CERIAS

The Center for Education and Research in Information Assurance and Security

Computer and Information Technology

WASI-SN: Portable and Secure Low-Footprint WebAssembly Sensor Interface with Networked Access Control

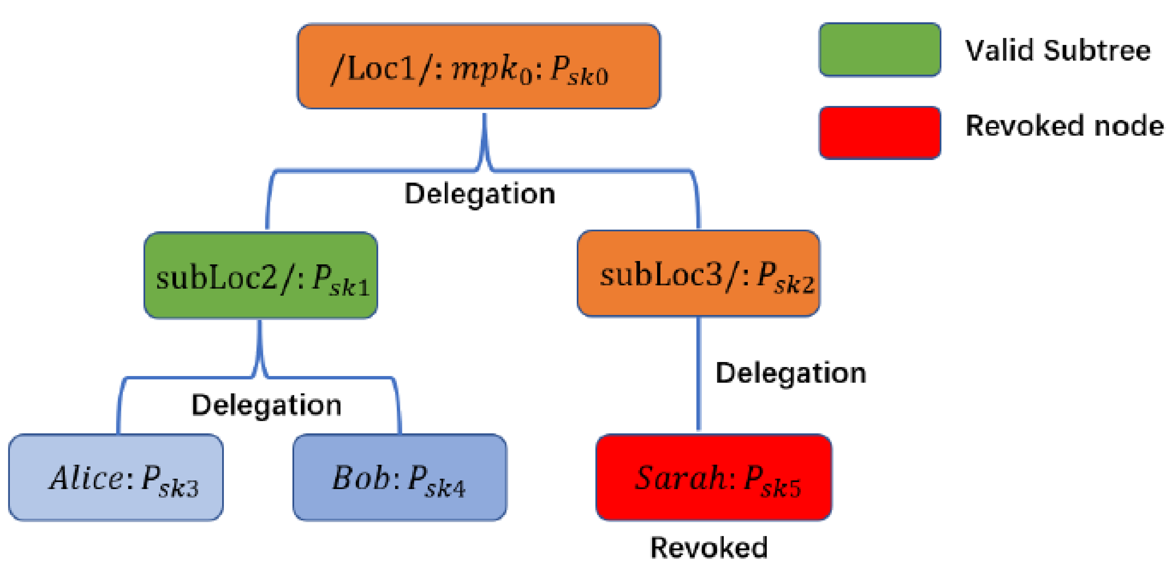
Botong Ou, Baijian Yang
{bou, byang}@purdue.edu

Research Questions

- How can WebAssembly and software fault isolation be used to mitigate software-based attacks on IoT devices?
- How can access control be included in the application-layer network protocol to guard against network-based attacks on IoT devices?
- How can the WebAssembly System Interface (WASI) be extended to offer secure access to on-board sensors in IoT devices?

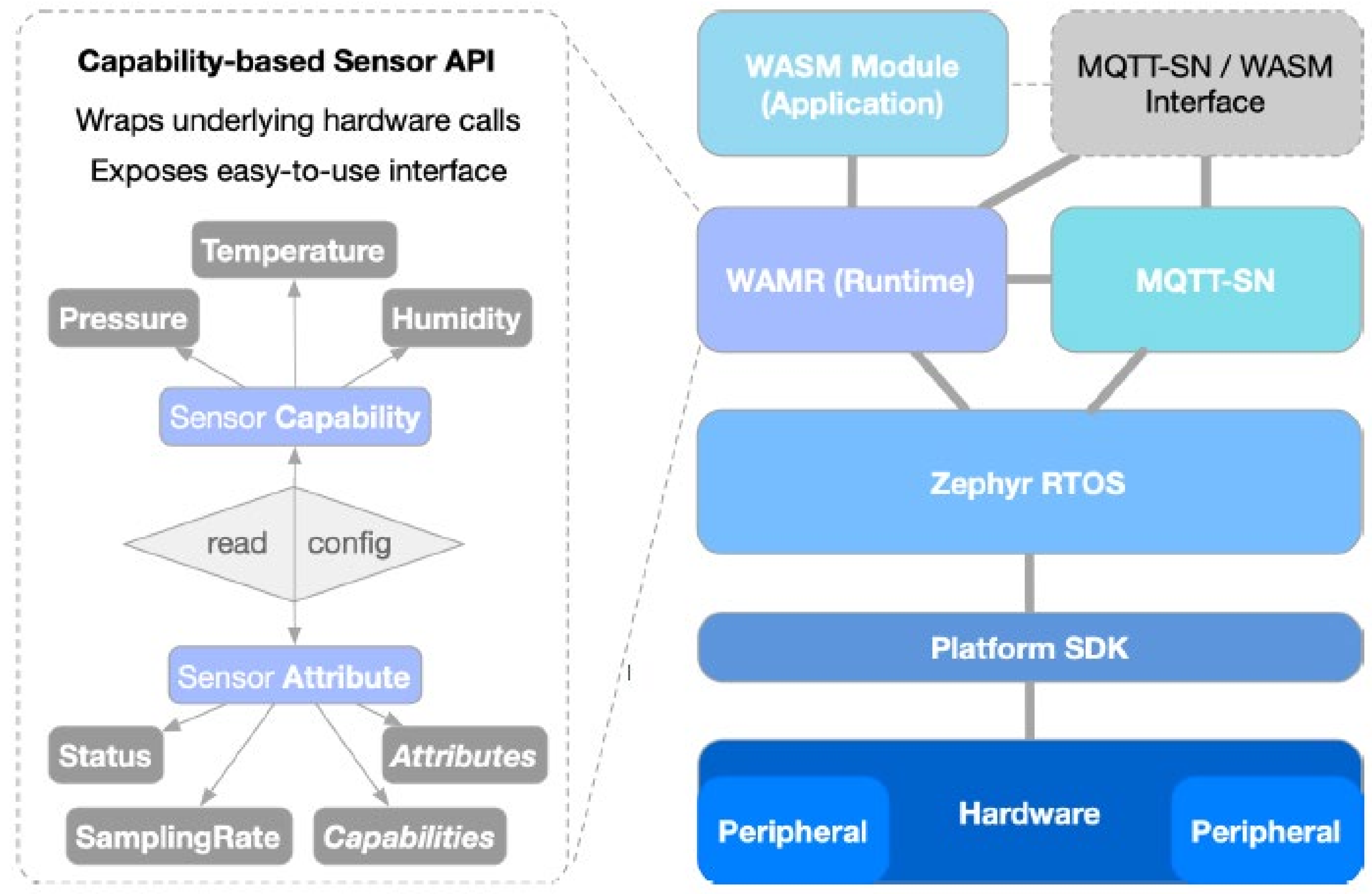
WKD-IBE

- A large fraction of attacks are network-based attacks.
- Most microcontroller and RTOS do not provide a substantial access control scheme to restrict the application behavior.
- Introduced wildcard-identity-based encryption (WKD-IBE) (Blazy, 2019) to enable data driven, end-to-end lightweight encryption while supporting flexible key delegation and revocation.



Key management of complete tree

Methodology

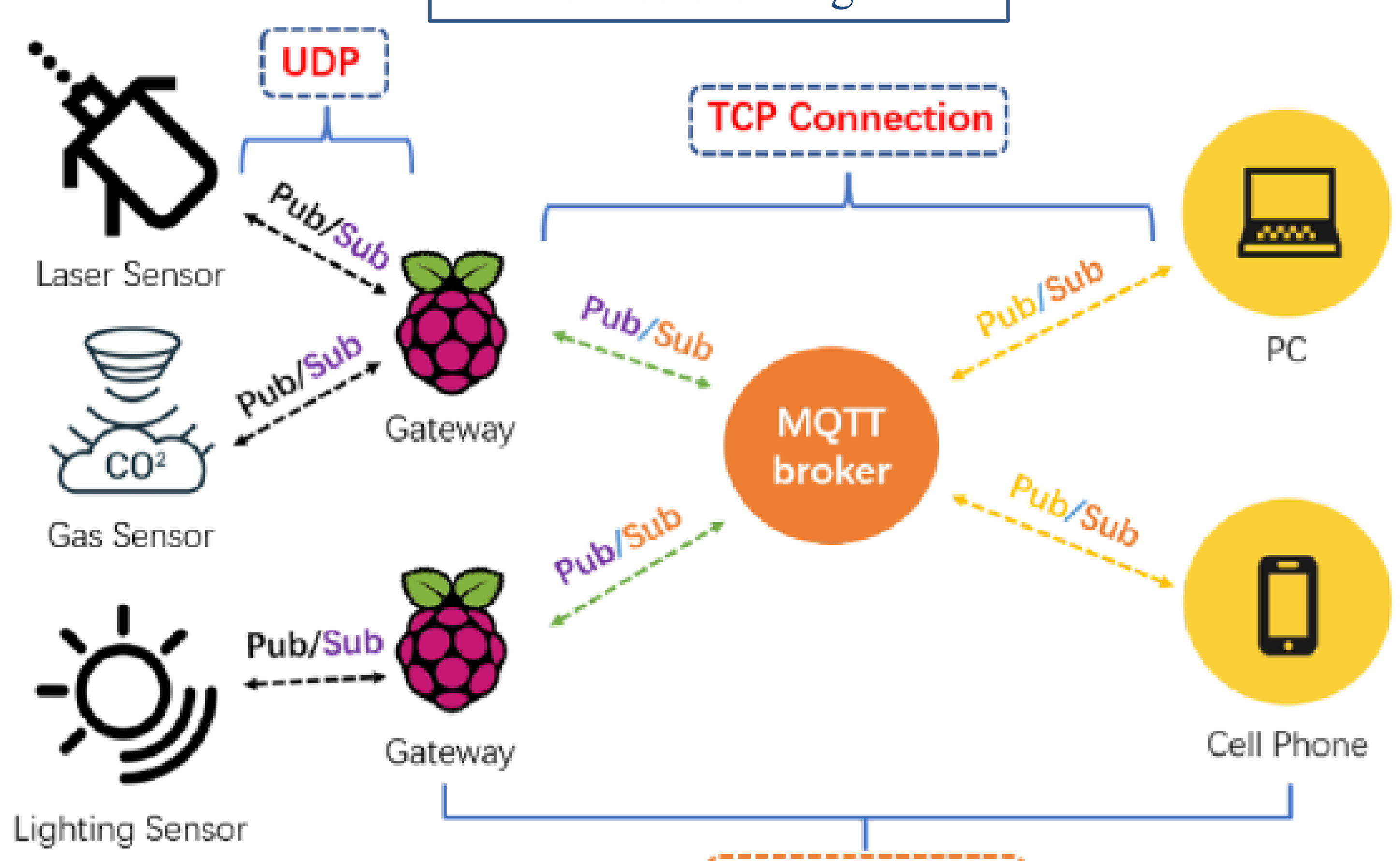


Architecture Diagram

- Sensor is defined by a set of capabilities and attributes.
- Capabilities: Sensor functionalities such as Temperature, Humidity, Pressure etc.
- Attributes: Configurable states such as sampling rate.

```
int main(){
  turnOn("BME280");
  int rate = 1000000000; //ns
  config("BME280", "SampRate", rate);
  char buf[] = {0,0,0,0};
  read("BME280", "humidity", buf, 4);
}
```

Sensor Interface Example

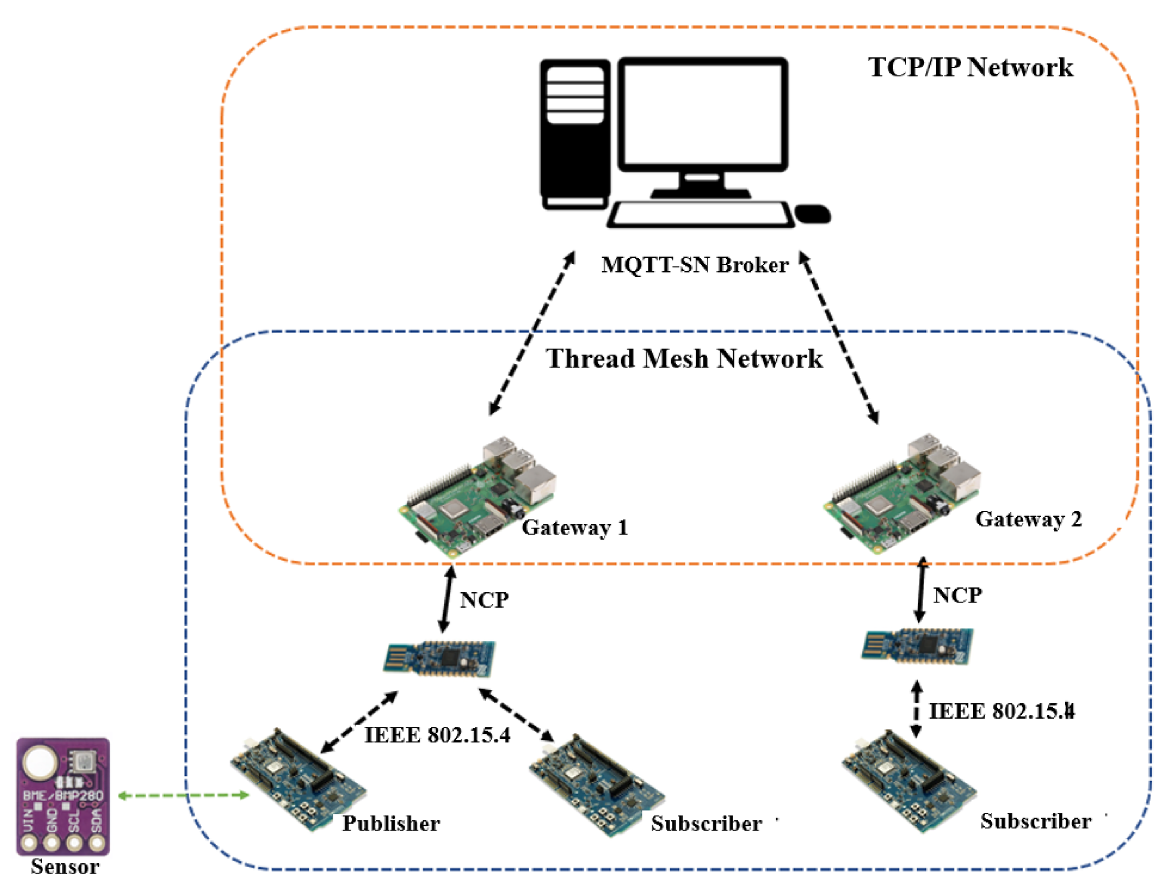


- Network primitives: Exposing MQTT-SN (Sadio, 2019) interfaces to WASM module including basic functionality such as *publish/subscribe*

```
int main(){
  int KeepAlive = 30; //sec
  string ClientID="WASM"
  string IP="fdde:ad00..."
  int Port = 47193;
  start(1000);
  connect(ClientID,KeepAlive,IP,Port);
  int topicId = register("humidity");
  publish(topicId, 2, data);
  disconnect();
}
```

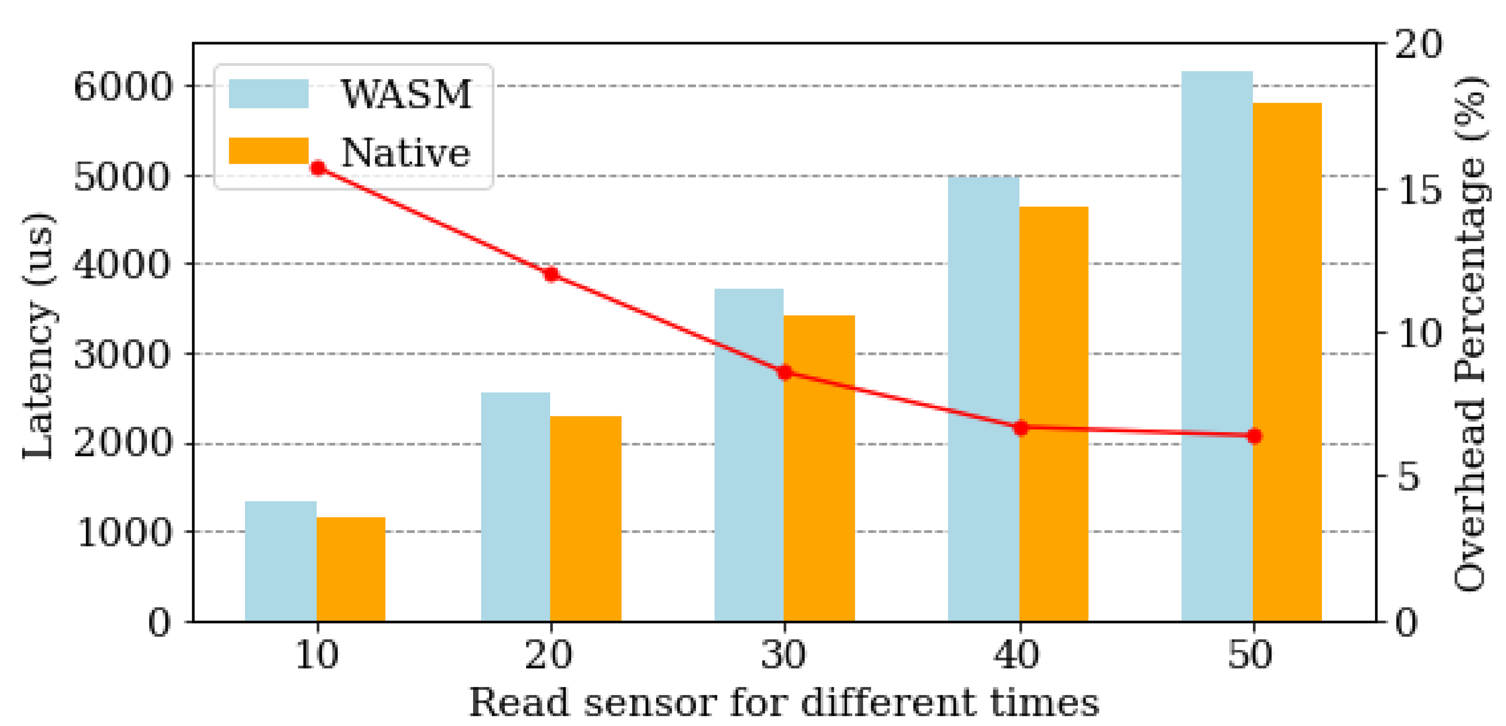
MQTT-SN Primitives Example

Experiment Setup

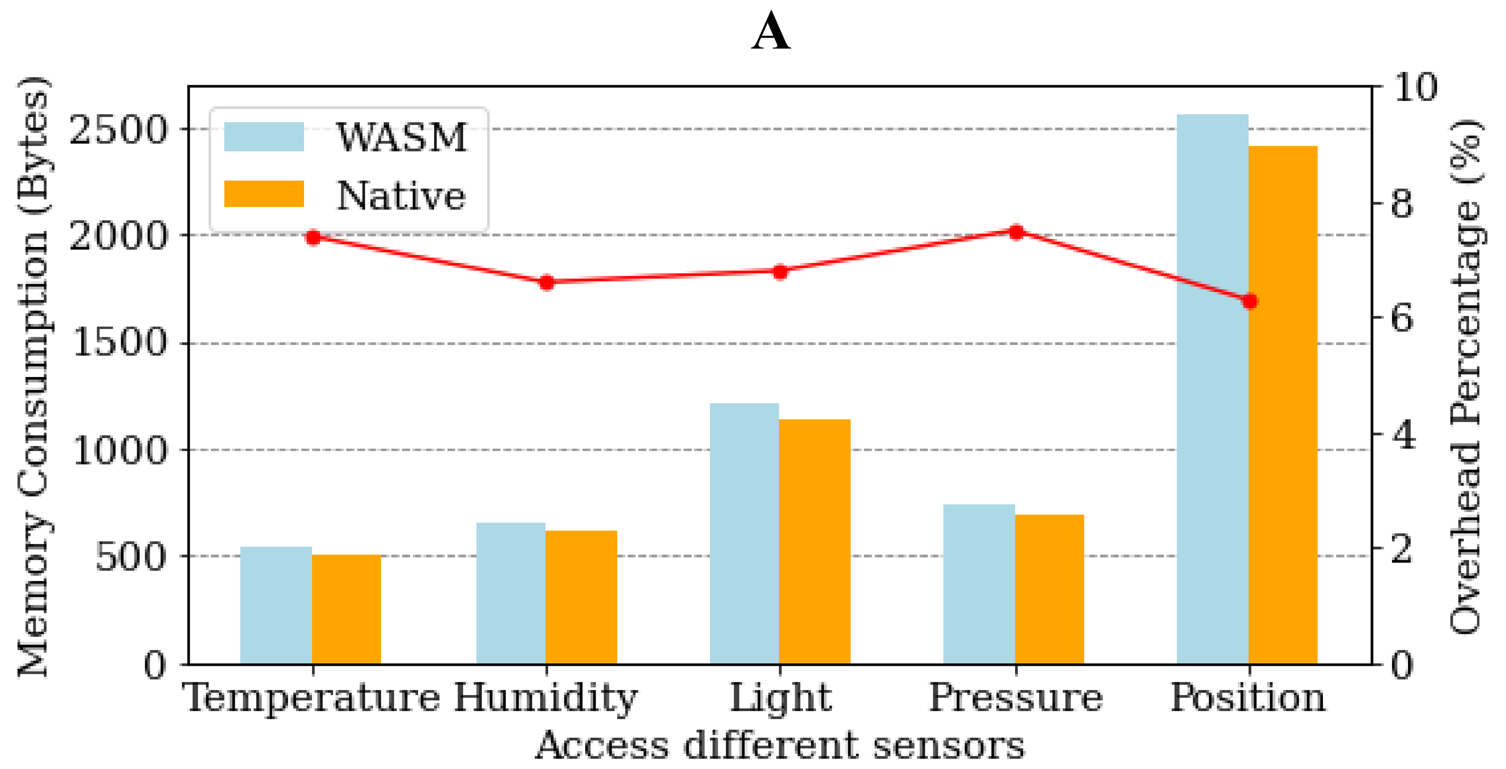


- End-device:
  - Device: NRF52840-DK
  - MCU: Cortex-M4F@64 MHz
  - RAM: 256KB
- Gateway:
  - Device: Rasperrypi 3B+
  - MCU: Cortex-A53@1.4GHz
- Broker:
  - Device: PC
  - MCU: Intel i7-6700@4 GHz
- Network: Google Thread Network

Results



A



B

Chart A:

- WebAssembly naturally introduced 16% overhead when running WASM runtime.
- The overhead proportion decreases as the application's time complexity grow up. The overhead will remain stable around 6.5% in the end

Chart B:

- For different sensors, WASM runtime will only introduce around 7% memory consumption compare to native C application.

Summary

- The first WebAssemblySystem Interface (WASI) extension that support secure, portable and low-footprint sandboxing.
- Support application memory isolation and ensure resource privileges are protected.
- Support multi-tenant access to heterogenous embedded devices.
- Support remote key delegation and revocation with little runtime overhead.

PURDUE UNIVERSITY

Sadio, O., Ngom, I., & Lishou, C. (2019, October). Lightweight security scheme for mqtt/mqtt-sn protocol. In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS) (pp. 119-123). IEEE.

Blazy, O., Germouty, P., & Phan, D. H. (2019, February). Downgradable identity-based encryption and applications. In Topics in Cryptology–CT-RSA 2019: The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4–8, 2019, Proceedings (pp. 44-61). Cham: Springer International Publishing.

CERIAS