Certificate-Based Adult Authentication Mechanism for Digital Content

SEOKLAE LEE[1], INKYUNG JEUN[1], JAEIL LEE[1], AND JOOSEOK SONG[2]
[1]Korea Information Security Agency
78, Garak-dong, Songpa-Gu, Seoul 138-803, Korea

[2]Dept. of Computer Science, Yonsei University
134, Shinchon-dong, Soedaemun-gu, Seoul 120-749, Korea

Abstract: - Today, we have access to an enormous amount of information through the Internet, anytime and anywhere. Ease of access to a variety of digital content, such as images, sound, and text, improves our quality of life quite significantly. However, the relative lack of restraint on access to digital content allows not only adults, but also minors, access to harmful sexual material. This results in serious damages to society. Based on the understanding that there are few mechanisms to screen out minors from accessing inappropriate content available on the market, this paper suggests an approach whereby a confirmation of age of a user, using a X.509 certificate of electronic signature is applied when the user attempts to access certain material. To do this, the additional service of the certificate authority and the on-line identity(ID) certificate is suggested. Using this PKI system to distinguish minors from adults, we can ensure the safe use of digital content for everybody.

Key-Words: - PKI, X.509 Certificate, Digital Content, Adult Authentication

1 Introduction

Development in information and communication technology has brought about innovations in a variety of segments in our community, such as politics, economics, society, and culture. As high-speed Internet continues to penetrate our daily lives, free communication exceeding the limits of time and space has been made possible. This has allowed us to share information anytime and anywhere. Voice, image, and text provided through either wired or wireless Internet access is referred to as digital content, to which we have very easy access. Today, digital content is circulated and provided over the Internet without restraint.

The volume of the worldwide digital content market in 2004 was $151,223 million[1][3]. The provision of digital content is surely promising for the IT industry, but there have been a number of side effects. There is a strong and growing demand for adult content to be made accessible by adults only. In reality, there are no measures taken to prevent minors from gaining access to such content. Most digital content sites lack a mechanism to block the access to minors. Those that did were only using a very simple mechanism of merely checking names, addresses, and mobile phone numbers to which minors have very easy access. Such measures do not function as safe and reliable tools to confirm user identity. The most reliable and the safest way to confirm the ID of a subscriber to adult content and prevent damage caused to and by those who utilize the ID of others is using a X.509 certificate[2]. The certificate has been used in applications that require integrity of user information, such as Internet banking. It has been used as a security mechanism to ensure the security of electronic transactions. However, the certificate currently in use does not contain information of the age of the subscriber. What we need to do is develop another mechanism capable of determining whether or not a user is an adult.

This paper suggests using such a certificate system to confirm the age of a user or subscriber in an attempt to prevent minors from accessing harmful adult sites. In Chapter 2, we will assess the current status of the digital content market and the problems found in the adult authentication approach. In Chapter 3 I will offer a certificate approach to enhance the user verification process for access to digital content. Chapter 4 reviews the efficiency of the certificate approach suggested in the paper, and Chapter 5 presents the conclusion reached.

2 Background and Motivation

With information technology being developed so rapidly, the digital content industry has been growing rapidly. Digital content here refers to intangible goods, such as images, pictures, voice, and text transmitted through a network in digital format, which can be used on a computer immediately. However, the nature of the on-line environment makes it very difficult to confirm the identity of users who access digital content provided over the Internet. In order to promote a constructive and healthy growth of the digital content industry, a mechanism to prevent minors from accessing harmful content should be put in place. Already, some digital Content Providers (CP) already adopted the access control mechanism for screening out minors. The first mechanism is simply to ask for personal information, such as the name, address etc of the user, and does not involve going through a specific adult authentication process. Most content providers have adopted this approach. Unlike off-line stores, there is no way to confirm the user in person on internet. This information doesn’t include any adult information of user. So, CP cannot possibly verify that the personal information the user has entered is correct or not. This is why most CPs offer digital content without going through the process of confirming the age of the user.

A second approach is to use the confidence information of a residential registration number (hereinafter referred to as RRN), credit card number, bank account, and other such information, based on the government policy, in order to confirm the age of the user. This approach has been adopted by some countries, including Korea. However, this approach also has limitations. Most users are not willing to offer particularly private or personal information, such as their RRN or credit card number. They fear the risk that the information may be stolen and abused. This raises issues about privacy protection. Furthermore, there is no way to check the information is actually their own (and not, for example, their parents'). This approach, therefore, falls short of being a reliable adult authentication mechanism.

The third approach is to request ID confirmation using the Short Message Service(SMS) of a user's mobile phone. In other words, the user enters his mobile phone number and CP establishes whether the person is an adult or not using the information on their phone subscription records. Once confirmed as an adult, the operator sends a identity number to the user. This approach also has the shortcoming of not being capable of verifying whether or not the person in possession of the mobile phone is the mobile phone account owner. Many young people are using their parents' mobile phone accounts, so they can access the adult content easily. In conclusion, none of the three mechanisms aforementioned is a perfectly safe approach to adult authentication. None, as yet, have the solution for the growing concern of the protection of privacy, and none are perfectly capable of verifying the identity of the user.

3 Certificate-based Adult Authentication

Both the lack of mechanisms of adult authentication and the indiscriminate consumption of adult content by youth have created serious harm to society[4]. This paper suggests that the solution to this issue is the safe and reliable approach of performing adult authentication using the X.509 certificate.

The X.509 certificate is being used widely to confirm user identities in a number of on-line service sites, such internet shopping malls. The certificate contains information about the certificate owner and issuer, such as the name of the certificate holder, the date when the certificate was issued, the serial number of the certificate, and the name of the certificate issuer [5][6].

3.1 Using the Additional Service of CA

This approach utilizes the database that the Certificate Authority(CA) has on the owners of digital certificates. This uses a digital certificate which is issued after confirming the identity of a person by Registration Authority(RA). Before detailing the system further, let's clearly define the terms used

User : Person who receives a certificate issued by an certification authority for the purposes of utilizing digital content.

Content Provider(CP): Internet content providers who offer digital content to users.

Certificate Authority(CA): The party that holds the registration information of the user on its system, and issues digital certificates to the user.

Registration Authority (RA): The party that applies for certificate issuance. This party is in charge of confirming the identity of the user and delivering the registration information to CA.

Adult authentication procedure by using the additional service of CA is constructed 2 phase, one is the process of issuing a certificate, and the other is that of confirming adult authentication using the certificate.

[Procedures 1] : Procedures for issuing a certificate

Users who wish to obtain adult certificate apply for the certificate issuing through CA or RA. For the identification of users, personal information such as name, age, address, telephone number, gender, RRN, or credit card number can be confirmed. And these information are stored of CA or RA database. Users whose identity is confirmed apply for the issue of a certificate through CA or RA. And then, CA or RA issues a certificate to the user, publishes the certificate in the directory.

[Procedures 2] : Adult authentication process using a additional service of CA

① User accesses the adult content site.

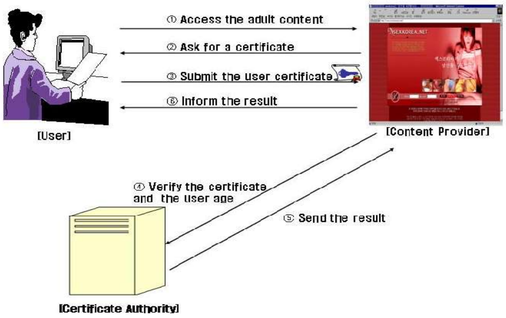
② CP asks for adult authentication before allowing the user access to the site.

③ User submits their certificate.

④ CP asks CA to confirm the validity of the certificate, establishing that the user is an adult.

⑤ CA confirms the validity of the certificate, establishing that the user is an adult using the registration information.

The procedure 2 is described in Fig1.



[Fig 1] Adult authentication process using certificate

If user uses this approach, he does not need to provide his personal information to CP each time they intend to access adult content, except their certificate. This method eliminates any controversy over privacy infringement. As identity checking is done through a reliable CA, the method is considered a safe approach to confirming identity. It also increases the user's convenience, as one certificate can be utilized for on-line financial transaction services including Internet banking, establishing user age. However, there is one pitfall. This approach assumes that the CA that issues a certificate holds the registration information required to confirm the identity of the user. This means that the user needs to have provided his or her personal registration information. CA or RA has an obligation to check that the registration information of a user is true. As CP is required to be connected with CA in order to verify the user's identity, there may be additional costs.

3.2

Using online ID certificate

The above service which is using the additional service of CA has the problem of placing a burden on CA, as all inquiries are delivered through the CA system. Also, CP needs to wait for a response from CA. This can result in an over-reliance and a heavy burden on the CA system. This problem could be resolved if the CP can verify the user's identity itself.

As a solution to this, CP can employ a function enabling it to verify certificates on its own. Another issue, however, with the verification process then arises. In case of the X.509 certificate aforementioned, none of the personal information held is suitable for determining whether the user is an adult or a minor. Unless CP holds all the registration information of the subscriber, it cannot independently verify user age. To solve this, this paper suggests using an on-line ID certificate to check user identity on-line. Unlike the existing certificate, this on-line ID certificate contains a field that can distinguish minors from adults. So, CP enables CP itself to establish user age without using the personal information of a subscriber. This certificate can be used in e-commerce, internet banking as well as adult authentication.

In the on-line ID certificate, the issue is how to include a user age in the certificate, This is solved as follows. Firstly, an extension field inside the certificate, referred to as the “Subject Alternative Name”, can be used to indicate whether the person is an adult or not. For example, 'adult' or 'minor' is entered into value of “Other Name” field as below, and is then provided to the CP.

SubjectAltName ::= GeneralNames,

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {

otherName [0] OtherName,

... }

OtherName ::= SEQUENCE{

type-id OBJECT IDENTIFIER,

value [0] EXPLICIT ANY DEFINED BY type-id }

Second approach is to use the CN information inside the “Subject Name” field of the certificate owner instead of using a separate extension field. In other words, if the CN value behind the actual name is "Alice_1", this indicates the subscriber name is "Alice" and she is an adult, that is a '1' indicates she is an adult, whereas a '0' indicates they are a minor.

Using these methods, CP can verify the user’s identity using the certificate. We can use the qualified certificate instead digital certificate[7]. But, this on-line ID certificate has a merit that it can be used in e-transaction as well as e-identity.

Adult authentication processing is same as the process using additional service of CA in phase 3.1 except the CP verify the identity of user as follows.

① User accesses the adult content site.

② CP asks for adult authentication before allowing the user access to the site.

③ User submits their on-line ID certificate.

④ CP confirms the validity of he certificate, establishing that the user is an adult using the registration information.

This approach don’t need that CP is connected with CA in order to verify the user’s certificate, so there is no additional casts. In short, the on-line ID certificate approach is one that involves lower additional costs for CP, as CP is able to maintain an independent verification system without having to connect its system with CA. Also, this method eliminates any controversy over privacy infringement

4 Analysis

This chapter will analyze and compare the features and security elements of the existing approach of adult authentication with the one suggested here. Authentication approaches are classified and summarized as follows in Table 1 (see the Table 1 at the end of the paper). The authentication approach using the certificate as shown in Class 1 and Class 2 above can be used in the area of e-commerce as well as identity confirmation and adult authentication, as it utilizes a certificate issued after a person-to-person interview conducted by RA and CA. This means that it can be used safely when making purchases of high-cost content that also require adult authentication, as well as for a number of e-commerce transactions, ranging from Internet banking to on-line securities transactions, etc. In addition, the personal information registered at CA is specifically utilized in order to perform adult authentication of the user. This means the user does not need to transmit his or her personal information. There is no risk, therefore, of personal information being disclosed to others. However, in the case of Class 1, additional costs are borne as the CP needs to be linked with CA. Also, in the Class 2, the CP needs to implementation the certificate verification model in it.

The authentication approach outlined in Class 3,using the name, RRN,or mobile phone SMS certification number, is currently widely used to perform adult authentication and is not considered as firm as those proposed in Class 1 or 2. Its use in financial transactions is therefore limited. Its use should be reserved for confirming user identity at the time of subscription to a certain program. As the information required in this approach, such as name, RRN, credit card number, etc, can be easily obtained by a minor, this approach should not be considered a solid certificate approach for the purposes of adult verification. Its benefits are the lack of installation costs as, unlike in Class 1 and 2, it does not require certificate verification installation.

The approach described in Class 1 is considered the best approach in terms of user convenience, as it can be used in almost all application sites, as well as for the sake of adult authentication and e-commerce. The certificate issued based on a person-to-person interview can be used in the important areas of e-commerce, adult authentication, and on-line shopping with no restraints. Those subscribers who utilize a variety of Internet applications services would be better served by a certificate.

Different authentication approaches can be used depending on the type of applications sites the user accesses, and the decision made by CP. No one can be forced to utilize any one approach. However, the use of a certificate is absolutely necessary when dealing with the issue of preventing minors from accessing sites with harmful sexual material.

5 Conclusion

Internet has enabled people to be connected with each other whenever they want, wherever they want. Behind this glorious snapshot lie hidden problems, such as forfeiting one's rights to privacy, the exposure of young people to sexually explicit material, and many others. This paper analyzed the weaknesses that current adult authentication approaches have when it comes to digital content utilization. It proposes the use of an adult authentication approach based on certificate issuance. The approaches currently used for adult authentication actually lack genuine adult authentication functions. They are also susceptible to users using the personal information of another individual. It is doubtful whether such approaches can be relied upon with confidence to perform actual adult verification functions. As an alternative to current approaches, we propose the use of a certificate-based system.

The certificate approach provides a user authentication function that users can also trust and rely on for use across a variety of different applications. In addition, the safety of this approach for e-commerce purposes has already been proven. I hope to see a day where minors may safely sit at a computer without the risk of exposure to harmful sexual material. This may be realized with a certificate-based adult authentication system as described in this paper.

References:

[1]KIPA, *A Study on Global Digital Content Industry : Executive*, March 2005

[2]ITU-T, *ITU-T Recommendation X.509 (1997) ISO/IEC9594-8:1998, Information technology - Open Systems Interconnection - The Directory : Authentication Framework*, 1998

[3]D-Lib Magazine*, The Growth of Digital Contents*, December 2004

[4]ITU, *World Telecommunication Indicators Database*, 2004

[5]Russ Hously, Tim Polk, *Planning for PKI*, Wiely Computer Publishing, 2001

[6]R.Housley et al., *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, RFC3280, IETF, April, 2002

[7]S.Santesson et al., *Internet X.509 Public Key Infrastructure: Qualified Certificates Profile,* IETF, 2004

<Table 1> Analysis of Adult authentication method

Level	**Class 1**	**Class 2**	**Class 3**
Authentication Method	CA additional Service	Online ID Certificate	Personal Information
Feature	Certificate-based	Certificate-based	RRN-based
Privacy	Safe	Safe	Unsafe
Reliability	High	High	Low
Verify Subject	CA	CP	CP
Implementation	CA-CP connect	Only CP	Only CP
Function	Integrity Authentication Non-repudiation	Integrity Authentication Non-repudiation	Authentication