Generic Attacks against MAC Algorithms

Gaëtan Leurent

Inria, France
Gaetan.Leurent@inria.fr

Message Authentication Codes (MACs) are important cryptographic constructions, used to ensure the authenticity of messages. MACs can be built from scratch (SipHash, Chaskey), from block ciphers (CBC-MAC, PMAC), from hash functions (HMAC), or from universal hash functions (GMAC, Poly1305). Constructions based on a lower level primitive are usually studied with a provable security approach: for commonly used MAC algorithms, security proofs rule out any attack on the MAC with complexity less than $2^{n/2}$ (the birthday bound), when using an ideal n-bit block cipher or compression function. On the other hand, a generic collision attack against iterated MACs by Preneel and van Oorschot [8] using $2^{n/2}$ queries show that the security proofs are tight.

The security of MAC algorithms seems to be well understood, but the generic attack of Preneel and van Oorschot is only an existential forgery attack, and stronger attacks (*e.g.* key-recovery attacks) are usually more expensive. In order to evaluate the security of common MAC algorithms below the birthday bound, we now focus on generic attacks, rather than on security proofs. The two approaches are complementary: generic attacks yields upper bounds on the security of a mode, and security proofs yield a lower bound. It is important to comin both, because constructions with a similar security proof can actually have a very different loss of security after the birthday bound.

For instance, there is a collision-based almost universal forgery attack against several CBC-MAC variants with birthday complexity [4]. There is also an attack with birthday complexity recovering the secret mask in PMAC using collisions [5]; this implies a universal forgery attack. More recently, a similar attack was shown against AEZ v3, but it yields a full key-recovery attack because of the way the secret mask is derived from the master key [2].

Hash-based MACs also have varying security beyond the birthday bound. The main constructions process the message with an unkeyed iteration, and use the key only in the initialization (secret-prefix MAC), in the finalization (secret-suffix MAC), or both in the initialization and finalization (HMAC, envelope MAC, sandwich MAC). All these constructions are good MACs when used with a random oracle, but they offer different levels of security in practice. Constructions using the key only in the finalization are much less secure, because collisions in the hash function directly lead to forgeries independently of the key. In particular, these collisions can be computed offline, and do not require any queries to a MAC oracle. Secret-suffix MAC and envelope MAC are also susceptible to a key-recovery attack based on collisions with partial blocks [9]. Interestingly, the key-recovery attack can be applied to envelope MAC but not to sandwich MAC, although the construction are very close and have a similar security proof.

Over the last years, a series of papers have studied more complex generic attacks against HMAC and similar hash-based MAC algorithms [6,7,3,1]. This proved that distinguishing-H, state-recovery, and universal forgery attacks against HMAC require less than 2^n operations, contrary to what was previously assumed. The first attacks used the structure of the cycle graph of random functions in an elegant way to build a distinguishing-H and state-recovery attack with complexity $2^{n/2}$ [6]. Variants with short messages were also given, using the entropy loss of random functions (with complexity $2^{2n/3}$), and later extended to HAIFA hash functions (with complexity $2^{4n/5}$) [1]. Surprisingly, extensions of those techniques also lead to universal forgery attacks against long messages [7,3]. In addition, the state recovery attacks can be extended to key-recovery attacks for HMAC based on a hash function with an internal checksum. In particular, this gives a key-recovery attack with complexity 2^{192} against HMAC-GOST (with $n = 256$), and 2^{419} against HMAC-Streebog (with $n = 512$).

All those examples show a large variety in the attack techniques and complexity, with several key-recovery attacks more efficient than exhaustive search. This highlights the importance of studying generic attacks in addition to the provable security driven approach to the design of MAC algorithms.

References

1. Dinur, I., Leurent, G.: Improved Generic Attacks against Hash-Based MACs and HAIFA. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO (1). Lecture Notes in Computer Science, vol. 8616, pp. 149–168. Springer (2014)
2. Fuhr, T., Leurent, G., Suder, V.: Collision Attacks against CAESAR Candidates. In: Iwata, T., Cheon, J.H. (eds.) Advances in Cryptology - ASIACRYPT 2015. Lecture Notes in Computer Science, Springer (2015)
3. Guo, J., Peyrin, T., Sasaki, Y., Wang, L.: Updates on Generic Attacks against HMAC and NMAC. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO (1). Lecture Notes in Computer Science, vol. 8616, pp. 131–148. Springer (2014)
4. Jia, K., Wang, X., Yuan, Z., Xu, G.: Distinguishing and Second-Preimage Attacks on CBC-Like MACs. In: Garay, J.A., Miyaji, A., Otsuka, A. (eds.) CANS. Lecture Notes in Computer Science, vol. 5888, pp. 349–361. Springer (2009)
5. Lee, C., Kim, J., Sung, J., Hong, S., Lee, S.: Forgery and Key Recovery Attacks on PMAC and Mitchell's TMAC Variant. In: Batten, L.M., Safavi-Naini, R. (eds.) ACISP. Lecture Notes in Computer Science, vol. 4058, pp. 421–431. Springer (2006)
6. Leurent, G., Peyrin, T., Wang, L.: New Generic Attacks against Hash-Based MACs. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT (2). Lecture Notes in Computer Science, vol. 8270, pp. 1–20. Springer (2013)
7. Peyrin, T., Wang, L.: Generic Universal Forgery Attack on Iterative Hash-Based MACs. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT. Lecture Notes in Computer Science, vol. 8441, pp. 147–164. Springer (2014)
8. Preneel, B., van Oorschot, P.C.: MDx-MAC and Building Fast MACs from Hash Functions. In: Coppersmith, D. (ed.) CRYPTO. Lecture Notes in Computer Science, vol. 963, pp. 1–14. Springer (1995)
9. Preneel, B., van Oorschot, P.C.: On the Security of Two MAC Algorithms. In: Maurer, U.M. (ed.) EUROCRYPT. Lecture Notes in Computer Science, vol. 1070, pp. 19–32. Springer (1996)