Security Goals for an Accordion Mode: Release of Unverified Plaintext and Multi-user Security

UK National Cyber Security Centre

This talk will discuss two topics in security goals for an accordion mode: security against the Release of Unverified Plaintext (RUP), and advantage bounds for multi-user security under different assumptions.

Release of Unverified Plaintext

RUP happens when implementations leak information about failed decryption attempts. Examples include omission of authentication checks, reordering of the authentication with follow-on processing, and non-clearing of buffers containing putative plaintext. Attacks such as EFAIL [citation 1] and Lucky 13 [citation 2] show that RUP vulnerabilities can be exploited by an adversary to enable practical attacks.

There are several different RUP security games in the literature, with important differences between them. In the typical setup, the adversary is given access to a "leakage" oracle, *Leak*, alongside the usual *Enc* and *Dec* oracles. The adversary wins if *Enc, Dec, Leak* can be distinguished from $\$, \perp, \mathcal{S}$, where these simulate a random function of the appropriate length, the function which always rejects, and the "ideal" leakage, respectively. Modelling *Leak* is subtle – for example, AEZ has strong RUP security [citation 3], but early-abort AEZ does not [citation 4]. Moreover, defining $\mathcal{S}$ is subtle. For example, the RUP notions PA1 [citation 5] and AE-RUP [citation 6] allow $\mathcal{S}$ to use the transcript of queries to the *Enc* oracle, which implies the leakage can contain information about the plaintexts. AES-GCM is PA1 secure, but would not fully block EFAIL in some circumstances. The SAE notion [citation 4] is stronger, but still allows the attacker to exert control over leakage. We support the strongest notion, RUPAE, proposed in [citation 7], which says that on fresh inputs, $\mathcal{S}$ should output uniform random data.

NIST have proposed [citation 8] developing a new AEAD derived function from an accordion mode using the Encode-then-Encipher technique. Strong RUP security can be achieved using this approach [citation 4], without compromising other security goals. The NCSC is in favour of adding strong RUP security as a design goal for the proposed accordion mode.

Multi-user security

When NCSC assure the use of a mode, we reason about the security of the entire system or protocol the mode is deployed within, rather than the security of individual users or keys within that system. To enable this assurance, we require security proofs to give a concrete advantage bound in a multi-user setting, and we use these bounds to derive practical usage limits to impose on our end-users. Per-user encryption limits are more easily enforced than global usage limits, and decryption limits are difficult to enforce. For reasons of interoperability, we also have an essential requirement that the modes we use support AES, which has a 128-bit block size.

Using plausible real-world figures for a large system with many users, one can show that beyond-birthday-bound security is likely to be necessary when using a mode of a 128-bit block cipher. We believe the same considerations may apply for other organisations with similar use-cases, especially where multi-user security and compatibility with AES is required.

Bibliography

1. EFAIL: Damian Poddebniak, Christian Dresen, Jens Müller, Fabian Ising, Sebastian Schinzel, Simon Friedberger, Juraj Somorovsky, and Jörg Schwenk. Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels. In 27th USENIX Security Symposium (USENIX Security 18), pages 549–566, 2018.
2. Lucky13: Nadhem J. AlFardan and Kenneth G. Paterson. Lucky Thirteen: Breaking the TLS and DTLS Record Protocols. In 2013 IEEE Symposium on Security and Privacy, pages 526–540, Berkeley, CA, USA, May 19–22, 2013. IEEE Computer Society Press.
3. RUP security of AEZ and EtE: Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust Authenticated-Encryption AEZ and the Problem That It Solves. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology – EUROCRYPT 2015, Part I, volume 9056 of Lecture Notes in Computer Science, pages 15–44, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany.
4. AEZ absence of RUP security and SAE: Guy Barwell, Daniel Page, and Martijn Stam. Rogue Decryption Failures: Reconciling AE Robustness Notions. In Jens Groth, editor, 15th IMA International Conference on Cryptography and Coding, volume 9496 of Lecture Notes in Computer Science, pages 94–111, Oxford, UK, December 15–17, 2015. Springer, Heidelberg, Germany.
5. PA1: Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda. How to Securely Release Unverified Plaintext in Authenticated Encryption. In Palash Sarkar and Tetsu Iwata, editors, Advances in Cryptology – ASIACRYPT 2014, Part I, volume 8873 of Lecture Notes in Computer Science, pages 105–125, Kaoshiung, Taiwan, R.O.C., December 7–11, 2014. Springer, Heidelberg, Germany.
6. AE-RUP: Donghoon Chang, Nilanjan Datta, Avijit Dutta, Bart Mennink, Mridul Nandi, Somitra Sanadhya, and Ferdinand Sibleyras. Release of Unverified Plaintext: Tight Unified Model and Application to ANYDAE. IACR Transactions on Symmetric Cryptology, 2019(4):119–146, 2019.
7. RUPAE: Tomer Ashur, Orr Dunkelman, and Atul Luykx. Boosting Authenticated Encryption Robustness with Minimal Modifications. In Jonathan Katz and Hovav Shacham, editors, Advances in Cryptology – CRYPTO 2017, Part III, volume 10403 of Lecture Notes in Computer Science, pages 3–33, Santa Barbara, CA, USA, August 20–24, 2017. Springer, Heidelberg, Germany.
8. NIST Proposal of Requirements for an Accordion Mode: Yu Long Chen, Michael Davidson, Morris Dworkin, Jinkeon Kang, John Kelsey, Yu Sasaki, Meltem Sönmez Turan, Donghoon Chang, Nicky Mouha, Alyssa Thompson.