DOI:10.3745/JIPS.2007.3.2.054

Actual Condition and Issues for Mobile Security System

Kouichi Sakurai* and Kazuhide Fukushima**

Abstract: The high-speed mobile Internet has recently been expanded, many attractive services are provided. However, these services require some form of security-related technology.
This paper outlines Japanese mobile services and exposits some mobile security topics including mobile spam, mobile malware, mobile DRM system, mobile WiMAX security, and mobile key management.

Keywords: *Mobile Security, Mobile Malware, Mobile DRM System, Mobile WiMAX Security, Group Key Management*

1. Introduction

The high-speed mobile Internet has recently been expanded to include 3G mobile services. Mobile music distribution has become a major service, and, pay-broadcasting, TV telephone, and TV conference based on multicast/broadcast technology are expected to become a new mobile service of particular importance in the near future. Moreover payment services are now available on many mobile phones.

However, these attractive services require some form of security-related technology.

First, the mobile phones have much important data such as address book and personal schedule; thus, countermeasures to loss are required. Spam mail is a big issue for all the mobile users as well as PC users. Content distribution service needs digital right management (DRM) system to protect the copyright of content. Anti-malware is essential component to establish a reliable payment system, since platforms of mobile phones are being unified, that is, it is getting easy to develop malicious programs. Furthermore, a group key management scheme is required for multicast/broadcast service, since active clients must share a common key (the group key) for encrypting the group traffic in order to afford message confidentiality.

Mobile Security versus Fixed Security

Major difference between mobile security and fixed security is summarized into three points: 1) low bandwidth, 2) high risk of eavesdropping, and 3) client/device mobility. To tackle these issues, we must minimize the message sizes and number of messages, use link-level and end-to-end encryption. Furthermore, we must ensure authentication and privacy of clients.

This paper surveys actual condition and issues for mobile security system in Japan. Firstly, we show the mobile service in Japan. Then, we describe, mobile spam, mobile malware, mobile DRM system, mobile WiMAX security, and mobile key management.

2. Mobile Services in Japan

There are three major mobile operates in Japanese market: NTT DoCoMo, KDDI and Softbank Mobile. Their market shares are around 50%, 30%, and 20%, respectively. NTT DoCoMo is the largest operator and sells their stability. KDDI sells new service plans based on high-end mobile phones, and Softbank Mobile sells reasonable price plans.

Mobile Number Portability

Mobile number portability (MNP) service enables customers to switch mobile operator while keeping the existing phone number. This service started on 24th Oct. 2006 in Japan, and the service fee is 2,100 JPY (18,000 KRW). KDDI gain around 1,230,000 customers through the MNP service, while NTT DoCoMo and Softbank Mobile did not announce their gains and losses. However, the usage rate of MNP service stays within three percents. Some customers hate changing their e-mail address or complicated procedure, that is, they must go to two offices of the existing operator and the new operator.

2.1 Mobile Music Distribution Service

MP3 music content can be played on many of mobile phones in Korea and other countries having GSM systems. In this situation, a pay music distribution serves for mobile phones will not have a great run; that is, users will simply move their MP3 files obtained from music CDs or web sites to mobile phones at free fee. On the other hand, very few mobile phones can play MP3 music content in Japan, due to intent of content providers. Thus, Japanese operators collaborated with content providers and developed mobile music distribution services. These services distribute music content in distinct formats protected by some DRM systems.

Manuscript received December 3, 2007; accepted December 26, 2007.
Corresponding Author: Kazuhide Fukushima

***** Kyushu University(sakurai@csce.kyushu-u.ac.jp)
** KDDI R&D Laboratories, Inc(ka-fukushima@kddilabs.jp)

Chaku-Uta Service

KDDI started Chaku-Uta service that distributes bridge parts of songs (around 30 seconds, 100KB) in Dec. 2002. The short content can be registered as a ringing tone and alarm. Usage fee of content is paid to recording label and music publisher and as well as the composer; thus, the price of Chaku-Uta content, around 80 to 120 JPY (700 to 1,000 KRW), is higher than that of a normal ringing tune. Vodafone (currently Softbank Mobile) and NTT DoCoMo also started Chaku-Uta service in Dec. 2003 and Feb. 2004, respectively. However, these services have no compatibility due to difference in codec.

NTT DoCoMo uses 3GPP format, Softbank mobile uses MP4, and KDDI adopts 3GPP2 or AMC format.

Chaku-Uta Full Service

KDDI started Chaku-Uta Full service that distributes full songs (around 3 to 5 minutes, 500KB to 2MB) in Nov. 2004. A Chaku-Uta Full content and clipped part of it can be registered as a ringing tone and alarm as with Chaku-Uta content. The price of Chaku-Uta Full content is around 210 to 420 JPY (1,800 to 3600 KRW). Content is compressed by 40 to 48 kbps HE-AAC codec. Some content includes artist photo or lyric sheet. Softbank Mobile and NTT DoCoMo also started the same service on Aug. 2005 and Jun. 2006, respectively. These services have no compatibility due to difference in data format.

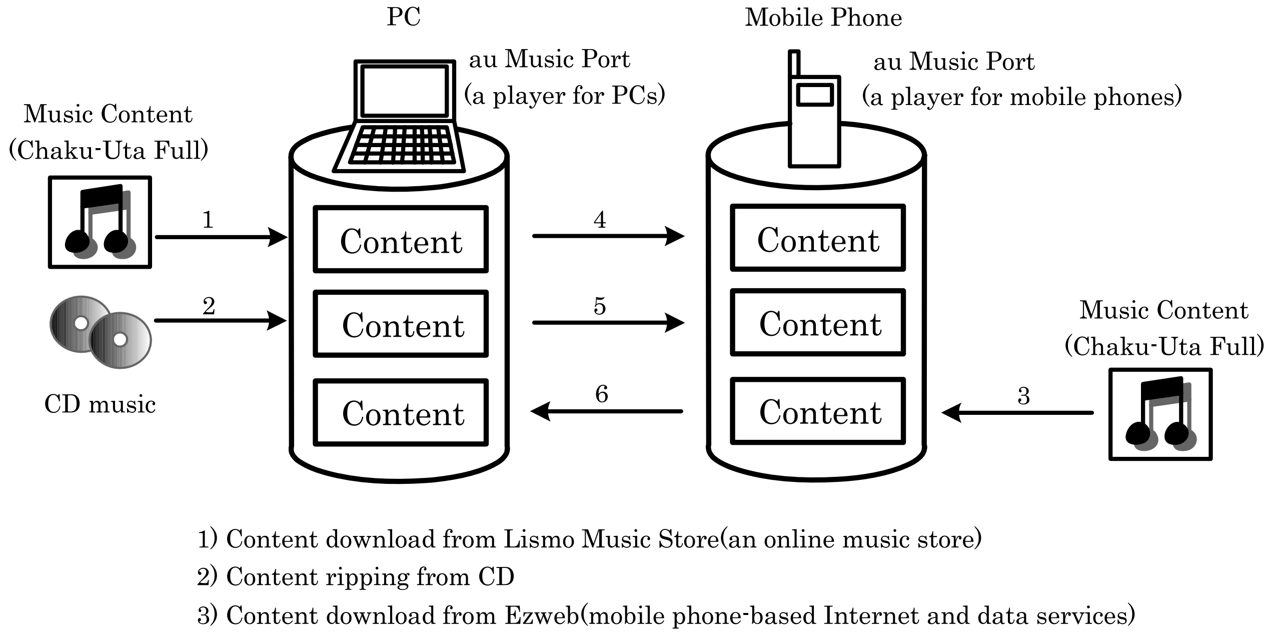
Additionally, content is encrypted based on the phone number. Thus, content can be played only on the mobile phone in which the user downloaded the content or phones that have the same phone number. If we renew a mobile phone without changing the number, content can be play on new mobile phones. Content can be moved through PCs or memory cards such as mini/micro SD cards.

au LISTEN MOBILE SERVICE (LISMO)

KDDI started an original content distribution service for PC and mobile phones in Jan. 2006. Chaku-Uta Full content can by played on PC software, au Music Port, by connecting a mobile phone; furthermore, the content, address book, and photos in the mobile phone can be backed up. Users can purchase Chaku-Uta Full content and rip content from music CDs using au Music Port. The content can be move to mobile phones, and can be played on au Music Player, which is a music player for mobile phones.

2.2 Payment Service

In Korea, Teledit, a mobile payment service, is started in Jul. 2000. This service allows users to pay for on-line content and products by simply inputting their mobile phone number and social security numbers. In Japan, NTT DoCoMo started a mobile payment service in Jul. 2004; then KDDI and Softbank followed. On 18th Mar. 2007, the Tokyo-area private railways, bus companies, and subways implemented PASMO, a contactless smart card used in payment. Through collaboration with JR East, passengers can use Suica cards interchangeably with Pasmo. Suica is a contactless smart card used as a fare card on JR East train started in Nov. 2001 and mobile Suica for mobile phones is



1) Content download from Lismo Music Store(an online music store)
2) Content ripping from CD
3) Content download from Ezweb(mobile phone-based Internet and data services)
4) Content copy from PC to phone(can be registered as a ringing tone)
5) Content copy from PC to phone(cannot be registered as a ringing tone)
6) Content copy from phone to PC

Fig. 1. Overview of au LISTEN MOBILE SERVICE

started in Jan. 2006. Now, a passenger who has a mobile phone with a Mobile Suica application can get on any railway, subway, or bus in the Tokyo metropolitan area.

Small Payment Service

NTT DoCoMo started small payment service, Osaifu-Keitai (mobile wallet in English) in Jul. 2004. The service is based on a contact-free card, FeliCa chip, embedded in mobile phones. A mobile phone with a FeliCa chip is available as a member's point card, e-money card e.g., Edy, and a transportation ticket e.g., Mobile Suica. Though Osaifu-Keitai is registered trade of NTT DoCoMo and the payment system was developed by them, the license of the service is granted to KDDI and Softbank Mobile. KDDI and Softbank Mobile started the same service in Sep. 2005 and Nov. 2005, respectively.

Large Payment Service

Currently, these payment services have a restriction like as Korean services. The payments and deposits of Osaifu-Keitai service are limited up to 50,000 JPY (430,000 KRW) and 25,000 JPY (220,000 KRW) in Edy, and 20,000 JPY (170,000 KRW) and 10,000 JPY (87,000 KRW) in Mobile Suica. In the near future, large payments will be available on mobile phones and they may be used for payment just as a credit card.

2.3 Security Solution Services

The personal information protection law was completely enforced on 1st Apr. 2005 in Japan. Thereafter, Japanese companies assume that data in mobile phones are critical, and considered countermeasures to loss of mobile phones.

Remote Auto Rock and Data Erase

KDDI provides remote auto lock service. A mobile phone can be locked so as not to be operable by making calls certain times e.g., 3 to 10 times. The calls must come from the registered phone number and be within the specified of time e.g., 1 to 10 minutes. The target mobile phone must be turned on and inside of the service area. This service is available at almost all the KDDI mobile phones since Feb. 2005. Additionally, remote data erase is available at mobile phones for Business, au Business mobile, since Mar. 2006. All data including address book and schedule data in the memory are removed. NTT DoCoMo and Softbank Mobile also provide the remote auto lock service but do not provide the data erase service.

Public Relation Support System

KDDI provides a public relations support system as a solution business. In this system, public relations staff can securely access to customer DB through KDDI's closed network by using a BREW application. When the mobile phone is lost, the remote auto lock and data erase are available at the server in the headquarters office. Additionally, the location of the mobile phone is detected by the GPS system; then, it is notified to the service. The service is employed by a Japanese city bank.

Mobile Data Encryption

Data encryption software is now available in Personal Digital Assistants (PDA). In the near future, such software is required in mobile phone in order to protect address book, personal schedule, and so on. Check Point Software Technologies, a Swedish company, provides Check Point Full Disk Encryption[1] and Utimaco Safeware AG, a German company, provides SafeGuard PDA[2] ~. The software can protect secret data in PDA by encrypting internal flash memory and external memory, such as CF and SD card.

Thin Client

A thin client is a client PC, mobile phone, or client software in client-server architecture networks that depends primarily on the central server for processing activities. The client PC mainly focuses on conveying input and output between a user and the server.

Many thin client devices run only web browsers or remote desktop software; that is, all significant processing occurs on the server. Therefore, a thin client system can allow user to access security-sensitive databases with less risk of lost or compromised data should the laptop be lost or stolen since it has no local storage.

NTT Neomate, a NTT group company in Japan, started a service in which a user can remotely control his/her Windows PC via a DoCoMo mobile phone in Mar. 2007. Currently, this service is available on DoCoMo mobile phones with 480x864 (Wide VGA) resolution display.

3. Mobile Spam

Mobile spam refers to unsolicited messages to mobile phones with the aims of accomplishing any one of the following activities: trying to sell an item or service, asking the user to call a number (which may be a premium rate number), sending messages that may be harmful or attempt to change the mobile phone settings, or commercial messages that are threatening or intrusive to privacy. Mobile spam is a more serious issues than PC spam since users must pay unnecessary money if they use a pay-as-you-go internet service. There are two forms for mobile spam: Short Message Service (SMS) and e-mail.

Spam SMS

In Japan, each mobile operator provides SMS services. NTT DoCoMo provides Short Mail service, KDDI provides C-Mail service, and Softbank Mobile also provided a distinct SMS service. However, these SMS services do not have compatibility. The usage fee of these SMS services is around 3 to 5 JPY (26 to 43 KRW) for each message.

To reduce spam SMS, each mobile operator establishes an upper limit on the number of sending messages per day or multiple addressing. Additionally, mobile operators provide SMS filters and SMS blocking functions where user can specify to reject SMS messages.

Spam E-mail

E-mails can be sent from PCs to mobile phone and vice versa. Thus, mobile operator and Internet Service Providers (ISPs) must corroborate to reduce spam e-mails. In Japan, mobile operators and ISPs establish Japan Email Anti-Abuse Group (JEAG)[3], an organization aiming to eradicate spam mails.

Means to send spam e-mails can be classified to the following three types:

- A user sends spam e-mails using Message Transfer Agent (MTA) provided by ISP.
- A user sends spam e-mails to the Internet directory, or send them using own MTA, where the IP address of the user is determined dynamically.
- A user sends spam e-mails to the Internet directory, or send them using own MTA, where the IP address of the user is fixed. In this case, the illegal users can be easily traced using the fixed IP address.

To reduce spam mails in the first type, mobile operators and ISPs should impose a rate restriction, e.g., the number of e-mail per day. Outbound Port 25 Blocking (OP25B) is effective to prevent spam mails in second type. In this practice, firewalls and routers are programmed not to allow SMTP traffic (TCP port 25) from machines that are not supposed to run MTAs or send e-mails. The practice is somewhat controversial when ISPs block legal users, especially if the ISPs do not allow the blocking to be turned off upon request. E-mails can still be sent from these computers to designated smart hosts via port 25 and to other smart hosts via the e-mail submission port 587.

As a mobile operator, KDDI established an upper limit on the number of sending e-mail per day and multiple addressing. Additionally, KDDI introduce OP25B in Dec. 2006 as an ISP.

4. Mobile Malware

Threats in mobile phones become multifaceted as information assets increases. KDDI predicated that mobile phone will be exposed to the threat of malware and illegal access in few years. Thus, KDDI had been researched techniques against these threats.

However, mobile malware is not so big problem in the current status. One cause was that there were few advantages to attacking to mobile phones. For example, a mobile malware that targets the Symbian platforms was developed in 2004. Still, it was only a ``proof of concept worm" that repeatedly sends itself to the first Bluetooth-enabled device, and did not attempt to analyze information in mobile phones. Another cause was that operation systems and software development kits are different for each manufacture in many cases and they are hardly disclosed.

In the near future, mobile malware will be a serious problem. Now, there is much important information in mobile phones. Full music content and FeliCa chip for small payments are currently on KDDI's mobile phones. Additionally, mobile phones may have credit card numbers for large payment soon. These data will attract not only customers but also attackers. Furthermore, operating system is going to the common architecture, such as Windows Mobile, Linux, or Symbian OS, or KCP+ in KCP+: Common Mobile Platforms in KDDI Mobile Phones Fig. 2. Fig. 3 shows the progress of PCs and mobile phones in term of memory size and CPU frequency. The figure shows that current mobile phones have same capability as PCs in ten years ago while the development environment is much poorer because of non-public OS and SDK. The timing of the appearance of a serious malware is hard to predict, since it depend on not only the progress of hardware but also trend of platforms.

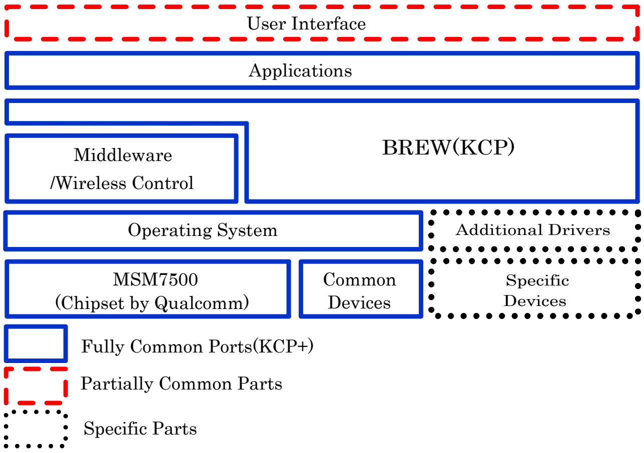


Fig. 2. KCP+: Common Mobile Platforms in KDDI Mobile Phones

Anti-Malware for Mobile Phones

Existing anti-virus software for PCs is hard to apply to mobile phones because of memory shortage. For example, Virus Buster 2007 by Trend Micro requires more than 60 MB of memory. Exiting mobile phones have only 32 to 64 MB of memory. Thus, we must development specialized anti-malware for mobile phones.

Some security vendors provide anti-malware.

For example, Symantec Mobile AntiVirus and Trend Micro Mobile Security for Windows Mobile, and

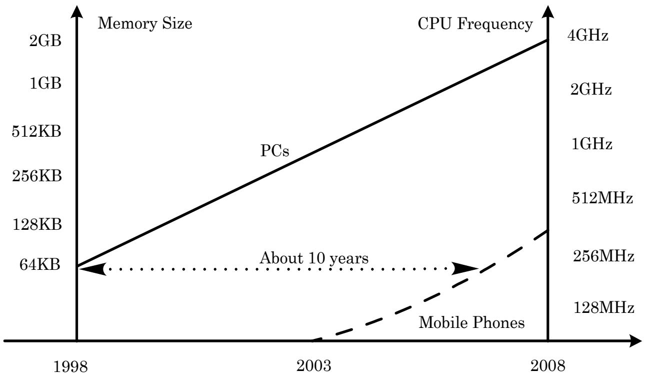


Fig. 3. Progress of PCs and Mobile Phones

Kaspersky Anti-Virus Mobile for Symbian OS and Windows Mobile are anti-virus software for mobile devices.

Mobile malware in the near future is discussed in a few papers[4][5][6][7][8].

Mobile Forensic

Mobile forensics is a technique of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods. A mobile forensic technique used to fire employees, convict criminals, and demonstrate innocence. For example, a user must present evidence of innocence when his/her mobile phone is invaded by mobile Malware or an attacker, and send spam mails illegally.

In the near future, mobile phones will be heading towards convergence with other digital devices such as laptop computers and PDAs. Therefore, more data will be used on such devices, and the need for direct access to the data in a forensically sound manner will dramatically increase because of the complexity and the sheer amount of data stored on mobile devices. However, mobile phones, especially those with advanced capabilities, are a relatively recent phenomenon, not usually covered in classical computer forensics.

In a mobile forensic system, it is essential to recover potential evidence from a mobile phone in a well documented manner and in a scientifically reliable manner with affecting the data on the device as little as possible. All examinations must be conducted within the law.

National Institute of Standards and Technology (NIST) in USA established guidelines on cell phone forensics[9] and some papers about mobile forensic are published[10][11][12]

Verification of Programs

Verification of program is a countermeasure against vulnerable software or malware.

KDDI mobile phones support Binary Runtime Environment for Wireless (BREW) platform.

BREW is an application development platform created by Qualcomm for mobile phones.

It was originally developed for CDMA handsets, but has since been ported to other air interfaces including GSM/GPRS, and UMTS.

BREW provide a software platform that can download and run small programs for playing games, sending messages, sharing photos, etc.

In KDDI mobile phones, a user cannot execute own BREW application.

Content provider must pass application verification by KDDI to distribute a BREW application.

KDDI checks the application manually; then, issues a signature file (SIG file) that attests the validity of the application.

A BREW application with a SIG file can be downloaded and executed on mobile phones.

In NTT DoCoMo and Softbank Mobile mobile phone, and KDDI mobile phones that support Open Application Player, a user cannot execute own Java application.

A Java application can be downloaded via web uploader and executed on mobile phones.

In this case, the validity of application is secured by the byte code verifier on Java Virtual Machine (JVM) and other security function of Java.

5. Mobile Digital Right Management System

Past DRM systems on mobile phones were simpler than that on PCs. Mobile phones had different and closed platforms for each vendor; thus, they were difficult to analyze and assumed to be secure devices. Additionally, content for mobile phones could not be moved to other mobile phones or PCs. All we have to do was to encrypt content and store the key in mobile phones.

However, platforms on mobile phones are being unified. There are some common platforms for mobile phones e.g., Symbian OS, Windows Mobile, Linux, and KCP+ in KDDI. Mobile phones now face to the threat of analysis as well as PCs. Furthermore, content usage is diversified into various kinds. Mobile operators develop Fixed-Mobile Convergence (FMC) Service in which content can be used on mobile phones and PCs. For example, mobile content can be played or backed up to PCs, and it can be moved to other mobile phones though memory card. The content may be analyzed on PCs.

Secure chips, e.g., Trusted Platform Module (TPM) in PCs or User Identify Module (UIM) in mobile phones, are going to be used in near future DRM system. UIM is an IC card with computational capability and secure storage for a PKI certificate with a public key, and the corresponding private key. OMA DRM 2.0[13] is a DRM system based on securely stored individual certificate and private key.

OMA DRM 2.0

OMA DRM is a digital rights management system defined by the Open Mobile Alliance whose members represent the entire value chain, including mobile phone manufacturers (e.g. Nokia, Motorola, Samsung, Sony-Ericsson, BenQ-Siemens), mobile system manufacturers (e.g. Ericsson, Siemens, Openwave), operators (e.g. Vodafone, O2, Cingular, Deutsche Telekom, Orange), and IT companies (e.g. Microsoft, IBM, Sun).

OMA DRM 2.0 was approved in Mar. 2006. Each device in OMA DRM 2.0 has an individual PKI certificate with a public key, and the corresponding private key.

Each Rights Object for a receiving device is encrypted with the device public key so that sensitive information is protected. A Right Object is a collection of permissions and other attributes which are linked to protected content, and contains the key that is used to decrypt the content. Delivery of Rights Objects requires a registration with the Rights Issuer (RI). During this registration, the server checks the validity of device certificate by using an Online Certificate Status Protocol (OCSP) verification.

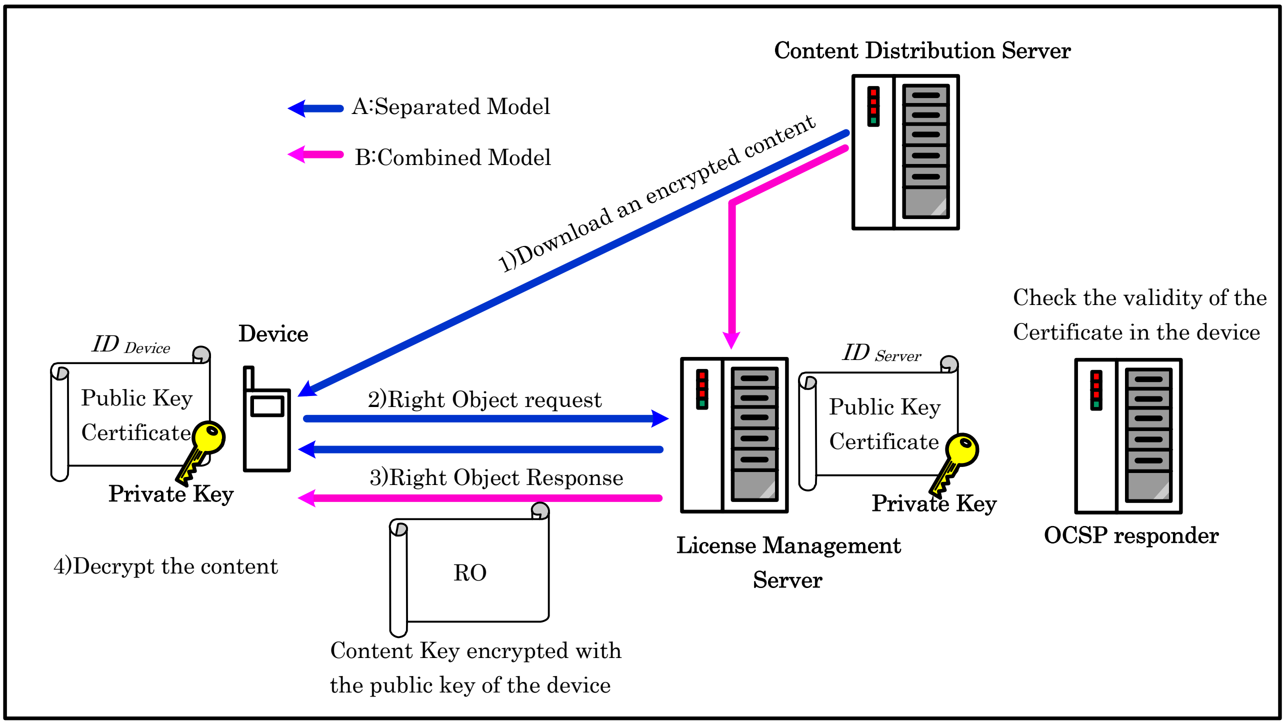


Fig. 4. Overview of OMA DRM 2.0

6. Mobile WiMAX Security

Mobile WiMAX is a standard that provides higher-speed and low-cost wireless communications than 3G mobile phone system. It provides high quality broadcasting and personal communication service based on large downlink/uplink throughput, quick connection, and less multi-pass interference in urban area.

Milestones in Japan

In Jun. 2007, Ministry of Internal Affairs and Communication of Japan released the licenses assignment policy. The ministry planed to grant licenses to use the new bandwidth to up to two companies that are not existing 3G mobile operators. However, a mobile operator was able to offer new services through that bandwidth by forming a joint company in which it owns a stake of one-third or less. Thus, 3G mobile operators NTT DoCoMo, KDDI, and Softbank mobile established joint companies. NTT DoCoMo worked with a broadband service provider, Acca Networks Co, and KDDI worked with partnerships with Kyocera Corp., Intel Corp. and East Japan Railway Co. Softbank Mobile collaborated with a broadband service provider, eAccess. WILLCOM, a PHS operator expressed their independent participation. The licenses were going to be granted to two of the four candidates. Resultingly, the KDDI group and WILLCOM obtained the licenses in Dec. 2007. Mobile WiMAX services will be available in 2009.

IEEE Standards

The development of IEEE 802.16 was started by the IEEE in 2001. After that it was revised several times and ended in the final standard IEEE 802.16-2004 which corresponds to revision D and is often called Fixed WiMAX. It defines Wireless Metropolitan Broadband access for stationary and nomadic use. This means end devices can not move between base stations (BS) but they can enter the network at different locations. This specification was extended by the development of IEEE 802.16e which supports mobility so mobile stations (MS) can handover between BS while communicating. IEEE 802.16e is often called Mobile WiMAX and is an amendment to the IEEE 802.16-2004 standard. Commercial services of Mobile WiMAX are already planned for several countries. On the link layer Mobile WiMAX introduces new features like different handover types, power saving methods and multi- and broadcast support.

Furthermore IEEE 802.16e eliminates most of the security vulnerabilities discovered in its predecessors. It uses EAP-based mutual authentication, a variety of strong encryption algorithms, nonce and packet numbers to protect against replay attacks and reduced key lifetimes.

Security Specification of Mobile WiMAX

The service provider wants to know the identity of users and devices connected to their network, to provide services to authorized users, and to charge to users for the services they have used. On the other hand, the users want to confirm their privacy, the integrity of data, accessibility to the services they have subscribed to, and the correct charges. These requirements can be achieved by the security specifications of mobile WiMAX.

Mobile WiMAX specified by the IEEE 802.16e-2005 includes the definition of data link layer and physical layer. Especially, the security sublayer only deal with the data link layer security. The key aspects of WiMAX security are as follows[14][15]:

Data Encryption
User data are encrypted using symmetric cryptographic algorithms. Advanced Encryption Standard (AES) with CBC, CCM, and CTR mode, and Data Encryption Standard (DES) with CBC mode are supported.

Key Encryption
Key data are encrypted using symmetric and asymmetric cryptographic algorithms. Triple DES (3DES) with EDE mode, RSA, AES with ECB mode, AES Key Wrap (in RFC3394) are supported.

Message Integrity
The integrity of over-the-air control messages is protected by using message authentication code. HMAC-SHA-1 and AES with CMAC mode are supported.

Device/User Authentication
WiMAX provides a flexible means for authenticating subscriber stations and users to prevent unauthorized use. The authentication framework is based on the Internet Engineering Task Force (IETF) EAP, which supports a variety of credentials, such as username/password, digital certificates, and smart cards. WiMAX terminal devices come with built-in X.509 digital certificates that contain their public key and MAC address. WiMAX operators can use the certificates for device authentication and use a username/password or smart card authentication on top of it for user authentication.

Key Management Protocol
The Privacy and Key Management Protocol Version 2 (PKMv2) is used for securely transferring keying material from the base station to the mobile station, periodically re-authorizing and refreshing the keys.

Support for Fast Handover
To support fast handovers, WiMAX allows the Mobile Station (MS) to use pre-authentication with a particular target Base Station (BS) to facilitate accelerated reentry. A three-way handshake scheme is supported in order to optimize the re-authentication mechanisms for supporting fast handovers, while preventing man-in-the-middle attacks.

Security issues on mobile WiMAX are discussed in a few papers [8][16][17].

7. Mobile Key Management

Multicast services for mobile phones such as content distribution, pay-per-view and online auction require some form of secure communication. Group key management schemes provide secure communication by sharing the group key between clients. Thus, group key management schemes are essential functions in order to ensure the security of these services.

Group key management schemes enable the center to transmit a message to all the clients, such that any active devices can decrypt the message correctly and any coalition of inactive clients in cannot decrypt it. Active clients share the group key that is used to encrypt the message. An active client may dynamically change to being inactive, and vice versa. The center updates the group key to prevent the joining device from obtaining the former messages and the leaving device from obtaining the latter messages.

In IETF, some group key management protocols have been discussed in RFC2093[18], RFC2094[19], RFC2627[20], RFC3547[21], and RFC4535[22]. RFC3740[23] provides information for the security architecture of group key management schemes. RFC2627, RFC3547 and RFC4535 support tree-based rekeying which contributes to raise the efficiency of key distribution. However, there are no drafts that provide a systematic survey on mechanisms of group key management schemes.

7.1 Key Management Mechanisms

Group key management schemes can be classified by their logical structures to assign keys to users, and rekeying process. Thus, there are four key management mechanisms based on 1) star-based structure with individual rekeying, 2) star-based structure with batched rekeying, 3) tree-based structure with individual rekeying, and 4) tree-based with batched rekeying. We assume that each client shares an individual KEK with the center, and trusts the center.

Key Management Structure
We show the star-based structure, the tree-based structure and the intermediate scheme.

Star-Based Structure
The group key-management protocols in RFC2093 and RFC2094, and the scheme based on star key graph uses a logical star-based structure. Fig. 5 shows the star-based structure. In these group key management schemes, each client has two keys: 1) the group key and 2) the individual key encryption key (KEK) or 1) the group key and 2) the common KEK. In the former case, the updated group key can be encrypted with each individual KEK of existing clients in order to prevent leaving clients from obtain the updated key; however, the communication overhead is high. In the latter case, the scheme is not secure since leaving clients can obtain the updated key since they also have the common KEK.

Tree-Based Structure
The group key management protocols in RFC2627, RFC3547, and RFC4535, and the scheme based on tree key graph[24] uses a logical star-based structure, which is called Logical Key Hierarchy (LKH). Fig. 5 show the tree-

based structure.

The group key, which is shared by all the clients, is assigned to the root node of the tree. Each client shares an individual KEK with the group controller (GC) and the KEKs are assigned to the leaf nodes of the tree. Additionally, KEKs are assigned to the other intermediate nodes. The KEKs are shared by multiple clients whose individual KEKs are assigned to the descendant of the node where the KEK is assigned. The communication overhead of leave process can be reduced by using the key. Each client has all the keys assigned to the nodes on the path from the root node to the leaf node where the individual KEK of the client is assigned. Thus, the number of keys a client has is proportional to the logarithm of the total number of clients.

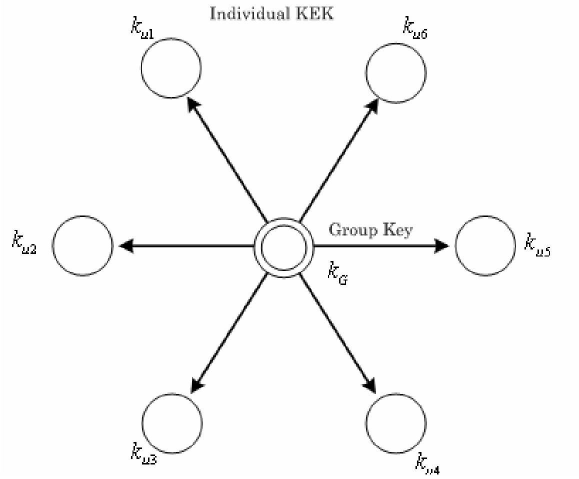


Fig. 5. The Star-Based Structure

Rekeying Method

Group key management schemes can be classified by their rekeying method.

We show individual rekeying and batched rekeying.

Rekeying method in group key management scheme can be classified into individual rekeying and batched rekeying.

Individual Rekeying

In this rekeying process, the group key, and KEKs are updated when a client joins or leaves.

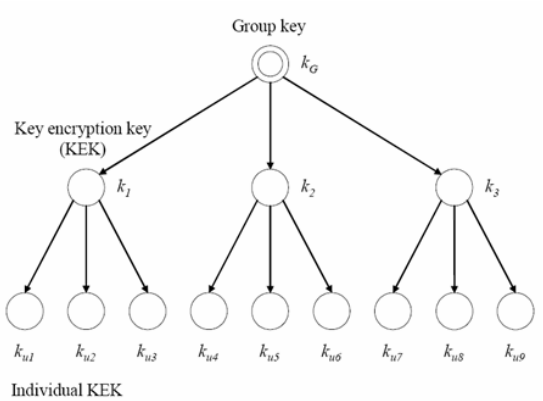


Fig. 6. The Tree-Based Structure (logical key hierarchy with a complete ternary tree)

Batched Rekeying

In this rekeying process, the group key, and KEKs are updated for every rekeying interval, τ [seconds]. The parameter τ has a strong impact on the security of a group key management scheme; thus, the value of the parameter must be determined as a security policy.

7.2 Security and Efficiency

Three is a tradeoff between security and efficiency e.g., communication overhead, and computation cost. Mobile phones have restriction on communication bandwidth and computational capacity. Thus, we must maximize the efficiency while maintaining the required security level.

Security

The security of a group key management mechanism depends on rekeying method.

Individual rekeying provides the perfect backward security and forward security; that is, a joining client cannot obtain any former group keys, and the leaving client cannot obtain latter group keys. The formal definitions of the perfect backward security and forward security are as follows:

- **Perfect Backward Security (PBS)**

A client that joined at time t_0 can obtain no group keys at time $t < t_0$.

- **Perfect Forward Security (PFS)**

A client that left at time t_0 can obtain no group keys at time $t > t_0$.

On the other hand, batched rekeying provides the relaxed security requirements, backward security and forward security with interval τ.

The formal definitions of the perfect backward security and forward security are as follows:

- **Backward Security with Interval** τ (τ-BS)

A client that joined at time t_0 can obtain no group keys at time $t < t_0 - \tau$.

- **Forward Security with Interval** τ (τ-FS)

A client that left at time t_0 can obtain no group keys at time $t > t_0 + \tau$.

Table 1 shows the security of the mechanisms.

Table 1. The comparison of the mechanisms

Mechanism	Security	Comm.Overhead	Comp.Cost
Star&Individual	PBS and PFS	(N+2) λ	λ
Star & Batched	τ-BS and τ-FS	$\lambda + N / \tau$	$1/\tau$
Tree & Individual	PBS and PFS	$(k+2)\log_k N \cdot \lambda$	$\log_k N \cdot \lambda$
Tree & Batched	τ-BS and τ-FS	$(1+\log_k N)\lambda$	$\log_k N / \tau$

Efficiency

We evaluate the communication overhead and computational cost imposed on a client in the four mechanisms. The communication overhead is defined by the average number of distinct encrypted keys that the center issues per second. The computational cost imposed on a client is defined by the maximum number of keys that an existing client device receives per second. We assume that λ clients join and λ clients leave per second, the degree of the tree-based structure is *k* and the number of active clients is constant, *N*. Table 1 shows the communication overhead and computational cost imposed on a client in the mechanisms.

8. Conclusion

In this paper, we outlined Japanese mobile services and exposited some mobile security topics including mobile spam, mobile malware, mobile DRM system, mobile WiMAX security, and mobile key management. We should watch for the trend since mobile phone technologies are evolving quickly.

Reference

[1] Check Point Software Technologies. Check Point Full Disk Encryption. http://www.checkpoint.com/ products/ datasecurity/pc/index.html

[2] Utimaco Safeware. SafeGuard PDA. http://americas.utimaco.com/safeguard_pda/.

[3] JEAG. Japan Email Anti-Abuse Group(JEAG), http://www.jeag.jp/ (Japanese only), 2005.

[4] Inc.) Shane Coursena (Senior Technical Consultant aKaspersky Lab. The future of mobile malware. *ScienceDirect -- Network Security*, 2007(8):7--11, 2007.

[5] Mikko Hypponen. Malware Goes Mobile. *Scientific American Magazine 2006*, pages 70--77, 2006.

[6] David Dagon, Tom Martin, and Thad Starner. Mobile Phones as Computing Devices: The Viruses are Coming! *IEEE Pervasive Computing*, 3(4):11--15, 2004.

[7] Neal Leavitt. Mobile Phones: The Next Frontier for Hackers? *Computer*, 38(4):20--23, 4 2005.

[8] David Johnston and Jesse Walker. Overview of IEEE 802.16 Security. *IEEE Security & Privacy*, 2(3):40--48, 6 2004.

[9] Wayne Jansen and Rick Ayers. Guidelines on Cell Phone Forensics. Recommendations of the National Institute of Standards and Technology, Special Publication 800-101, http://csrc.nist.gov/publications/ nistpubs/800-101/SP800-101.pdf, 5 2007.

[10] Frank Adelstein. MFP: The Mobile Forensic Platform. *International Journal of Digital Evidence (IJDE)*, 2(1), 2003.

[11] Marwan Al-Zarouni. Mobile Handset Forensic Evidence: a challenge for Law Enforcement. In *Proc. 4th Australian Digital Forensics Conference*, 12 2006.

[12] Marwan Al-Zarouni. Introduction to Mobile Phone Flasher Devices and Considerations for their Use in. Mobile Phone Forensics. In *Proc. of 5th Australian Digital Forensics Conference*, 12 2007.

[13] Open Mobile Alliance. OMA Digital Rights Management V2.0. http://www.openmobilealliance. org/Technical/release_program/drm_v2_0.aspx, 3 2006.

[14] Airspan. Mobile Wimax Security. http://www.airspan. com/pdfs/WP_Mobile_WiMAX_Security.pdf, 2007

[15] WiMAX Forum. Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation. http://www.wimaxforum.org/news/downloads/Mobile _WiMAX_Part1_Overview_and_Performance.pdf, 8 2006.

[16] Taeshik Shon and Wook Choi. An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions. *Proc. of First International Conference Network-Based Information Systems (NBiS 2007), Lecture Notes in Computer Science 4658*, pages 88--97, 8 2007.

[17] Andreas Deininger, Shinsaku Kiyomoto, Jun Kurihara, and Toshiaki Tanaka. Security Vulnerabilities and Solutions in Mobile WiMAX. *IJCSNS International Journal of Computer Science and Network Security*, 7(11):7--15, 11 2007.

[18] H. Harney and C. Muckenhirn. Group Key Management Protocol (GKMP) Specification. RFC2093, http://ietf.org/rfc/rfc2093.txt, 7 1997.

[19] H. Harney and C. Muckenhirn. Group Key Management Protocol (GKMP) Architecture. RFC 2094, http://ietf.org/rfc/rfc2094.txt, 7 1997.

[20] D. Wallner, E. Harder, and R. Agee. Key Management for Multicast: Issues and Architectures. RFC2627, http://ietf.org/rfc/rfc2627.txt, 6 1999.

[21] B. Weis, T. Hardjono, and H. Harney. The Group Domain of Interpretation. RFC3547, http://ietf.org /rfc/rfc3547.txt, 7 2003.

[22] H. Harney, U. Meth, A. Colegrove, and G. Gross. GSAKMP: Group Secure Association Key Management Protocol. RFC4535, http://ietf.org/ rfc/rfc4535.txt, 6 2006.

[23] T. Hardjono and B. Weis. The Multicast Group Security Architecture. RFC3740, http://ietf.org/rfc/ rfc3740.txt, 3 2004.

[24] Chung Kei Wong and Mohamed Gouda and Simon S. Lam, "Secure Group Communications Using Key Graphs", "IEEE/ACM Trans. on Networking",

Kouichi Sakurai received the B.S. degree in mathematics from Faculty of Science, Kyushu University and the M.S. degree in applied science from the Faculty of Engineering, Kyushu University in 1986 and 1988, respectively. He was engaged in research and development on cryptography and information security at the Computer and Information Systems Laboratory at Mitsubishi Electric Corporation from 1988 to 1994. He received his doctorate in engineering from the Faculty of Engineering, Kyushu University in 1993. From 1994, he worked for the Department of Computer Science of Kyushu University in the capacity of associate professor, and became a full professor in 2002. His current research interests are in cryptography and information security. Dr. Sakurai is a member of the Information Processing Society of Japan, the Mathematical Society of Japan, ACM, IEEE and the International Association for Cryptologic Research.

Kazuhide Fukushima received his M.E. in Engineering from Kyushu University, Japan, in 2004. He joined KDDI and has been engaged in research on digital rights management technologies, including software obfuscation and key-management schemes. He is currently a researcher at the Information Security Lab. of KDDI R & D Laboratories Inc. He is a member of the Institute of Electronics, Information and Communication Engineers, Information Processing Society of Japan, and ACM.