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

PI: Selcuk Uluagac
Cyber-Physical Systems Security Lab (CSL)
Electrical & Computer Engineering Department
Florida International University, Miami, Florida
E-mail: suluagac@fiu.edu, Web: http://csl.fiu.edu
https: //csl.fiu.edu/6thsense/

Abstract

Cyber-Physical Systems (CPS) integrate devices that can interact with each other and the physical world around them. With CPS applications, engineers monitor the structural health of highways and bridges, farmers check the health of their crops, and ecologists observe wildlife in their natural habitat. Using sensory side-channels (e.g., light, temperature, infrared, acoustic), an adversary can successfully attack CPS devices and applications by (1) triggering existing malware, (2) transferring malware, (3) combining multiple side-channels to increase the impact of a threat, or (4) leaking sensitive information. The project investigates the sensory side-channel (e.g., acoustic, seismic, light, temperature) threats to CPS devices and applications and evaluates the feasibility and practicality of the attacks on real CPS equipment. The result is novel sensory side-channel-aware security tools and techniques for the CPS devices. Specifically, the principal investigator (1) analyzes the physical characteristics of the sensory CPS side-channels to understand how the physical world impacts the cyber world of CPS devices; (2) investigates the information leakage through the sensory side-channels on the CPS devices; and (3) develops a novel IDS particularly designed to be aware of the sensory CPS side-channels [1, 2, 3, 4, 5].

World of CPS…

CPS: convergence of all these technologies, they are everywhere!

Sensors in CPS

Smartwatch

Smart home

Smart city

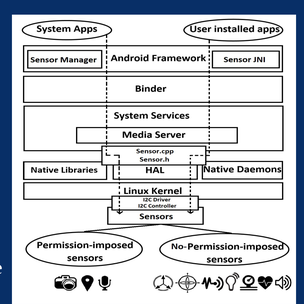
Medical

Sensors are everywhere!

Existing sensor management systems

Features

- Existing operating systems (e.g., iOS, Android, Windows, Blackberry) have similar sensor management frameworks.
- Permission-based access provided by the system.
- Only selective sensors are covered.
- Sensor access to different apps provided by Hardware Abstraction Layer (HAL).



Android Sensor Management System

Limitations

- Permission based management system.
- Only enforced in selective sensors.
- On screen sensors (e.g., accelerometer, gyroscope, light sensor) are considered secure and no permission is needed.
- After granting permission, users cannot control how apps use sensors.

A novel solution is needed for securing sensory-channels of CPS devices.

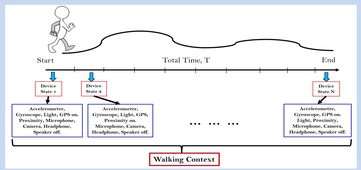
Our Contributions

- Design of a context-aware sensor-based threat detector to address the limitations of existing sensor management systems.
- Implementing proposed framework in both standalone smart devices (smartphone, smart watch) and connected smart environment (smart home and Office).
- 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	• Malicious app installed in the device triggered by a message via sensors (e.g., light sensor).
Information Leakage via Sensor	• Information saved or recorded in the device transferred via sensor.
Denial-of-Service	• Malicious app installed in the device impede the normal operation using sensors.
Transfer Malware via Sensor	• Exploiting sensory channels to transfer malware to a device.

Context Awareness



- Total time of activity context is divided into one second slots.
- Each second represents one or multiple device states.
- Each device state consists of different sensor conditions (on/off state of the sensors).

Sensor Co-dependence

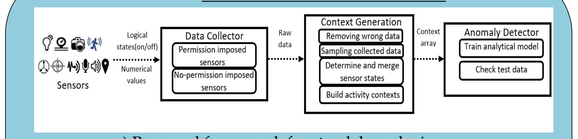
Accelerometer
Gyroscope
Light
GPS

Accelerometer
Gyroscope
Proximity
Audio

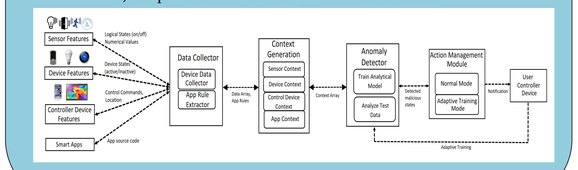
Accelerometer
Gyroscope
Light
Audio

• For each user activity, a specific set of sensors remains active.
• Sensors can be considered as co-dependent entities for each activity.
• By observing the active sensors for a task, it is possible to differentiate between user and malicious activities.

Framework Overview

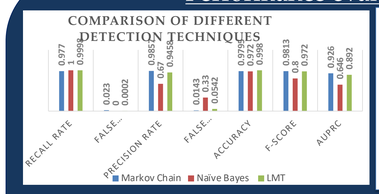


a) Proposed framework for standalone device



b) Proposed framework for connected smart environment

Performance evaluation on Smart Watch



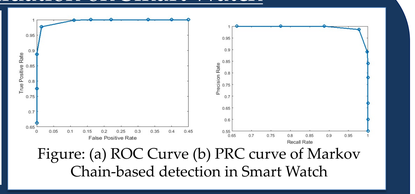


Figure: (a) ROC Curve (b) PRC curve of Markov Chain-based detection in Smart Watch

Data Collected from
- 42 users
- 7 different activities!
- LG Watch Sport

Task Category	Task Name
Generic Activities	1. Sleeping 2. Driving as driver 3. Driving as passenger
User-related Activities	1. Walking with smart watch in hand 2. Playing games 3. Browsing 4. Making phone calls

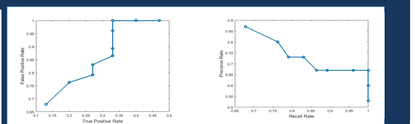
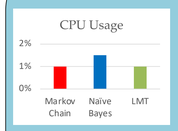
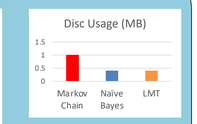
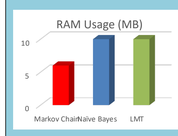


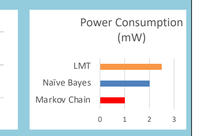
Figure: (a) ROC Curve (b) PRC curve of Naïve Bayes-based detection in Smart Watch

Performance Overhead



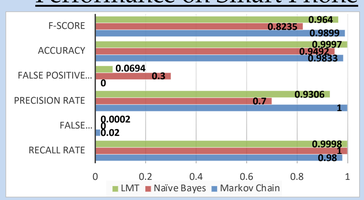






Performance overhead of data analysis on smart watch

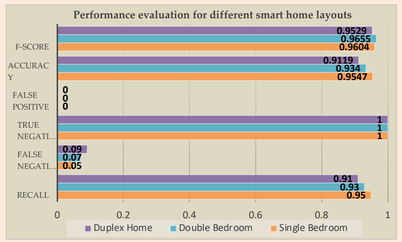
Performance on Smart Phone



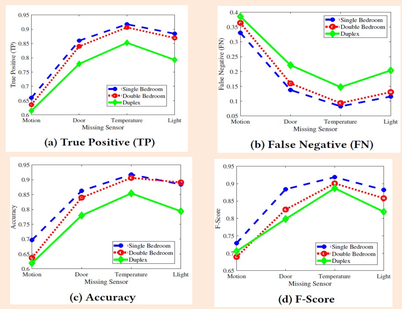
Data Collected from
- 50 users
- 9 different activities!
- Samsung Galaxy S5 Due

Task Category	Task Name
Generic Activities	1. Sleeping 2. Driving as driver 3. Driving as passenger
User-related Activities	1. Walking with phone in hand 2. Walking with phone in pocket/bag 3. Playing games 4. Browsing 5. Making phone calls 6. Making video calls

Performance evaluation on Smart Home System



Data Collected from
- 15 users
- 11 different devices!
- 35000 events



Performance evaluation with different sensors

SmartThings
PHILIPS hue
ecobee
Yale smart Living

Future Work

1. Test proposed framework on different CPS devices.
2. Evaluate performance of the framework against different active malware.
3. Comprehensive evaluation of the framework including frequency, battery, accuracy trade-off.

References

[1] A. Selcuk Uluagac, Venkatachalam S., and R. A. Beyah,"Sensory Channel Threats to Cyber Physical Systems: A Wake-up Call," In Proceedings of the IEEE Conference on Communications and Network Security (CNS), San Francisco, California, 2014
[2] Amit Kumar Skder, Hidayet Aksu, and A. Selcuk Uluagac "6thsense: A context-aware sensor-based attack detector for smart devices," in 26th USENIX Security Symposium, Vancouver, BC, Canada, 2017.
[3] Amit K. Sikder, H. Aksu, and A. Selcuk Uluagac,"A Context-aware Framework for Detecting Sensor-based Threats on Smart Devices," in IEEE Transactions on Mobile Computing, 2019
[4] Amit K. Sikder, L. Babun, H. Aksu, and A. Selcuk Uluagac, "AEGIS: A Context-aware Security Framework for Smart Home Systems ", in Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC), San Juan, Puerto Rico, 2019
[5] Amit Kumar Sikder, Guiseppe Petraca, Hidayet Aksu, Trent Jaeger, and A. Selcuk Uluagac, "A Survey on Sensor-based Threats and Attacks to Smart Devices and Applications," IEEE Communications Surveys & Tutorials, 2021

2021 NSF Cyber-Physical Systems Principal Investigators' Meeting
June 2-4, 2021

Award ID#: NSF-CAREER-CNS-1453647