Secure Authentication and Document Signature with Cryptogram Smart Card in an Insecure Environment

Peter Sweeney[1], Xiyu Shi[1], David Burgess[1], Alain Rhelimi[2]

[1]Centre for Communication Systems Research, University of Surrey, Guildford, GU2 7XH, UK

[2]Axalto, 50 Avenue Jean Jaures, 92120 Montrouge Cedex, France

Keywords. authentication, security, digital signature, smart card, concept

Abstract. This paper describes a mechanism for secure online user authentication and document signature with a cryptogram Java card in an insecure environment. The mechanism requires possession of both the card and some secrets, known as Concepts, to authenticate the user. The concepts are represented in image form. A method of secure document signing with the concept-based images is also outlined. Possible security weakness and attack methods are analysed in the paper. An implementation of the mechanism is also described in brief. It is anticipated that the mechanism would provide security and non-repudiation for e-Commerce customers in an insecure operating environment.

1 Introduction

Authentication is the process of one entity to verify another entity as being the claimed one. It is essential for such applications as online payment systems and security access control systems to be assured that the user is a legitimate user as claimed. Authentication can be usually carried out based on user knowing something (e.g. a password), possession of something (e.g. a certificate or card), or something unique (e.g. fingerprint, signature). It is generally used with any two combinations of these three factors. The most common method in use is the user password in conjunction with a conventional card (e.g. a magnetic strip card). It is, however, not safe enough to count numerous online frauds, forgeries and counterfeiting.

The secure user authentication mechanism described in the following sections takes advantage of the latest smart card technology with cryptogram functionality. The objective of this mechanism is to provide two-factor authentication so that possession of both the smart card and some secrets, known as *Concepts*, are required to authenticate the user. This would provide security, for example, for card payments

Sweeney P., Shi X., Burgess D. and Rhelimi A. (2004).
Secure Authentication and Document Signature with Cryptogram Smart Card in an Insecure Environment.
In *Proceedings of the 1st International Workshop on Electronic Government and Commerce: Design, Modeling, Analysis and Security*, pages 82-90
DOI: 10.5220/0001401900820090

made over the Internet. The mechanism is also to enable a contract to be drawn up and to be signed with adequate provision to guard against repudiation, despite the fact that the cardholder will be operating in an insecure environment, namely a networked PC.
The mechanism approach is first discussed in following section. The concept, image and their relations are explained in Section 3, followed with the description of document signature in Section 4 and an implementation of the mechanism in Section 5. A security analysis and possible attacks are also given in Section 6.2

2 Approach

It is important for commercial reasons that the approach avoids the need for any special equipment. Approaches using biometrics, for instances iris, fingerprint and voice, have therefore been rejected in favour of an approach in which the user proves identity by possession of a piece of knowledge, similar to the way in which a Personal Identification Number (PIN) is used in conjunction with a conventional card. However the conventional card is vulnerable both to skim and counterfeit attacks. By contrast, a smart card is considered to be more secure than a conventional card, hence it is chosen for the secure authentication mechanism described here. The first step of security is that the smart cards are resistant to cloning and so someone obtaining the secret cannot make use of it without physical possession of the card. Even so, in present applications secure PIN pads are used, so it is obviously still required that the secret should be protected. Of course on a networked PC, it is possible for a process to be installed that could eavesdrop on the secret and take possession of the card. Therefore the system must provide a reasonable degree of security for the secret and protect against processes that could operate the smart card remotely. This latter point is addressed through provision of a contact on the card that can be connected only by external physical means - the pressing of a button on a card connector. It is therefore possible to ensure the physical presence of the cardholder while the authentication is being carried out. The way that the secret is protected is one subject of this paper.

The difficulties with a conventional PIN are that it is easy to forget and also easy to acquire through some attacking process. It has therefore been decided that, in addition to the simple PIN used to unlock the card, an additional level of security should be provided using a secret represented and identified through a sequence of images, in a manner to be described. It is hoped that it will be possible to provide something that is memorable but difficult for an outsider to recognize. The method should guard against automatic acquisition of the secret, although any attack requiring human intervention to succeed is judged to be an acceptable risk.

3 Representing Secret With Concept Based Images

There are several ways to represent a secret by a sequence of images. A basic scheme would be for a user's secret to consist of a set of fixed images. Alternatively the images representing the secret might vary. Either of the representations requires a direct relation linking the image to the secret. Using concept-based image to represent a secret is more complex and secure.

3.1 Fixed Image Secrets

With the secret being represented by fixed images, the identifiers of images constituting the secret are stored on the card and transmitted to an authentication server during authentication. The user requiring authentication is presented with a page of images, of which one corresponds to the secret. This is selected and further pages are presented in succession, each containing one of the secret images. The pages could consist always of the same set of images in different positions, with the user required to select the secret images in a fixed order. This would be very similar to a PIN scheme except that the numbers are represented by images and change their position on the screen. Alternatively, with a larger number of images on the page, it might be possible for the user to select all the secret images on a single page. However this would require, for example, 24 images on a page for a selection of 4 to give the same degree of security as a 4-digit PIN (assuming the order of selection is not considered). Requiring more images to be selected does enhance the security, but to provide equivalent to a 5-digit PIN, five images out of 29 are needed.

If the same set of images is displayed every time, there are only a very limited number of possible secrets. It is interesting to consider what would happen if the images not corresponding to the secret were to be generated randomly so as to increase the range of possible secrets. This is actually less secure than a fixed set of images because after a small number of observations of the pages being presented it would be possible to deduce the secret without observing the user's responses. In this case the images being sent to the user would certainly need to be in encrypted format, for decryption by the card.

Ultimately, however, any scheme on these lines fails the criteria because it is certainly possible for an automatic process to recognize images and collect the key-strokes or mouse inputs identifying the secret.

3.2 Variable Image Secrets

In this scheme, the images representing the secret might vary. For example, if one of the secrets is a woman, there are lots of pictures of women that could be used, or even other representations such as the $_{y}$ symbol representing female.

Now of course the recognition task for any attacking process becomes more severe because it has to recognize the underlying secret for any user selected image and be able to identify the corresponding images on any page, despite the fact that there

might be a large number of images in the database for any secret and various geometric manipulations could be applied to any image for display without affecting the underlying secret. Moreover the problem with randomly generated dummy images is less severe because the secret images will vary from one occasion to the next. On the other hand, care needs to be taken in setting up the image database to ensure that there is no ambiguity in any of the images, i.e. that each image conveys only one out of the possible set of secrets.

3.3 Concept-Based Images

Based on the schemes above, we can go further to use a sequence of concepts rather than fixed images and objects to represent the secret. A concept is an attribute of an image or object in the image. It is conveyed in the image and may be extracted from the image. The user's secret - the set of Concepts - is stored on the smart card. An user is authenticated by recognizing the secret concepts from a series of displayed images. For a single concept to be satisfactorily represented by an image, the concept will almost certainly be an animate object. Other possible concepts reflecting abstract ideas, emotions, relative position or movement will require multiple objects in the image. It is possible, therefore, for a single image with multiple objects to convey several concepts, some of them not directly implied by any one of the objects on its own.

Fig. 1. Example of Authentication Image

For example, a very simple description of the image in Figure 1 is that *"a woman walking her dog"*. However we might easily use this image where the secret includes the concept of humour, because the image has the appearance of a cartoon and the woman strikes a comical pose. The semantic analysis needed to extract automatically such concepts from images is beyond current computational techniques. On the other hand it could certainly be done by humans and it may be possible for a human observer to identify the underlying similarities between chosen images. However, as stated previously, it is considered that this type of threat can be accepted.

For a feasible use of the concept-based image scheme, a large number of images and their corresponding concepts are required and a relational database can be used to hold these data. Technically we can index images by their underlying concepts and access the appropriate concept combinations through the database. However when it comes to putting images into the database, a human analysis is needed of each image to extract the concepts. Moreover different people may see different concepts in a single image, so some grading is needed to identify whether a particular concept is strongly or weakly in a given image or perhaps whether the image conveys an opposing concept. For example a dangerous situation would be definitely not be

confused with a secret containing the concept of safety and so could be presented as one of the dummy images. However once primary concepts have been extracted, a dictionary could be used to extract secondary and related concepts.

There is also the matter of deciding what are good and bad secrets. This is not unique to this type of secret - a PIN of 1234 or 9999 would not be considered a good value. In the context of our concepts, it is certainly not a good idea to choose two concepts where one is an attribute of another. For example if an animal is part of the secret, it is a bad idea to also have a specific animal as another secret because the more general concept is effectively wasted. Having concepts that are too specific is a bad idea, but this can perhaps be recognized by the scarceness of database entries with that concept.

4 Document Signature

It is a simple enough task for the smart card to sign a document using its RSA private key. The issues are how to be sure that the user has seen the document and that the document displayed is the same as that received by the card. The issue of ensuring that the user has seen the document is addressed by overlaying the images for authentication on the document itself. Ensuring that the document has not been modified between the card and the display is more difficult. With the help of a card-enabled stand-alone device it would be possible for the user to draw up the contract, or some part of it, and include a signature that would verify the important details. Unfortunately, human beings have low computational capability and cannot check RSA signatures. We are therefore left with a difficult problem, namely how can we put something into a document that will be checked by the card, such that an attacking process will find it difficult to amend properly but errors in the amendment will be easily spotted by the user. As stated above, formatting the document as an image with sensitive information in words and figures will help.

The scheme is designed such that the document to be signed is passed to the cardholder system prior to the authentication and is passed to the card for integrity checking. The authentication test (i.e. images) is applied as an overlay on the document to be signed, thus ensuring that the cardholder has seen the document. If the user makes the correct authentication response, the card recognizes this as described in Authentication Decision of Section 5.3 and is able to sign the document using a hashing function (SHA-1) encrypted using the card's private key. The signed document can then be sent to other partner, e.g. to a merchant in a message corresponding to the purchase request.

5 The Implementation of the Scheme

5.1 Requirements

The described user authentication and document signature mechanism involve three entities: a cryptogram smart card, a cardholder's system and an authentication server. The smart card should be able to complete RSA public key encryption and decryption, digital signature and SHA-1 hash function. A card reader connects the smart card with the cardholder system. The cardholder system communicates with the authentication server via the general Internet. A connection between the authentication server and a concept-based image database also requires to be established.

The smart card that stores a cardholder's secret concepts must be presented whenever the user authentication and signature are requested. The cardholder is challenged with a series of test questions - the concept-based images - and there should be no direct relation linking the questions with the secrets the cardholder possessed. A decision of whether or not the cardholder is authenticated must be solely made by the card and on the card. All messages transferred in the session of authentication must be authenticated in order to protect for data
integrity. Responses to the questions must be enciphered in order to protect for data confidentiality.

5.2 Concept Challenge and Response

User authentication is performed by a verification test which involves a challenge and a corresponding correct response. The test is passed if the correct response, after decryption, is the same as the cardholder's response.

The challenge data comprises four (or possibly more) ordered sets of ten images,

$S_i = \{I_{i,1}, I_{i,2}, ., I_{i,j}, ., I_{i,10}\}$ (1)

Where $i = 1, 2, 3, 4$

S_i: the i^{th} set of ten images

$I_{i,j}$: the j^{th} image in Set i

Each of the sets must contain exactly one image $Ii,f(i)$ (i = 1, 2, 3, 4)which conveys the cardholder's concept(s). The correct response is simply the sequence of numbers f(1), f(2), f(3),.f(4), encrypted. To avoid susceptibility to a simple frequency count, the image database needs to be large enough. For further security, the positions of all of the individual images within the ten are chosen randomly for each session of authentication.

The scheme is developed such that the secret is not simply the sets of images $Ii,f(i)$ (i = 1, 2, 3, 4), but a set of concepts which are contained only in these images out of forty presented. In this case, as each of the images $Ii,f(i)$ (i = 1, 2, 3, 4)varies from authentication to authentication, so will the other images in its set.

5.3 Message Flow

The message flow between the main components of the scheme is illustrated in Figure 2.

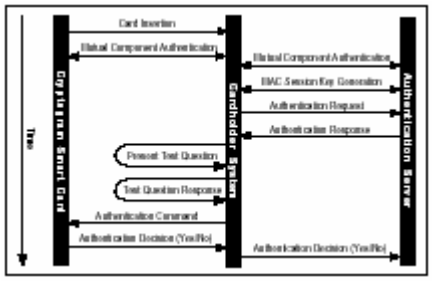

Fig. 2. Diagram of Message Flow Between Components

Card Insertion - The cardholder inserts the smart card into the card reader that is connected to the Cardholder System. The insertion therefore invokes the authentication procedure.

Mutual Component Authentication between the smart card and the Cardholder System - The card only sends meaningful data to a verified Cardholder System and the Cardholder System only receives data from a verified card. The card and the Cardholder System use RSA digital signature to verify each other. This step involves exchange of public keys, random numbers and signatures. If the mutual authentication is successful, the card and the Cardholder System satisfy each other and can transfer sensitive data from now on. Notice that similar mutual component authentication is also required for the cardholder system and the authentication server.

MAC Session Key Generation - The Cardholder System and the Authentication Server compute a secret key for encryption of the MAC (Message Authentication Code) of transmitted messages in this session of user authentication. The session key is a shared secret without explicit exchange of the secret.

Authentication Request - The Cardholder System requests test questions by sending an authentication request to the Authentication Server.

Authentication Response - The Authentication Server uses the concepts in the authentication request message to generate an appropriate authentication response message and returns to the Cardholder System. The response includes a group of test questions and correct test responses. To do this, the Authentication Server needs to first decrypt the concepts part of the authentication request message and generate the suitable images as the test questions. The images should be arranged in such a way that the sequence appeared in the question series is randomly decided, the images stands for only a group of concepts not related to any specific numbers.

Present Test Question - The Cardholder System presents the cardholder with the test questions and waits for responses from the cardholder. Usually the test questions are produced on the screen of the Cardholder System.

Test Question Response - The cardholder responses the test questions by selecting images which convey the cardholder's secret concepts. The steps of present test

questions and the test question response may be repeated several times depending on the way the questions are presented and the complexity of the concepts.

Authentication Command - The Cardholder System sends the Test Question Response and the encrypted Correct Test Response coming from the authentication response to the smart card for a matching verification.

Authentication Decision - The smart card compares the cardholder's response with the Correct Test Response. If no difference is found, the cardholder is authenticated and the authentication decision is true. Any other comparison results will result in a failed user authentication and the authentication decision is false. If the decision is false, the smart card must destroy any data received for this session of user authentication and must block any further data leaving the card. Whether or not the card lets the Cardholder System and the Authentication Server know the authentication decision is an optional step accomplished by an individual implementation of this scheme according to the requirements. In our implementation, the decision is transmitted to the Cardholder System and the Authentication Server. It is a compulsory requirement to encipher the decision with a proper recipient's public key.

6 Possible Effective Security Attacks

The implemented scheme is based on EMV [1] functions and the SET [2] specification, thereby protecting against most attacks. A Substitution attack is only really successful against a very limited range of authentication methods and encryptions and Exhaustive Search is not really appropriate to most Internet transactions. The only effective weakness of the scheme lies in the fact that no part of the PC can be considered a tamper evident device and so information cannot be reliably encrypted thereon. In particular, information transferred from the keyboard or mouse of the PC to the smart card interface device is not secure. This is not an issue if the question and answer involved in authentication reveal no information to enable future correct response to some question. If however they do, the Man in the Middle attack, in conjunction with obtaining a copy of the smart card could be successful for attaining the ability to make fraudulent authentication if the following procedure is achieved:

The Cardholder's response to the question can be accessed via the channel connecting keyboard or mouse of the PC to its processor or that connecting the latter to the card interface device. This can be compared with the question, accessed via the general Internet channel connecting the Authentication Server to the Cardholder System, after timing differences are allowed for. Repeated observations for the cardholder over a number of authentication sessions can compromise the secret to enable false authentication provided a copy of the smart card is available to the attacker. Note, however, that the proximity of the user to the smart card can be verified by the use of a physical contact on the card connector. As a result remote access to the card during the user authentication procedure can be prevented.

Note that the success of this attack necessitates each of five components:

1) Access to a copy of the smart card;

2) Ability to undetectably read and interpret at the correct time the information on

the channel connecting keyboard or mouse via PC processor to smart card interface device;
3) Ability to undetectably read and interpret at the correct time the information on the channel connecting the Authentication Server to the Cardholder System;
4) Ability to confirm that the information from 2) and 3) correspond to each other; sufficient number of observations to deduce the secret defining the connection;
5) Between answers and questions, an ability to make the appropriate deduction and a connection which is susceptible to being discovered by this means.

7 Summary

Concept-based image user authentication is a secure scheme designed for online authentication and signature in conjunction with a cryptogram smart card. Concepts are contained in visual images and only the legitimate cardholder can link the images to the secret concepts so that there is effective protection against the common shoulder-surfing attack on a traditional PIN (or the electronic equivalent). It is possible that no two presentations of the same group of concepts are the same, which is a great advantage over traditional PIN authentication. The scheme can be used in many applications such as online banking, security access control where user authentication is required.

Acknowledgement

This work is supported by the European Commission as part of the 5` Framework IST Program.

References

1. EMV (2000) *Integrated Circuit Card Specification for Payment Systems*, Version 4.0. December, 2000 [WWW] http://www.emvco.com

2. SET (1997) *MasterCard, PISA Secure Electronic Transaction Specification*, Version 1.0. 31 May 1997