A remark on the security of RMAC in the related-key security model

Éliane Jaulmes, Antoine Joux and Frédéric Valette

DCSSI Crypto Lab
18, rue du Dr. Zamenhof
F-92131 Issy-Les-Moulineaux.

Abstract. In this short note, we study the security of RMAC using a block cipher with n-bit keys without the ideal cipher model. We show that, given a block cipher that achieves the definition of related key attacks resistance recently proposed by Bellare and Kohno, it is easy to prove that RMAC is secure up to the birthday paradox limit, even when the adversary is granted full control of the random numbers used in the RMAC computations. This shows that the extra security offered in the ideal cipher model is not bought at the cost of security in more standard models.

1 Introduction

In this short note, we review the security of RMAC using a block cipher with n-bit keys when the underlying block cipher satisfies weaker assumptions than used in [3]. We assume that the reader is familiar with the description of RMAC and we use the same notations as in [3]. First of all, we remark that in [3], only the last call to the block cipher, during the final and randomized encryption of the MAC value, needs to be considered in the ideal cipher model. The lemmas concerning the collision probabilities present in [3] hold in the standard model. However, for the last call to the block cipher, the standard security notion for block cipher, i.e, indistinguishablity from a pseudo-random permutation is not sufficient. Indeed, a form of related key attack resistance is required. This was illustrated by Knudsen's attack [4] against RMAC instanciated with the Triple-DES as introduced by NIST in [5]. A standard style security model that addresses the issue of related-key attacks was recently proposed by Bellare and Kohno, it is scheduled for publication in the Eurocrypt'2003 proceedings [1] and also exists in the form of a full paper [2]. In this new model, related-key attacks is achieved with respect to a class of related key deriving functions that should meet some restrictions. In the case of RMAC, we are using one of the possible classes which is denoted by $\Phi_k^{\oplus}$ in [2] and consists of all functions XOR_Δ that xor the key with some constant Δ. Using this notion of related key attack resistance with respect to $\Phi_k^{\oplus}$, we show that RMAC is secure (up to the birthday paradox limit) even when the adversary is granted full control of the random numbers used in the final encryption step. As a consequence, we claim that the extra security of RMAC offered in the ideal cipher model is just that, extra security. In the extension of the standard model given in [2], RMAC is as secure as its determistic ancestor: encrypted CBC-MAC.

2 RMAC and related key attacks

The standard security notion of indistinguishablity from a pseudo-random permutation is less restrictive than the state-of-the-art in block cipher construction. Indeed, some properties of block-ciphers, which are now considered to be unbearable weaknesses, are not ruled out by this security notion. Let us give two examples of such properties. Our first example of related key weaknesses, somehow theoretical but present in many implementations of the DES, happens when some key bits are unused. In the case of DES implementations, the 56-bit key is often encoded as 8 bytes with the higher order bit in each byte ignored. In that case, two different (but related) 64-bit keys correspond to identical permutations. Another example is the complementation property of the DES, which directly yields a related key attack that identifies this property.

In RMAC, such weaknesses should be avoided. Moreover, since all the keys used in the final encryption are obtained by xoring a base key with some constant, chosen at random by the MAC producer and known to the

adversary (it is part of the published MAC value), more general related key attacks that use the XOR function should be avoided. This is achieved in the related key security model of [2] by requiring related key attack resistance with the class of related key deriving functions called Φ . In this context, it is easy to prove the security of RMAC (up to the birthday paradox limit). We can even allow the adversary to choose the random numbers used during MAC computations.

The sketch of proof is very simple. Since, the adversary controls the random value, the MAC verification oracle is no longer needed, we work with a MAC computation oracle only, as done with deterministic MACs. The first step of the proof is to replace the final (related-key) encryption of the MAC computation, that uses the block cipher E with key $K_2 \oplus R$ by a random permutation G_R (G_R is a different random permutation for each value of R). With the notion of related key proposed in [2], the advantage gained by the adversary is at most $\mathbf{Adv}^{prp-rka}_{\Phi^{\oplus}_k,E}$. Once this is done, we replace all the instances of the block cipher E used with K_1 in the CBC chain by a random permutation Π. The advantage gained by the adversary is at most $\mathbf{Adv}^{prp}_{E}$. Finally, we terminate the proof as in [6] by bounding the probability of (non-trivial) collision among the CBC intermediate values. Thus, the total advantage of an adversary (that controls the random values) against RMAC is at most:

$$\mathbf{Adv}^{prp-rka}_{\Phi^{\oplus}_k,E} + \mathbf{Adv}^{prp}_{E} + \frac{2 \cdot L^2}{2^n},$$

where n is the block size and L the total number of block in all the queries of the adversary (including the eventual test query).

References

1. M. Bellare and T. Kohno. A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In E. Biham, editor, *Advances in Cryptology — Proceedings of EUROCRYPT 2003*, Lecture Notes in Computer Science. Springer, 2003.
2. M. Bellare and T. Kohno. A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. Available from the authors, 2003. Full version of [1].
3. É. Jaulmes, A. Joux, and F. Valette. On the Security of Randomized CBC–MAC beyond the Birthday Paradox Limit — A New Construction. Cryptology ePrint Archive, Report 2001/074, 2002. `http://eprint.iacr.org`.
4. L.R. Knudsen. Analysis of RMAC. NIST Modes of Operation, Comment on Draft SP 800-38B, November 2002. Avaiblable at `http://csrc.nist.gov/CryptoToolkit/modes/comments/`.
5. NIST Special Publication 800-38B, Springfield, Virginia. *NIST. DRAFT Recommendation for Block-Cipher Modes of Operation: The RMAC Authentication Mode*, October 2002.
6. E. Petrank and C. Rackoff. CBC-MAC for Real-Time Data Sources. Technical Report 97-10, Dimacs, 1997.