Let's not call it MR

(A Drunken-Monkey Contestant, and a Complaint about APE)

Phillip Rogaway

Cryptography and Information Security Group
ETH Zürich, Switzerland

August 23, 2014

Abstract. Everyone needs a pet peeve [4]. For me, today, it's use of the term *misuse resistance* (MR) for a security goal, online-AE (OAE), that has little to do with the original definition of MR, and provides limited security against nonce-reuse. Papers dealing with the scheme APE are among the worst of offenders [1–3], repeatedly claiming misuse resistance and strong security in the face of nonce reuse.

Keywords: Bad nomenclature, easy attacks, grumpy cryptographers, shameless attempts to win hard-to-get beer.

1 Introduction

Tom and I defined the term *misuse-resistant authenticated-encryption* (MRAE) in 2006 [9]. It's not a great name. The problem is that it sounds like it provides something quite general—a scheme unfazed by any sort of unpleasant abuse [11]—yet delivers something quite specific—a strong security property even if nonces are absent or reused. Thus a more accurate name would have been something like *nonce-reuse misuse-resistance*. But how are you going to sell something with an acronym like NRMRAE? A name as well chosen as *TIA* [12] or *blob* [7].

Still, the misuse-resistant / MR moniker is out there, and people have come to understand it to mean that no harm will come if nonces are reused. I think it should mean *at least* that much: my criticism above was that it doesn't mean *more*.

Yet, rather recently, MR has come to be used for *online AE* (OAE). Here I refer to the notion defined by Fleischmann, Forler, Lucks, and Wenzel [8], who took the privacy definition of Bellare, Boldyreva, Knudsen, Namprempre [5], cleaned up a bit by Rogaway and Zhang [10], and conjoined it with the usual authenticity notion for AE.

2 Philosophy

The fundamental problem is that OAE isn't very strong and doesn't imply that you'll be OK if you don't use a nonce. Things can easily go amok.

First, people fail to adequately emphasize that, to be meaningful, online-AE needs to be parameterized by a number r, the *block length*. Then the privacy definition is relaxed so that, when nonces get reused, one reveals the longest block-aligned prefix, for blocks of r-bits. In APE, $r = 40$.

Frankly, online-AE is a kind of flaky notion no matter what name you use for it, as the number r is never regarded as a user-selectable parameter (eg, to be instantiated by the anticipated size of L2

cache), but, instead, matches whatever primitive happens to be employed when someone dreams up a scheme. That's a basic "philosophical" error—selecting a security definition that's strongly tied to an implementation-associated artifact. But I digress. I am not here to discuss definitional philosophy; I am here to win a crate of beer. And that means I have to give some sort of attack. Even if I'm not even close to being a competent cryptanalyst.

3 A Trivial Attack

Still, I think it's easy to give attacks on APE that violate that which "should" be achieved by something deserving the label *misuse-resistance* and claiming 80 or 120 bits of security. Look at the picture in Fig. 1 of the paper on APE [1]. Fix the associated data A so we can ignore the top part of that figure and regard the lefthand $V_r \,\|\, V_c$ as being some key-dependent constant. Suppose you have a 100-byte ciphertext C that you'd like to decrypt. That's 20 blocks relative to the 5-byte blocksize that APE employs. Now I give you an encryption oracle (no decryption oracle needed) and ask: *how many encryption queries suffice to decrypt C?* The answer: about 2^{44}.

The attack is trivial: just ask to encrypt all one-block plaintexts until you match the first block of C; then ask to encrypt all one-block extensions of what you've found already until you match the second block of C; and so on, until you recover all of C. We have 20 blocks to match, and each takes at most 2^{40} queries. If partial information about the plaintext is known, the attack can be correspondingly accelerated.

You can see how strongly the efficacy of the attack depends on r; had r been 1 instead of 40, then decrypting our 100-byte ciphertext would have only taken 800 queries instead of 2^{44}. That's why it's important to make the parameter visible in the name of the security notion, writing something like OAE[40]. The bigger the blocksize, the stronger the security notion.

Unfortunately, the number 40 isn't very big. Not that the notion gets any prettier when the constant 40 increases (which can happen, for example, if it consumes a big meal).

4 That's no Attack!

Well, it is pretty obvious, and it doesn't violate the OAE[40] definition, so, in that sense, it isn't an attack. The problem, for me, is one of communication and perception: if you have a mode you're calling *misuse resistant*, and claiming 80 or 120 bits of privacy to boot, then you're not delivering on what users will reasonably expect.

5 OAE is Nothing like MRAE

Unlike *actual* MRAE, the kind Tom and I defined and showed how to achieve [9], OAE[r] security provides no automatic exploitation of message novelty to get semantic security. There's no automatic exploitation of receiver-verifier redundancy to augment authenticity, either. These properties, which go back to [6], are a big part of what makes MRAE an interesting goal. Just as much as avoiding catastrophe should nonces get reused.

In the end, MRAE is very much like a tweakable blockcipher—one that achieves strong-PRP security. But OAE is nothing like a blockcipher. It's like nothing but OAE.

Dissimilar notions shouldn't go by similar names; it's a recipe for misunderstanding. And avoiding that is needed to minimize misuse—the central promise of AE.

6 Phil's Proposal

From this day forward,

- Nobody shall use the term *misuse resistance* when they mean *online-AE*. Similarly, nobody shall use the term *MR*, nor *MR* with some funky adjective in front, like *MAX-online Nonce MR* (the unwieldy term from the AE zoo).
- Every mention of OAE shall be accompanied by the blocksize parameter, as in OAE[40].
- Anyone who violates either of the above rules shall have to read every single page of every single CAESAR submission.

7 Geographic Bliss

Anyway, you can't really ship that beer to India: it would never get past that pot-bellied customs agent. Even if it did, it would explode in the Indian heat. In contrast, Phil is presently residing in Switzerland—*Confoederatio Helvetica*, you know. And this CH in which I live—I would like to point out that it is a *Schengen area country*. This means, concretely, that sending beer from Belgium to Switzerland is as easy as buying guns in the U.S.A..

Acknowledgments

Reza Reyhanitabar expressed similar ideas to me a few days ago.

References

1. Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda. APE: Authenticated permutation-based encryption for lightweight cryptography. IACR Cryptology ePrint Archive 2013/791, 2013. To appear in FSE 2014.
2. E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, N. Mouha, and K. Yasuda. How to securely release unverified plaintext in authenticated encryption. Cryptology ePrint report 2014/144. Feb 25, 2014.
3. Elena Andreeva, Andrey Bogdanov, Atul Luykx, Florian Mendel, Bart Mennink, Nicky Mouha, Qingju Wang, and Kan Yasuda. PRIMATEs v1: Submission to the CAESAR Competition. March 15, 2014.
4. Mihir Bellare. *Personal communications*. August 18, 2014.
5. Mihir Bellare, Alexandra Boldyreva, Lars Knudsen, and Chanathip Namprempre. Online ciphers and the Hash-CBC construction. *CRYPTO 2001*, pp. 292–309.
6. Mihir Bellare and Phillip Rogaway. Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography. ASIACRYPT 2000, pp. 317–330.
7. Gilles Brassard, David Chaum, and Claude Crépeau. Minimum Disclosure Proofs of Knowledge. *Journal of Computer and System Science*, 37, 156–189, 1988.
8. Ewan Fleischmann, Christian Forler, Stefan Lucks, and Jakob Wenzel. McOE: A foolproof on-line authenticated encryption scheme. *Fast Software Encryption*. Springer, LNCS vol. 7549, pp. 196-215, 2012.
9. Phillip Rogaway and Tom Shrimpton. A provable-security treatment of the key-wrap problem. *EUROCRYPT 2006*, LNCS vol. 4004, Springer, pp. 373–390, 2006. Also Cryptology ePrint Report 2006/221, retitled, Deterministic authenticated-encryption: a provable-security treatment of the key-wrap problem. 2006.
10. Phillip Rogaway and Haibin Zhang. *Online ciphers from tweakable blockciphers*. CT-RSA 2011, pp. 237–249.
11. Marquis de Sade (Donatien Alphonse François). *Les 120 journées de Sodome ou l'école du libertinage* (The 120 Days of Sodom, or the School of Libertinism). 1785.
12. William Safire. You Are a Suspect. The New York Times. November 14, 2002.