# AN EFFICIENT PROXY SIGNATURE SCHEME IN HOME NETWORK DRM

Xiaoyun Wang[1,2], Kefei Chen[1,2]
[1.] Department of Computer Science and Engineering, Shanghai Jiaotong University
1954 Huashan Road, Shanghai, People's Republic of China
[2.] State Key Laboratory of Information Security, Institute of Software of
Chinese Academy of Sciences, Beijing, People's Republic of China

Keywords: Home network DRM, Authorized domain, Certificate Chain, Proxy signature.

Abstract: In this paper we overview the existing home network DRM schemes and especially Philips' invention. Then we propose to use the proxy signature to simplify the authentication of certificate chain in Philips' scheme. And we also give an efficient scheme of proxy signature based on the characters of certificate chain. We then give a detailed security analysis to show that our scheme meets the six properties of proxy signature. Finally the paper points that we should go ahead to improve the efficiency of home network DRM scheme and show a kinder interface to digital home consumers.

## 1 INTRODUCTION

Digital contents are the main application in digital home. Home network Digital Rights management (DRM) is required by content providers to protect high-value digital assets and control their distribution and usage. In digital home DRM, Authorized Domains (AD) are introduced by DVB (Digital Video Broadcasting) as a means to enable the consumer be free to access and distribute contents within the entire home network.

There are several AD based home network DRM schemes. Philips's invention is one of them and based on certificate chains. The main problem in it is low efficiency and long feedback delay because of complex protocols and weak computing capability of consuming devices. So we should try to reduce the amount of protocol steps, or computation to improve efficiency and reduce the delay.

In this paper we will propose an efficient proxy signature scheme to simplify the device authentication protocol on content demanding in Philips invention. This proxy signature scheme could also be used in proxy signature scenario of home network. And this scheme is also an example to improve the efficiency of home DRM protocols and get a good person kind interface in home network DRM.

The rest of paper will be arranged as follows: Section 2 gives an overview of the home network DRM schemes. Then we propose the proxy signature to simplify the authentication protocol on content demanding in section 3. In section 4 we detail the efficient proxy signature scheme. In section 5 we give a security analysis to show that our scheme meets the six properties of proxy signature. Finally in section 6 we conclude it and give the future works.

## 2 OVERVIEW OF HOME NETWORK DRM SCHEMES

A number of implementations of AD-like DRM systems are known.

The SmartRight system (Smartright technical white paper, 2005) has been proposed by Thomson Electronic, and relies on smart cards modules incorporated into CE devices. This scheme is mainly based on public key certificates and devices in the domain share the same symmetric domain key, which is used to encrypt the protected contents. The main drawback of this approach is its poor designed protocols and that it's hard to revoke devices and update the domain key.

The xCP architecture (xCP Cluster Protocol,

Wang X. (2005).
AN EFFICIENT PROXY SIGNATURE SCHEME IN HOME NETWORK DRM.
In *Proceedings of the Second International Conference on e-Business and Telecommunication Networks*, pages 191-194
DOI: 10.5220/0001419801910194

2005) has been proposed by IBM, and is based on broadcast encryption. This is great improvement from an economical point of view. However the P2P model are not well suitable for the home network. In home network there are always administrators-parents.

The Philips patents WO2004027588 (Philips patent WO2004027588, 2005) is based on the idea that an authorized domain is set up with a central device administering the network. When a device enters the network, the central device registers the entering device and issues a domain certificate to the entering device. This invention designs a certificate chain, illustrated in Fig. 1, contains the following certificates:

- The (external) Certificate Authority (CA) root certificate, self-signed and is used to sign device certificates.
- The device certificate, signed by the CA root private key and containing the device public key.
- The AD root certificate, which is generated by the ADM (AD Manager) at AD setup and which signs a new key pair.
- The private key corresponding to this certificate will be used to issue AD device certificates.
- The AD device certificate, issued by the ADM when the device joins an AD.

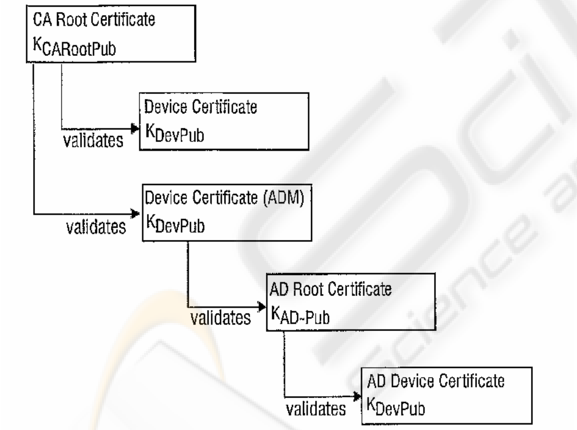

Figure1: Certificate Chain (Redrawn from (Philips patent WO2004027588, 2005)).

Philips' scheme is suitable for today's digital home, which is centralized in management but distributed in location. And the public key encryption is also more popular than broadcast encryption in today's consuming devices.

# 3 THE AUTHENTICATION PROTOCOL ON CONTENT DEMANDING

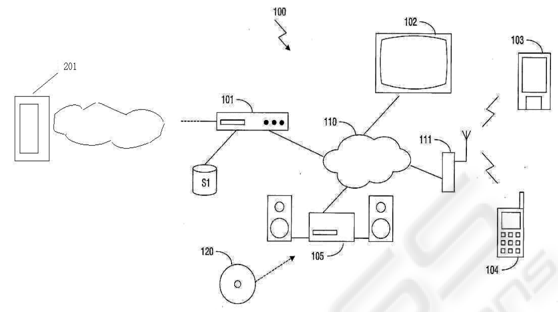

Figure 2: Home network System (Redrawn from (Philips patent WO2004027588, 2005))

Fig.2 shows an in-home network system 100 comprising devices 101-105 interconnected via a network 110. In this system a set top box 101 is the central administrating device, providing central control over the others.

When the portable device 103 demands content from content provider 201, the device 103 should show the content provider 201 not only its device certificate, which is issued by device manufacturer (CA Root), but also its AD device certificate. Since the certificate is in chain and the content provider only trusts the CA Root, the device 103 should show content server 201 the device's AD device certificate, AD Root Certificate and the ADM's certificate. And the content provider 201 verifies all the certificates in turn. The certificate chain makes much complexity in authentication.

We notice that the certificate chain could be expressed by proxy signature. So we try to use proxy signature to simplify the authentication.

There're many paper about proxy signature, the primary schemes are (Mambo et al., 1996 a) (Mambo et al., 1996 b)(Usuda et al., 1996) (Kim et al., 1997) (Jiguo, 2002).

M-U-O proxy signature schemes (Mambo et al., 1996 a) (Mambo et al., 1996 b)are the first two schemes of proxy signature but donnot provide nonrepudiation. It is impossible to decide who is the actual signer of a proxy signature in their schemes. Another drawback of these schemes is that they require a secure channel to transmit the proxy signature key from the original signer to the proxy signer. Anyone who can intercept this proxy signature key can impersonate the proxy signer.

(Usuda et al., 1996) (Kim et al., 1997) (Jiguo, 2002) give some improvement to M-U-O's scheme.

But they all have the drawbacks that the protocols are too complicated to consuming devices.

In the next section, we will give an efficient scheme. And it also meets the six properties of the proxy signature—Unforgeability, Verifiability, Undeniability, Distinguishability, Proxysigner's Deviation and Stong Identifiability.

# 4 AN EFFICIENT SCHEME OF PROXY SIGNATURE

We suppose that the CA Root has the private key $s \in_R Z_q$ and the corresponding public key $V = g^s \bmod p$. And ADM has the key pair $h_1 \in_R Z_q$ and $H_1 = g^{h_1} \bmod p$. And AD Root has the key pair $h_2 \in_R Z_q$ and $H_2 = g^{h_2} \bmod p$. $f()$ is a one-way hash function.

So in the step (1), CA Root select $k \in_R Z_q$ and compute $K = g^k \bmod p$ and $\sigma = sf(V,H_1) + kK \bmod q$,

Step (2) CA Root sends $(\sigma, K, V)$ to ADM. Since $\sigma$ has the hash of $H_1$, so this message should not send in secure channel since no one can impersonate ADM.

Step (3) ADM checks if $g^{\sigma} = V^{f(V,H_1)} K^K \bmod p$.

Step (4) ADM select $l \in_R Z_q$ and compute $L = g^l \bmod p$ and computer

$$\sigma' = sf(V,H_1) + kK + h_1 f(H_1,H_2) + lL \bmod q$$

Step (5) ADM sends $(\sigma', V, K, H_1, L)$ to AD Root. Since $\sigma'$ has the hash of $H_2$, so this message shouldn't send in secure channel since no one can impersonate AD Root.

Step (6) AD Root signs message $m$ by $(\sigma' + h_2)$, the message m is the certificate of device.

So in step (7) content provider just uses the public information $(V, K, H_1, L, H_2)$ and constructs a new $V' = V^{f(V,H_1)} K^K H_1^{f(H_1,H_2)} L^L H_2 \bmod p$ to verify if device is a valid AD device permitted by CA Root and if the AD device certificate is issued by ADM and AD root.

# 5 SECURITY ANALYSIS

**Scenario1:** $(\sigma, K, H_1)$ and $(\sigma', K, H_1, L, H_2)$ needs no secure channel. Since $\sigma$ has the hash of $H_1$, no one except ADM could reconstructs $\sigma'$. And since $\sigma'$ has the hash of $H_2$, so only AD Root could sign message m by its proxy signature key $(\sigma' + h_2)$.

**Scenario2:** The difficulty of finding the corresponding proxy signature key $\sigma$ from the equation $g^{\sigma} = V^{f(V,H_1)} K^K \bmod p$ under the attacker knowing $V, H_1, K$ is equivalent to solving discrete logarithm hard problem. Hence, it is computationally infeasible for the attacker to derive proxy signer's signature key $\sigma$. And this is same to the final signature key $\sigma'$

**Scenario3:** Given a valid proxy signature

$$(Message,(sf(V,H_1)+kK+h_1 f(H_1,H_2)+lL \bmod q),K,L)$$

. Since the proxy signature includes the proxy signer's private $h_2$, the original signer could not forge another valid proxy signature. And if it randomly selects one number and tries to solve $K'$, this problem seems to be more difficult than discrete logarithm hard problem.

**Scenario4:** Given a valid proxy signature

$$(Message,(sf(V,H_1)+kK+h_1 f(H_1,H_2)+lL \bmod q),K,L)$$

. Since the original signer's public key is included in the hash function, neither the original signer nor an attacker could forge a proxy signature key by public key substitution attack.

**Scenario5:** Given a valid signature

$$(Message,(sf(V,H_1)+kK+h_1 f(H_1,H_2)+lL \bmod q),K,L)$$

Since no one could forge the signature except the proxy signer, the proxy signer could not deny the signature.

## 6 CONCLUSION

In this paper we overview the existing home network DRM schemes. And then we give an efficient proxy signature scheme to simplify the device authentication on content demanding in the Philips scheme. Finally we analyze the security of our scheme.

And this efficient scheme is also an example to improve the efficiency of home DRM protocol and get a kinder interface to consumers. The proxy signature could be used not only in device authentication, but also on the scenarios when mobile device acts as an agent of the central administering device and the family member takes the charge of AD administrator. And we should think over other security technologies to improve the efficiency of home DRM protocol also.

## REFERENCES

Smartright technical white paper.. Retrieved from Thomson company website. Jan. 2005. http://www.smartright.org/images/smr/content/ /SmartRight_tech_whitepaper_jan28.pdf,

xCP Cluster Protocol. Retrived from IBM company website. Jan 2005 http://www.almaden.ibm.com/software/ds/ContentAssurance/papers/xCP-DVB.pdf

Philips patent WO2004027588, Retrieved Jan. 2005, from http://v3.espacenet.com/textdoc?DB=EPODOC&IDX=WO2004027588&F=0

M. Mambo, K. Usuda and E. Okamoto. Proxy signatures for delegating signing operation. Proc. 3rd ACM Conference on Computer and Communications Security, ACM Press, 1996, 48-57, Retrieved from ACM online database

M. Mambo, K. Usuda and E. Okamoto. Proxy signatures: Delegation of the power to sign messages. IEICE Trans. Fundam., 1996, E79-A, (9), 1338-1354

K.Usuda, M.Mambo, T.uyematsu, and E. Okamoto, "Proposal of an automatic signature scheme using a compiler", IEICE Trans. Fundamentals, vol.E79-A,no.1,1996,pp.48-57.

S. Kim, S. Park, and D. Won, "Proxy signatures, revisited", Proc. Of ICICS'97, International Conference on Information and Communications Security, LNCS 1334, Springer-Verlag, pp. 223-232, 1997. Retrieved from Springer online database

Li Jiguo, Cao Zhenfu, Zhang Yichen. Improvement of M-U-O and K-P-W Proxy Signature Schemes. Journal of Harbin Institute of Technology. 2002,9(2): 145~148.