7ZF-07 Systematic Building of E-Learning Contents for Secure IoT

Yiyi Wang* Alaa Allakany** Srishti Kulshrestha*** Wei Shi****Koji Okamura***** and Ranjan Bose******

* Department of Information Science, Kyushu University, Japan

** Cybersecurity Center, Kyushu University, Jaapan.

*** School of Information Technology, IIT Delhi, India.

****Innovation Center for Educational Resources (ICER), Kyushu University

*****Research Institute for Information Technology Kyushu University, Japan.

****** Research Institute for Information Technology Department of Electrical Engineering, IIT Delhi, India

Abstract**—***Recent years the Internet-of-Things(IoT) has been deeply interwoven in our lives but at the same time the IoT security issue (cyber-attacks) causing severe risks is the main upshot in IoT domain. In this research, we aim to improve users' security awareness through a systematic E-learning system based on an ontology method. Firstly, we classified, analyzed and characterized concepts of both cyber security and IoT domain, and extracted useful information and vocabularies then provided them as learning materials for users. Secondly, we built an IoT security ontology based on our classification and analysis. Then, we used the Ontology description to develop a software which can automatically generate multiple choice questions. Finally, to evaluate users' awareness level after using our E-learning system we utilized Moodle to create a quiz.*

Keywords**—** *Internet-of-Thing (IoT), E-learning, Ontology, IoT security*

I. INTRODUCTION

A. *IoT security as core knowledge of this research*

The IoT application has been deeply interwoven in our lives and it's implemented by connected heterogeneous devices with various techniques through pervasive network [1]. At the same time, the vulnerability of such interconnectivity also causes serve cyber-attacks [2], such as Dos, Man in the Middle and many other attacks. And all of them would lead severe security issues to IoT assets. For instance, the identification, data privacy and integrity etc.

According to a study conducted by McAfee, the main institution information security issues actually come from the lack of information security knowledge and awareness to its employees. Therefore, in this paper, we mainly discuss the Specialist Education for Secure IoT to improve users' security awareness utilizing a flexible E-learning Education Method.

B. *Ontology as core technique of this research*

The ontology is a representation of concepts and relationships existing in the domain of interest. Generally, the ontology is used for sharing information because of people's different needs. The term 'concepts' describes the main components of a domain namely the classes and their individuals whereas the term 'relationships' represents the hierarchy between the classes. In our research we used ontology as a tool to represent our knowledge.

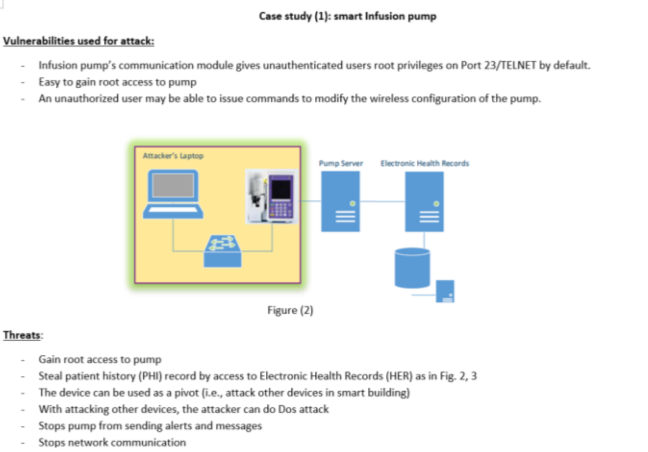
II. IMPLEMENTATION

A. *Classification and Analysis of the contents of IoT security domains*

The IoT security threats such as Dos, Sybil and Reply attacks can exist on different IoT assets and be enabled by different vulnerabilities. Because we used Ontology to describe concepts and their relationships. Firstly, we classified the IoT security threats, corresponding countermeasures, the core contents of IoT (devices, sensors and services) and their relationships.

B. *Creation of E-learning materials*

The E-learning system needs some learning materials to educate users and let them fully understand IoT knowledge. For creating those materials, we summarized each investigated case and made the contents dapper and straightway. The materials should contain the vulnerabilities and results of each attack as the example shown in Figure 1.



Case study (1): smart Infusion pump

Vulnerabilities used for attack:

- Infusion pump's communication module gives unauthenticated users root privileges on Port 23/TELNET by default.
- Easy to gain root access to pump
- An unauthorized user may be able to issue commands to modify the wireless configuration of the pump.

Attacker's Laptop
Pump Server
Electronic Health Records

Figure (2)

Threats:

- Gain root access to pump
- Steal patient history (PHI) record by access to Electronic Health Records (HER) as in Fig. 2, 3
- The device can be used as a pivot (i.e., attack other devices in smart building)
- With attacking other devices, the attacker can do Dos attack
- Stops pump from sending alerts and messages
- Stops network communication

Figure 1: Example of educational material

C. *Creation of IoTSec Ontology*

For developing our IoTSec Ontology we followed the guide Ontology Development 101[3] which proposed seven

Yiyi Wang
Department of Information Science, Kyushu University, Japan

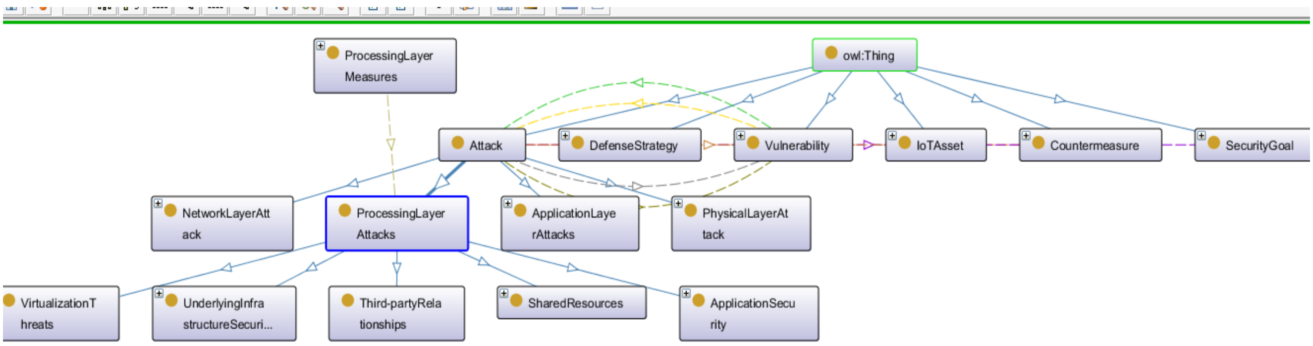


Figure 2: Classes and Class hierarchy

steps to create an ontology. Firstly, we determined to fix our ontology on IoT security domain then used the IoT-Lite Ontology (http://iot.ee.surrey.ac.uk/fiware/ontologies/iot-lite) which is a meta and lightweight Ontology to represent IoT resource, entities and services as a reference ontology for our IoTSec Ontology. Then we enumerated important terms in our ontology based on our classification and analysis before we started ontology development. Such as Threat, Countermeasure, Vulnerability, IoT Asset, Device and much more. Then we defined the classes, classes hierarchy, their properties and also facets of those properties.

The proposed IoTSec Ontology describes the classes: attacks, vulnerabilities, countermeasures and the properties among them as shown in Figure 2. And it was developed as an extension to IoT-Lite Ontology by adding security components.

D. *Automatic Creation of MCQs Based on IoTSec Ontology*

To evaluate users' security awareness changes and their effort after using this E-learning system, we need to provide some questions to test them. In this paper, we took advantage of ontology descriptions to implement a function of automatic generation of MCQs.

1) Take IoTSec Ontology file as an input and then sore it into memory instead of usual database.

2) Generate strategies such as Instance-of-class strategy, Object property strategy and Data property strategy to extract information from knowledge in order to generate MCQs. All those strategies use the elements in our Ontology to generate the correct answer and the distractors in a question item.

3) Use a programming library includes JENA SemanticWebFramework[4](http://jena.sourceforge.net/index.html) to decipher the ontology file and store the result in memory. Then Simple Natural LanguageGenerationframework[4] is used to make sure the generated questions are transformed in fully understandable syntactically and grammatically correctness.

4) The output of this step is some MCQs.

III. Output of the System

The result of this system is a live (Q&A) bank. Then we used the Moodle to generate random questions for evaluating the security awareness for each user. Then we use this system to test users in order to evaluate their changes before and after using our system.

IV. CONCLUSION

This research focuses on providing specialized online IoT Security training for institutes' employees through E-learning system. And it provides straightway learning materials to let users have comprehensive understanding of IoT security domain and improve their security awareness..

Acknowledgment

This research was supported by Strategic International Research Cooperative Program, Japan Science and Technology Agency (JST), SICORP and JSPS KAKENHI Grant Number JP16K00480.

References

[1] D. Evans, "The Internet of Things-How the Next Evolution of Internet is Changing Everything". White Paper. April 2011.

[2] Abdul Wahab Ahmed, "A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT". (IJACSA) Vol.8. No.7,2017

[3] N.F.Noy and D.L.McGuinness, " Ontology development 101: A guide to creating your first ontology.

[4] Andress Papasalouros, "AUTOMATIC GENERATION OF MULTIPLE CHOICE QUESTIONS FROM DOMAIN ONTOLOGIES

Yiyi Wang
Department of Information Science, Kyushu University, Japan