

Preliminary Diagnosis Model for a New IT Service: Improving the Information Security of u-Services with Zigbee

Ik-Seob Lee, Ki-Hyang Hong, Gang-Shin Lee, and Jae-Il Lee

Abstract—With the advent of the ubiquitous society, it is expected that there will be a surge in the volume of unethical and anti-social contents, along with an increase in new threats to information security such as online crimes involving personal properties and even people's lives. Systematic information management and protection are required in order to minimize the damages caused by such online threats in this new IT age. This thesis proposes essential security measures for planning and designing new IT services, not to mention pre-installation services, while applying Zigbee to KISA's preliminary diagnosis of an information protection model that secures stability and reliability before installation. Analysis of Zigbee, a wireless PAN technology, regarding its weaknesses and the related countermeasures, and real-world examples of Zigbee's application to u-services will also be dealt with in this work.

Keywords—Preliminary Diagnosis Model, u-Service, Information Security Assessment, Zigbee.

I. INTRODUCTION

WITH the advent of the ubiquitous society, it is expected that there will be a surge in the volume of unethical and anti-social contents, along with an increase in new threats to information security such as online crimes involving personal properties and even lives. Systematic information management and protection are required in order to minimize the damage caused by such online threats in this IT age. The establishment and good management of the systems required to address this situation is essential.

From the general standpoint of a service provider who develops a new IT service, the need to win a market share as soon as possible is quite a pressure, which often leads them to disregard the need for information security. The low stability and reliability of a new IT service in these cases lead to higher security threats and any potential security problem will incur high restoration costs. Such costs for locating potential security loopholes are higher at the stage of installation and testing than during the initial designing process. Fig. 1 shows that such a difference in cost can be as much as 60 to a 100 times greater.

Manuscript received July 4, 2007.

Ik-Seob LEE is with the Korea Information Security Agency, Seoul, Korea (phone: +82-405-5276; fax: +82-405-5219; e-mail: islee@kisa.or.kr).

Ki-hyang Hong, Gang-Shin Lee and Jae-Il LEE are with the Korea Information Security Agency, Seoul, Korea.

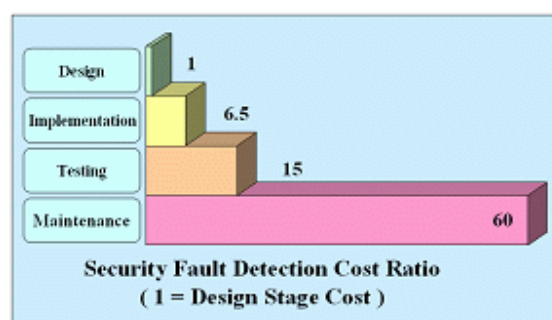


Fig. 1 Security Fault Detection Cost (IBM)

Keeping this analysis and the facts in mind, this thesis will suggest essential security measures for planning and designing new IT services, not to mention pre-installation services, while applying Zigbee to KISA's preliminary diagnosis of an information protection model that secures stability and reliability before installation. Analysis of Zigbee, a wireless PAN technology, regarding its weaknesses and the related countermeasures, and real-world examples of Zigbee's application to the management of u-City will also be dealt with in my work.

II. METHODOLOGY OF PRELIMINARY DIAGNOSIS OF INFORMATION SECURITY FOR NEW IT SERVICES (KISA)

A. Overview

A methodology for a preliminary diagnosis of information security for new IT services was developed by KISA in 2006 so that new IT service providers can analyze information security weaknesses before operating their services, such as WiBro and VoIP, and develop and apply countermeasures for the weaknesses by themselves.

B. Structure

The methodology is made up of Stages, Tasks and Activities. Stages are categorized based on core activities during the preliminary diagnosis, while Tasks and Activities respectively show the details for accomplishing the goals of each stage and the requirements for each activity. Fig. 2 shows the contents of the three constituents.



Fig. 2 Detailed Activities for the Preliminary Diagnosis Methodology

The activity results relation diagram in Stages describes the sequence and results of the detailed activities defined at each stage. Basically the sequence must be followed but it can be adjusted according to the situation.

‘Reference’ in Activities is a sample from the results of the activities. Revisions can be made to the provided sample according to each service provider’s way of applying the methodology.

C. Process

As can be seen in Fig. 3, this methodology consists of 5 stages, 12 tasks, and 23 activities, along with ‘Security Management Status Checklist’ and ‘Basic DB for Threat/Weakness/Protection Measure’ which are required in order to execute the methodology.

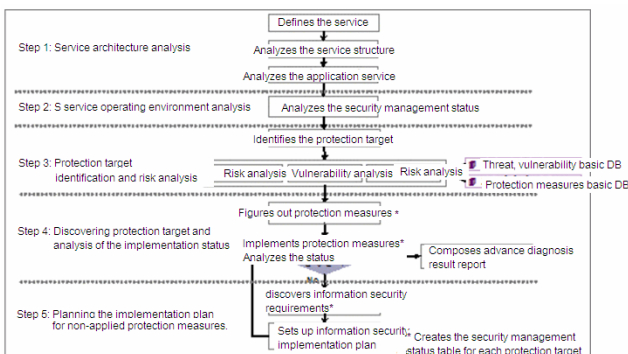


Fig. 3 Preliminary Diagnosis Process

- Stage 1: Analysis of the Service Architecture
Define the concept of the service and determine the service structure and its elements. Identify the applied services and analyze the relationship between the services by evaluating the flow of major data and wired / wireless communication protocols.
- Stage 2: Analysis of Service Operation Environment
Analyze the operation environment of the new IT service with a focus on security management.
- Stage 3: Identification of Targets for Protection and Threat Analysis
Identify potential threats that may influence the confidentiality, perfection and availability of the new service, and deduce and evaluate the relevant weaknesses in analyzing potential threats and their levels for future service installation.

- Stage 4: Deduce Protection Measures and Analyze Execution Status
Establish protection plans from the viewpoints of management, technology and physics based on each protection target and the security management status.
- Stage 5: Prepare Protection Plans for Unprotected Areas
Determine the status of the fields yet to be protected by the suggested protection measures for minimizing threats to the new IT service and set up plans taking into consideration information protection requirements.

III. PRELIMINARY DIAGNOSIS OF U-SERVICE WITH ZIGBEE

A. Overview of Zigbee Technology

Zigbee is the technology of choice for wireless communication between sensors whose priority is less power consumption, despite the slower speed and lower bit rates. The features of Zigbee are as follows:

- Relatively small power consumption (one battery lasts from months to years).
- Ease of use (Bluetooth confuses users with too many functions, while Zigbee has only two modes – active (transmit/receive) and sleep).
- Reasonable price.
- Low cost of installation and maintenance.
- Supports an unlimited number of nodes.
- Simple protocols and their implementation

B. Reservoir Management Service with Zigbee

The reservoir management service with Zigbee allows the customer to keep up to date with the status of water quality, water level and pollution through real-time monitoring via a Zigbee-based preinstalled sensor network. Fig. 4 shows a diagram of the service’s elements and data flow.

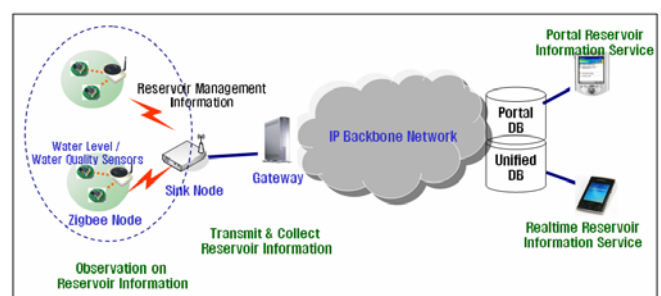


Fig. 4 Service Structure Diagram for u-Reservoir Management Service

C. Analysis of Security Weakness

Including IEEE802.15.4, the Zigbee standards still have unclear definitions of the following with regard to security services. These may not be categorized as critical problems without actual implementation but they must be taken care of before implementation.

- No definition of an out-of-hand method for key configuration: All keys can be configured out-of-hand, but there is a risk of exposing the keys from the initial configuration.
- Dilemma between security and cost: Link keys and network keys should be selected in consideration of safety and cost, which can lead to weaker security.
- No definition of the network participation policy for a new node: Reliability Center does not define the required policies with regard to whether it will allow the network participation of a new node
- Weakness of key distribution for new nodes: No password-based protection during initial key distribution for the nodes that newly participate in the network
- No definition of such cases as: Errors in the security services / Faults occurring during the synchronization of relaying counters / Failure of key synchronization / Policies for key expiration and renewal.

The abovementioned innate weaknesses of Zigbee can result in service threats including information leakage from either Zigbee's wireless communication area or a lack of verification between Zigbee and the Sink nodes.

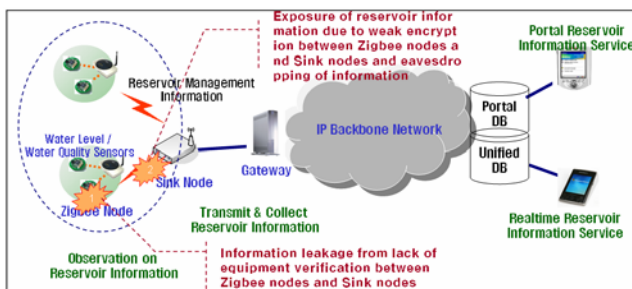


Fig. 5 Potential Threats to the u-Reservoir Service

D. Technical Protection Measures

Through an analysis of the potential threats to each element, the following protection measures can be prepared.

o Banning AES-CTR

AES-CTR, which has no support for message-based verification, cannot help exposing itself to serious threats, which means that it is better not to support AES-CTR in actual application, regardless of the situation.

o Implementing ACK Verification for the Actual Application Stage

Since Zigbee does not offer any verification method for ACK packets, it may fall victim to DoS attacks. Therefore, the application developer must be aware that reliability of communication cannot be secured by ACK packets from Zigbee, and make sure to implement ACK functions for the actual application stage if the need arises, in which case complexity with implementation may increase but there will be greater security.

o Maximum Number of Supported ACL Items

In order to prevent the same keys being used for

communication between different items of equipment, support for the maximum number of ACL items defined in the standards is required.

o Maintaining ACL in the Power Saving Mode

ACL may be re-initialized due to a lack of ACL maintenance in the power saving mode, which may lead to security breaches because the same keys can be used. Therefore, be sure to maintain ACL even in the power saving mode. Also, saving the nonce value when shutting down the equipment normally (turning off power) can be a good countermeasure for nonce reuse vulnerability.

o Nonce Exposure for Received Packets

If one password is used for more than two nodes, vulnerability in the resend protection mechanism from Zigbee may occur due to the existence of the ACL's default items. In other words, the default items of the ACL receive packets from various nodes, but only keep one resend counter for all the nodes. This easily leads to the maximum limit of the counter and nullification of the resend protection mechanism. It is a hardware problem so it may not even be possible to deal with the problem on the hardware itself. In order to overcome such limits, the resend protection mechanism needs to be activated at the application stage, and for this to happen, the resend counter value must be handed over to a higher level of hardware. This kind of countermeasure is not mentioned in the standards. If the application stage becomes aware of the resend counter value, it can reconfigure the maximum limit of the value so that the protection mechanism may be activated without a problem.

o Banning AES-CTR

Implementation of AES-CTR in the standards is optional rather than compulsory. This means that giving up the hardware support for AES-CTR can improve security.

E. Things to take into Consideration for the Installation and Operation of the Service

Based on the aforementioned weaknesses of Zigbee's security services and the related countermeasures, we can take the following points into consideration when implementing the service with Zigbee.

Consideration item of management part is as following.

- Establish security policies about WPAN and Zigbee before setting up the network.
- Run instruction sessions for future Zigbee users to inform them of the potential security threats, as well as basic network security.
- Carry out periodic security evaluation and assessment after setting up the network.
- Maintain the wireless network including WPAN on the same level as the wired network.
- Check if WPAN is available for use outside of the network environment.
- Control the entrance and exit for the network environment.

- If possible, apply an antitheft device for Zigbee equipment and other antitheft measures, if any.
- Be sure to turn the Zigbee equipment off when it is not in use.

Consideration item of technicality part is as following:

- Make revisions to the default configuration of the Zigbee equipment in accordance with the operation environment based on the existing security policies
- Allow the equipment to provide services only within the necessary ranges by configuring the Zigbee equipment's power supply level and others.
- Control the access to the Zigbee equipment with such methods as a password and locks..

Consideration item of operation part is as following:

- Encrypt all communication through Zigbee
- Perform verification among the devices for all and any access.
- Make the password the longest one possible.
- If possible, apply separate security mechanisms to a higher level of Zigbee (i.e.: VPN). This arrangement is needed for highly confidential information.
- Install vaccine and anti-malware software on the Zigbee equipment.
- Periodically check the version of the software / firmware on the Zigbee equipment and update them if newer versions are available.
- If possible, introduce and apply a security system that can effectively protect the Zigbee network.
- The network operator must continuously check security-related technologies regarding Zigbee

IV. CONCLUSION AND FUTURE RESEARCH

More and more people are paying attention to 'ubiquitous computing' that enables communication between humans and non-humans or between non-humans. Research on technological bases for such ubiquitous computing and business with the technologies are actively under way.

However, newly available u-Services in this age of ubiquity are frequently exposed to online crimes including hacking and privacy violation. In order to minimize the damage from such threats, systematic information management and operation is a must, along with the establishment of security systems.

In this respect, this thesis suggests essential security measures for planning and designing new IT services, while applying Zigbee, the wireless PAN technology, to a u-Reservoir management service with Zigbee in order to prove the efficiency of the preliminary diagnosis model for information protection from KISA.

Many services with diverse IT technologies will be available in the near future. And, for the future services to prosper, constant research is needed to improve the diagnosis model from this thesis and to concretize it into a general methodology that can be applied to the services.

REFERENCES

- [1] NIST, SP 800-37-Final, Guide for the Security Certification and Accreditation of Federal Information Systems, 2004. 5.
- [2] Carlos M. Gutierrez, Robert Cresanti, William Jeffrey, NIST Special Publication 800-100, Information Security Handbook: A Guide for Managers, NIST, 2006. 6
- [3] Tom Karygiannis, Les Owens, NIST Special Publication 800-48, Wireless Network Security, NIST, 2002.11
- [4] IBM Systems Science Institute
- [5] Bob Heile, "Emerging standards", ZigBee Alliance, 2004. 10.
- [6] <http://www.zigbee.org>
- [7] TTA WPAN PG304, www.tta.or.kr