Using ShangMi in the Internet Key Exchange Protocol Version 2 (IKEv2)

draft-guo-ipsecme-ikev2-using-shangmi-00

Yanfei Guo, Liang Xia Huawei

Yu Fu China Unicom

China ShangMi Cryptography Algorithms Background

- SM2: a set of cryptographic algorithms based on elliptic curve cryptography, including a digital signature, public key encryption (not defined in this draft for IKEv2) and key exchange scheme. ISO/IEC 14888-3:2018 , GBT.32918.2-2016, GBT.32918.5-2017

- SM3: a hash function that produces an output of 256 bits. ISO/IEC 10118-3:2018, GBT.32905-2016

- SM3: a set of block cipher encryption algorithms. 18033-3:2010, GBT.32907-2016

Proposal: IKEv2 Support ShangMi without any Protocol Change, Only Add Several New Transform Types and IDs

◆**New added Transform Types and IDs:**

1、Transform Type 1 - Encryption Algorithm Transform IDs

- ✓ENCR_SM4_CBC CBC
- ✓ENCR_SM4_GCM AEAD
- ✓ENCR_SM4_CCM AEAD

2、Transform Type 2 - Pseudorandom Function Transform IDs

- ✓PRF_HMAC_SM3

3、Transform Type 3 - Integrity Algorithm Transform IDs

- ✓AUTH_HMAC_SM3

4、Transform Type 4 - Key Exchange Method Transform IDs

- ✓curveSM2

5、IKEv2 Hash Algorithms

- ✓SM3

6、IKEv2 Authentication Method

- ✓SM2 Digital Signature

Table of Contents

Security Considerations

- At the time of writing, there are no known weak keys for SM cryptographic algorithms SM2, SM3 and SM4, and no security issues have been found for these algorithms.
- cryptanalysis of SM2:
  - ✓ Zhang, K Yang, J Zhang, C Chen, Z., "Security of the SM2 signature scheme against generalized key substitution attacks", International Conference on Research in Security Standardisation (pp. 140-153) , December 2015
  - ✓ Cui, X Qin, C Cai, T Yuen, H., "Security on SM2 and GOST signatures against related key attacks", 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 155-163) , October 2021.
- cryptanalysis of SM4 (especially for side-channel attacks):
  - ✓ LOU, F ZHANG, J HUANG, X ZHAO, H LIU, X., "Research on trace driven Cache analysis on SM4", Journal of Cryptologic Research, 2018, 5(4) 430–441, 2018
  - ✓ WU, Z DU, M WANG, Y WANG, K WANG, T YU, Z., "Chosen plaintext algorithm for chosen-plaintext power analysis against SM4", Journal of Cryptologic Research, 2018, 5(4) 421–429, 2018
  - ✓ JIN, H YANG, X WANG, Q YUAN, Y., "Improved differential fault attack for SM4 cipher", Journal of Cryptologic Research, 2020, 7(4) 453–464, July 2020, <[{"DOI"=>"10.13868/j.cnki.jcr.000380"}]>

Latest Discussion, Next Step Suggestion?

- Comments from Paul Wouters (SEC AD):

"*Thanks for the document.* ***I believe the best way forward for these would be via the ISE****. In which case the Working Group and Intended Status would need to be updated. But if the document proceeds that way, please* ***keep the IPsecME WG in the loop. All the registries involved are "Expert Review"****, so it can be registered regardless of where or how the specification is published.*

As for the draft itself, I have two questions.

Is the CBC variant really neccessary? CBS is being made historic or deprecated for all other IETF uses (eg see TLS 1.3). Why introduce it now for IKEv2 and ESP in combination with ShangMi ?

For the GCM variants, do you know if these can make use of the ghash hardware instructions? As in, would ENCR_SM4_GCM also benefit from CPU hardware instructions available?

"

- About next step, welcome WG's suggestions!

Thank you!