From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Monday, July 8, 2019 12:37 PM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: [lwc-forum] OFFICIAL COMMENT: SUNDAE-GIFT

Dear All,

It seems SUNDAE-GIFT is vulnerable to collisions in the internal state leading to loss of confidentiality.

This vulnerability is caused by the small active internal state of 128 bits during encryption that leads to a non-negligible probability of state collision during on-line processing.

Description of SUNDAE-GIFT message encryption from specification

V <= Tag

The message blocks are encrypted block by block without padding as follows
V <= E_K(V)
C[i] <= E_K(V) ⊕M[i]

Attack description

Step 1

1) Chose a data block Ma, then Encrypt the Message M = M1 | M2 | M3 | M4 |.... with up to 2^49 bytes.
2) Extract the Ciphering Stream CS[i] = C[i] ⊕ Mi for i = 1,2,3,4,....
   The values of CS[i] are directly linked to the internal state at step i of encryption.

   This leads to 2^49/(128/8) = 2^45 Candidate states for collision.

Step2

3) Get the result of encrypting the unknown data block XX for various Nounces N[j] => Result is : Tag[j] | C[j]
   To stay under the 2^50 ciphered Bytes limit, the maximum number of ciphered messages is 2^49/(2*128/8) = 2^44

Step3

4) Look for a collision between the Tags T[j] and the CS values from Step1.

=> The probability to have a collision between the two sets is approximately:

(2^45 * 2^44)/2^128 = 2^-39 for a complexity of 2^46 ciphered blocks, 2^49 memory Bytes and 2^45 Memory Look Up.

A collision allows recovery of the value of XX since the value of Ek(V) is then known from Step1, and XX is recovered as C[j] ⊕ Ek(V)

Cost of attack:

This attack has a cost equivalent of 39 + 49 = 88 bits.

Best regards,

Alexandre Mège

From: Thomas Peyrin (Assoc Prof) <thomas.peyrin@ntu.edu.sg>
Sent: Wednesday, July 10, 2019 2:45 AM
To: MEGE, Alexandre; lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: RE: OFFICIAL COMMENT: SUNDAE-GIFT

Dear all,

We would like to thank Alexandre for his comment and interest in SUNDAE-GIFT. However, what he describes is a straightforward generic birthday attack and we would advise to read the SUNDAE article, where it is explained how these birthday attacks are taken into account in the security proof:
https://tosc.iacr.org/index.php/ToSC/article/download/7296/6470

Moreover, as clearly stated in Table 3 of our submission, with 2^{50} bytes of data processed, the expected adversarial advantage is not more than 2^{-30}. Thus, Alexandre's observation is as expected within our security bounds and actually demonstrates that our security claims hold. To conclude, of course no modification of SUNDAE-GIFT will be made based on this comment.

Thomas.