StreamBox-TZ:
Secure Stream Analytics at the Edge with TrustZone

Heejin Park¹, Shuang Zhai¹, Long Lu², and Felix Xiaozhu Lin¹
¹Purdue ECE, ²Northeastern University
Scenario: Edge Processing

- Large telemetry data streams come from IoT sensors
  - Smart grid: 140 million power samples per day
  - Oil production line: 1-2 TB of data

- Edge processing is emerging
  - Cleanses telemetry data
  - Reports the results to cloud servers
Problem: Exposing High Security Threats

- **Common IoT threats**
  - Lack of professional supervision
  - Delayed security updates

- **Edge processing threats**
  - High-value target
  - Wide attack surface on software stack

Edge

- Access confidential data
- Delete or fabricate result
- Threaten the integrity of an entire IoT deployment

Common IoT threats

- Lack of professional supervision
- Delayed security updates

Edge processing threats

- High-value target
- Wide attack surface on software stack

Threaten the integrity of an entire IoT deployment
StreamBox-TZ

Designed for data-intensive, parallel computations on minimal TCB inside ARM TrustZone

- **Approach:** Isolate data and computations

- Architecting data plane for **protection**
  - Trusted primitives: low level stream algorithms

- **Performance** optimization within TEE
  - Memory management / trusted IO

- **Verifying** analytics execution
  - Remote attestation with audit log
StreamBox-TZ:
Secure Stream Analytics at the Edge with TrustZone

Come to our talk on July 11 at
Track II, Security #2: Isolation