J. Cryptology (1999) 12: 155–159

Journal of
CRYPTOLOGY

On a Fallacious Bound for Authentication Codes*

Carlo Blundo and Alfredo De Santis
Dipartimento di Informatica ed Applicazioni,
Università di Salerno, 84081 Baronissi (SA), Italy
{carblu,ads}@dia.unisa.it
http://www.unisa.it/{∼carblu/,∼ads/}

Kaoru Kurosawa
Department of Electrical and Electronic Engineering,
Faculty of Engineering, Tokyo Institute of Technology,
2-12-1 O-okayama, Meguro-ku, Tokyo 152, Japan
kurosawa@ss.titech.ac.jp
http://tsk-www.ss.titech.ac.jp/∼kurosawa

Wakaha Ogata
Department of Computer Engineering,
Faculty of Engineering, Himeji Institute of Technology,
2167 Shosha, Himeji, Hyogo 671-22, Japan
wakaha@comp.eng.himeji-tech.ac.jp

Communicated by James L. Massey

Received 13 March 1996 and revised 21 May 1997

Abstract. We show that the lower bound on substitution success probability P_S provided by Theorem 3.8 in De Soete's paper [4], which appeared earlier in this journal, is not correct by exhibiting a counterexample. We identify the flaw in the "proof" of this theorem and we prove a valid lower bound on P_S.

Key words. Authentication codes, Substitution, Spoofing attack.

1. Introduction

An authentication code permits the communication of some information over an insecure channel, from a transmitter to a receiver. An opponent, who has access to the insecure channel, tries to deceive the receiver by getting him to accept either a message inserted by the opponent himself (*impersonation*) or a message different from the legitimate one sent by the transmitter but intercepted by the opponent (*substitution*). For an up-to-date bibliography on authentication codes, the reader is referred to [6].

* The research of C. Blundo and A. De Santis was partially supported by the Italian Ministry of University and Research (M.U.R.S.T.) and by the National Council for Research (C.N.R.).

In authentication codes, a quantity of particular interest is P_s, the probability of successfully deceiving the receiver by using an optimum substitution attack. De Soete [4] proposed a combinatorial bound on P_s. In this paper we show by exhibiting a counterexample that the lower bound on P_s provided by Theorem 3.8 in [4] is not correct. We identify the flaw in the proof of this theorem and we prove a valid lower bound on P_s.

2. Authentication Codes with Splitting

Consider the following scenario with three parties, a *transmitter* T, a *receiver* R, and an *opponent* O. The transmitter wants to communicate some information s, called the *source state*, to the receiver. He does this by sending a *message* m over an insecure channel to which the opponent has access. The message $m \in \mathcal{M}$ is a function of $s \in \mathcal{S}$ and of the encoding rule $e \in \mathcal{E}$, where the particular e is known to the transmitter T and receiver R but not to the opponent O. The opponent O tries to deceive the receiver R by getting R to accept either a message inserted by O (*impersonation*) or a message different from the legitimate one sent by T but intercepted by O (*substitution*). An authentication code is a code intended to thwart such deception.

When more than one message can be used to communicate a source state s under the same encoding rule e, the authentication code is said to have *splitting*. We denote by $e(s)$ the set of possible messages encoding a source state $s \in \mathcal{S}$ under the encoding rule $e \in \mathcal{E}$. With splitting, there exists an $e \in \mathcal{E}$ and an $s \in \mathcal{S}$ such that $|e(s)| > 1$. In an authentication code with splitting, one requires that $e(s) \cap e(s') = \emptyset$ for every $e \in \mathcal{E}$ and $s, s' \in \mathcal{S}$ such that $s \neq s'$.

Definition 2.1. An *authentication code with splitting* is a triple $(\mathcal{S}, \mathcal{M}, \mathcal{E})$, together with probability distributions $\{p_{\mathcal{S}}(s)\}_{s\in\mathcal{S}}$, $\{p_{\mathcal{E}}(e)\}_{e\in\mathcal{E}}$, and $\{\{p(m|e,s)\}_{m\in\mathcal{M}} : e \in \mathcal{E} \text{ and } s \in \mathcal{S}\}$, such that:

1. $\mathcal{S}$ is a finite set of k *source states*.
2. $\mathcal{M}$ is a finite set of v *messages*.
3. $\mathcal{E}$ is a finite set of b *encoding rules* associating to a source state $s \in \mathcal{S}$ one or more messages in $\mathcal{M}$. That is, any $e \in \mathcal{E}$ is such that e: $\mathcal{S} \to 2^{\mathcal{M}}$.

We describe the family of encoding rules of an authentication code by a $b \times k$ matrix having entries in $2^{\mathcal{M}}$. The rows of the matrix are indexed by the elements of $\mathcal{E}$, the columns are indexed by the elements of $\mathcal{S}$, and the entry (e, s) of the matrix is the set $e(s)$.

Let P_s denote the probability of successfully deceiving the receiver by using an optimum substitution attack. Suppose that the transmitter sends the message m to the receiver and that the opponent replaces it with $m' \neq m$. As in [4], we denote the probability that the message m' is accepted by the receiver as authentic by payoff(m, m'), i.e.,

$$\text{payoff}(m, m') = \frac{\sum_{\substack{e\in E(m,m') \\ f_e(m)\neq f_e(m')}} p_{\mathcal{E}}(e) \cdot p_{\mathcal{S}}(f_e(m)) \cdot p_{\mathcal{M}|\mathcal{E}\mathcal{S}}(m|e, f_e(m))}{\sum_{e\in E(m)} p_{\mathcal{E}}(e) \cdot p_{\mathcal{S}}(f_e(m)) \cdot p_{\mathcal{M}|\mathcal{E}\mathcal{S}}(m|e, f_e(m))}, \qquad (1)$$

where $f_e(m)$ denotes the source state s corresponding to the message m under encoding

Table 1. Encoding rules for the authentication code $\mathcal{A}$.

$\mathcal{E}\backslash\mathcal{S}$	0	1
0	{0, 1}	{2, 3}
1	{0, 2}	{1, 4}
2	{1, 3}	{0, 4}
3	{2, 4}	{0, 3}
4	{3, 4}	{1, 2}

rule e. Let $P_s(m)$ denote the maximum probability of successfully deceiving R once the message m has been replaced, i.e., $P_s(m) \stackrel{\Delta}{=} \max\{\text{payoff}(m, m') : m' \neq m\}$. Then

$$P_s \stackrel{\Delta}{=} \sum_{m\in\mathcal{M}} p_{\mathcal{M}}(m) \cdot P_s(m).$$

De Soete (Theorem 3.8 in [4]) claimed that, for any authentication code with splitting,

$$P_s \geq \min_{e\in\mathcal{E}} \frac{\kappa(e) - \max_{s\in\mathcal{S}}|e(s)|}{v - \min_{s\in\mathcal{S}}|e(s)|}, \tag{2}$$

where $\kappa(e)$ is the total number of distinct messages m that can result from the encoding rule e.

The following counterexample shows that the bound (2) does not always hold. Consider the authentication code with splitting, $\mathcal{A}$, whose encoding rules are depicted in Table 1, where $\mathcal{S} = \{0, 1\}$, $\mathcal{E} = \{0, 1, 2, 3, 4\}$, and $\mathcal{M} = \{0, 1, 2, 3, 4\}$. Assume, for all $s \in \mathcal{S}$, $e \in \mathcal{E}$, and $m \in \mathcal{M}$, that $p_{\mathcal{S}}(s) = \frac{1}{2}$, that $p_{\mathcal{E}}(e) = \frac{1}{5}$, and that $p_{\mathcal{M}|\mathcal{E}\mathcal{S}}(m|e, s) = \frac{1}{2}$ if $f_e(m) = s$ and $p_{\mathcal{M}|\mathcal{E}\mathcal{S}}(m|e, s) = 0$ otherwise. Note, for all $m, m' \in \mathcal{M}$ with $m' \neq m$, that $|E(m, m')| = 3$ and $|\{e \in E(m, m') : f_e(m) \neq f_e(m')\}| = 2$ and, for every $m \in \mathcal{M}$, that $|E(m)| = 4$ and $p_{\mathcal{M}}(m) = \frac{1}{5}$. It follows, for all $m, m' \in \mathcal{M}$ with $m' \neq m$, that $\text{payoff}(m, m') = \frac{1}{2}$. Therefore, $P_s = \frac{1}{2}$. Moreover, for any $e \in \mathcal{E}$ and $s \in \mathcal{S}$, we have that $\kappa(e) = 4$ and $|e(s)| = 2$. However, (2) gives the erroneous bound $P_s \geq \frac{2}{3}$.

We first identify the flaw in Theorem 3.8 of [4]. Having introduced (1), the author states: "It follows that

$$\sum_{\substack{m\neq m' \\ \exists e\in E: f_e(m)\neq f_e(m')}} \text{payoff}(m, m') \geq \min_{e\in\mathcal{E}} \left(\kappa(e) - \max_{s\in\mathcal{S}} |e(s)|\right). \tag{3}$$

Hence, there must be some m_0, $m_0 \neq m$ and, for at least one encoding rule e, $f_e(m_0) \neq f_e(m)$, such that

$$\max_{e\in E(m)} \left(v - \min_{s\in\mathcal{S}}|e(s)|\right) \cdot \text{payoff}(m, m_0) \geq \min_{e\in\mathcal{E}}\left(\kappa(e) - \max_{s\in\mathcal{S}} |e(s)|\right) \tag{4}$$

holds." The latter claim, however, does not always hold. In the counterexample above, for every $e \in \mathcal{E}$ and $s \in \mathcal{S}$, $\kappa(e) = 4$ and $|e(s)| = 2$. Moreover, for all $m, m' \in \mathcal{M}$, with

$m \neq m'$, $\text{payoff}(m, m') = \frac{1}{2}$. Hence, the left side of (4) evaluates to 1.5 while the right side evaluates to 2, i.e., inequality (4) is contradicted.

We now fix the identified flaw. Since inequality (3) holds in any authentication code with splitting, to get a lower bound on P_S, it suffices to get an upper bound on

$$\sum_{\substack{m \neq m' \\ \exists e \in E: f_e(m) \neq f_e(m')}} \text{payoff}(m, m'). \tag{5}$$

The following simple upper bound

$$(v-1) \cdot P_S(m) \geq \sum_{\substack{m \neq m' \\ \exists e \in E: f_e(m) \neq f_e(m')}} \text{payoff}(m, m') \tag{6}$$

together with (3) gives the following bound on P_S:

Theorem 2.2. *For every authentication code with splitting,*

$$P_S \geq \min_{e \in \mathcal{E}} \frac{\kappa(e) - \max_{s \in \mathcal{S}} |e(s)|}{v-1}.$$

Remark. The authentication code with splitting $\mathcal{A}$ in our counterexample meets the bound of Theorem 2.2 with equality.

In the scenario of authentication codes, a *spoofing attack of order i* describes the attack carried out by the opponent once he has observed i messages sent by T to R using the same encoding rule. The quantity P_{d_i} denotes the maximum probability of successfully deceiving the receiver after having observed i messages. De Soete (Theorem 3.9 in [4]) generalized the (erroneous) bound (2) for a spoofing attack of order L, claiming that, for any authentication code with splitting,

$$P_{d_i} \geq \min_{e \in \mathcal{E}} \frac{\kappa(e) - i \cdot \max_{s \in \mathcal{S}} |e(s)|}{v - i \cdot \min_{s \in \mathcal{S}} |e(s)|},$$

for any $0 \leq i \leq L$. This bound is also incorrect and can be corrected as follows.

Theorem 2.3. *For every authentication code with splitting and for every* $0 \leq i \leq L$,

$$P_{d_i} \geq \min_{e \in \mathcal{E}} \frac{\kappa(e) - i \cdot \max_{s \in \mathcal{S}} |e(s)|}{v - i}.$$

There is a close relationship between authentication codes and secret sharing schemes (see, for instance, [5]): From any secret sharing scheme we can construct an authentication code. Therefore results for authentication codes provide alternative formulations of results for secret sharing or new results. The bound on the size of the shares for different models of c-compact (k, n) threshold schemes with cheaters provided by Theorem 15 and Corollaries 16 and 20 of [5] are not correct since their derivation is based on the erroneous bound (2). For instance, the $(2, 2)$ robust threshold scheme depicted in

Table 2. A (2, 2) robust threshold scheme.

T	P_1	P_2	T	P_1	P_2
0	0	0	1	0	2
0	0	1	1	0	3
0	1	0	1	1	1
0	1	2	1	1	4
0	2	1	1	2	0
0	2	3	1	2	4
0	3	2	1	3	0
0	3	4	1	3	3
0	4	3	1	4	1
0	4	4	1	4	2

Table 2 violates the bound provided by Theorem 15 of [5]. Using the corrected version of De Soete's bound given by Theorem 2.2 in the proof of Theorem 15 in [5], we get the valid bound

$$|\mathcal{D}| \geq \frac{c(|\mathcal{S}| - 1)}{\varepsilon} + 1.$$

For secret sharing schemes with cheaters, the authors in [1] provide a new bound which relates the size of the shares, the size of the secret, the probability of cheating, and the probability of guessing. The new bound is an application of the technique used in the proof of Theorem 15 in [5] and of the corrected version of the bound for authentication codes with splitting provided in this paper. A different proof of this bound that does not use results borrowed from authentication codes with splitting can be found in [2]. Moreover, an analysis of different models and bounds, including ours, for secret sharing schemes with cheaters is given in [3].

Acknowledgments

We would like to thank Donatella Camelia for fruitful discussions on the topics of this paper, and James L. Massey and an anonymous referee for their comments.

References

[1] C. Blundo and A. De Santis, Lower Bounds for Robust Secret Sharing Schemes, *Information Processing Letters*, vol. 6 (1997), pp. 317–321.

[2] C. Blundo and A. De Santis, Authentication Codes and Robust Secret Sharing Schemes, Technical Report, Università di Salerno, March 1996.

[3] D. Camelia, Schemi Robusti per la Condivisione di Segreti, Tesi di Laurea, Università di Salerno, March 1996 (in Italian).

[4] M. De Soete, New Bounds and Constructions for Authentication Secrecy Codes with Splitting, *Journal of Cryptology*, vol. 3, no. 3 (1991), pp. 173–186.

[5] K. Kurosawa, S. Obana, and W. Ogata, t-Cheater Identifiable (k, n) Threshold Schemes, *Advances in Cryptology—CRYPTO* 95, Lecture Notes in Computer Science, vol. 963, 1995, Springer-Verlag, Berlin, pp. 410–423.

[6] D. R. Stinson, *Bibliography on Authentication Codes*, http://bibd.unl.edu/∼stinson/acbib.html.