STATE OF THE ART SURVEY ON DSPL SECURITY CHALLENGES

Mohamed AMOUD, Ounsa ROUDIES

SIWeb Team - École Mohammadia d'Ingénieurs (EMI)
Mohammed V University in Rabat, Morocco

ABSTRACT

The Dynamic Software Product Line (DSPL) is becoming the system with high vulnerability and high confidentiality in which the adaptive security is a challenging task and critical for it to operate. Adaptive security is able to automatically select security mechanisms and their parameters at runtime in order to preserve the required security level in a changing environment. This paper presents a literature review of security adaptation approaches for DSPL, and evaluates them in terms of how well they support critical security services and what level of adaptation they achieve. This work will be done following the Systematic Review approach. Our results concluded that the research field of security approaches for DSPL is still poor of methods and metrics for evaluating and comparing different techniques. The comparison reveals that the existing adaptive security approaches widely cover the information gathering. However, comparative approaches do not describe how to decide on a method for performing adaptive security DSPL or how to provide knowledge input for adapting security. Therefore, these areas of research are promising.

Keywords

Dynamic Software Product Lines; DSPL; Security; Systematic Review; State of the Art

1. INTRODUCTION

For more than twenty years, companies have introduced product lines successfully to build cheaper and faster software with top quality. Several experiences have demonstrated the benefits of the adoption of a product line approach. Software product lines (SPL) have been used successfully in industry for building families of systems of related products, maximizing reuse, and exploiting their variable and configurable options. Software product line engineering (SPLE) practices offer desirable characteristics such as reduced time-to-market, rapid product development and more affordable development costs as a result of systematic representation of the variabilities of a domain of discourse that leads to methodical reuse of software assets. Giant companies reveal that the use of an approach to the SPL development can generate significant quantitative and qualitative improvements in productivity and customer satisfaction. This practice can also efficiently satisfy the current need for mass customization of software. Their growing success is due to their ability to offer companies ways to exploit their software products commonalities to achieve economies of production. The development lifecycle of a product line consists of two main phases: domain engineering, which deals with the understanding and formally modeling of the target domain; and application engineering that is concerned with the configuration of a product line into one concrete product based on the preferences and requirements of the stakeholders.

DSPL extend the concept of conventional SPL by enabling software-variant generation at runtime and produce software capable of adapting to such fluctuations. In contrast with traditional SPLs, DSPL bind variation points at runtime, when software is launched to adapt to the current environment, as well as during operation to adapt to changes in the environment.

Building a product line that dynamically adapts itself to changing requirements implies a deployment of the product configuration at runtime. It also means that the system requires monitoring capabilities for detecting changes in the environment. As a response to these changes, the system adapts by triggering a change in its configuration, providing context-relevant services or meeting quality requirements. Dynamic software reconfiguration is concerned with changing the application configuration at runtime after it has been deployed.

DOI:10.5121/ijcses.2016.7501

From the security point of view, dynamically changing DSPLs are a challenge, as static security mechanisms are not able to offer an optimal security level for the varying situations. Moreover, it is impossible at design-time to anticipate all situations in which a DSPL application will be utilized. These challenges cause a need for self-adaptive security, which is able to select security mechanisms and tune their parameters at runtime.

Currently, several security adaptation approaches exist. On the one hand, approaches concentrate on adapting a particular security mechanism or supporting a specific security attribute. On the other hand, some approaches are generic; that is, they support different attributes and mechanisms. Hence, it is difficult to select the most suitable adaptation approach for different usages. Moreover, it is difficult to know what research steps are needed in the future.

The objective of this paper is to give an overview of the state of the art in the adaptive security issues for a DSPL by doing a Systematic Literature Review (SLR) on simple and clear question in this regard. In particular, we identify and compare different security adaptation approaches for DSPL, and evaluate them in terms of how well they support critical security services and what level of adaptation they achieve.

In the section 2 we describe our method for conducting the review. Results are presented in Section 3. Section 4 answers our questions. Finally, the Conclusion and future work Section close the paper.

2. METHOD

The aim of this study is identifying and comparing different security adaptation approaches for DSPL. We used guidelines proposed by Barbara Kitchenham [1] for performing our study. The main steps are explained in the next parts of this section.

2.1. SYSTEMATIC LITERATURE REVIEWS (SLR)

Systematic Literature Reviews (SLR) is a rigorous method for assessing, reviewing and aggregating research results. Unlike an ordinary literature review consisting of an annotated bibliography, SLR analyzes existing literature with reference to specific research questions on a topic of interest. Furthermore, it can be considered as much more effort prone than an ordinary literature survey.

2.2. RESEARCH QUESTIONS

RQ1: What is the focus of research in adaptive security of DSPL?

RQ2: What are the claimed benefits of self-adaptive security in DSPL and what are the tradeoffs implied by self-adaptive?

RQ3: how can DSPLs autonomously evaluate changes and threats in their environment in order to adaptively reconfigure themselves?

RQ4: What are the limitations of the existing approaches, and interesting areas for future research?

Regarding to RQ1, We were looking for researches and case studies need to get insight in the research trends in adaptive security of DSPL, providing context for the study.

Regarding to RQ2, it was important for us to know the claims associated with adaptive security, the evidence that exists for these claims and the tradeoffs implied by this adaptive security.

Regarding to RQ3, we want to know how applications with stringent safety requirements require security mechanisms that reduce human intervention when DSPL features change.

The goal of RQ4 is to help deriving conclusions from the study.

2.3. Research Process

Our search process for review was based on online searching in famous online databases which are addressed as table1. Since these databases cover almost all major journals and conference proceedings, manually review of journal was not required. Review has been carried on by mean of search facilities in these databases and using appropriate logical expressions. In first stage, our focus was on title and abstract of articles found in search process and select appropriate and relevant studies. If there was any doubt, our decision was based on reviewing it at one glance.

Table 1. Studies Resource

Source	Address
Scopus	www.scopus.com
IEEE Xplore	ieeexplore.ieee.org
ACM Digital Library	Portal.acm.org
Springer Link	www.springerlink.com
Science Direct	www.sciencedirect.com

2.4. Inclusion and Exclusion Criteria

Our primary goal is to understand the claims and supporting evidence of adaptive security in DSPL, we excluded papers about theoretical aspects, as well as surveys and roadmap papers. We also excluded short papers of 1 or 2 pages.

There were some papers that were relevant to our study indirectly in our defined process. This will strengthen our review, because all relevant documents were included and our review covered sufficiently direct and indirect studies in this research.

All studies are assessed through a quality check, which is an inherent part of a thorough literature study. Checking the originality and quality of the studies is important for data synthesis and interpretation of results later on.

2.5. Quality Assessment

For assessing studies we defined the following questions:

QA1: Does study agree with existence of the focus of research in adaptive security for DSPL?
QA2: Does the security of DSPL recognise the need for adaptation?
QA3: Does study report any similar practices in the claimed benefits of adaptive security in DSPL and the tradeoffs implied by self-adaptive security?
QA4: Does study report show how to face securely unexpected risks and activate appropriate countermeasures to respond to new threats?
QA5: Is it possible to avoid specifying all the behaviours in advance for Autonomous and Adaptive Security?

We scored questions as bellow:
QA1. Y (Yes) study explicitly agrees with existence of any objectives; P (Partially) study implicitly agrees and N (No) study disagrees with existence of any objectives.

QA2. Y, study explicitly agrees with existence of any needs; P, study implicitly agrees and N, there is no need for adaptation.

QA3. Y, the authors address one or more similar practices; P, some of the ones practices could be tailored and customized in the second and N, there is no similar and adaptable practices in them.

QA4. Y, the authors report provide sufficient arguments; P, so not enough and N, there is no argument.

QA5. Y, study addresses possibility to avoid specifying all the behaviours in advance for Autonomous and Adaptive Security; P, study partly agrees (or implicitly) and N, there is no possibility.

We defined Y=1, P=0.5 and N=0 or Unknown where information is not clearly specified. All authors assessed every article and if there is no agreement in scoring, we discussed enough to reach agreement.

We defined Y=1, P=0.5 and N=0 or Unknown where information is not clearly specified. All authors assessed every article and if there is no agreement in scoring, we discussed enough to reach agreement.

2.6. DATA COLLECTION

These data were extracted from each article:

- The full source and references
- The author(s) information and details
- Research issues
- Main ideas

All articles were reviewed and data was extracted and checked. This idea was chosen for better consistency in reviewing all papers and improving quality of review.

2.7. DATA ANALYSIS

Our collect data was organized to address:

-Whether study agrees with existence of the objectives of adaptive security for DSPL or not? (Addressing RQ1)

-Whether study agrees with existence of any needs for adaptation or no? (Addressing RQ1, RQ2)

-Whether study mentions similar practice/concept in either methods or no? (Addressing RQ3)

-Whether study provides sufficient arguments to face securely unexpected risks and activate appropriate countermeasures or no? (Addressing RQ2 and RQ4)

-Whether study agrees with existence of possibility to avoid specifying all the behaviours in advance for Autonomous and Adaptive Security or not? (Addressing QR5)

-Whether authors believe that this area is promising or no? (Addressing QR5)

3. RESULTS

In this section we explain results of our review.

3.1. SEARCH RESULTS

Table 2 shows the results of our selection procedure. In this table, results of searching in all databases are provided, but, some of the studies were repeated in more than one online database, so, final number of unique studies selected for our review was distinguished after elimination of repeated articles. Final selected studies are listed in table 3.

3.2. QUALITY EVALUATION OF STUDIES

During this phase, we found that some of the selected articles discussing security in general or only the SPL, but, they do not provide any valuable information to our research, so, we decided to delete them from scope of our study. Assessment of each study was done by means of criteria explained in section 2.4 and the scores for each of them are shown in table 4.

3.3. QUALITY FACTORS

For assessing results of our quality questions, we use average of total scores. This average is useful for some questions, but it is not useful for some other. For instance, we cannot answer the question about possibility of integration with average of scores because of the nature of the question; instead, we use negative ideas for rejecting possibility.

Table 2. Results of Study Selection Procedure

Source	Search Results	Selected Studies
Scopus	91	7
IEEE Xplore	85	10
ACM Digital Library	22	5
Springer Link	36	7
Science Direct	04	1
Total	**238**	**30**
Repeated articles		12
Finally selected articles		**18**

Table 3. Selected Studies For Conducting Review

ID	Title	Authors	Main Topic	Year
S1	Strategies for Variability Transformation at Run-time	O. Haugen and al. [2]	the security of DSPL recognises the need for adaptation	2009
S2	Self-Adaptive Software: Landscape and Research Challenges	M. Salehie and al. [3]	Self-protecting is the capability of recovering from their effects and detecting security breaches	2009
S3	Security Requirements Engineering Framework for Software Product Lines	D. Mellado and al. [4]	To describe a security requirements engineering in order to facilitate the development of secure SPLs	2010
S4	A Security Requirements Engineering Tool For Domain Engineering In SPL	J. Rodríguez and al. [5]	how to provide automated support through which to facilitate the application of the security quality requirements engineering process for SPL	2011
S5	Claims and Supporting Evidence for Self-Adaptive Systems: A Literature Study	D. Weyns and al. [6]	Claims versus the tradeoffs of adaptive security	2012
S6	Non-functional Properties in Software Product Lines - taxonomy for classification	M. Noorian [7]	The adaptive security attribute should be measured at runtime.	2012
S7	Automated Planning for Feature Model Configuration based on	S. Soltani and al. [8]	Adaptive security is a non-functional requirements in	2012

	functional and non-functional requirements		DSPL	
S8	A Systematic Review of Model-Driven Security	H. Nguyen [9]	How to improve the productivity of the development process and quality of the resulting secure systems	2013
S9	Runtime Monitoring and Auditing of self-adaptive systems	D. H. Carmo and al. [10]	How to avoid specifying all the behaviours in advance for Autonomous and Adaptive Security	2013
S10	Comparison of Adaptive Information Security Approaches	A. Evesti and al. [11]	Limitations and prospects of adaptive security	2013
S11	Architecture and Knowledge-Driven Self-Adaptive Security in smart space	A. Evesti and al. [12]	Self-adaptive security as an applicable solution to anticipate all the possible changes at design-time.	2013
S12	An overview of Dynamic Software Product Line architectures and techniques	R. Capilla and al. [13]	Challenges and solutions are necessary to support runtime variability and adaptive security mechanisms in DSPL models and software architectures.	2014
S13	A Systematic Survey of Self-Protecting Software Systems	E. Yuan and al. [14]	autonomic systems capable of detecting and mitigating security threats at runtime	2014
S14	Policy -Based Language for Autonomous and Adaptive Security	F. Cuppens [15]	how to simultaneously address both adaptive and autonomy in DSPL	2014
S15	Dynamic Reconfiguration of Security Policies in Wireless Sensor Networks	Mónica Pinto and al. [16]	self-protection solution based on the combination of dynamic adaptation and reconfiguration of security	2015
S16	Representing and Configuring Security Variability in Software Product Lines	V. Myllärniemi [17]	Security variability can be represented and distinguished as countermeasures	2015
S17	Security Systems Engineering Approach in Evaluating Commercial and Open Source Software Products	Jesus Abelarde [18]	The amount of security resources and time necessary to accommodate proper security evaluations is underestimated.	2016
S18	**TRUSTWORTHY VARIANT DERIVATION WITH TRANSLATION VALIDATION FOR SAFETY CRITICAL PRODUCT LINES**	J. Almendros-Jiménez and al. [19]	Propose a general technique of checking correctness through translation validation to automatically verify runs of a variant derivation tool.	2016

Table 4. Quality Evaluation

Source	QA1	QA2	QA3	QA4	QA5
1	Y	P	N	Y	Y
2	Y	Y	P	Y	Y
3	P	Y	Y	P	Y
4	P	Y	P	Y	P
5	P	Y	Y	P	Y
6	Y	Y	Y	Y	Y
7	N	P	P	Y	Y
8	P	Y	Y	N	Y
9	Y	P	P	Y	Y
10	P	N	P	Y	P
11	N	P	P	Y	P
12	P	Y	N	Y	P
13	N	P	P	Y	Y
14	P	N	Y	Y	Y
15	P	Y	N	P	Y
16	N	P	Y	Y	P
17	Y	Y	P	P	Y
18	Y	Y	Y	Y	P
Average	**0,58**	**0,72**	**0,61**	**0,83**	**0,83**

4. Discussion

In this part, the answers to our study questions will be discussed.

4.1. What is the Focus of Research in Adaptive Security of DSPL?

Most of the articles agree that there are the objectives of research in adaptive security for DSPL. By reviewing them, it seems that this research focus is derived from the following concerns: category of the study, subject, concrete focus and application domain. Overall, fifty eight percent of the studies focus on one or more activities of adaptive security (monitoring, analyzing, planning, execution), runtime models, multiple control loops and on reflection [10]- [19].

More than two thirds of the articles agree that the security of DSPL recognise the need for adaptation in order to achieve the required security level. On the one hand, a survey by D. Weyns et al. [6] reveals that the existing security approaches DSPL are not generic, but rather approaches focus on specific security objectives. Furthermore, a study of Yuan et al. [14] compares over 30 self-protection approaches and shows that most existing approaches focus on the part of the adaptive control loop, instead of covering the entire adaptation loop. In the adaptive security approaches, such as: Self-Adaptive Security in smart space [12], Self-Adaptive Software [3], Strategies for Variability Transformation at Run-time [2], A Security Requirements Engineering Tool For Domain Engineering In SPL [5] and Runtime Monitoring and Auditing of self-adaptive systems [10], Architectural Approach for Self-managing Security Services in [17]- [18], authors notice that any of these approaches support all security objectives but concentrate on specific and pre-selected objectives

4.2. What are the Claimed Benefits of Self-Adaptive Security in DSPL and what are the Tradeoffs Implied by Self-Adaptive?

Eight studies examine the claims versus the tradeoffs of adaptive security and clearly demonstrate that the researches mainly report on claimed benefits, while little attention is given to the implications of adaptive security. It is remarkable that the efficiency/performance ratio is almost the only quality attribute with a negative effect due to the adaptive security [11]. We also evaluated the type of claims that have been made to the quality attributes and found that the dominant demand is improving quality attributes of the software. The main reported tradeoff implied by the adaptive security is the top performance [6]-[18].

4.3. How can DSPLs Autonomously Evaluate Changes and Threats in their Environment to Adaptively Reconfigure Themselves?

Most of the articles agree that it is possible to have an autonomous and adaptive security in DSPL [10]-[15]-[19]. Mónica Pinto and al. [16] present an approach to building adaptive security at runtime. They extend SPLs by adding the ability to automatically derive changed configurations by monitoring the context, and to automatically reconfigure the security application while it is running. The adaptation platform of this approach provides a conceptual model and reference architecture for adaptive system. A. Evesti and al. [12] address SPL that allow mobile devices in smart space to download software configurations on-demand. When a device enters a particular context, the application provider service must deduce and create a variant for the device. As devices enter a context, their unique capabilities must be discovered and dealt with efficiently and correctly. D. H. Carmo and al. [10] present a new approach where they meet challenges in adaptive security construction and execution by combining certain aspect oriented and model driven techniques in order to deal with complexity through abstractions used both to specify the dynamic variability at design time and to manage run time adaptations.

4.4. What are the Limitations of the Existing Approaches and Interesting Areas for Future Research?

The issue of security in SPL is long, but most solutions are based on the assumption that the SPL is a closed environment. Given current trends, where the SPL is dynamic and open system, these solutions are not sufficient to ensure the adaptive security [4]. Although there are researchers working in this field and solutions are provided to be better, but the mechanism of adaptive security for DSPL is not yet mature. In addition, the existing security solutions are based on the features of the current DSPL; since DSPL reveals more and more new features that may be supported in the future; the adaptive security mechanism has to be modernized and new security issues have to be identified [1]-[9]-[11].

The majority of articles are optimistic about the potential prospects of this promising area. The research should focus on the following areas: -1- Policy, model and design of the security architecture -2- Securing the management and sharing of knowledge...etc.

5. Conclusion and Future Work

The objective of this literature study was to summarize existing research on engineering self-adaptive software systems and shed light on the claimed benefits and provided evidence of adaptive security in DSPL. The study shows that the existing adaptive security approaches widely cover the information gathering. However, comparative approaches do not describe how to decide on a method for performing adaptive security DSPL or how to provide knowledge input for adapting security. Therefore, these areas of research are promising.

Future research is still necessary to provide more efficient mechanisms able to manage the dynamic and adaptive characteristics of security in DSPL and also to determine how security can be deployed and redeployed automatically using variability mechanisms and multiple binding times, reducing human intervention and effort required by engineering operations when certain system features change. As an emerging topic, we expect that promising new research will bring better and integrated a self-adaptive security solution for Mobile Devices based on the combination of the MAPE- K reference model and DSPL approach.

REFERENCES

[1] B. Kitchenham, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey and Stephen Linkman," Systematic literature reviews in software engineering- A Systematic literature reviews", Keele University 2008

[2] O. Haugen C. Cetina, X. Zhang, F. Fleurey, V. Pelechano : '' Strategies for variability transformation at run-time'', SPLC '09 Proceedings of the 13th International Software Product Line Conference, Pages 61-70, Carnegie Mellon University Pittsburgh, PA, USA, 2009

[3] M. Salehie and L. Tahvildari, "Self-adaptive software: Landscape and research challenges," ACM TAAS, vol. 4, 2009.

[4] D. Mellado, E. Fernández-Medina, M. Piattini: '' Security Requirements Engineering Framework for Software Product Lines'', Information and Software Technology, 2010. Volume 52: p. 1094-1117. Oct. 2010

[5] Jesús Rodríguez, Eduardo Fernández-Medina, Mario Piattini, Daniel Mellado:'' A Security Requirements Engineering Tool for Domain Engineering in Software Product Lines '', part of the ESFINGE Project of the Ministry of Science and Innovation (Spain), 2011

[6] D. Weyns1, M. Usman Iftikhar, Sam Malek, J. Andersson, '' Claims and Supporting Evidence for Self-Adaptive Systems: A Literature Study'', 2012 ICSE Workshop on SEAMS, Zurich, pp.89-98, 4-5 June 2012.

[7] M. Noorian, E. Bagheri, W. Du:'' Non-functional Properties in Software Product Lines: A Taxonomy for Classification'', In Proceedings of "SEKE'12", Peges 663-667, 2012

[8] S. Soltani, M. Asadi, D. Gasevic, M. Hatala, E. Bagheri :'' Automated planning for feature model configuration based on functional and non-functional requirements'', SPLC '12 Proceedings of the 16th International Software Product Line Conference - Volume 1 Pages 56-65 ACM New York, NY, USA, 2012

[9] Phu H. Nguyen:'' A Systematic Review of Model-Driven Security'', Software Engineering Conference (APSEC, 2013 20th Asia-Pacific (Volume: 1) , IEEE, Univ. of Luxembourg, Dec. 2013

[10] D. H. Carmo, Sergio T. Carvalho, Leonardo G. P. Murta, Orlando Loques, '' Runtime Monitoring and Auditing of Self-Adaptive Systems'',8th IEEE International Conference on Global Software Engineering (ICGSE), Brazil 2013.

[11] A. Evesti; E. Ovaska, '' Comparison of Adaptive Information Security Approaches'', ISRN Artificial Intelligence, Article ID 482949, 18 pages. Volume 2013.

[12] A. Evesti. '' Adaptive security in smart spaces''. PhD's thesis, University of Oulu, on the 31st of January 2014.

[13] Capilla, R., et al., ''An overview of Dynamic Software Product Line architectures and techniques: Observations from research and industry''. J. Syst. Software, 2014,

[14] E. Yuan, N. Esfahani, S. Malek:'' A Systematic Survey of Self-Protecting Software Systems'', ACM Transactions on Autonomous and Adaptive Systems (TAAS), Volume 8 Issue 4, New York, NY, USA . 2014.

[15] F. Cuppens:'' Policy -Based Language for Autonomous and Adaptive Security'', the Concordia Institute for Information Systems Engineering, Canada, Jan. 2014

[16] Mónica Pinto and al.,'' Dynamic Reconfiguration of Security Policies in Wireless Sensor Networks'', Sensors 2015, 15, 5251-5280; doi:10.3390/s150305251, 2015

[17] Varvana Myllärniemi : ''Representing and Configuring Security Variability in Software Product Lines'', Proceedings of the 11th International ACM SIGSOFT Conference on Quality of Software Architectures, pp: 1-10, ACM New York, NY, USA, 2015

[18] Jesus Abelarde, '' Security Systems Engineering Approach in Evaluating Commercial and Open Source Software Products'', SANS Institute InfoSec Reading Room, January 25, 2016

[19] Jesús M. Almendros-Jiménez, Luis Iribarne, Jesús López-Fernández, Ángel Mora-Segura, '' Trustworthy variant derivation with translation validation for safety critical product lines'', Journal of Logical and Algebraic Methods in Programming, Vol. 85, Issue 2, February 2016