Right Management Infrastructure for Home Content

György Kálmán, Josef Noll
UniK, University Graduate Center, Kjeller, Norway
{gyorgy, josef}@unik.no

***Abstract*— Users are creating and sharing their own content. Based on various properties, user groups are created, which may need to share content only between members. This induces the need for a rights management solution, which keeps the user and his content in focus. Such a solution will enable fine grained rights control over distributed material in an easy and secure way. In order to make the life of the user easier, devices in the home network and in personal area networks may form a device domain, which can be managed as one entity. To manage such a device domain and to have it tamper resistant, an always online device would be the best focal point. An entity called Digital Rights Management (DRM) broker is introduced to serve as a home agent, cache for user right definitions and to act as a gateway for external access of home content. This node provides connection interface between the various DRM standards used by external content provider companies. The possiblity of user-centric content sharing with the help of a home DRM architecture is shown. In this paper, a solution is shown for efficient device domain management, a tamper resistant central unit is recommended and a service example is shown.**

***Index Terms*— seamless, authentication, rights management, SIM, home networks, PAN, content management, device domain, smartcard, cryptography, DRM**

I. Introduction

With the spread of always-online Internet connections, user behaviour started to change. Traditional user and provider roles are not separated any more. The end user is creating his content and sharing it over the network.

Social life over the net is becoming more important, enforcing the need to share information with different user groups. A user may want to share pictures with his friends and family, with a society or just with one person. Currently, lots of web services are available to make content sharing possible, but until now, no fine grained right management solution is designed with user needs in mind, and with support of home content.

II. Motivation

A pleasant user authentication solution is required to ensure good user experience. For some purposes, it would be beneficial to use seamless authentication, like it is implemented for certain Wireless Application Protocol (WAP) services in the mobile networks. Because no user interaction is needed it is recommended to use it in personalisation and content adaptation services [1].

Content adaptation has a growing importance in pervasive computing, since terminals with very different capabilities are used to access the same information sources. Beside the technical problems associated with conversion, the commercial content protection solutions usually do not provide a method to make transformations.

To provide good user experience, these incompatibilities may be hidden with deploying a DRM broker into the home network, which can cooperate with user devices and is able to distribute licenses in a secure and easy way. A central device for controlling a home network was introduced in the IST ePerSpace [2] project, which provides service discovery and content adaptation services for compatible devices. However, the ePerSpace solution lacks support for content management.

There are numerous solutions for key distribution and management, but most of them are not optimized for the special circumstances in a home environment. These are in particular, the mobility of devices, energy constraints, computational power and trustworthiness.

Mobility can be addressed with secured transport protocols to provide secure and easy access to home content from the Internet side.

Entertainment devices usually have limited computing capability, thus they might be supported through a specific network device which is able to carry out complex cryptographic operations and exchange the generated information with other parties using a secure and easy method. A solution to computational problems and trusted devices could be to deploy smartcard based authentication in the home environment [3].

Most users are not aware of the possible threats and problems associated with their wireless home network. A secure authentication system would help reducing some of the risks. Wireless access points are often not secured, or use the easy to crack Wired Equivalent Privacy (WEP) protocol. Industrial grade solutions address security for wireless networks through the IEEE 802.11X standard for authentication or IEEE 802.11i as a complete solution.

In this paper we show a solution which can bridge the gap between the DRM solution shown in [4] and the smartcard based authentication architecture in [3] in order to enable cheap, easy and secure user authentication and personalisation services.

First, an overview is given about typical devices and their capabilities in a home network, then an overview about smartcards, their possible area of use and possible candidates for widespread use. A possible secure and widely available device, which can help to overcome the problematic deployment of a smartcard infrastructure, the mobile phone and its

Subscriber Identity Module (SIM) capabilities are shown. An example architecture is given for managing a home network and creating device domains for content sharing. An example service for key distribution and delivery is shown. At last, an evaluation of the proposed architecture is given and areas of further investigation described.

III. Devices in the home network

A home network can be composed of PCs, media players, mobile phones, storage units, STBs or other devices. Most of these devices are mobile and move between different networks. Wireless networks also made it easier to welcome guests on the home network, like a friend of the user can come to his house and access the local network.

The problems begin with securing access to a home network. Mostly there is no or just weak security applied on those, so they are wide open for malicious intruders. For example, lots of WLANs use no encryption at all or employ the compromised WEP standard. These mean, that the users are broadcasting their data for everyone in a considerably large area.

Setting up a secure network may be problematic, since keys have to be transmitted and devices have to authenticate themselves. This may be done by using out of band key delivery methods (like using an USB stick or in an SMS via the mobile network). Even if the user is able to do this process, convenience considerations might cause him to neglect security. Also, currently, the user may decide to grant access or not, but inside the network it is extremely rare to use some kind of additional access restriction. This means, that either no access is given or the guest can access practically all network resources.

While keeping secure access, content adaptation is becoming more important. In order to ensure good representation of content, profile management methods, such as UAprof [5] were introduced. These technologies free content creators from the problems associated with content adaptation.

Content stored in a home network may be also adapted to the different devices, to ensure good results. Content adaptation can be problematic, because current DRM solutions usually do not allow changes in the content. If a device could provide connection between the content providers rules and user needs, the adapted and legal content would improve the user experience. Such a device could act as an end entity for the content provider and hide the inner network of user devices.

IV. Rights management

Since users are starting to create and share content with others, the home infrastructure has to support some kind of rights management. This not only includes storage of acquired licences from content provider companies, but taking care of own content. Home networks store a great deal of personal information which should be secured.

Based on their various roles, a need to share with a specified group of users arise. This can be done by introducing community content access, based on group authentication.

A design with the end user in the focus is needed to enable secure and easy sharing of content over the internet. This means, that while preserving ease of use, the system has to use strong encryption, group authentication and efficient key management.

A DRM solution for home networks is proposed in [4], where creating device domains in the home environment is shown. This paper points out, that problems associated with the mobile environment (battery powered consumer devices in particular), and the possibility of reducing the number of expensive calculations.

Group authentication is essential to enable sharing between different user groups based on various properties, like friends, school classes or other interests.

The basic problem of home DRM is, that these systems usually rely on *compliant devices*. A device needs to meet certain requirements in order to get accepted by the system. Compliance raises a problem with the restricted and optimised nature of home devices. If individual authentication is used, public key operations need to be carried out, because mutual authentication is required between the DRM system and the terminal. This could be problematic for simple devices, like an MP3 player and resource consuming for a device like a PDA.

Content adaptation has a growing importance in pervasive computing, since terminals with very different capabilities are used to access the same information sources. Beside the technical problems associated with conversion, the commercial content protection solutions usually does not provide a method to make transformations.

The use of group authentication can help to overcome the problems associated with content adaptation and personal content sharing. This solution fits much better to the general use of home devices, because in this scenario, a device has only to prove, that it is part of a group, which can be done by simple hash calculations for example.

After authenticating the devices, also securing of the transmission environment is advised. This could be done by negotiating symmetric session keys or calculating hash values for example.

It can not be assumed, that all devices have cryptographic hardware and tamper resistant hardware. This can be solved by adding a smartcard into the system.

V. Authentication and Encryption

Most devices does not have extensive encryption capabilities and to use secure infrastructure, they may rely on external units, like a smartcard. This is a tamper resistant device, which may support complex encryption functions and provide them to compatible devices.

In [3] a smartcard is shown, which implements the Extensible Authentication Protocol (EAP) stack in hardware thus providing high security on a widespread protocol family for WLAN authentication.

While these hardware elements provide good security capabilities, it can be problematic to add those to all the devices in the home network. Besides the costs to equip every single node

with a smartcard reader, compatibility issues and additional battery powered devices for certain hardware will make the smartcard solution difficult. Compatibility is the main reason why the Norwegian BankID consortium drop the use of smartcards.

To keep the advantage of a tamper resistant cryptography device and keep costs low, we propose to use the mobile phone's SIM to calculate and the phone hardware to distribute keys for devices.

The phone is becoming a permanent part of the user's personal area. In many cases the handset is already part of the user's identity, because of it's services, look and important role in social connections. Users are taking care of it, since a phone holds a great deal of social and personal information.

According to [6] it could be possible to use the SIM as a fully featured smartcard as the SIM is capable of storing keys and providing cryptographic functions for third party services, not only for mobile providers.

While the phone is capable of generating a key, the problem of key delivery still remains. If the user has to connect the phone via USB or Bluetooth, it can be problematic, since Bluetooth needs pairing and USB is not supported by a considerable amount of devices.

To solve this problem, we propose to use NFC technology to transmit encryption keys between devices. NFC is a short range communication technology based on RFID, but with more limited range and the possibility of using active devices on both sides. An NFC reader adds only a small cost overhead to devices, does not need to be powered continuously and provides contactless transfers for very limited ranges.

Through the mobile phone, the user has full control over the identification process either based on the location e.g. putting the phone close to the reader or on knowledge e.g. typing in a PIN when requested by the remote service.

A key problem is the correct selection of the identifier to be used in a transaction. This can be done either by profiles or by asking the user to allow access to the data, requested by the service.

The public key of the phone represents the root trust in the system. The key pair can be placed to the SIM either by the mobile provider or other, verifiable source, to ensure correct user identity association.

If the private key of the SIM gets compromised, the identifier can be revoked by the identity provider and the user can get a new key without losing access to the services. The remote revocation and user control makes the SIM an ideal device for making payments and gaining access to services.

VI. Service Architecture

We propose to incorporate the device domain management capabilities and the EAP capable smartcard functions. The EAP family is used for easier cooperation with current network authentication technologies.

With using the SIM's cryptographic functions [6], we build a device domain, and distribute these keys through the NFC interface.

The constraints, the system has to face are

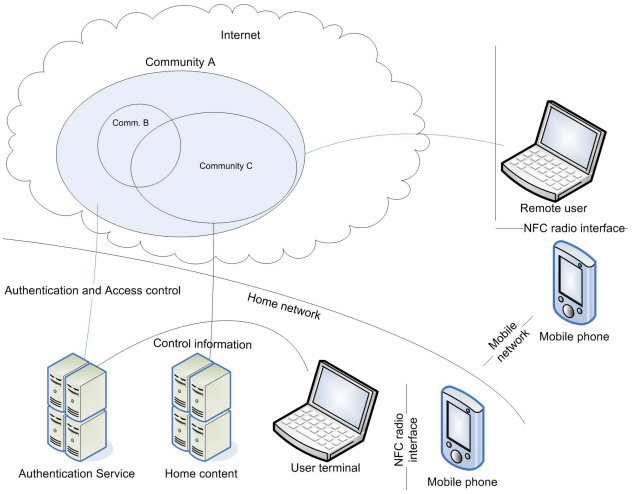

Fig. 1. Home network with Access Control and out of band key distribution

- continuous network connectivity cannot be assumed between the members of the domain,
- there are no secure clocks in the system,
- no cryptographic hardware is available in the devices,
- key management must be efficient even for large number of devices.

The CPU power of current smartphones makes possible the use of public key operations and so act as a proxy between the provider and the user devices. The provider can be either the DRM broker on the home network or external content providers.

The DRM broker handles rights associated to local and user created content outside the home network. This entity certifies approved devices and revokes expired or compromised ones. No global device identification key is proposed because the phone can deal with the domain's internal right management issues.

This lowers the resource needs at commercial right management providers and also keeps user privacy on a higher level, because he does not have to disclose, what kind of devices he is using. With a DRM broker and an always online phone in the system, we can also extend the proposed systems functionality to physical media, like DVD-s since the networked media played is connected to the broker, which is accessible for example through any mobile IP service.

If a new device is added to the domain, a request is shown on the display of the phone and requires response from the user. This ensures, that access is only granted, if the remote party gets a correct key and in addition, the user confirms his will to permit access. This can be requested once or any other period, based on user preferences.

We recommend the use of NFC interface for distributing keys out of band. With this short range transfer method it is possible to allow the phone to negotiate or generate an authentication and encryption key for the user device, and send it to the mobile device, where no expensive cryptographic methods are needed.

The loss of the mobile phone does not compromise the system's security, since the SIM can be disabled remotely (if

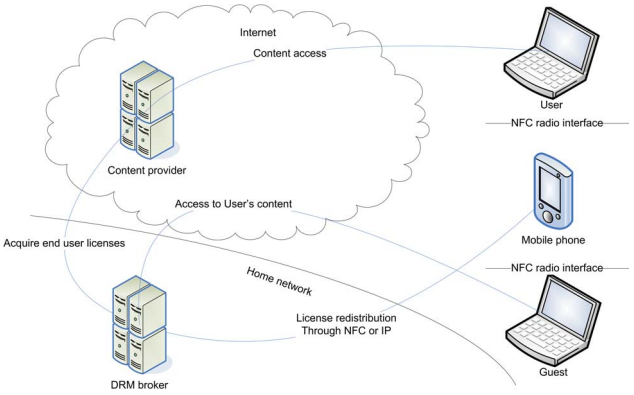

Fig. 2. License redistribution with NFC enabled phone

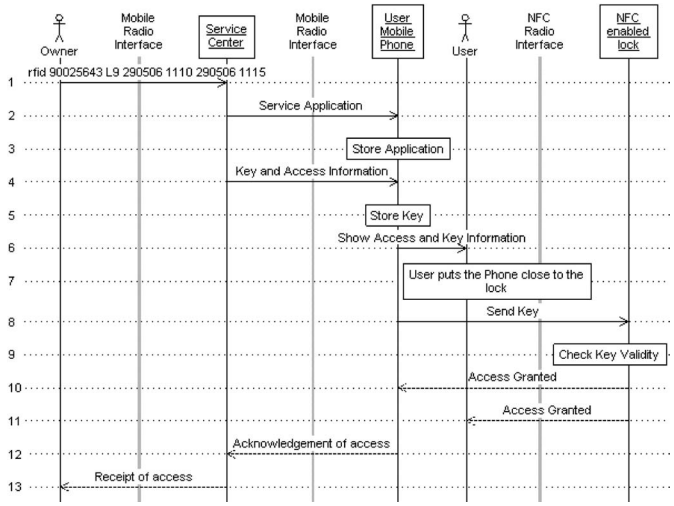

Fig. 3. Admittance Service with NFC

the intruder wants to generate a new key, they have to connect to the network). After getting a replacement, the existing keys of the domain will be revoked and the user has to distribute them again.

Usability of the proposed system depends mainly on the easiness and security of key distribution. In the demo system we use either NFC technology to deliver keys to local devices or the mobile network for remote users.

Local key delivery can be accomplished with NFC, because it has very limited range and is convenient for the users, just to put the phone close to the device they want to exchange a key with.

To enable remote access to home content, it is possible to send the access key out of band, via the mobile network to the remote user's phone, where he can use the NFC interface to download the key to the terminal, he wants to use for content access.

VII. Prototyping key exchange

Realisation of our suggested rights management solution depends mainly on the capability of distributing keys. The architecture suggested in this paper consists of a home server, a mobile device and various media players. The home server is responsible for content adaptation and encryption, based on keys generated from the master key of the mobile phone's SIM card. Thus we address two ways of distributing keys, through *(i)* the mobile network or *(ii)* the NFC interface.

A generic solution demonstrating the key exchange in NFC and mobile networks was provided by the authors [7]. The service is an SMS initiated admittance, and generates access keys distributed through binary short messages (SMS) and NFC. The provider of access (user) initiates an SMS to the service centre, which generates a binary SMS providing the access key to the mobile phone of the person requesting access (guest). The guest's mobile phone can then use NFC to achieve access to a property.

The functional diagram is presented in fig. 3, and is realized as follows: The user is authenticated through the mobile network and a key sent to the guest is stored in the SmartMX card of the phones used for this prototype. The key is transmitted from the card over NFC to the door-lock, when it is put close to the reader.

This prototype shows the basic mechanisms needed for rights management of the home content. The device domain manager takes the task of service initiation, requesting a key for decryption of home content. The mobile phone will generate the key, and send it back to the device domain manager or alternatively leave it on the mobile phone, from where it is transmitted through NFC to decrypt home content. To ensure safety, secure key negotiation procedures shall be implemented.

VIII. Evaluation

The current prototype is using the SmartMX chip instead of the SIM for key storage, which limits the possible range of devices. This is a technological limit, which is in the process of being resolved. Nodes need to be equipped with NFC readers to enable key transfer with this technology. NFC readers are not usual in the home environment. The security of the system depends on the tamper resistance of cryptographic functions on user devices.

Our proposal shows an improvement over the original idea of [4] by using the possibilities of the mobile phone and the inclusion of a DRM broker, which act as a gateway between different DRM solutions and acts like a home agent for the user's right entities. A possible drawback of using the SIM is that the mobile providers usually do not allow access to the SIM in order to ensure correct functionality of the network.

The authors want to point out, that by using the SIM as secure storage and executing signature and session key generation routines over the SIM (which would be included by the operator on the EAP capable SIM) does not interfere with any networking function of the phone while keeping the advantage of being a widespread device which lowers the introduction costs.

Storage may be also limited, but since an encryption key (for example the master key for adding domain members) can be quite short, well under one kilobyte, even current SIM capacities seem to be enough, but also, high capacity SIMs are already on the horizon [8].

NFC technology is just entering the contactless market, so additional tests are required to test its security against various attacks.

IX. Conclusion

This paper provides an architecture of rights management for home content. While current solutions are device centric, our solution supports both an I-centric and a community centric approach. The architecture consists of a home server, a mobile device and various media players. The home server is responsible for content adaptation and encryption, and the mobile phone creates rights management keys, which are distributed through the mobile network or NFC.

We have shown that the mobile phone with the SIM card has the potential to provide strong encryption services, being applicable for securing home content. Key generation and distribution are the main functions of the phone, supported by the capability to interconnect devices in the home network. It may also be used to enable access to guests and store device profiles for content adaptation. Because the phone is practically always online, update and revocation of profiles or keys can be done remotely and nearly instantly. The SIM is trusted by mobile providers and can be the tamper resistant device, which the user needs for building an I-centric rights management infrastructure.

References

[1] C. M. M. Rahman and J. Noll, "Service interaction through role based identity," in *Proceedings of WWRF 17*, 2006.

[2] IST ePerSpace, "Towards the era of personal services at home and everywhere." [Online]. Available: http://www.ist-eperspace.org/

[3] G. Pujolle, P. Urien, and M. Loutrel, "A smartcard for authentication in wlans," in *Proceedings of the 2003 IFIP/ACM Latin America conference on Towards a Latin American agenda for network research*, 2003.

[4] B. C. Popescu, B. Crispo, A. S. Tanenbaum, and F. L. Kamperman, "A drm security architecture for home networks," in *Proceedings of the 4th ACM workshop on Digital rights management*, 2006.

[5] WAP Forum, "UAProf specification." [Online]. Available: http://www.openmobilealliance.org/tech/affiliates/wap/wap-248-uaprof-20011020-a.pdf

[6] ETSI, "TS 102 350 V7.0.0 smart cards, identity files and procedures on a uicc," in *ETSI Technical Specification*, 2005.

[7] J. Noll, J. L. Calvet, and K. Myksvoll, "Admittance service through mobile phone short messages," in *Proceedings of the ICWMC 2006, Bucharest*, 2006.

[8] M-Systems, "M-systems and microelectronica announce plan for 1 gigabyte sim cards by end of 2006," in *Press Release, 3GSM World Congress, Barcelona, Feb. 15*, 2006.