IETF Hackathon

IETF 120
20–21 July 2024
Vancouver, Canada

Hackathon Plan

- **Problem:** Ensuring IoT security in the face of emerging quantum computing threats.

- **Solution:** Integrating Post-Quantum Cryptography (PQC) to protect IoT devices from potential quantum decryption capabilities.

- **Drafts Involved:** NIST Post-Quantum Cryptography Standardization, The Transition from Classical to Post-Quantum Cryptography

- **Goal:** Future-proof IoT ecosystems by securing data transmission, key management, and firmware updates using PQC algorithms.

What got done

- Developing a repository that can be used by IoT developers to use encryption using Kyber for KEM
- https://github.com/noumerica2023/PQ-IoT-Shield/tree/main

Diagram (Proposal 1)

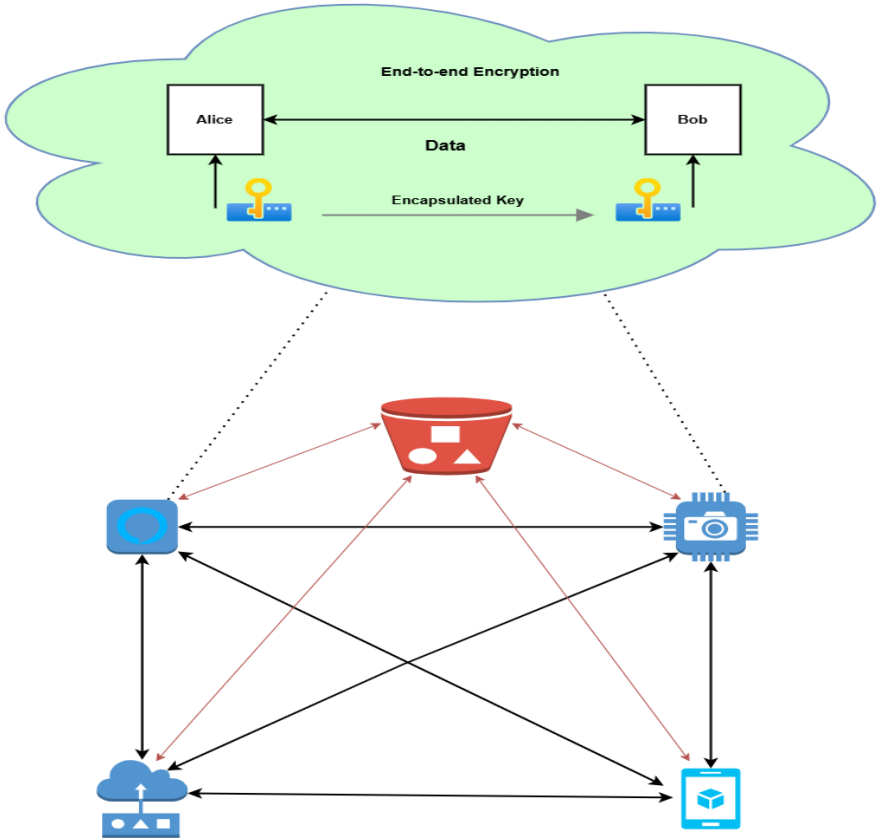
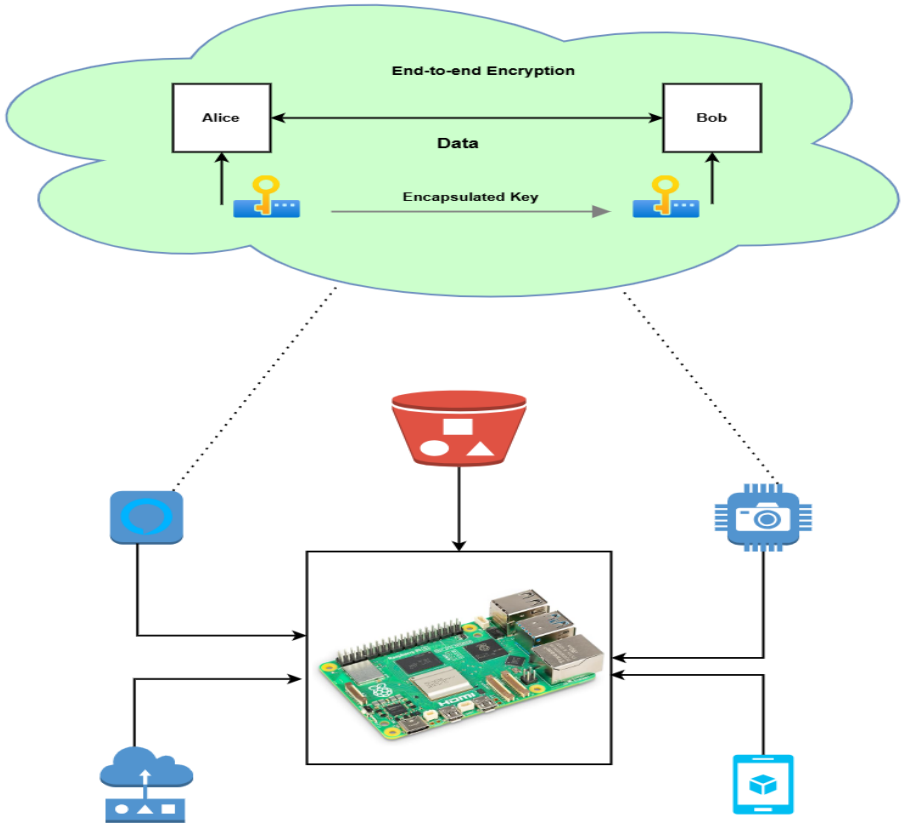


Diagram (Proposal 2)



Raspberry Pie's Interface

Rasberry-pi-hub-01

List devices

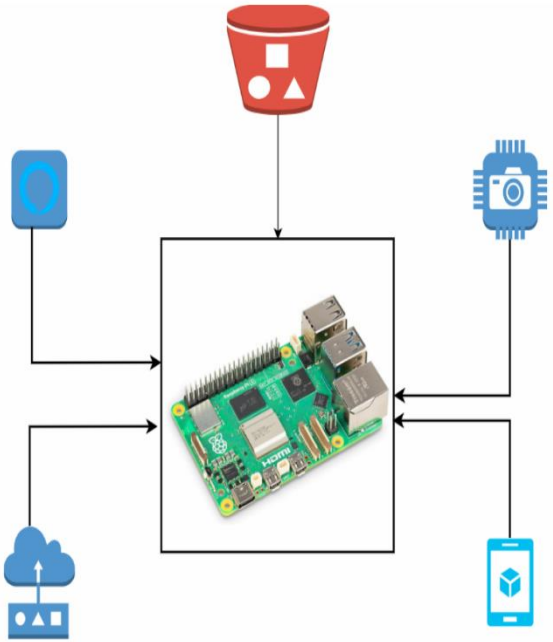
Configure Devices

Rasberry-pi-hub-01

Connected Devices

- IoT-camera-01
- IoT-camera-02
- Samsung-01
- Iphone-01
- IoT-camera-03
- IoT-camera-04
- Alexa-01
- IoT-camera-04

Rasberry-pi-hub-01



What to be done

- Implementing more lightweight (speed and energy) ciphers for data encryption (Noum Cipher?)
- Developing compliance framework

What we learned

- **Lessons learned:** Interdisciplinary Collaboration
- **Issues with existing drafts/RFCs:** Insufficient Guidance for IoT, Scalability and Performance
- **New implementation guidance?** Algorithm Selection, Security vs. Performance Trade-off
- **New feedback to take to WG?** Enhanced IoT Focus, Benchmarking and Standards
- **New work to take to WG?** Development of IoT-Specific PQC Protocols, Research into hybrid approaches

Wrap Up

Team members:

1- Elias Hassani

2- Vasif Nawaz

First timers @ IETF/Hackathon: Elias Hassani, Vasif Nawaz