Design of Context-Aware based Information Prevention

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

[1, *] 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. 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.

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[1].

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.

* Corresponding author

2 CA-based Algorithm for Information Prevention

2.1 Suggested CAIP Algorithm

Suggested CAIP(Context-Aware based Information Prevention) algorithm in this paper uses context information and incorporates the use of RBR[2] and CBR[3] 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.

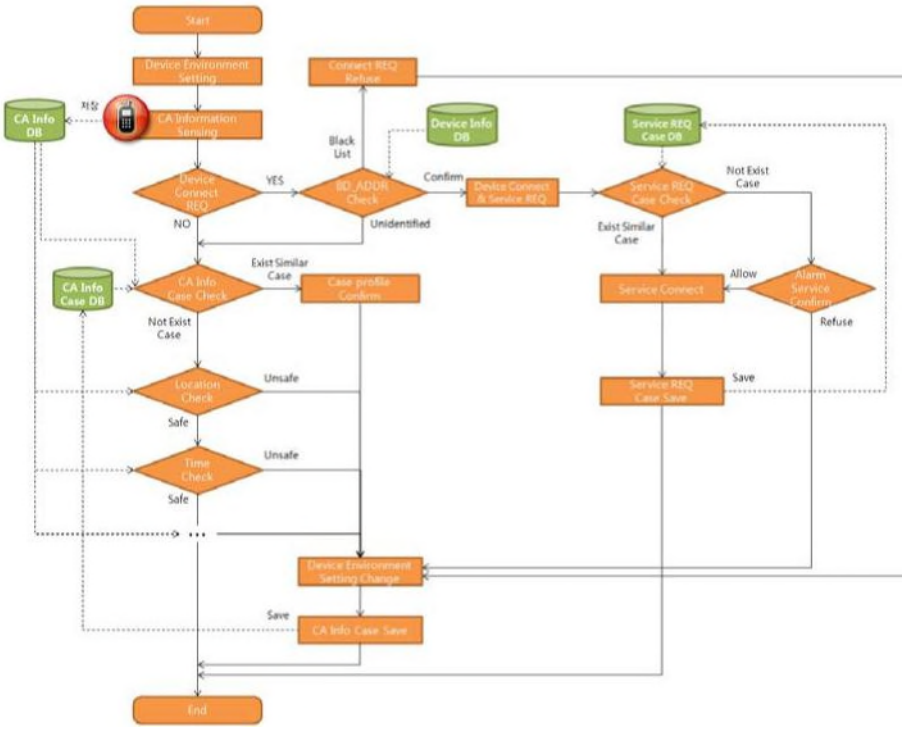

Fig. 1. Suggested CAIP Algorithm Structure

2.2 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 1. 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.

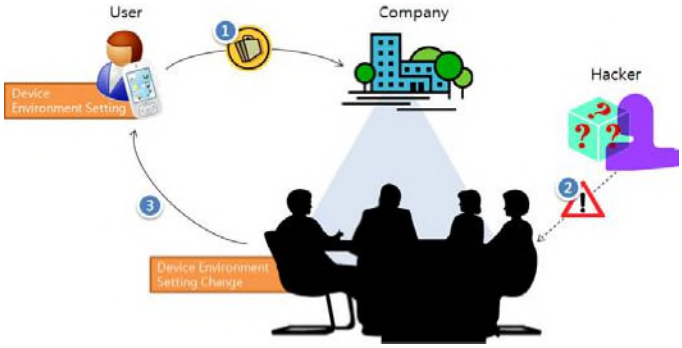

Fig. 3. Scenario Process

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.

3 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.

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. Sunguk Lee, Haniph A. Latchman and Byungjoo Park: ELRR – Enhanced Limited Round Robin Mechanism using Priority Policy over Bluetooth Networks, International Journal of Advanced Science and Technology, Vol.6, pp.69--78 (2009)
2. Haesung Lee, Joonhee Kwon: Combining Context-Awareness with Wearable Computing for Emotion-based Contents Service, International Journal of Advanced Science and Technology, Vol.22, pp.13--24 (2010)
3. A. Idhammad, A. Abdali and P. BussyNumerical: Simulation of the Process of Bone Remodeling in the Context of Damaged Elastic, International Journal of Advanced Science and Technology, Vol.37, pp.87--98 (2011)