Authentication Codes with Multiple Arbiters

(Extended Abstract)

Ernest F. Brickell*
Sandia National Laboratories
Albuquerque, NM 87185

Doug R. Stinson**
Dept. of Computer Science
University of Manitoba
Winnipeg, Manitoba
Canada R3T 2N2

An authentication system provides a means for a transmitter to send a message to a receiver so that the receiver is convinced that the message was sent by the transmitter and not by an opponent. Authentication codes provide a design for authentication systems which are unconditionally secure. Specifically, the codes provide a provable level of security which depends on the parameters of the code but which does not depend on any assumptions (for instance assumptions about the computational complexity of some problem).

In 1987, Simmons [Si1] introduced authentication codes that permit arbitration. These codes allow for an arbiter who can settle disputes between the transmitter and receiver. The disputes that an arbiter can resolve are that the receiver might claim to have received a certain message when in fact he didn't, or the transmitter might try to disavow a message that he actually sent. The arbiter cannot resolve a dispute in which the transmitter claims to have sent a message and the receiver claims that he did not receive a message. These systems are also unconditionally secure. One drawback to the system is that the transmitter and receiver must have complete trust in the arbiter, because an arbiter has the potential to cheat in many ways.

In this paper, we show that by having multiple arbiters, the probability that any individual arbiter can successfully cheat is greatly reduced.

The Model

We will be using the same terminology and the same model of authentication with arbitration that was used by Simmons [Si1], [Si2]. The system that will be used must be known to all players, i.e., transmitter, receiver, opponent, and arbiter. This includes a fixed set of source states that the transmitter might send to the receiver. The receiver

* This work performed in part at Sandia National Laboratories supported by the U. S. Department of Energy under contract No. DE-AC04-76DP00789.

** This work partially supported by NSERC operating grant No. A9287.

and arbiter secretly agree on which messages the receiver will accept as authentic for each source state. Then the arbiter gives the transmitter one message for each source state that the receiver will accept as authentic. The arbiter will no longer be used unless there is a dispute.

There are five types of cheating that this system is designed to protect against.

Opponent cheating:

- O_0 Impersonation: Without waiting to see any communication, the opponent sends a message to the receiver. He wins if it is accepted as authentic.
- O_1 Substitution: The opponent intercepts a message and substitutes a different message. He wins if his message is accepted as authentic and the receiver is misled about the state of the source.

Receiver cheating:

- R_0 The receiver, without receiving any message from the transmitter, tries to convince the arbiter that he did receive a message.
- R_1 The receiver, after receiving a message from the transmitter, tries to convince the arbiter that he received a different message.

Transmitter cheating:

- T The transmitter, after sending a message to the receiver that the receiver authenticated, tries to deny that he sent a message.

The model does not attempt to protect against all types of cheating. For example, the transmitter could claim that he sent a message that he did not send or the opponent could disrupt communications between the transmitter and receiver. For cheating of type X, let P_X be the probability that the cheating will be successful. Let $P_R = \max(P_{R_0}, P_{R_1})$ and $P_O = \max(P_{O_0}, P_{O_1})$.

The problem presented here cannot be directly solved by the general multi-party protocols of [CCD] and [BGW] because in those protocols, it is necessary for all parties in the protocol (transmitter, receiver, and arbiters) to play an active part in any communication.

Multiple Arbiters

Simmons showed how to construct authentication with arbitration codes, which he called A^2 codes, for any q a prime power such that the probability of successful cheating is $\frac{1}{q}$ for each of the five types of cheating. He expressed concern, however, that these systems required complete trust in the arbiter. A cheating arbiter could assist the opponent, receiver, or transmitter and cheat in any of the five types. We now show that by having multiple arbiters, the power of any individual arbiter to cheat is greatly reduced.

Suppose we have arbiters $A_1, \dots, A_n$ and for each arbiter, we have an authentication with arbitration code with the probability of deception of $\frac{1}{q}$ for each of the five types of cheating. Each of the communications between the receiver and an arbiter or the transmitter and an arbiter will be in secret from all of the other arbiters. These communications will be handled in the same way as in the single arbiter case. So for each arbiter, A_i , and each source state, s_j , the receiver will give the arbiter A_i a set of messages, M_{ij} , that he will accept as authentic and the arbiter A_i will give the transmitter a single message, $m_{ij} \in M_{ij}$, that the arbiter A_i will validate as an authentic transmission of s_j . When the transmitter wants to send a source state, s_j , to the receiver, he must send m_{ij} for $1 \leq i \leq n$. The receiver will only accept such a communication as authentic if and only if $m_{ij} \in M_{ij}$ for $1 \leq i \leq n$. If a dispute arises, a judge will accept a communication $p_1, \dots, p_n$ as an authentic transmission of source state s_j if and only if at least d of the arbiters claim the communication is authentic, i.e., for at least d of the i 's, $1 \leq i \leq n$, arbiter A_i claims that $p_i = m_{ij}$.

Let us now examine the probabilities of cheating given that t arbiters are bad. To simplify the discussion, assume that $A_1, \dots, A_t$ are bad. An opponent can collude with the t bad arbiters and learn M_{ij} for $1 \leq i \leq t$. To deceive the receiver, he must cheat successfully on each of other $n-t$ A^2 codes. Since these are independent, his probability of success is $\left(\frac{1}{q}\right)^{n-t}$. Thus $P_{0_0} = P_{0_1} = \left(\frac{1}{q}\right)^{n-t}$.

The receiver can collude with the t bad arbiters and learn m_{ij} for $1 \leq i \leq t$. To deceive the judge, he must cheat successfully on at least $d-t$ of the other $n-t$ A^2 codes. His probability of success is

$$P_{R_0} - P_{R_1} = \sum_{i=d-t}^{n-t} \binom{n-t}{i} \left(\frac{1}{q}\right)^i \left(\frac{q-1}{q}\right)^{n-t-i}.$$

$\left[\binom{n-t}{i} \left(\frac{1}{q}\right)^i \left(\frac{q-1}{q}\right)^{n-t-i}\right]$ is the probability of cheating successfully on exactly i of the independent $n-t$ A^2 codes.]

Assuming that the transmitter knows M_{ij} for $1 \leq i \leq t$, his best strategy for success at deceit of type T is to send $m'_{ij} \in M_{ij}/m_{ij}$ for $1 \leq i \leq t$, m_{ij} for $t+1 \leq i \leq d+t-1$, and then try to cheat successfully on the $n-(d+t-1)$ remaining A^2 codes. So $P_T = \left(\frac{1}{q}\right)^{n-d-t+1}$.

To achieve $P_R < 1$ and $P_T < 1$, we must have $t < \frac{n}{2}$. If $t = \left\lfloor \frac{n-1}{2} \right\rfloor$, and if $d = \left\lceil \frac{n+1}{2} \right\rceil$, then for fixed n , q can be chosen large enough to satisfy any desired level of confidence. For example, if $n = 2t+1$ and setting $d = t+1$ we obtain $P_T = \frac{1}{q}$ and $P_R = 1 - \left(1 - \frac{1}{q}\right)^{t+1}$.

Additional Comments

A bad arbiter could completely disrupt the communication by sending the transmitter an m_{ij} with $m_{ij} \notin M_{ij}$. It is possible to protect against a few arbiters doing this by allowing the receiver to accept a communication if it is authentic in "most" of the A^2 codes. However, this reduces the security against the opponent.

To be more precise, assume that the receiver will accept a communication $p_1, \dots, p_n$ as transmitting source state s_j if $p_i \in M_{ij}$ for at least α of the i 's, $1 \leq i \leq n$, and that a judge will accept it as authentic if at least d of the arbiters claim it is authentic. Assume that at most u arbiters will try to disrupt the communication and at most t arbiters will try to help one of the other participants to cheat. This model allows for the possibility that a particular arbiter might try to disrupt the communication but might not help any participant to cheat.

The transmitter and receiver can successfully cheat only when the judge is deceived. When computing P_{R_0} , P_{R_1} , and P_T , we will assume that no arbiters are disrupting (i.e., $u=0$) since this assumption provides the worst case (i.e., maximizes) P_{R_0} , P_{R_1} , and P_T . Since the criterion for the judge's decision is unchanged from the previous model, P_{R_0} , P_{R_1} , and P_T are also unchanged.

To compute P_0 , assume that the opponent knows M_{ij} for $1 \leq i \leq t$. To deceive the transmitter, he must successfully cheat on at least $\alpha \cdot t$ of the other $n-t$ independent A^2 codes. His probability of success is

$$P_0 = \sum_{i=\alpha \cdot t}^{n-t} \binom{n-t}{i} \left(\frac{1}{q}\right)^i \left(\frac{q-1}{q}\right)^{n-t-i}.$$

Finally, the u arbitors can disrupt the communication if and only if $u > n-\alpha$ or $u \geq \alpha$. In the case $\frac{n}{2} \geq u \geq \alpha$, the bad arbitors could deceive the transmitter into sending a message that, according to protocol, the receiver would accept as transmitting two different source states.

To achieve $u \leq n-\alpha$ and $u < \alpha$, we must have $u < \frac{n}{2}$. If $u = t = \left\lfloor \frac{n-1}{2} \right\rfloor$, and if $d = \alpha = \left\lceil \frac{n+1}{2} \right\rceil$, then for fixed n , q can be chosen large enough to satisfy any desired level of confidence.

References

- [BGW] Michael Ben-Or, Shafi Goldwasser and Avi Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation," to appear in Proceedings of the 20th ACM Symposium on the Theory of Computing, 1988.
- [CCD] David Chaum, Claude Crepeau and Ivan Damgard "Multiparty Unconditionally Secure Protocols," to appear in Proceedings of the 20th ACM Symposium on the Theory of Computing, 1988.
- [Si1] G. J. Simmons, "Message Authentication with Arbitration of Transmitter/Receiver Disputes," to appear in Advances in Cryptology, Eurocrypt'87, Springer-Verlag, 1987.
- [Si2] G. J. Simmons, "A Cartesian Product Construction for Unconditionally Secure Authentication Codes that Permit Arbitration," submitted to Journal of Cryptology.