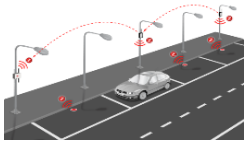
CAREER: Securing Sensory Side-Channels in Cyber-Physical Systems

Sensors in different domains


Smartwatch


Smart home


Medical

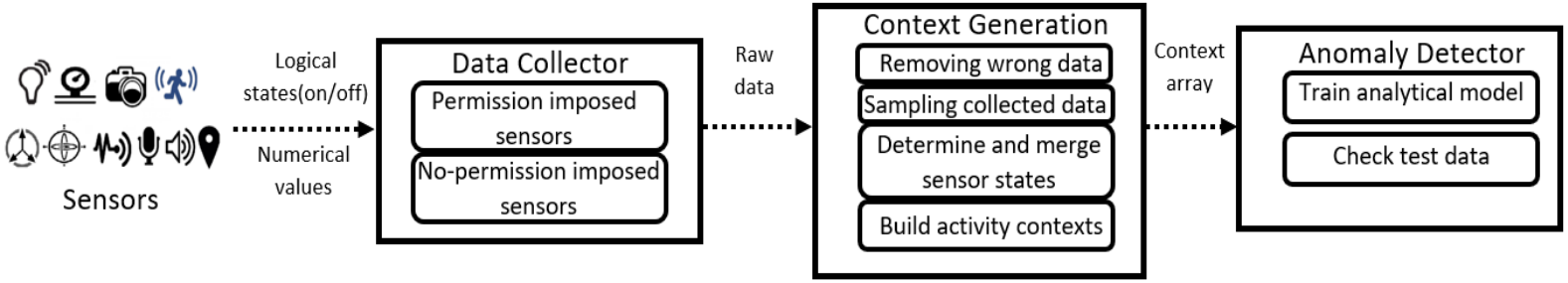

Smart city

Motivation

* Less information available about sensor-based threats among users.
* Unawareness about consequences among users.
* Rapid growth of threats in recent years.
* Failure of existing sensor management systems.
* No effective security mechanism available yet.

Contribution

* Design and implementation of a context-aware sensor-based threat detector in standalone and connected smart devices (e.g., smart home).
* Training the framework with real-life user data for different activities and device configurations.
* Testing proposed framework against different threats to both standalone and connected smart devices.
* High accuracy in sensor-based threat detection with minimum system overhead.



Adversary Model

- Triggering Malware via Sensor
- Information Leakage via Sensor
- Denial-of-Service
- Transfer Malware via Sensor

Performance Summary

Standalone devices

- High accuracy and F-score (above 96%) for smartphone and smart watch.
- Tested with data collected from 100 real-life users.
- Minimal performance overhead in terms of CPU, RAM, and power usage.

Connected devices

- High accuracy and F-score (above 91%) for three different smart home layouts.
- Tested with data collected from 15 real-life users and 22 real devices.
- Minimum performance overhead in terms of latency

Project no - NSF-CNS-CAREER-1453647
Institution - Florida International University **PI - A. Selcuk Uluagac** **Email - suluagac@fiu.edu**