LUND UNIVERSITY

Lower bounds on the probability of deception in authentication

Johansson, Thomas

Published in:
[Host publication title missing]

1993

Link to publication

Citation for published version (APA):
Johansson, T. (1993). Lower bounds on the probability of deception in authentication. In *[Host publication title missing]* (pp. 231) http://ieeexplore.ieee.org/iel4/5602/14996/00748545.pdf

Total number of authors:
1

General rights
Unless other specific re-use rights are stated the following general rights apply:
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.
• Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
• You may not further distribute the material or use it for any profit-making activity or commercial gain
• You may freely distribute the URL identifying the publication in the public portal

Read more about Creative commons licenses: https://creativecommons.org/licenses/

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

LUND UNIVERSITY

PO Box 117
221 00 Lund
+46 46-222 00 00

LOWER BOUNDS ON THE PROBABILITY OF DECEPTION IN AUTHENTICATION WITH ARBITRATION

Thomas Johansson
Department of Information Theory
Lund University, Box 118
S-221 00 Lund, Sweden

Abstract — Lower bounds on the probability of success for the different kinds of attacks in authentication with arbitration are derived. These bounds give rise to combinatorial lower bounds on the number of encoding rules and on the number of messages necessary in an authentication code with arbitration.

Summary — In the model for normal authentication the transmitter and the receiver are using the same encoding rule and are thus trusting each other. However, it is not always the case that the two communicating parties want to trust each other. Inspired by this problem Simmons has introduced an extended authentication model, here referred to as the authentication model with arbitration, [1]. In this model caution is taken against deception from both outsiders (opponent) and insiders (transmitter and receiver). The model includes a fourth person, called the arbiter. The arbiter has access to all key information and is by definition not cheating. The arbiter does not take part in any communication activities on the channel but has to solve disputes between the transmitter and the receiver whenever such occur.

There are essentially five different kinds of attacks to cheat which are possible. The attacks are the following:
I, Impersonation by the opponent. The opponent sends a message to the receiver and succeeds if the message is accepted by the receiver as authentic.
S, Substitution by the opponent. The opponent observes a message that is transmitted and substitutes this message with another. The opponent succeeds if this other message is accepted by the receiver as authentic.
T, Impersonation by the transmitter. The transmitter sends a message to the receiver and denies having sent it. The transmitter succeeds if the message is accepted by the receiver as authentic and if the message is not one of the messages that the transmitter could have generated due to his encoding rule.
$\mathbf{R_0}$, Impersonation by the receiver. The receiver claims to have received a message from the transmitter. The receiver succeeds if the message could have been generated by the transmitter due to his encoding rule.
$\mathbf{R_1}$, Substitution by the receiver. The receiver receives a message from the transmitter but claims to have received another message. The receiver succeeds if this other message could have been generated by the transmitter due to his encoding rule.
In all these possible attacks to cheat it is understood that the cheating person is using an optimal strategy when choosing a message. For each way of cheating, we denote the probability of success with P_I, P_S, P_T, P_{R_0} and P_{R_1}. The overall probability of deception is denoted P_D and is defined to be $P_D = \max(P_I, P_S, P_T, P_{R_0}, P_{R_1})$.

For unconditionally secure authentication codes we derive the following lower bounds on the probability of success for the different kinds of deceptions:

$$P_I \geq 2^{-I(E_R;E_T)+I(E_R;E_T|M)}$$
$$P_S \geq 2^{-I(E_R;E_T|M)}$$
$$P_T \geq 2^{-H(E_R|E_T)}$$
$$P_{R_0} \geq 2^{-I(E_T;M|E_R)}$$
$$P_{R_1} \geq 2^{-H(E_T|M,E_R)}$$

Here E_R is the receiver's encoding rule and E_T is the transmitter's encoding rule. The bounds are valid for all authentication codes with $|S| > 1$ except for a class of degenerate codes which all have $P_{R_0} = 1$ and hence not very interesting.

From the above bounds we also derive lower bounds on the number of encoding rules and on the number of messages to be used in an authentication code with arbitration. Assume that the number of source states for a symmetric source is $|\mathcal{S}|$ and let $P_D = 1/q$ for an authentication code with arbitration. Let $\mathcal{E}_\mathcal{R} \circ \mathcal{E}_\mathcal{T}$ denote the set of possible pairs (E_R, E_T). Then the following lower bounds are valid on the number of encoding rules and on the number of messages that are necessary in the code,

$$|\mathcal{E}_\mathcal{R}| \geq q^3$$
$$|\mathcal{E}_\mathcal{T}| \geq q^4$$
$$|\mathcal{E}_\mathcal{R} \circ \mathcal{E}_\mathcal{T}| \geq q^5$$
$$|\mathcal{M}| \geq q^2|\mathcal{S}|.$$

Using these combinatorial lower bounds it is for example possible to show that the cartesian product construction for authentication codes with arbitration does not meet all lower bounds with equality, [1].

References

[1] G. Simmons, "A Cartesian Product Construction for Unconditionally Secure Authentication Codes that Permit Arbitration", *Journal of Cryptology*, Vol. 2, no 2, 1990, pp. 77-104.

This work was supported by the TFR grant 222 92-662