# Practical Administering Security to the University Research Working Group Knowledge Management System Website

Suwarin Pattamavorakun, Jaturapith Krohkaew, and Chawanwit Poolsri
Rajamangala University of Technology Thanyaburi, Pathumthani, Thailand
Email: suwarinp@yahoo.com, kjatura@yahoo.com, goddabinahead@gmail.com

***Abstract*—Technological innovation comprises of creating new knowledge and generating technical ideas. To be globally competitive, it is important for every organization to be innovative. For university, it is necessary to develop and manage institution as knowledge based organization. The website namely Rajamangala University of Technology Thanyaburi research working group is as the knowledge portal by retrieving the necessary knowledge and establishing wide contact within and outside the organization, and for converting the value of tacit knowledge to explicit knowledge. The practical mechanisms security administering was applied to the website. Hardware control such as firewalls intrusion detection system was followed the university policy. The cryptography which are key exchange protocol with public key and the digital signature was used for authentication and the authorization part. The access data control is for preventing SQL injection attack. The program for preventing the forbidden information was built. The user's side protection was concentrates not only visible to and invoked by users of operating systems but also the security was from the operating system designer. The penetration test and continuing attention were periodically done as the description of current situation and as the plan for activity improvement.**

***Index Terms*—authentication, authorization, cryptography, knowledge management system, website security administering**

## I. Introduction

One of the most important changes that Internet and Information Technology has brought to the world of conventional academic processes is knowledge Management system (KMS) on the website. KMS on the website refers to use of computer networks for administration, creation, codification, dispersion, refinement and use of knowledge. It integrates E-Mail, E-card, poster, Web Board, Web Blog, self-Learning, and similar techniques into a comprehensive, electronic system of sharing via website. Therefore KMS is becoming an important means of dealing in the environment of knowledge sharing and increasing organization performance. In fact many academic organizations have already made high commitments in terms of investment in developing infrastructure for KMS. Unfortunately most of these institutions seem to have hurriedly attempted to cash-on the opportunities offered by KMS without giving attention to the security issues associated with it. Rajamangala University of Technology Thanyaburi (RMUTT) has been created a website namely research working group knowledge management system for which a framework to share and gain the knowledge of the research individuals within and outside the university. This web site of RMUTT has gathered the 10 groups of present research works. It is the presentation website which consists of 3 groups of users: general users (who interested in researches), researchers (members) and system administrator. In order to bring a realizable performance and effectiveness in the KMS website, so a comprehensive security management system and its penetration test operations defense has to be embedded / built into the RMUTT research working group KMS website.

Manuscript received May 20, 2013; revised July 15, 2013.

## II. Context of the System

### A. Knowledge Management System

Today, organization even the educational institution needs are rapidly becoming more diversified and technologically innovative. There is a need to transform the university into an oasis of creativity and innovation Knowledge is a fluid mix of framed experience, values, contextual information, and expert insight that provides a framework for evaluating and incorporating new experiences and information [1]. The use of knowledge management (KM) is essential to improve quality production and organization excellence in the global competitive world. The knowledge sharing is the promising tool to achieve the objectives that organization shift from problem solving to creativity and innovation of ideas, cost is saving to value addition, corrective action to elimination of problem through continuous improvements.

### B. Internet Security Policy

The Internet does not have a governing security policy per user, because it is a federation of users. Nevertheless, the Internet society drafted a security policy for its members [2]. The policy contains the following portions [3].


doi: 10.12720/joams.1.3.308-312

- Users are individually responsible for understanding and respecting the security policies of the systems (computers and networks) they are using. Users are individually accountable for their own behavior.
- Users have a responsibility to employ available security mechanisms and procedures for protecting their own data. They also have a responsibility for assisting in the protection of the systems they use.
- Computer and network service providers are responsible for maintaining the security of the systems they operate. They are further responsible for notifying users of their security policies and any changes to these policies.
- Vendors and system developers are responsible for providing systems which are sound and which embody adequate security controls.
- Users, service providers, and hardware and software vendors are responsible for cooperating to provide security.
- Technical improvements in Internet security protocols should be sought on a continuing basis. At the same time, personnel developing new protocols, hardware or software for the Internet are expected to include security considerations as part of the design and development process.

These policies clearly state to whom they apply and for what each party is responsible.

The Software Engineering Institute at Carnegie Mellon University has created a framework for building a security plan [4]. The framework, called OCTAVE, includes eight steps:

- Identify enterprise knowledge.
- Identify operational area knowledge.
- Identify staff knowledge.
- Establish security requirements.
- Map high-priority information assets to information infrastructure.
- Perform an infrastructure vulnerability evaluation.
- Conduct a multidimensional risk analysis.
- Develop a protection strategy.

These steps lead a project manager or security analyst in determining the security risks and finding controls to address them.

### C. Security Context Concerns

Research working group KMS of RMUTT website is the portal which created and used to enhance the working of a key index quality system of RMUTT. This KMS should facilitate people within and outside university to understand their tacit and explicit knowledge and must exploit the research knowledge to enhance their individual performance at par with mission and goals of the university; the website security protection depends on many aspects of computer system. Researchers begin with the security policy of the university which related services that protect against threats to the security of the university website. So the network administering security policy of this local system is under the office of Academic Resource and Information Technology of RMUTT. The researchers had given some thought to the overall architecture and planned to build in security as one of the key constructs. A security mechanism (which is the method for enforcing the university security policy) is a system that starts in an authorized state and cannot enter an unauthorized state. The three controls are specific to networks: firewalls, intrusion detection systems, and secure e-mail.

The security for users which are memory protection, object access control and users authentication had been addressed. Fences, base / bound registers, tagged architecture and segmentation were designed both for addressing and for protection. File protection schemes on Windows XP based on user-group-all format were used. Access control was addressed by an access control matrix on per-object or per-user basis. User authentication which was the plaintext password file was used when unacquainted users seek to share facilities. Additional protocol was used to perform mutual authentication in an atmosphere of distrust. The mechanisms for shutting down the weak points of the web application were used for security protection from the cracking such as SQL injection, XSS (Cross Site Scripting), remote file inclusion, and session hijacking.

### D. Research Concerns

#### 1) Statistics showing the important of security

Internet security objective is to establish rules and measures to use against attacks over the Internet [5]. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion on fraud. Different methods have been used to protect the transfer of data, including encryption [6].

Web browser statistics was exploited to see the amount of Web browser affect the malicious intent. For example, Internet Explorer 6, which used to own a majority of the Web browser market share [7], is considered extremely insecure [8] because vulnerabilities were commonly exploited due to its former popularity. Now, however, browser choice is more evenly distributed (Internet Explorer at 18.9%, Firefox at 36.3%, Google Chrome at 37.3%, and so on) [7], vulnerabilities are commonly exploited in many browsers [9], [10], [11].

#### 2) Why universities are prime targets

Many sites record network traffic data, some publicize the data and many use the data internally to monitor performance, manage resources, or demonstrate usage. The security company ISS (Internet Security Systems) tracked the status of actual Internet security risk. Its four point scale goes from 1 (normal risk from random malicious attacks experienced by all site administrators) to 4 (actual or potential catastrophic security event requiring immediate defense). During a period from April to June 2002, ISS reported 56 days at level 1, 22 at level 2, and 7 at level 3 [12]. Universities make very good targets for attack, according to an Associated Press study in June 2006 [3], Richard Power, editorial director for the Computer Security Institute, had reported that universities often run systems with vulnerabilities and little

monitoring or management. Universities are havens for free exchange of ideas. Thus, their access controls typically are configured to promote sharing and wide access to a population that changes significantly every semester. A worse problem is that universities are really loose federations of departments and research groups. The administrator for one group's computers may even know other administrators, let alone share intelligence or tools. Often, computers are bought for a teaching or research project, but there is not funding for ongoing maintenance, either buying upgrades or installing patches.

*3) Continuing increase in cyber attacks*

Carnegie Mellon University's Computer Emergency Response Team (CERT) tracks the number and kinds of vulnerabilities and cyber-attacks reported worldwide. Part of CERT's mission is to warn users and developers of new problems and also to provide information on ways to fix them. Moreover, as of June 2006, Symantec's Norton antivirus software checked for over 72,000 known virus patterns. The Computer Security Institute and the FBI cooperate to take an annual survey of approximately 500 large institutions, companies, government organizations, and educational institutions. The response from 1999 through 2005 has been fairly constant. In each year approximately 40 percent of respondents reported from one to five incidents, 20 percent six to ten, and 10 percent more than ten. The respondents reported total losses exceeding $42 million due to virus attacks. It is clearly time to take security seriously, both as users and developers [3], [13].

## III. PRACTICAL IMPLEMENTATION

### A. Technical Process Framework

There are the elements of the overall effective processes in administering security for RMUTT research working group KMS website. The researchers asked the account number as database administrator for managing the MySQL DBMS namely KMIS which is the section in responsibility of Institute of Research and Development, and uploaded the webpages on the www.ird.rmutt.ac.th/KMIS.

Since the inside contents of the KMS website are the research works and considered as the intellectual properties. The Website security protection consists of authentication part, authorization part and the part of preventing rude or obscene words. For the user authentication, the researchers used the user's citizen identification card number by the check sum method. For preventing an exhaustive or brute force attack which block the cracker could not use the cached-session ID or cookie, of this the researchers used the significant cryptography method as in Fig. 1.


Figure 1. Preventing the Brute Force attack.

For the authorized part which preventing the SQL injection from the cracker, the researchers used the methodologies: (1) prevent the cracker to input the special characters via log-in form to the database of password (2) limit the length of the field-input of username (3) move the prevent script files from the client side to the server side.

The practical implementation of the system is shown in Fig. 2; the authentication using the citizen ID number is in Fig. 3.

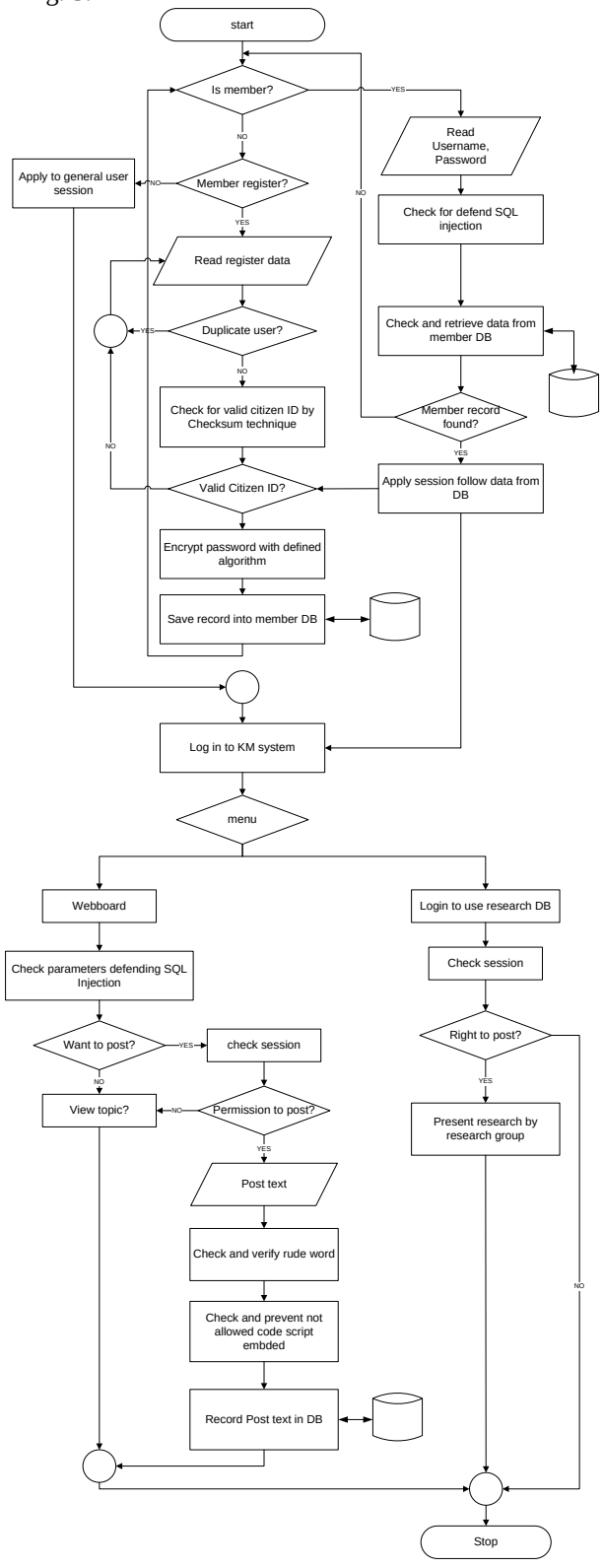



Figure 2. Overall technique of the security system.

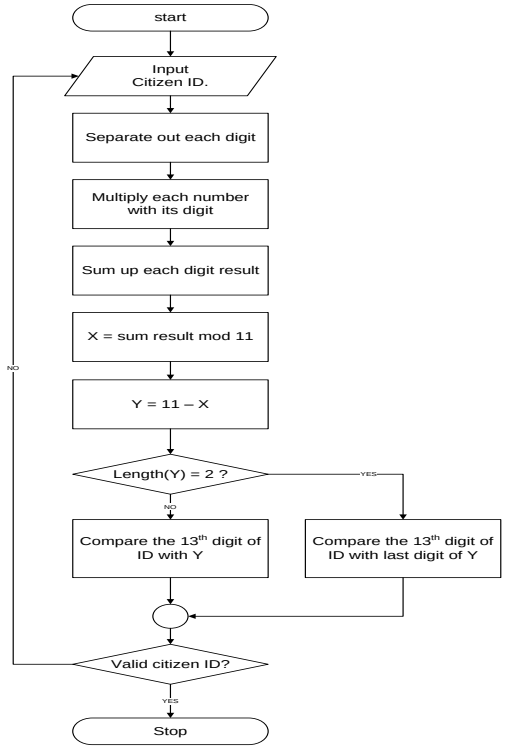



Figure 3. . The check digit method using citizen ID number.


Figure 4. The main website of RMUTT research working group KMS.


Figure 5. The page for member register.


Figure 6. The incorrect ID number warning

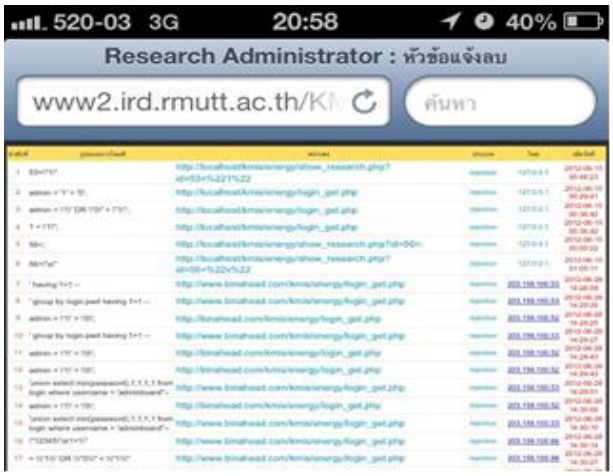



Figure 7. The information of attack recorded to admin

## IV. Results

The website of the KMS of research working group is under the website of the university's Institute of Research and Development, so, the researchers followed the university's policy put a warning screen, and the rules are from the Computer Crime Act 2007 of Thailand. The examples of some web pages are shown in Fig. 4- Fig. 5.

Some Results while the check sum procedure for citizen ID number was incorrect are shown in Fig. 6, some results of penetration test are shown in Fig. 7.

## V. Conclusion

During the past three decades, organization even the academic institution had been adopting quality knowledge base for the improvement in quality production and organization excellence in competitive world. The Internet and IT have evolved a new dimension of the university's knowledge management system. However, knowledge management system environment is under security threats giving rise to a variety of security risks because of the intrinsic properties of the Internet are major source of its vulnerability to failures and attacks. For this purpose there is a need for developing a practical security administration in order to control the risks. The research presents the security practices to the website of the university research working group knowledge management system. The researchers must decide whether to implement by concerning and specifying the following: the administering security policy of the university such as the organization's goals on security, where the responsibility for security lies and what should be the responsibility rest with our small computer security group. The user's side protection, authentication

mechanisms used to confirm user's identity, cryptography method used to prevent the attacks of SQL injection and Brute Force. There is a program use to filter the disallow words and information. The penetration test was conducted for ensuring that the security management is fully protected the website.

## REFERENCES


[1] V. M. Sivakumar, S. R. Devadasan, and S. Jaisankar, "Knowledge based quality circle programe," in *Quality, Reliability and Information Technology: Trends and Future Directions*, Ed. P. K. Kapur and A. K. Verma, Narosa Publishing House, India, 2005. pp. 216-222.

[2] R. Rethia, *et al.*, *Guidelines for the Secure Operation of the Internet*, Internet Report, RFC 1281, Nov 1991.

[3] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, 4th Eds; Peason Education International, Prentice Hall, USA. 2007.

[4] C. Alberts, *et al*, *OCTAVE Catalog of Practices*, Software Engineering Institute Report, CMU/SEI-2001-TR-020, Oct 2001.

[5] P. Gralla, *How the Internet Works*, Que Pub., USA. 2007.

[6] M. Y. Rhee, *Internet Security: Cryptographic Principles, Algorithms and Protocols*, Chichester: Wiley, 2003.

[7] Browser Statistics. [Online]. Available: www.w3schools.com/browsers_stats.asp [Retrieved 10 August 2012].

[8] T. Bradly. It's time to finally drop internet explorer 6. (19 November 2012). [Online]. Available: www.pcworld.com/its_time_to_finally_drop_I

[9] E. Messmer. Ellen and Network World. (19 November 201). Google Chrome Tops 'Dirty Dozen' vulnerable Apps List. [Online]. Available: www.networkworld.com/Home/

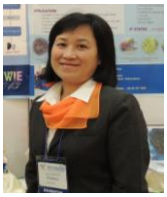
[10] G. Keizer, *Firefox 3.5 Vulnerability Confirmed*, retrieved 19 November 2012.

[11] C.-A. Skinner, *Opera Plugs "Severe" Browser Hole*, retrieved 19 November 2012.

[12] Internet Security Systems. Internet Risk Impact Summary for March 26, 2002 through June 24, 2002. ISS Report. 2002. [Online]. Available: www.iss.net

[13] Canadian System Security Centre. Canadian Trusted Computer Product Evaluation Criteria, Jan 1993.


**Jaturapith Krohkaew** obtained an Ms in Computer Engineering degree at King Mongkut's Institute of Technology Ladkrabang, Thailand. He is a research engineer in the field of computer embedded system and database. Currently he serves as the leader and does a project for Electricity Production Authority of Thailand. Today one of his main interests is the development of the computer inventions for visually impaired.



**Suwarin Pattamavorakun** is an associate professor of Faculty of Science and Technology, Rajamangala University of Technology. She obtained a Ph.D in Information Management at Asian Institute of Technology, Thailand. Her research interests are simulation and modeling and artificial intelligent comprising both theoretical and practical aspects. Today one of her main interests is the development of the computer inventions for visually impaired.

**Chawanwit Poolsri** graduated BSc. from Faculty of Science and Technology, Rajamangala University of Technology and now is a supporting person, works at Faculty of Engineering, Rajamangala University of Technology Thailand. He has done the research as the team worker of the project of Electricity Production Authority of Thailand.