Summary of WESPr-18: The International Workshop on Evidence-based Security and Privacy in the Wild

Hironori Washizaki
Waseda Univeristy / National Institute of Informatics / SYSTEM INFORMATION / eXmotion
Tokyo, Japan
washizaki@waseda.jp

Nobukazu Yoshioka
National Institute of Informatics
Tokyo, Japan
nobukazu@nii.ac.jp

Eduardo B. Fernandez
Florida Atlantic University
Boca Raton, USA
fernande@fau.edu

Tomoko Kaneko
Information-technology Promotion Agency
Tokyo, Japan
t-kaneko@ipa.go.jp

Shuichiro Yamamoto
Nagoya University
Nagoya, Japan
yamamotosui@icts.nagoya-u.ac.jp

***Abstract*—This paper summarizes the objectives and results of the WESPr-18: The International Workshop on Evidence-based Security and Privacy in the Wild held on December 4th in Nara, Japan. The workshop was collocated with APSEC 2018.**

Keywords—security and privacy, IoT systems, cloud computing, AI and machine learning systems, patterns

I. Introduction

Smart and ubiquitous software systems manages everything in our lives. In such complex software-intensive systems, software engineering is required to face wild challenges rather than tame problems especially in terms of security and privacy in a dependable way since there are many difficulties on these aspects for complex systems in an uncertain world.

In 2016, we addressed a part of these difficulties by holding the 1st International Workshop for Models and Modelling on Security and Privacy (WM2SP-16) collocated with ER 2016 [1]. By extending the scope to evidence-based security and privacy in complex systems, we held the International Workshop on Evidence-based Security and Privacy in the Wild (WESPr-18) on December 4th in Nara, Japan collocated with APSEC 2018 [2]. There were around 12 participants including the authors of this paper as workshop organizers.

In this paper, we summarize the objective and result of the WESPr-18.

II. Objective

Cloud Computing has led to a global shift in the computing world and the paradigm itself is evolving as new functions or technologies become available. Intelligent and interactive environments like Internet of Things (IoT) have found application in various domains. Billions of smart devices are connected to the internet and are producing huge amounts of data, increasing both complexity and uncertainty of humans, physical objects and machine-learning modules, especially on security and privacy, which we must manage. We need to tackle such difficulties on security and privacy for complex systems in an uncertain world in a dependable way, such as models of evidence-based reasoning, argumentation, traceability or/and big data. Security evidences make a system trusted and dependable in a big data era.

This workshop aimed to bring together researchers and practitioners in the areas of evidence-based modelling, security patterns, reasoning, argumentation, traceability, forensics in big data for secure and privacy-aware software development for complex and uncertain systems, to exchange ideas and preliminary results. Especially, we wanted to discuss how to utilize security evidence in security engineering.

The objective of the workshop reveals (1) important problems to be tackled for Security and Privacy on Complex and Uncertain Systems and (2) research challenges through presentations and discussion. The topics included security and privacy models, pattern-based security and privacy modelling, knowledge base for security, reasoning, argumentation, traceability, and forensics in big data and/or privacy-aware software development, security and privacy modelling and reasoning tools, and experiences for secure and/or privacy-aware software development.

III. Program

A. *Technical Papers*

There were six paper submissions by the due date. The program committee conducted a rigorous peer review by assigning at least two reviewers to each submission. The workshop organizers finally selected the following four papers for presentation and inclusion into the proceedings.

- "Using a variety of patterns in a secure software development methodology" by Eduardo B. Fernandez and Nobukazu Yoshioka
- "An Assurance Case Approach for Software Code Security" by Ryota Miyabayashi, Noritoshi Atsumi, Shuji Morisaki and Shuichiro Yamamoto

- "Restructuring Attack Trees to Identify Incorrect or Missing Relationships between Nodes" by Cai Hua, Hironori Washizaki, Yoshiaki Fukazawa, Takao Okubo, Kaiya Haruhiko and Yoshioka Nobukazu,
- "Threat analysis using STRIDE with STAMP/STPA" by Tomoko Kaneko, Yuji Takahashi, Takao Okubo and Ryoichii Sasaki

B. *Invited talk and minitutorial*

In addition to the technical paper presentations, the workshop had the following two invited talks and one mini-tutorial.

- Invited talk: "Safety and Security Co-engineering – A new emerging discipline for safe and secure system development" by Kenji Taguchi
- Invited talk: "Developing Secure and Privacy-Preserving Applications" by Emiliano Tramontana
- Mini-tutorial: "Evaluating the degree of security of a system built using security patterns" by Eduardo B. Fernandez

IV. Discusssion Results

The workshop organizers and participants had open discussions to dig deeper into the topics addressed by the paper presentations and talks.

During the discussion, we confirmed the necessity of clarification of difficulties and research directions for security and privacy in complex systems such as IoT, AI and Blockchain-based systems. For example, we need to address the nature of IoT ecosystem such as diversity and dynamic heterogeneous configuration of devices. In relation to that, we also need to address the nature of attacks for Cyber-Physical Systems (CPSs) such as physical attacks and information ones. Although some papers in the workshop employed STRIDE [3, 4] as a threat model for clarifying threats in complex systems, we discussed a possibility of extension of STRIDE for IoT and CPS.

In addition to threat models, we also discussed the necessity of having and classifying security and misuse patterns for IoT and CPS. For such purpose, reference architectures and frameworks for IoT such as [5, 6] may be needed as foundations.

We discussed that it is also important to consider people, organizational and operational aspects such as the operation phase and the concept of operation for IoT and CPS in terms of security and privacy concerns.

V. Conclusions and Future Prospective

The workshop was successful to start research and discussion on security and privacy in complex systems including IoT and AI-based systems. Figure 1 shows the group photo taken when closing the workshop (it does not include all the participants).

We considered further editions of the workshop. Possible venues include AsianPLoP 2019 [7], SISA 2019 [8] as a part of COMPSAC 2019, and APSEC 2019 [9].

Figure 1. WESPr-18 group photo

References

[1] Takao Okubo, Atsuo Hazeyama and Eduardo B. Fernandez, "Models and Modelling on Security and Privacy – The 1st International Workshop for Models and Modelling on Security and Privacy (WM2SP-16) ," in "Advances in Conceptual Modeling – ER 2016 Workshops," edited bySebastian Link and Juan C. Trujillo, LNCS, Vol. 9975, p. 229, 2006.

[2] Katsuhisa Maruyama, Naoyasu Ubayashi, Hironori Washizaki and Hongyu Zhang, "Proceedings of the 25th Asia-Pacific Software Engineering Conference (APSEC 2018)," IEEE Computer Society, 2018.

[3] Microsoft, "The STRIDE Threat Model", 2002, https://msdn.microsoft.com/enus/library/ee823878(v=cs.20).aspx

[4] Bruce Potter, "Microsoft SDL Threat Modelling Tool," Network Security, Vol. 2009, No. 1, pp. 15-18, 2009.

[5] Microsoft, "Microsoft Azure IoT Reference Architecture Version 2.1," 2018, https://aka.ms/iotrefarchitecture

[6] Mohab Aly, Foutse Khomh, Yann-Gaël Guéhéneuc, Hironori Washizaki, and Soumaya Yacout, "Is Fragmentation a Threat to the Success of the Internet of Things?," IEEE Internet of Things Journal, Early Access, 2018.

[7] AsianPLoP 2019: 8th Asian Conference on Pattern Languages of Programs, http://asianplop.org

[8] IEEE International Symposium on Smart IoT Systems and Applications (SISA 2019), https://ieeecompsac.computer.org/2019/iot/

[9] Asia-Pacific Software Engineering Conference, http://www.apsec-conferences.org/