From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Monday, July 15, 2019 11:02 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: Triad

Dear All,

It seems TRIAD is vulnerable to forgery attack.

This vulnerability comes from the absence of domain separation between AD and PT processing.

This leads to a forgery attack where the padding pattern including the AD length separating AD and PT data is moved from the correct pattern limit to a decoy pattern embedded in the PT data.

This could be solved by using different tweaks for processing the AD and PT part of the input data.

Ex for triadaev1:

Key=0x000102030405060708090a0b0c0d0e0f

Nonce=0x2a2b2c2d2e2f303132333435

Pt=0x08000000000000

Ad=0x00

Ct=0xab19f549a3f272**3e5e17360726c51b**

Key=0x000102030405060708090a0b0c0d0e0f

Nonce=0x2a2b2c2d2e2f303132333435

Pt=0x

Ad=0x0001000000000000

Ct=0x**3e5e17360726c51b**

Best regards,

Alexandre Mège

From: Takanori Isobe <takanori.isobe@ai.u-hyogo.ac.jp>
Sent: Thursday, July 18, 2019 7:03 PM
To: MEGE, Alexandre
Cc: lightweight-crypto; triad-designers@googlegroups.com; lwc-forum@list.nist.gov
Subject: Re: [lwc-forum] OFFICIAL COMMENT: Triad

Dear Alexandre,

Thank you very much for your analysis.
As you pointed out, our padding is not proper.
We will add the length padding for PT after absorbing the message, which totally defends the forgery attack.

Best Regards,
Triad Team

On 2019/07/16 0:02, MEGE, Alexandre wrote:

> Dear All,
>
> It seems TRIAD is vulnerable to forgery attack.
>
> This vulnerability comes from the absence of domain separation between AD and PT processing.
>
> This leads to a forgery attack where the padding pattern including the AD length separating AD and PT data is moved from the correct pattern limit to a decoy pattern embedded in the PT data.
>
> This could be solved by using different tweaks for processing the AD and PT part of the input data.
>
> **Ex for triadaev1:**
>
> Key=0x000102030405060708090a0b0c0d0e0f
>
> Nonce=0x2a2b2c2d2e2f303132333435
>
> Pt=0x08000000000000
>
> Ad=0x00
>
> Ct=0xab19f549a3f272**3e5e17360726c51b**
>
> Key=0x000102030405060708090a0b0c0d0e0f
>
> Nonce=0x2a2b2c2d2e2f303132333435