Home network application security (MHP)

Junchun Luo
Department of Computer Science and Engineering
Helsinki University of Technology
junchluo@cc.hut.fi

Abstract

Multimedia Home Platform is the open standard platform for interactive TV and multimedia services. This paper generally introduces the security mechanism the MHP provides, defines the security requirements for the consumer, the service provider and the broadcaster. Finally based on criteria: confidentiality, integrity, availability, privacy and non-reputability, the security mechanism in MHP is analyzed.

1 Introduction

Since the Digital Video Broadcasting (DVB) project was established in 1993, a large family of standards for almost every aspect of digital broadcasting have been published and adopted by European Telecommunications Standards Institute (ETSI) [2]. Numerous DVB-type services have been introduced since then in Europe, even in the worldwide. From another point, Internet plays more and more important role in the world, especially the foundation of the World Wide Web. As the global solution for digital television and related multimedia services, Multimedia Home Platform (MHP) will stimulate the growth of the broadcasting Industry into the multimedia age, which will link the broadcasting and Internet worlds together.

This paper first briefly introduces architecture of MHP. Then it analyses different security requirements of the consumer and the operator. Next the basic security mechanism provided by MHP is stated. Finally, based on general security metrics like confidentiality, integrity, availability, non-reputability and privacy, some conclusions about the MHP security mechanism are made. Among these criteria, the availability is related to capacity of the broadcast channel and IP network routes. This paper has not discussed it in detail.

2 Multimedia Home Platform

2.1 Overview of MHP

The MHP is the open standard platform for interactive TV and multimedia services. MHP is based on Internet and web standards, so it offers compatibility and convergence between TV and the Internet [1]. There are several MHP standard versions defined by ETSI. At the

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

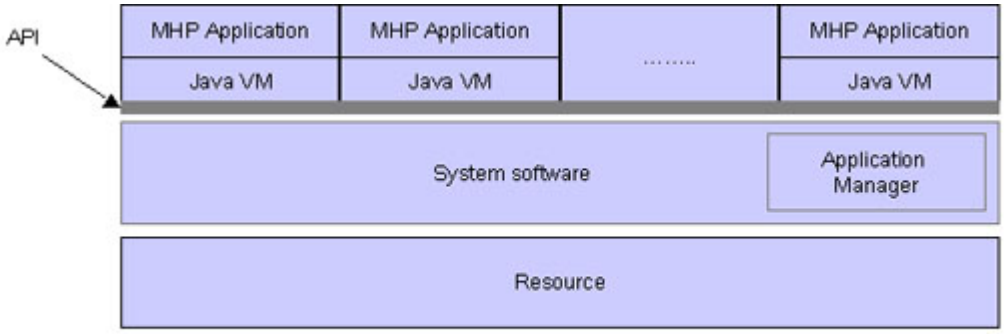

Figure 1: MHP basic architecture

moment, all broadcasting is done using version 1.0.1, which will be replaced by 1.0.2 after it has become public. Next standard version is 1.1 which can be downloaded from ETSI, it will be used for the future applications.

MHP is in fact a common Application Programming Interface (API) defined by DVB project. DVB is a European-based consortium of broadcast companies and regulatory bodies. DVB standards are published by the ETSI. MHP allows for the creation and broadcast of interactive television applications that will run on any set-top box (STB). It is independent of the hardware platform that it is running on [2]. In other words, MHP defines a generic interface between interactive digital applications and the terminals on which those applications execute. This interface enables digital content providers to address all types of terminals such as set-top boxes, integrated digital TV sets and multimedia PCs.

The architecture of the MHP is defined in terms of three layers: *resources, system software* and *applications* [1, 2, 4].

The *resources* include hardware resources and software resources, which are representatives of hardware entities in the platform. The resources are provided to the MHP transparently. An application should be able to access all locally connected resources as if they were elements of a single entity. Typical MHP resources are MPEG processing, I/O devices, CPU, memory and a graphics system.

The *system software* uses the available resources in order to provide an abstract view of the platform to the applications. Implementations include an application manager (also known as a "navigator") to control the MHP and the applications running on it.

The *applications* implement interactive services as software running in one or more hardware entities. The interface for MHP application is a top view from application to the system software.

The core of the MHP is based around a platform known as DVB-J [2]. This includes a virtual machine as defined in the Java Virtual Machine (JVM) specification from Sun Microsystems. A number of software packages provide generic APIs to a wide range of features of the platform. MHP applications access the platform only via these specified APIs. MHP implementations are required to perform a mapping between these specified

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

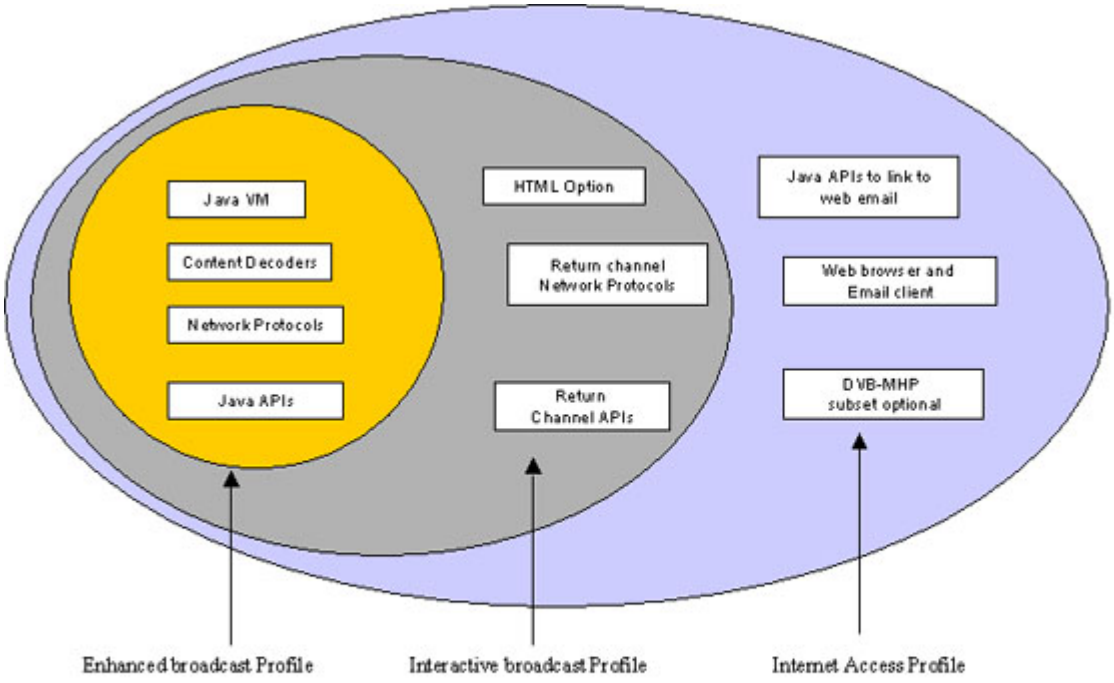

Figure 2: MHP profiles

APIs and the underlying resources and system software.

2.2 Application Models

The MHP 1.0.1 defines two modes called profiles:[1, 2, 11]

- *Enhanced broadcasting profile*: for one-way broadcast services. The enhanced broadcasting downloads of Java applications through the broadcast channel. It combines digital broadcast of audio/video with downloaded applications that enable local interactivity. It uses advanced digital technologies to improve quality of broadcasting and efficient use of frequency. This profile has no ability to enable user interactive with the broadcasting programs, so the interaction channel is not needed.
- *Interactive broadcasting profile*: for two way interactive services. These profile enables users operate interactive to the broadcasting programs. The operation needs support of worldwide communication network. So this profile needs return channels for the users to request services.

The MHP 1.1 adds the third profile:

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

- *Internet access profile*: Internet based services. This is the next target of MHP-DVB. This profile enables the user to access Internet via digital TV or set-top box, which means that the user can browse the Internet with their TV instead of a PC. And PC can be used to view the the broadcasting programs too. This profile can achieve real interaction between user and operator in Internet field and broadcasting field.

2.3 Users of MHP

The MHP extends the existing and successful open DVB standards for broadcast and interactive services in all transmission networks including satellite, cable, terrestrial and microwave systems. It supports many kinds of applications including the following typical examples [2, 12]:

- Electronic program guides (EPG),
- Information services (super teletext, news tickers, stock tickers)
- Applications synchronized to TV content - score cards, local play-along games
- E-commerce and secure transactions
- Educational

The user of MHP platform can be divided into three main categories [6]:

- **Consumer** - the person at the end of the chain, who actually watches, listens to or interacts with the content.
- **Broadcaster** - an entity that operates channels of popular one-to-many multicast content.
- **Service Provider** - an entity that provides services to consumers, which are either paid for by the consumer, or funded in some other way.

The consumer represents the end-user of the MHP platform. They don't care about the technical details in MHP. Their focus is on the service they got. So how to get attractive service with low price is the main point of consumer. In the mean time, the consumers also take care of their privacy in network. Their credit card numbers, passwords, user accounts, private contact information must be kept secret to any unauthorized users.

The broadcaster operates the channel carrying audio, video data to consumer or IP packet back to the service provider. They care about that the channel will not be misused. The use of channel must be paid. The information transferred on the channel is legal.

The service providers rent the channel to broadcast program to consumer. They often store consumers' information in some database servers. Assign user account to the authorized consumer. Only these consumers can listen to or view the programs. Others could not decrypt the program even if they can receive it. They should also protect against malicious users who will do harmful operations via back channel.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

For example, Multimedia Car Platform (MCP) is a practical usage of MHP as its fundament. MCP security is based on MHP in the following fields: Java security related to MHP, application priorities, access rights to resources, Permission Request File for signed applications and hash codes of hierarchical file systems. [9]

3 Security Requirements in MHP

This chapter first defines general security requirements in MHP application. Second the security requirements for consumers, service providers and broadcaster are discussed.

3.1 General security requirements

The MHP security model should embrace all the functions and components like the hardware, operating system, applications and content data of the MHP. It must maintain the integrity of the MHP terminal, the integrity and validity of the content, software and data held in the MHP or transmitted to or from it.

In general, the MHP security model should guard against the following problems: [5]

- Malicious damage of the MHP device by an application
- "Denial of Service" through competing applications, malicious attacks or other means
- Unauthorized use of user data
- Unauthorized use or theft of content
- Maintaining integrity of content in the content delivery chain
- Prevent unauthorized use of the return channel
- Unauthorized access to the communication on the return channel

In other words, the MHP should provide authentication and verification systems that validate incoming applications to the MHP. How to check the operation of application and their use of the MHP's resources is also needed. A password system that allow access to secure applications or online sites is necessary. Furthermore, a copyright system that manage the storage of content within the MHP should be considered, an encryption system that guard against the theft of content is of course needed.

Moreover, DVB has defined some security requirements: [4]

- The API should be accompanied by a system, which incorporates a common security model for the applications and data. It should enable full compatibility between the signals transmitted by the different broadcasters and content providers.
- The security model should include a description of the procedures and entities that must be put into place to support the associated secret management issues.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

- The security model should be independent of Conditional Access (CA) systems. The MHP API should give access to CA functions, if and when required. The CA is related to pay-TV issues. In many cases DVB-based services will either be of the "pay" type or will at least include some elements, which are not supposed to be freely available to the public at large [13]. The CA describes systems that enable the control over the access to programs, services. One should not consider this CA as Certificate Authorization that is a general concept in PKI.

Machine protection against abusive requests for system resources is one important security aspect. Another aspect to be addressed is protection against non-authorized access to data.

3.2 Security requirements for consumers

The main security problem for consumers is privacy. How to protect their private information, how to get service without intruding by unauthorized users are their main considerations. So the requirements defined here concentrated on privacy.

An application running on the MHP shall not be able to access private information such as Personal Identification Number (PIN) or credit card numbers that have been supplied to previous applications. An application shall not access private information without preliminary authorization from the consumer also. The MHP terminal shall not allow unauthorized access to private data, which is stored in the MHP terminal or other device connected to the home network by third party. An application running on the MHP platform shall be able to request and use security resources when available. A common internal, operational and API-related security model needs to be defined for data and applications. It shall be conditional access independent. MHP should have internal and operational security aspects including anti-piracy mechanism, secure transaction, value transfer and user authorization mechanism [5]. Cross-application data management, sharing of private sensitive information and secure time stamping should be included in MHP security too. The owner of the MHP should be able to change the resources that are granted to unauthorized applications. Sensitive user data stored in MHP terminals must be encrypted.

3.3 Security requirements for service provider

The main security problems for a service provider are information confidentiality, integrity and non-reputability. The service provider must keep almost all types of information in confidentially to enhance its competition in the market. Information should be integrity and consistent to make it usable. When some consumers want to deny the service the provider has provided, how to give evidence is also important for a service provider.

For example, the service provider should store user information in secure and safe repository, including both physical security and information security storage. The application should not do harm operations on consumer's equipment. The service provided and relative confirmation from consumer must be logged, so any malicious operation can be recorded to provide evidence for punishing the intruders. System crashes can be graceful recovered quickly, any user in the system will not be affected heavily. Of course it's better if it does not affect the users. User must be able to escape from unaccepted application whenever

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

he wants. Applications can terminate appropriately and resources are correctly released when the users want. Unauthorized user could not access system information via return channel, this is because the MHP applications can be downloaded from return channel. As an IP based connection, return channel must provide additional security mechanisms. Access rights to authorized applications must be carefully considered. This can ensure that users with different privileges can access different levels of resources. The virus checking is needed to consider from both data transmission directions. The service should detect possible viruses from return channel. The same happened to the consumer. Their STBs, TVs or other instruments must be protected against the virus.

3.4 Security requirements for broadcaster

The broadcaster is responsible for operating channels. So how to keep the communication secure between the consumer and the service provider is the main task.

One important task is that the sensitive information transferred must be encrypted. Because the radio signal is unavoidable to be listened by malicious users, the information transferred must be encrypted so that it is difficult for intruders to get useful information from the radio signals. The connection from the consumer to the service provider should be authenticated and encrypted including both the broadcast stream and return channel data. A secure connection could guard variety general attacks on the information system. The broadcaster should detect malicious tampering with application code and non-real-time data [5]. Unauthorized application could not request return channel for interaction with service provider. Since return channel gives the consumer ability to interact with the servers, it is dangerous for an unauthorized user to access such servers.

4 Security Mechanism In MHP

MHP provides complicated security mechanism. This chapter first gives an overview of this mechanism, then introduces security provides by MHP in detail including authentication of applications, security policy for applications, authentication and privacy of the return channel communications and certification management.

DVB-MHP has defined a security model in MHP210R8 [5] that MHP solution must support. This model ensures the smooth operation and privacy of the MHP. It also guards the MHP against a number of different problems without preventing reasonable business models.

4.1 Overview of MHP security framework

The MHP security framework enables a receiver to authenticate the source of application code or other files. All the authentication messages are stored as files in specific directories, transferred to the receiver along the broadcast information. The system uses three different security messages [1]:

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

- **Cryptographic hash codes** This provides a summary of a quantity of data - typically a subset of the total set of data under consideration.
- **Signatures** These deliver a master hash code (computed over all of the appropriate data) that has been "signed" by an authorizing organization. The signing process securely associates the master hash code with the signatory. The hash code process shows that the data has not been tampered with since it was signed by the signatory.
- **Certificates** These provide a "chain of trust" from the authorizing organization up to some trusted third party (the root certificate authority) that is well known to the receiver.

The messages are delivered within files of the file system so this authentication scheme is applied to any hierarchical file system operating over the broadcast channels.

4.2 Authentication of application

The authentication of applications uses three message types: hash codes, signature and certificates. Each message is placed in a file.

Files and directories are two types of information for application hash codes. The hash computation considers the content and attributes of the objects rather than transport specific information. So the authentication is independent of the underlying transport protocol.

The signature references a certificate containing the public key required to decode the signature. It also identifies the hash algorithm used and the value of the signature.

Finally, the certificate provides a public key that can be used to decode a hash code contained in a signature and so enable a tree to be verified. A higher certification authority signs the certificate itself.

Since objects are organized hierarchically, authentication is on such hierarchical structures. Hash codes are computed systematically and accumulative across some or all of the objects in the hierarchy. The algorithm used in hash computation is MD-5 or SHA.

A signature at the top of the hierarchy identifies the source of the objects. This framework enables the authentication of a file system with a single signature. And only the objects that are loaded need real-time hash code checking.

A certificate mechanism is specified to embraces key distribution to ensure that the key used to compute the signature is valid and used by a certified service provider.

The authentication rules are: [1]

1. Confirm that the file is listed in the hash file located in the same directory as the file to be authenticated
2. Verify that the file contents and corresponding digest value are consistent
3. Recursively ascent the directory hierarchy checking that each directory is authenticated by its parent directory until a directory is found that contains one or more signature files

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

4. For a signature file locate the corresponding certificate file
5. Follow the certificate chain contained within the certificate file verifying each link in the chain until the link to root certificate is found
6. If the identified root certificate and all the intermediate certificates leading to it are "satisfactory", accept the files as being authenticated
7. Dependant on receiver policy returns to step 3 and repeat for other signature files.

4.3 Security policy for applications

The security policy for applications focuses on the resource accesses policy for the download applications. [1] The resource access policy depends on two factors: access rights requested by the broadcaster through the signaling and the access rights granted by the user. The ultimate access rights that are granted to the applications are the intersection of the requested rights and granted rights.

In general, unsigned application and signed application have the same access rights to platform resources. An application broadcaster can request additional permission to access specific resources by providing a signed "Permission Request File" (PRF) along with the application [1]. The PRF may also contain a credential that indicates that a persistent file owned by another organization may be accessed. If the PRF is not correctly authenticated the application is not granted any additional permission.

When an application first requests to retrieve data from a file that is signaled as being signed, the hash value is compared. If the MHP failed to match the computed hash value with the expected hash value, the API concerned shall fail too. Since the API must be kept consistent with the pre-defined behavior when the file exists but has no content in it.

The authentication of a file is evaluated each time that the file is loaded from a transport connection. File version information in the transport system cannot be assumed to be secure.

The time that the implementation must decide if an application has permission or not is:

- When the application queries the presence of this permission for the first time,
- When the application invokes an action that requires the permission for the first time.

An MHP terminal is required to be able to operate in a mode where it grants permission to provide access to all of the functionality required by the profiles and options that it supports when appropriately requested.

4.4 Certificate management

Certificates may be revoked prior to their expiration time, e.g. if the broadcaster’s private key is assumed to be compromised, or the broadcaster is no longer to be certified by the CA. Each CA publishes a list of revoked certificates, called a Certificate Revocation List

(CRL) [1]. Distribution of CRLs can via the return channel or the broadcast MPEG stream. The CRLs are retained in persistent storage by MHP terminal.

Receivers inspect the set of CRL files periodically and cache the revocation information for future use. During the validation process of a certificate chain, the CRL of each certificate authority on the certification path is checked .

Root certificate management is another important issue in MHP security framework. Every compliant MHP terminal will have to maintain a set of X.509 root certificates in persistent storage. When the root certificates are updated, a standard mechanism using messages called Root Certificate Management Messages (RCMM) [1] is used to finish this task.

RCMM is authenticated by multiple signatures. An RCMM message will be accepted by an MHP terminal if and only if it has at least N signatures. The N is 2-12 currently, and the initial value is expected to be 2.

The use of multiple signatures guarantees that the set of root certificates can be updated securely even if one of the root certificates has been compromised.

4.5 Security on the return channel

General purpose security for the return channel is provided by the Transport Layer Security (TLS) protocol as described in RFC 2246 [10]. The MHP shall implement the cipher suites RSA, MD5, SHA-1 and DES. The MHP needs not to implement the whole TLS. The server part, the compliance with SSL 3.0 and TLS client authentication is not required in MHP implementation.

Before the TLS connection can be established, the MHP has to ensure that the certificate list sent by a server contains at least one trusted certificate. In a MHP environment, a downloadable application can establish a TLS session. This can be used for sensitive transactions. In such a scenario, the application knows which server to connect to, and also knows one certificate against which it can check that a given certificate chain contains the expected certificate that it knows and trusts.

One or several TLS root certificates can be optionally broadcast along with the application. The certificate files shall be authenticated members of the same authenticated sub-tree as the application.

When there are no TLS certificates sent with the application, then the implementation will allow connection to be established to any server. The application can then use the JSSE API to retrieve the certificate chain and check that it contains what the application requires [1]. In such a case both name and public keys need to be checked by the application if the application wants to be sure of the remote server.

An unsigned application may not use the return channel. By default, a signed application may not access the return channel, unless otherwise specified by the permission request file. The syntax of the return channel permission is so that it describes the phone numbers that the application may try to dial .

4.6 Application Information Table

The Application Information Table (AIT) plays also an important role in MHP security mechanism. The AIT provides full information on the data broadcast, the required state of the application carried by it.

Data in the AIT allows the broadcaster to request that the receiver change the activation state of an application. If errors found in AITs, they will be processed accordingly. Processing of the application or the AIT will continue. Applications shall not launch broadcast applications that are not signaled in the AIT of the same service. [1]

5 Analysis

This chapter first briefly introduce the security criteria: confidentiality, integrity, availability, non-reputability and privacy. Next the MHP security mechanism is analyzed based on these criteria.

Confidentiality: The protection of information so that someone not authorised to access the information cannot read the information even though the unauthorized person might see the information's container. [7]

Integrity: No user of the system, even if authorized, may be permitted to modify data items in such a way that assets or accounting records of the company are lost or corrupted. [8]

Availability: The property that a product's services are accessible when needed and without undue delay [8]

Non-reputability: To create evidence that data has been sent or received, so that the sender (or receiver) cannot later falsely deny this fact. [8]

Privacy: The protection of personal data so that unauthorized person could not access them.

The authentication tree in MHP gives strong protection of the consumer and service provider. The MHP security model divides applications to signed application and unsigned application. Unsigned application has restricted access rights to resources and services. The hash codes in MHP ensure the data integrity and confidentiality, because hash codes are computed with the content and attributes of the objects. And a hash file indicating objects to be authenticated will be put in each directory containing such objects. This mechanism protects that only authenticated application can modify related objects. Moreover, an authenticated application could not modify the objects that not listed in the hash file it used to authenticate itself. Under strict authentication, the MHP resources could be accessed only by the authorized users.

The non-reputability is mostly ensured through the signatures. Digital signature in MHP is stored in a signature file located in the root directory of the sub tree that it signs. The signature value is computed upon the ASN.1 DER encoded tbsCertificate. By generating this signature, a certification authority certifies the validity of the information, especially

the binding between the public key material and the subject of the certificate. Since applications have to sign a digital signature, and this signature is stored in a file including the public key, the hash algorithm and the computed signature values. Any user that has signed for an application could not deny that he has done such operations. This protects against the non-repudiation. From other point of view, non-reputability exists also in the opposite direction. The service provider and broadcaster could not deny any kind of operations they have done to the consumer, especially when such operations may cause consumer's STBs damaged.

The availability should be guaranteed by all the participants: consumers, service providers and broadcasters. The strict authentication rules can promise that unauthorized person will not misuse a user's private information in the normal way. But the privacy could not be promised by the person who can access the information. For example, the network administrator in the service providers' company can access many types of consumers' private information like their PIN code, their credit card number. If such person misused these information, it is difficult to detect and prevent by the MHP security mechanism. The AIT table in some points provides the availability protection. The applications could not be launched without an AIT definition. This ensures that only signed application can access the MHP resources.

From another point, since Secure Socket Layer (SSL) is used in return channel, the detection of sensitive information on the transferring becomes difficult. The privacy is protected very well without considering personnel factor.

The availability needs co-operation of the service provider and broadcaster. The broadcaster must keep the channel working appropriate at any situation. The transmission rate should be kept stable and the quality should be promised. When consider return channel, this issue becomes more complicated because the user can access resources via return channel.

The certificate file contains all of the certificates in the certificate chain up to, and including the root certificate. A certificate chain is a hierarchy of certificates that enable the implementation to verify the validity of the key used to check a signature. In the MHP environment, the root certificate is embedded in the MHP. So the file structure shall carry all of the certificate chain apart from the root certificate.

In the root directory of an authenticated sub tree there shall be one certificate file for each signature file. This certificate file ensures that the signature is the right one who signed it.

Since Java is used as the development platform both in MHP 1.01 and MHP 1.1, the security feature like sandbox, which can limit access to system resource can also be used in MHP applications. Actually, Java plays an important role in enforcing strong typing and preventing application from executing common attacks such as stack overflows [3].

Finally, the security requirements for the three profiles are certainly not identical. The more powerful service needs more security guards. The enhanced broadcast profile focuses more on broadcaster's security issue. While keep at least the same level of enhanced broadcast on broadcaster, the Interactive broadcast must keep an eye on the return channel. The Internet Access should give more power on the return channel security issues than the other two profiles. At the same time, it should keep the same power on security issue of broadcaster and service provider as the two other profiles.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

6 Conclusion

Under present situation, the broadcaster is the gatekeeper of the MHP platform. Because all applications are launched via broadcast stream even if the return channel exists. In the future, the return channel can be used to download the content, but it is not allowed to use the broadcast stream simultaneously with the return channel in interactive applications. If all the users are considered, the broadcaster has the high priority security requirements among them.

From analysis, we can get some ideas about current security mechanism in MHP. It could authenticate incoming applications that are from valid sources, verify that the user is appropriately authorised to use the application. The application integrity can be verified. An application's access to private data can be controlled. When one task is finished, the application can terminate and resources are correctly released.

In summary, the security model in MHP gives an efficient protection of the users' data from technical point. The broadcasting program is protected well by the MHP security model. From the ETSI standard, the security mechanism is one of the essential parts in the MHP, especially for the broadcaster. The privacy should be the main point of the consumer. The data integrity and confidentiality are concerned by the service provider. The non-reputability should be cared by all the users in MHP. The availability is related to capacity of the broadcast channel and IP network routes. This paper has not discussed it in detail.

References

[1] ETSI TS 102 812 V1.1.1, Digital Video Broadcasting (DVB);Multimedia Home Platform (MHP) Specification 1.1 November 2001

[2] http://www.mhp.org/html_index.html

[3] Jon Piesing *The DVB multimedia home platform - "MHP"* The institution of Electrical Enginerres, 1999.

[4] J.P.evain, The Multimedia Home Platform, http://www.dvb.org/resources/pdf/evain.pdf

[5] http://www.mhp.org/technical_essen/pdf_and_other_files/a062.pdf

[6] http://www.mhp.org/technical_essen/tech_essentials.html

[7] N. Haller, R. Atkinson, On Internet Authentication, RFC 1704, IETF Network Working Group, October 1994.

[8] D. Gollmann *Computer Security*, John Wiley and Sons. Inc., 1999

[9] Th. Dorsch, Multiradio Multimedia Communications Workshop MMC , 2001,22-23. November 2001, Berlin, http://www.ist-drive.org/MMC2001/

[10] T. Dierks, C. Allen The TLS protocol, RFC 2246, IETF Network Working Group, January 1999.

HUT TML Course T-110.551 ISBN 951-22-5959-1 ISSN 1455-9749
http://www.tml.hut.fi/Studies/T-110.551/2002/papers/May/index.html

[11] J.C.Newell, I.Childs Strategies for supporting the DVB in an MHEG-5 environment, BBC Research & Development Department.

[12] Norsk Regnesentral Digital TV, Seminar: Multimedia coding and transmission, Hostsemester 2001.

[13] ETSI TR 101 200 v1.1.1 Digital Video Broadcasting(DVB); A guideline for the use of DVB specification and standards September 1997.