Poster Abstract: Securing Edge-Based Real-Time IoT Systems

Dongha Kim
dongha@asu.edu
Arizona State University, USA

Hokeun Kim
hokeun@asu.edu
Arizona State University, USA

ABSTRACT

The advent of the Internet of Things (IoT) has led to an increased demand for security and real-time guarantees in distributed embedded systems comprising the IoT. Securing edge-based systems with limited resources can be especially problematic due to challenges in adapting traditional network security protocols. In this work, we introduce two methods to provide security guarantees in resource-constrained devices-based ioT systems. As a case study, we propose an integration of Secure Swarm Toolkit (SST), an open-source framework for IoT security, with Lingua Franca (LF), a software platform for concurrent and time-sensitive applications. We report preliminary results on our work-in-progress implementation and experiments, followed by concrete future research plans.

KEYWORDS

Security, Distributed embedded systems, Real-time systems, IoT

ACM Reference Format:
Dongha Kim and Hokeun Kim. 2023. Poster Abstract: Securing Edge-Based Real-Time IoT Systems. In *The 21st ACM Conference on Embedded Networked Sensor Systems (SenSys '23), November 12–17, 2023, Istanbul, Turkiye.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3625687.3628408

1 INTRODUCTION

Communication security is a crucial element when designing real-time distributed systems, including the IoT. However, many newly developed research frameworks for the IoT do not always prioritize security [3], rendering research frameworks not suitable for commercial use. Furthermore, many IoT frameworks do not provide enough security options for resource-constrained devices.

The key security guarantees for distributed embedded systems or IoT include cryptographic key distribution, authentication, authorization, data confidentiality, and integrity. While TLS, the most widely used security solution for the Internet, provides the aforementioned security guarantees but authorization, TLS does not support resource-constrained embedded devices of the IoT. Data Distribution Service (DDS) [11] is used by distributed embedded systems, including ROS2 and AUTOSAR, however, DDS still suffers non-determinism in real-time embedded and IoT systems [2].

To secure existing real-time IoT frameworks, in this abstract, we introduce our work-in-progress methods to secure time-sensitive applications running on edge-based IoT environments.

SenSys '23, November 12–17, 2023, Istanbul, Turkiye

ACM ISBN 979-8-4007-0414-7/23/11…$15.00
https://doi.org/10.1145/3625687.3628408

2 BACKGROUND

This section discusses technologies used to prototype our approach.
Secure Swarm Toolkit (SST) [6] is an open-source framework for authorization and authentication using a key element called *Auth* [7]. Auth is an edge-based local authentication and authorization entity that manages and distributes cryptographic keys for its local registered IoT entities. SST supports scalability and heterogeneity with a C language API [4], a widely used language for many embedded systems with resource-constrained devices.
Lingua Franca (LF) is a software platform for concurrent and time-sensitive applications, based on *reactors* [9]. LF supports distributed execution environments called *federated execution*. LF generates code for distributed reactors called *federates* and binaries deployed on distributed machines. *Runtime infrastructure (RTI)* in LF coordinates time advancements and communication among federates. LF guarantees determinism critical for real-time IoT applications while maintaining performance [10] with lightweight computation.

3 APPROACH

We apply two methods to secure LF federated execution: (1) HMAC-based authentication and (2) LF-SST integration.

The baseline implementation of LF's federated execution lacks authentication and encryption mechanisms to prevent adversarial federates from joining the federation or sending malicious messages (e.g., bad timing messages or sensor data). As shown in Figure 1a, in the original protocol, the RTI only checks the federation ID[1] sent in plaintext from federates for authentication. Thus, any malicious federate can eavesdrop on the federation ID and join the federation.
Preliminary HMAC-based Authentication: First, we applied secure authentication to the baseline LF protocol when the federate tries to join the federation by connecting to the RTI. We added a simple 3-way handshake with an HMAC[2] authentication process, shown in Figure 1b. To prevent the malicious federate from joining the federation, the RTI and the federate use a *federation ID*, which was shared at bootstrapping, as a secret key, creating the HMAC. The federate and RTI each create a random eight-byte nonce, challenges, and responses to each other, preventing replay attacks. This three-way handshake provides secure authentication between two nodes, and this may be applied when confidentiality is less important. For example, the sensor data of a thermostat can be in plain text, but the sensor should be surely authenticated.
Work-in-progress LF-SST integration: The next step is to add authentication, authorization, key distribution, and data protection using SST. When federates request a secure communication session with the RTI, the Auth should distribute session keys after performing authentication of each federate and the RTI. We anticipate challenges during the integration of LF and SST, especially for the

[1] A unique identifier in string for each federation.
[2] Key-hashed message authentication code.

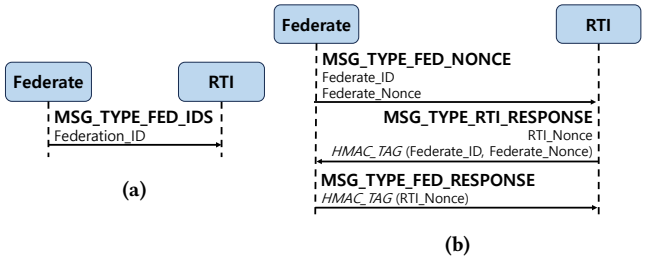

Figure 1: (a) Current LF protocol sending the federation ID in plaintext (b) 3-way handshake including HMAC tags for authentication, using the federation ID as an HMAC key.

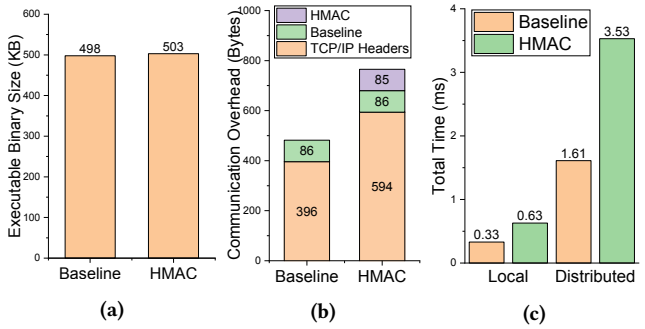

Figure 2: Comparison between the *baseline LF* and *LF with HMAC-based authentication*. (a) Executable binary sizes in KB. (b) Communication overheads for initial authentication. (c) Total execution times of initial authentication.

encryption and decryption of messages. For example, LF's C implementation of handling network messages involves multiple reads due to the current design of the RTI-federate message protocols.

Another challenge is that the size of encrypted messages may leak information about the message types, making the communication vulnerable to side-channel attacks where the attackers guess the current state of an LF application. To address this, we apply padding to the shorter messages when encrypting them to make the message sizes identical, obfuscating the information of types of messages. We also expect our LF-SST integration will address the challenges of resource constraints, fault tolerance, support of pub-sub communications, and data-centric security in the IoT [5, 6].

4 EVALUATION

Preliminary Evaluation: We performed experiments using our HMAC-based authentication under two environments: (1) locally on a laptop[3] running RTI and federates, and (2) in a distributed environment with the laptop running RTI and two Raspberry Pis[4] running federates, connected to the same WiFi router. We measured the overheads in binary sizes, communication, and execution time. As shown in Figure 2a, the binary size increased by 5 KB with the HMAC approach, including the OpenSSL library. We measured the number of bytes sent over the network using Wireshark, including the 66-byte-long TCP/IP headers. The communication overhead of the HMAC approach was 283 bytes, as shown in Figure 2b. We measured the average execution time for the federate to join the federation out of 40 runs. As shown in Figure 2c, the HMAC approach's initialization took 1.92 ms longer on average in the distributed environment. Our HMAC-based approach only incurs a relatively low overhead while enabling authentication.

[3]LG Laptop with Intel i7 and 16 GB RAM running Ubuntu 20.04.
[4]Raspberry Pi 4 Model B with 8 GB RAM.

Table 1: Security guarantees for integration options with LF.

Security Guarantees \ LF Options	Base	HMAC	TLS	DDS	SST
Secure Authentication	N/A	✓	✓	✓	✓
Access Control	N/A	N/A	N/A	✓	✓
Data Protection	N/A	N/A	✓	✓	✓
Deployment Support	N/A	N/A	N/A	N/A	✓
Limited Resources Support	N/A	N/A	N/A	N/A	✓

Future Plans: In the long run, we will conduct a comparative study of different approaches to securing the edge-based, time-sensitive IoT. The expected security guarantees for each integration option with LF are shown in Table 1. Specifically, we will integrate TLS and DDS with LF and compare them against LF-SST integration and the baseline without security. Also, we plan to analyze the security of the integrated platform. For example, we will use a formal verification method such as AVISPA [1], which automatically checks the security of protocols and applications. To prove that our approach is resistant to various attacks, such as replay attacks, we can leverage approaches like the one used by EqualNet [8].

5 CONCLUSION

This abstract introduces our work-in-progress research to secure distributed IoT systems with real-time requirements and resource constraints through a case study using LF and SST. Our preliminary experimental results using our prototype implementation of one of our approaches show that we can provide basic security guarantees at a minimal cost in terms of the executable size, communication overhead, and execution time. We also sketch out our plans for future research and evaluation of our work-in-progress approaches.

REFERENCES

[1] Alessandro Armando et al. 2005. The AVISPA tool for the automated validation of internet security protocols and applications. In *CAV 2005*. Springer, 281–285.
[2] Soroush Bateni et al. 2023. Risk and Mitigation of Nondeterminism in Distributed Cyber-Physical Systems. In *MEMOCODE'23*. ACM.
[3] Kamalanathan Kandasamy et al. 2020. IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP J. on Info. Security* 8 (2020).
[4] Dongha Kim, Yeongbin Jo, Taekyung Kim, and Hokeun Kim. 2023. SST v1.0.0 with C API: Pluggable security solution for the Internet of Things. *SoftwareX* 22 (2023).
[5] Hokeun Kim, Eunsuk Kang, David Broman, and Edward A Lee. 2017. An architectural mechanism for resilient IoT services. In *SafeThings 2017*. 8–13.
[6] Hokeun Kim, Eunsuk Kang, Edward A. Lee, and David Broman. 2017. A Toolkit for Construction of Authorization Service Infrastructure for the Internet of Things. In *IoTDI'17*. ACM, 147–158.
[7] Hokeun Kim, Armin Wasicek, Benjamin Mehne, and Edward A Lee. 2016. A secure network architecture for the internet of things based on local authorization entities. In *FiCloud 2016*. IEEE, 114–122.
[8] Jinwoo Kim, Eduard Marin, Mauro Conti, and Seungwon Shin. 2022. EqualNet: a secure and practical defense for long-term network topology obfuscation. *USENIX NDSS 2022* (2022).
[9] Marten Lohstroh et al. 2020. Reactors: A deterministic model for composable reactive systems. In *CyPhy 2019, WESE 2019*. Springer, 59–85.
[10] Christian Menard et al. 2023. High-Performance Deterministic Concurrency Using Lingua Franca. *ACM TACO* (aug 2023).
[11] Object Management Group (OMG). 2015. OMG Data Distribution Service (DDS), Version 1.4. (http://www.omg.org/spec/DDS/1.4).