A PIN Management scheme based on the Needham's scheme

Jong-Hyeon Lee

University of Cambridge, Computer Laboratory
Pembroke Street, Cambridge CB2 3QG
jhl21@cl.cam.ac.uk

Abstract. In a recent meeting, RM Needham mentioned a Personal Identification Number (PIN) management scheme for bank's cash dispenser transactions, which provides enhanced privacy and responsibility separation. This scheme was described as a brief example that supports his idea on security research under the changing computing environment. In this memo, we suggest a practical PIN management scheme based on his scheme.
Indexing terms: authentication, access control, PIN.

Introduction: As an example, RM Needham suggested a Personal Identification Number (PIN) management scheme for Automated Teller Machine (ATM) transactions with enhanced privacy and responsibility separation [1]. The main difference of this scheme from currently used ones is generation and handling of the PIN code. Banks do not know customers' PINs and definitely they don't need to maintain PINs. In this scheme, the PIN code is generated by the customer for him/herself, and is not stored in the bank's database. From a bank's point of view, this scheme removes its responsibility for internal leakage of PINs and its maintenance complexity. Banks have a solid defense against an allegation that it negligently permitted the PIN to become known. For customers, they can obtain more privacy by generating their own PINs and by keeping them for themselves.

Analysis of Needham's scheme: Needham's scheme is described under the assumption that a customer has a PC and a card writer. At first, the customer writes on the card a random R and a hash $H(N, B)$ of his/her name N and birthdate B. He/she writes $H(N, B)$ and $H(R, PIN)$ on a floppy disk, where the PIN is chosen by him/herself. He/she then takes the floppy to the bank and says "Please connect $H(R, PIN)$ to my personal details $H(N, B)$ and my account number is 401608 80614874."

A cash machine accepts the card, reads the two quantities on it, works out $H(R, PIN)$ where PIN is the PIN as entered, and sends the two hashes to the center. Note that there is an assumption that the hash is good, the PIN is never sent to the center even in encrypted form. The center looks up $H(R, PIN)$

where in a substantial in-memory table. If it is found, the table yields the $H(N, B)$ for checking and also gives the account number.

In this scheme, there are two principals and one intermediate: a customer and a bank are principals and an ATM is an intermediate. A banking transaction is performed between the customer and the bank, but authentication procedures are done by the ATM and the bank. The ATM checks validity of owner of the card by PIN entered, the bank checks customer's information and account number by $H(R, PIN)$.

Needham assumed that the PIN is never sent to the center even in encrypted form. It requires the customer's trust on the ATM and its operator such as a bank. In this scheme, the role of ATM is more important than that of existing ATM. A false-terminal attack using a corrupted ATM is also available. Needham mentioned this attack and said that some kinds of smart card can be used to defend such an attack. Anyhow the mechanism to cope such a flaw is necessary.

A replay attack for the pair of hash values $H(N, B)$ and $H(R, PIN)$ is possible on the line between an ATM and the center. If an attacker takes the hash pair from the communication line, he/she can replay this pair on the same line and can be authorized as a valid customer by the center. The mechanism to avoid such an attack should be considered.

The hash $H(R, PIN)$ is used as a searching key in the bank's database, but it is possible to obtain multiple tuples with the same hash, because the random and PIN are generated by customers, not by a centralised body. Even though the probability of having another tuple with the same pair $\{H(N, B), H(R, PIN)\}$ is low, there is a possibility to find such collisions. We need a different searching key for the database.

The modified scheme: Our scheme is described in two procedures: the card generation procedure and the ATM transaction procedure. The card generation procedure is as follows: First, a customer gets a smart card and its serial number from the bank which contains a hash function and the signed serial number of the card. The signature of the bank on the card is encrypted serial number by bank's public key. It is used for the card verification. The customer generates random R and his/her PIN, he/she calculates $H(N, B)$, and writes $H(N, B)$ and R on the card. To avoid customer's illegal modification of data on the card, it should be allowed to write data on the card just once. He/she then sends an email to the bank with encrypted by the bank's public key. The mail says "Please connect $H(R, PIN)$ to my personal details $H(N, B)$ and the serial number of my card is 40160880614874". When an account for a customer is opened, the serial number of the customer's card is connected to the customer's information. After storing this pair $\{H(N, B), H(R, PIN)\}$, the bank sends an ac-

knowledgement to the customer.

The ATM transaction procedure is as follows: When a card is inserted to the ATM, the card requests the PIN to the customer, and calculates $H(R, PIN)$, where PIN is the PIN as entered. To avoid replay attacks, the bank sends a challenge C to the card. Then the card calculates the response $H(C \oplus H(R, PIN))$, and sends the triple $\{H(N, B), H(R, PIN), H(C \oplus H(R, PIN))\}$ to the ATM. The ATM relays this triple to the bank. The bank checks the response value and the signature, gets the serial number of the card from the signature, and checks the validity of the pair $\{H(N, B), H(R, PIN)\}$ by using the serial number.

When a customer cannot remember his/her PIN, he/she informs the bank of the fact, disposes his/her card for him/herself in the bank, receives another blank card from the bank, and follows above card generation procedure.

Conclusion: By using a smart card, we can separate role of the ATM in Needham's scheme, and the customer does not need to trust either the ATM or the bank. We can assume that no trust between principals is necessary. Due to the challenge-response step, the replay attacks are not available for the modified scheme.

Needham's scheme is a light-weight and efficient scheme with enhanced privacy. Furthermore, it provides duty separation between the customer and the bank. It reflects changing paradigm in the application of security protocols as described in his recent article [1].

References

1. R. M. Needham. The changing environment for security protocols. *IEEE Network*, pages 12–15, May/June 1997.