IETF Hackathon
Ultra Low-Latency Crypto, Areion

IETF 118
4-5 November 2023
Prague, Czech Republic

Yumi Sakemi - GMO Cybersecurity by Ierae

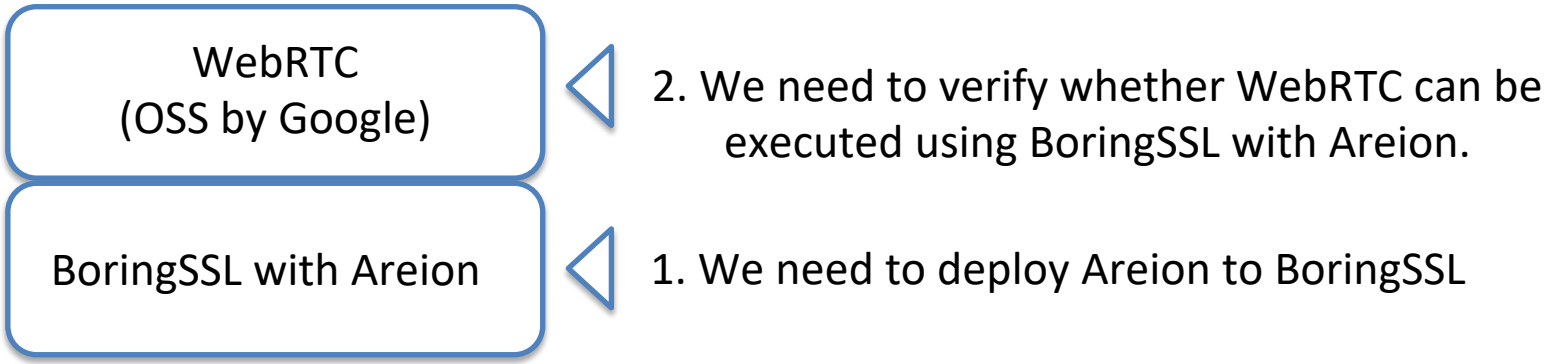
What is Areion

- Low-latency crypto, Areion
  - Areion is a secure and low-latency cryptographic scheme
    - 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

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

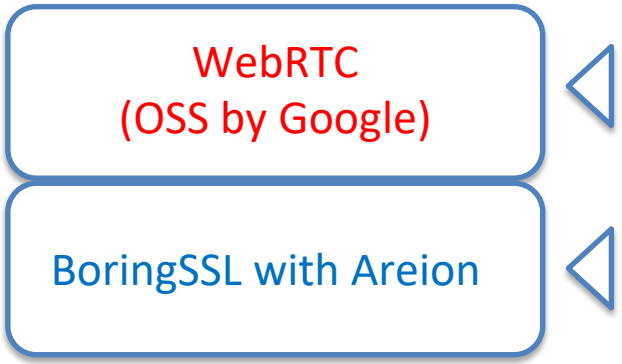
Hackathon Plan

- Goal
  - To prepare environment of WebRTC with Areion



Hackathon Result

- Result
  - We successfully added Areion to BoringSSL



NG

(We have some errors at the level of WebRTC… ☹)

OK

（Successfully connected with DTLS with Areion☺）

Next Step

- Implementation
  - WebRTC with Areion
    - debug
  - Hash functions
    - reference implementation
    - add into OpenSSL
  - Encryption modes
    - OTR mode
  - Independent implementations
    - Call for volunteers!
      - If you are interested in our activities, please contact us!
- Performance
  - Compare and evaluate the performance of AES256-GCM and AREION256-OPP
- Application
  - Discussion with experts

Wrap Up

Champions:

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

Participants:

- Vukašin Karadžić
  - Thank you, Vukašin!

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/