From: MEGE, Alexandre <alexandre.mege@airbus.com>
Sent: Friday, July 12, 2019 8:50 AM
To: lightweight-crypto
Cc: lwc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: HERN & HERON

Dear All,

It seems HERN is vulnerable to forgery attack and probably Key recovery attack.

Those vulnerabilities come from a weak separation between AD and PT processing.

More specifically, the tags obtained from ciphering Pt=0x00 Ad=0x and Pt=0x, Ad=0x00 collide with probability 2^-8.

Root Cause
This collision happens because the only difference when processing the last Byte of Ad and first Byte of Pt is:

- 'H_if_step' performing an additional application of 'Addb' function versus what is performed in 'H_enc_step'.

The function 'Addb' performs the xoring into the state of a bit called 'b'.
This xoring is performed for each bit to process, so eight times for a Byte.
If those eight 'b' bits are all '0', then there is no more separation between Ad and Pt, and a Tag collision happens.

Practical attack
For a practical implementation of the attack, the attacker can encrypt Pt=0x00 Ad=0x , get the result Ct | Tag, and then try to decrypt Pt = 0x, Ad=0x00 with the same Tag.
Repeat this process with different nonces until the forged message is accepted. The tags will match and the messages will be accepted in around 2^8 tries.

Potential Key recovery
Those matching events leak the value of the 8 'b' bits just after the nonce and Ad processing (in fact during the last byte of Ad processing).
This leaks state data before the cryptographic permutation is applied.
This early in the processing, the mixing of Key/Nonce/Ad is quite limited.
I am quite confident an effective key recovery attack could be developed based on the leakage of those 'b' values.

Example of collision:

Key=0x02000000000000000000000000000000, Nonce=0x10000000000000000000000000000000,
Pt=0x, Ad=0x00,
Ct=0xca3526160f2d1c02eb9bbd96c1a2a77b,

Key=0x02000000000000000000000000000000, Nonce=0x10000000000000000000000000000000,
Pt=0x00, Ad=0x,
Ct=0x00ca3526160f2d1c02eb9bbd96c1a2a77b,

Best regards,

Alexandre Mège

From: 王鹏 <wp@is.ac.cn>
Sent: Saturday, July 13, 2019 12:14 AM
To: MEGE, Alexandre; lightweight-crypto
Cc: iraghvendrarohit; andre.schrottenloher; lwc-forum
Subject: Re:[lwc-forum] OFFICIAL COMMENT: HERN & HERON

Dear Alexandre,

The attack is obviously correct. We also received emails previously pointing out the same issue of HERM, including
- from Raghvendra Rohit on May 26 and
- from André Schrottenloher on Jul 11.

Rohit also suggested that a simple fix would be to invert a state bit once AD/M processing phase is done and then run H_if_step(0) for 512 times.

We are grateful to Alexandre Mège, Raghvendra Rohit and André Schrottenloher for observing this issue. Thank you all.

Best regards,

Peng Wang
On behalf of the HERN & HERON Team

ps. The last mail does not applear in the mail list, so I send it again with cc to lwc-forum@list.nist.gov.

---------- Original ----------
From: "MEGE, Alexandre"<alexandre.mege@airbus.com>;
Date: Fri, Jul 12, 2019 08:50 PM
To: "lightweight-crypto@nist.gov"<lightweight-crypto@nist.gov>;
Cc: "lwc-forum@list.nist.gov"<lwc-forum@list.nist.gov>;
Subject: [lwc-forum] OFFICIAL COMMENT: HERN & HERON

Dear All,

It seems HERN is vulnerable to forgery attack and probably Key recovery attack.

Those vulnerabilities come from a weak separation between AD and PT processing.

More specifically, the tags obtained from ciphering Pt=0x00 Ad=0x and Pt=0x, Ad=0x00 collide with probability 2^-8.

Root Cause

This collision happens because the only difference when processing the last Byte of Ad and first Byte of Pt is:

- ‘H_if_step’ performing an additional application of ‘Addb’ function versus what is performed in ‘H_enc_step’.