On the design of secure DRM in ubiquitous environment+

한규석*, 이송원*, 김광조*, 인소란**

*한국정보통신대학교 국제정보보호기술연구소

**Nitz Corp.

On the design of secure DRM in ubiquitous environment

Kyusuk Han*, Songwon Lee*, Kwangjo Kim*, So Ran Ine**

*International Research center for Information Security, ICU

**Nitz Corp

Abstract

Communication between devices with different computing power, like a PDA and a powerful desktop PC, different needs of each user should be considered in ubiquitous environment. Many unknown security breaches may exist. Recently, many researches about security issues have been done in this ubiquitous environment. For different needs and various situations of each user, applying security technology must be flexible.

In this paper, we issue DRM in ubiquitous environment. We describe DRM in current client-server model, and difference of client-server environment and ubiquitous environment. And then, we show the scenario of using DRM, and security requirements of this scenario. Finally, we show a DRM model in ubiquitous environment adapting context-aware based security.

I. Introduction

Recently, digital contents are getting common. For example, more and more people are using portable music players like MP3 player which stores the music as in files, VOD service via internet, and so on. The importance of digital contents is getting bigger and bigger. In case of music, Nepster, Kazza, and Soribada provided music download service, while they didn't get any legal licenses from music companies. With these services, music companies lost their profit, since many people didn't buy music, but download the music for free.

Protecting the right of content is important, and protecting the right of digital content is also important, but more difficult than the 'normal' contents like novel in paper books, picture in a frame. Since, the most feature of digital contents is that they are easy to be duplicated. One music file can be distributed to numbers of users without loss, without any extra cost, since it doesn't require any effort for physical packaging.

To protect the right of digital content, the research on digital right management is being studied many years and is a set of technologies content owners can use to protect their copyrights and stay in closer contact with their customers. In most instances, DRM is a system that encrypts

+ 과기부 신기술융합사업(R&D Program for Fusion Strategy of Advanced Technologies) 니츠에서 수행하는 유비쿼터스 시스템 보안 기술 개발 과제 수행의 일부임

digital media content and limits access to only those people who have acquired a proper license to play the content. That is, DRM is a technology that enables the secure distribution, promotion, and sale of digital media content on the Internet.

In the ubiquitous computing environment, service provider and user are possibly connected in wireless network and user will move dynamically anywhere maintaining network connection. Many researches about ubiquitous environment like Oxygen project of MIT[1], Portolano project of Washington University [2], Aura project of CMU[3] are studied. These works focused on how to keep users away from complicated computer controlling. Daedalus project of Berkeley University [4] focused on wide overlay network which connecting buildings, cities, even nations. In these ubiquitous computing environments users expect to access resources and services anytime and anywhere. People do not care about computing, but only care about services they will get.

Content distribution in ubiquitous computing environment has to follow the requirement of ubiquitous computing, removing user's distraction. After the user once registers the name in the customer list, whenever he wants to access the digital contents, he can purchase the permission for contents without any complicated procedure

The property of ubiquitous computing, 'any time, any where' makes protecting the right of distribution of digital contents more difficult. Researches on DRM are only focused on the relation between contents distributor and user, contents creator and distributor, and so on. There was lack of the concept in the right of content to be kept by laws. Local distributors have the right of distribution, and in their places, other distributor, even the content owner cannot distribute the content. In real world, it was not serious problem that a user purchases the same content like music or movie from other country, since tax and delivery fee made the price of the content much higher than his residence. But, digital content, distributed over the network, are same to all over world. Form Korea, from Japan, from U.S., and from any other place, user can purchase digital contents technologically.

In the ubiquitous environment, physical distance between shop and consumer is not important via network. That means, it is possible to buy digital contents in U.S. shop from Korea. But in 'real' space, the price of contents in each country is not same. The price of a music album or a DVD is different in each country. For example, in U.S., a music album will be charged as about 20 dollars, but in Korea, about 10 dollars. As this different price, consumer will look for the cheapest price for the same content. Then in some place, the local market is able to be collapsed in local consumer will find the cheapest place. We focus on the DRM for protecting each local market.

In chapter 2 we describe several related works on DRM and security on ubiquitous computing environment. Chapter 3 shows scenarios of content distribution in ubiquitous environment. We show security requirement of DRM in chapter 4 and simplified protocol procedure in chapter 5. We argue the future works on our model and conclude in chapter 6.

II. Related works

We describe several researches on DRM and security in ubiquitous computing environment.

1. Security in ubiquitous computing

Researches on security in ubiquitous computing environment are in many aspects. To authenticate entities in a distributed system, Kerberos, a network protocol [5, 6] is used. Subject role authentication and delegation are addressed in [7]. A set of security models have been proposed for specific distributed technologies such as Jini [8] a Java technology released by Sun Microsystems and dedicated to build fault tolerant distributed systems. These models are surveyed in [9]. In addition, significant work has been addressed the modeling of PKIs[10] and role-based access control [11,12]. Trust in ubiquitous environments is discussed in [13, 14]. Context based security is issued in [15]. Enforcing security with contextual information is a recent research direction. Recently, Covington et al in [16], [17] and [18] investigated the problem of securing context-aware applications. They focus on controlling access in an intelligent home environment. Their approach relies on environment roles and partial authentication. Shankar and Balfanz in [19] propose a generic contextual security service for securing ad-hoc communications using contextual information. Kato proposes system architecture to organize distributed objects and to prevent an organized group from experiencing an intentional or accidental denial of service [20].

Enforcing security with contextual information is a recent research direction.

2. Digital Right Management

Early research of DRM focused on security and encryption as a means of solving the issue of unauthorized copying, that is, lock the content and limit its distribution to only those who pay. Next step of DRM research covers the description, identification, trading, and protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders' relationships.

Early research on DRM is from IMPRIMATUR project [21] in 1995 (end in 1998), which studied the design of generic business model, watermarking, and so on. Their model is early business model of MPEG-21 [22]. INDECS [23] project in 1998 (end in 2000) formalized basic architecture of DRM. Their work is continued in MPEG-21. MPEG-21 proposes general DRM framework. AAP (American Association of Publishers) and CNRI (Corporation for National Research Initiatives) proposed DOI (Digital Object Identifier) [24]. From 1999, AAP proposed ONIX (Online Information eXchange) [25] which is based on INDECS and focusing distribution of e-book contents.

There are two critical architectures to consider in designing and implementing DRM systems. The first is the functional architecture, which covers high-level modules and components of the DRM system that together provide an end-to-end management of rights. The second critical architecture is the Information Architecture, which covers the modeling of the entities within a DRM system as well as their relationships. Microsoft deployed DRM in their Windows Media Player [26].

Functional requirements and technological requirements are described in [27].

2.1 Functional Requirements

Persistent protection - Guarantee confidentiality and integrity of digital contents, protect from various threat. Transfer digital contents and Meta data of contents securely. Users cannot forge user validated licenses without permission.

Flexible business model - Support various use. Rates for ages, support level for free users or VIPs, and so on.

Trusted relationship - Guarantee integrity and trust between entities, users, contents distributors, contents creators and so on.

Easy to integration - Make easy to integrate to existing system or applications

Easy to use - User's interaction like installing programs, manual authenticating procedure, etc should be minimized.

2.2 Technical Requirements

Authority Management - Authentication on user and devices. For user, password based authentication or digital signature, and biometrics are used. For device, device's unique information like CPU, HDD, etc are used to check the authority.

Cryptography -PKI, encryption,

steganography are used.

Security Transaction - Between entities, SSL, SET and so on are used.

Tamper resistance - Protection from forging internal part of software, cheating time, capturing critical data, etc are needed.

Policy management - Flexible policy to allow various rules and conditions.

Contents packaging - support packaging multi number of contents and various content formats. When the content is packing, Meta data like rules are contained in the package. Managing the permission of changing rules and re-packaging is required.

3. DRM in ubiquitous computing

Current researches on DRM are focused on the communication between single entities of user, content distributor, content creator, and so on. We do not focus on vulnerabilities of security of DRM in client-server model, but focus on the possible problem when DRM is deployed in ubiquitous environment.

In the ubiquitous computing environment, current DRM model may fail to protect the right of the content. There was lack of study on user's access control to reach distributors, since there has been always assumption that user manually registers to distributors, and distributors can control the user's access permission. In current DRM model, to purchase user manually contact content distributor, register user's ID.

In real, there is no single distributor, but various competitive distributors for the same contents. In client-server model, there is no problem from this various distributors, as the principles of political economy. Distributors should make the price of content lower than others.

In the ubiquitous computing environment, the user's intrusions for the service are minimized. In that case, unlike client-server model, user do not manually contact service provider, but agent do the role [28]. User only request 'purchase' content, and delegate contacting provider, comparing the best choice to agent. Moreover the world wide networks remove the barrier of nations.

In that case, the purchasing from different country will be new problem of DRM. The right of content is protected by law in each country. The license of contents in Korea do not affect in Japan, in France, and so on. And the price of content is different in every country. The same music album may cheaper in Korea than in U.S. Since there is no technological barrier, customer in U.S. may want to buy the album from Korea in cheaper price. In case of DVD, which is not based on on-line distribution, DVD has regional code to protect local market. In Asia market, the same DVD is much cheaper than in European market. So, with regional code, user cannot play the DVD from other region.

Like the case of DVD, we focus on the new requirement for DRM, 'Location based access control'. This location based access control is required for protect the right of distribution of local distributors. Protecting from content transferring over other location is required. Distribution of content should be possible only in the same location.

III. Scenarios

We show several scenarios in ubiquitous computing to address the possible problem. These scenarios follow the same situation in real world.

1. Scenario 1

Bob lives in London. Bob usually buy songs from on-line music store. Bob knows that new album of Britney spears has been released. But the price of album in London is higher than in Seoul. As a customer, Bob want to buy the same thing in cheaper price, and try to contact the store in Seoul.

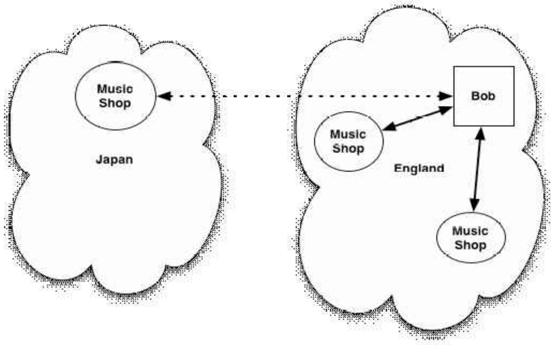


Fig 1 Scenario 1

In this case, the markets in London meet critical threat that nobody buy from them. This situation will make the market in London be collapsed. Moreover, it is illegal since the market in Seoul has no right to sell their content in London.

So, there should be some protection that makes Bob buy only from markets in London. (Fig 1)

2. Scenario 2

When Bob is visiting Korea, Bob wants to buy a song. Even Bob is British; he can purchase the song from Korean market. Bob want to transfer the music to his girl friend Julie in London, but he cannot give the right to his girl friend in London from Korea. But, when he returns to London, he can transfer the right of song to Julie. (Fig 2)

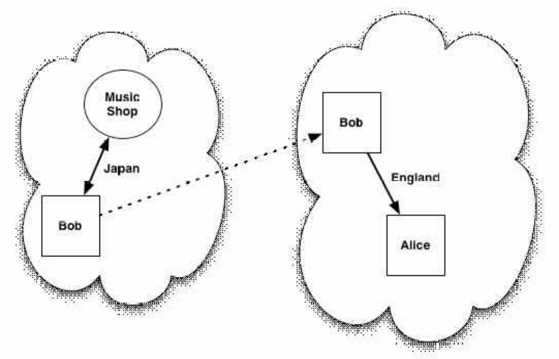


Fig 2 Scenario 2

3. Scenario 3

Bob wants to give a movie to his friend Tanaka in Tokyo. Bob purchases a song from Japanese market and gives it to Tanaka. Tanaka receives the music and send a e-mail for appreciation to Bob. Bob pays as the price in Japan.

These three scenarios are general in real world. In real world, people do not buy stuffs from over-seas countries when they can buy from their local market, since even the price in other countries are cheaper, total cost is more expensive with delivery fee and duty included. But in the ubiquitous environment, there are no extra charge of delivery and duty, only competition of price. The competitor of content distributor will be one in other countries. (Fig 3)

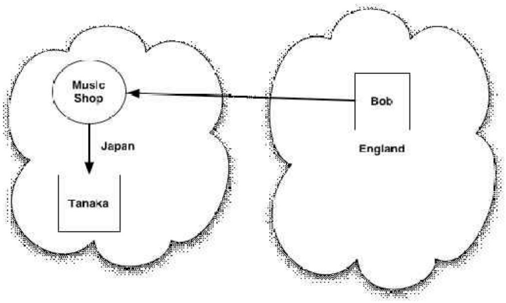


Fig 3 Scenario 3

IV. Model

We focused on the right protection in each location which has different rules for the same content. To meet our scenario, we define new concept locality. In real, people are located in different countries. There are different rules, laws, and economic structures in each country. Distribution of digital contents has to follow these different environments in countries. So, we divide this as section, and we call it zone. We generalized scenarios as follows.

1. Generalized Scenario

Assume there are two zones, zone 1 and zone 2. The price for the same content is different in zone 1 and zone 2. User 1 in zone 1 can purchase a license of content from contents provider. User 1 can send the license to user 2 but not user 3, since user 3 is in other zone. User 1 or user 2 can send the license to user 3 when they purchase the license from contents provider for user 3. User 3 gets the license directly from provider. In this case, the price for content is follows by the policy for zone 2. User 1 can send his license to user 3 if he moves to zone 2. Then user 1 can send the license to user 3 since they are in the same zone. In this case the price for the content follows the policy for zone 1. (Fig 4)

V. Protocol

Mainly there are three actions in users view. Purchasing for self, transferring to others, purchasing for others, as a gift, are user side work. Four these three cases, following procedures are required.

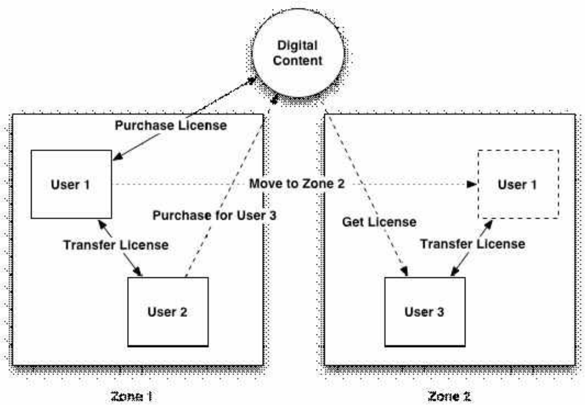


Fig 4. Generalized Scenario

1. Procedures

1.1 Purchasing - self use

User 1 request and then agent check content provider (CP) and user 1's location. Agent checks physical location of user 1 and logical location of content provider. Agent finds the best choice in the same zone. After that agent proceed purchasing for user 1.

1.2 Transferring license

User 1 requests to transfer his right to user 2. Agent checks user 1 and user 2's physical location. If both are in the same zone, proceed transferring the right and revoke user 1's permission.

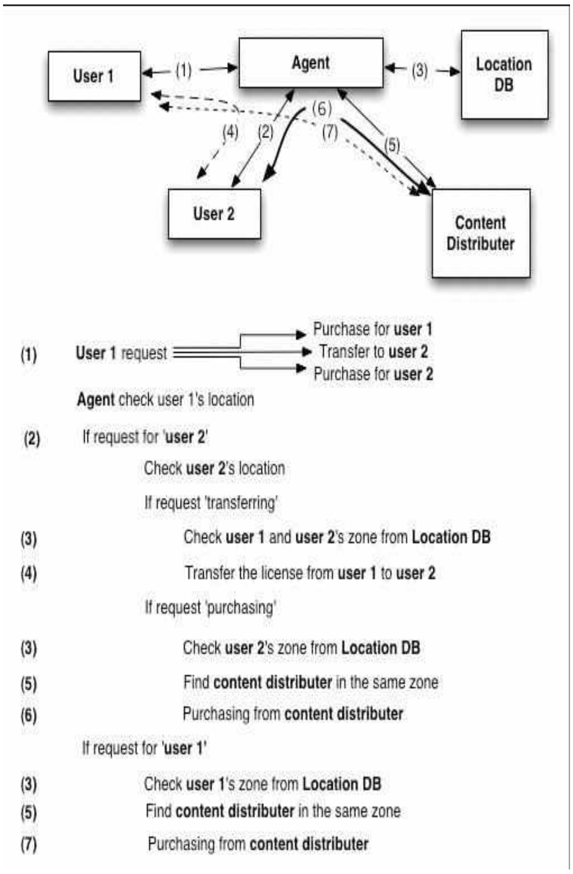
1.3 Purchasing - for others

User 1 requests for user 2. Agent checks user 2's physical location and find CPs in the same zone. Agent proceeds purchasing, this is receiving payment from user 1, and transfer user 2 the license.

2. Basic protocol

We simply show a DRM model with locality. We don't show any specific protocol here, since we focuses on showing how our model to be applied. General procedures like purchasing after checking user's zone are assumed to be followed by existing DRM standards. We define Location DB which can contains location information to check the proper zone.

Step1. User 1 chooses the music to listen in the list. User 1 request 'purchase for user 1', 'transfer user 1's license to user 2', or 'purchase for user 2'. Agent receive user 1's request and ask the user's location. Here, we don't argue how the agent gets the user location information. There are several works on context-awareness. GPS, sensing device are studied in [1, 2, and 3].



(1) User 1 request ⇒ Purchase for user 1 / Transfer to user 2 / Purchase for user 2

Agent check user 1's location

(2) If request for 'user 2'

Check user 2's location

If request 'transferring'

(3) Check user 1 and user 2's zone from Location DB

(4) Transfer the license from user 1 to user 2

If request 'purchasing'

(3) Check user 2's zone from Location DB

(5) Find content distributer in the same zone

(6) Purchasing from content distributer

If request for 'user 1'

(3) Check user 1's zone from Location DB

(5) Find content distributer in the same zone

(7) Purchasing from content distributer

Fig 5. Basic procedure of protocol

Step2. In case user 1 requested 'transfer to user 2', or 'purchase for user 2', agent check user 2's location.

Step3. Agent checks the user 1 and user 2's zone from Location DB. Location DB answers user's regional information.

Step4. In case user 1 requested 'transfer to user 2', if user 1 and user 2 are in the same zone, agent proceed transferring between user 1 and user 2. (We skip detailed process.)

Step5. Agent find content distributor in the same zone where user is located. There are many researches about this process [1, 2, and 3].

Step6. Proceed purchasing from content distributor. (We assume the process follows general DRM, and skip detailed procedure.)

Step7. In case user 1 requested 'purchase for user 1', agent contact the content distributors in the same zone.

With checking the location information of user, our protocol protects the content distribution over different zone. Also, our protocol allows content distribution in the same zone, purchasing and transferring contents.

VI. Concluding Remarks

We showed a new DRM model in ubiquitous computing environment. We extended current DRM models whose researches were focused on the secure transaction among the different entities like content creator, content distributor, user(customer), and so on. We added the new concept of locality which protects local distributor's right on digital contents. We believe that our location based access control model will solve the region problem of digital content distribution.

Every country has different price for the same content, and it is obvious that the price of digital content will follow the current price of content. The price of the same digital content like music, movie or any kinds must be different in every country. In practical, iTunes music store and Nepster provides on-line music store in U.S. They sell each song as 99 cents, but this price is not sufficient in Korea. And their DRM system is limited to only in U.S.

To success DRM in ubiquitous environment, the requirements of real world, that the right of distribution should be considered, and our works are focused on this aspect. We believe that our work will lead the expansion of DRM in ubiquitous computing. Not only problem of pricing, many other problem like releasing date and prohibition rule, *etc* are factors to be considered. Our next step is integration to DRM standards like MPEG21 and build more detailed framework of DRM in the ubiquitous environment. Constructing the DRM system which enables registering once and using anywhere and any country is also our future work.

References

[1] Project Oxygen, MIT, http://oxygen.lcs.mit.edu

[2] Project Portolano, Washington University, http:// portolano.cs. washington.edu/

[3] Project Aura, CMU, http://www-2.cs.cmu.edu/~aura/

[4] Project Daedalus, Berkeley University, http://daedalus.cs.berkeley.edu/

[5] Clifford Neuman, B. and Ts'o, T., "Kerberos: An Authentication Service for Computer Networks", IEEE Communications Magazine, Vol. 32, No. 9, pp. 33-38, Sep. 1994

[6] Kohl, J.T., Clifford Neuman, B. and T'so, T., "The Evolution of the Kerberos Authentication System", IEEE Computer Society Press, 78-94, 1994

[7] Lampson, B., Abadi, M., Burrows, M. and Wobber, E., "Authentication in distributed systems: Theory and practice", ACM Transactions on Computer Systems, 10(4):265-310, 1992

[8] Sum Microsystems Inc., "Jini(TM) Architecture Specification", Version 1.2, http://wwws. sun.com/software/jini/specs /index.html

[9] Kouadri Mostefaoui G., Pasquier-Rocha, J. and Gachet, A., "Security Models for the Jini Networking Technology: A Case Study", Internal Working Paper No 02-07, Department of Informatics, University of Fribourg, May 2002.

[10] Branchaud M., "A Survey of Public Key Infrastructures", Master Thesis, Department of Computer Science, McGill University, Montreal 1997.

[11] Sandhu, R., "Engineering authority and trust

in cyberspace: the OM-AM and RBAC way", Proceedings of the fifth ACM workshop on Role-based access control, 111-119, 2000

[12] Park, J., Sandhu, R. and Ahn, G., "Role-Based Access Control on the Web", ACM Transactions on Information and System Security (TISSEC), Vol. 4, No. 1, pages 37-71, February 2001

[13] English, C., Nixon, P. Terzis, S., McGettrick, A. and Lowe, H., "Dynamic Trust Models for Ubiquitous Computing Environments", Proceedings of UBICOMP2002- Workshop on Security in Ubiquitous Computing, Goteborg, Sweden, September 2002

[14] Kagal, L., Undercoffer, J. Perich, F., Joshi, A. and Finin, T., "A Security Architecture Based on Trust Management for Pervasive Computing Systems", Proceedings of Grace Hopper Celebration of Women in Computing 2002

[15] G. K. Mostefaoui, "Security in Pervasive Environments, What's Next?"

[16] Covington, M.J., Ahamad, M., Srinivasan, S., "A Security Architecture for Context-Aware Applications", Technical Report GIT-CC-01-12, College of Computing, Georgia Institute of Technology, 2001

[17] Covington, M.J., Wende, L., Srinivasan, S., Dey, D., Ahamad, M., and Abowd, G., "Securing Context-Aware Applications Using Environment Roles" Proceedings of the 6th ACM Symposium on Access Control Models and Technoligies (SACMAT '01), Chantilly, Virginia, USA, 10-20, May 2001

[18] Covington, M.J., Fogla, P., Zhan, Z. and Ahamad M., "A Context-aware Security Architecture for Emerging Applications", Proceedings of the Annual Computer Security Applications Conference (ACSAC), Las Vegas, Nevada, USA, December 2002

[19] Shankar, N., Balfanz D., "Enabling Secure Ad-hoc Communication using Context-Aware Security Services", Proceedings of UBICOMP2002-Workshop on Security in Ubiquitous Computing. Goteborg, Sweden, September 2002

[20] Kato, H., "Context Aware and Yet Another Service AYA", Proceedings of UBICOMP2002-Workshop on Security in Ubiquitous Computing, Goteborg, Sweden, September 2002

[21] Project IMPRIMATUR. The Project is finished in 1998, and its work is being carried forward by Imprimatur Services Ltd. All publications are available here. http://www.imprimatur.net

[22] ISO/IEC JTC1/SC29/WG11/N5231

[23] An international initiative of rights owners creating metadata standards for e-commerce, http://www.indecs.org/

[24] William Y. Arms, "Digital Object Identifiers (DOIs) and Clifford Lynch's five questions on identifiers". ARL Newsletter, October 1997.

[25] Now supported by EDItEUR, http://www.editeur.org/

[26] Jim Skinner, "Protecting Audio and Video Content with Digital Rights Management", Nov 2002, http://www.microsoft.com/windows/windowsmedia/howto/articles/DRMProtect.aspx

[27] J., Kim, "Functional requirement and technological requirement of DRM for testing DRM solutions", SEDICA, 2001 (Korean)

[28] Q. He, et al, "A Practical Study on Security of Agent-Based Ubiquitous Computing", AAMAS 2002, LNAI 2631, pp. 194-208, 2003