LeakThief : Stealing the Behavior Information of Laptop via Leakage Current

Dian Ding[1], Yi-Chao Chen[1], Xiaoyu Ji[2], Guangtao Xue[1]

[1]Shanghai Jiao Tong University

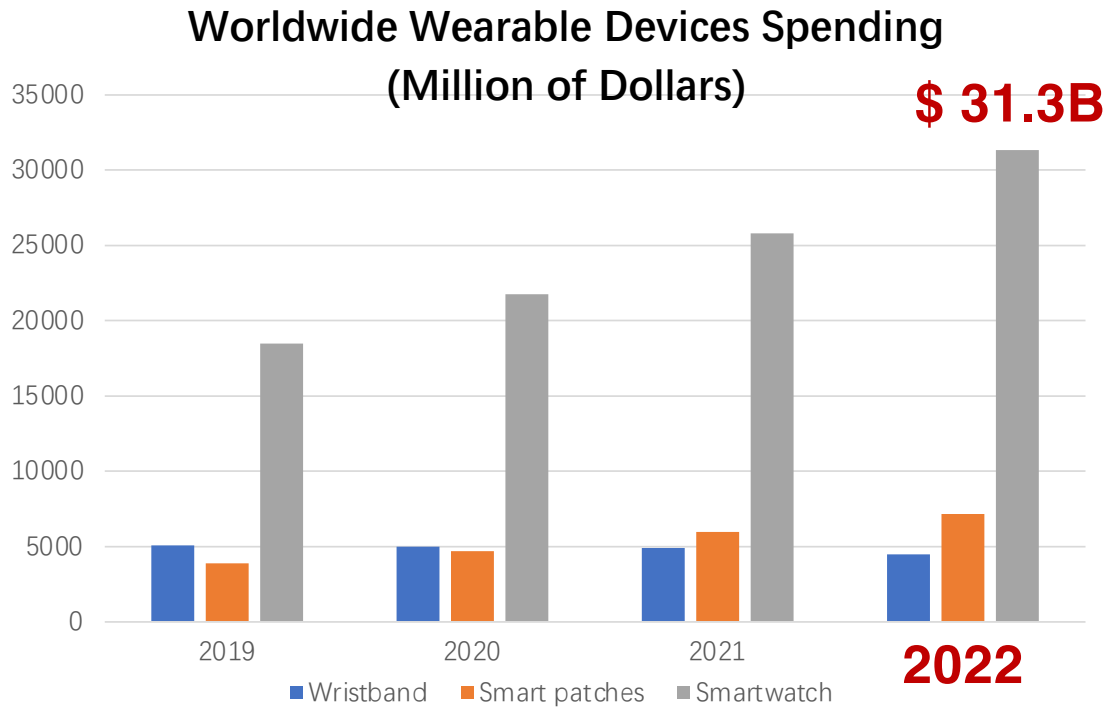
[2]Zhejiang University

Outline

- Background
- Motivation
- Preliminary
- System
- Evaluation
- Discussion
- Conclusion

Background

Smartwatches are taking the world.



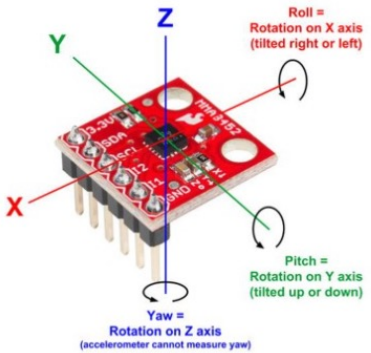
* Gartner Forecasts Global Spending on Wearable Devices to Total $81.5 Billion in 2021

health monitor

sports management

Background

Prolonged wear increases the potential for attack.



motion sensor

microphone

keystroke inference (CCS'15, INFOCOM'19)

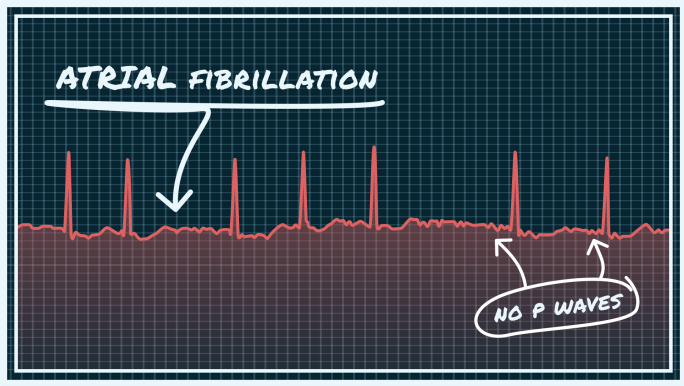
handwriting inference (INFOCOM'18)

Motivation

Electrodes are widely configured in smartwatches.

built-in electrode

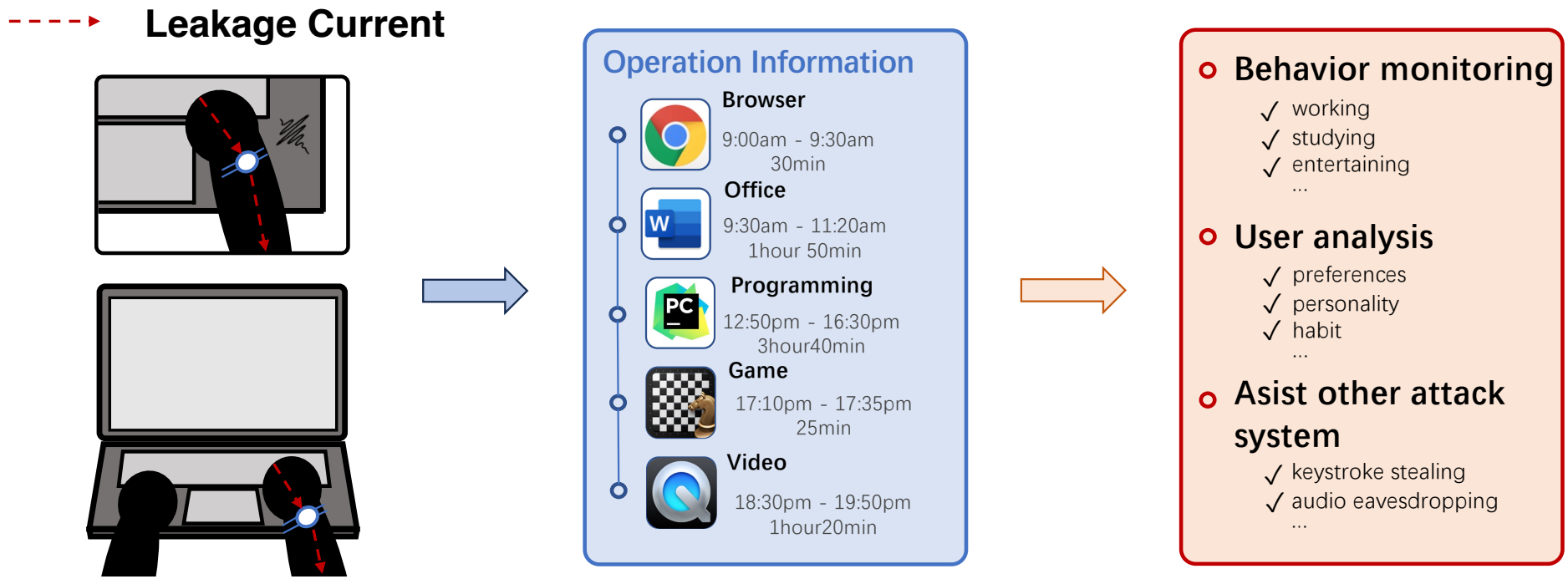
ECG



atrial fibrillation test

Motivation

The potential risk of electrodes while using the laptop.



(a) contact with laptops (b) sniffing user operations (c) potential risk of electrodes

Motivation

Laptops are indispensable in everyday life.

(a) study

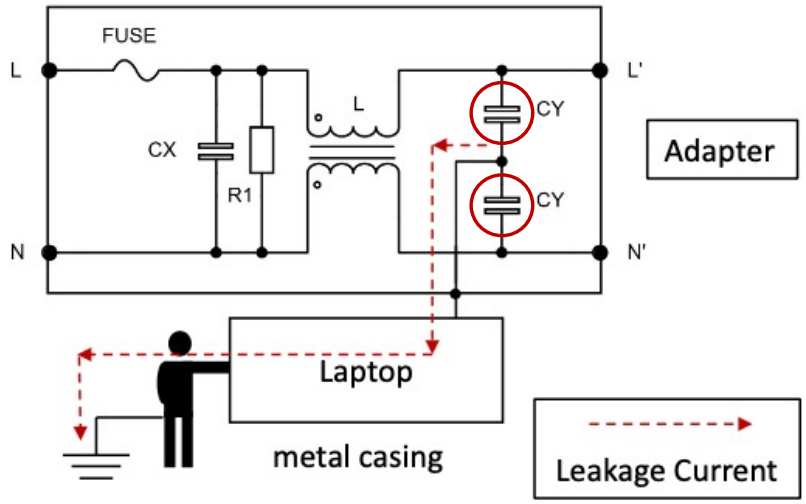
(b) work

(c) entertainment

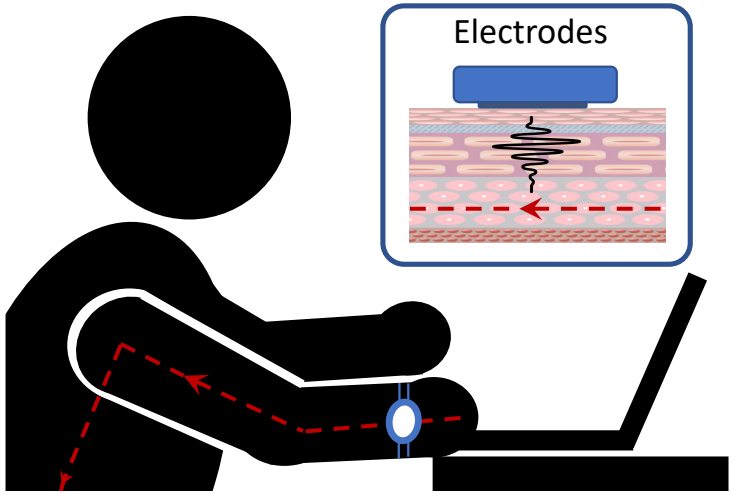
The potential threat of information leakage from electrodes cannot be ignored.

Preliminary

leakage current from laptops



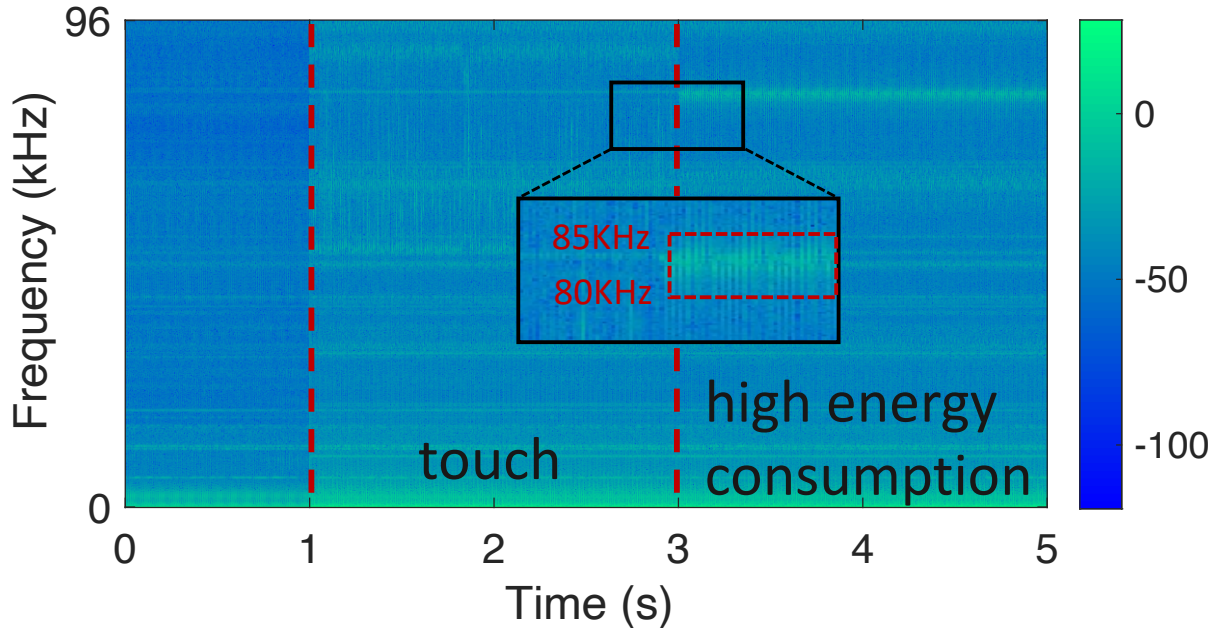
(a) safety capacitors in the adapter



(b) capture the current in the body with electrodes

Preliminary

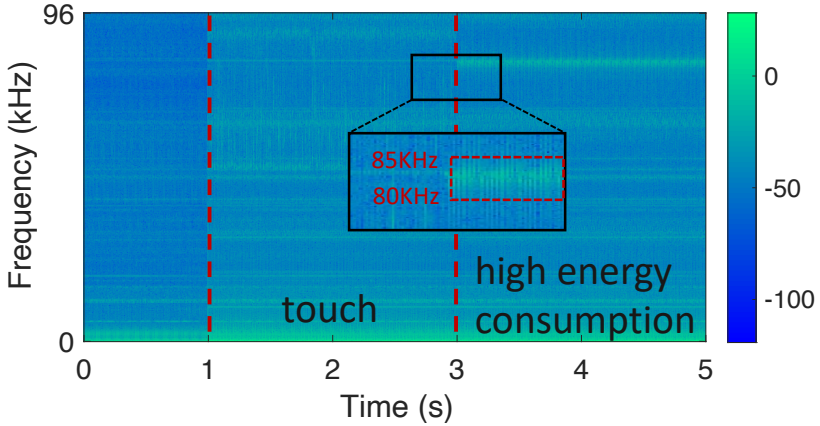
correlation between leakage current and laptop



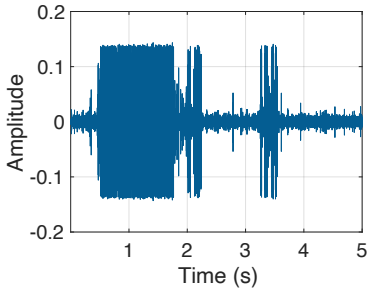
- user touch behavior detection
- CPU working condition monitoring

Preliminary

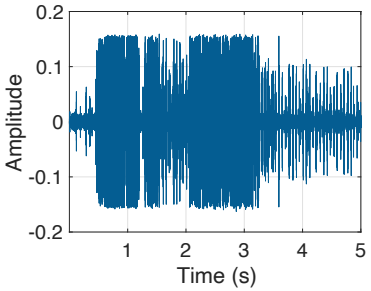
CPU operating state fluctuations driven by applications



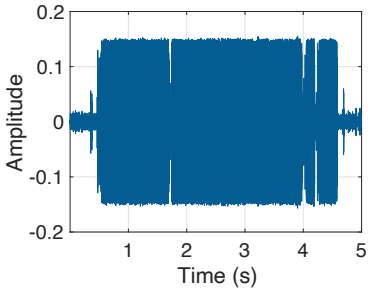
high-frequency fluctuations during application launching



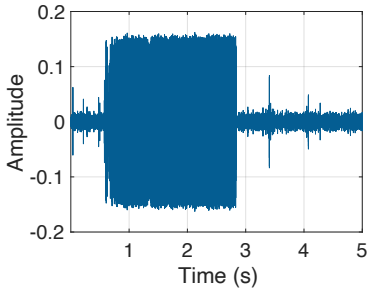
(a) Chrome



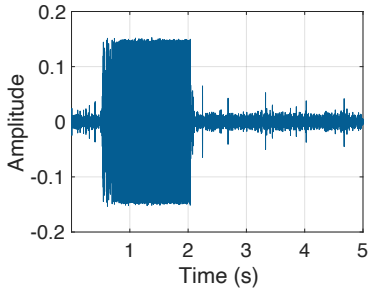
(b) Chess



(c) Pycharm

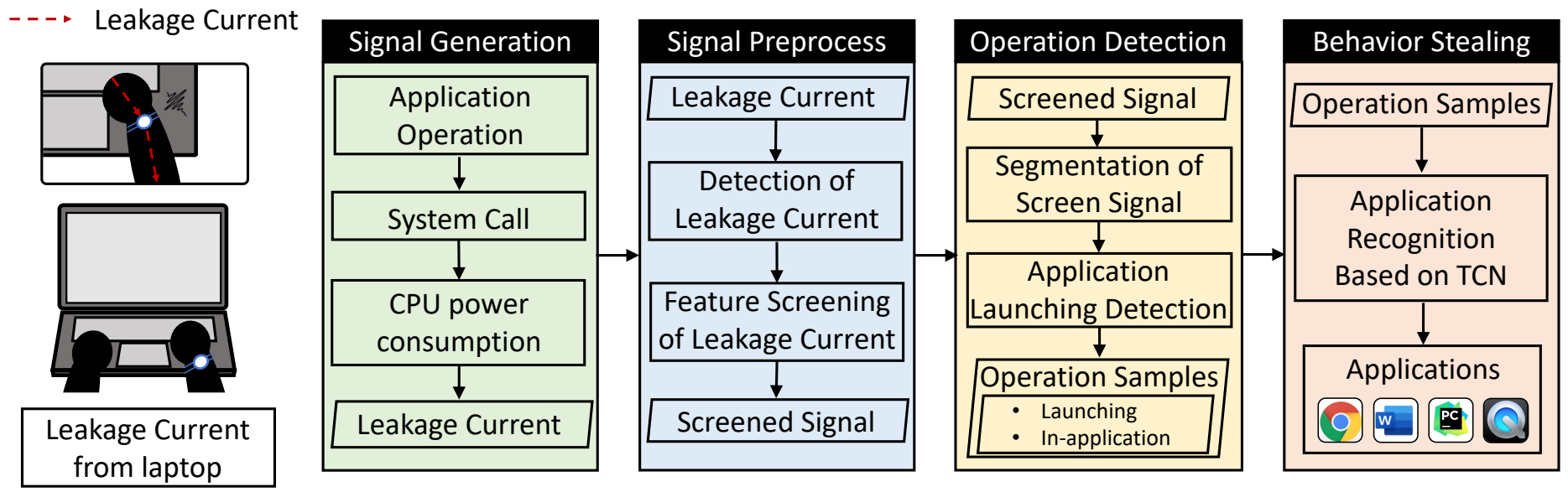


(d) QuickTime



(e) Word

System Overview

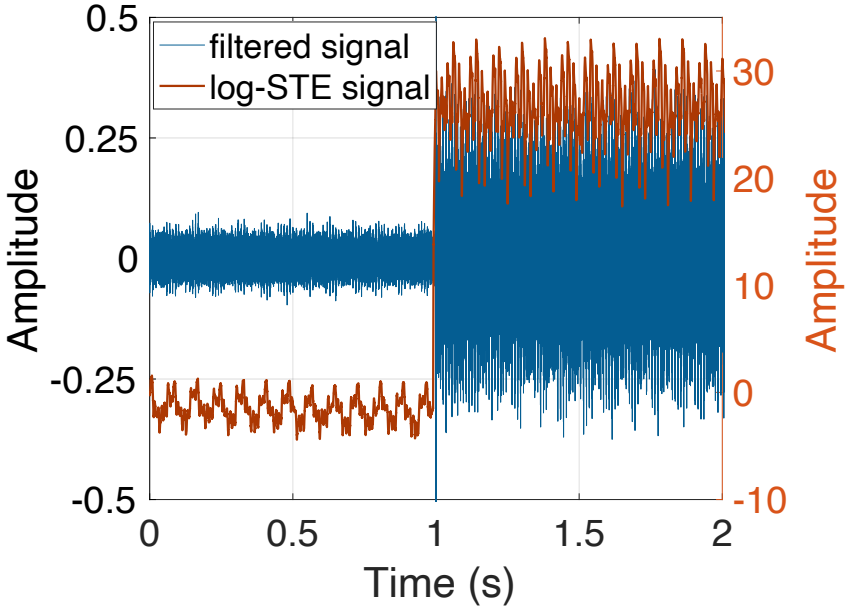


The victim uses a laptop with a metal casing and keeps the laptop charged

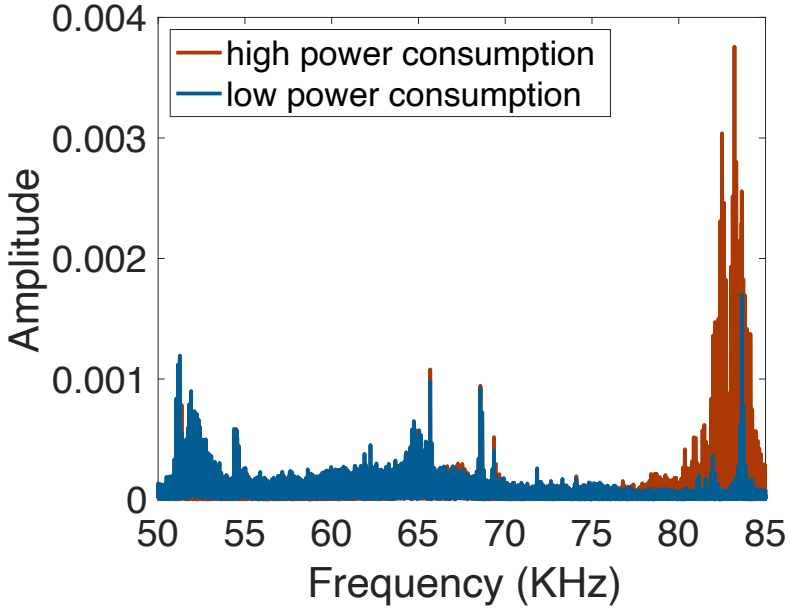
- **Not using gloves and external devices**
- **Wear a smartwatch with built-in electrode**

System

Preprocess of Leakage Current



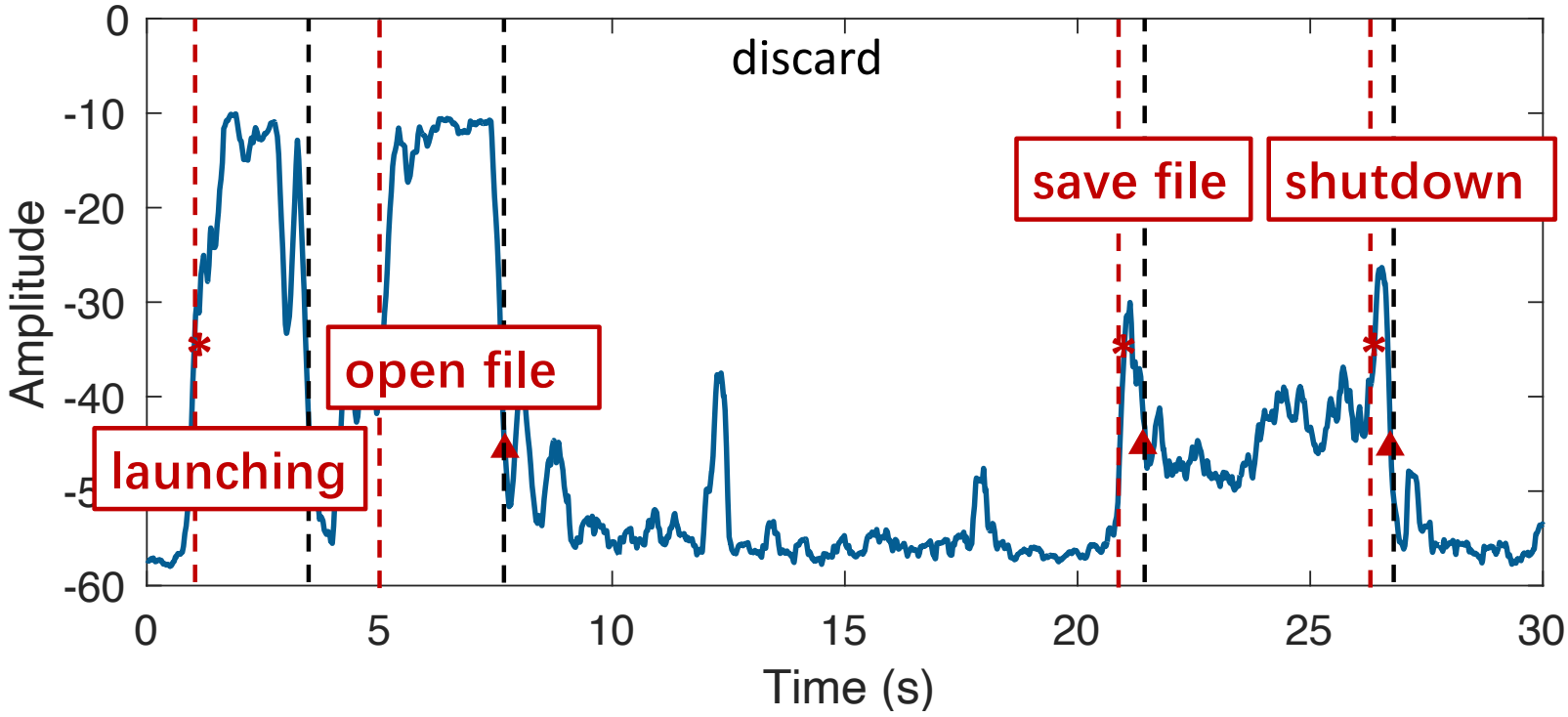
(a) touch detection



(b) frequency screening

System

Operation Segmentation



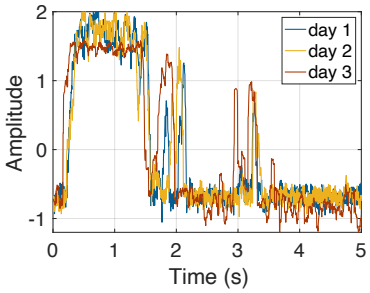
denoised leakage current of using Microsoft Word

System

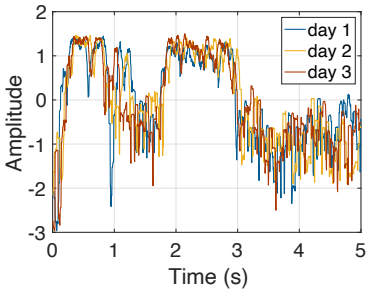
Application Recognition

Tab.1 summary of applications

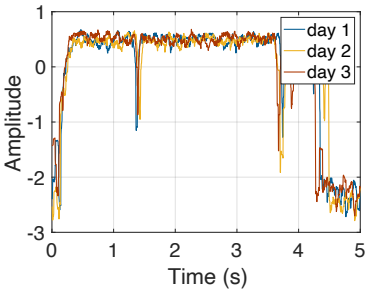
Category	Application list
Multimedia	QuickTime, IINA, AppleTV, NetEase Music
Office	Microsoft Word, Microsoft PPT, Sublime Text, Skim
Programming	PyCharm, CLion, Android Studio, Matlab
Browser	Chrome, Safari, FireFox
Game	Chess, Stardew Valley, Steam, Battle.Net
Social Networking	Zoom, Line, WeChat
Others	Audacity, WaveForms, iMovie



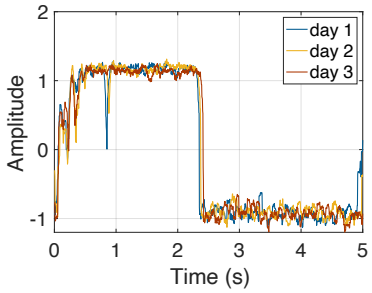
(a) Chrome



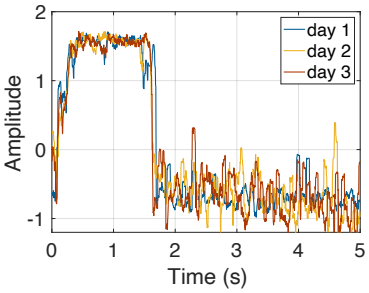
(b) Chess



(c) Pycharm



(d) QuickTime



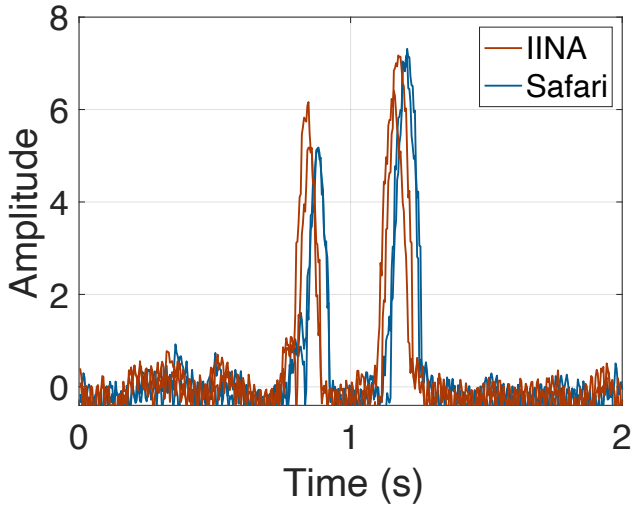
(e) Word

System

Application Recognition

Tab.2 application launching detection

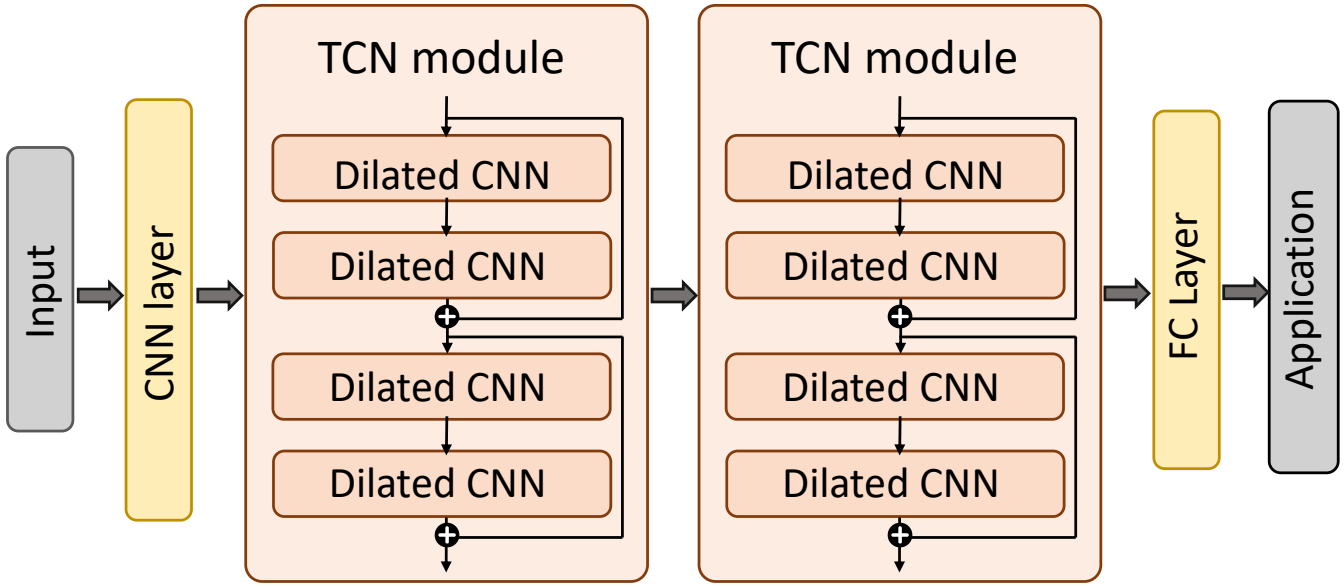
KNN	LDA	SVM	RF	CNN
93.7%	96.3%	98.6%	97.5%	99.3%



application shutdown poses similar features

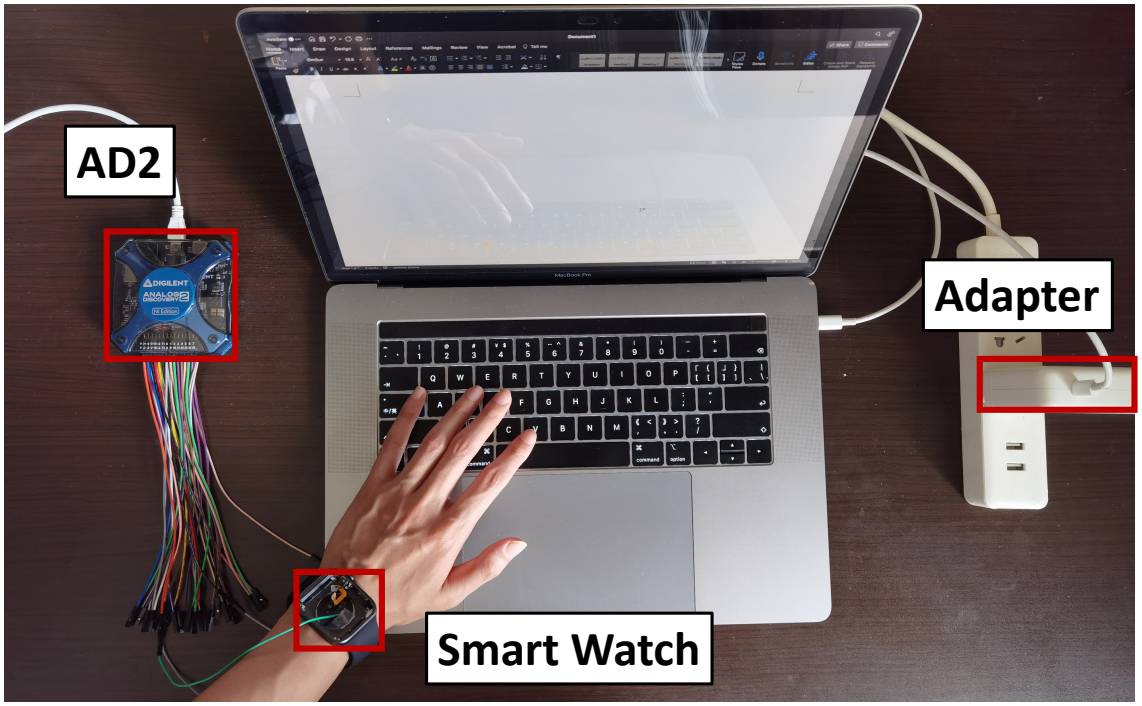
System

Application Recognition



TCN based application recognition network

Experimental Setup



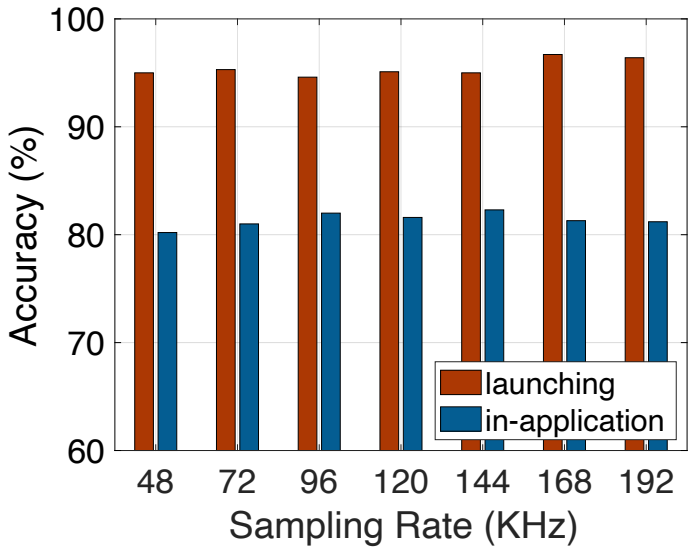
- ***User:*** use the laptop without **external devices and gloves**
- ***Smartwatch*:** leakage current acquisition via external AD2
- ***Laptop*:** connect to the adapter and keep in charge

Evaluation

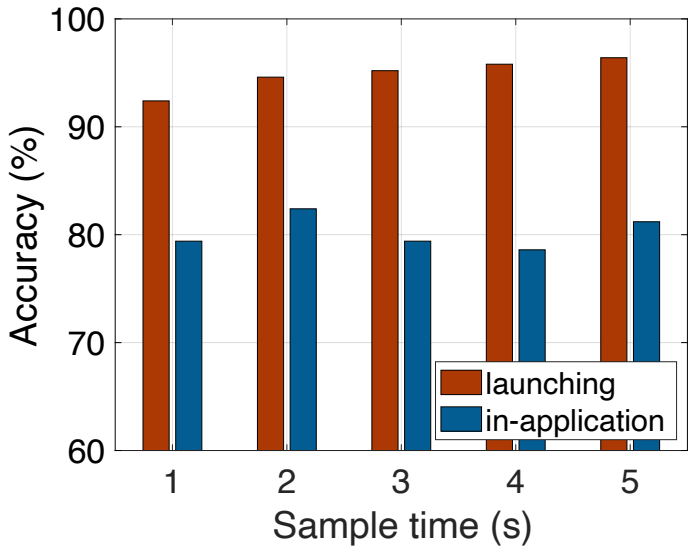
Mirco Benchmark

App category: 7
App number: 25

launching process: 97.5%
In-application operation: 83.8%



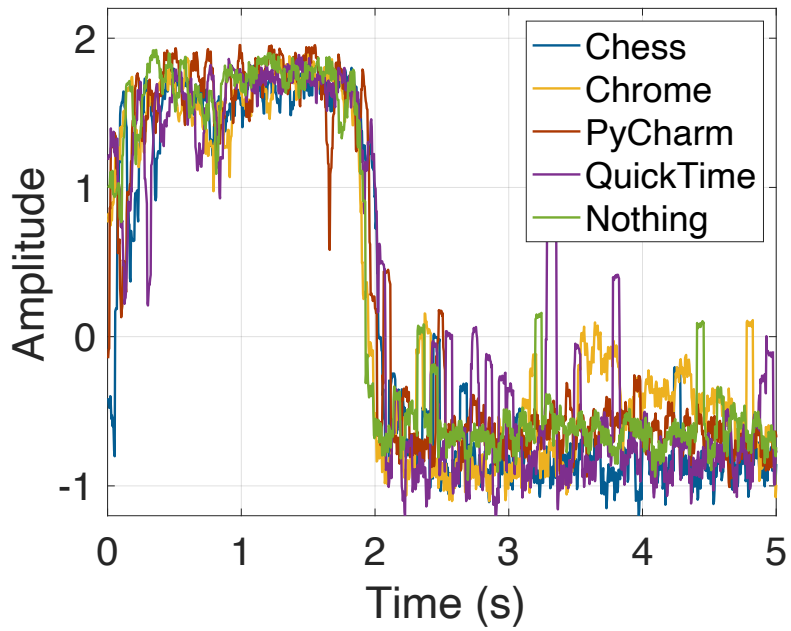
(a) influence of sampling rate



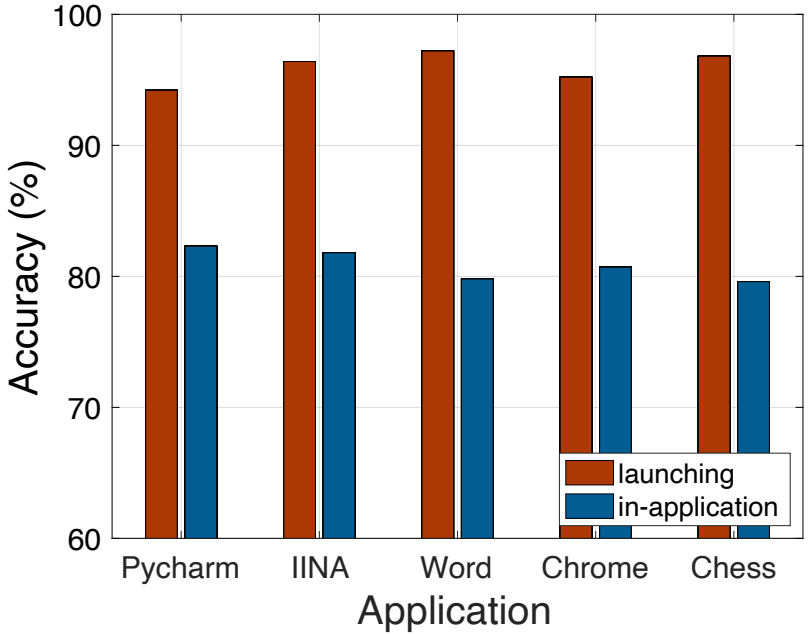
(b) influence of sampling time

Evaluation

Influence of other applications



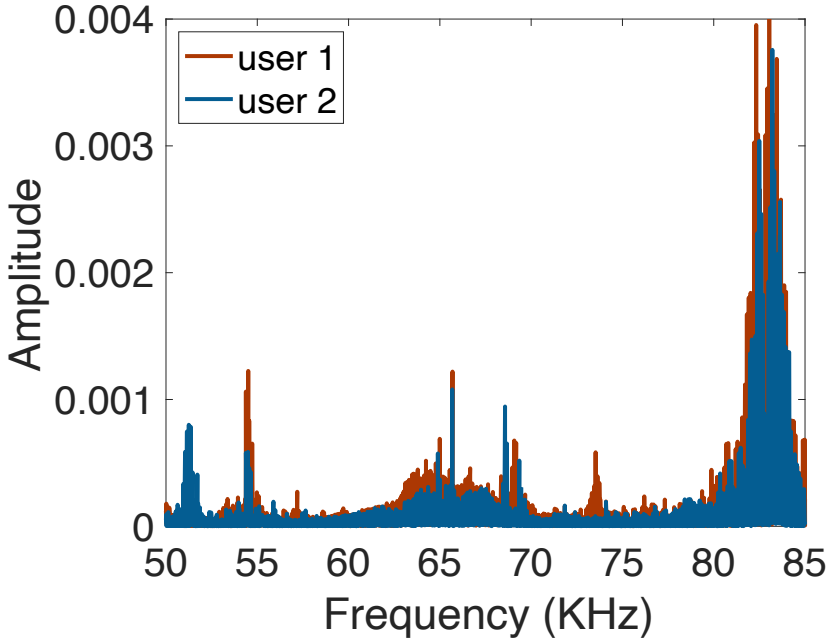
(a) launching process of Word



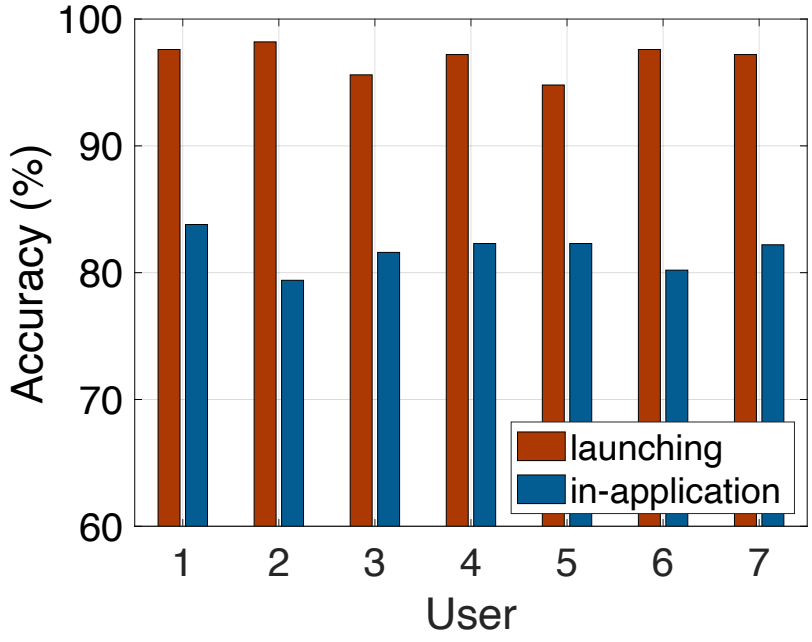
(b) application recognition accuracy

Evaluation

Influence of different users



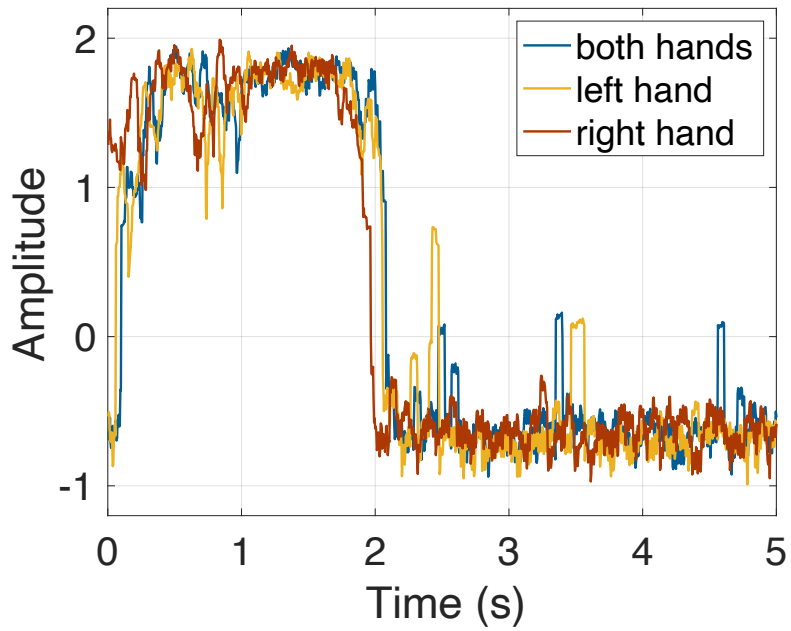
(a) spectrogram of different users



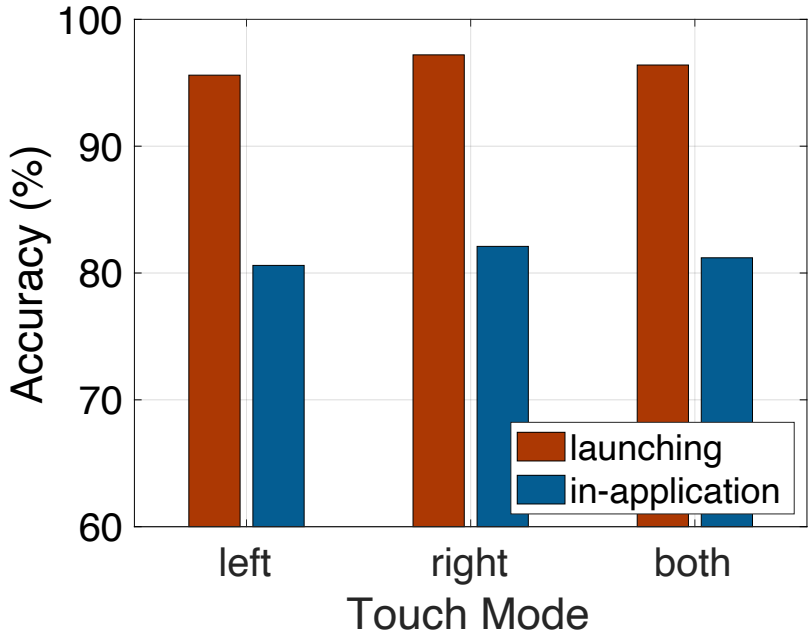
(b) application recognition accuracy

Evaluation

Influence of touch mode



(a) launching process of Word



(b) application recognition accuracy

Discussion

Defense

hardware-based: **disconnect the laptop from the adapter** to cut off the source of the signals
use an external mouse and keyboard to avoid direct contact with the laptop

software-based: add random noise to the leakage current by **randomly modulating the CPU**

Limitation

sampling rate: **low sampling rate available** in commercially devices

permission: **lack the API** for accessing the built-in electrode

Conclusion

- Reveals **the information security risks** of **built-in electrodes** in wearable devices**.**
- Validated **the correlation** between the **leakage current** and the **CPU operating state** of a laptop.
- Implemented **user behavior sniffing** based on **application launching** and **in-application operations.**

Thank you !