SERE **(A26)**
M. Solinas et al. 2009. Embedding security patterns into a domain model, DEXA **(A14)**
A.V. Uzunov, E.B. Fernandez, and K. Falkner. 2012. Engineering Security into Distributed Systems: A Survey of Methodologies, Journal of Universal Computer Science, Vol.18, No.20, pp.2920-3006
H. Washizaki et al. 2014. Network Analysis for Software Patterns including Organizational Patterns in Portland Pattern Repository. Agile
M. Weiss et al. 2008. Selecting security patterns that fulfill security requirements, RE **(A18)**
N. Yoshioka, H. Washizaki, and K. Maruyama. 2008. A survey on security patterns, Progress in Informatics 5(2)
K. Yskout et al. 2012. Does organizing security patterns focus architectural choices? ICSE **(A6)**

Received May 2015; revised September 2015; accepted February 2016