Design of Context-Aware based Information Prevention for Digital Signage

Sungmo Jung[1], Younsam Chae[2], Jonghun Shin[2], Uyeol Baek[2] and Seoksoo Kim[3]

[1,3]Department of Multimedia, Hannam University, 306-791 Daejeon, Korea
[2]KPD, 10F Daegu Gyeongbuk Design Center, 701-824 Daegu, Korea
sungmoj@gmail.com, kpd7542007@gmail.com, sskim0123@naver.com

Abstract

Many applications using the Bluetooth technology for the revitalization of smart phones have emerged, and hacking these applications has caused vulnerability of wireless networks. Bluetooth is authenticated through unique address value of each device. However, hackers can attack the information of unique address value in the process. Despite this situation, many people do not know anything about the attack. To prevent this, experts are encouraging to turn off unused network services. However, in their proposed method, many users cannot perform it properly. Therefore, in this paper, a context-aware based algorithm for prevention of Bluetooth device attack was designed so that users have better security options in any situation for digital signage.

Keywords: *Context Aware, Bluetooth Device, Information Prevention*

1. Introduction

In recent years, many Bluetooth-based applications and devices are gaining wide popularity with consumers. The emergence of Smartphone, in particular, has fueled its popularity and development of a variety of contents. Bluetooth's key strength lies in the fact that it is wireless and convenient to use. On the other hand, wireless nature of its technology invites frequent attacks from hackers and the theft of personal information has risen sharply. In light of this, security measures that can prevent Bluetooth device attacks beforehand have become a focal point for many in the industry.

With advancements in sensor networks and digitalization of information, information prevention is increasingly recognized as a new paradigm in digital signage. This ubiquitous technology can efficiently manage machines status, and enables appropriate and effective response to emergency situations through updated information prevention services. The significance of information prevention lies in its precise and convenient provision of digital signage.

This technology has prompted ongoing research on user-centered context-aware systems for the rendering of medical services in accordance with user demands. Information prevention is recognized as a method for flexibly delivering diverse services using sensor network technology.

The characteristics of context information make obtaining precise meaning highly difficult. Substantial volumes of data are required to understand user intentions and situations. Furthermore, digital signage-related services require precision. In existing research that focuses on digital signage systems in ubiquitous computing environments, context

[3] Corresponding Author

information is classified and defined using collective categorization. These categories are developed particularly to present business models or systems that provide and confirm specific information over a preset scenario using mobile devices.

There are numerous researches that are taking places around the world to reduce the vulnerability against attacks and many experts recommend that unused network services be turned off to minimize the risk of attacks. Despite its recommendation, many users are either unable to perform properly or faced with inconvenience of setting the device every time. Also, some users are hesitant to turn off Bluetooth. Thus, in this paper, through the recognition of users' location, time, and other elements, we designed the algorithm so that Bluetooth setting is changed accordingly to given situations and subsequently, minimize the damage from attacks.

2. Related Works

2.1. Bluetooth Network Architecture

Bluetooth is an open, wireless technology standard for exchanging data over short distances and its specifications are developed by the Bluetooth Special Interest Group (SIG) [1]. Unlike other wireless network, its operation is based on frequency hopping sequence that hops 1,600 times per second from ISM 2.4 GHz short-range radio frequency band. Its channel has 1MHz bandwidth and to avoid interference with other devices, its frequency range from 2MHz to 3.5MHz with a total of 79 channels and transmits via frame.

Bluetooth connection is piconet based and the technology allows for one master device to interconnect with up to seven slave devices [2]. Master and slave device can communicate 1:1 but communication between slave devices is not possible. When a number of piconets come together, it can be expanded to form Scatternet and the structure is shown below.

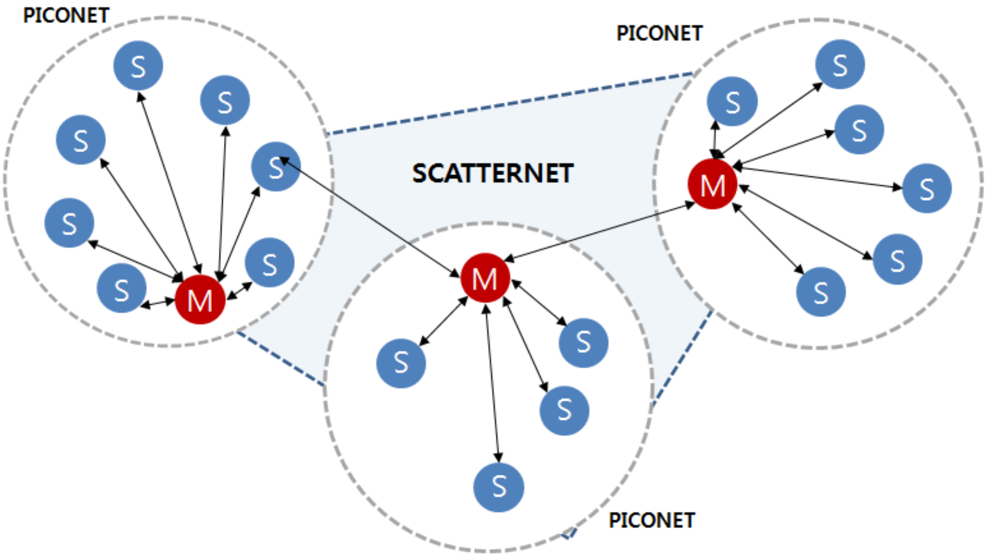

Figure 1. Bluetooth Piconet & Scatternet

2.2. Bluetooth Vulnerabilities and Attacks

Bluetooth's vulnerabilities include possible exposure of PIN (Personal Identification Number), eavesdropping, weakness in encryption, location tracking and MITM [3, 4, 5].

Three of the most prevalent attacks are Bluejacking, Bluesnarfing, and BlueBugging and their main features are shown on the following table.

Table 1. Bluetooth Attacks

Type	Feature
Bluejacking	Sends anonymous spam mail but has low security risk.
Bluesnarfing	Unauthorized access of information to device’s address book, calendar, mails, and others.
BlueBugging	Unauthorized access and direct command of devices without the user’s knowledge

2.3. Bluetooth Device

As shown on Table 2 below, the range of Bluetooth is largely divided into three classes and its classes are determined by a power level and an operating range [6]. Most of Bluetooth devices used by users belong to Class 2 and devices that required long operating range such as Bluetooth AP and dongle belong to Class 1. As Class 3 is limited by the short range, it is infrequently used. This paper has developed an algorithm for devices’ environment applicable to that of Class 2.

Table 2. Bluetooth Device Class

Type	Power Level	Operating Range
Class 1	100mW	90~100m
Class 2	2.5mW	10~20m
Class 3	1mW	1~10m

2.4. Bluetooth Security Mechanism

Bluetooth security mechanism has four security modes that take account of three security elements, consisting of certification, confidentiality, and permission [2]. Only one security mode can be set to devices. That is, duplicated mode is not possible.

Table 3. Security Mode

Type	Feature
Security Mode 1	Non-secure Mode
Security Mode 2	Security Mode of Service Level
Security Mode 3	Security Mode of Link Level
Security Mode 4	Enhanced Mode of Security Mode2

Security Mode 1 is a non-secure mode where it does not undergo any security procedures. It is easily exposed to hacker's attacks and as such, it should be used only in a safe location.

Security Mode 2, initiates security procedures after the L2CAP (Logical Link Control and Adaptation Protocol)'s channel is established. Through a security manager, it controls access to services or devices and maintains security policy in accordance with requests.

Security Mode 3, on the other hand, initiates security procedures before the channel is established. It follows the internal security mechanism and undergoes certification and encryption process with other devices.

Security Mode 4 is similar to Mode 2 except that SSP (Secure Simple Pairing) is applied, simplifying the pairing process and strengthening the security function.

By applying the appropriate security mode taking into consideration of users' location and time, these security modes seek to minimize the damage caused by attacks from hackers.

2.5. Context-Aware

Context awareness is generally defined as the detection of "conditions related to existence or occurrence of something." Many scholars have defined context through various examples. Schilit classified context into three categories [7]:

- computing context, which includes network connection status, communication bandwidth, printers, displays, and workstations and peripherals;
- user context, which comprises user profiles, locations, people around a given area, etc.; and
- physical context, which covers lighting, noise level, traffic condition, temperature, etc.
- Chen and Kotz stated that "time" is an essential factor that makes up context and suggested a fourth category [8]:
- time context, which includes time, week, month, season, etc.

Context-aware technology is that which is used to acquire accurate context information through visualization, categorization, and integration [9]. Classifying the categories of basic context information is crucial for performing context-aware processes, and all contexts can be recognized within the range of their categories. Tags have recently been used to interpret context, but these are not widely adopted because they require very broad standards while having very narrow development ranges. The use of information classification standards is said to be the most important aspect in processing context information. A study adopted 5W1H for processing such information [10].

3. CA-based Algorithm for Information Prevention

3.1. Suggested CAIP Algorithm

Suggested CAIP (Context-Aware based Information Prevention) algorithm in this paper uses context information and incorporates the use of RBR and CBR and sets Bluetooth environment such as user's location and time, security mode and others that are deemed safe. After the setting and sensing of context information by user's device sensors, it is largely divided into two categories: when there is a request by other devices and when there is no request.

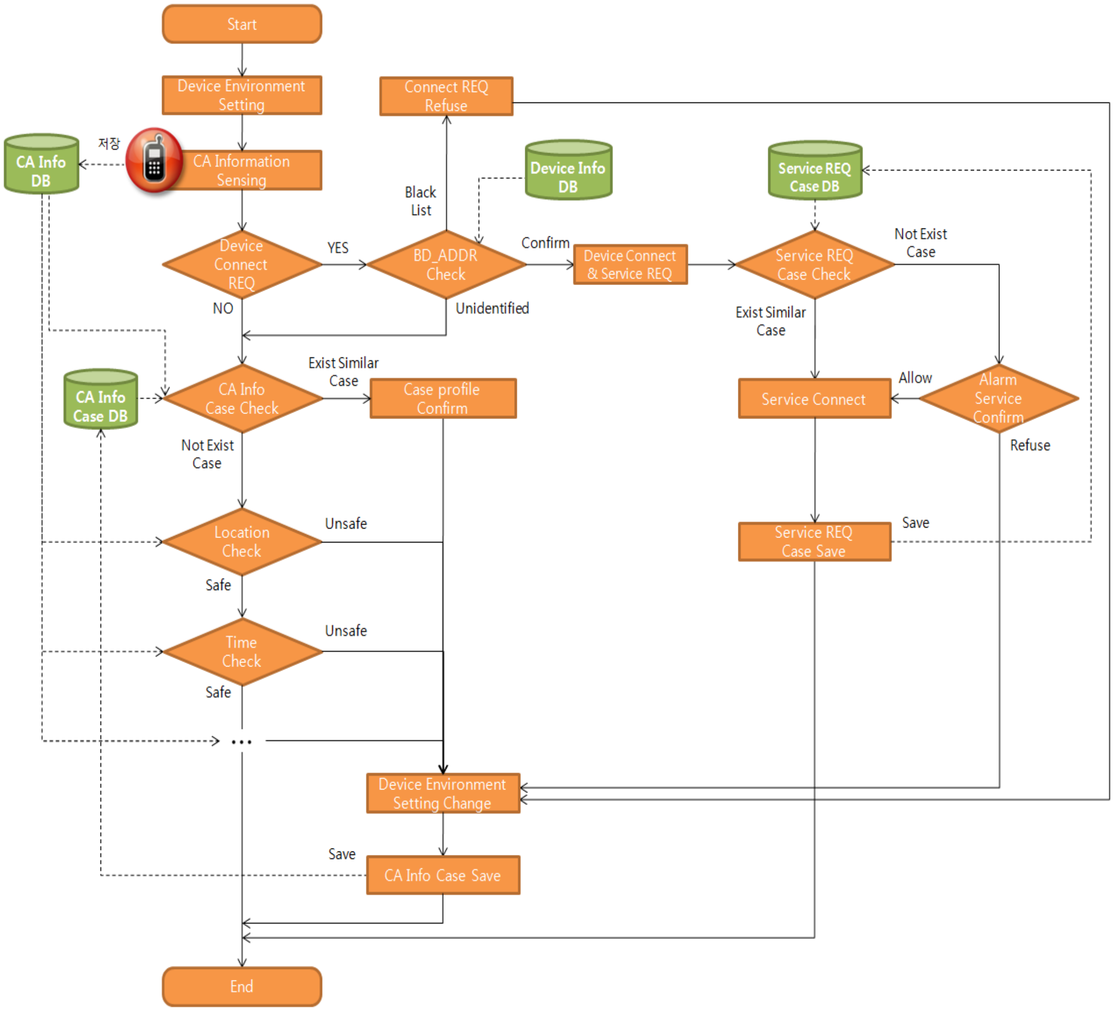

Figure 2. Suggested CAIP Algorithm Structure

3.2. Scenario

In this scenario, users taking account of information's level of importance, a number of people, and location's characteristics, classify and set as either safe location or unsafe location. Similarly, users classify time as safe time or unsafe time corresponding with aforesaid location's characteristics.

For instance, if the user determines that the location is a restaurant, as many more patrons will frequent the restaurant during breakfast, lunch, and dinner hours, these hours will be determined to be unsafe as hackers will be prone to attack during these hours. For this scenario, employed device is a Smartphone with the signal strength of 10 to 100 meter and the security is set to Mode 1, which is non-secure.

Table 4. Basic Setting of Device

Type	Contents
Used Device	Smart Phone
Signal Strength	Within 10~100m (Class2)
Device Security Mode	Security Mode1(non-secure)

The process for scenario is as follows.

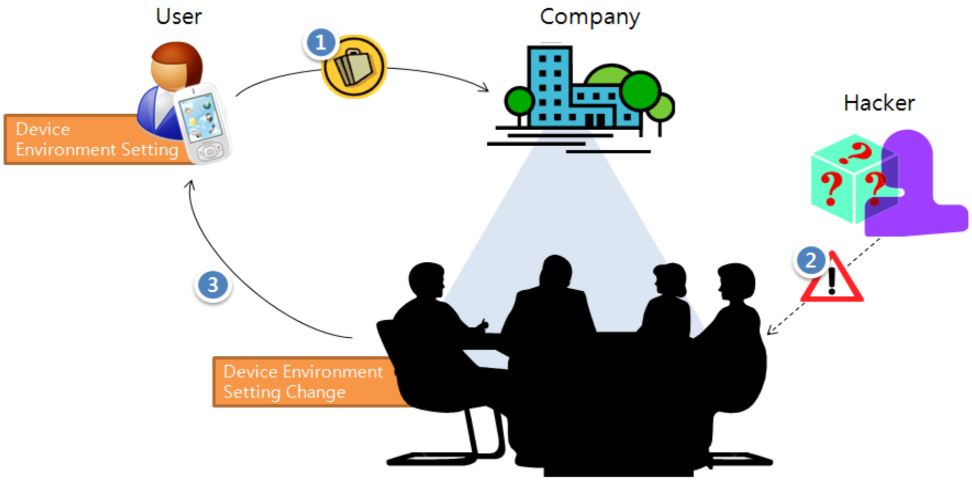

Figure 3. Scenario Process

① A user who has a business meeting everyday with concerns for possible leak of company’s sensitive information sets his Smartphone’s Bluetooth setting as unsafe location, meeting time as 30 minutes, and Security Mode 3, before arriving at the company.

② The user enters a conference room to participate in the meeting. At that moment, his Smartphone utilizes GPS, sensor, surrounding environment, and others and checks whether there are similar cases in the past with the current situation. If not, via currently sensed coordinate points, determines that current location is a conference room within the company and temporarily terminates the Bluetooth connection. When there is a similar case in the future, it will undergo a checking of the past cases and set the environment accordingly.

③ When the meeting is over, the user leaves the conference room and at that time, the Bluetooth setting will be reset as the conditions – leaving the conference room or meeting time has expired – is met. In turn, the security mode is changed to low and connection is now possible again.

4. Conclusion

For Bluetooth device security algorithm based on context-aware that was recommended to users to reduce the security risk associated with using Bluetooth devices, it was designed to protect from attacks by changing the Bluetooth setting through the recognition of users' relevant conditions and surroundings. We examined one possible scenario considering location and time.

A recent trend is the identification of approaches that enable real-time response to digital signage situations. Information prevention uses wireless telecommunication to provide digital signage services to people without being constrained by distance limitations. Some mobile devices are equipped with sensors that can check the machine status. However, relying only on the digital signage-related data from mobile devices may be an insufficient approach because such devices have limitations that may cause misuses. Users may also be confused when warning events other than those detected by sensors occur. For these reasons, various studies have been conducted to collect more diverse information for the use of personnel. Some of the technologies developed include sensors and mobile devices that collect more concrete data on medical conditions.

With the recent popularity of Smartphone and subsequent increase of contents that use Bluetooth technology, it has easier for users to use the technology anytime and anywhere. Conversely, associated risks with using such technology have risen as well. Thus, it is important to propose suggestions that can reduce the security risk and various educations and campaigns should be in placed to make users aware of the risk. This paper has limited the values to location and time but there are other values that can be obtained from various sensors and surroundings and apply them with other security and context-aware technology to further the study from different approaches.

Acknowledgement

This paper has been supported by the Technology Innovation program of MKE. [10042844, Development of Digital Signage Design applying Augmented Reality Technology].

References

[1] The Bluetooth SIG, About the Bluetooth SIG, http://www.bluetooth.com.

[2] K. Scarfone and J. Padgette, "Guide to Bluetooth Security", NIST Special Publication, **(2008)**, pp. 800-121.

[3] Y. Shaked and A. Wool, "Cracking the Bluetooth PIN", Proceedings of the 3rd international conference on Mobile systems, applications, and services, **(2005)**, pp. 39-50.

[4] K. Hypponen and K. Haataja, "Nino" Man-In-The-Middle Attack on Bluetooth Secure Simple Pairing", Proceedings of the IEEE Third International Conference in Central Asia on Internet, The Next Generation of Mobile, Wireless and Optical Communications Networks (ICI'2007), Tashkent, Uzbekistan, **(2007)**, pp. 26-28.

[5] S. Lee, H. A. Latchman and B. J. Park, "ELRR – Enhanced Limited Round Robin Mechanism using Priority Policy over Bluetooth Networks", International Journal of Advanced Science and Technology, vol. 6, **(2009)**, pp. 69-78.

[6] G. Legg, "The Bluejacking, Bluesnarfing, Bluebugging Blues: Bluetooth Faces Perception of Vulnerability in Wireless Net", Design Line, **(2007)**.

[7] H. Lee and J. Kwon, "Combining Context-Awareness with Wearable Computing for Emotion-based Contents Service", International Journal of Advanced Science and Technology, vol. 22, **(2010)**, pp. 13-24.

[8] G. Chen and D. Kotz, “A survey of context-aware mobile computing research”, Dartmouth computer science technical report, TR2000-381, Dartmouth College, Hanover, N.H, USA, **(2000)**.

[9] H. Liberma and T. Selker, “Out of context: Computer systems that adapts to, and learn from, context”, IBM systems journal, vol. 39, no. 3&4, **(2000)**, pp. 617-632.

[10] A. Idhammad, A. Abdali and P. Bussy, “Numerical: Simulation of the Process of Bone Remodeling in the Context of Damaged Elastic”, International Journal of Advanced Science and Technology, vol. 37, **(2011)**, pp. 87-98.

Authors

Sungmo Jung received his B.S. degree in Department of Multimedia Engineering from Hannam University, Daejoen, Korea in 2008, and the M.S. degree in Department of Multimedia Engineering from Hannam University, Daejeon, Korea in 2010. Now, he completed in course of the Ph.D’s degree in Multimedia Engineering from Hannam University. He is a member of IEEE and IEEE Communication Society. He has the international license CEH(Certified Ethical Hacker) for network penetration test. His research interests include Machine-to-Machine Architecture, Multimedia Communications, and Network Security.

Younsam Chae conferred academic degree on 2006 from Daegu University, with Degree of Ph.D. Conferred academic degree on 2001 from Daegu University, with Degree of M.A. Graduated on 1995 from College of Arts(Department of Crafts), Daegu University, with Degree of Bachelor of Fine Art. He is CEO & designer of KPD.co., ltd. His research interests include Technique of Casting and Holistic Arts Healing. He is a member of The Korea Society of Art&Design, MMC and KODFA.

Jonghun Shin received a B.S degree in Department of Industrial Design from Daegu University. He has been working as a Chief designer at KPD Company from 2010 to present. His research interests include Industrial Design and Digital Sinage.

Uyeol Baek received a B.S. degree in Department of Industrial Design from Keimyung University. He has been working as a product designer at KPD Company from 2006 to present. His research interests include Industrial Design and Digital Signage.

Seoksoo Kim received a B.S. degree in Computer Engineering from Kyungnam University, Korea, 1989 and M.S. degree in Information Engineering from Sungkyun-kwan University, Korea, 1991 and Ph.D. degree in Information Engineering from Sungkyun-kwan University, Korea, 2002. In 2003, he joined the faculty of Hannam University, Korea, where he is currently a professor in the Department of Multimedia Engineering. His research interests include multimedia communication systems, distance learning, multimedia authoring, telemedicine, multimedia programming, computer networking, and information security. He is a member of KCA, KICS, KIMICS, KIPS, KMS, and DCS. He is editor-in-chief of IJMUE.