Practical Proven Secure Authentication with Arbitration

Yvo Desmedt[1]* ** and Jennifer Seberry[2]*** †

[1] EE & CS Department, University of Wisconsin–Milwaukee, WI 53201, U.S.A.
[2] Department of Computer Science, The University of Wollongong Wollongong, NSW, 2522, Australia

Abstract. Proven secure signature schemes and unconditionally secure authentication schemes with arbiter have been proposed. The former are not practical (too slow) and the latter cannot be reused. All these limitations are solved in this paper by presenting a resuable conditionally secure authentication scheme with arbiter. The scheme is unconditionally secure against denial by the sender of having sent a message (which signatures do *not* have) and conditionally secure against a receiver impersonating the sender or substituting a message and conditionally secure against a similar fraud by the arbiter.

1 Introduction

One can make a proven secure signature scheme [9, 11] based on any one way function. Unfortunately all proven secure signature schemes [7, 9, 1, 11, 2] are very impractical (to make some of them more practical the authentication tree could be used instead of pseudo random functions but this approach requires a lot of memory). So from a practical viewpoint it could be advantageous to use symmetric authentication schemes, however one then loses the signature property. In the classical notion of arbiter [8, p. 409] the arbiter has to be active when messages are transmitted.

Simmons [14] introduced unconditionally secure authentication schemes with arbitration. From a functional viewpoint the arbiter is not active, in Simmons'

* Part of this work was done while he was visiting professor at University of New South Wales, Department of Computer Science, ADFA, Australia, part while he was visiting the Center for Communication and Information Science, University of Nebraska–Lincoln and part while visiting the Department of Computer Science at the University of Wollongong, Australia.

** A part of this work has been supported by NSF Grant NCR-9106327 and Telecom Project 7027, Australia, 1991.

*** Written while on faculty of the Department of Electrical Engineering and the Department of Computer Science and Engineering, and Head of the Center for Communication and Information Science, University of Nebraska–Lincoln, NE 68588, USA.

† Research funded by Telecom grant 7027, ARC grant A49130102 and an ATERB grant.

scheme, during the transmission of the authenticated message while in the classical notion the arbiter must be active. Desmedt and Yung [6] (see also Brickell and Stinson [4]) improved Simmons' scheme by protecting the receiver against an impersonation (substitution) attack by the arbiter. Unfortunately all these schemes can only be used once (because otherwise they lose their security) and hence new keys have to be distributed for each new message as in a one time pad.

The purpose of this paper is to develop a practical proven secure conditional authentication scheme with arbitration. Our scheme has some similarities with [10], however our scheme is non-interactive and the keys can be re-used.

2 Definitions

Let us call S the sender, R the receiver, A the arbiter, and O the outside opponent. We can distinguish three stages in Simmons' solution [14]. The three stages are:

The key initialization phase in which S, R and A interact to come up with the necessary keys.

The authentication phase in which R receives a message and wants to ascertain that the message is authentic. A does *not* interact in this stage.

The dispute phase in which A is requested to resolve a dispute between S and R. Using some information gathered by A during the initialization phase A solves the dispute.

Our scheme contains these three stages as well.

Let us describe more precisely the threats with which we are faced. We follow closely Simmons's description of such threats (for the first three threats see [14]).

The outside opponent. The outsider, O, can try to impersonate the sender and/or substitute some message(s) for one sent from S to R, but which O has intercepted (actively eavesdropped).
The attack is said to be successful if and only if R accepts the message as authentic when it is not.

The sender. A dishonest $\tilde{S}$ can attempt to cheat by sending a message which R will accept as authentic, but which he can later deny having sent.
The attack is successful if and only if the following two conditions hold. First, R accepts the fraudulent message, and second, in a dispute A will decide that the message is *not* authentic.

The receiver. A dishonest $\tilde{R}$ can falsely claim to have received the message M from S. Two subcases can be distinguished: $\tilde{R}$ never received a message at all, or $\tilde{R}$ has received some authentic message(s) from S which he tries to alter.
The attack is successful if and only if in a dispute A certifies the message as being authentic.

The arbiter. A dishonest $\tilde{A}$ can send a message to R which R will accept as authentic. As in the case of the opponent's attack the arbiter can either choose an impersonation or a substitution attack.
The attack is successful if and only if the message originating at $\tilde{A}$ will be accepted by R.

We remark that it is not A's task *to force* R to accept messages originating from S.

The reader who is interested in formalizing the above informal definitions is referred to [6]. Although these definitions have been given for unconditionally secure schemes, they can very easily be adapted for conditionally secure ones.

3 The Scheme

We use S for the sender, R for the receiver and A for the arbiter. We assume the existence of a conditionally proven secure authentication scheme. When we mention keys we assume that these (symmetric) keys were chosen according to a prescribed algorithm and belong to the set K.

3.1 Distribution Phase

Step 1 A sends S an ordered tuple $(k_1, k_2, \ldots, k_n)$ of random, independently chosen, keys privately.

Step 2 A chooses with uniform probability distribution a random subset, I, of $\lfloor n/2 \rfloor$ indices between 1 and n and privately sends to R the tuple $(k'_1, k'_2, \ldots, k'_n)$ where $k'_i = k_i$ if $i \in I$, otherwise $k'_i = \epsilon$, where $\epsilon \notin K$, (for example ϵ may be the empty string).

Step 3 S privately sends a key, k_{n+1}, to R.

3.2 Authentication Phase

To send a message M the sender S forms $n+1$ message authentication codes (MACs) by processing the message with each of the $n+1$ keys, n provided by the arbiter and one by himself, using a proven secure authentication scheme. Call these MACs $MAC_1, MAC_2, \ldots, MAC_{n+1}$. The sender sends $(M, MAC_1, MAC_2, \ldots, MAC_{n+1})$ where MAC_i is generated using the key k_i, the message M and the agreed authentication algorithm to R.

To verify whether R should accept M as (probably) being authentic R proceeds as follows: if $k'_i \neq \epsilon$ then R checks that MAC_i is correct, and does this for all i, $1 \leq i \leq n$, and additionally checks if MAC_{n+1} also matches. If these $\lfloor n/2 \rfloor + 1$ MACs are correct R accepts M as authentic, otherwise R rejects. In the case R rejects R erases his keys and requests new keys unless all the MACs were wrong.

3.3 Dispute Phase

If a dispute occurs the receiver presents $(M, MAC_1, MAC_2, \ldots, MAC_n)$ to the arbiter. The arbiter will accept the message plus the MACs as correct if among $(M, MAC_1, MAC_2, \ldots, MAC_n)$ all those MACs that R should have known were correct are indeed correct plus at least one more MAC is correct.

4 Proof of Security

We will use h as a security parameter so that the complexity of performing an attack on the underlying authentication scheme is bounded above by $1/p(h)$ where p is any polynomial. We assume S receives feedback from R whether he has accepted the message M or not.

Theorem 1. *Let n in our scheme be chosen linear in h the security parameter. Now if a conditionally proven secure authentication scheme exists then our scheme is secure against a denial attack by the sender, conditionally secure against an attack in which the receiver, the arbiter or an outsider attempts to modify the message or impersonate the sender.*

Proof. The receiver's attack will not succeed as he does not know enough keys and the authentication scheme was assumed to be secure. A similar proof holds for the arbiter's and an outsider's attacks. We now consider denial by the sender. We do not consider MAC_{n+1} as this was used only to protect against the arbiter.

If the sender wishes to have a false message accepted and then deny sending the message he optimizes his chance of winning by adopting a game plan. He wants *R to accept* and *A to reject*. Now if S has sent i $\{i : 0, \ldots, \lfloor (n-2)/2 \rfloor\}$ correct MACs and $n-i$ incorrect MACs then R will reject the message and so *S loses*. If S sends i $\{i : \lfloor (n+2)/2 \rfloor, \ldots, n\}$ correct MACs and $n-i$ incorrect MACs then if R accepts the message as genuine then so will A and again *S loses*. If S sends $\lfloor n/2 \rfloor$ correct MACs and $n - \lfloor n/2 \rfloor$ incorrect MACs, then S can *win* if he has chosen exactly the $\lfloor n/2 \rfloor$ MACs that R has, R will accept but the arbiter will reject. There are exactly

$$\binom{n}{\lfloor n/2 \rfloor}$$

ways of choosing subsets of the indices of the MACs with $\lfloor n/2 \rfloor$ elements .

Our assumption that S receives feedback from R whether a message M was accepted or not implies S can *win next time* if he guesses all the indices of the keys, $k'_j = \epsilon$, and sends the MAC_js of these $n - \lfloor n/2 \rfloor$ keys correctly and all other MACs incorrectly. In this case R will reject the message but not erase his keys (so R will not ask for new keys). The probability of this succeeding without detection is also

$$\frac{1}{\binom{n}{\lfloor n/2 \rfloor}} .$$

So the probability is negligible of an attack succeeding (even if repeated[3] polynomially many times). □

5 Conclusions

We have presented an authentication scheme with arbiter which is unconditionally secure against denial by the sender of having sent a message and conditionally secure against a receiver impersonating the sender or substituting a message and conditionally secure against a similar fraud by the arbiter.

The security obtained is the same as for the symmetric authentication scheme on which it is based. We observe that making practical proven secure authentication schemes is easy to achieve starting from pseudo-noise generators [12, 13] and unconditionally secure authentication schemes [5].

It is clear that the scheme presented in Section 3, can be adapted for DES. We remind the reader that DES is not a proven secure scheme and that some weaknesses have been found in the protocol for generating MACs [3].

Acknowledgement

The authors thank Bart Preneel of the University of Louvain, Belgium for bringing [10] to their attention.

References

1. Bellare, M., Goldwasser, S.: New paradigms for digital signatures and message authentication based on non-interactive zero-knowledge proofs. In Advances in Cryptology — Crypto '89, Proceedings (Lecture Notes in Computer Science 435) (1990) G. Brassard, Ed. Springer-Verlag pp. 194–211
2. Bellare, M., Micali, S.: How to sign given any trapdoor function. Journal of the ACM **39** (1992) 214–233
3. Bird, R., Gopal, I., A.Herzberg, Jansen, P., Kutten, S., Molva, R., Yung, M.: Systematic design of two-party authentication protocols. In Advances in Cryptology — Crypto '91, Proceedings (Lecture Notes in Computer Science 576) (1992) J. Feigenbaum, Ed. Springer-Verlag pp. 44–61

[3] For the first type of attack, if the sender successfully modified i_1 MACs the first time, i_2 different MACs the second time and so on. Then observing

$$\frac{\binom{n-\lfloor n/2\rfloor}{i_1}}{\binom{n}{i_1}} \cdot \frac{\binom{n-\lfloor n/2\rfloor-i_1}{i_2}}{\binom{n-i_1}{i_2}} = \frac{\binom{n-\lfloor n/2\rfloor}{i_1+i_2}}{\binom{n}{i_1+i_2}}$$

the numerate reader can show that the probability of successful attack remains the same as above. The same can be said for the second type of attack or a combination of both types.

4. Brickell, E. F., Stinson, D. R.: Authentication codes with multiple arbiters. In Advances in Cryptology, Proc. of Eurocrypt '88 (Lecture Notes in Computer Science 330) (May 1988) C. G. Günther, Ed. Springer-Verlag pp. 51–55
5. den Boer, B.: A simple and key-economical authentication scheme, March 30–April 3, 1992. Presented at System Security, Dagstuhl, Germany
6. Desmedt, Y., Yung, M.: Arbitrated unconditionally secure authentication can be unconditionally protected against arbiter's attacks. In Advances in Cryptology — Crypto '90, Proceedings (Lecture Notes in Computer Science 537) (1991) A. J. Menezes and S. A. Vanstone, Eds. Springer-Verlag pp. 177–188
7. Goldwasser, S., Micali, S., Rivest, R.: A digital signature scheme secure against adaptive chosen-message attacks. Siam J. Comput. **17** (1988) 281–308
8. Meyer, C. H., Matyas, S. M.: Cryptography: A New Dimension in Computer Data Security. J. Wiley New York 1982
9. Naor, M., Yung, M.: Universal one-way hash functions and their cryptographic applications.. In Proceedings of the twenty first annual ACM Symp. Theory of Computing, STOC (May 15–17, 1989) pp. 33–43
10. Rabin, M. O.: Digitized signatures. In Foundations of Secure Computation (New York, 1978) R. A. DeMillo, D. P. Dobkin, A. K. Jones, and R. J. Lipton, Eds. Academic Press pp. 155–168
11. Rompel, J.: One-way functions are necessary and sufficient for secure signatures. In Proceedings of the twenty second annual ACM Symp. Theory of Computing, STOC (May 14–16, 1990) pp. 387–394
12. Rueppel, R. A.: Stream ciphers. In Contemporary Cryptology, G. J. Simmons, Ed. IEEE Press 1992 pp. 65–134
13. Schrift, A. W., Shamir, A.: The discrete log is very discreet. In Proceedings of the twenty second annual ACM Symp. Theory of Computing, STOC (May 14–16, 1990) pp. 405–415
14. Simmons, G. J.: A Cartesian product construction for unconditionally secure authentication codes that permit arbitration. Journal of Cryptology **2** (1990) 77–104