From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Wednesday, June 5, 2019 3:53 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: SPIX

Dear All,

It seems spix is vulnerable to forgery attacks in the Associated Data.
Messages with padded associated Data can collide with messages with associated Data containing the padding.

This is a similar vulnerability as the one identified in SIV_Rijndeal256-AEAD by NILanjan Datta.

Use of different tweaks during the final associated Data block processing based on full/partial block will protect against this attack.

Reagrds,
Alexandre Mège

Ex: for spix128v1

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 000102030405060708090A0B0C0D0E0F
PT = 00
AD = 0000000000
CT = 775162FEE30F96148D16BDF513C83DF907

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 000102030405060708090A0B0C0D0E0F
PT = 00
AD = 0000000000800000
CT = 775162FEE30F96148D16BDF513C83DF907

And

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 2A2B2C2D2E2F30313233343536373839
PT = 0000
AD = 0000000000
CT = 47C9C7F578BA5851DB695DB82B3BA1F215E5

Key = 000102030405060708090A0B0C0D0E0F
Nonce = 2A2B2C2D2E2F30313233343536373839
PT = 0000

AD = 0000000000800000
CT = 47C9C7F578BA5851DB695DB82B3BA1F215E5

This document, technology or software does not contain French national dual-use or military controlled data nor US national dual-use or military controlled data.

From: Raghvendra Rohit <iraghvendrarohit@gmail.com>
Sent: Wednesday, June 5, 2019 5:51 PM
To: lwc-forum
Cc: lightweight-crypto; Kalikinkar Mandal; Riham AlTawy
Subject: Re: OFFICIAL COMMENT: SPIX
Attachments: spixv1-june05-2019.tar.gz

Dear Alexandre,

Thanks for your observation. Note that according to the specifications (Section 2.2.2) **"AD is always padded irrespective of whether it is a partial or complete block (except when |AD|=0)"**. Thus, a partial AD block without padding and another complete AD block with padding will always result in different tags. As for the examples you have mentioned, they resulted because of a minor part was missing in the reference implementation (more specifically, the proc_ad function did not process the padded block when AD length is a multiple of 8).

Hence, the presented forgery is due to an error in our reference implementation only, which is not related to SIV-Rijndeal256 forgery.

Dear all,

We have fixed the above issue in the reference implementation. Attached is the updated copy of SPIX's reference implementation.
Note that there are no changes in the specifications of SPIX.

Thanks and regards,
SPIX Team

On Wednesday, June 5, 2019 at 3:53:02 AM UTC-4, alexandre.mege wrote:

> Dear All,
>
> It seems spix is vulnerable to forgery attacks in the Associated Data.
>
> Messages with padded associated Data can collide with messages with associated Data containing the padding.
>
> This is a similar vulnerability as the one identified in SIV_Rijndeal256-AEAD by NILanjan Datta.