Using RUP Security to Protect Tor Against Crypto Tagging

Tomer Ashur[1], Orr Dunkelman[2], and Atul Luykx[1,3]

[1] Dept. Electrical Engineering, ESAT/COSIC, KU Leuven, and imec, Belgium
tashur@esat.kuleuven.be,atul.luykx@esat.kuleuven.be
[2] University of Haifa, Haifa, Israel
orrd@cs.haifa.ac.il
[3] Department of Computer Science, University of California, Davis

Authenticated encryption (AE) combines the symmetric-key goals of data confidentiality and authenticity. Although well-established, widely deployed AE algorithms are fragile, since their security collapses when deployed in the wrong environments. Recent research has sought to formalize and design AE that remains robust under Release of Unverified Plaintext (RUP), capturing security when decrypted ciphertext cannot remain hidden before verification is complete.

An advantage of RUP-secure schemes is that they provide another line of defense with faulty implementations: if an implementation for whatever reason fails to check authenticity, then RUP-confidentiality guarantees that if the ciphertext did not originate from the sender or was modified en route, the resulting decrypted plaintext will look like garbage. Furthermore, there are settings where a RUP-secure AE scheme provides desirable properties beyond confidentiality and authenticity.

State-of-the-art research might give the impression that achieving RUP security by minimally modifying existing schemes is out of reach: all designs providing such security either require significant changes, a completely new design, or an additional pass, making the schemes slower and adding design complexity. This is because so far the only solutions provided are essentially variable-input-length (VIL) ciphers, which can be viewed as block ciphers that can process arbitrarily long messages. However, VIL ciphers are "heavy" constructions, requiring often three or more passes over the plaintext in order to ensure sufficient mixing, or relying on subtle design choices to achieve security.

We present a minor modification to GCM which achieves both RUP confidentiality and authenticity. The core idea is to use a digest of the ciphertext to "hide" the nonce in such a way that recovering it properly requires that no change was made to the ciphertext. As a result, if a change *did* occur, it would affect the nonce, which, when used by the decryption algorithm, would decrypt the ciphertext into meaningless data.

We show how RUP security can be used to defend Tor from the crypto tagging attack where the entry node makes a change to the message. The change goes undetected through the middle node, and removed by the exit node. If, after removing the change, the message is properly authenticated, the entry and the exit nodes can link the source and the target of the message thus violate the user anonymity.