How can wireless users identify themselves with the security issues? -- the integrated vulnerability management system

Yeu-Pong Lai*, Shih-I Chou, and Guang-Yuh Su

Department of Computer Science and Information Engineering

Chung Cheng Institute of Technology, National Defense University

Tauyuan 335, Taiwan, ROC

{lai, g971210, yuh} @ccit.edu.tw

Received 26 March 2007; Revised 1 May 2007 ; Accepted 24 May 2007

Abstract. With the growing in computer network usages of fixed or wireless infrastructures, the information security becomes more important. Most security issues are focused on preventing attacks from the outsiders or wireless users. However, these authorized wireless users have no right to take part in the drawing-up security policy of an organization. They do not even know the security level of the fixed network provided. They can only connect by chance. Besides, the larger network scales the more difficulty to be maintained. Patching and managing the mass of computer vulnerabilities are a timely but critical issue. The Integrated Vulnerabilities Management System helps the network administrators to make sure what security vulnerabilities are really critical and offers the wireless and fixed network users to present what solutions they suggest. This paper proposes a system to help users efficiently accessing information, easily getting solutions and conveniently communicating others. Not only the security administrators can get aid but also the other managers and employees could be supported with this system.

Keywords: wireless communications, collaborative works, knowledge management, group decision support, vulnerability analyses

1 Introduction

Many countries have set up governmentally wireless infrastructures for mobile computing. Recently, these infrastructures are upgraded and planned to support ubiquitous computer services for ubiquitous society. Some persons or organizations also build their wireless environment via setting up their wireless Access Points(APs). In other words, people, powering on their laptops at home, may find some many available wireless APs. Researches and engineers are only dedicated in designing or developing these security facilities or schemes for protecting these APs, authentication servers, network devices, and so on. Authorized person using laptops is always treated and examined as an intruder in prejudicing. The wireless users have no reciprocal right the same as the fixed network users. As known, the security policy should be drawn up by representatives from every department. These wireless users obviously have been banished from representatives.

Nevertheless, the wireless AP may be setup by malicious "fishers" for trapping these persons into confessing their usernames and passwords. The users are disadvantage minority in the security competition. That may be very important to wireless users to realize which APs are more secure compared to others, if these are many available APs shown on their laptops. There is no information provided to them about security mechanism through these APs. They can only make decisions with referring the communication quality, bandwidth of the APs. Some may select the least security one, since there is little constraint in surfing network via this AP. The selection however makes your data in danger.

The information security issues become more important day after day. Every organization plot schemes to deal with critical threats. The larger network scales however the more difficulty to be maintained. Generally, the focus of Information Security is integrity, confidentiality and availability but now they're weakened by security vulnerabilities [1]. According to the latest National Vulnerability Database [2], there were above 20 vulnerabilities publication per day. The vulnerability information increases exponentially from 1980 to now. It's vital to pay more efforts and attentions to security vulnerabilities as well as enterprises and the general users.

Above all, we think an integrated vulnerability management system is required to deal the massive vulnerability information. The system integrates with the collaborative system, group decision support system, and knowledge management system. It functions as an electric board for exchanging information of solutions, centralizing

* Correspondence author

the threat of vulnerabilities, ensuring the patching-up priority of vulnerabilities, demonstrating the statistical data of networks security. Therefore, the wireless users can take part in drawing up the security policy and they also know how secure the network is. The network administrator can get the global view in the network with referring to the proper suggestions and feasible solutions to protect the fixed and wireless networks.

The following section will be literature review for background knowledge, which includes introductions to the vulnerability circumstance, group decision support system, collaborative systems, knowledge management system, useful assessment of vulnerability, and Web-based systems development. According to the information in cross-research areas presented in Section 2, the system framework is introduced in Section 3. The conclusions are then given in Section 4.

2 Backgrounds

This section is for the background knowledge in implementing the proposed system. That includes the introduction of vulnerability information, group decision support systems, knowledge management systems, and Web-based system, and so on. These will be introduced in the following sections. The vulnerability information is the key to judge the potential risk in the fixed network. It will be introduced firstly in Section 2.1. The security policies and the patch-up procedures should be discussed by sub-managers or network users, so that Section 2.2 and Section 2.3 are for the introductions of the group decision system and the collaborative system, respectively. The implementation for the system is then a Web-base knowledge system. Therefore, the concept of knowledge systems is introduced in Section 2.4. Section 2.6 is for Web-based system development. After the integrated system developed, wireless users can know the security level of the fixed network that they are using via looking-up the information in the knowledge management system. Users can also take part in the policy making in security policies or decision making in patching-up vulnerabilities.

2.1 Vulnerability Current Circumstance

The Symantec Internet Security Threat Report shows that the number of found vulnerabilities raise dramatically in the intervals of each six-month from Jan-Jun 2005(1,874), Jul-Dec 2005(1912) to Jan-Jun 2006(2,249), in Figure 1. It's a 20% increase over every last reporting period.[3] There are more than three thousand vulnerabilities found in one year. The vulnerability Information are labeled and announced by several authoritative institutes, such as NVD[1], Bugtra[3] and CERT[5]. According to the observation made by SecurityFocus[4], system security administrators now spend 2.1 hours per day in average for hunting security information on all kinds of security bulletins.[6]

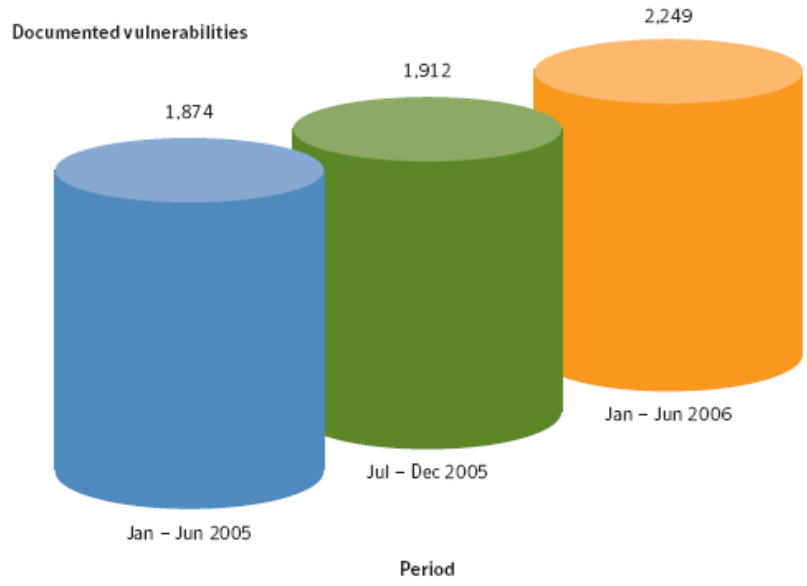

Fig. 1. Symantec documented vulnerabilities [3]

2.2 Group Decision Support System(GDSS)

The Wiki website has the definition for GDSS -- “Group Decision Support Systems (GDSS) were referred to as a Group Support System (GSS) or an electronic meeting system since they shared similar foundations”.[7] The incorporation of computational schemes and techniques to support group activities was originated from nearly 15 years ago. GDSS supports a group to find the fitting solutions for unstructured problems. Discussion-oriented tasks could be fulfilled by a group with GDSS.[8] Those can be considered as a group for example, the system administrators, sub-system managers, and wireless users. They can discuss together via direct or indirect ways to make decisions.

2.3 Collaborative Systems

“A report on collaboratories, prepared under the auspices of the National Research Council, described a collaboratory as a . . . center without walls in which the nation's researchers can perform research without regard to geographical location -- interacting with colleagues, accessing instrumentation, sharing data and computational resources, and accessing information from digital libraries”.[9] People can communicate wherever they are in a virtual meeting room offered by collaborative systems, if their computers have connected to internet. So that, the time and money spends of organizations or enterprises can be saved obviously. Besides, they can also be the auxiliaries to evaluate decisions, discuss policies, or find solutions.[8]

2.4 Knowledge Management System

Knowledge Management (KM) performs beyond the supporting technical, collaborative tools or debate systems, in providing complex support tools. [10][11] The traditional collaborative tools are commercialized such as Lotus Notes, which are collecting separate data together for generating useful information. The debate systems, such as Issue-Based Information Systems (IBIS) and knowledge-base techniques, are then the variety of discussion boards. Different from them, the KM systems involve complex support tools in process information, such as ordering, indexing, categorizing, case-base searching, fuzzy retrieving, semantic- correspondence defining, hyper-structures defining, etc. KM systems imply a fundamental change in knowledge distribution for an activity. They also shift knowledge that was possessed exclusively by the authority’s internal members to company employees and business partners.[10][12]

One of key issues in the current KM researches is how to facilitate the use of contextual information in a KM system. It indicates that the contextual information management is an essential but critical element for fully understanding knowledge.[13-17] To facilitate the use of the knowledge contexts in creation, accumulation, and utilization of knowledge in virtual collaborative works, an operational model of the knowledge contexts should be designed. Ahn et al. proposed a knowledge context model called KC-V that is shown in Figure 2. The construct of knowledge contexts could be useful for knowledge understanding.[13] In Section 3, the model is referred to structure the mechanism of the vulnerabilities knowledge management database.

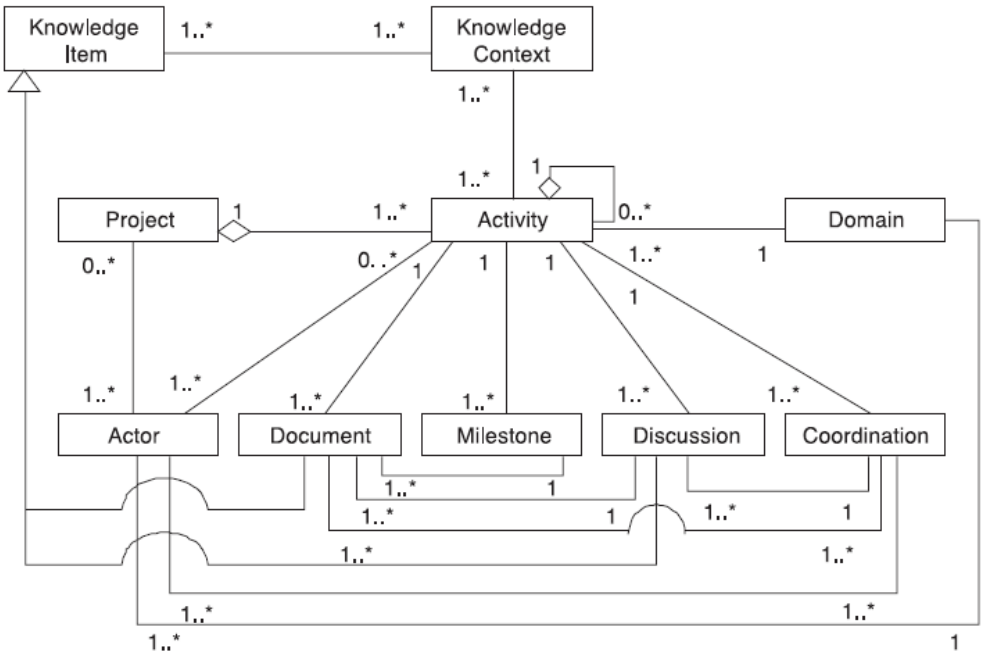

Fig. 2. KC-V knowledge context model [13]

2.5 Useful Assessment Ways for Computer Vulnerabilities

Gerhard Eschelbeck concluded some laws of computer vulnerabilities according to his discoveries in vulnerability analyzing statistics for three years. [1][19] The laws are:

- Half-life is longer for internal vulnerabilities and the vulnerabilities have to be spent 19 days and 48 days on patching external and internal systems
- Prevalence is different for internal versus external networks, and every year, the new vulnerabilities will replace the half critical vulnerabilities
- Persistence: unlimited lifespan for some vulnerabilities and worms
- Focus: 10% critical vulnerabilities produce nearly all exploitations
- Exposure: The remediation cycle can't catch up the time-to-exploit cycle
- Exploitation is shrinking and 85% damage is created by the automatic attacks during the first 15 days

Corresponding guides are in the followings.[1][18]

- Asset prioritization: Classify a hierarchy of assets by value to business
- Discovery, assessment and analysis: Prioritize the remediation efforts of organizations based on the asset classification and severity of vulnerabilities
- Remediation: Integrate operational process against vulnerability goals to improve and raise the effectiveness of vulnerability awareness and level
- Verification: Measure the networks of enterprises to against the half-life curve and persistence curve of vulnerabilities
- Policy compliance: Audit the security policies and security performance by the evaluation of metrics so that develop best practices
- A systematic vulnerability management process steps: (1)Discovery → (2)Asset prioritization→ (3)Assessment and analysis→ (4)Remediation→ (5)Verification→ (6)Policy compliance

2.6 Web-Based Systems Development

The proposed system will be presented in a Web site, so these authorized members can access and use the systems without installing any other software. By this way, the web implementation can provide the efficiency of collaborative works and unify the format of database systems in the meantime. Besides, Web technologies benefits group works in four aspects. [8] They are structuring group processes, encouraging communications, improving information processes, and supplying modeling capabilities. On Web sites, Virtual meeting rooms can be

generated on demand. The manager can have a meeting over internet. Participators only need to login the system and then wait for the conference being started.

3 Framework of The System Development

The integrated system is composed of collaborative system, group decision support system, knowledge management system, and vulnerability scan engine. Figure 3 shows the framework of the system. Every node in the figure stands for an entity. The links are then for the actions the entities should take. The entities include people and information, such as experts, security administrators, KM managers, sub-system managers, employees, decision makers, patching-up priority, policy evaluation, analysis report, network topology information, vulnerability database, KM database. These entities are interactive to several systems, Collaborative System (CS), Group Decision Support System (GDSS), Knowledge Management System (KMS), and Vulnerability Scan Engine (VSE), whose functions are illustrated in Sections 3.1, 3.2, 3.3, and 3.4, respectively. Section 3.5 shows the infrastructure in designing the system in the internet environment. The short discussions are then given in Section 3.6 for the integrated vulnerabilities management system.

3.1 A Scenario of Using Collaborative system (CS)

Security administrators can announce the specific vulnerabilities and worms waiting for security experts finding proper solutions to these threats. Via the system, the security managers can get timely assistance and information of the latest solutions. In our country, there are several projects supported by government to organize the security exports. This system is for them to update and share their knowledge, hopefully, which can be reserved and preserved from attackers. The system can be accessed by all security administrators in official departments or commercial companies. The blueprint of the CS is shown in Figure 4. It also provides some interactive functions such as online meeting, files transferring, and information publishing. This system is a hub of security information to security exports and security administrators. Besides, it provides a collaborative environment to help them work efficiently.

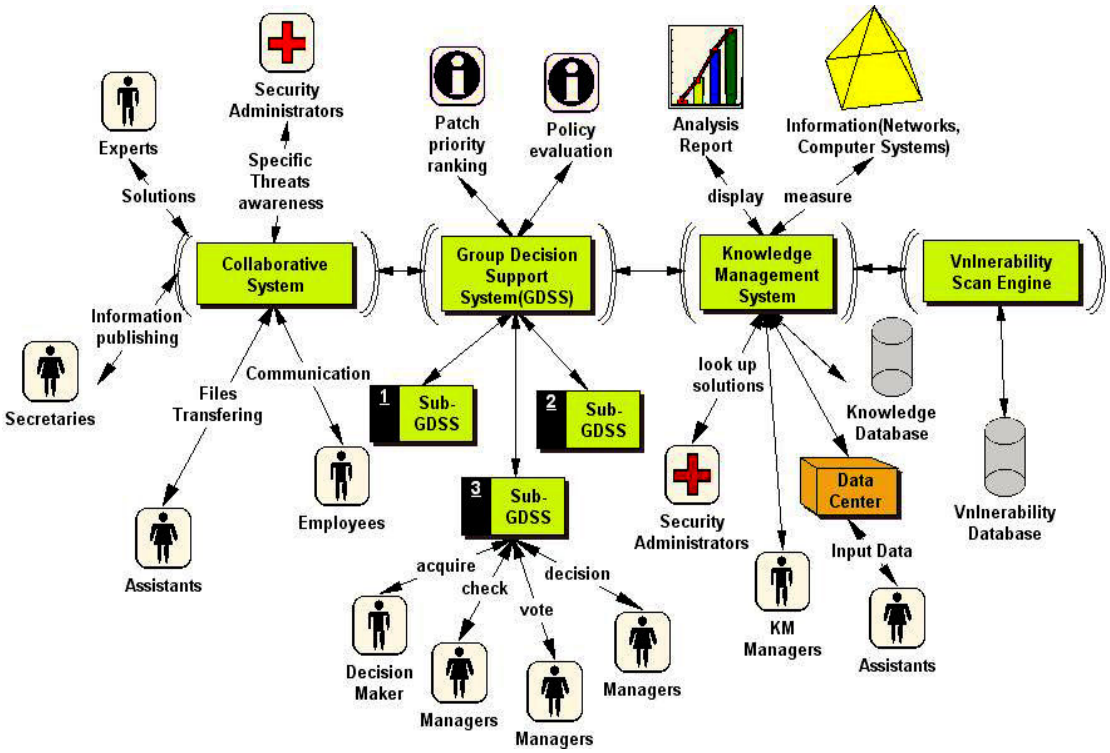

Fig. 3. A framework of proposed systems

3.2 A Scenario of Using Group Decision Support System (GDSS)

When some security polices legislated or modified, regulations have to be voted or discussed, for example in the enforcement section of security policies. The GDSS is a valid way to draw up these regulations. Managers can express their opinions and suggestions on this system. The GDSS will illustrate the results collected from several participates in statistic charts for the decision makers. The operations of the GDSS show in Figure 5. By using it in decision making, the information could be collected effortlessly and directly.

3.3 A Scenario of Using Knowledge Management System (KMS)

The KMS database consists of the collection of vulnerabilities solutions, the importance of assets, the network topology of the company, and the maintenance of security policies. In KMS, security administrators can lookup the applied solutions for vulnerabilities. After their problem solved, they can attach their solutions or suggestions to the database, as shown in Figure 6. The "EXP Security Administrators" are the experienced-solutions/notes providers. The "EX_Table" presents the table of saving the experienced-solutions/notes. The "Scores=_initial" is the default scores in KMS database. The experienced administrators can try and score the experienced-solution. If it's score is higher than the original one's or equal to the standard, the experienced-solution will be upgraded and become a new official solution or note. Other datasets could be evaluation as well by the resembling mode to notify the improper information for the KMS database managers.

3.4 A scenario of using vulnerability scan engine (VSE)

To scan the internal and external networks/systems is the main job of the Vulnerability Scan Engine. The security administrators operate this engine to discover these known vulnerabilities in their network and get vulnerabilities reports in desired format. After reports get, they can look up the solutions and information within the KMS. The engine regularly scans at night or the moment of low communication traffic requirements for servers in the network; randomly scan the portable devices as connected. Besides, if the new vulnerabilities or plug-ins are announced, the engine will be upgraded and performed immediately also. Figure 7 illustrates the operations of VSE that scans the wire and wireless networks for reporting the discovered vulnerabilities to the security administrators.

3.5 Physical Environment Design

To build the secure environment, the sub-systems must setup on separate servers, which includes an authorization server. The authorization server provides the AAA mechanism, authentication, authorization, and accounting, for users to access and use the facilities in the network. The architecture is shown in Figure 8. The authorization server authenticates every user's account with referring to certain IP address, MAC, etc. Both, Internet login and Intranet login, are accepted, so users can use mobile devices, wireless devices or other network communication protocols to login the authorization. However, these users who login from Internet can not access some critical information or perform certain functions and actions.

3.6 The Integrated Vulnerabilities Management

The integrated vulnerabilities Management are composed with four sub systems, Collaborative System (CS), Group Decision Support System (GDSS), Knowledge Management System (KMS) and Vulnerabilities Scan Engine (VSE) to support data communication, information transmission, problem solving, decision making, and vulnerability discovery. It makes the vulnerability handling and security controlling easier. The integrated system can not only help security administrators protect and maintain the network security of the enterprise timely but also make the subsystem managers and normal employees get convenience in contributing their opinions in securing this network. Besides, users can know the security situation within networks, so that they can determine where their information is protected well enough in the network. For example, they will not transmit classified information over a not-very secure network. On the other hand, if the integrated vulnerabilities management system shows the network is very secure, they can use it to transmit those classified or critical information over it.

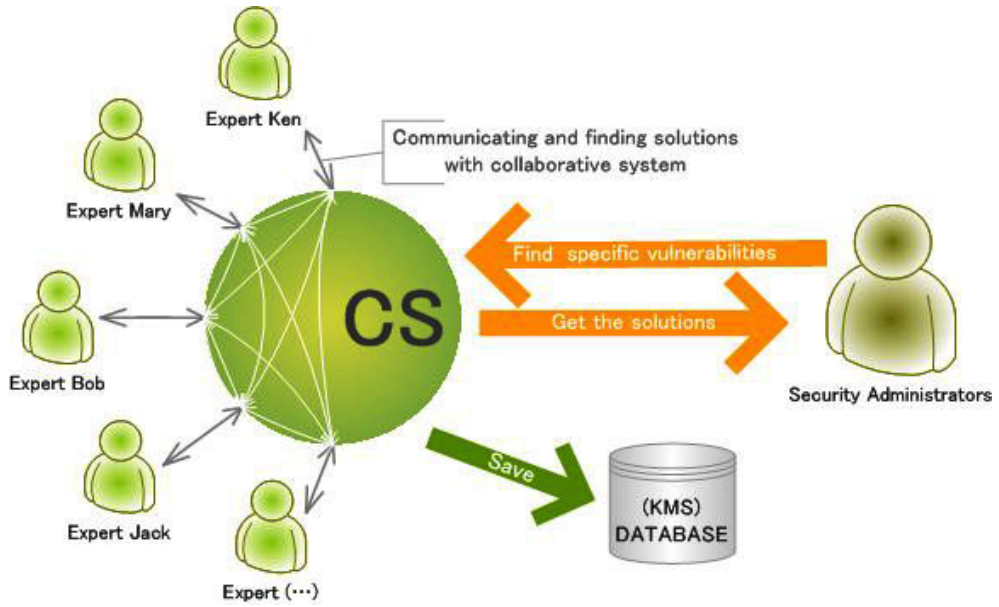

Fig. 4. Collaborative system, the mode of solving the specific vulnerabilities

Fig. 5. GDSS help routine job

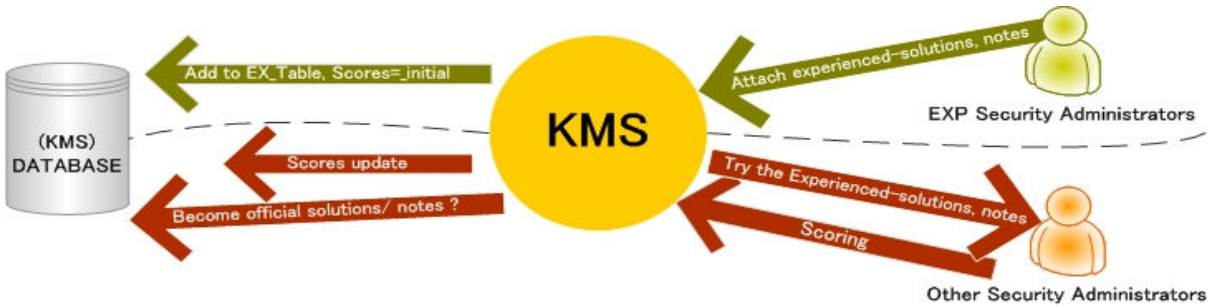

Fig. 6. Experienced-solutions sharing and scoring flows

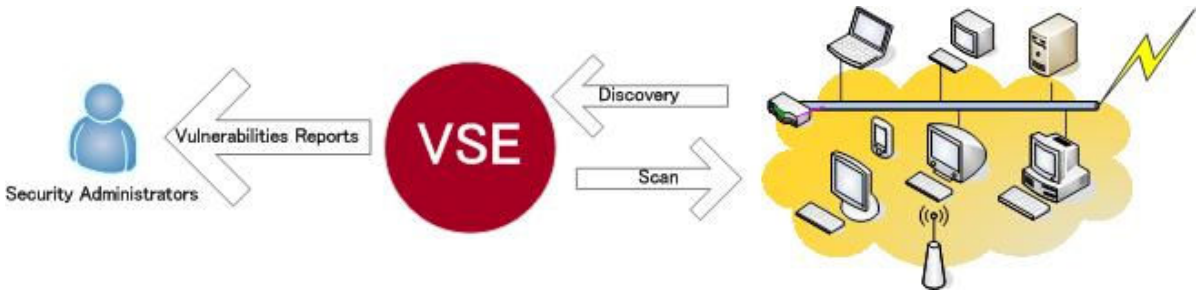

Fig. 7. Vulnerability scanning flows

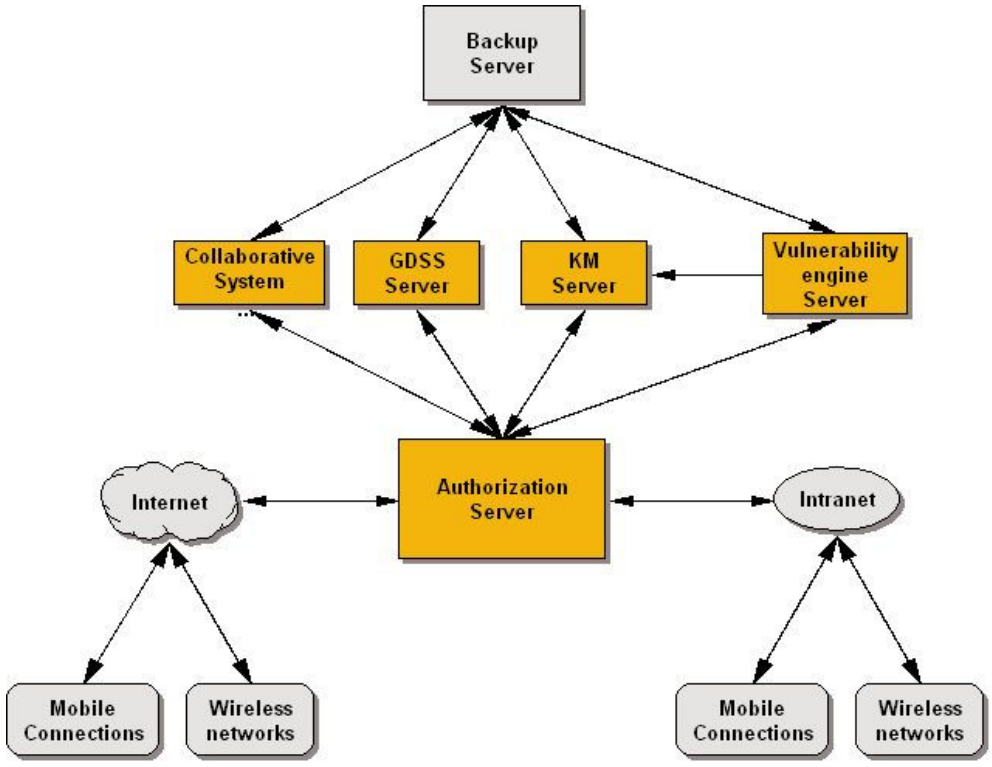

Fig. 8. The construct of the physical environment

4 Conclusions

During this age, who can lead the information is the winner. The integrated approach helps security administrators and security exports standardize their knowledge to be managed in a KM system. New system managers can learn quickly via this system. Users, no matter accessing the network via wireless or fixed, can realize the security situation within this network. Besides, all can participate the drawing-up procedures for these SOP in the KM system. As known, the wireless users normally have choices in connecting to an access point for surfing internet. There are so many persons share their APs to others. However, the wireless users do not have any idea about which AP is the most secure one. All security techniques in wireless are focused on protecting the APs. The wireless users were treated like intruders. The rights for these wireless users are not enough equal to the facility owner who maybe a phisher. By the integrated system, wireless users can know the security situation of the network they accessing. Besides, they can take part in the procedures for drawing up the security policies. This paper proposed the framework of the integrated system that consists of four subsystems. Each subsystem will be developed modularly. The system will be employed mainly for training new system mangers and managing network risks with an efficient way. The system managers can find the solutions to vulnerability handling easily and efficiently. Also, by the system, the normal users and system managers can know the security situation and take part in the discussions for drawing up security policies together.

Acknowledgement

This work was supported in part by International Collaboration for Advancing Security Technology (iCAST) project, National Science Council under the Grants NSC 95-3114-P-001-002-Y02, and NSC 95-31114-P-606-001-Y.

References

[1] G. Eschelbeck, “The Laws of Vulnerabilities: Which security vulnerabilities really matter?,” *Information Security Technical Report*, Vol.10, Elsevier Science, 2005, pp.213-219.

[2] http://nvd.nist.gov, accessed at 2007/3/15

[3] http://www.symantec.com, accessed at 2007/3/16

[4] http://www.securityfocus.com, accessed at 2007/4/9

[5] http://www.cert.org accessed at 2007/4/9

[6] H.T.Tian, L.S.Huang, Z.Zhou and Y.L.Luo, “Arm up Administrators: Automated Vulnerability Management,” *Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms and Networks*, Hefei China, pp.587-593, May 2004.

[7] http://en.wikipedia.org/wiki/Group_decision_support_systems, accessed at 2007/3/16

[8] I. Cil, O. Alpturk and H. R. Yazgan, “A new collaborative system framework based on a multiple perspective approach: InteliTeam,” *Decision Support Systems*, Vol.39, No.4, pp.619-641, 2005.

[9] http://en.wikipedia.org/wiki/Computer-supported_collaboration#Collaborative_content, accessed at 2007/3/16

[10] W. K. McHenry, “Using Knowledge management to reform the Russian Criminal Procedural Codex,” *Decision Support Systems*, Vol.34, No.3, pp.339-357, 2002.

[11] K. Lenk and R. Traunmüller, “A framework for electronic government,” *Proceedings of the 7th Workshop on Database and Expert Systems Applications*, Greenwich, UK, pp.271-277, 2000.

[12] M.A. Wimmer and R. Trauumüller, “Trends in electronic government: managing distributed knowledge,” *Proceedings of the 7th International Workshop on Database and Expert Systems Applications,, Greenwich*, UK, pp.240-345, 2000.

[13] H. J. Ahn, H. J. Lee, K. Cho and S. J. Park, "Utlizing knowledge context in virtual collaborative work," *Decision Support Systems*, Vol.39, No.4, pp.563-582, 2004.

[14] J.H. Cook, "XML sets stage for efficient knowledge management," *IT Professionals*, Vol.2, No.3, pp.55-57, 2000.

[15] D. Fensel, *Ontologies: A Silver Bullet for Knowledge Management and Electronic Commerce*, Spring Verlag , 2004.

[16] J. Gundry and G. Metes, "Team knowledge management: a computer-mediated approach," http://www.knowab.co.uk/wbwteam.html, assessed at 2007/4/9.

[17] R. Klemke, "Context framework-an open approach to enhance organizational memory systems with context modeling techniques," *Proceedings of PAKM2000: Third International Conference on Practical Aspects of Knowledge Management*, Basel, Switzerland, 2000.

[18] S. Mollerbaug, "Useful vulnerability assessment," *Information Security Technical Report*, Vol.8, No.4, pp. 78-84, 2003.

[19] The Laws of Vulnerabilities White Paper, *The Laws of Vulnerabilities: Six Axioms for Understanding Risk*, http://www.qualys.com/research/rnd/vulnlaws/, accessed at 2007/3/19