User Controlled Content Access

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

***Abstract*—In this paper we investigate the problem of the growing amount of personal content available online and the privacy problems associated with this area. Different levels of security requirements and possible solutions are shown. Finally, we propose a smartcard based right management solution, which is using the SIM of a mobile phone as trusted entity.**

***Index Terms*—rigths management, content sharing, secure access, pki, sim**

I. Introduction

While user base of online services is continuously growing, an unfortunate gap between security solutions is getting wider. The average user is slowly losing control over his own online life. The security of the user is attacked from several sides: the access medium has lost it's moderate security with the spread of wireless networks, where encryption is optional. The forums or mailing lists are not islands any more, as many of them are moving under social networking sites, which allows malicious users to monitor one's activity easier. This tendency is supported by the trend, that users are now using their real names and data instead of usernames or nicks, which was typical before.

The spread of internet connectivity also opened access to more vulnerable user groups, such as children and elderly people, who are much more defenseless against attacks. Users are willing to share their own content (pictures, videos etc.), but lack the capability and the knowledge to protect themselves against theft, delusion and exploitation. 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. Background

A pleasant user authentication solution is required to ensure good user experience. The usage area of a service defines it's security requirements. If just better-than-nothing security is required, the user could be authenticated seamlessly and could get personalised content easily [1]. Since no user interaction is needed, the security depends on the environment [2]. To share content, in this case, it would be enough, if the communicating parties will exchange an encryption key (based on Diffie-Hellman key exchange for example), which will ensure confidentiality, but will not protect against trojans nor will ensure the identity of the parties.

Solving these limitations lead to more secure communication approaches. Chowdhury [3] showed an approach for identity management, which will allow easier service access and identity representation based on semantics. The next step is to insert a trusted entity into the system. This would provide protection against trojans or other malicious entities, which may invisibly gather information about the user. In [4] the use of a smartcard is introduced. In our approach, we take this idea further, and show, that the Subscriber Identity Module of a phone could be used.

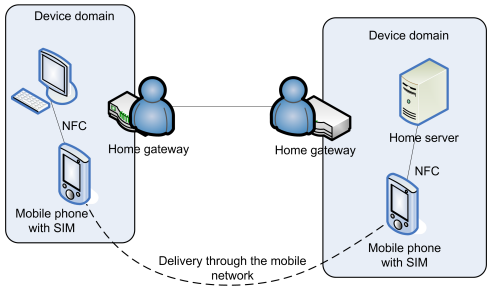

Fig. 1. Content sharing with identity management and trusted component

In this paper we propose an architecture which can bridge the gap between the DRM solution shown in [5] and the smartcard based authentication architecture in [4] in order to enable cheap, easy and secure user authentication and personalisation services.

III. Usage scenario

This paper concetrates on content sharing from the user perspective. As such, the concept is shown, where a user wants to share content with one of his friends.

In this scenario, the user shares a piece of content (e.g. picture) for an other user. The content is served by the home server and can be accessed through the local internet connection. The user selects the remote one with the help of a graphical user interface on a pc, then, when requested puts his mobile phone close to the pc and a request to the SIM (the trusted element) is transferred through the contact less interface (Near Field Communication, NFC).

The SIM generates the access key and sends the appropriate information back to the pc, which updates access tokens in the home network. The user is asked about how the key delivery should proceed, where he chooses out-of-band delivery, which means in this case, that the key is transmitted over the mobile network to the phone of the remote party. This solution works only, if the phone number of the remote party is known.

To offer such a service, the system needs to be secured in several areas, to lock out typical attack methods.

IV. Proposed architecture

Our system is composed from the mobile phone with the SIM inside, an optional Certificate Authority and user-run

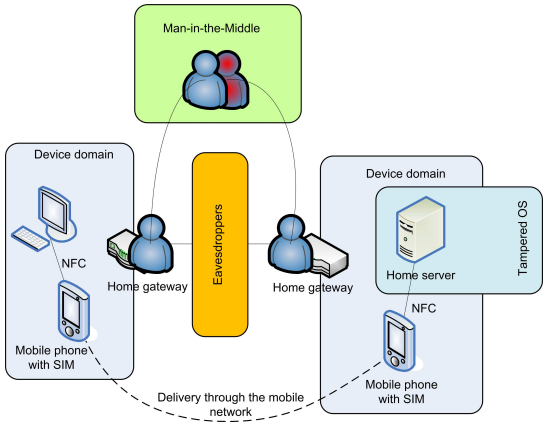

Fig. 2. Problem areas in the user content sharing scenario

services.

The SIM is the key element in our proposal. As a fully-featured smartcard, it provides storage and key management functions. By default, a certain level of idenity assurance is provided by the SIM itself, as it authenticates the user towards the mobile network and proves the subscriber's identity.

Identity management is the point, where this proposal leads behind [5] [4]. Without third party support, the receiver's identity can only be suspected, although, it would be a much stronger suspicion, than without. This alone leads to a system, where the sender user can be nearly sure, that the content is shared with the person it is meant to be, as mobile phones are considered as private property.

The phone provides the user interface for cryptographic functions and also the possibility to deliver the rights objects directly through the mobile network to the receiver's phone (if available). The actual piece of content can be accessible through a private or a public service.

In case of a private service, the application from the phone will also deliver the access information to the local server, we propose to use an NFC contactless interface, and update the access rights accordingly. A public service differs in updating the access rights, but this is not shown towards the user.

V. Threats

The system shown on figure 1 has several points, where weaknesses can lead to severe security problems.

Figure 2 highlights the problem areas. These include the communication channel, which can not be trusted. Eavesdroppers can easily monitor an insecure wireless LAN or, with more effort, attach to the wired uplink. In our system, the transmission medium is not trusted. As an additional security measure, the keys are delivered over the mobile network, if requested. Without identity management, a malicious user could start a Man-in-the-Middle attack, since the key exchange and the communication will mimic the normal behavior. A third point is to attack with a trojan or other internal monitoring application. This could be for example a rootkit, which runs on the local machine and diverts system calls addressed to the security subsystem towards a tampered one. Even if the security subsystems self-check routines could filter out such attempts, there are several ways to change the system behavior (e.g. multiplying the original data unit, before encryption).

A. Eavesdroppers

The transmission medium can not be trusted. The uplink of the user may be monitored and with the spread of Wireless LANs (WLAN), the local network may also pose a risk. Badly configured WLANs broadcast information in a considerable range. This allows passive eavesdropping or active intrusions if the access is not limited. This is especially problematic on home networks, where usually no additional authentication is needed to reach network resources. Confidentiality can reached by using fast, symmetric encryption with for example Diffie-Hellman key exchange.

B. Man in the Middle

Since users are sharing content between eachother, by default, no third party is involved in the exchange. In order to efficiently lock out a man in the middle attack, identity checks must be included into the system. There are several methods. For example, if no third party is involved, the users could meet and exchange a secret, which can be used in later communication sessions. While this can ensure mutual identification, it could be problematic and does not solve the problem, if the user's do not know eachother in forehand.

As an alternative, the identification process can involve third parties. Still staying in the non-commercial area, a web-of-trust [6] solution can be used, where the identity of the user can be represented as a Bayesian variable, which is more confident if more users trust, that the credential is connected to the specified user. A possible addition is the use of the mobile network for delivery, since the mobile phone is mostly a personal belonging and as such closely related to the user and it can be assumed with a certain plausibility, that if we send a message to a persons number, then that message will reach the one it is intended to.

The highest level of assurance may be reached with a trusted third party, for example a Certificate Authority (CA), which supplies the users with assured information. In our scenario this solution may be an over reaction in the sense, that the flexibility of generating own access tokens and the ease of user management would be sacrificed.

C. Tampered software

Modified software seems to be the hardest to fight against. In this case, attackers may change the original code, install a trojan or hide other malicious program with the help of a rootkit. Since in most cases the operating system may also be changed (or bypassed with a rootkit), a tamper resistant entity may be included into the system, which can be the first link in the trust chain. A possible solution is to use a SIM included in every mobile phone. This unit is a tamper resistant smart card and has wide cryptographic capabilities.

VI. Limitations of the environment

Most devices does not have extensive encryption capabilities and to use secure infrastructure, they may rely on external units, like a smartcard. In [4] 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. 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.

According to [7] 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.

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.

A master key on the phone represents the root trust in the system. Since this can be used for generating new access tokes, and mutual identification would be based on this, PKI may be used. 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 required. For a web of trust type requirement, a user generated key may be sufficient, where the identity assurance will rely on, that the system is contacting the user both via the internet (e.g. sending the link to the content) and via the mobile network (e.g. sending the access key), leaving only a small chance open, that some attacker got in control of both methods.

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.

We propose to incorporate the device domain management [5] 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 [7], we build a device domain, and distribute these keys through the NFC interface.

The constraints, the system has to face are

- 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. 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 deliver a new key, they have to connect to the mobile network). Usability of the proposed system depends mainly on the easiness and security of key distribution.

VII. Conclusion

Our proposal shows an improvement over the original idea of [5] by using the possibilities of the mobile phone 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.

We show a possible architecture of access control and rights management for home content. We have shown that the mobile phone with the SIM 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 flexible management infrastructure.

References

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

[2] L. a. S. R. a. T. B. Bertino, E. and Khan, "Secure knowledge management: confidentiality, trust, and privacy," in *Systems, Man and Cybernetics, Part A, IEEE Transactions on*, vol. 36, no. 3, 2006, pp. 429–438.

[3] M. M. R. Chowdhury, J. M. Gomez, J. Noll, and A. G. Crespo, "Semid:combining semantics with identity management," in *Proceedings of International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2007*, 2007, pp. 18–23.

[4] 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.

[5] 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.

[6] G. Caronni, "Walking the web of trust," in *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2000. (WET ICE 2000). Proeedings. IEEE 9th International Workshops on*, pp. 153–158.

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