IETF Hackathon
Ultra Low-Latency Crypto, Areion

IETF 121
2-3 November 2024
Dublin, Ireland

Yumi Sakemi - GMO Cybersecurity by Ierae

What is Areion

- Low-latency crypto, Areion
  - Areion is a secure and low-latency cryptographic permutation
    - cryptographic permutation based AES instructions
    - Areion can be applied to **encryption** and **hashing**
  - For more details, please refer the IETF117 hackathon slides and I-D

- Use case of Areion
  - Use case that requires real-time secure communication
    - ex) e-Sports, remote surgery, satellite communication…

Performance Characteristics of Areion

- Following performance characteristics are confirmed during IETF120 hackathon
  - it was experimentally found that Areion is faster than current cryptography (AES256-GCM and SHA-256)
    - A situation where keys are frequently updated.
    - The message length is short (around 32 ~ 256 bytes)

IETF121 Hackathon Plan

- We tried to two tasks in this hackathon
  - Implement Areion by Rust
  - Evaluate Areion on a mobile device

Result

- Rust Implementation
  - We have successfully implemented Areion by Rust
    - It is reference code
  - We plan to publish the codes as OSS soon

- Evaluate performance on a mobile device
  - We have successfully evaluated the performance of Areion on pixel 7

Result

- Performance on a pixel 7 device
  - AEAD Encryption

Average		mlen					
primitive		16	32	64	128	256	512
areion-opp-256-encrypt	keylen=32	NA	40.45271	20.18786	10.093504	5.03983	2.515271

Cycles per byte

  - Hash function

Average		mlen					
primitive		16	32	64	128	256	512
areion-md		NA	6.098581	8.589316	4.909511	4.327783	4.029161

Cycles per byte

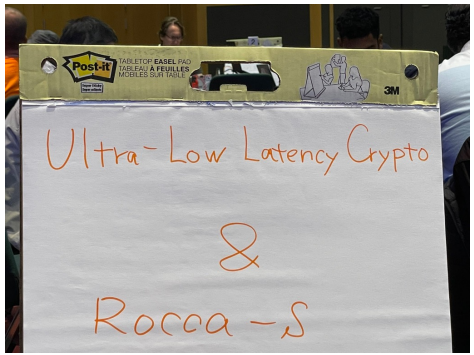
Next Steps

- Rust implementation
  - optimize Rust codes
- Evaluation on pixel 7
  - The expected effects have not been achieved, so further investigation is necessary
- Looking for effective applications ☺
  - Your comments are welcome!!
    - We have received feedback from the field of gaming, NW router…

Wrap Up

Champions:

- 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

・Internet Draft

- https://datatracker.ietf.org/doc/draft-sakemi-areion/