A Metamodel for Security and Privacy Knowledge in Cloud Services

Hironori Washizaki Sota Fukumoto Misato Yamamoto
Masatoshi Yoshizawa Yoshiaki Fukazawa
Waseda University, Tokyo, Japan
washizaki@waseda.jp

Shinpei Ogata
Shinshu University, Japan

Eduardo B. Fernandez
Florida Atlantic University, USA

Nobukazu Yoshioka
National Institute of Informatics, Japan

Takehisa Kato
Toshiba Corporation, Japan
Haruhiko Kaiya
Kanagawa University, Japan

Hideyuki Kanuka Yuki Kondo
Hitachi, Ltd., Japan

Takao Okubo
Institute of Information Security, Japan

Atsuo Hazeyama
Tokyo Gakugei University, Japan

Abstract— It is important to ensure security and privacy in cloud services. Although there are many security and privacy patterns and much non-pattern-based knowledge such as practices and principles in cloud services, it is difficult to select and combine the right ones due to the large number of those items and the nature of the layered cloud stack. In this paper, we propose a metamodel for handling security and privacy in cloud service development and operation. The metamodel is expected to be utilized for building a knowledge base to accumulate, classify and reuse existing cloud security and privacy patterns and practices in a consistent and uniform way. Moreover the metamodel and knowledge base are expected to be utilized for designing and maintaining architectures for cloud service systems incorporating security and privacy.

Keywords— cloud computing; security patterns; privacy patterns; knowledge base; software and system architecture

I. INTRODUCTION

It is particularly important to ensure security and privacy in cloud services since service providers centrally control services and data while these are remotely available and often connected with other services [1]. However, since not all software engineers are experts on security and privacy (S&P) [2], it is difficult to incorporate a variety of S&P concerns at various software lifecycle stages.

A pattern is the abstraction from a concrete form which keeps recurring in specific non-arbitrary contexts, and pattern catalogs (and pattern languages as well) are expected to be a mean to coherently integrate and present their relevant background, leitmotif, and metaphors [3]. In the area of cloud computing and services, many security and privacy patterns have been published, such as [4-8]. Moreover there is much non-pattern-based knowledge in the form of practices and principles documented to address security and privacy issues in cloud services.

The large number of S&P patterns and documents describing related knowledge in cloud services makes the selection (and combination) of the right ones a difficult task. This problem is common to security patterns in general [2,9,10], but it is much more severe in cloud services mainly due to the following two reasons. Firstly, cloud services and underlying mechanisms are related to various layers in the layered stack of cloud [11] and often integrated over different layers [1]. Secondly, cloud computing systems involve a variety of devices connected to them, which may require different deployment models, and provide a variety of services, all of which result in a highly complex system [12]; leading to many concerns including S&P.

Metamodels or reference architectures that capture essential concepts related to S&P in the layered stack of cloud are expected to address the above-mentioned problem since engineers can describe security and privacy-related knowledge and design system and service using the knowledge in consistent way over different layers. There are several metamodels [12,13] and abstract reference architectures [14] for addressing cloud security; however none of these addresses privacy in cloud services. Since it is known that the relation between security and privacy is complex [15], it is preferable to deal with both S&P together. On the other hand, there are several metamodels and conceptual models dealing with both of S&P [16,17]; however, these are generally defined so that it is hard to apply them to cloud services directly.

Thus, we propose a metamodel for addressing S&P in cloud services by integrating and extending existing cloud security metamodels together with newly added concepts. Figure 1 shows how the metamodel would be used in cloud services development and maintenance. Our metamodel provides a basis for describing and accumulating security and privacy-related knowledge over different layers so that it becomes much easier to select and combine the right patterns and related knowledge for addressing S&P issues in cloud services. Moreover, engineers and developers could refer to the metamodel for designing high-level architectures of cloud service systems in efficient and effective manner. To confirm the usefulness and feasibility of the metamodel, we conducted a case study that describes a cloud security pattern based on the metamodel.

The remainder of this paper is organized as follows. First, we propose our metamodel in Section II. In Section III, we describe the case study of pattern description. Finally, we conclude our work and discuss future work in Section IV.

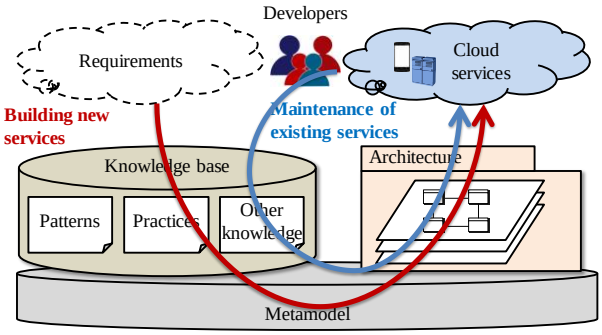

Fig. 1. Metamodel and cloud services

II. METAMODEL

Based on the preliminaries described in Section I, we identified the following three requirements for designing the metamodel:

- R1. The metamodel has to deal consistently with security and privacy-related knowledge over different layers including the software application layer, the platform layer and the infrastructure layer. Services corresponding to these layers are SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service). From the user's point of view, each service is provided at a certain layer; however, the data controlled by the service may be related to any layer [11]. Moreover, cloud services are often integrated over different layers so that careful consideration of security over different layers is important [18]. This is also important for privacy as well.
- R2. The metamodel has to be mostly consistent with existing cloud security metamodels and reference architectures so that engineers and developers can utilize assets based on our metamodel and those based on existing metamodels (and reference architectures).
- R3. The metamodel allows engineers and developers convenient access to a knowledge base containing cloud-specific and cloud-independent knowledge. For example there are many S&P patterns that are not specific to cloud services [19,20]; these could be applicable to or support cloud service development.

We designed the metamodel (shown in Figure 2) to consist of four packages while satisfying the above-mentioned requirements: (a) core, (b) software, (c) platform and (d) infrastructure. By separating general concepts from those specific to a certain layer, it is intended to make easier access to cloud-specific and cloud independent knowledge (R3).

We explain below some details of each package.

(a) The core package captures concepts common to all layers, and organizes relationships among them. Figure 2 shows it in the form of a UML class diagram. Having this package as a foundation for all layers obtains consistent handling of security and privacy-related knowledge over different layers (R1). Moreover it incorporates the most of concepts with relationships defined in existing metamodels [12][13], so that the entire metamodel is mostly consistent with existing metamodels (R2).

(b) The software package defines concepts specific to the software application layer. For example, the coding rules are included in this package since it is basically handled in application implementations.

(c) The platform package defines concepts specific to the platform layer, such as the virtual environment.

(d) The infrastructure package defines concepts specific to the infrastructure layer, such as the virtual machine and the hardware.

III. CASE STUDY: MODELING SECURITY PATTERNS

To confirm usefulness and feasibility of the metamodel, we described a misuse pattern "Resource Usage Monitoring Inference in Cloud Computing"[4]. This misuse pattern describes how attackers obtain some information on a victim's resource usage such as estimating traffic rates or detecting cache activity spikes.

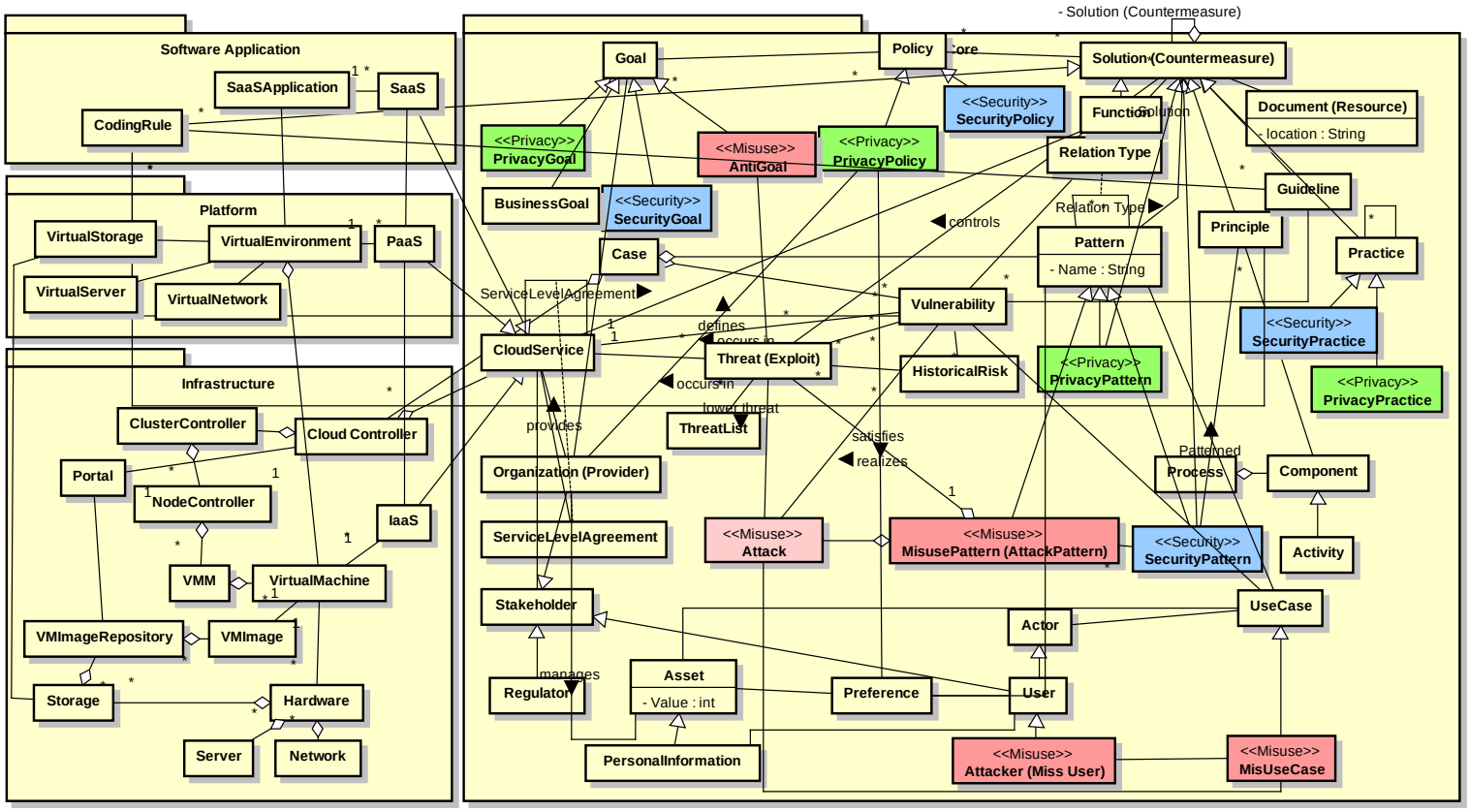

Fig. 2. Metamodel for security and privacy in cloud services

Figure 3 shows the structure of the pattern as an instance of the metamodel; it shows how threats using vulnerability associated with cloud service elements are realized as actual attacks. Figure 4 shows the dynamics of the misuse; it shows how an attacker monitors the resource usage. Figure 5 shows the corresponding structure after applying countermeasures of the pattern; it shows that control accesses as counter measures could protect the service from the misuse. In these figures, we confirmed that the necessary elements involved in the pattern and their relationships can be clearly modeled by instantiating the metamodel. Developers and engineers are expected to easily recognize when and how to avoid the misuse.

IV. Conclusion and Future Work

We proposed a metamodel for addressing security and privacy in cloud services and its simple case study. We have a plan to conduct more complex case studies such as integration of multiple S&P patterns, designing cloud service architectures based on the metamodel, and implementing them; these cases will be comprehensive and consistent ones covering from requirements to implementations.

ACKNOWLEDGEMENT

This work was supported by IISF SSR Forum 2015. This work was also partially supported by JSPS KAKENHI Grants Number 25330091 and 15H02686.

REFERENCES

[1] R. F. El-Gazzar, “A Literature Review on Cloud Computing Adoption Issues in Enterprises,” IFIP Advances in Information and Communication Technology, Volume 429, 2014, pp 214-242.

[2] N. Yoshioka, H. Washizaki and K. Maruyama, “A Survey on Security Patterns,” Progress in Informatics, No.5, pp.35-47, 2008.

[3] D. Riehle and H. Zullighoven, “Understanding and Using Patterns in Software Development," Theory and Practice of Object Systems, Vol.2, No.1, pp.3-13, 1996.

[4] K. Hashizume, N. Yoshioka and E.B. Fernandez, “Misuse Patterns for Cloud Computing,” 2nd Asian Conference on Pattern Languages of Programs (AsianPLoP’11) , 2011.

[5] K. Hashizume, N. Yoshioka and E.B. Fernandez, “Three Misuse Patterns for Cloud Computing,” in “Security Engineering for Cloud Computing: Approaches and Tools,” IGI Global, 2013.

[6] T. Reimer, P. Abraham and Q. Tan, Federated Identity Access Broker Pattern for Cloud Computing, 16th International Conference on Network-Based Information Systems (NBiS), 2013.

[7] E.B. Fernandez, N. Yoshioka, H. Washizaki, Patterns for Security and Privacy in Cloud Ecosystems, 2nd International Workshop on Evolving Security and Privacy Requirements Engineering (ESPRE 2015), 2015.

[8] E.B. Fernandez, N. Yoshioka and H. Washizaki, “Cloud Access Security Broker (CASB),” 4th Asian Conference on Pattern Languages of Programs (AsianPLoP 2015), 2015.

[9] K. Supapporn, N. Prompoon and T. Rojkangsadan, “An approach: Constructing the grammar from security pattern,” 4th International Joint Conference on Computer Science and Sofware Engineering (JCSSE2007), 2007.

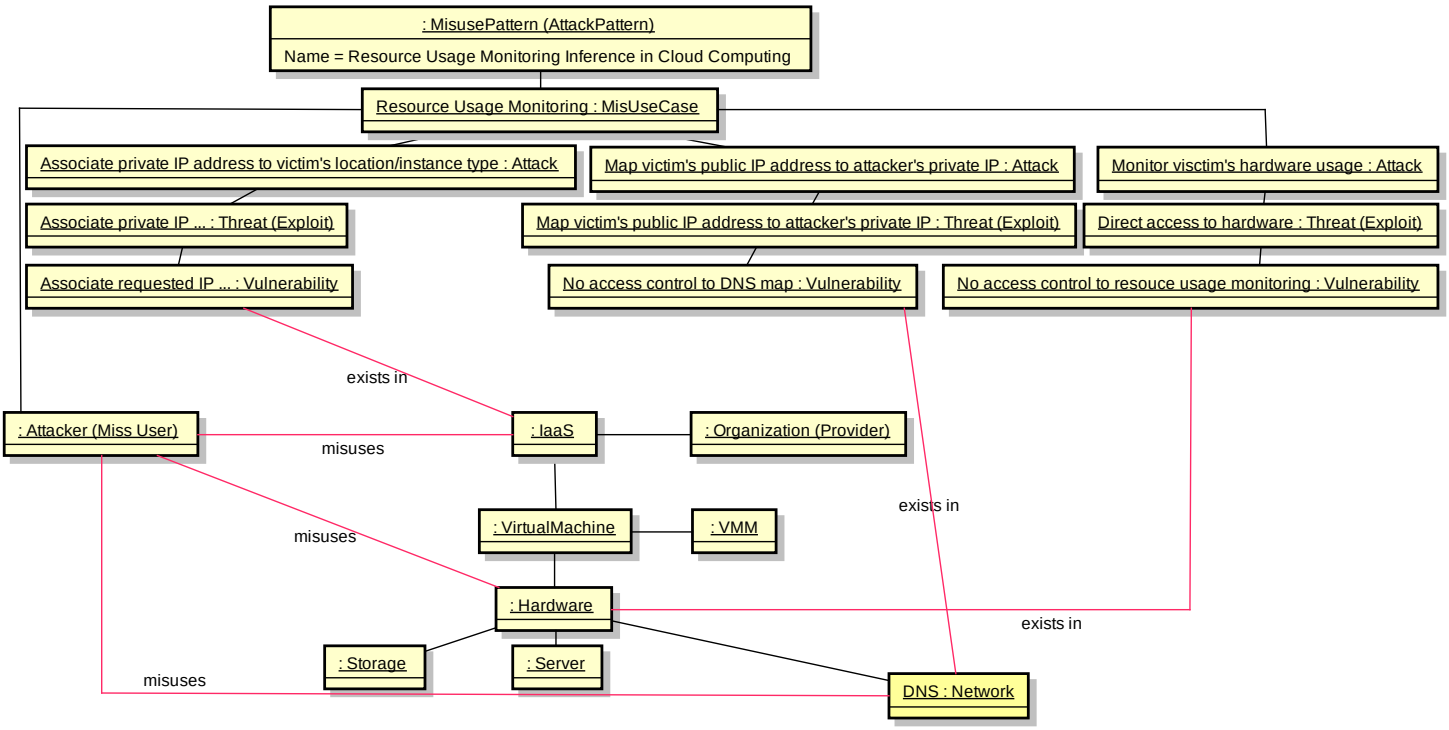

Fig. 3. Structure of resource usage monitoring inference in cloud computing

[10] K. Yskout, R. Scandariato and W. Joosen, "Do security patterns really help designers?," International Conference on Software Engineering (ICSE), 2015.

[11] S. Subashini, , V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, Vol.34, No.1, pp.1–11, 2011.

[12] E. B. Fernandez, et al, "Building a security reference architecture for cloud systems," Requirements Engineering Journal, Jan. 2015.

[13] A. Hazeyama, "Survey on Body of Knowledge Regarding Software Security," 13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD 2012), 2012.

[14] NIST Cloud Computing Security WG, "Cloud computing security reference architecture," 2013

[15] V. Katos and A. Patel, "A partial equilibrium view on security and privacy," Information Management & Computer Security, Vol.16, No.1, pp.74-83, 2008.

[16] C. Kalloniatis, E. Kavakli, S. Gritzalis, "Addressing privacy requirements in system design: the pris method," Requirements Engineering, Vol.13, No.3, pp.241–255, 2008.

[17] R. Tesoriero, et al. "Model-Driven Privacy and Security in Multi-modal Social Media Uis," International Workshops MSM 2011.

[18] A.A. Almutairi, M.I. Sarfraz, S. Basalamah, W.G. Aref, A. Ghafoor, "A Distributed Access Control Architecture for Cloud Computing," IEEE Software, Vol. 29, No. 2, pp.36-44, 2012.

[19] E. B. Fernandez, N. Yoshioka, H. Washizaki, et al., "Using security patterns to develop secure systems", in "Software Engineering for Secure Systems", IGI Global, pp16-31, 2010

[20] L.L. Lobato, E.B. Fernandez and S.D. Zorzo, "Patterns to support the development of privacy policies", International Conference on Availability, Reliability and Security (ARES'09), 2009.

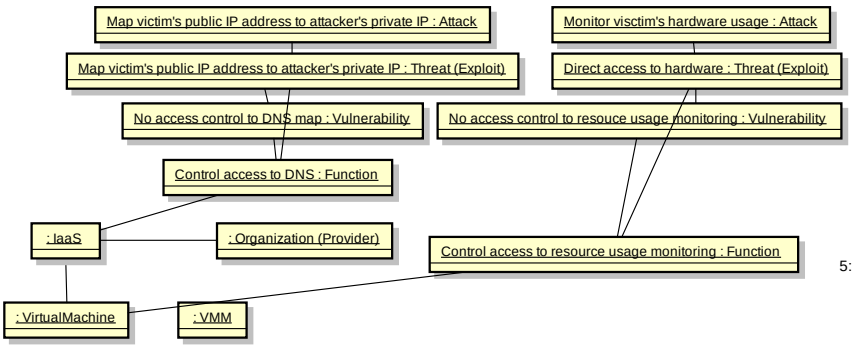

Fig. 5. Structure after applying countermeasures (excerpt.)

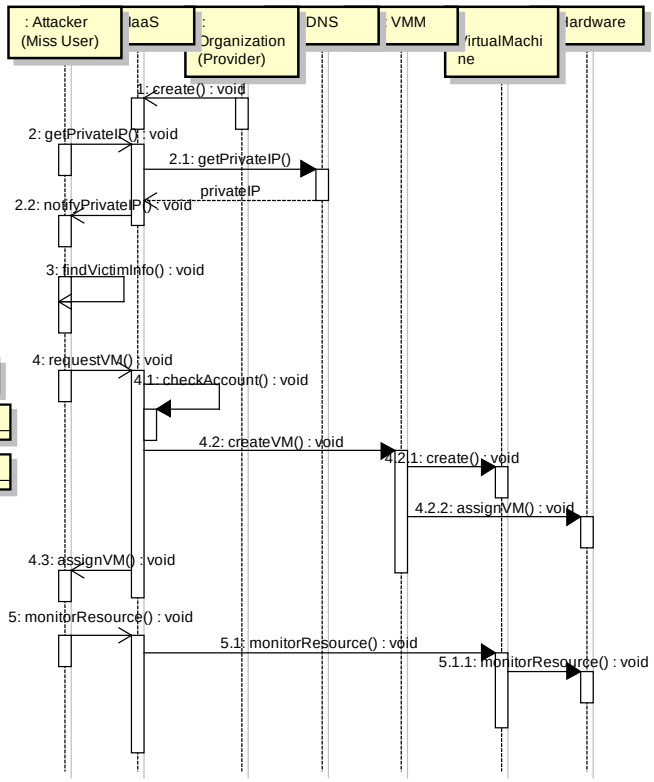

Fig. 4. Dynamics of the misuse adopted from [4] with modifications