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.

Methodology

- 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.

WKD-IBE

- 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.

Experiment Setup

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

Results

- 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 heterogeneous embedded devices.
- Support remote key delegation and revocation with little runtime overhead.
