Design of IT Keys and Its Real Practice Specialist Program to Promote Key Engineers as Security Specialists

Atsuo Inomata, Satoshi Matsuura, Kenji Ohira, Youki Kadobayashi, Kazutoshi Fujikawa, Hideki Sunahara and Suguru Yamaguchi
Graduate School of Information Science
Nara Institute of Science and Technology
Ikoma-city, Nara-pref, Japan
e-mail: {atsuo, matsuura, k-ohira, youki-k, fujikawa, suna, suguru}@itc.naist.jp

***Abstract*—We introduce a practical teaching strategy called "IT Keys" for information security management. The educational goal is to put the work-ready graduates out into the social as a security expert (CSO: Chief Security Officer or CISO: Chief Information Security Officer). We collaborated with four universities and some departments of the Japanese government for IT Keys program. In this paper, we describe how to construct the teaching strategy, based on a combination of problem-based and project-based learning for promoting security expert. Furthermore, through the use of IT Keys for 5 years since 2008, we report evaluations of some special lectures and exercises according to every feedback each of year.**

Keywords-IT Keys; information security; education; problem-based learning; project-based learning; government.

I. INTRODUCTION

Information technology is an important and integral part of the current social infrastructure. Internet has come to play an important role in various foundations of our society and life. To maintain all our systems and ensure infrastructure safety, many organizations, government bodies, and companies employ security experts. In addition, they have engineers to carry out their work properly. However, very few people must have heard of a management technique or a policy for information security. Training these professionals is costly because their training involves imparting not only technical skills such as machine installation or specific procedures, but also special skills concerning law, policies, inspection, management, and ethics. These are necessary for taking decisions regarding the security policy of organizations, which is called the information security literacy. We believe that it is very important for future security experts to acquire and promote information security literacy more safely and reliably. Further, we believe that communities of students from different universities, organizations, and fields are important factors in the education for the information security.

In this paper, we propose a novel and practical teaching strategy called IT Keys that is a combination of problem-based and project-based learning. We particularly focus on "HORENSO" (in Japanese) [7], which is an information sharing technique based on members' understanding and synchronizing actions for changing circumstances within and outside an organization. The "HO" is the short form of "report," meaning timely and adequate reporting. Its flow is usually from subordinates to superiors. However, superiors or administrators must also ensure that subordinates are kept informed in order to ensure timely reporting. "REN" is "contact" and "SO" is "consult". This says that when a problem occurs, workers should report the issue, and not keep it to themselves. They should contact the relevant people, the foreman or the Japanese coordinator in this case. Instead of assuming that they can fix it themselves, they should consult with others to get their advice. Therefore, we believe that "HORENSO" is the most important factor for the information security experts to understand correctly.

In Japan, IPA [8] is an organization of professionals that contributes to the growth and advancement of Japan's economy by providing the strategic technology and human resource infrastructure required to support sustainable development of software and information processing systems. IPA provides a skill map of information security management to different categories of IT users. The map defines the security skill level in terms of a set of some technological elements. Further, it presents the quantification and visualization of the security skill required to grasp a level of each element. It can be considered as a measure that evaluates the level of competency required for information security management. Companies, organizations, and institutes can customize skill maps themselves according to their requirements. Skill maps can be classified into 16 classes on the basis of the type of technical skills to be acquired by information security professionals.

II. IT KEYS PROGRAM

IT Keys program (special IT program to promote key engineers as security specialists) was started in October 2008 as one of "IT Specialist Training Promotion Program" by the Ministry of Education, Culture, Sports, Science and

 ISBN: 978-1-61208-231-8

Technology (MEXT), Japan, for the promotion of the best standards in the field of information security. The purpose is to establish a strong and practical education foundation through industry-university cooperation to allow skilled people in the field of management of advanced and practical information security to interact. This is achieved by the cooperation of the teachers from four universities (NAIST, Kyoto University, Osaka University, JAIST) and working members of NTT Communications) and three organizations (NICT, JPCERT/CC, NPO-the Research Institute of Information Security). We aim lead to realize the following by training talented people in IT Keys.

Fig. 1 shows three fundamental keys for IT Keys knowledge acquisitions: (1) advanced knowledge, (2) practical knowledge, and (3) fundamental knowledge. In the case of acquisition of advanced knowledge, it focuses on comprehensive and rigorous social knowledge for information security, consisting of security policies, laws, security management, and ethical issues. In the case of acquisition of practical knowledge, it targets latest knowledge on information security, especially the cryptography theory, network security techniques, standardization of these techniques, network operation, etc. In the case of acquisition of fundamental knowledge, the study is based on basic computer science and mathematics knowledge in order to logically understand.

1. We make all learners study and understand not only the technology involved but also laws, policies, management techniques, and ethics with stress on systematic learning. We train about 20 people every year.

2. Through industry-university cooperation, we established a new educational foundation that helps in raising talented people who can take multifaceted information security countermeasure that a company or an organization needs.

3. We train students at a single center and make them study and exercise together closely. They can not only learn but also generate future human resource by forming human networks. So, we think that to get student together is a most important factor of IT Keys for them.

4. We realized social cognition by (1) conducting open lectures to present exercises and results to the public, (2) considering the results of an evaluation carried out by organizations for many kinds of IT business, (3) extending the cooperation of various external organizations, and (4) continuously improving the IT Keys program.

5. We contribute to the realization of an IT society in Japan, which will ensure the safety of all people, by reducing the social IT risk and establishing high-level information security through training security engineers and administrators and spreading awareness regarding information security among people.

III. HOW TO DESIGN

A. *Problem-based and Project-based learning on IT Keys*

We focused on the integration of problem- and project-based learning in IT Keys. Problem-based learning is conventionally restricted to classrooms. A group of learners (for example, 2 to 6 members) meet at a place where an instructor can facilitate a discussion on learning issues. Individual research may be conducted off-campus, but collaborative learning integral to this methodology is enabled by face-to-face communication and the process of negotiation of important learning issues. Savin-Baden introduced computer-mediated collaborative problem-based learning as a model that combines the current trend of online learning within universities, with problem-based learning focused on instructional methodology. Meanwhile, project-based learning is an instructional methodology adopted for the “Interactive design for multimedia” course that had a multiphase project as the major assessment component.

A combination delivery mode, for example, was used, and non-compulsory lectures were given and supplemented with practical sessions that involved support groups. This is based on a combination of problem- and project-based learning. Hence, we set up various problem scenarios in which a clear solution does not exist and then adopted both planning and learning to obtain a solution not by a single person but by cooperative work. IT Keys consist of the following 2 lectures and 5 exercises: information security management literacy, most recent information security issues, accident response exercise, risk management exercise, system attack and defense exercise, system break-in and analysis exercise, and IT crisis management exercise.

B. *Lecture on information security management literacy*

In a lecture on information security management literacy, some expert engineers gave information on the latest technologies to learners; for example, an engineer presented real raw traffic data and a case on an accident associated with an Internet service provider. This lecture was developed by an ISP engineer and manager, a lawyer, a government administrator (National Information Security Center, NISC), an auditing company, etc. This lecture provides a comprehensive and rigorous account of information security, consisting of topics on security policies, laws, security management, and ethical issues besides latest technologies. Thus, learners are also taught management techniques. According to hot security incidents on every year, we are updating the courseware, especially at

 ISBN: 978-1-61208-231-8

this year, we have added the digital forensics, cloud security and smartphone security.

C. Lecture on latest information security issues

In a lecture on latest information security issues, some professors presented theoretical and technical issues. The former deal with the basic algebra, fundamentals of public key infrastructure, and development of digital signature and elliptic curve cryptography [9]. Elliptic curve cryptography is the most attractive public key cryptosystem since it realizes the privacy protection with a small key size while maintaining the security high. This is why the elliptic curve is currently attracting a great deal of attention from a low power machine such as a smart card. Furthermore, a new tool from elliptic called a bilinear pairing, cast a new light on various problems on cryptology. In this lecture, we execute an exercise for implementing a bilinear pairing on Python language. Also the technical issues deal with basic network security mechanisms such as intrusion detection systems or development of firewalls. We provide some information systematically so that they can trouble shoot and take countermeasures against various accidents.

D. Exercise in IT crisis management

In the exercise called IT crisis management, learners work on a virtual ISP, and each group consists of 4 learners. They are responsible for the operation and management of web-hosting services for virtual customers. Further, they develop network equipment and some servers for this exercise in advance. Each group has an IP telephone, some routers and switches, network devices, PCs, etc. In practical situations, several security accidents can occur. The exercise staffs in backyard call and claim as various customers and then force their servers and services suspend or stop (Fig. 2). Each learner attempts to take countermeasures for unexpected accidents, to restore web-hosting services, deal with claims from customers, and find the reasons behind accidents. Finally, each group gives a clear and detailed explanation about the accidents and countermeasures to the CEO or President of ISP (Fig. 3).

E. Exercise in dealing with security incident

In the exercise called dealing with security accidents, learners work on a real security testbed called “StarBED” developed by National Institute of Information and Communications Technology (NICT).

Real computers and network equipment are required to evaluate the software practically for the Internet. In StarBED, there are many computers and switches, which connect these computers. We reproduce situations close to real situations using real equipment that are used on Internet. This idea is based on our previous work [5]. If developers want to evaluate their real implementation, they have to use real equipment. We believe that it is important for learners to emphasize on hands-on learning in real complicated Internet environments such as in the case of “StarBED” to monitor, analyze, and prevent Internet accidents and a variety of attacks and to deal with them. Another important factor is to learn more about computer viruses and malwares in order to understand the mechanism of cyber attacks. Fig. 4 shows snapshots of this exercise. We analyzed malware attacks (8 specimens) sampled from over 5000 e-mail viruses.

F. Exercise in risk management

In the exercise called risk management, learners learn the “internal behavior” of real malwares after the exercise on dealing with security accidents, which comprises learning the external behavior. Learners were studying at Telecom-ISAC Japan. The objective of Telecom-ISAC Japan is to enhance security countermeasures for the information and telecommunication industry, by establishing the systems for sharing between the members and analyzing the security accidents. Hence, it is important for them to study practical countermeasures against new malwares. Learners are responsible for analyzing and determining the internal behavior of malwares using analyzing tools. This also helps in taking the right action when a computer access accident comes to light. To recognize and respond to these situations, they learn about an analyzing technique at the machine language level (in this exercise, only Intel IA32 [10] Architecture) to detect suspicious codes or operations at the early stage. Fig. 5 shows snapshots of this exercise.

IV. EVALUATION

In order to verify the validity of the learning method for IT Keys, we carried out two evaluations. One was based on a questionnaire.

・Two or more traps were baited and devised in one incident scenario, it was very interesting for each other.

・For various situations and causes for an incident case which were occurred in this exercise, a communication to customer or a negotiation to group members simultaneously, these various experiences became future good tips.

・Since we could tackle some problems only by forming a small group and the exercise equipment and system was ready, we were able to play as each role for a virtual security division. However, since there were too many tasks to be completed in a short time, it was difficult and tough to complete unexpected incident.

Furthermore, we conducted a test based on the skill map, repeating the test 3 times from 2008 to 2011. This skill test was given twice to all learners, before and after the completion of the IT Keys courseware. For 2008, the average score in the first test was 52.7 and in the final test was 71.3; for 2011, the score in the first test was 55.7 and in the final test was 85.1 (out of 100). On 2008, we confirmed that the scores of tests on the topics “information security management,” “application security,” and “law, ordinance, and standard” had increased greatly. However, we found that the overall scores for “cryptography” and “law, ordinance, and standard” were low. In order to improve

 ISBN: 978-1-61208-231-8

comprehension, we implemented some feedbacks in the IT Keys courseware. For better understanding of the cryptography theory, we made learners use the Mathematica and Python language to implement a protocol for elliptic curves themselves. Then, we clarified the cryptography theory and its applications systematically. In addition, we subdivided the chapter on law, ordinance, and standard into 2 chapters and then evaluated their comprehension clearly from 2009. Consequently, the scores increased considerably. We found that the most important thing for educating a security expert is to keep on updating and feedback due to learner's level of understanding.

V. SUMMARY

We have conducted the special security expert education program supported by MEXT. From 2011, we continue it on our independent efforts. At March 2012, finally MEXT gave IT Keys a very good evaluation (most high degree) [6].

REFERENCES

[1] Slavin, R.E., Cooperative Learning: Theory, Research and Practice (2nd edition), Boston: Allyn and Bacon press, 1995.

[2] Savin-Baden M., Facilitating Problem-based Learning: Illuminating Perspectives, Open University Press, 2003.

[3] Savery, John R., "Overview of Problem-based Learning: Definitions and Distinctions", Interdisciplinary Journal of Problem-based Learning, Vol.1, Article 3, pp.9-20, 2006.

[4] Frank K.. and Michelle R., "Project-based learning and learning environment", Issues in Information Science and Information Technology press, Vol. 4, pp.503-510, 2007.

[5] Gregory Blanc, Youki Kadobayashi, "A step towards static script malware abstraction: Rewriting obfuscated script with Maude", IEICE Transactions on Information and Systems, Vol. E94-D, No.11, pp.2159-2166, 2011.

[6] MEXT, available at http://www.mext.go.jp/a_menu/koutou/it/h19/1321120.htm (japanese), 2012.

[7] Japan Intercultural consulting, available at http://www.japanintercultural.com/en/news/default.aspx?newsid=169

[8] IPA, http://www.ipa.go.jp/

[9] Steven Galbraith, available at http://www.isg.rhul.ac.uk/~sdg/ecc.html

[10] Intel, available at http://www.intel.com/content/www /us/en/processors/architectures-software-developer-manuals.html

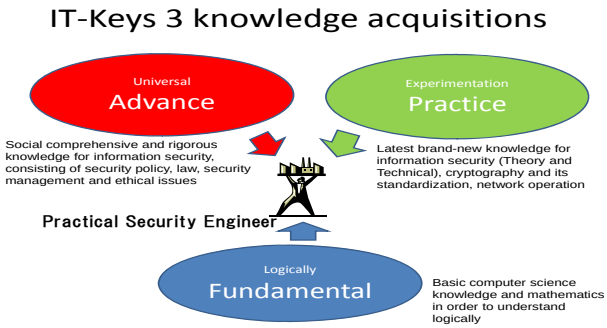

Figure 1. IT Keys' 3 knowledge acquisitions.

Figure 2. Exercise staff and learner responds to unexpected accidents.

Figure 3. Discussion in each group and presentation to CEO.

Figure 4. Exercise in dealing with security accidents using StarBED.

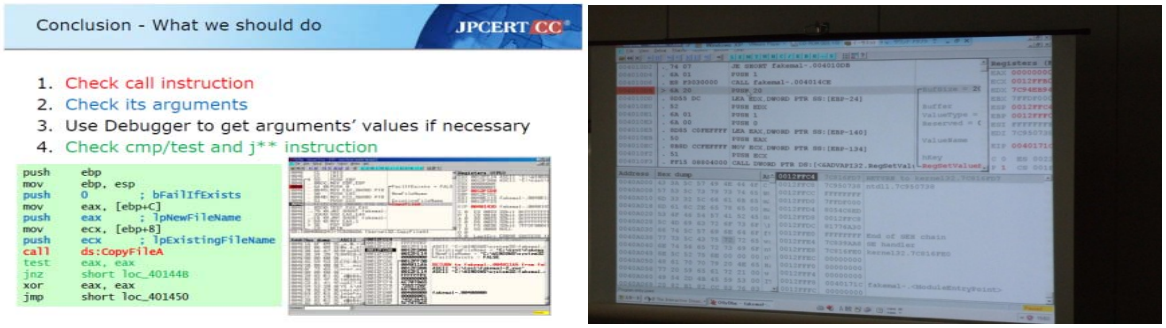

Fig.5 An assemble code for the malware static analysis.

 ISBN: 978-1-61208-231-8