Secure Programming Platform for Edge-Based IoT

Wild-and-Crazy-Idea Paper

Hokeun Kim, Ph.D.

Assistant Professor
School of Computing and Augmented Intelligence
Arizona State University

Forum on specification and Design Languages (FDL) 2023 @ Turin, Italy

Session 2: Security and Machine Learning on the Edge

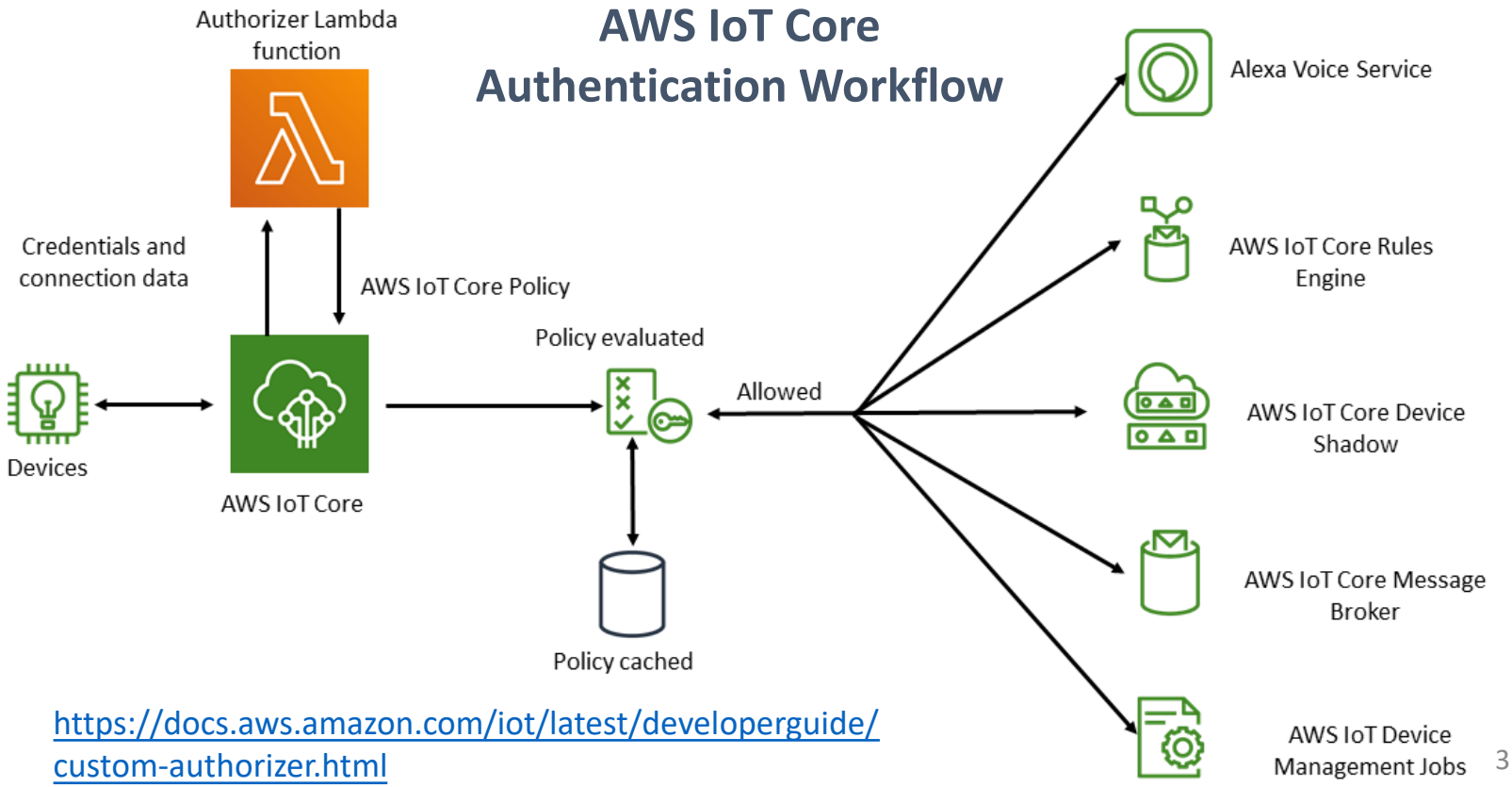
Wednesday, September 13, 2023

Disclaimer

- This is a Wild-and-Crazy-Idea Paper
- Concrete and realizable ideas not implemented yet
- Includes futuristic and immature agendas/plans needing more discussions

Introduction

- *Auth Services* are essential for safe operation of IoT
  - Auth Services – authentication & authorization services



https://docs.aws.amazon.com/iot/latest/developerguide/custom-authorizer.html

Motivation

Google: We're sorry but our cloud wiped out your Wifi and OnHub routers

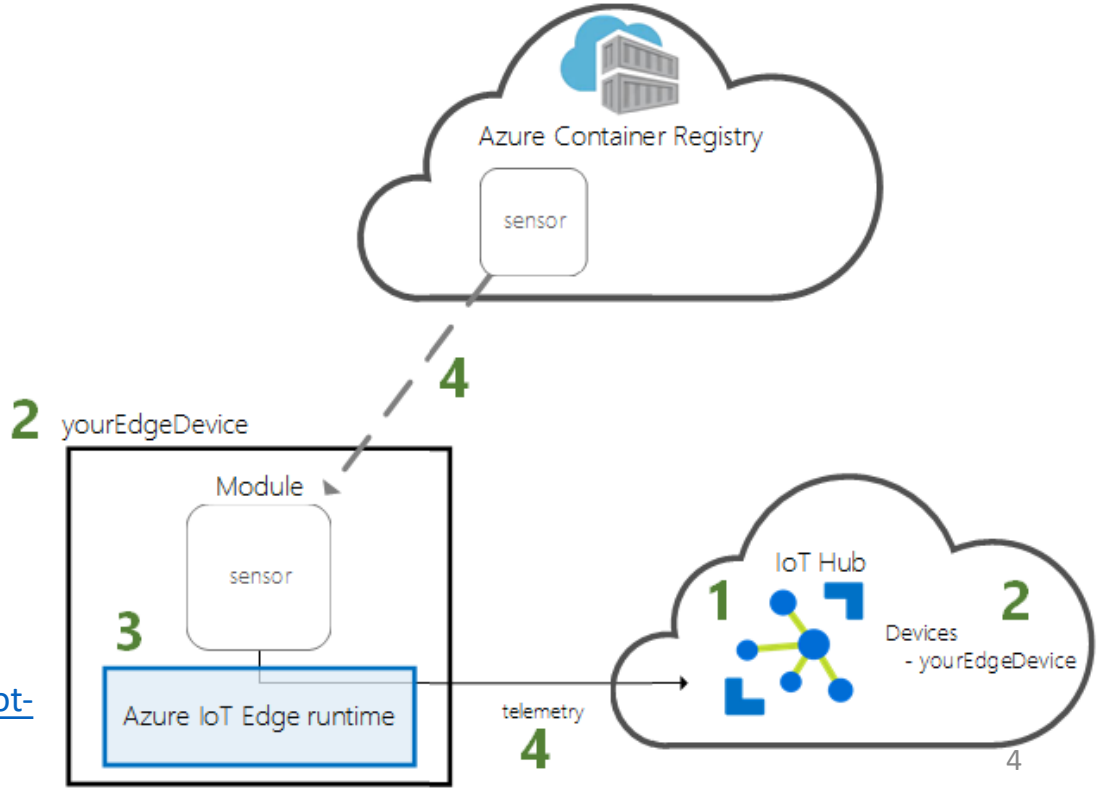
A mystery bug at Google's end caused a mass outage on Wifi and OnHub routers connected to networks that were operating normally.

Written by **Liam Tung,** Contributing Writer on Feb. 24, 2017

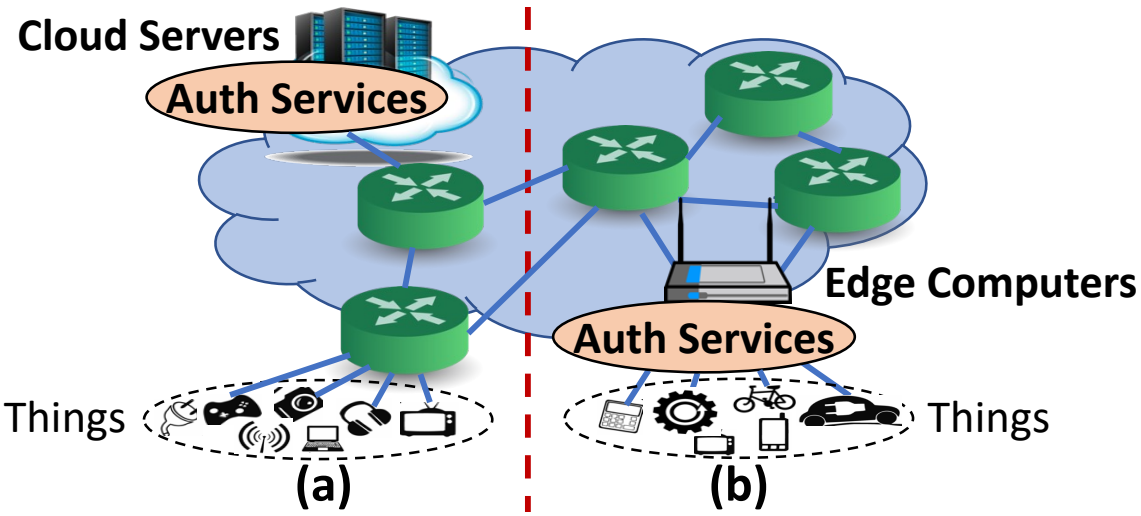
https://www.zdnet.com/home-and-office/networking/google-were-sorry-but-our-cloud-wiped-out-your-wifi-and-onhub-routers/

https://learn.microsoft.com/en-us/azure/iot-edge/quickstart?view=iotedge-1.4

Even with Azure IoT Edge ...



Motivation



Using Edge Computing for Auth Services

- **Low latency**
- **Privacy**
- **Local context**
- **Domain expertise**
- **Robust against network failures**

- Programming platform for Auth Services in fully edge-based IoT environments?
  - Heterogeneity
  - Trust[1]
  - Management overhead
  - (Relatively) limited resources
  - And more …

[1] L. Fotia, F. Delicato, and G. Fortino, "Trust in edge-based Internet of Things architectures: state of the art and research challenges," ACM Computing Surveys, vol. 55, no. 9, pp. 1–34, 2023.

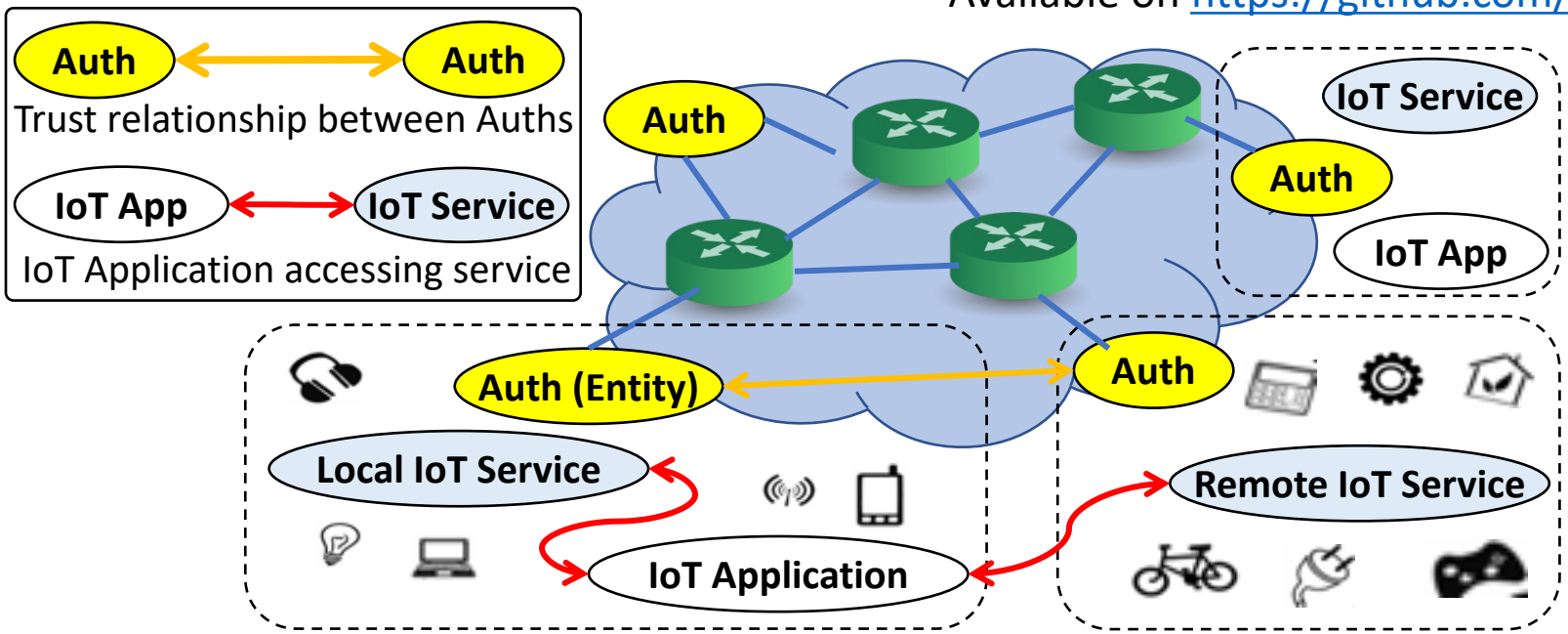
Problem Statement

- Easy to securely program, even for non-security experts
- Easy to deploy on edge (locally), including security configurations
- Must not create vulnerabilities, especially when integrated with other libraries or systems
- Enable anomaly detection & ensure correct behavior
- Use underlying middleware/hardware support for enhanced security
- Check whether the Things are running valid programs (remote attestation)

Background

- SST – Secure Swarm Toolkit[2]
  - An open-source toolkit* for locally centralized and globally distributed Auth Services

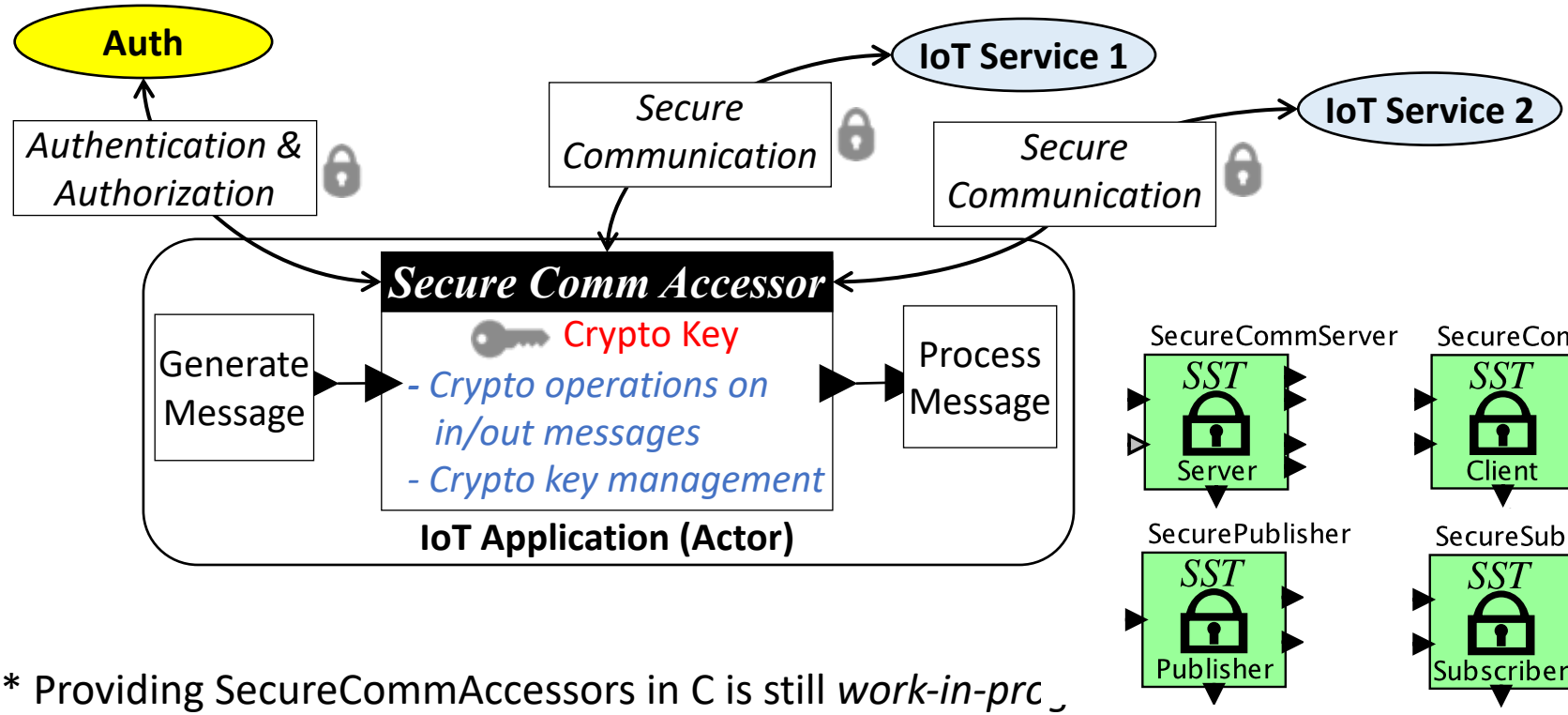
* Available on https://github.com/iotauth



[2] H. Kim, E. Kang, E. A. Lee, and D. Broman, "A toolkit for construction of authorization service infrastructure for the Internet of Things," in The 2nd ACM/IEEE International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA, Apr. 2017, pp. 147–158. ACM/IEEE Best Paper Award

Background

- Secure Communication Accessors
  - SST's programming components (in Node.js and C*[3])



* Providing SecureCommAccessors in C is still *work-in-prc*

[3] D. Kim, Y. Jo, T. Kim, and H. Kim, "SSTv1.0.0 with C API: Pluggable security solution for the Internet of Things," SoftwareX, vol. 22, p. 101390, May 2023.

Proposed Approach

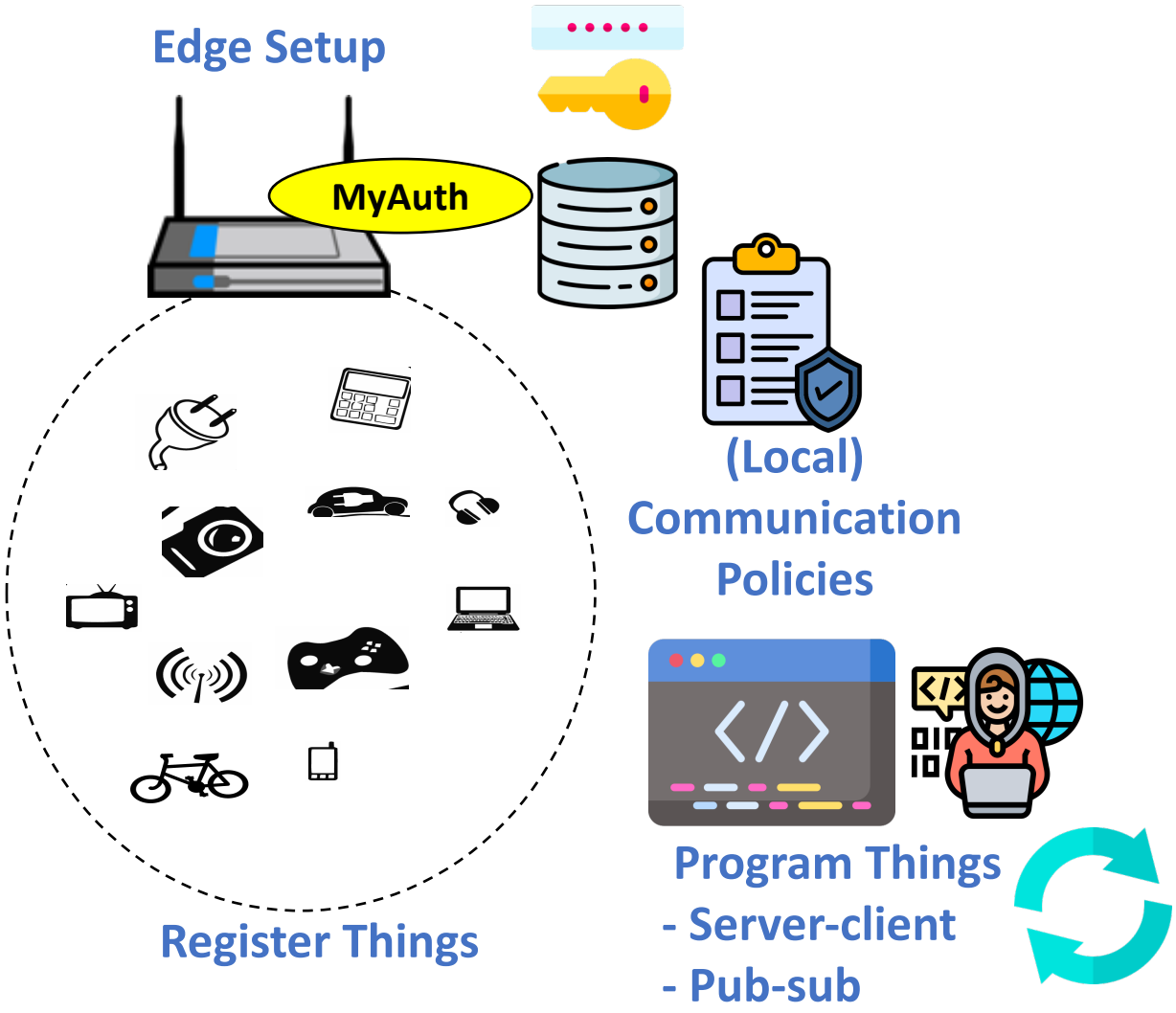
SSPP – Secure Swarm Programming Platform

- Programming platform for edge-based IoT *using SST*
- Provide fault-tolerant, scalable Auth Services and end-to-end IoT security

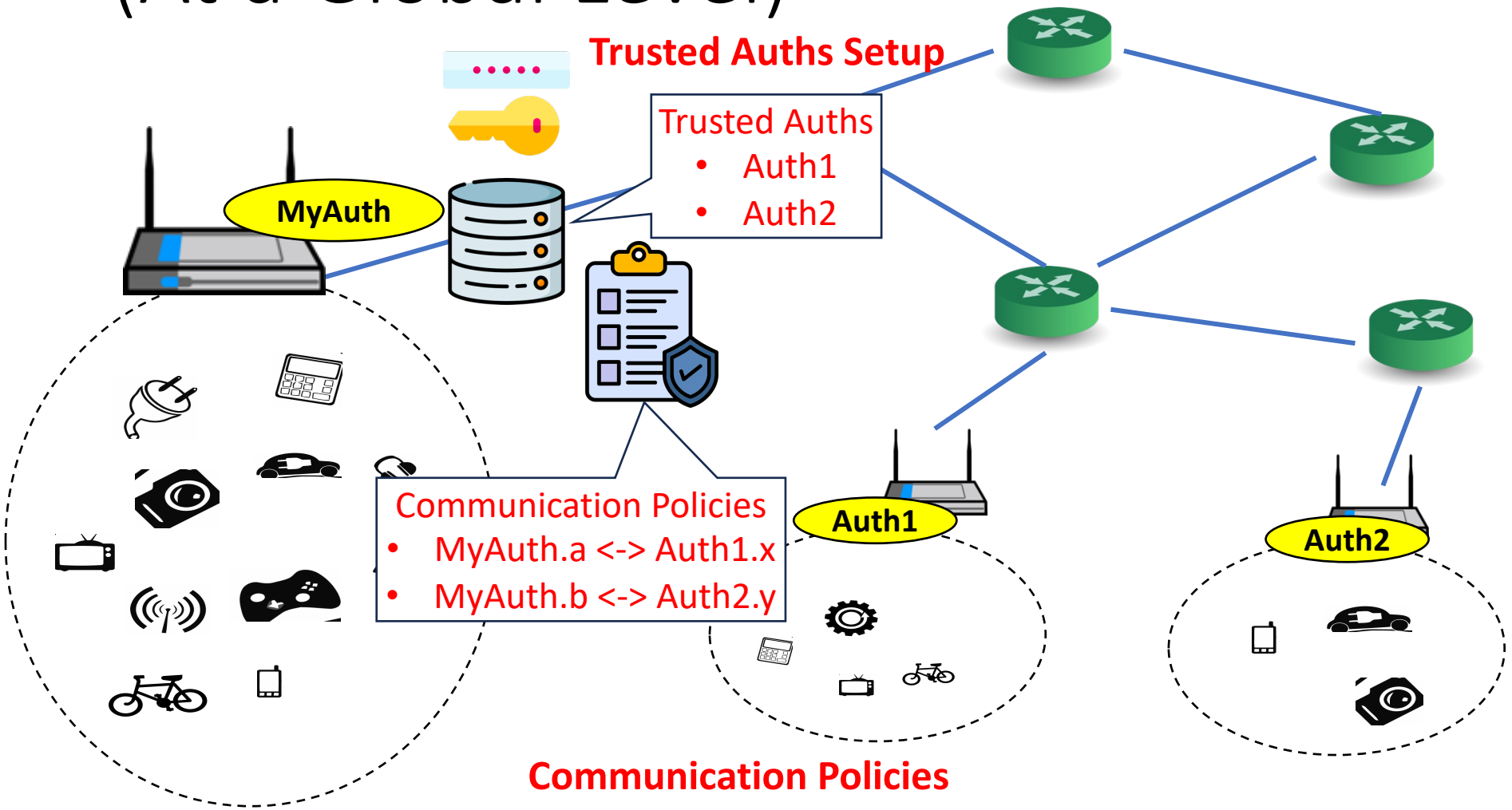
A programming model that will enable:

- Encapsulation of security details
- Easier programming & deployment
- Simpler security analysis (e.g., restricted data flow)
- Remote SW attestation
- Straightforward use of support of underlying HW

Proposed Programming Workflow (at a Local Edge Level)



Proposed Programming Workflow (At a Global Level)



Research and Evaluation Plans

Programmability

Remote Attestation

Security Analysis

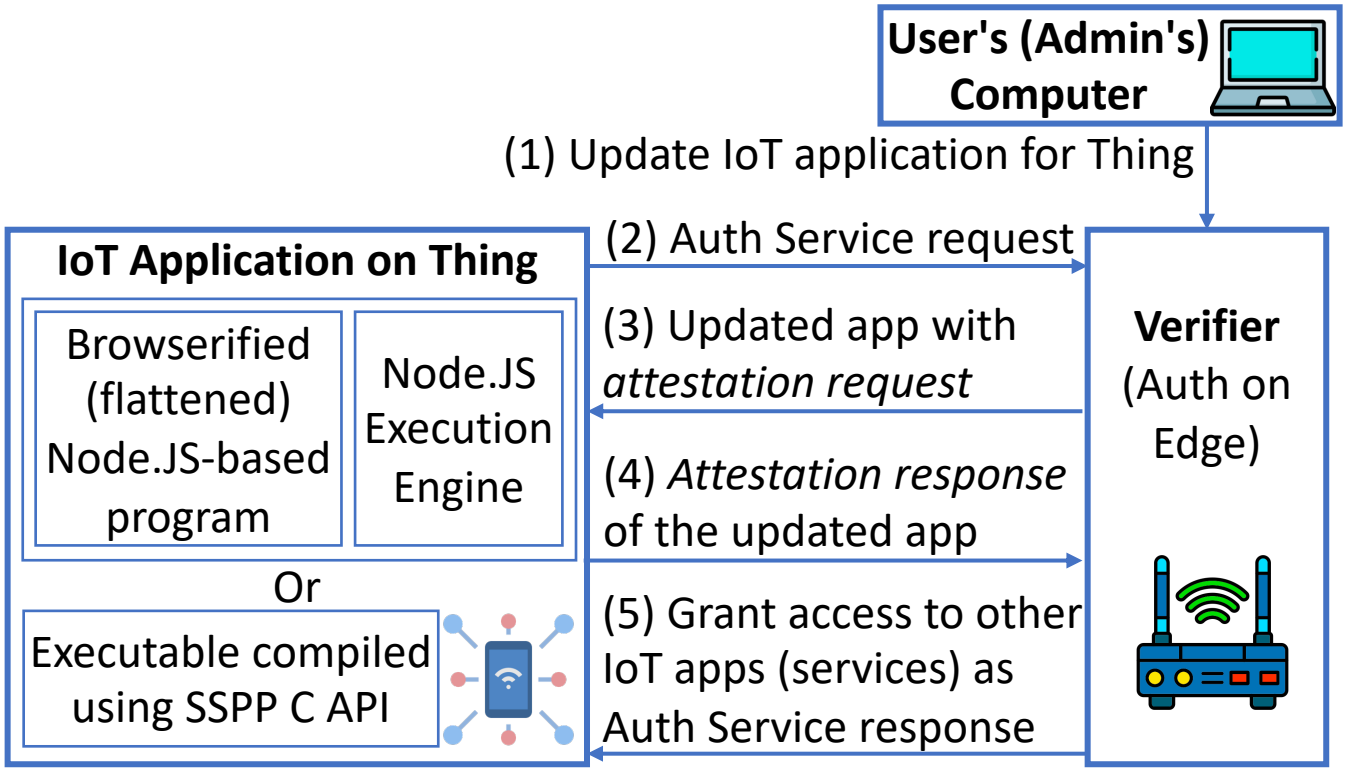
Research and Evaluation Plans

Programmability Goals of SSPP

	W/o Programming Platform (C, Py, Node.js, etc. w/ Sec Lib)	SSPP (w/ Platform Layer Support)
Crypto Key Init & Exchange	Manual	Automated or Simplified by SSPP
Crypto Key Loading	Device Dependent	Automated by SSPP
Key Agreement w/ Edge	Device & Edge Dependent	Handled by Accessor
Crypto Implementation	Language Dependent	Implemented by Accessor
Key Management & Updates	Implemented by Developer	Handled by Accessor
Security Config Updates	Manual	Simplified by SSPP

Research and Evaluation Plans

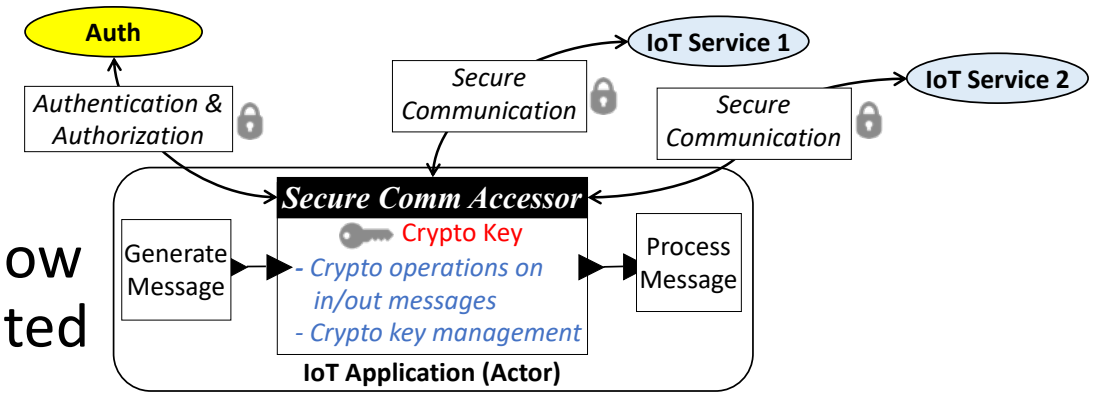
Updated and Attested by Auth on Edge



Research and Evaluation Plans

Security Analysis

- Static analysis (pre-deployment)
  - Data flow analysis (flow of sensitive data limited by accessors)



- Dynamic analysis (runtime)
  - Rule-based (monitoring unauthorized access attempts)
  - Statistical or ML-based (access patterns monitored by Auth on edge)

Thank you for your attention!

Summary of Wild and Crazy Ideas

- Need for programming platform for IoT Auth Services
- Target: edge-based IoT (independent of Cloud)
- SSPP – Secure Swarm Programming Platform
- Programmability – easy to program & deploy
- Remote attestation on edge
- Static and dynamic security analysis

Contact Information for Further Discussions

- https://hokeun.github.io, hokeun@asu.edu