From: Mouha, Nicky W. (IntlAssoc)
To: Calik, Cagdas (IntlAssoc); lightweight-crypto
Subject: Re: early submissions kat verification - early analysis
Date: Wednesday, January 30, 2019 12:36:04 PM

Hi,

I just had a short discussion with Cagdas. We also spoke about the unix-or-windows-style line endings.

To make a long story short: Cagdas is right, and I stand corrected. We said that Ubuntu is the test vector verification platform, so the authors should have unix-style line endings.

Regards,
Nicky

From: Calik, Cagdas (IntlAssoc)
Sent: Tuesday, January 29, 2019 2:00 PM
To: lightweight-crypto
Subject: early submissions kat verification - early analysis

I'd like to share with you my findings on the verification of KAT values for the early submissions.

- We can make all the early-submissions pass the KAT verification.
  - "Gage_and_ingage, gimliv1, Lilliput-ae, and photon" pass the KAT verification without requiring any tweaks from us.
  - "Comet, limdolen, and lotus" pass the KAT verification provided that their version of generated KAT file is in the correct location. (They put it inside the "ref" folder as opposed to one level higher)
  - SAEAES passes the KAT verification if the line endings is converted to unix-style. (They have windows-style line endings)
- Some of the submissions had additional .c files in their ref directory and it's not obvious to know whether they should be included in the compilation. So, I tried both ways (compiling all .c files vs compiling just encrypt.c and genkat.c) and if at least one of the cases succeeds, then I proceeded with that.
- A flag we used in compilation (-fsanitize=address,undefined) causes problems in the newer versions of the gcc build chain. The compilation succeeds but the executable does not run. I removed this flag from the compilation for now but I'll figure out a solution for the new compilers.

I’ll be inspecting the source codes for any irregularities in the upcoming days.

Cagdas