Survey the Interactive Broadcast Management System in Smart Devices

Hye-ri Kim1,*, Hyun-mi Jang1, Kyong-jin Kim1, Ji-young Kim1, Seng-phil Hong1,*, Dongyul Roh1, Woongjae Lee2, Jin-Gwang Koh3 and Min Kyoungsik4

1Sungshin Women’s University, 2Seoul Women’s University
3Sunchon National University, 4Korea Internet & Security Agency
E-mail: {hrkim, nicemiya, kyongjin, jybara, philhong, rohdory}@sungshin.ac.kr, wjlee@swu.ac.kr, kjg@scnu.ac.kr, kyoungsik@kisa.or.kr
*First author, **Corresponding author

Abstract

Smart spaces are dynamic environments for sharing information. People use phones to store and contact personal information and increasingly they have high-speed Internet connections. The smartphone has become a powerful computer in its own hands. In addition, smartphones are now being widely used in interactive broadcast systems. But this makes these attractive devices to challenges. The key challenges for smart spaces include security and interoperability between heterogeneous devices. To solve this problem, we survey these trends and propose the Interactive Broadcast Management System Architecture.

Keywords: smart device, information security, privacy, interactive broadcast

1. Introduction

The worldwide smart connected device market, meaning smartphone, tablets, and PCs combined, grow up every year. The smart device shipments are on track to top 2.1 billion units in 2016, with a market value of $796.7 billion worldwide[1]. It also forecasts a continual decline in PC market share, dropping from 39.1% of the smart connected device market in 2010 to 19.9% by 2016[1]. The proliferation of smart devices and the users through a variety of services to increase convergence is changing computing paradigm. In addition, big data, social networks, and new services such as interactive broadcast with smart devices market is expected to grow even more.

Figure 1. Worldwide Smart Connected Device Shipments 2010-2016 [1]
The proliferation of smart devices and mobile convergence services provide convenience to the user in a variety of fields, but devices in smart spaces are vulnerable to several security attacks[2]. The amount of mobile vulnerabilities continues to rise.

In this work we survey these trends and propose a model secure interactive broadcast management system in smart devices environment. The paper is organized as follows: Section 2 gives related academic work, Section 3 describes the problem statement, Section 4 describes Interactive Broadcast Management System, and Section 5 prototyping. Finally, conclusions and future work close the paper.

2. Related Work

Security is a major problem in smart spaces. With personal devices, the availability of services and privacy of information may be more in the focus. In public smart spaces, the critical issue is to find authentic services and protect ourselves from malicious input[3].

Antti Evesti[4] presents a micro-architecture for security adaptation security in smart spaces. They presented the taxonomy of context information for security. The taxonomy contains concepts describing: the usage of smart spaces application, the smart space itself, and the physical features of the environment.

Henman Pathak[5] identifies the major issues related with the security of mobile agents and presents an architecture which is hybrid in nature i.e. uses different approaches and techniques to solve the security related problems of mobile agents. Proposed architecture is centralized at one level and distributed at other. In this paper, we take note that they regard political solutions and suggest Security Manager(SM) and Policy Manager(PM)

Finally, Jose M. del Alamo[6] describes a framework for identity management in mobile services that empowers users to govern the use and release of their personal information. The framework is based on a brokering approach that intermediates between the mobile operator’s information services and the Web service providers.

In these papers, we take note that they regard technical aspects and political aspects. And they express using XML. Heterogeneity of devices and interoperability solutions in smart spaces imply versatile protocols and messaging formats[7]. Processing and parsing of input and XML documents has been a major source of security problems and, therefore, attention should be given for reliable parsing implementations[8]. This issue may be more critical in smart spaces as many embedded devices do not have direct Internet access for security patches. XML compression can be considered as key to some of the issues regarding mobile computing[9,10].

3. Problem Statement

The following table relates to the analysis on the vulnerabilities of personal/sensitive information based on the life cycle and type in smart devices.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Collection</th>
<th>Storage &amp; Transmission</th>
<th>Use/Sharing</th>
<th>Destruction</th>
</tr>
</thead>
</table>
| Human         | - Leakage/exposure of personal information due to the lack of awareness towards the management of personal information among the businesses/enterprises entrusted to handle and manage the personal information  
- Inadequate policies and enterprise-wide management systems for personal information in mobile environment |
|              | - Leakage/exposure of personal |
|              | - Risk of the external leakage of personal |
|              | - Absolute lack of clarity of the responsible |
|              | - Leakage of personal |
4. Interactive Broadcast Management System

4.1. Interactive Broadcast Management Architecture

![Interactive Broadcast Management System Architecture](image)

Figure 2. Interactive Broadcast Management System Architecture
The following Figure 2 is architecture which can be shown when registering, using, and transferring contents with smart device that users have. Smarter Mediator should complete user registration based on user and equipment information to make User A register, use, and share contents. If User A whose registration is completed wants to upload contents, the Smarter Mediator gets to collect contents and their additional information (registration date, contents type, size) based on user registration information. At this moment, the policy bank in the Smarter Mediator gets to give security levels to contents that User A requested it to register after checking their violence, sexuality, and charges finally. If User A requests the Smarter Mediator to transfer contents to User B, User B gets to receive the same security level with that of User A. However, if User C whose security level is lower requests the Smarter Mediator to share User B’s content, sharing is impossible due to conflicts between contents levels.

Based on our proposed architecture described in the previous section, we present using flowchart for the delegate and the conflict mechanism. The key point is to prevent contents from being leaked by third parties, and to minimize the damage. It is also possible to process errors and other exception handling tasks from causing the process to terminate.

![Flowchart Image](#)

**Figure 3. Delegation and Conflict Management Flowchart**
The defined rule in our model is built on machine-readable language, and thus it can convert a XML format.

![Diagram of Parsing Policy Bank]

**Figure 4.** Example of Defined Rule for Delegation using XML

### 5. Prototyping

To realize the proposed architecture, it is implemented work as an Interactive Broadcast Management System Architecture-based in the form of interface. This prototype has been developed using JAVA language, JSP and XML. As shown in Figure.5, system administrator could manage the contents delegation. The administrator could see detailed information of the users who send or receive the contents. Also contents’ security level can be shown. In Figure.6, the administrator can adjust policy priority when the policy conflicts.
6. Conclusion and Future Work

In this paper, we discuss the architecture for secure interactive broadcast management system in smart devices. It consists of 3 parts: Contents Priority Handling Manager, Complicit Manager, and Delegate Manager. This enables prevent contents from being leaked by third parties, and to minimize the damage. It is also possible to process errors and other exception handling tasks from causing the process to terminate. The future study will continue to focus the design and implement of our suggested model and we will expand to new devices and environments.

Acknowledgements

This research was supported by the MSIP(Ministry of Science, ICT & Future Planning), Korea, under the support program for producing bi-direction TV programs supervised by the KISA(Korea Internet & Security Agency).

References