December 2002

A MUTUAL AUTHENTICATION SCHEME FOR LOW COST SMART CARD APPLICATIONS

Rupak Rauniar
University of Toledo

Deepak Rauniar
Tribhuvan University

Subarna Shakya
Tribhuvan University

Carlos Urcuyo
University of Toledo

A MUTUAL AUTHENTICATION SCHEME FOR LOW COST SMART CARD APPLICATIONS

Rupak Rauniar
University of Toledo

Deepak Rauniar
Tribhuvan University

Subarna Shakya
Tribhuvan University

Carlos Urcuyo
University of Toledo

Abstract

Smart cards will soon exist in virtually every area of our lives. These IC chip cards will control our access to a growing number of public facilities. The technology promises much and is very flexible - in the sense that it can be designed and manufactured to serve a multitude of purposes. The power of these cards lies in their ability to store and manipulate data, to handle multiple applications on the card, and to perform secure transactions. Considering the sensitive nature of information that these cards will eventually carry, there is a strong need to protect these cards and hence the data inside the cards from misuse, be it from card theft or through a fake terminals. Authentication is one such technique, which provides the first line of defense in any security system. Authentication is the process whereby a process can verify the claimed identity of the other party in a communicating pair. In this paper, we propose a mutual authentication protocol for smart cards based on Blom's scheme. The proposed scheme can be used to provide secure authentication between a smart card and a smart card terminal, where the smart card will eventually be inserted to access a service. The scheme provides a mechanism whereby a terminal will be able to distinguish an authorized smart card from an unauthorized one. It also provides a means where a smart card will be able to distinguish an authorized terminal from an unauthorized one.

Introduction

As the world has evolved with the Information Technology (IT) revolution, so has emerged the need to process tremendous amounts of information in our daily lives. Computers are no longer a tool that only few fortune companies can afford to use to shape their future. Over the years, computers have influenced our lives as never before. Nobody has been spared the impact and benefits of the ongoing IT revolution. Computers, and to be more precise the microprocessors behind them, have delivered the ability to control, process and access information. The smart card can now provide this power and versatility of the microprocessor in our own wallet [URL02].

On inspection a smart card may look like a regular sized credit card. However, the similarity ends with the physical appearance. Simply speaking a regular credit card is a magnetic stripe card that is widely employed mainly by the banking sector. These magnetic stripe cards simply act as a token, which the owner of the card possesses to identify himself in a financial transaction. However a smart card is smart in the sense that it can make decisions during a transaction. The powers of smart cards lie in their ability to store and manipulate data, to perform secure transactions and to handle multiple applications on one card. A single smart card can be configured to access a bank account, to pay bills, to access various public utilities as well as to store personal information including high-level medical information. [LIND, 97]. A typical card consists of a complete Central Processing Unit (CPU) with a memory (ROM) for the operating system. It also contains a main memory (RAM) and a memory sector for the application data. Further some cards contain an extra cryptographic processor to achieve high level of security [URL02], [RANK, 97], [HEND, 97], [FUCH, 95].

These cards provide a high level of security with their ability to control who can access the information they contain, which is not possible in magnetic stripe cards. With the embedded microprocessor in the card, these cards possess the power to apply both

symmetric as well as asymmetric cryptography, a powerful tool for any security system, to enhance security. Some of these cards also contain arithmetic coprocessors to enhance the overall computing power to support advanced public cryptographic algorithms, providing better security with minimum delay cards developed. [FUCH, 95]].

The major disadvantage of the magnetic stripe card lies in the very simplicity of the concept, which has lead to financial fraud in massive scale. These cards simply cannot authenticate its owner as well as the terminal, where they are ultimately used to access a service. In 991 alone, magnetic-stripe card fraud losses were estimated to be as high as £ 400 Million in UK alone [URL01]. With the increased fraud and security concerns, smart cards offer a top security alternative. As per the latest study, it has been found that card fraud has decreased heavily (a massive 80 % from 1988 to 1993) with the increase in the use of smart card [LIND, 97].

Security functions of any system, including smart cards, revolve around three basic security requirements: integrity, confidentiality and availability. One of the major security concerns of present security system in general is the authentication problem. Like any other environment, in a smart card environment, three authentication issues arise [KONI, 91] [GARF, 97], [BOVE, 95]:

- is the user genuine (user authentication).
- is the smart card genuine (card authentication)
- is the system/terminal genuine (system authentication)

Before a secure card transaction can take place, the above issues needs to be resolved. Speaking broadly, whenever a smart card is used for a transaction by inserting it in a terminal, a mechanism is required such that all of the above mentioned security issues are checked before actually entering into a transaction. First, the person presenting the card needs to be verified as the rightful owner of the card, thus limiting an unauthorized third party from using the card. Secondly the terminal needs to verify the card hence presented to it, such that a transaction doesn't take place with an unauthorized cards. Lastly the card should also verify that terminal being used is an authorized one before actually entering into the transaction and revealing any sensitive information contained inside.

In this paper, we propose a mutual authentication protocol for smart cards. The scheme is quite simple and can be applied in low cost smart cards applications. In this paper, by low cost smart cards we mean to represent those applications involving smart cards, where some security mechanism is required, however, the security requirement is not as high as is offered by some of the popular public key cryptography schemes. In this paper we show how Blom's scheme, which is a key distribution scheme for computer networks, can be applied to provide secured mutual authentication between a smart card and a smart card terminal, where the smart card will eventually be inserted to access a service. Our proposal provides a mechanism such that a terminal will be able to distinguish an authorized smart card from a fake one. Similarly as it is also desired that smart cards do not enter into a transaction with a fake terminal, our proposal also allows a smart card to distinguish an authorized terminal from a fake one.

Research Motivation

In a typical card system, there are basically three different entities that are associated with the system. Besides the cardholder i.e. the consumer of whatever goods or services are offered by the system, there is a supplier of those services (e.g. supermarkets) and an operator of the card system (e.g. a bank). Almost inevitably, in accessing security threats it is implicitly assumed that some individuals will try to get the card system to produce goods or services for which they have not paid, often with the aid of stolen or doctored cards. In other words, it is assumed that it is the supplier of the services that is at risk and thus in most of the systems employing traditional magnetic stripe cards (e.g. bank automated teller machines), the overall security revolves around identifying the genuine nature of the card.

However, a full analysis needs to consider security threats from the points of view of all participants involved. In particular, the legitimate cardholder can be equally vulnerable to fraud. As more and more outlets offering card-based transactions begin to appear and considering the large number of systems (e.g. POS terminals) that eventually need to be monitored, it may not be possible for a single organisation to physically monitor them all. As such, one of the security concerns that immediately arises is that since the terminals in these outlets are under the direct physical control of the service providers (e.g the retail outlet merchants), it is possible that a dishonest service provider may set up fake terminals. The fake terminal can be designed to appear just like a real terminal with similar interfaces to fool a cardholder and eventually induce him to carry out a transaction with the fake terminal. Since the owner of the card has no way of differentiating between a genuine and a fake terminal, based on the familiarity of the interfaces when he inserts his card into the terminal, the terminal can make an unauthorised attempt to duplicate

the data from the card into its memory. Similarly, after the required PIN data has been acquired, the terminal can then come up with a false message (e.g. transaction not approved) prompting the cardholder to remove his card and eventually leave. Armed with the information revealed, the fraudulent service provider can easily duplicate a new card and then make a genuine request with the duplicated card together with the PIN, thereby emptying the cardholder's account as a genuine withdrawal [GLAS, 91].

Another security concern that arises is that it is also possible for a dishonest service provider to tamper with genuine terminals in his premises such that the terminals can buffer the communication between the card and the terminal [TEMP, 96]. He can then use this information from the buffer to his benefit as already discussed above.

The above examples clearly illustrate a realistic scenario where the cardholder can be equally at risk. Hence from a card holder's point of view it becomes equally important to check for the authenticity of the terminal before revealing any secret and eventually engaging in a transaction.

Unlike magnetic stripe cards, since smart cards do possess the power to execute cryptographic protocols, secured systems employing smart cards can be designed which can take care of the concerns of the card holder regarding the authenticity of the terminal. In general, the overall security of a smart card based system can be significantly improved if a smart card is designed to release its data only after the successful authentication of the terminal engaged in the transaction.

Authentication

Authentication is a technique whereby a process verifies the claimed identity of another distributed process over an insecure channel. A successful authentication results in authenticity, whereby a verifying process becomes sure of the identity of the claimant entity as the one, which it claims to be [OPPL, 96]. Proper authentication between distributed processes is important considering the insecure nature of the underlying physical channel where messages can be tapped, modified, deleted and initiated by an intruder. Authentication provides a mean through which distributed resources can properly verify the identity of the remote process before entering into a transaction.

When entities are authenticated, which is typically done by exchanging a series of messages based upon a protocol, both the entities in the communicating pair become confident about each other’s identity. They know for sure that they are not talking to someone else, who is impersonating as the other.

Cryptography is extensively used in authentication and a secure mutual authentication protocol is a two-party protocol, where both parties accept (at least with overwhelmingly probability) if their adversary is benign, but reject with overwhelmingly probability in the presence of an active attacker [LUCK, 97].

The core of any authentication protocol providing unidirectional/mutual identification of a distributed entity, revolves around challenge-response technique [TANE, 96], [SCHN, 96], [STIN, 95], [FORD, 94], [PFLE, 89]. In a typical run of challenge-response protocol, one of the parties involved issues what is known as a challenge to the other party, who in turn is required to come out with a proper response to the challenge. The party issuing the challenge is known as the challenger while the later responding to the challenge as the responder. The challenge itself typically involves a random number, and the entity responding to the challenge is required to transform it in some special way (often involving its private key, which is known only to the bona fide parties) and return the result. After receiving the result of its challenge, the challenger confirms it with the desired result, which also generally involves some computation locally by the challenger. If the result hence obtained matches with the desired result, then and only then the responder is authenticated. The grounds for such authentication is the fact that the responder has demonstrated the possession of a secret, which is supposedly known only to the bona fide party, and thus it is the bona fide party. By changing the roles of the challenger and the responder, mutual authentication is possible.

Blom's Scheme

Blom's scheme [STIN, 95]is a key distribution scheme for network users. The scheme provides a means such that when the protocol is finally executed, the two parties involved in the communication over an insecure channel end up possessing a secret key. The secret key thereby delivered remains secret to the communicating pair and any intruder who might have monitored the entire communication is unable to obtain the key.

Once the key is successfully delivered, the parties involved can employ it along with a suitable encryption technology to communicate securely over an insecure channel. Since the key is not known to any third party, the communication remains hidden from prying eyes.

The general algorithm of Blom's scheme is as follows:

- A prime number p is made public. For each user a distinct element $r_U \in Z_p$, where Z_p is the finite field of characteristic p is also made public.

- A trusted third party chooses three random elements a, b and $c \in Z_p$ (not necessarily distinct), and forms the polynomial

  $f(x, y) = a + b(x+y) + c*x*y \mod p$

  where a, b and c are kept secret.

- For each user U, the trusted third party computes the polynomial $g_U(x) = f(x, r_U) \mod p$ and transmits $g_U(x)$ to U over a secure channel. Since $g_U(x)$ is a linear polynomial in x, it can be written as

  $g_U(x) = a_U + b_U * x$

  where $a_U = a + b * r_U \mod p$
  $b_U = b + c * r_U \mod p$

  When users U and V wish to communicate with each other, they compute a common secret key locally as

  $K_{U-V} = K_{V-U} = f(r_U, r_V)$

  $= a + b(r_U, r_V)+c * r_U * r_V \mod p$

  where user U computes K_{U-V} as
  $f(r_U, r_V) = g_U(r_V)$

  and user V computes K_{V-U} as
  $f(r_U, r_V) = g_V(r_U)$

  With a common key in their possession, users U and V can employ a suitable encryption algorithm to communicate securely thereafter.

Proposed Authentication Scheme for Low Cost Smart Cards

In this section we propose how Blom's scheme, which is basically a key distribution scheme for computer networks, can be adapted as a mutual authentication protocol to provide mutual authentication between a smart card and a terminal whenever a smart card is used for a transaction.

In the preceding section we saw that once the polynomial was distributed by a trusted third party to users U and V, Blom's scheme allowed users U and V to communicate securely whenever they wished over a computer network. All that the users U and V were required to do was to get the public element of the other party involved in the communication and locally compute the secret key. The secret key thus computed remained known only to the bona fide parties and was hidden from any third party, who might have seen all the messages.

In short, the general model of Blom's scheme involves two users wishing to communicate securely, some computing power at each user's end, and a trusted third party to compute and distribute the initial polynomial. Given the fact that a smart card also possesses considerable computing power, involves two parties (the card and the terminal) in a transaction, plus a service provider (who ultimately sets up the smart card / terminal infrastructure to provide a service), we feel that the model involving smart cards is also quite similar to that of Blom's scheme.

In the following paragraphs, we show how Blom's scheme, which is basically a network scheme can also be implemented in a smart card environment to provide security.

Initially, when a service provider decides to offer smart card based services to its clients, the service provider randomly chooses three values a, b and c from a finite field Z_p with p a prime number. These values remain constant and are kept highly secret through out. The service provider then computes the polynomial $f(x, y) = a + b(x+y) + c * x * y \mod p$, and puts this in an inaccessible area of all of its terminals. Here x and y are variables.

Whenever a new smart card is issued to a customer, the service provider places the same polynomial as placed in the terminals i.e. $f(x, y) = a + b(x+y) + c * x * y \mod p$. and burns this in an inaccessible memory area of the card. A customer's identification word I which can comprise of customer name, card chip number, card expiry date etc. is also burnt into the smart card. In short I, is used to represent the customer identification word in this paper.

Whenever a smart card is inserted into a terminal to access a service by a customer, mutual authentication (employing challenge-response technique) between the card and the terminal and hence secure transaction can be ensured as follows:

- The smart card generates a random number R_1 and sends it to the terminal.
- The terminal generates a random pair r_S and r_T locally and computes its key e.g. K_{T-S} as

  $K_{T-S} = f(r_S, r_T) = a + b(r_S+r_T) + c * r_S * r_T \mod p$.

  It then generates its own random number R_2 to use it as a challenge to authenticate the smart card. It encrypts R_1 with K_{T-S} and sends it to the smart card along with R_2, r_S and r_T.
- After receiving the message from step (2), the smart card locally computes its key e.g. K_{S-T} as

  $K_{S-T} = f(r_S, r_T) = a + b(r_S+r_T) + c * r_S * r_T \mod p$.

  It then decrypts the encrypted message using K_{S-T} and authenticates the terminal when it sees its R_1 back. It then encrypts the identification word I and R_2, with K_{S-T} and sends it to the terminal.

  The basis for the authentication is the fact that the card will be able to properly decrypt the encrypted R_1 only when $K_{S-T} = K_{T-S}$. The two keys will be equal only when the polynomial $f(x, y)$ residing in the card and the terminal is equal. Given the fact that the polynomials $f(x, y)$ is computed using secret components (the coefficients a, b and c, and the prime number p) which is known only to the service provider both the devices can be verified as genuine when $K_{S-T} = K_{T-S}$. The basis of the authentication becomes further strong considering the fact that these polynomials are kept in an inaccessible area of both the smart card and the terminal, and it never leaves the host.

  Considering a scenario, where either one of the party is fake. In that case the locally computed keys by the smart card and the terminal i.e. K_{S-T} and K_{T-S} will not be equal. Thus the party receiving a challenge will not be able to respond properly (by encrypting the challenge) and hence will not be authenticated by the other party.

These three steps are shown in figure 2.

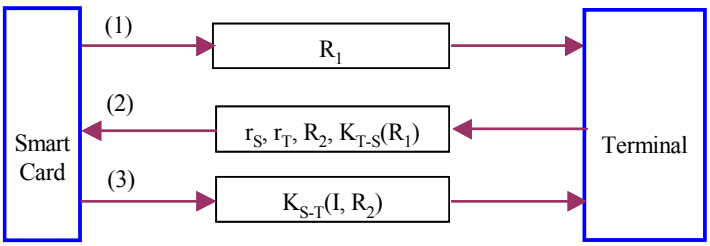

Figure 2. Mutual Authentication Between a Smart Card and a Terminal Based on Blom's Scheme

When the terminal receives the encrypted message it tries to decrypt it using its key K_{T-S}. As discussed above the terminal will be able to decrypt the message only when $K_{T-S} = K_{S-T}$. When it sees its R_2 back after decrypting the message, it authenticates the smart card.

The identification word I, can be used to further strengthen the security of the system by having the terminal to display the information on the screen for manual verification. However, the same is not required for the authentication.

Thus in this way mutual authentication, and hence secured transaction can be provided between a smart card and a terminal.

Merits of the Proposed System

Our proposal provides a framework whereby mutual authentication can be provided between genuine smart cards and terminals. The proposed protocol satisfies all concerns raised in section 2. By using the above protocol both fake smart cards and terminal can easily be singled out and hence the overall security of a card-based system can be significantly improved. Given the fact that a genuine smart card can isolate fake terminals and hence do not engage in a transaction at all with them can significantly help to promote a cardholder's confidence in using the card.

Given the limited resources that a smart card possesses, the above scheme is quite attractive. The above scheme is not computation as well as resource hungry as generally most of the public key cryptography algorithms often are. As far as computation requirement of the card is concerned, the card requires a simple addition and multiplications, which are not mathematically intensive. Given the current card configurations available, the proposed scheme can be easily implemented even in the lowest configuration of the cards available without much computational delay during a transaction. As such it is recommended that the above scheme can be handy in applications involving low cost cards, which have a bare microprocessor and where the nature of application demands some security but not that high.

Further, the overall security might be improved (we need to see) considering the fact that in the traditional approach, the card is required to carry both its key as well as the terminal's key [KONI, 91], where as in our scheme keys are calculated online during the transaction.

Conclusion

Smart cards will soon exist in virtually every area of our lives. Even though, its current use is mainly focussed on electronic money, however in the future, it will also control our access to a growing number of public facilities. Considering the sensitive nature of information that these cards will eventually carry, there is a strong need to protect these cards and hence the data inside the cards from misuse, be it from card theft or through a fake terminals. In this paper, we have proposed a mutual authentication protocol for smart cards based on Blom's scheme. The proposed scheme can be used to provide secure authentication between a low cost smart card and a smart card terminal, where the smart card will eventually be inserted to access a service. The scheme allows a mechanism to distinguish a genuine smart card from a fake one as well as a genuine terminal from a fake one.

References

[BOVE, 95] BOVELANDER.E and RENESSE.R.L.V, “Smartcards and Biometric: an Overview”, 12th Compsec Conference, UK, 1995.

[FUCH, 95] FUCHSBERGER.A, GOLLMANN.D, LOTHIAN.P, PATERSON.K.G and SIDROPOULOS.A, "Public-Key Cryptography on Smart Cards", In Proceedings of Cryptography: Policy and Algorithms, pp. 250-269, Brisbane, 1995.

[FORD, 94] FORD.W, "Computer Communications Security", PTR Prentice Hall, New Jersy, 1994.

[GARF, 97] GARFINKEL.S and SPAFFORD.G, “Web Security and Commerce”, O’reilly, Cambridge, 1997.

[HEND, 97] HENDRY.M, “Smart card Security and Applications”, Artech House, Boston, 1997.

[KONI, 91] KONIGS.H.P, “Cryptographic Identification Methods for Smart Cards in the Process of Standardization”, In IEEE Communications Magazine, 1991.

[LIND, 97] LINDLEY.R, “Smart card Innovation”, Saim Pty Ltd., Wollongong, 1997.

[LUCK, 97] LUCKS.S, "Open Key Exchange: How to Defeat Dictionary Attacks Without Encrypting Public Keys", In Proceedings of Security Protocols - 5th International workshop, pp. 79-90, Paris, 1997.
[OPPL, 96] OPPLIGER.R, “Authentication Systems for Secure Networks”, Artech House, Boston, 1996.
[PFLE, 89] PFLEEGER.C.P, “Security in Computing”, Prentice Hall, New Jersy, 1989.
[RANK, 97] RANKL.W and EFFING.W, “Smart Card Handbook”, Wiley, New York, 1997.
[SCHN, 96] SCHNEIER.B, “Applied Cryptography: Protocol, Algorithms and Source Code in C”, Wiley, New York, 1996.
[STIN, 95] STINSON.D.R, “Cryptography: Theory and Practice”, CRC Press, Florida, 1995.
[TANE, 96] TANENBAUM.A.S, “Computer Networks”, Prentice Hall, New Jersy, 1996.
[URL01] "Fraud, Smartcards, Biometrics", Internet WWW page at URL <http://www.gare.co.uk/smart.html>.
[URL02] "Smart Cards : The Latest in Finance Technology", Internet WWW page at URL <http://www.oberthurkirk.com/smartc.html>.