Security in Mobile Digital Rights Management

K. Bokunić, L. Budin, M. Golub
Department of Electronics, Microelectronics, Computer and Intelligent Systems
Faculty of Electrical Engineering and Computing, University Of Zagreb
Complete Address: Unska 3, HR-10000 Zagreb, Croatia
Phone: (+385-1) 6129 967, E-mail: kbokunic@vip.hr, leo.budin@fer.hr, marin.golub@fer.hr

This paper represents a technical overview of a current state in the Mobile Digital Rights Management (MDRM). It describes Download architecture and different DRM use cases specified by Open Mobile Alliance (OMA) DRM standards. OMA DRM technologies, such as Rights Expression Language, DRM Content Format, and Cryptography are discussed. The paper analyzes security model, specially, rights integrity, content confidentiality and rights-content association integrity. It points out problems in security model that were not solved in OMA DRM version 1 specification. The paper also shows the limitations for developing security model in MDRM systems.

I. INTRODUCTION

Mobile phones have become a very important part of our daily lives. Today, they are more widespread than personal computers and everybody are using them. The first generation of mobile phones offered analog communication capabilities, the second generation offered digital radio technologies with high-speed data transfer technologies throw the use of GPRS and EDGE technologies and multimedia capabilities, and the third generation with the use of UMTS will offer even more speed needed for live-streaming services. With the arrival of multimedia mobile phones, new business opportunities, such as selling of valuable digital content like images, ring tones, games, emerged. But the big problem exists, because of which these business opportunities cannot be fully exploited. The problem is in possibility to copy and share valuable digital content among mobile devices with no cost for intellectual and usage rights. Solutions for this problem are in introduction of Mobile Digital Rights Management. MDRM can be defined as a set of actions, procedures, policies, product properties, and tools that an entity uses to manage its rights in digital contents according to requirements over the mobile networks. MDRM technology will probably become the most important component of the future mobile devices.

II. MOBILE PHONES LIMITATIONS

The mobile phones are small devices with limited processing power and memory. Their batteries have limited lifetime and they still use low-bandwidth communication technologies. Mainly because of limited processing and memory resources, mobile devices cannot accommodate the most strong, computationally intensive encryption technologies that would enable the implementation and the use of strong DRM protection methods. The connection and communication speed, in the most cases, are to slow and the transaction performance are too bad for many people to accept. There are also limitations on user interface design because services must be designed to satisfy small display of the mobile devices and they must be simple so usability could be acceptable by potential users. Mobile devices have also limited hardware resources that also restrict the embedded software. In the most cases devices cannot support large code libraries to fulfill various functions as personal computers can. Because of that, the essential code for strong security cannot be implemented in small, computationally limited mobile devices.

III. OPEN MOBILE ALLIANCE DIGITAL RIGHTS MANAGEMENT

The Open Mobile Alliance (OMA) is an open standardization body dedicated to defining an open standard based framework for mobile services and with a membership of more than 250 worldwide companies.

In November 2002, OMA has defined and published the first version of standard for MDRM, which was immediately available for the companies to implement in their mobile products. The specification concentrates on content packaging and expression of rights, permissions and constraints. It does not include strong security mechanisms to protect the content. The DRM solution specified in the first version should not be considered as a strong secure DRM system, rather to be seen as a system that intends to keep the honest people honest.

From the first release, the OMA is working on definition of second version of standard for MDRM but it still has not been finished and published in final form.

IV. OMA DRM USE CASES

As already said, there exists a need for content provider and mobile operators to control the usage of downloaded media objects. By means of download a media object is delivered to the device, and MDRM is the mean to control the usage of the media object once it has been downloaded. MDRM enables content providers and operators, by the means of digital rights, to define rules for how the media object should be used. With the use of MDRM, the value lies in the rights object and not in the media object itself, so it is possible to sell the rights to use the media object, rather then selling the media object itself.

OMA DRM defines three different use cases or downlaod methods for DRM protection of mobile content and delivery of the rights object:

- Forward-lock method
- Combined delivery method
- Separate delivery method

Forward-lock download method does not provide real DRM protection for the media content. In this case media content is not protected with any cryptographic method. All this method prevents is just the possible forwarding of the content from one mobile device to another. DRM message format has an implicit restriction, namely that the DRM message and the included media object cannot leave the receiving mobile device after reception. It can be stored on the device and consumed without restriction, but only on that device. In this method rights object is not present, so content providers have to package only media content into DRM message, and then by using OMA Download mechanism deliver it to the consumer mobile device.

Combined delivery is more complex download method then the forward-lock. It also does not include any cryptographic method for the protection of media content but it introduces concept of rights definition on content usage, which enables the possibility to define more fine-grained access control over the content. Permissions and constraints on content usage can be defined through the means of rights, and without them media content cannot be used and is useless. In the case of combined delivery rights object is, together with the media content, packed into one DRM message and by the use of OMA Download mechanism delivered to the consumer mobile device. The media object and the rights object are bound to each other by a unique content identifier.

Separate delivery method is the most complex download method and it provides cryptographic means for the protection of media content. In this method, media object is in the special format, which is called DRM Content Format, delivered separately from rights object to consumer mobile device. The content providers by the means of symmetric encryption need to encrypt plaintext media object, packed it into protected DRM content format and then by using OMA Download mechanism deliver it to the consumer device. After the protected content has been delivered, content providers can deliver the rights object which in this case, besides the usage rules, contains content encryption key for decryption of protected media object. When mobile device receives rights object it can use encryption key to decrypt and render the media object according to the permissions granted in the rights object. The protected media object and the rights object are bound to each other by a unique content identifier. One of the problems in this approach is latency time between receiving the content object and the rights object. In order to enable a good user experience this must be taken into account by service implementers.

Separate delivery has one big advantage considering other methods and that is the possibility to super-distribute media content. The mobile device can forward, super-distribute, the protected media content in DRM content format to another device. The rights object are not allowed to be forwarded to other devices, or to leave, by any means device that has received it. Receiving mobile device cannot use protected media content, since it is encrypted, without buying and downloading rights object with the proper usage permissions and content encryption key, from content provider or rights issuer.

Separate delivery is the only download method, at the present time, which provides certain level of security and protection over the usage of mobile content, although it has its weaknesses.

The biggest advantage of separate delivery method is the possibility for users to try the content before they fully buy it. This is achieved with separate delivery of encrypted media object and rights object. Users have to download only once the full version of media content they are interested to buy. After that, in order to only try it, they have to request and download only limited, usually free set of permissions on content usage. After preview, if they like the content, they do not need to download it once again, all they have to do is to request and download additional permissions on content usage. Separate delivery is also the only method that provides some level of content protection with the content encryption, and because of that it is suitable for distribution of more value content. The main weakness of this method is in the lack of rights object integrity and this will be discussed latter in text.

Forward-lock method was designed with the purpose to prevent content forwarding from one device to another. It also had to be easily and quickly deployed on mobile devices so it must have stayed as simple as possible. Its main task, content forwarding this method satisfy, and as it was not imagined and designed for the strong content protection with the use of encryption mechanisms this lack is not its disadvantage. This method can be successfully applied as a protection from forwarding of low-value media content.

Combined delivery method is a transitive concept between forward-lock and separate delivery method but it is too complex to be implemented and used because it has too few advantages and too many disadvantages. The main advantage for this method is introducing the concept of fain-grained management of permission on content usage. Unfortunately because of combined delivery of content object and media object this advantage is not exploited good enough. This method, like forward-lock method, does not use any cryptographic method to protect content and rights object. Compared to other methods, this method is almost as complex as separate delivery method, but its level of protection is as low as in forward-lock method, so it is abandoned.

Although, these three methods for media content delivery and protection have many weaknesses, they have solved two big problems with content distribution in the mobile domain. The first problem that was mainly solved was the introduction of standardized way to prevent users from forwarding media object from one device to another, which was achieved by forward-lock method. The second problem, which was solved with separate delivery method, was possibility for users to preview and try content before it is purchased. Without separate delivery method, users either have to pay before even having a chance to preview the media object, or they are presented with a “crippled” low-quality variant of the content that they want to buy. With the introduction of fine-grained access control over media content through the rights object and possibility to deliver rights independently from media content, users must only once download the content they want, acquire the rights on limited usage and if they like it, they can always acquire additional permissions on content usage.

V. POSSIBLE ARCHITECTURE OF AN OMA COMPLIANT DRM SYSTEM FOR MOBILE DOMAIN

OMA DRM specification does not specify system architecture or required entities for the MDRM systems. However some components are essential and are in practice needed in an OMA compliant DRM system.

Those components could be:

- Packaging server for converting media content into DRM content format
- License server for issuing rights, determine permissions and constraints and managing content
- Content server for hosting and presenting content in OMA DRM format
- Download server for downloading protected content in DRM content format
- Payment server for monetary transaction
- Compliant DRM agents implemented in mobile devices

Moreover, several of these server side components can be integrated into one server.

Compliant DRM mobile devices must have implemented DRM agent that could recognize and in proper way handle DRM content and rights objects and that can control and limit content usage based on its rights. They must also have tamper-resistant memory for storing rights object and content encryption keys, and depending on the implemented method, encrypted or decrypted media content object.

VI. RIGHTS EXPRESSION LANGUAGE

The Rights Expression Language (REL) is the part of OMA DRM specification, and it defines the syntax and semantics of rights governing the usage of DRM content. DRM content is consumed according to the rights specified in rights object and not in the content object itself. Rights are the collection of permissions and constraints defining under which circumstances access is granted to DRM content and they also define what that content is allowed or restricted to do.

The structure of the REL enables the following functionality:

a) Metadata, such as version and unique content identifier;
b) The actual rights specification consisting of:
    a. Linking to and providing protection information for the content
    b. Specification of usage rights and constraints

One of the most important parts of DRM REL is security model that is designed to:

a) Enforce the integrity of rights;
b) Ensure the controlled consumption of DRM content;
c) Enforce the integrity of the association between rights and DRM content.

Unfortunately only the controlled consumption of DRM content is a normative part of the first OMA DRM specification, and other part of the security model should become normative in the second OMA DRM specification.

VII. DIGITAL RIGHTS MANAGEMENT CONTENT FORMAT

DRM Content Format, as a part of the OMA DRM specification, defines format for DRM protected encrypted media object and its associated metadata and is intended to be used in the separate delivery DRM download method in which the media object is delivered in encrypted form. Content Format is closely related to the REL.

Besides defining encrypted media object, content format contains following metadata:

- Original content type of the media object;
- Unique identifier for this DRM protected media object to associate it with rights;
- Information about the encryption details;
- Information about the right issuing service for this DRM protected media object.

In the first OMA DRM specification, AES symmetric encryption algorithm is defined as the encryption method. In this case, it uses 128 bit encryption keys, cipher block chaining mode and 128-bit initialization vector prefixing the cipher text. At the present time, AES symmetric encryption with 128 bit key length is considered completely secure cryptographic method.

VIII. SECURITY MODEL

Security of the media content in MDRM systems is based on rights integrity, content confidentiality and right-content association integrity.

RIGHTS INTEGRITY

Rights integrity protection prevents illegitimately modifying the rights specified over DRM content. It includes adding, deleting, and modifying permissions and constraints over an asset, reference to the asset itself, and meta information included in the rights.

Unfortunately, in the OMA DRM specification version 1, rights integrity is not protected by encryption methods, so it depends on the rights storage protection and the delivery mechanism of the rights object.

CONTENT CONFIDENTIALITY

In the specification of OMA DRM systems content confidentiality is protected by:

- encryption of DRM content in the separate delivery method,
- sharing the key required to decrypt the DRM content only with the parties that are authorized to consume the content.

Media content is encrypted using a symmetric algorithm AES, which means that content confidentiality is achieved by the controlled distribution and the confidentiality of the content encryption key (CEK), from which content decryption key can be derived. CEK is a part of rights object, and is distributed to the consumer devices together with the usage rights and constraints. However the big problem is that by the specification, CEK inside the rights object is not encrypted and thus its confidentiality depends on the delivery mechanism of the rights object, and rights object integrity.

RIGHTS-CONTENT ASSOCIATION INTEGRITY

Rights object contains permissions and constraints on the usage of media content, and the DRM systems must not allowed usage of the content in any way without proper rights object. Because of that, the ability to replace the DRM content governed by rights amounts to the ability of changing the rights itself. Rights-content association integrity is achieved by content unique identifier, which is present in the rights object and DRM content format object, and it connects content with its usage rights. The association between rights and the corresponding DRM content must be integrity protected, as much as the specified right itself, in order to prevent content replacement on which rights relates.

Unfortunately since the rights object is not protected by encryption methods, rights-content association integrity in the rights object is as save as the rights itself and it depends on the rights storage protection, the delivery mechanism of the rights object and rights integrity.

IX. POSSIBLE IMPROVEMENTS IN THE SECURITY MODEL

OMA DRM specification version 1 has many insufficiently good and detailed specified parts of the security model that can endanger content usage and rights object protection.

Concerning rights object protection, a big drawback is a lack of encryption protection of the rights object. Rights object contains crucial information such as permissions and constraints on content usage, content encryption key, content confidentiality and rights-content association integrity. Rights integrity can ensure that permissions and constraints cannot be modified without detection. The problem is that there is no normative specification for the rights integrity. Rights integrity could be enable throughout encryption of the rights object. The encryption of the rights object, rise another problem and that is nonexistence of something like Public Key Infrastructure (PKI), with private and public keys, in the mobile domain at the present time. When PKI would exist in the mobile domain, content providers and operators could guarantee rights integrity by encrypting the rights object with the public key of the device for which the rights are intended, and only that device could access rights by decrypting them with its own private key.

Without encryption methods, rights integrity, lies on the rights storage protection and the delivery mechanism of the rights object, which is not adequate protection.

The protection of the content confidentiality is an essential part of enforcing consumption control of DRM content, and it is done by encryption of the DRM content. The content encryption key, by which end devices can decrypt the DRM content in order to use it, is stored in rights object together with permissions on content usage. The content encryption key inside the rights object is not encrypted and thus its confidentiality depends on the rights object protection and integrity. As already said, rights object protection is not adequate and confidentiality of the encryption key is not on needed level. With the encryption of the rights object, content confidentiality problem would also be solved.

Another problem is lack of strong protection for rights-content association integrity. Rights-content association integrity, which in fact is content unique identifier, must be protected on both sides, in the DRM content and in the rights object. Content unique identifier inside rights object is a reference to the DRM content object that contains encrypted media object on which usage permissions and constraints should be applied. Content unique identifier inside rights object is in plain text format so it means that its protection and no changeability depend on the rights object protection and integrity. As we already know, protection of data inside rights object and rights object itself is very weak and is not adequate to protect content unique identifier from possible modification. With the encryption of the rights object, content unique identifier could not be modified on the side of the rights object but there is a problem with content unique identifier protection in DRM content. Strong protection of the content unique identifier does not mean much if it can be easily changed in the DRM content. Unfortunately content unique identifier in the DRM content is a parameter in the plain text format, so it does not have any kind of protection. One of the possible ways to secure content side of the rights content association without addition signing or encrypting of DRM content is by the hash value. The hash value of the encrypted content with content unique identifier, stored in the rights object would guarantee unmodified DRM content on which hash value was calculated. The integrity and no changeability of the encrypted content and content unique identifier are guaranteed by the characteristics of the hash function itself. Any modification of the object upon which hash value was calculated would cause a new hash value of the tempered object. The new hash value would not correspond to the hash value of the original object stored in the rights object, and that content would be rejected.

Including the hash value of the DRM encrypted content with content unique identifier in rights object would only make sense if the integrity protection of the rights object is achieved. As it was emphasizes earlier, the rights object integrity can be achieved by encrypting rights object, and together with including the hash value of the DRM encrypted content with content unique identifier in rights object would solved rights-content association integrity problem.

X. CONTENT PROTECTION BY INTERNATIONAL MOBILE EQUIPMENT IDENTITY

Beside PKI, for better content protection and integrity problem solution it is possible to use some other unique information that already exists on mobile devices. Every mobile device has its own unique International Mobile Equipment Identity (IMEI), 15-digit number which value is device aware of. This unique value, IMEI, could be used for content protection in the way it could serve like content encryption key or it could be used for content signing. The media content could be encrypted with the IMEI so only the device with right IMEI value could decrypted it and use it. Other approach is to use IMEI for signing media content so only one device could use it. Or maybe plain text content could be packed in the protected message with unique identification value that could be derived from IMEI so it could be used only on one device with that IMEI value.

This approach, with IMEI signing of media content was already tried and implemented by some content providers and mobile device manufactures. In their implementation, media content objects were signed with IMEI of the device for which content was intended. Only that device could use the content signed in this way, so if a user would forward content to other device, its IMEI value would be different and content could not be used.

In this way content could be forwarded to other devices, and there was no protection against this because that device could not use it and forwarding of the content was useless. This approach was adequate for content protection although it does not possess strong cryptographic mechanisms.

This approach of content signing was not become very popular and used method for content protection, and was abandon by the most mobile operators. One of its disadvantages was the lack of fain-grained control of content usage through the possibility of defining permissions and constraints in the rights object that in fact did not exist. But the main reason for its failure was in too bad user experience and unfriendliness, because of which it was badly accepted by the users. In order to sign the content with the IMEI value, content providers or mobile operators had to know it. Most mobile operators do not know or have database with the IMEI values of the devices their users possess, so they could not sign the content without users involvement. Users had to send their devices IMEI value before starting every content download. This approach was to difficult and unfriendly for the most users so they did not accept and used services based on it. Because of this reasons this protection method was mainly abandon.

XI. SECURITY TRADE-OFFS

There exists security trade-offs mainly because of the missing key management infrastructure, low user experience in some cases and the nature of the threat on the content. Reusing of existing solutions, like IMEI signing protection, or emerging key management solutions like Wireless Identity Module (WIM) is not directly possible for MDRM purpose because the threat models in DRM and WIM are different. In WIM the end user is the target of attacks, but in MDRM systems the end user is the potential attacker on the content himself, and the content must be protected from the end user as well.

Without the appropriate terminal key management infrastructures and device storage security there are no good enough cryptographic means to protect against all security threats on high-value media content. The use of separate rights and content delivery can increase the content security and protection due to increased complexity of stealing the rights from the device without which media content is useless.

XII. CONCLUSION

This paper analyzes current state in the Mobile Digital Rights Management. In the past few years, mobile devices have developed from strictly voice to multimedia enable devices, capable of using high-value media contents. From business and intellectual property point of view, such contents cannot be distributed and used without DRM technology in order to protect it from illegal distribution and usage. Initiated by the lack of usable Mobile DRM standard, the Open Mobile Alliance has developed a first open mobile DRM standard, which was widely accepted from content providers, device manufactures and mobile operators. The standard in its first version does not define strong cryptographic methods for content protection, than it is more concentrated on content packaging and the specification of usage rights and constraints. It defines three different methods for DRM protection of media content and delivery of the rights; forward-lock, combined delivery and separate delivery. All the methods have their weaknesses but the most complex method, separate delivery, is good enough to make its breaking worthless considering the present content value distributed through the mobile networks. As the present value of distributing content has intension to grow, stronger and more secure content protection mechanisms are needed. For the last few years, OMA is developing second version of standard for MDRM which will have stronger security mechanism for content protection based on cryptography methods, secure download protocols and mobile version of the PKI solutions. It success will mainly depend on implemented security technology, usable business models, its acceptability by content and service providers and, the most important of all, content users.

REFERENCES

[1] E. Becker, W. Buhse, D. Gunnewig, N. Rump, *Digital Rights Management: Technological, Economic, Legal and Political Aspects*, M&T Books, New York, 2002.

[2] B. Rosenblatt, B. Trippe, S. Mooney, *Digital Rights Management; Business and Technology*, Springer-Verlag, Berlin Heidelberg, 2003.

[3] Z. Yan, "Mobile Digital Rights Management", *T-110.501 Seminar on Network Security 2001*, ISBN: 951-22-5807-2, available from: http://www.tml.hut.fi/Studies/T-110.501/2001/papers/index.html

[4] "Developers Guideline Digital Rights Management", Sony Ericsson Mobile Communication AB, Lund Sweden, 2004.

[5] T.S.Messerges, E.A.Dabbish, “Digital Rights Management in a 3G Mobile Phone and Beyond”, *ACM Workshop On Digital Rights Management*, ISBN: 1-58113-786-9, p. 27-38, ACM Press New York USA, 2003.

[6] Q.Liu, R. Safavi-Naini, N.P. Sheppard, “Digital Rights Management for Content Distribution”, *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003 - Volume 21*, p. 49-58, Australian Computer Society Inc, Darlinghurst, Australia, 2003.

[7] “DRM Content Format Version 1.0”, Open Mobile Alliance™, OMA-Download-DRMCF-v1_0.*, 2002. available from: http://www.openmobilealliance.org/

[8] “Rights Expression Language Version 1.0”, Open Mobile Alliance™, OMA-Download-DRMREL-v1_0.*, 2002. available from: http://www.openmobilealliance.org/

[9] “Digital Rights Management Version 1.0”, Open Mobile Alliance™, OMA-Download-DRM-v1_0.*, 2002. available from: http://www.openmobilealliance.org/

[10] “Enabler Release Definition for DRM Version 1.0”, Open Mobile Alliance™, OMA-ERELD-DRM-V1_0.*, 2002. available from: http://www.openmobilealliance.org/

[11] “Generic Content Download Over The Air Specification Version 1.0”, Open Mobile Alliance™, OMA-Downlaod-OTA-v1_0.*, 2003. available from: http://www.openmobilealliance.org/

[12] Open Mobile Alliance, available from: http://www.openmobilealliance.org/

[13] Forum Nokia – Developer Resources, available from: http://www.forum.nokia.com/main.html

[14] Sony Ericsson Developer World, available from: http://developer.sonyericsson.com/

[15] Synergenix Interactive AB, available from: http://www.synergenix.se/