INTEGRATED RIGHT MANAGEMENT FOR HOME CONTENT
A SIM based Right Management Solution for Home Networks

György Kálmán and Josef Noll
UniK, University Graduate Center, Kjeller, Norway

Keywords: Seamless, authentication, smartcard, cryptography, rights management, SIM, home networks, content management.

Abstract: With continous internet access, the user behavior is changing. Now, users are creating and sharing their content over the network. With content sharing, the need for protection arises. Currently, no fine grained security solution exists, which provides such functionality for users.
Easy and transparent user authentication and access control is of key importance. In this paper, we suggest a solution, where devices on the home network and in PANs may use a common right management infrastructure. Key of our recommendation is the mobile phone, which can act as a trusted key management and distribution unit for the user.
In this paper, a solution is shown for easy access right management, a tamper resistant central unit is recommended and a service example is shown.

1 INTRODUCTION

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 society or just with one person(Rahman and Noll, 2006).

Currently, no easy to use right management solution exist, which was designed for the end user market. To use the new services offered by Web 2.0 sites, the users need a solution, which enables easy and secure content sharing, possibly without third parties.

The extensive use of web services is narrowing the border between the traditional home network area and the external services. User content was traditionally stored in the home network, but now, with the help of various media sharing solutions, it is moving towards external servers. Also the home network infrastructure is getting more complex, which raises the basic concern of access security. Lack of technical knowledge leads to vulnerable home networks, where the security of the content solely relies on the sharing method used, hence the home environment is becoming a more hostile, like the external network outside the local router.

Because of the complexity and the lack of security measures, the home network is more vulnerable, then it was before. The fundamental problem is, that usually a security system is either secure or easy to use and manage. 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(Noll et al., 2006a). 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(Potlapally et al., 2006), computational power and trustworthiness(TCG Mobile Phone Working Group, 2005).

A solution could be to have a simple control device, with good cryptographic functions and key management capabilities. Because of the special requirements of the home network, a smartcard based authentication method is recommended. The smartcard is able to provide cryptographic functions with tamper resistant hardware, and provides also a certain level of protection against trojans. The smartcard is able to generate encryption keys, checking signatures and also provides secure key storage.

In this paper, the concept of a home right management system is shown, the use of the mobile phone as an authenticator is shown and as a key distribution example, an out-of-band Near Field Communication (NFC) admittance system is shown.

Kálmán G. and Noll J. (2007).
INTEGRATED RIGHT MANAGEMENT FOR HOME CONTENT - A SIM based Right Management Solution for Home Networks.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 107-111
DOI: 10.5220/0002127801070111

2 OPERATION OF HOME NETWORKS

The use of wireless technologies in home networks is dominant. But, 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 compromised Wired Equivalent Privacy (WEP) protocol(Borisov et al.,). Industrial grade solutions address security for wireless networks through the IEEE 802.11x standard for authentication or IEEE 802.11i. The use and management of these technologies requires high competence, which is not usual in the home area.

Because of the security problems associated with medium access in home networks, it has a big probability, that an intruder will get access to the network. In addition of the access control, current operating systems provide the possibility of using some kind of access restriction, for example either based on file or share basis. This can provide an additional line of defence.

On the Local Area Network (LAN), most of the content is accessible without additional authentication. If a guest arrives, the user grants access to his home network to show some content over the terminal of the guest. While access to the network for internet access might be acceptable, granting access also opens possibilities for content access. Getting an external user into the home network means to loose control over which content the guest can access, and be vulnerable to malicious attacks from the visitors devices. This can be also done by trojans, which are malicious even if the guest is unaware of its presence.

This paper proposes a solution in the form of a right management infrastructure for home networks. This service enables access right definition on user content. With rights associated, content access is not defined by the current place or network of the user, but on the credentials, which are owned by him.

With such an infrastructure, the user can grant network access to a guest without compromising his own content stored on the network. Also, if the medium access protection fails, this solution operates as a second line of defence. The problem is, that with such a system, all devices have to support this service. With more and more entertainment devices connected, this is a hard problem.

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(Pujolle et al., 2003).

In (Popescu et al., 2006) a rights management solution is proposed, which is based on device domains. These domains can be formed from the devices in the LAN, and also can have members from external networks. Mobility can be addressed with secured transport protocols to provide secure and easy access to home content from the Internet side. This proposal lacks a device, which can be used for easy and secure key generation. In (Pujolle et al., 2003) a smartcard based solution is shown for WLAN authentication.

Because of the expenses associated with deploying a smartcard infrastructure, we propose to have only one smartcard in the system, which can exchange the corresponding keys with the other terminals via a contactless interface.

3 AUTHENTICATION AND KEY MANAGEMENT

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

Currently, vast majority of the potential users already have SIM cards in their pockets. 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. Because of it's importance, they are taking care of it, since it holds a great deal of social and personal information.

According to (ETSI, 2005) 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.

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.

To solve the problem of convenient key distribution, we propose to use NFC technology to transmit encryption keys between devices. A 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.

The master key pair of the phone represents the root of trust in the proposed system. The keys can be placed to the SIM either by the mobile provider or other, verifiable source, to ensure correct user identity association if authenticity verification is required. Commercial uses will require a trusted third party in the system, but for private use, a shared, web of trust solution is more feasible. With such a service, the users could prove each others identity without the use of an expensive external service.

Alternatively, the user could also distribute keys for his friends off line, for example via the NFC interface during visits.

4 A SERVICE SCENARIO

Adam is at home, and Balazs is visiting him. He is a friend of Adam. He is at Adam, last weekend they had a hiking trip together. Both of them made several pictures, Balazs recorded short videos and Adam made a short text attached to the GPS tracklog. They want to make a webpage, which contains all the content and make it available for their friends.

The first step is allowing access for Balazs to the home network of Adam. Adam gives him the WPA key of the network and also enables his MAC in the router. The required information is sent via the NFC interface between his mobile phone and Balazs's laptop, so Adam has only to touch Balazs's laptop with his phone.

After, Adam creates a webpage on his home server. In the background, the system allocates space and grants the appropriate rights to Balazs. Both are uploading the content. When they finish with the page generation, they want to allow access for their friends. Of course, just read-only except for the forum, where verified users can leave messages.

They use a common group key, which is known to their friends. Using this key, a remote user can identify himself as a friend of Adam or Balazs and then access the content.

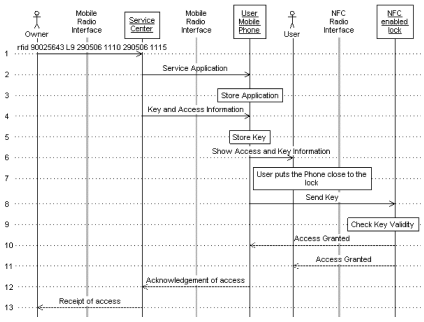

Figure 1: Admittance Service with NFC.

5 KEY EXCHANGE WITH AN NFC PHONE

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 (Noll et al., 2006b). 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. 1, 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 provides 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 used through NFC to decrypt home content.

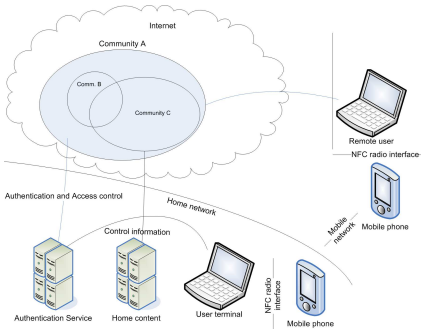

Figure 2: Home network with Access Control and out-of-band key distribution.

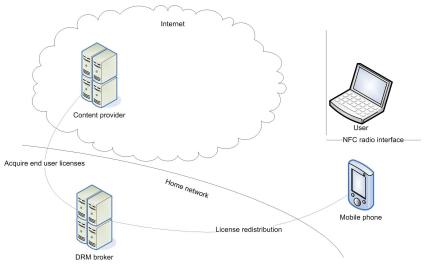

Figure 3: Right object distribution with NFC enabled phone.

6 SERVICE ARCHITECTURE

To enable safe remote access, interaction is needed between the nodes in the network. The phone needs to generate the appropriate keys and deliver it to the other units, local servers needs to provide authentication and the required cryptographic functions to ensure the operation of the network.

With the SIM's cryptographic functions, it can act as the central trusted cryptographic unit.

The constraints, the system has to face 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 content items and users.

If the user wants to add a new device to the domain, he can generate the access key for the user on the mobile phone and give it to the guest. After, the guest can use this key to identify himself to the network and access content. The user can easily compose the appropriate access rights to every piece of content stored in the network and use the identity represented by the key.

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 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.

The local services can use their old access methods, with the help of an abstraction layer, the system can look up the appropriate rights to the content.

7 EVALUATION

With the mobile phone, the users already have a device, which is capable of providing strong encryption services. With the help of the SIM, the user would be able to generate own right objects, which could be distributet either out-of-band, with NFC or through the mobile network. This enables easy content sharing with other users and groups.

8 CONCLUSION

Currently security in the home network is becoming a key problem. To ensure safe and convenient content management and sharing, new solutions have to emerge. One of this could be a system proposed by this paper, where the user can use contactless technology to deliver authentication keys to friends and securely share content over the internet.

With the SIM, the user already has a tamper resistant device, which, at one time, can even protect himself from trojans and malicious users. By extending the functionalities of the SIM, it could be easily the key device for the future home cryptographic infrastructure.

REFERENCES

Borisov, N., Goldberg, I., and Wagner, D. Intercepting mobile communications: The insecurity of 802.11.

ETSI (2005). TS 102 350 V7.0.0 smart cards, identity files and procedures on a uicc. In *ETSI Technical Specification*.

TCG Mobile Phone Working Group (2005). Use case scenarios v2.7.

Noll, J., Calvet, J. L., and Kálmán, G. (2006a). License transfer mechanisms through seamless sim authentication. In *Proceedings of Winsys 2006, Lisbon*.

Noll, J., Calvet, J. L., and Myksvoll, K. (2006b). Admittance service through mobile phone short messages. In *Proceedings of ICWMC 2006, Bucharest*.

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

Potlapally, N., Ravi, S., Raghunathan, A., and Jha, N. (2006). A study of the energy consumption characteristics of cryptographic algorithms and security protocols. In *Mobile Computing, IEEE Transactions on*.

Pujolle, G., Urien, P., and Loutrel, M. (2003). 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*.

Rahman, C. M. M. and Noll, J. (2006). Service interaction through role based identity. In *Proceedings of WWRF 17*.