Analysis of Practical Application of Lightweight Cryptographic Algorithm ASCON

Jeffrey Avery, PhD, Bryson Fraelich, William Duran, Andrew Lee, Agustin Sullivan, Zane Mechalke, Maj. Bobby Birrer, Sameul Dick, Jordon Cochran

Abstract

Cyber physical systems and embedded devices have become integral to our everyday lives. Internet of Things (IoT) capabilities continue to advance and are being applied to technology domains such as military, utility and healthcare. The criticality of the data within these domains requires strong security and integrity. Our research provides a novel evaluation of the lightweight cryptographic algorithm ASCON to real world applications. We evaluate the impact of ASCON using an IoT environment located at the United States of Airforce Academy (USAFA) We found that ASCON performs as expected when applied to the MQTT message protocol to encrypt messages without inhibiting information sharing but providing the necessary security and integrity. We show that ASCON is comparable to performance measures of AES but with a smaller memory footprint. This is significant in that it translates to broader applications and opportunities where compact systems are required. This is the first evaluation of ASCON in real world applications.

Introduction

Protecting cyber physical systems and the data they process is key to enabling more connection and integration among the tools available to critical infrastructure and warfighting systems. Enabling this capability will provide necessary data to the personnel and devices at the right time and place of need. Efficient data protection must be in place to properly and adequately protect the shared data. Encryption and decryption are the primary data protection approach, but we must evaluate the performance, speed, and the strength of the algorithms. This evaluation is vital to seek the next-generation cryptographic algorithms that can withstand the resourceful quantum-computing adversaries. This adversarial concern is a catalyst to increase the pace when it comes to applying post-quantum computing (PQC) algorithms to our systems, especially embedded systems that will be used across a military Joint All-Domain Command and Control (JADC2)[1] battlefield.

The determined adversaries have utilized the following tactics, techniques and procedures in their recent attacks on IoT systems:

- Spear phishing to obtain initial access to the organization's IT network before pivoting to the IoT network
- Deployment of commodity ransomware to encrypt data for impact on both networks

[1] For more background information on JADC2, see "Joint All-Domain Command, Control Framework Belongs to Warfighters," https://www.defense.gov/News/News-Stories/Article/Article/2427998/joint-all-domain-command-control-framework-belongs-to-warfighters/

- Connecting to internet-accessible programmable logic controllers (PLCs) requiring no authentication for initial access
- Using commonly used ports and standard application layer protocols to communicate with controllers and download modified control logic
- Use of vendor engineering software and program downloads
- Modifying control logic and parameters on PLCs

There is increasing demand to share data among embedded IoT devices and environments, but this needs to be done efficiently, securely, and privately. Current encryption algorithms that execute on our laptops and servers have too large a memory footprint to execute in small size, weight, power, and cost (SWaP-C) devices (Didla, 2008). This is what influenced a new class of cryptographic algorithms that are lightweight, secure and provide integrity guarantees (Adomnicai, 2018). Due to their low size, weight, and power (SWaP), most IoT devices rely on encryption present in network protocols, implement obfuscation-like encryption or have no encryption at all (Atwady, 2017). This leaves these devices vulnerable to exposing data such as passwords and serve as a starting point for lateral movement to attack other network devices.

The purpose of this study is to evaluate the performance and applicability of lightweight cryptographic algorithms to embedded devices in a representative environment. Specifically, we evaluate ASCON which is one of the NIST lightweight cryptographic algorithm finalists to analyze its impact on performance, implementation ability, and observe how it improves data security and integrity. We will evaluate the algorithm and device performance, including size, and execution speed in practical application. Our results will help inform NIST in their selection of the best-of-breed for the lightweight cryptographic standard that will have a key role in future civilian and military applications including autonomous vehicles, weapons' systems and sensors. Having the ability to send and receive encrypted data on these platforms will provide an advantage against adversaries.

Key research contributions:

1. The real-world application and analysis of ASCON – this work is one of the first practical applications of ASCON in a scenario where measurable data and results have been obtained.
2. First analysis of ASCON with MQTT – we provide an analysis of ASCON's application to the MQTT protocol by evaluating performance impact and observing secure data transfers.

The remaining sections in this research are organized as follows: Background provides an overview of lightweight cryptographic algorithms as well as embedded device infrastructure and communication methods, Related Work discusses current evaluations of ASCON, Approach details more about the Internet of Things (IoT) experimental environment used to evaluate ASCON, Results present our findings as we applied ASCON to nodes within the IoT environment, and Discussion expands the application of

lightweight crypto to address parallels to mission critical DoD systems and suggests future work within the space of lightweight crypto. Finally, our research discussion ends with our Conclusion.

Background

The pervasive nature of embedded devices has changed the way society uses technology. The ability to connect and share data has revolutionized a number of domains, but there is a need to ensure data confidentiality and integrity is maintained. This requires a closer evaluation of how data is shared between embedded devices and how this data is protected.

Embedded device communication

In the deployment of the Internet of Things development environment, the USAFA chose to use MQTT (formerly known as Message Queuing Telemetry Transport as it was originally conceived at IBM). In July, 2016, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) approved release of MQTT Version 3.1.1 after balloting through the Joint Technical Committee on Information Technology (JTC1) and it received the designation: ISO/IEC 20922. This growing industry standard is supported by the OASIS open standards consortium with updates and specialized versions, such as the MQTT-SN that provides improved support for distributed sensors. The MQTT transport standard provides a lightweight, publisher-subscriber messaging approach. It provides a simple application layer protocol for remote, low SWaP devices with minimal bandwidth. MQTT uses a broker and client approach where clients can publish, subscribe or both, see Figure 1. One of the features of MQTT is a configurable Quality of Service (QoS) method for reliable message delivery in a crowded communication environment or situations with intermittent connections. Messages can be sent at most once, at least once, or exactly once. If a subscribing client goes offline, brokers can buffer messages and send them if the client comes back online. This feature is very useful in dense communications environments or when clients are moving among radio opaque obstacles that may obscure receivers and make services intermittent.

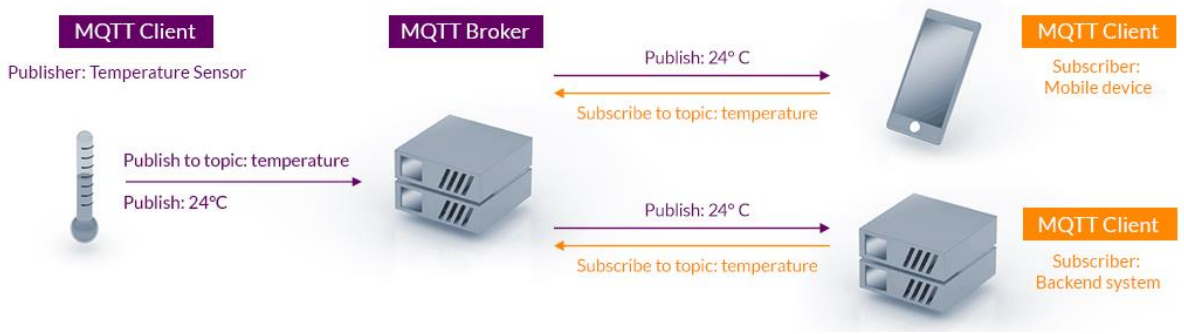

Figure 1 – MQTT infrastructure provides devices the ability to communicate without having to store large volumes of previous messages. MQTT is a lightweight message broker and widely used to connect embedded Internet of Things network devices.

MQTT does not inherently include cryptographic methods for message integrity, source authentication or confidentiality of the message in transit. Most MQTT products allow Transport Layer Security (TLS) as an option. Practical applications may find that TLS imposes inconvenient burdens on messages in an IoT environment. The NIST Lightweight Cryptographic standard would complement the MQTT and similar IoT message transfer standards by providing those cryptographic methods for integrity, authentication and confidentiality.

The US Air Force Academy (USAFA) Internet of Things (IoT) test bed environment includes a central MQTT broker service with a variety of publisher and subscriber devices. One of the devices to support the network function of providing the availability of faculty is a Bluetooth®-enabled device used as Smart Badges, see Figure 4. While the faculty member carries this token, the network identifies where the faculty member is and shows an estimate of how soon the faculty member will arrive back at the office location to meet for the requested student consultation. This information is displayed outside the office on an E-link Display as a subscriber to the information and may be available through the student's personal device.

Data protection

The lightweight cryptography research push was started by NIST in 2013 as the rise of small, resource constrained devices grew. A solicitation for submission was created and algorithms were evaluated based on performance metrics such as power consumption, latency and throughput, software metrics such as number of registers and bytes of RAM/ROM required during execution as well as hardware metrics of look-up tables, flip-flops and multiplexers required for the algorithm to execute (McKay, 2016). Numerous different algorithms were proposed including lightweight hash functions, lightweight message authentication codes and stream ciphers.

Another type of algorithm that was proposed called Authenticated Encryption (AE) or Authenticated Encryption Schemes with Associated Data (AEAD) schemes as part of the Competition for Authenticated Encryption: Security, applicability and Robustness (CAESAR) provides the ability to ensure confidentiality as well as validate message integrity. These algorithms have applications in several different scenarios such as unmanned aerial systems, IoT devices as well as in other protocols such as MQTT for message sharing (Driscoll, 2018) (Nabeel, 2021) (Amnalou, 2020). Within the AE space, algorithms have different constructs. This research presented in this paper will focus on the ASCON algorithm, which is a sponge-based AE algorithm that has properties that provide low latency and high throughput (Yalçın, 2012). ASCON is one of the NIST finalists currently in its evaluation window (NIST, 2021).

Related works

The ASCON AEAD algorithm is a leading choice for lightweight applications needing symmetric cryptography. This algorithm is designed for low memory footprints in hardware and software while maintaining speed and security. As an AEAD algorithm,

ASCON includes both the encrypted cipher text as well as associated data that is used to verify the integrity of the message that was sent. This guarantee of both confidentiality and integrity as a lightweight cryptographic algorithm provides the ability for low SWaP pervasive devices to secure data and communications, which need to be guaranteed (McKay, 2016).

Prior work to analyze ASCON has focused on security analysis and metrics. Measuring the amount of randomness or entropy in ciphertext output, differential analysis of the ASCON sponge-based algorithm to identify faults in its construction, cube attacks and other cryptanalysis have been performed on the algorithm (Dobraunig, Cryptanalysis of ascon., 2015) (Joshi, 2021) (Li, 2017) (Tezcan, 2016). This analysis resulted in mixed feedback, with some attacks being identified as well as mitigations being suggested that do not significantly alter the performance of the algorithm (Adomnicai, 2018).

These discussions and research are important to consider before applying ASCON to pervasive IoT devices and protocols. Our research provides context into **applying ASCON to real world pervasive devices**, the MQTT protocol and three applications to measure its' impact on performance and security of the data.

Approach

Our research environment at USAFA includes a progressive Internet of Things (IoT) development and test environment as shown in Figure 2.

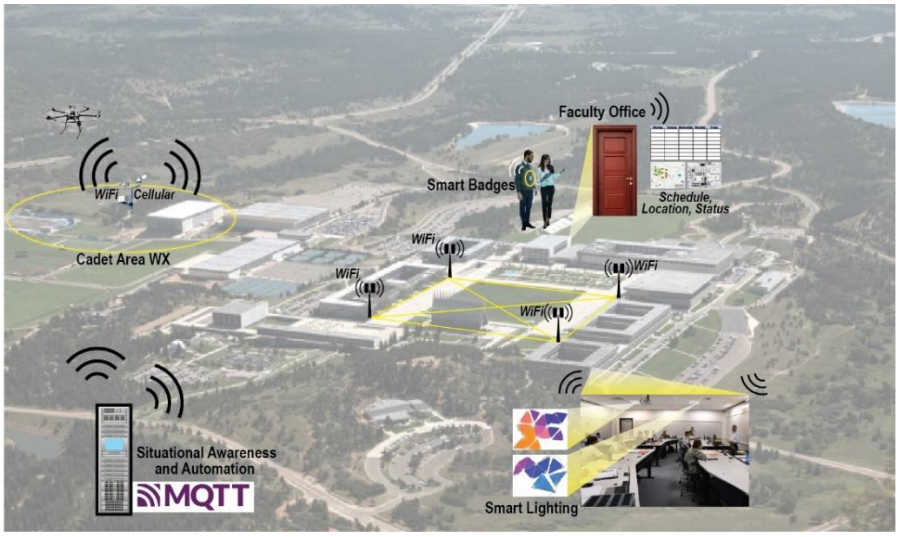

Figure 2 – The USAFA Internet of Things (IoT) Environment spans the entire USAFA campus. It includes both cellular and Wi-Fi connected devices that communicate via MQTT messaging protocol to provide real-time weather data and personnel tracking.

We conducted a series of experiments to evaluate ASCON's performance in several of these environments and measure its impact on overall system performance. The real-world applications included a test bench of Raspberry Pi devices connected via Wi-Fi located in a controlled lab environment, a weather data messaging system, and a personnel location tracking system. We first tested the general performance of ASCON

in the test bench environment, then applied the algorithm to the weather and personnel tracking system. Additional explanation of the weather data messaging and personnel tracking systems is provided below.

Controlled Lab Experimentation Infrastructure

Initially, algorithms were evaluated within a controlled test bench comprised of Raspberry Pi devices. Specifically, Raspberry Pi devices were used in all experiments within the test bench. We evaluated algorithm performance using a real-world message broker, MQTT, that is used in many IoT networks to send and receive short messages. To reiterate, the **MQTT natively does not encrypt data being sent/received.**

Experiments were run on a Raspberry Pi Zero with a 1 GHz, single core CPU and 512 MB of RAM. Raspberry Pi 3 and 4 sets were also tested. Experimental setup included two Pi's connected via Wi-Fi. The results were collected based on a roundtrip timing approach where the times reported are the total time to send a message, receive the message, decrypt, re-encrypt, send back, and finally decrypt the message. This roundtrip time measurement provides an exemplar use case to measure the impact of these algorithms on IoT device communications.

Messages are comprised of a randomly generated string of characters. The message lengths of 10, 100, and 500 bytes were determined using common message lengths within the test bench setup.

Weather Messaging System

The weather messaging system provides real-time weather metrics/readings of an outdoor drone airfield located at the US Air Force Academy. The weather messages vary in length and provide insight into potential flying conditions. The weather data messaging system is critical to the USAFA given their real-time requirement for localized weather awareness and understanding to inform key and essential flight aviation operations. Given the USAFA campus is located at the foot of the Eastern Range of the Rocky Mountains, large variances of campus weather conditions as compared to weather reported at other nearby airfields requires additional monitoring capabilities and reporting performed using sensors located directly at the Stillman field drone launch area. Key weather data (wind speed, direction, temperatures and pressure) from numerous sensors is available to inform faculty and students of the necessary, safe conditions at their aircraft launch and recovery. Figure 2 provides an OV-1 model style overview of the IoT testbed at USAFA that includes the weather station for drone operations. Exact locations are not represented in the figure.

The weather station located in the drone airfield publishes real time weather data to an MQTT server topic. This data is sent and received as plain text and can be viewed over the air in plain text. The MQTT server stores these messages for a configurable amount of time along with metadata including timestamps associated with the data with no data validation, integrity checks or authenticity checks. Within the USAFA campus,

E-Iink displays are powered by Raspberry Pi devices that subscribe to these topics and display the stored weather messages. This provides cadets and instructors with real time weather measurements, giving them the ability to determine if conditions are safe and suitable for flying. Figure 33 below provides the general workflow for the weather messaging system.

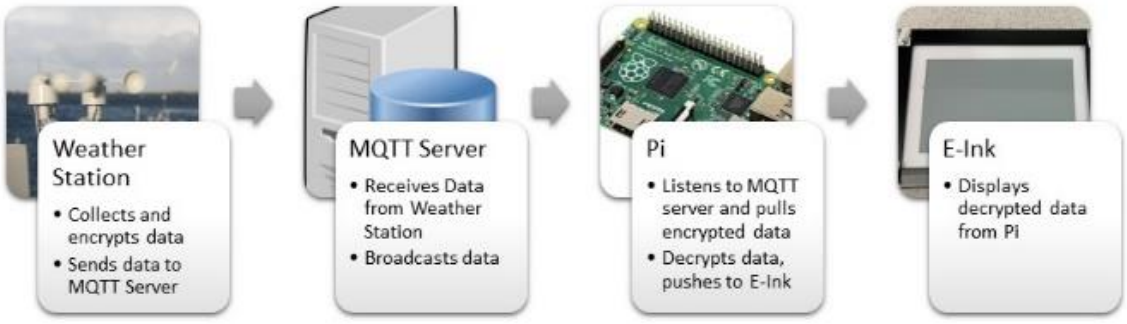

Figure 3 – The weather messaging system includes four components. The weather station itself collects real-time measurements on the airfield and publishes this data to the MQTT server. Raspberry Pi devices subscribe to these messages and display them using E-Ink.

Due to the embedded nature of the sensors and receiving Raspberry Pi's in this system, traditional encryption techniques are not suitable. Sending and receiving plaintext weather messages also provides an attack surface that an adversary could exploit, sending false weather data or sending malicious commands that could exploit vulnerabilities in the MQTT server or the subscribing devices (Pasknel, 2017 and Calabretta, 2018). Encrypting these messages from the various sensors located at the airfield provides and authenticating them provides greater security by preventing false or malicious messages injected into the MQTT traffic from successfully executing or being delivered to the destination Raspberry Pi devices.

We evaluate the impact of ASCON over the course of a 12-hour test where a *cron* job takes measurement ever half second. These measurements include CPU and RAM utilization as data is sent, received and decrypted. We also captured .pcap files of the traffic as it was delivered to the Raspberry Pi from the weather sensors to observe the encrypted packets.

Location Tracking System

The location tracking system provides location information for individuals wearing a GPS enabled embedded device as shown in Figure 4. USAFA professors wear these embedded Wi-Fi-enabled smart badge devices to track their location around campus. This system provides tracking and situational knowledge of the availability and proximity of instructors for students who are seeking consultation. Messages include the time stamp and location in latitude and longitude and this data is reported on a geospatial display. The data sent back to the display is received in plaintext without any encryption or data authentication. Encrypting these messages from the location tracking sensors

to the central display board preserves the integrity of the tracking system. This prevents spoofing attacks that could falsify the location of professors.

Figure 4 – The smart badge is worn by USAFA professors to provide students with real-time location data. The location tracking system allows students to observe when professors are close to their office in the event they are unreachable or absent for scheduled appointments.

Results

To evaluate ASCON, we execute a series of experiments in the various systems described in the Approach section. These experiments show the impact of ASCON on system performance as messages are shared over the MQTT message broker. Initial results in Table 1 below compare the timing metrics for encrypting various length messages using ASCON and AES compared to a control experiment, which does not apply any encryption. These measures were taken within the controlled lab setting that has a series of Raspberry Pi Zero devices connected via Wi-Fi. For each message size, we execute 20 roundtrip message transmit and receive instances and then average these 20 runs to provides the results in Table 1 (where the roundtrip times are the total time to send a message, receive the message, decrypt, re-encrypt, send back, and finally decrypt the message). The values below suggest AES provides faster encrypt and decrypt performance. These values are due to AES' superior implementation, but **AES is limited to execution on devices with more than 512 bytes of memory (Toshiko, 2017).** For smaller devices, this is not a viable encrypt/decrypt approach. This experiment also showed that lightweight cryptographic algorithms are within the acceptable threshold for cyber physical systems and real-time systems that we often find in weapon systems.

	Average time per trial (seconds)		
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

Table 1 – Execution run times for a control execution with no encryption, AES encryption and ASCON encryption. Values are the average of 20 runs to perform a roundtrip send and receive of a message between two Raspberry Pi's using MQTT.

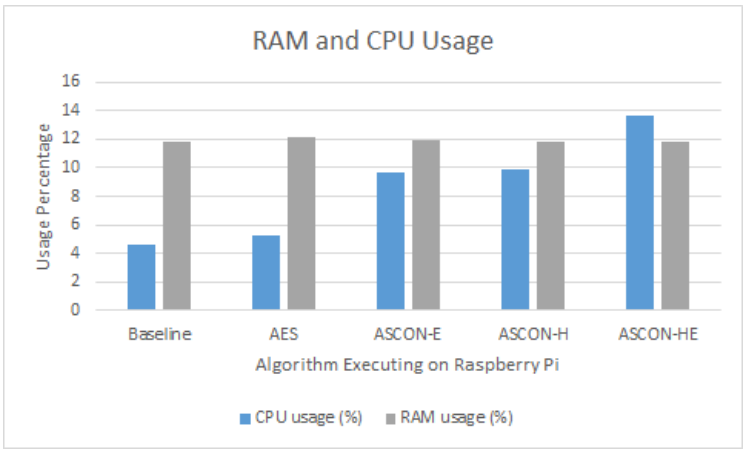

Figure 5 – RAM and CPU usage for a vanilla Raspberry Pi compared to a Raspberry Pi executing AES as well as the three different types of the ASCON algorithm.

The ASCON algorithm is comprised of hashing, encryption and both hash and encrypt execution. This graphic displays the average usage percentages across 20 points of measurement during the experiment. Each point of measurement is collected every half second. Figure 5 above shows ASCON's execution in terms of both CPU and RAM percentage-use compared to AES and the baseline control, i.e., an idle Raspberry Pi Zero. The comparison shows that RAM usage, across all execution is comparable with AES having negligibly higher usage. This could be due to noise with other processes executing in the background.

The CPU usage does differ across each these algorithms. AES fine-tuned implementation is verified as the increase in CPU usage during AES execution is less than 2% CPU usage increase compared to baseline (i.e., idle Raspberry Pi execution). ASCON utilized more CPU to execute across all three modes of execution (encryption, hash, hash and encryption). While these initial results would suggest AES over ASCON, the size of AES software precludes it from being applied to embedded systems with SWAP-C profiles. This also suggests there are optimizations that should be evaluated for ASCON and additional measurements to further validate these optimizations.

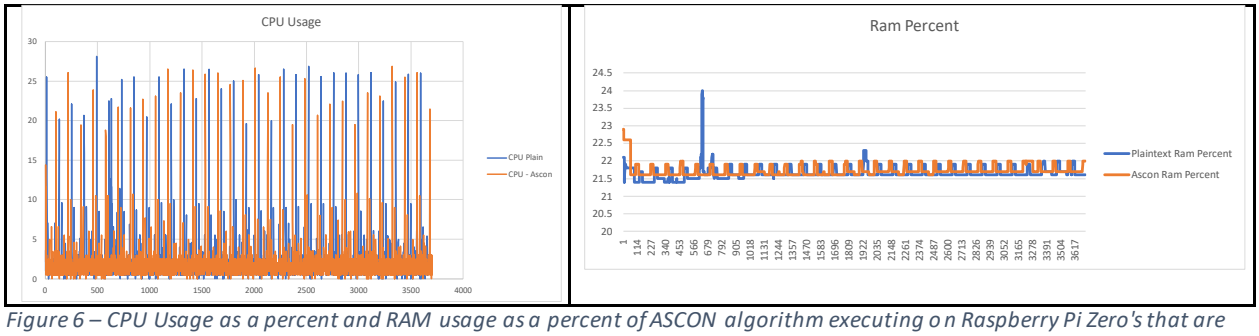

Figure 6 – CPU Usage as a percent and RAM usage as a percent of ASCON algorithm executing on Raspberry Pi Zero's that are part of the Weather Messaging station. These measurements are over a period of 30 minutes, with measurements taken every half second.

Figure 6 shows how ASCON impacts performance over a 30 minute timespan where CPU and RAM usage are presented as a percentage. This long running experiment suggests that ASCON does have an impact on performance, but this impact does not seem to be observable in system execution times/operation.

Discussion

The ASCON lightweight cryptographic algorithm provides cryptographic properties to embedded devices that otherwise have unencrypted or poor security. Our evaluation shows that ASCON, while not as optimal as AES, performance within expectation when executing on IoT devices. Additional experimentation to show specific security measurements such as entropy and impact of key exchange within the system would provide additional metrics that should be collected on ASCON.

As follow-on research in this project, the USAFA cadet testers will use ASCON on an FPGA to execute the algorithm as binary instructions instead of a runtime executable. We expect this will drastically improve ASCON performance. Those results are not available for this paper, but would be shared with the NIST if available at presentation time.

Use of the NIST Lightweight Cryptographic standard for authentication, integrity and confidentiality provide valuable cybersecurity capabilities not natively present in the MQTT protocol. By confirming the authentication of a publishing device, such as the Smart Badge, we provide protection against spoofing attempts by unauthorized publishers. By checking the integrity of messaging from those publishers, the cryptographic hash confirms the message arrived whole and unaltered by any potential malicious manipulation. And the confidentiality reduces the potential for exploitation of the information for other purposes than those designed in the system.

In addition to the IoT test environment at the USAFA, ASCON and other light weight cryptographic algorithms have a number of applications. These same Lightweight Cryptographic capabilities used on the USAFA IoT test bed have direct value to a variety of critical infrastructure and military Platform Information Technology applications. For example, when an aircraft returns from a mission and may need to be quickly prepared for a follow-on mission, there are several functions that must happen quickly and securely. Previous mission data must be captured (off-loaded) for analysis of mission performance. Information about success in targeting or weapons' employment effects may have a significant impact on follow-on missions. Faults and subsystem performance data is needed by maintenance crews to guide rapid repairs and assessment of the vehicle's readiness to return to operations. When a new mission is being prepared, mission data, weapon specific configurations and situational awareness data may be uploaded. A 'hot swap' rapid turn-around of an aircraft for follow-on missions may include not shutting down the engines while the aircraft is refueled and rearmed and may be only minutes in time on the ground. This brevity of connectivity to the vehicle drives a need for secure data sharing between ground

support equipment and the aircraft while both the embedded aircraft systems and the ground support equipment may be constrained in size, weight, and power. The NIST Lightweight Cryptographic standard would provide an important improvement in the weapon system's cybersecurity.

Conclusion

ASCON's lightweight cryptographic algorithm provides cryptographic properties to embedded devices that otherwise cannot execute standard cryptographic algorithms. We evaluate a series of experiments to execute ASCON in the USAFA IoT environment, which includes a controlled test bed with Raspberry Pi Zero devices, a weather messaging system and a smart badge system that communicate via MQTT, cellular signals and Wi-Fi. Our results show that while AES does perform efficiently, ASCON provides comparable performance that is within threshold values from DoD embedded systems. Additional work includes other measurements to evaluate security implications as well as other performance measures that can be collected in the IoT test environment.

References

Adomnicai, A. F. (2018). Masking the lightweight authenticated ciphers acorn and ascon in software. . *Cryptology ePrint Archive.*

Amnalou, S. A. (2020). Lightweight security mechanism over MQTT protocol for IoT devices. *Int. J. Adv. Comput. Sci. Appl*, 202-207.

Atwady, Y. A. (2017). A Survey on Authentication Techniques for the Internet of Things. *Proceedings of the International Conference on Future Networks and Distributed Systems.* New York: Association for Computing Machinery.

Didla, S. A. (2008). Optimizing AES for embedded devices and wireless sensor networks. *TridentCom.*

Dobraunig, C. E. (2015). Cryptanalysis of ascon. *Cryptographers Track at the RSA Conference* (pp. 371-387). Springer.

Dobraunig, C. E. (2016). *Ascon v1. 2. Submission to the CAESAR Competition.*

Driscoll, K. (2018). Lightweight crypto for lightweight unmanned arial systems. *Integrated Communications Navigation, Surveillance Concerence (ICNS)* (pp. 1-15). IEEE.

Gross, H. W. (2015). Suit up!--Made-to-Measure Hardware Implementations of ASCON. *Euromicro Conference on Digital System Design* (pp. 645-652). IEEE.

Joshi, P. &. (2021). SSFA: Subset fault analysis of ASCON-128 authenticated cipher. *Microelectronics Reliability, 123*.

Li, Z. D. (2017). Conditional cube attack on round-reduced ASCON. . *Cryptology ePrint Archive.*

McKay, K. B. (2016). *Report on lightweight cryptography (No. NIST Internal or Interagency Report (NISTIR) 8114 (Draft)).* National Institute of Standards and Technology.

Nabeel, N. H. (2021). Security Analysis of LNMNT-LightWeight Crypto Hash Function for IoT. *IEEE Access*.

National Institute of Standards and Technology (NIST) (2021). *Lightweight Cryptography Standardization: Finalists Announced*. https://csrc.nist.gov/News/2021/lightweight-crypto-finalists-announced.

Tezcan, C. (2016). Truncated, impossible, and improbable differential analysis of ASCON. *Cryptology ePrint Archive.*

Toshihiko, O. (2017). *Lightweight Cryptography Applicable to Various IoT Devices.* NEC Technical Journal. https://www.nec.com/en/global/techrep/journal/g17/n01/170114.html.

Yalçın, T. &. (2012). On the implementation aspects of sponge-based authenticated encryption for pervasive devices. *International Conference on Smart Card Research and Advanced Application* (pp. 141-157). Berlin, Heidelberg: Springer.