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

Award#: NSF-CNS-CAREER-1453647 PI: Selcuk Uluagac Florida International University

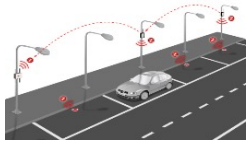
Project website: https: //csl.fiu.edu/6thsense

Sensors in Different Domains

Smartwatch

Smart home

Medical



Smart city

Challenges

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

Adversary Model

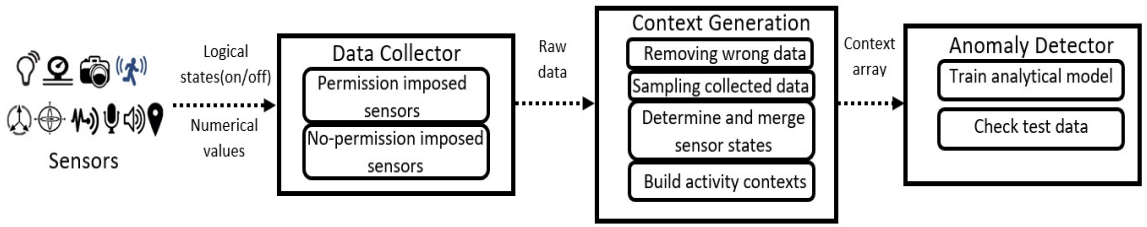
- Triggering Malware via Sensor
- Information Leakage via Sensor
- Denial-of-Service
- Transfer Malware via Sensor

Observations

Context-awareness: Sensors in smart devices change their states in a specific pattern for each user activity.

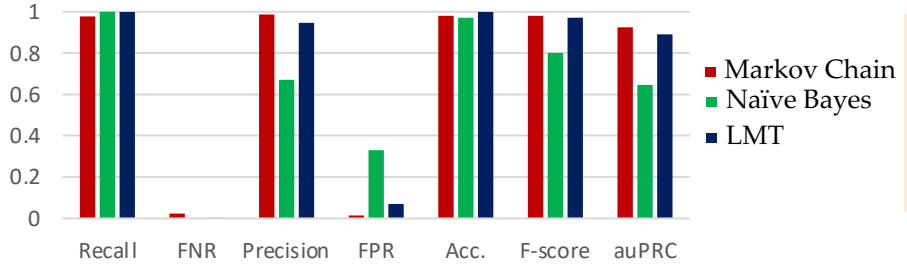
Sensor-codependence: For each user activity, a specific set of sensors remain active in smart devices.

Framework Overview



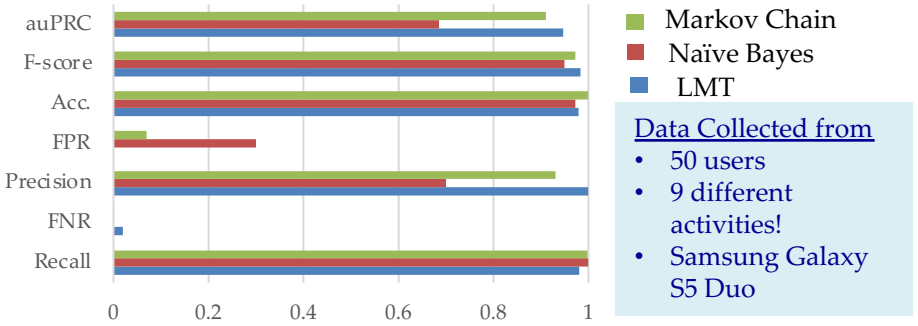
We considered different machine learning algorithms (Markov Chain, Naïve Bayes, LMT, etc.) to build our anomaly detector.

Performance Evaluation on Smart Watch



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

Performance Evaluation on Smartphone



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

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
	5. Walking with device in pocket/bag†
	6. Making video calls†

Scientific & Broader Impact

- **The project has produced:** 8 journal articles, 12 conference papers, 2 live-demos, 22 invited talks/seminars, 5 patents (1 awarded, 4 pending).
- **The project trained:** 2 PhD and numerous undergraduate students as part of the REU site at the PI's institution and 1 high school student.
- **Outreach in K-12:** PI demoed the project to thousands of K12 students visiting his lab in Miami.
- **Awards received** 2 awards by the PI and 1 by the PhD student were received at FIU for this research.

Sample References

[1] S. Uluagac, et al.,"Sensory Channel Threats to Cyber Physical Systems: A Wake-up Call," IEEE CNS, 2014

[2] Sikder et. al "6thsense: A context-aware sensor-based attack detector for smart devices," USENIX Security, 2017.

[3] Sikder et. al,"A Context-aware Framework for Detecting Sensor-based Threats on Smart Devices," IEEE Transactions on Mobile Computing, 2019

[4] Sikder et. al," A Survey on Sensor-based Threats and Attacks to Smart Devices and Applications," IEEE Communications Surveys & Tutorials, 2021