International Journal of Smart Home
Vol.8, No.1 (2014), pp.139-144
http://dx.doi.org/10.14257/ijsh.2014.8.1.15

Survey the Interactive Broadcast Management System in Smart Devices

Hye-ri Kim[1,*], Hyun-mi Jang[1], Kyong-jin Kim[1], Ji-young Kim[1], Seng-phil Hong[1,**], Dongyul Roh[1], Woongjae Lee[2], Jin-Gwang Koh[3] and Min Kyoungsik[4]

[1]Sungshin Women's University, [2]Seoul Women's University
[3]Sunchon National University, [4]Korea 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.

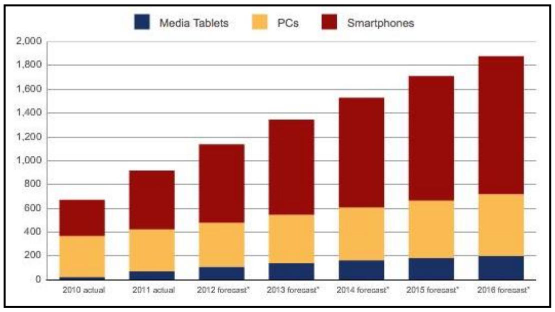


Figure 1. Worldwide Smart Connected Device Shipments 2010-2016 [1]

ISSN: 1975-4094 IJSH

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 1. Vulnerabilities of Personal/Sensitive Information Smart Devices

	Collection	Storage & Transmission	Use/Sharing	Destruction
Management/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

		information due to the synchronization of personal applications (apps)	information due to the absence of business-purpose terminal manager and inadequate management of terminal	for billing which results from the personalized use of business-purpose terminal	information stored on the terminal in case that the terminal is exchanged or lost
Technical	Mobile Device	- Leakage of personal information during the execution of malicious codes due to the installation of harmful applications(apps)			
		- Leakage of personal information due to the use of common login ID and the absence of authentication	- Spread of malicious codes in terminal due to the connection to external PC		- Deformation and destruction of personal information in the terminal from any third party due to the inadequate management of remote control
			- Leakage of important personal information, such as resident registration number stored on the mobile terminal, due to the temporary processing, etc.	- Leakage・exposure of personal information by inducing the App download or intercepting the URL through the QR code, thus causing the connection to malicious link	
	Network	- Risk of the leakage/exposure of personal information transmitted via various routes of wireless connection - Leakage of personal information during the transmission and reception of personal information through mobile communication network from mobile terminal			
	Server	- Leakage of personal information due to the inadequate protection measures for the mobile terminal management server			
			- Difficulty of tracking the misuse and abuse of personal information which result from the joint use of business-purpose terminal	- Insufficient management of the personal information retention period and lack of specific procedures for the destruction of personal information	

4. Interactive Broadcast Management System

4.1. Interactive Broadcast Management Architecture

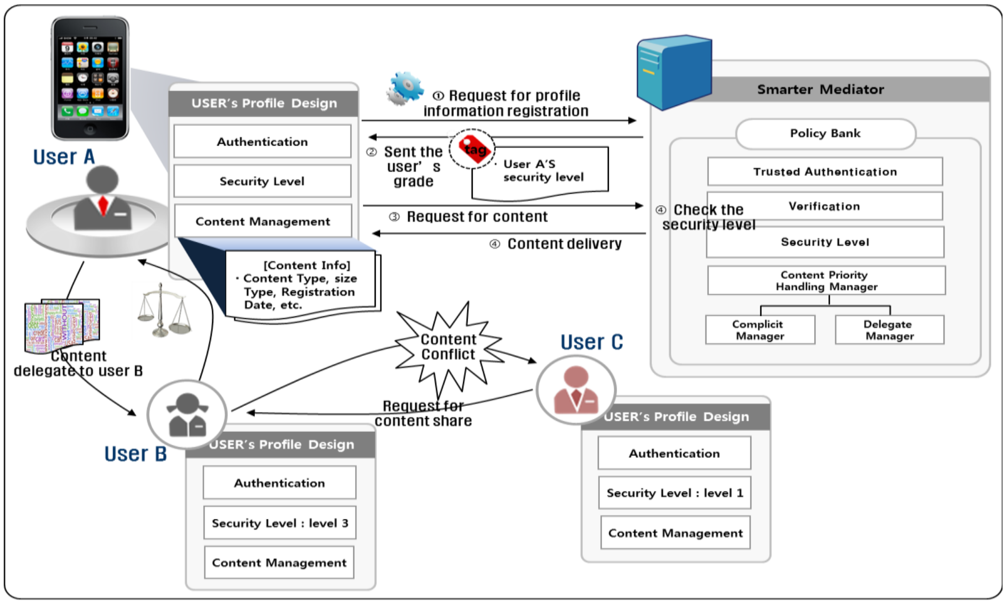
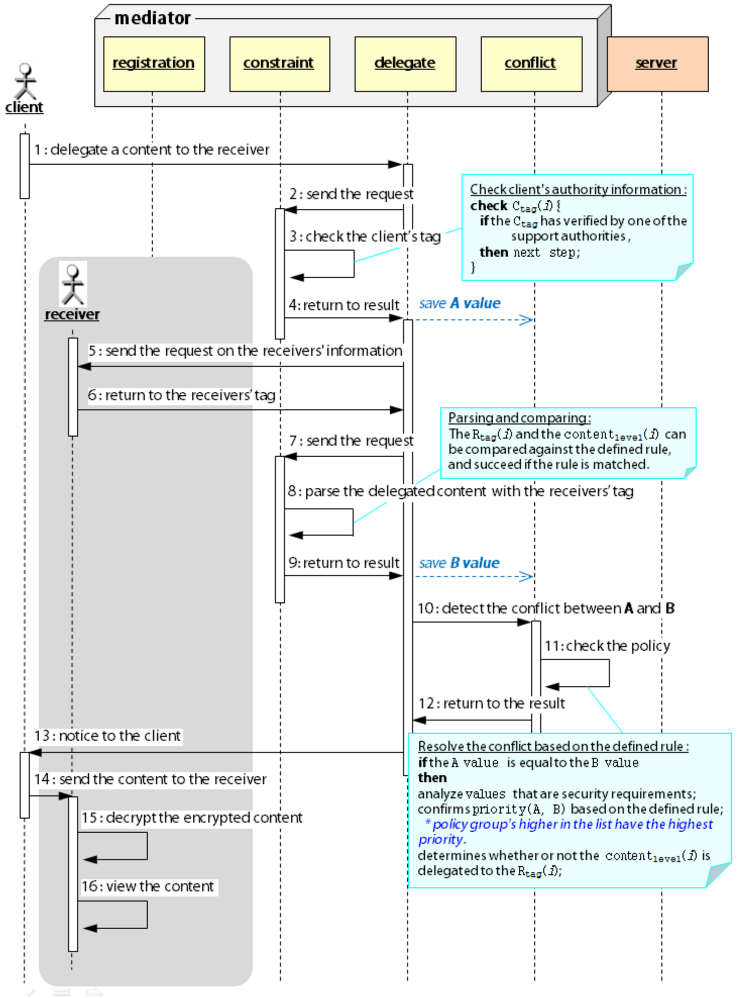


Figure 2. Interactive Broadcast Management System Architecture

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.


mediator
registration
constraint
delegate
conflict
server
client
receiver
1 : delegate a content to the receiver
2 : send the request
3 : check the client's tag
4 : return to result
save A value
5 : send the request on the receivers' information
6 : return to the receivers' tag
7 : send the request
8 : parse the delegated content with the receivers' tag
9 : return to result
save B value
10 : detect the conflict between A and B
11 : check the policy
12 : return to the result
13 : notice to the client
14 : send the content to the receiver
15 : decrypt the encrypted content
16 : view the content

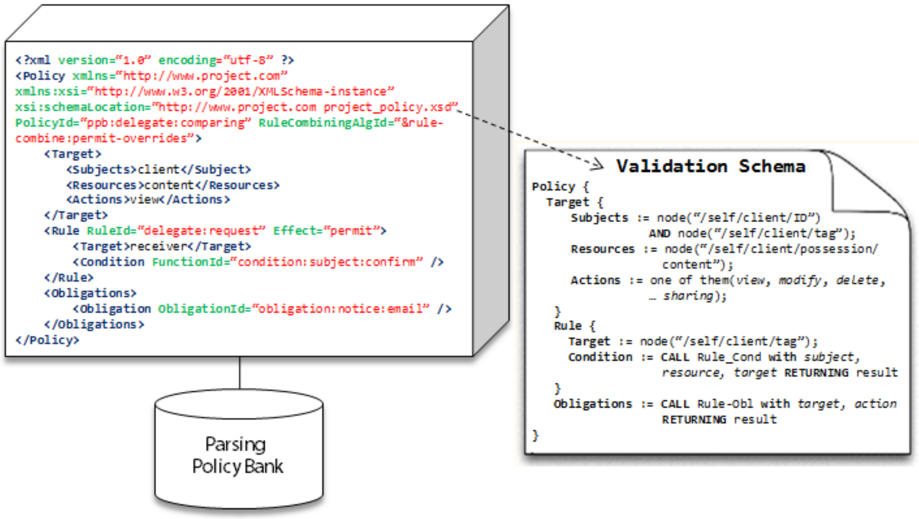
Check client's authority information :
```
check C_tag(i) {
  if the C_tag has verified by one of the
        support authorities ,
  then next step;
}
```

Parsing and comparing:
The $R_{tag}(i)$ and the $content_{level}(i)$ can be compared against the defined rule, and succeed if the rule is matched.

Resolve the conflict based on the defined rule :
```
if the A value is equal to the B value
then
analyze values that are security requirements;
confirms priority(A, B) based on the defined rule;
  * policy group's higher in the list have the highest
priority.
determines whether or not the content_level(i) is
delegated to the R_tag(i);
```

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.



```
<?xml version="1.0" encoding="utf-8" ?>
<Policy xmlns="http://www.project.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.project.com project_policy.xsd"
PolicyId="ppb:delegate:comparing" RuleCombiningAlgId="&rule-
combine:permit-overrides">
    <Target>
       <Subjects>client</Subject>
       <Resources>content</Resources>
       <Actions>view</Actions>
    </Target>
    <Rule RuleId="delegate:request" Effect="permit">
        <Target>receiver</Target>
        <Condition FunctionId="condition:subject:confirm" />
    </Rule>
    <Obligations>
        <Obligation ObligationId="obligation:notice:email" />
    </Obligations>
</Policy>
```

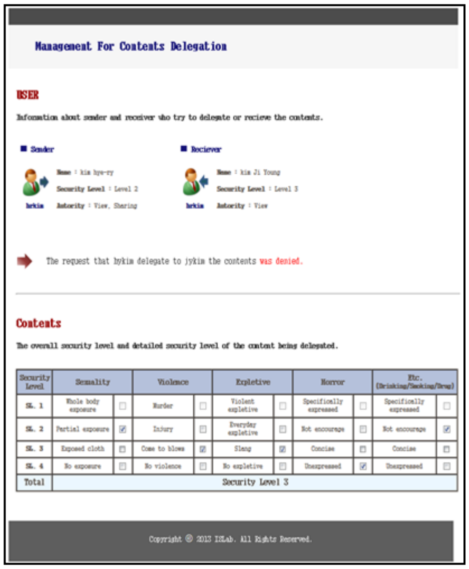
Validation Schema

```
Policy {
  Target {
     Subjects := node("/self/client/ID")
                 AND node("/self/client/tag");
     Resources := node("/self/client/possession/
                   content");
     Actions := one of them(view, modify, delete,
                 … sharing);
   }
   Rule {
     Target := node("/self/client/tag");
     Condition := CALL Rule_Cond with subject,
                   resource, target RETURNING result
   }
   Obligations := CALL Rule-Obl with target, action
                   RETURNING result
}
```

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.



Management For Contents Delegation

USER

Infomation about sender and receiver who try to delegate or recieve the contents.

■ Sender

Name : kim hye-ry
Security Level : Level 2
Autority : View, Sharing

hrkim

■ Reciever

Name : kim Ji Young
Security Level : Level 3
Autority : View

hrkim

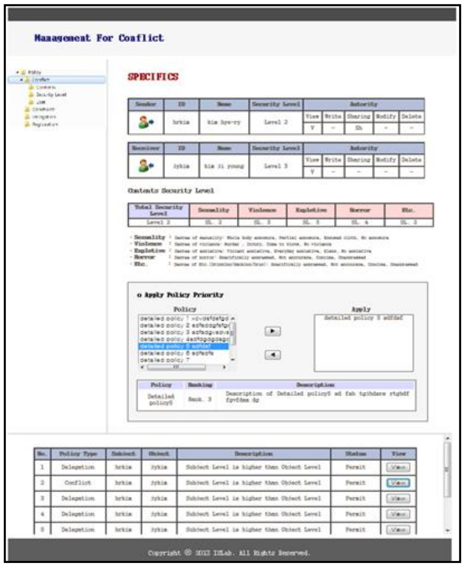
The request that hykim delegate to jykim the contents was denied.

Contents

The overall security level and detailed security level of the content being delegated.

Security Level	Sexuality		Violence		Expletive		Horror		Etc. (Drinking/Smoking/Drug)	
SL. 1	Whole body exposure	□	Murder	□	Violent expletive	□	Specifically expressed	□	Specifically expressed	□
SL. 2	Partial exposure	☑	Injury	□	Everyday expletive	□	Not encourage	□	Not encourage	☑
SL. 3	Exposed cloth	□	Come to blows	☑	Slang	☑	Concise	□	Concise	□
SL. 4	No exposure	□	No violence	□	No expletive	□	Unexpressed	☑	Unexpressed	□
Total	Security Level 3									

Copyright © 2013 ISLab. All Rights Reserved.



Management For Conflict

SPECIFICS

Sender	ID	Name	Security Level	Autority				
				View	Write	Sharing	Modify	Delete
	hrkim	kim hye-ry	Level 2	V	-	Sh	-	-

Receiver	ID	Name	Security Level	Autority				
				View	Write	Sharing	Modify	Delete
	jykim	kim Ji young	Level 3	V	-	-	-	-

Contents Security Level

Total Security Level	Sexuality	Violence	Expletive	Horror	Etc.
Level 2	SL. 2	SL. 3	SL. 3	SL. 4	SL. 2

- Sexuality : Degree of sexuality: Whole body exposure, Partial exposure, Exposed cloth, No exposure
- Violence : Degree of violence: Murder , Injury, Come to blows, No violence
- Expletive : Degree of expletive: Violent expletive, Everyday expletive, Slang, No expletive
- Horror : Degree of horror: Specifically expressed, Not encourage, Concise, Unexpressed
- Etc. : Degree of Etc.(Drinking/Smoking/Drug): Specifically expressed, Not encourage, Concise, Unexpressed

o Apply Policy Priority

Policy

detailed policy 1 xdvdefdefgd
detailed policy 2 edfedgfefgr
detailed policy 3 edfedgvedva
detailed policy dedfdgdgdegd
detailed policy 5 adfdaf
detailed policy 6 edfedfe
detailed policy 7

Apply

detailed policy 5 adfdaf

Policy	Ranking	Description
Detailed policy5	Rank. 3	Description of Detailed policy5 ad fah tgihdare rtgbdf fgvfdea dg

No.	Policy Type	Subject	Object	Description	Status	View
1	Delegation	hrkim	jykim	Subject Level is higher than Object Level	Permit	View
2	Conflict	hrkim	jykim	Subject Level is higher than Object Level	Permit	View
3	Delegation	hrkim	jykim	Subject Level is higher than Object Level	Permit	View
4	Delegation	hrkim	jykim	Subject Level is higher than Object Level	Permit	View
5	Delegation	hrkim	jykim	Subject Level is higher than Object Level	Permit	View

Copyright © 2013 ISLab. All Rights Reserved.

Figure 5. Management For Contents Delegation

Figure 6. Management For Conflict

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 is 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

[1] Worldwide Smart Connected Device Shipments 2010~2017, IDC, **(2013)**.

[2] Internet Security Threat Report 2013, Symantec, **(2013)**.

[3] J. Suomalainen, P. Hyttinen and P. Tarvainen, “Secure information sharing between heterogeneous embedded devices”, ECSA '10 Proceedings of the Fourth European Conference on Software Architecture, **(2010)**.

[4] A. Evesti and S. Pantsar-Syväniemi, “Towards micro architecture for security adaptation”, ECSA '10 Proceedings of the Fourth European Conference on Software Architecture: Companion, **(2010)**, pp. 181-188.

[5] H. Pathak, “Hybrid Security Architecture(HAS) for Secure Execution of Mobile Agents”, ICCCS’11, India, **(2011)** February 12-14.

[6] J. M. del Alamo, A. M. Fernandez, R. Trapero, J. C. Yelmo and M. A. Monjas, “A Privacy-Considerate Framework for Identity Management in Mobile Services”, Mobile Netw Appl., **(2011)**.

[7] P. Baronti, P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta and Y. F. Hu, “Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards”, Comput. Commun., vol. 30, no. 7, **(2007)** May 26, pp. 1655-1695.

[8] M. Chraibi, H. Harroud and A. Karmouch, “Policy-based Security Management in Mobile Environments”, MoMM '11 Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia, **(2011)**.

[9] E. Saunders, J. Greyling and L. Cowley, “An Intelligent Framework for Mobile Devices”, SAICSIT’10 Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists, **(2010)**, pp. 413-416.

[10] J. Chmielewski and K. Walczak, “Application architectures for smart multi-device applications”, Multi-Device '12 Proceedings of the Workshop on Multi-device App Middleware, no. 5, **(2012)**.