IETF Hackathon
Ultra Low-Latency Crypto, Areion

IETF 117
22-23 July 2023
San Francisco, California

Yumi Sakemi - GMO Cybersecurity by Ierae

Background

- The development of the Internet has made it easier to communicate large amounts of data and the requirements for cryptographic primitives (symmetric key cryptographies and hash functions) in Internet protocols are becoming more sophisticated, which will affect the future use of cryptography on the Internet.

- Concrete Examples:
  - Concerns of security limitation of 128-bit block size like AES-GCM are mentioned in NIST SP800-38A pubic comments
    - URL: https://csrc.nist.gov/csrc/media/Projects/crypto-publication-review-project/documents/initial-comments/sp800-38a-initial-public-comments-2021.pdf
  - Due to performance problems of Hash function in SFrame, authentication per sender is not provided
    - “No per sender authentication” is mentioned in security consideration
  - trends in NIST regarding wide block ciphers

Ultra low-latency crypto Areion

- Areion, an secure and ultra-low latency crypto, was designed by the University of Hyogo, NICT, NEC and Mitsubishi Electric in 2023 as a technology to solve these problems.
  - Cryptographic permutation based on AES instructions
  - Two functions (encryption and hash function)
    - **256-bit block cipher** (key size: 256, 512 bits) as an encryption
    - Hash function of Areion is **the most efficient latency among other hash functions** (ex.SHA-256)
  - This paper is accepted by TCHES 2023

Hackathon Plan

Our goal is to prepare an environment so as to everyone can try Areion.

- add Areion into OpenSSL in order to compare Areion and AES256-GCM
- add new TLS 1.3 ciphersuites with Areion to quictls.
  - “TLS_AREION256_OPP_SHA256”
    - OPP
      - Offset Public Permutation mode
      - Permutation-based AEAD scheme

What got done

- Successfully add encryption function of Areion to OpenSSL (quictls)
  - You can use AREION-256-OPP as one of ciphers in OpenSSL
  - The results of the comparison between AES-GCM and AREION is different depending on the choice of options for the “speed” command
    - we will publish the results after the reason is cleared.

- Successfully add new TLS1.3 ciphersuites with Areion
  - You can use secure communication with “TLS-AREION256-SHA256” by using sample program (s_server and s_client)

What we learned

- Areion's approximate performance has become clear!
  - The paper did not mention a performance comparison with AES-GCM due to differences in security levels
- It is worth writing an I-D!
  - because the performance prospects and high security are beneficial.
    - the elimination of block size restrictions for symmetric key cryptographies
    - the realization of forgery countermeasures for SFrame

Next Step

- Implementation
  - Hash functions
    - reference implementation
    - add into OpenSSL
- Performance
  - Compare and evaluate the performance of AES256-GCM and AREION256-OPP
- Application
  - Writing Internet Draft on Areion
  - Consider to applying to Internet protocols
    - areion could be useful for the topics in these WGs
      - QUIC, WebRTC, Sframe, etc

Wrap Up

Team members:

- Yumi Sakemi
  yumi.sakemi@gmo-cybersecurity.com
- Satoru Kanno
  satoru.kanno@gmo-cybersecurity.com

For more details

・Open Source

- Reference code
  https://github.com/gmo-ierae/low-latency-crypto-areion
- For OpenSSL
  https://github.com/gmo-ierae/areion-openssl (TBA at **23 July, 2023**)

・Internet Draft

- To be appeared at **next IETF**!