A Real-World Analysis of Lightweight Cryptographic Algorithm ASCON

NIST Lightweight Cryptography Workshop 2022

Jeffrey Avery, PhD

Agenda

- Background and Introduction
- Motivation and Problem Statement
- Experimental approach
- Results
- Discussion
- Summary, Next Steps, Conclusion

Introduction and Background

- Cyber-physical systems are growing exponentially
- Data sharing introduces new threat landscape
- Low SWaP-C devices cannot implement common cryptographic algorithms
  - This influenced lightweight cryptographic algorithms
- Literature lacks metrics on real world applications of lightweight crypto algorithms

https://news.usni.org/2022/04/06/panel-pentagon-needs-to-be-clearer-on-goals-for-jadc2Panel: Pentagon Needs to be Clearer On Goals for JADC2 - USNI News

Early implementation and analysis leads to future preparedness and better adoption.

Motivation

- Low SWaP-C/embedded device communication
  - IP/Internet backbone
  - Message Brokers
- Efficient data sharing is key, but data protection is paramount
  - IoT and Ransomware
  - IoT as a pivot point

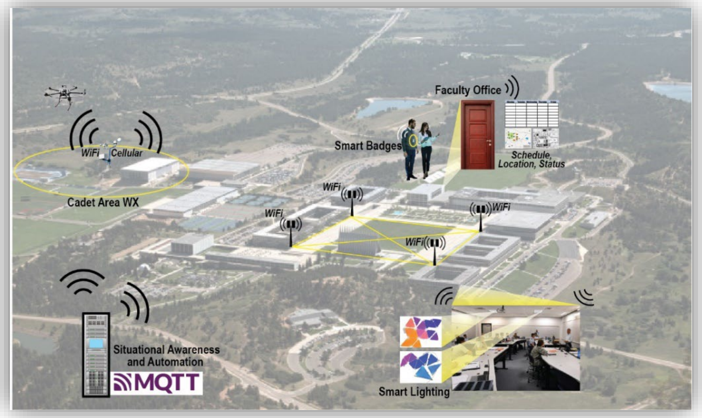
JADC2 and IoT require changes to cryptographic algorithms to support domain.

Lightweight Cryptographic Algorithm: ASCON

- Publicly available algorithm that provides both confidentiality and message integrity (Authenticated encryption with associated data (AEAD) and hashing)
- Finalist in the Competition for Authenticated Encryption: Security, Applicability and Robustness (2014 – 2019)
- Finalist in NIST Lightweight Cryptography Competition
- Post quantum capabilities and consistently a top performing algorithm across various benchmarks

Experimental Approach

- United States Air Force Academy Internet of things Development environment
  - Raspberry Pi devices
    - Raspberry Pi Zero with 1GHz, single core SoC, 512 MB RAM
    - Raspberry Pi 3 with 1.2 GHz, quad core SoC, 1 GB RAM
    - Raspberry Pi 4 with 1.5 GHz, quad core SoC, 1GB RAM
  - Weather data messaging system
  - Personnel location tracking system



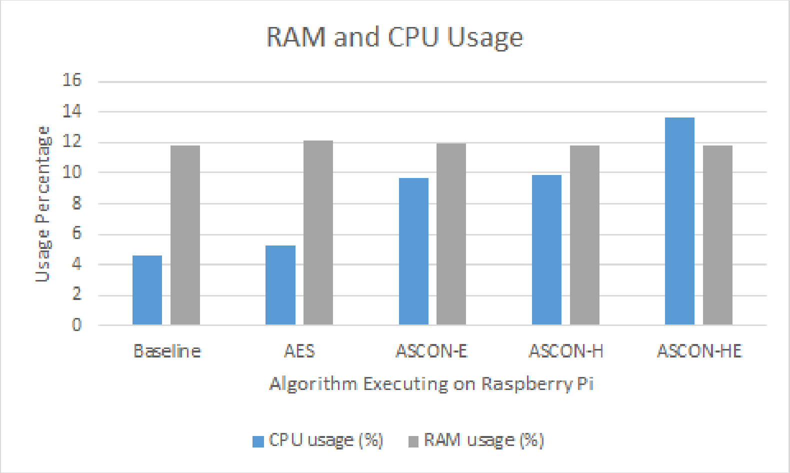
- Long running experiments performed over 30 min – 12 hours
  - RAM
  - CPU
- Roundtrip time experiments evaluate time for message sharing, encryption and decryption for different size messages

Experimental Results

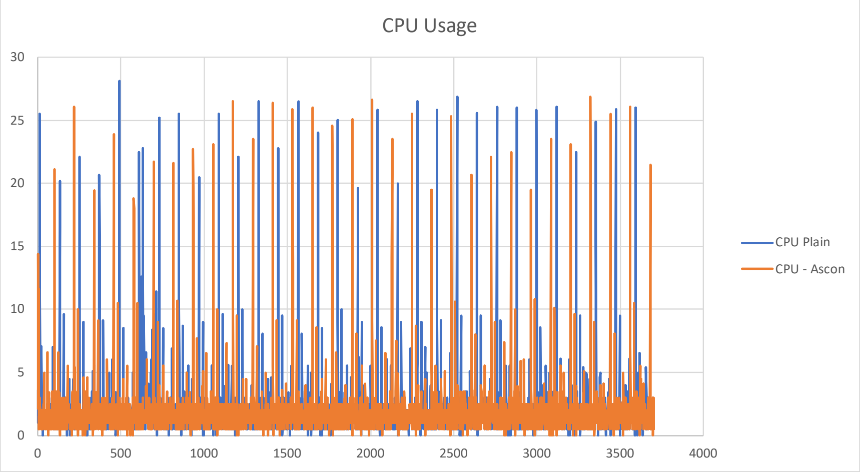
NORTHROP GRUMMAN

	Average time per trial		
Message length (bytes)	No encryption	ASCON	AES
10	2.67E-06	1.85E-04	6.96E-06
100	2.89E-06	3.61E-04	6.63E-06
500	2.42E-06	7.76E-04	5.30E-06

Experiment 1: Message length evaluation



Experiment 2: AES & ASCON Comparison



Experiment 3: 30 min ASCON CPU Usage

Discussion

- Performance was as expected for ASCON compared to AES
  - High degree of software design in AES and relative infancy of ASCON
  - Additional resource constrained devices will not be able to run AES without additional modifications
- Lightweight cryptographic standards provide necessary antispoofing capabilities
  - MQTT does not natively include this as a capability

Additional analysis and application of LWC algorithms will provide necessary confidentiality and availability to realize a secure JADC2 comms infrastructure.

NORTHROP GRUMMAN

Next Steps

- Perform additional security evaluations
  - Currently, cadets are evaluating spoofing capabilities and hardening their environment using ASCON to drive both confidentiality and integrity
- Implement additional lightweight cryptographic algorithms in the environment
  - This will provide additional measures of performance and flexibility to choose algorithms for different scenarios
- Key management
  - Additional experimentation to evaluate key management approaches and their impact on low SWaP-C devices

Summary and Thanks

Special thanks to the NIST LWC Project Team!

Samuel Dick, Bryson Fraelich, William Duran, Andrew Lee, Agustin Sullivan, Zane Maechalke, Maj. Bobby Birrer

Dr. Steve Fulton, Eric Payne, James Cantrell

Northrop Grumman Corporation

United States Air Force Academy