UNIVERSITY OF TEXAS ARLINGTON | COLLEGE OF ENGINEERING

TEXAS TECH UNIVERSITY

Continuous Authentication Using Human-Induced Electric Potential

Srinivasan Murali, *Wenqiang Jin, Vighnesh Sivaraman, Huadi Zhu, Tianxi Ji, Pan Li, Ming Li*

ACSAC 2023

CASE WESTERN RESERVE UNIVERSITY

HUNAN UNIVERSITY

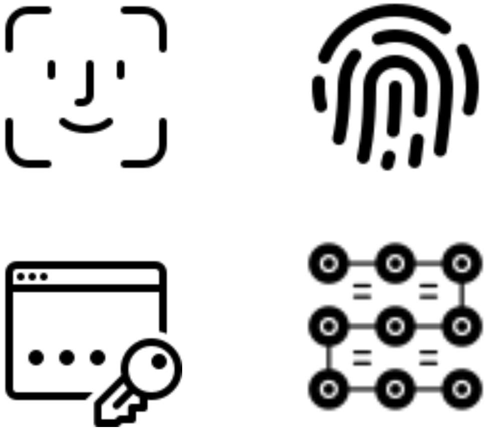
Motivation

- Shared workspaces:
  - Same room/individual cubic
- Terminals:
  - Store sensitive information
  - Security issue

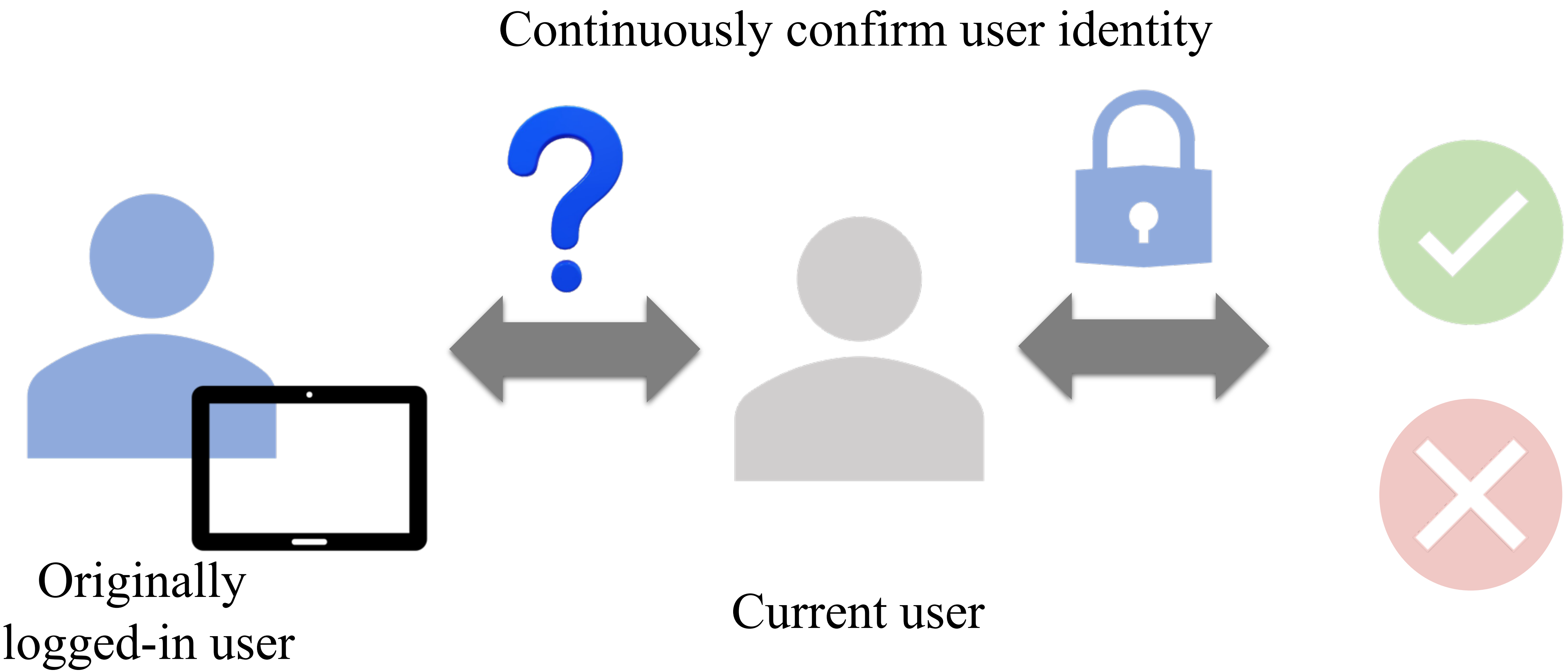
Motivation

- Shared workspaces:
  - Same room/individual cubic
- Terminals:
  - Store sensitive information
  - Security
- Conventio
  - Lim
    - V

One-time authentication is not enough!



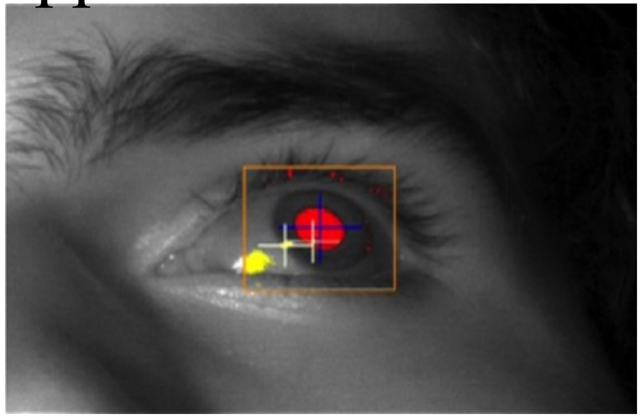
Continuous authentication



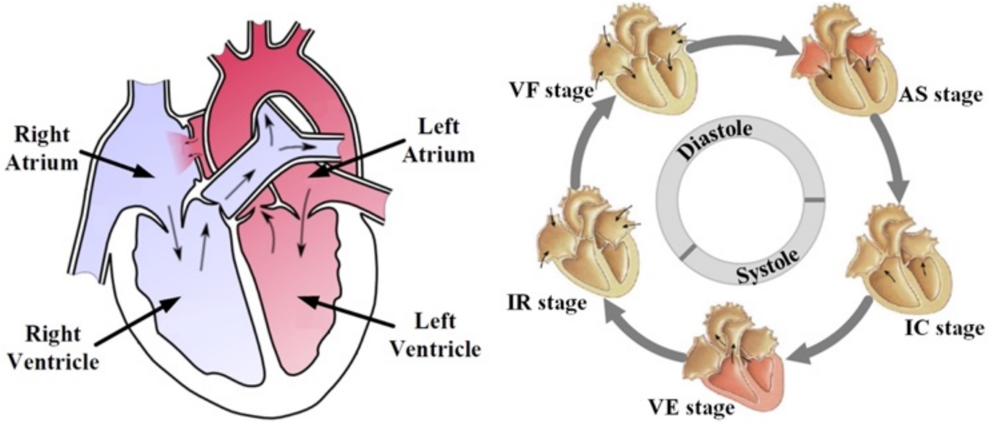
Related works

Physiological-based approaches:

ECG/PPG

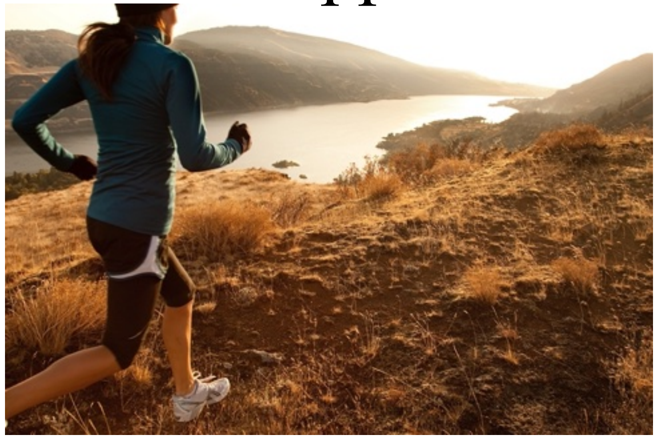


Eye-based

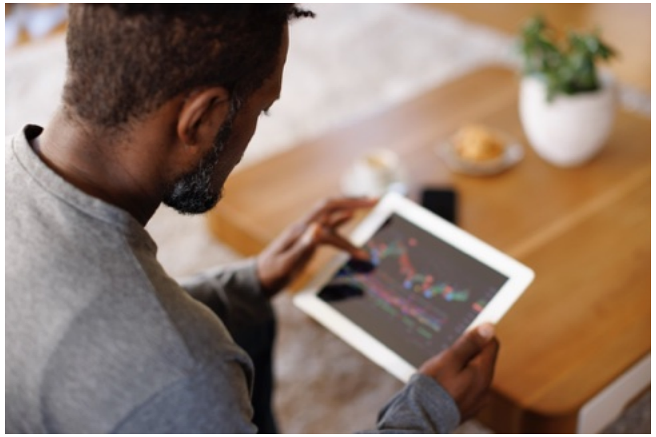


Heart based

Behavioral-based approaches:



Gait



Touch Gesture

Keystroke

Related works

Other approaches:

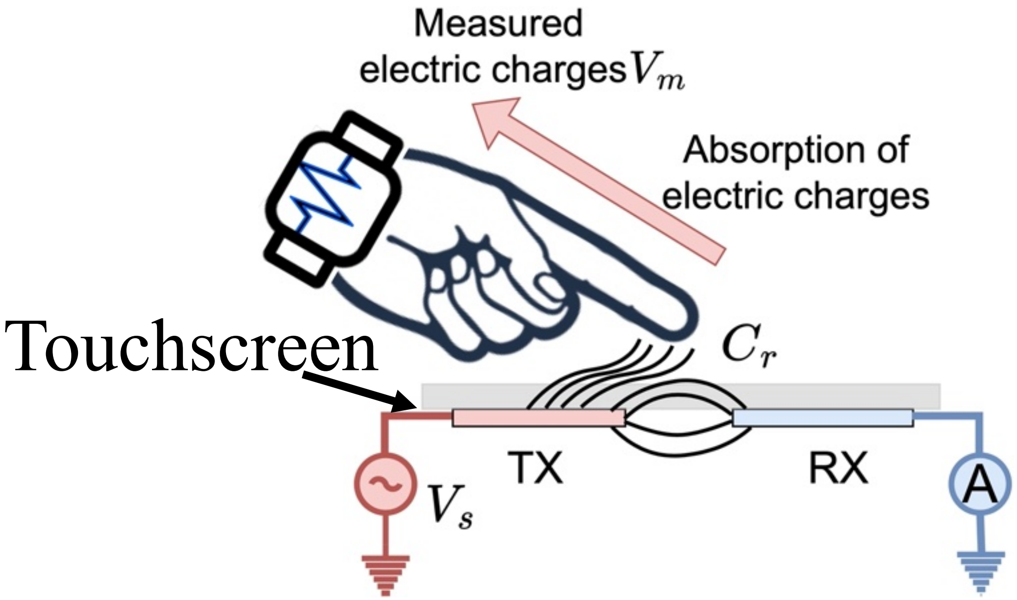
Proximity

Sub-meter accuracy issues

Timeout

Not entirely risk-free

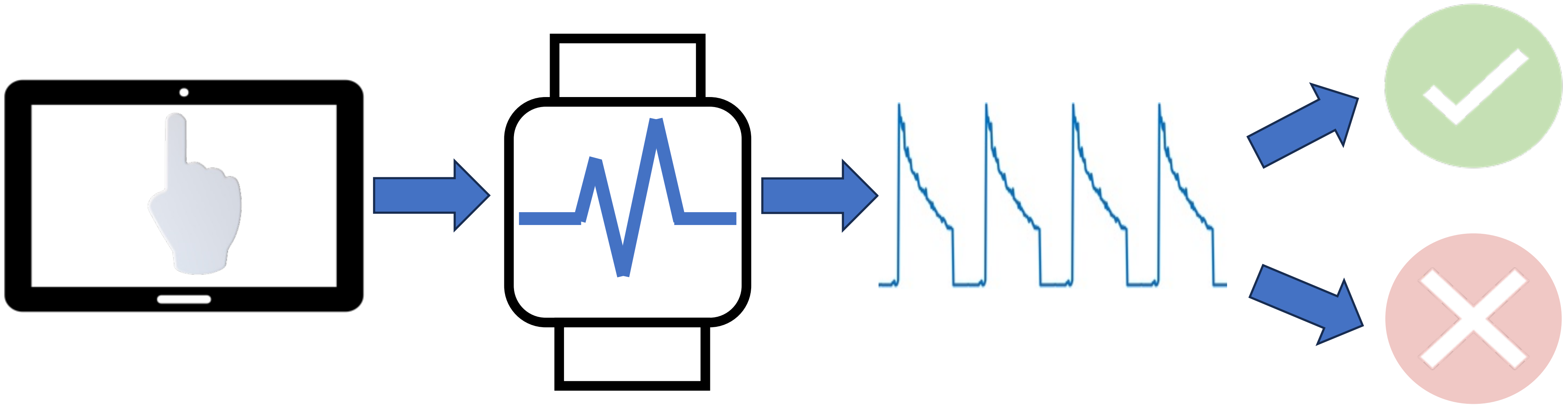
Background



A new type of signal:
Human-induced electric potential

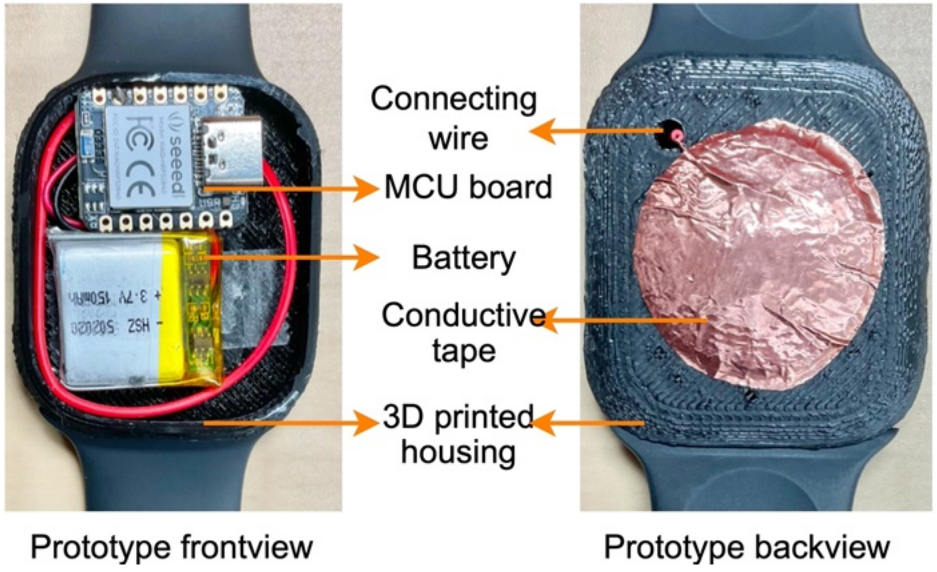
Overview

Leverage human-induced electric potential for continuous authentication

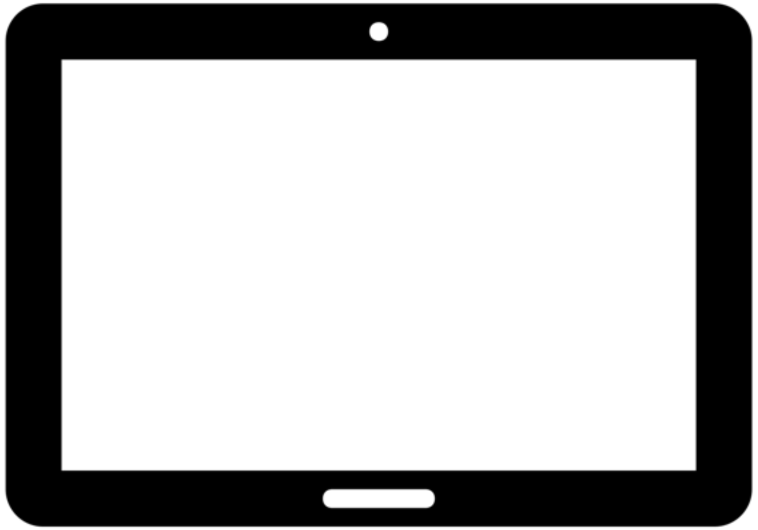


Feasibility study

- Experimental setup:
    - nRF52 MCU board-based wearable and Android tablet (Terminal)

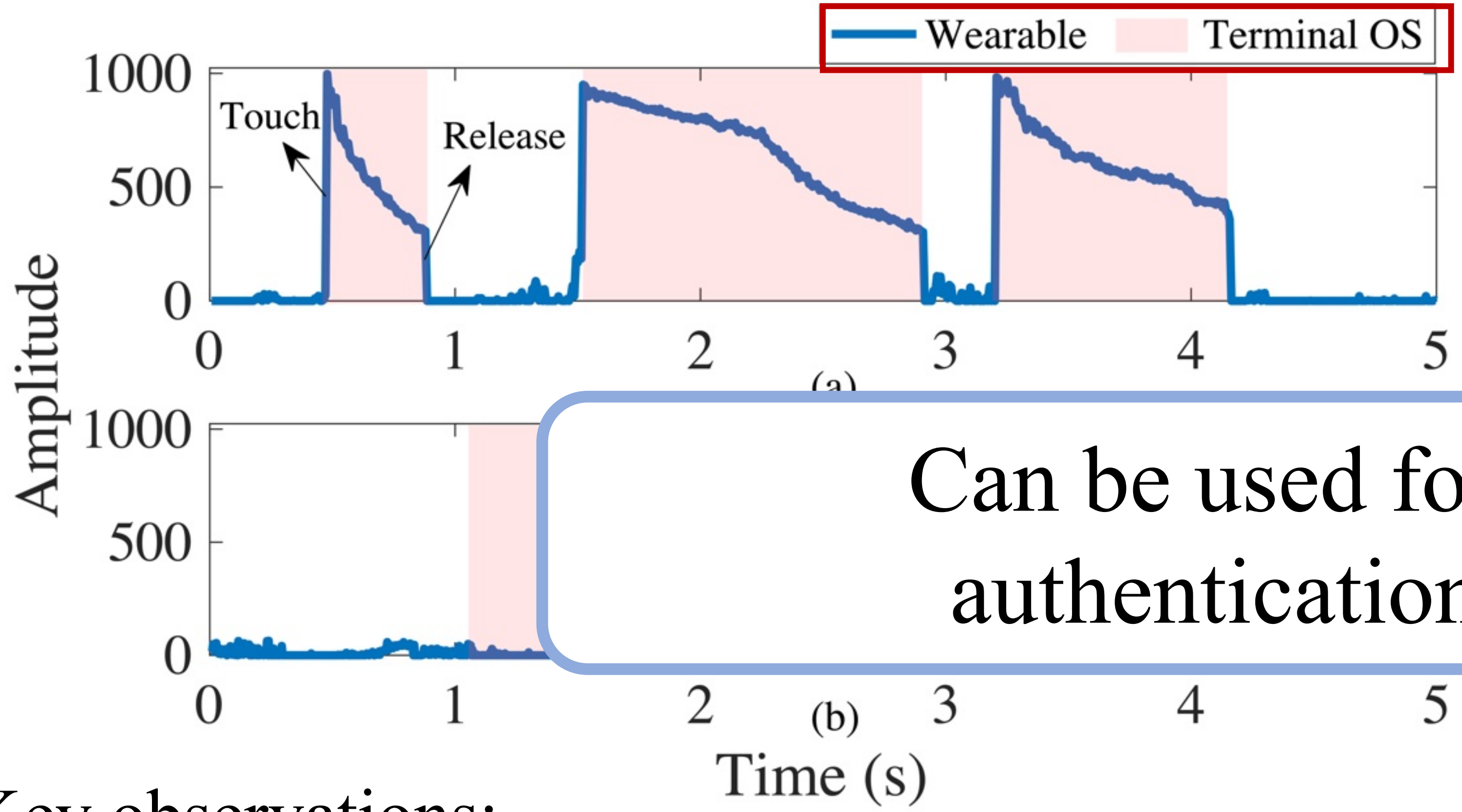


Wearable



Terminal

Feasibility study



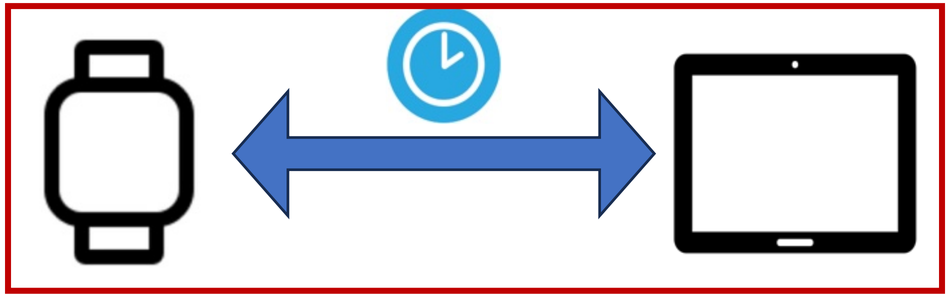
Legit user interacts with terminal

Can be used for authentication

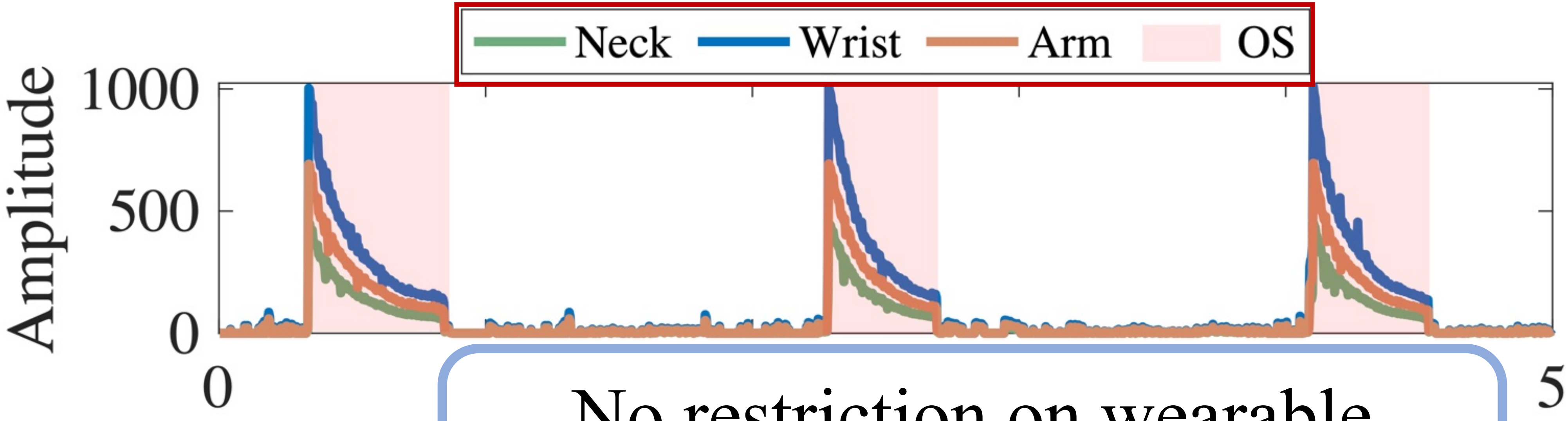
versary interacts with terminal

Key observations:

- Two sources' touch timestamps match well only for legitimate user



Feasibility study



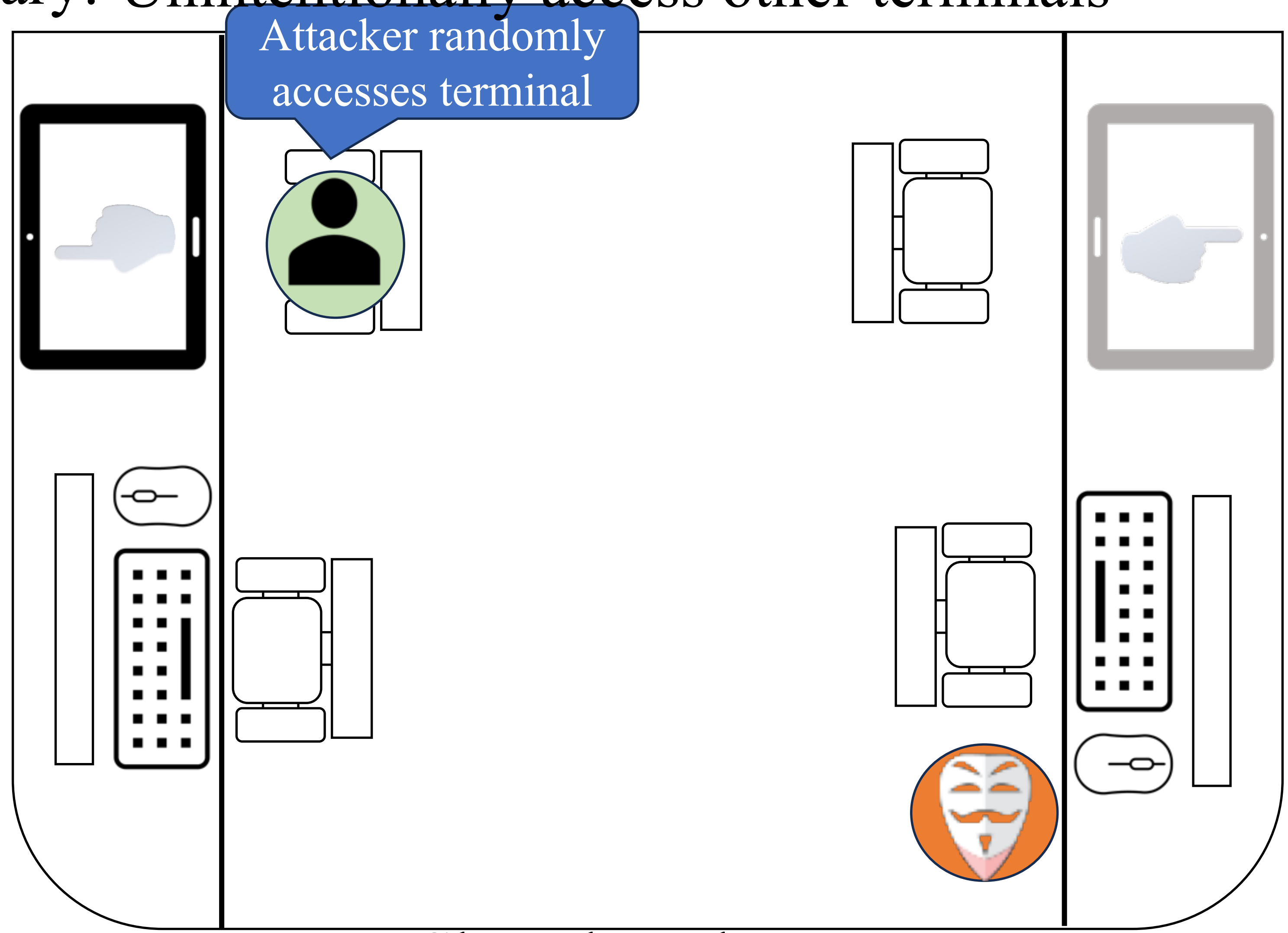
No restriction on wearable placement

Key observations:

- Two sources' touch timestamps match at different body positions as well

Adversarial model

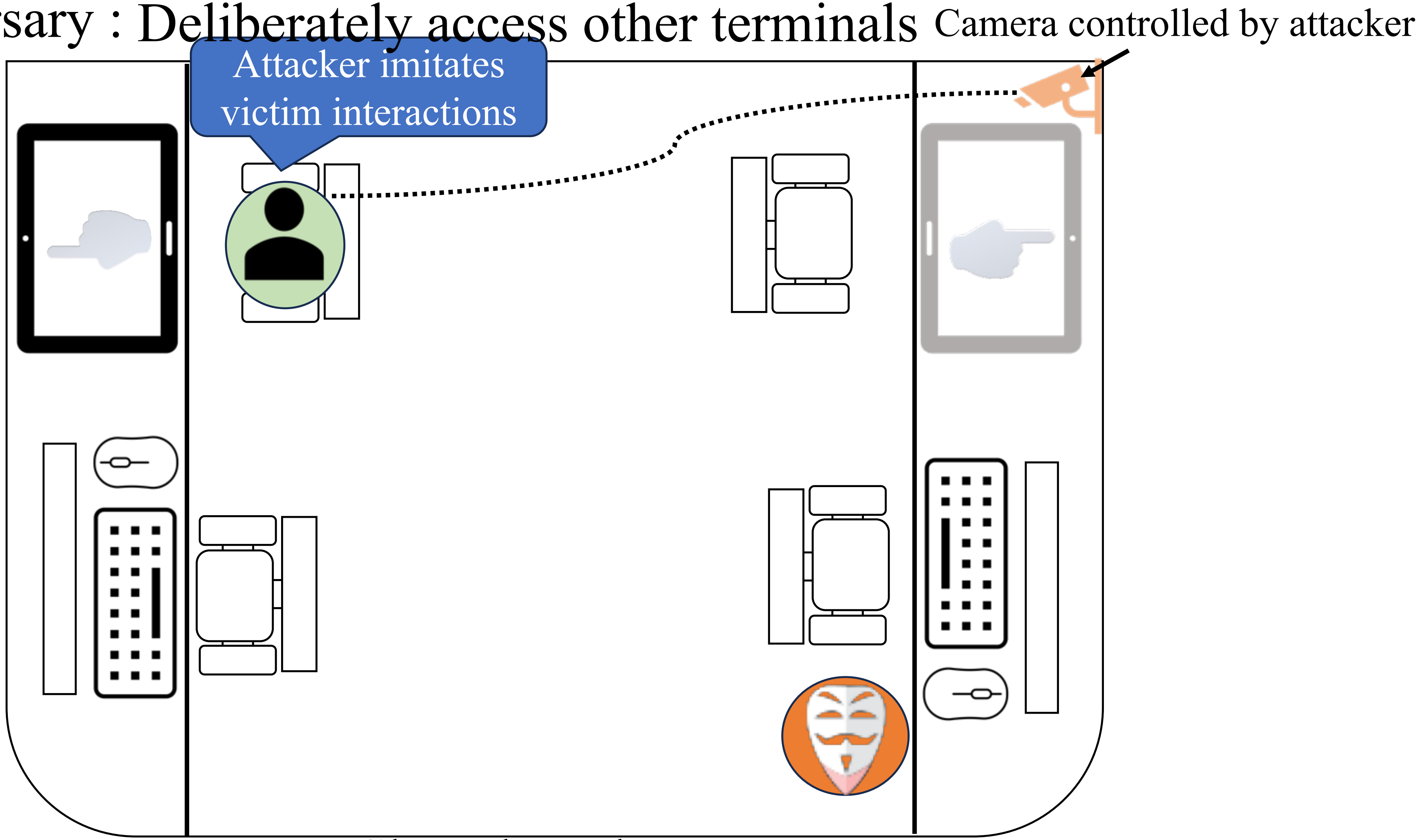
Innocent adversary: Unintentionally access other terminals



Shared workspace

Adversarial model

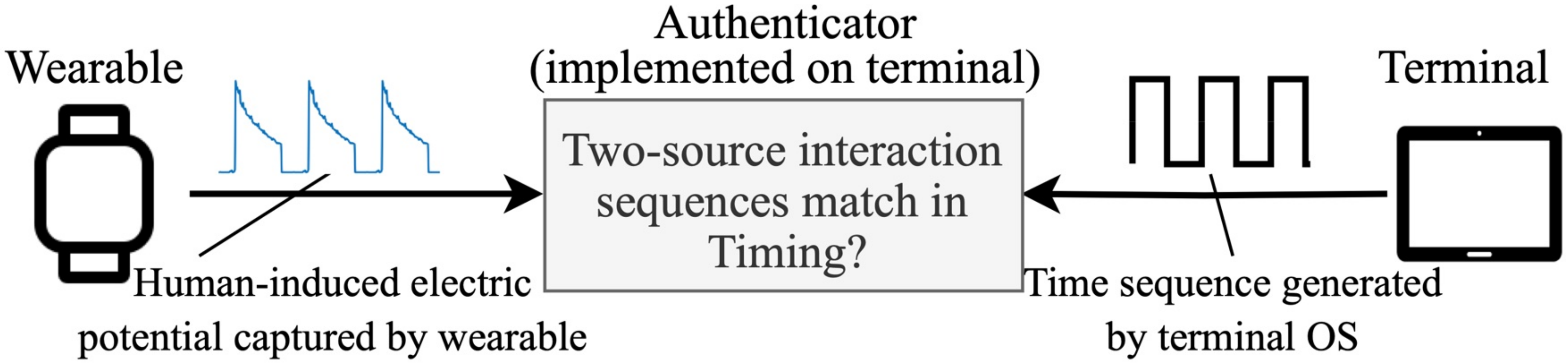
Malicious adversary : Deliberately access other terminals



Shared workspace

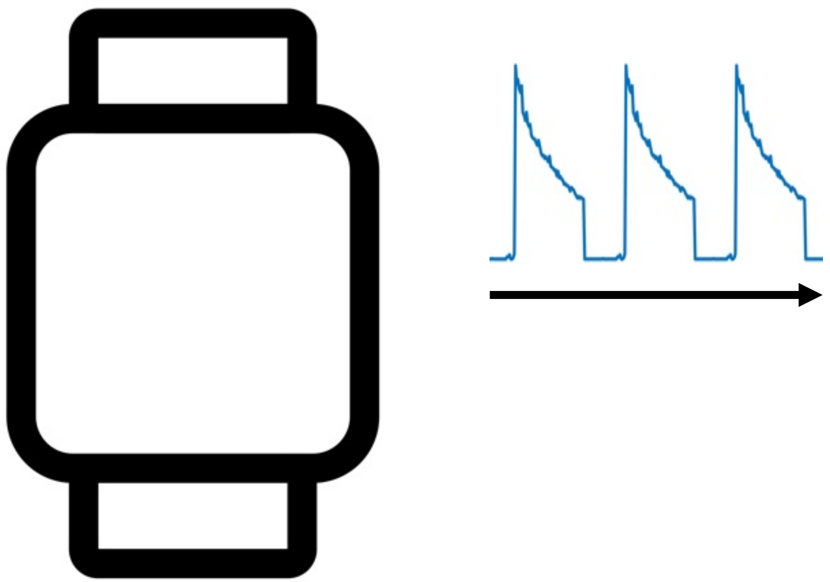
Handling the innocent adversary

Basic scheme:



Basic scheme

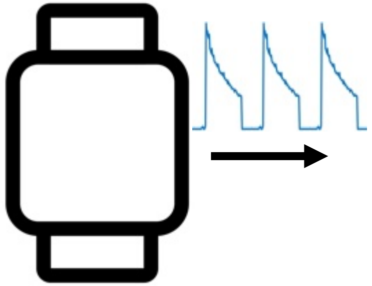
Signal acquisition:



Wearable

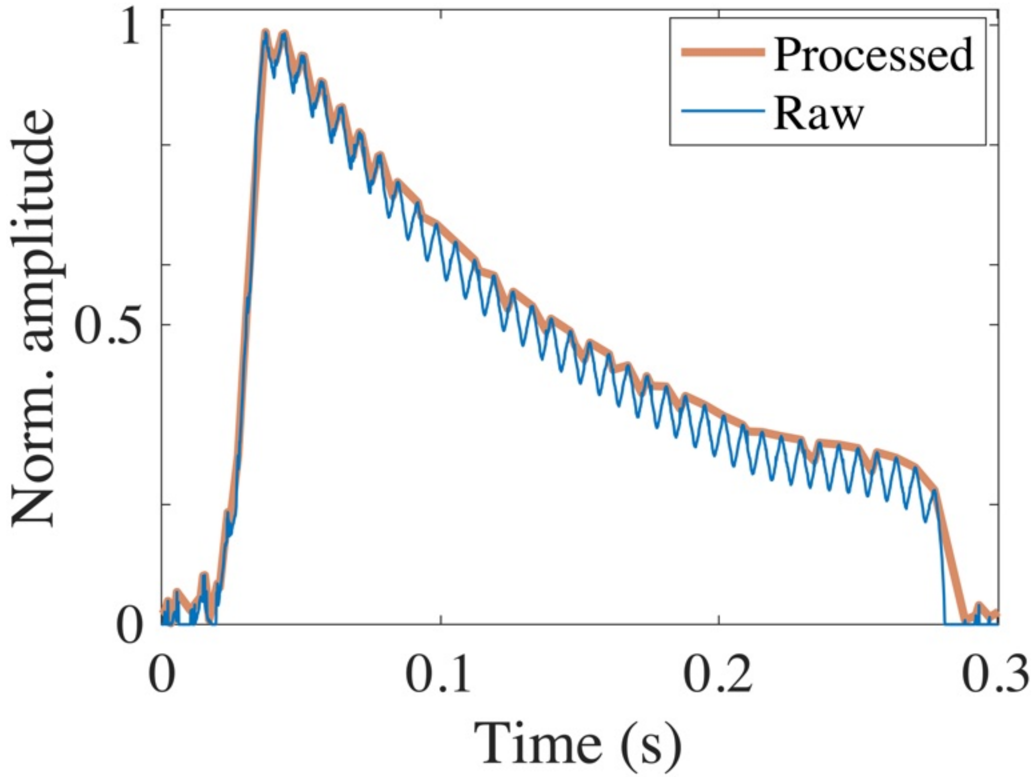
Acquire signal using wearable prototype

Basic scheme



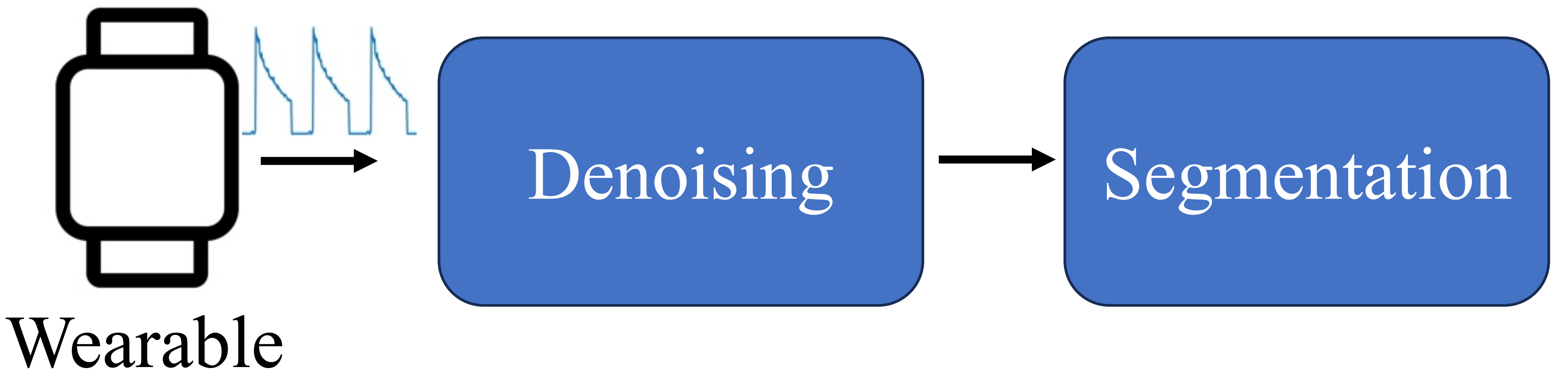
Wearable

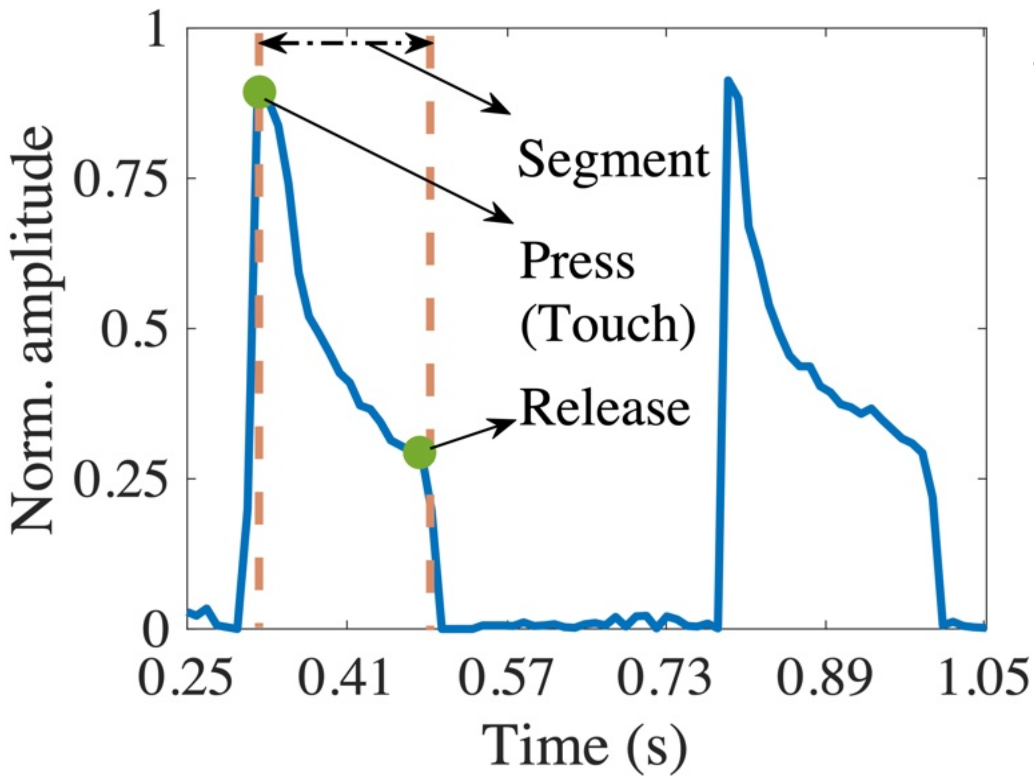
Denoising



Refine signal

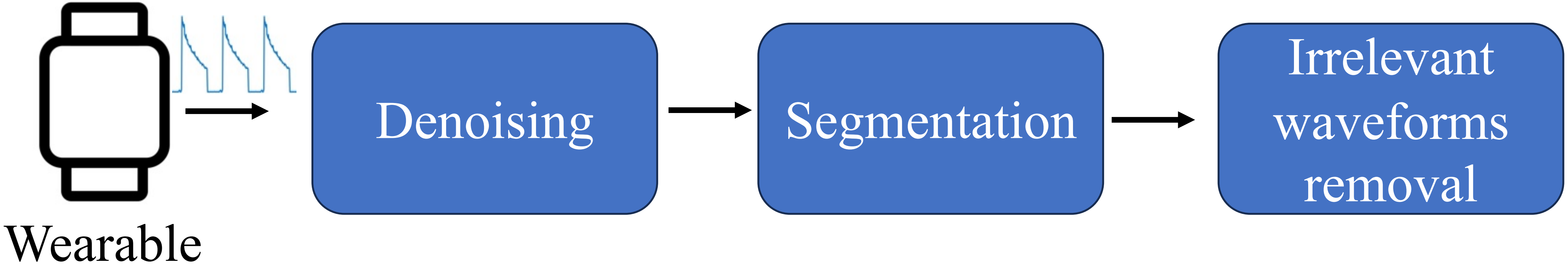
Basic scheme

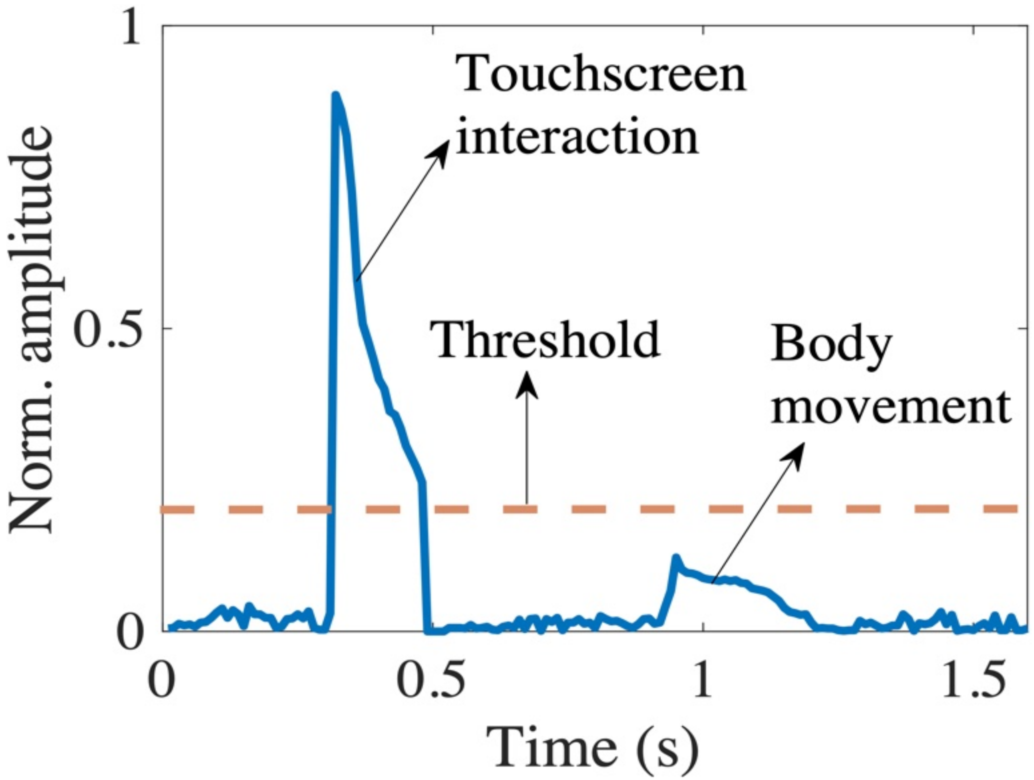




- Identify critical time instances

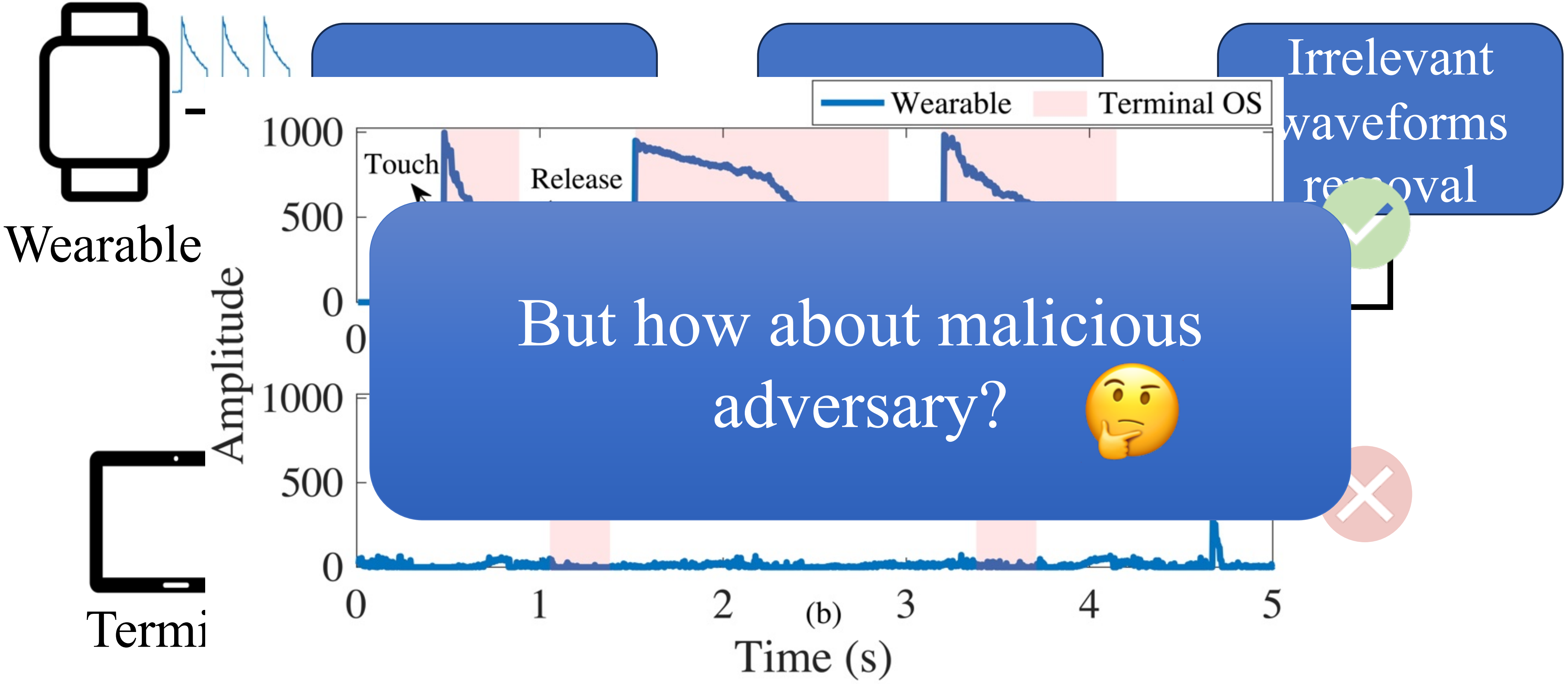
Basic scheme





To remove impact of user movement

Basic scheme

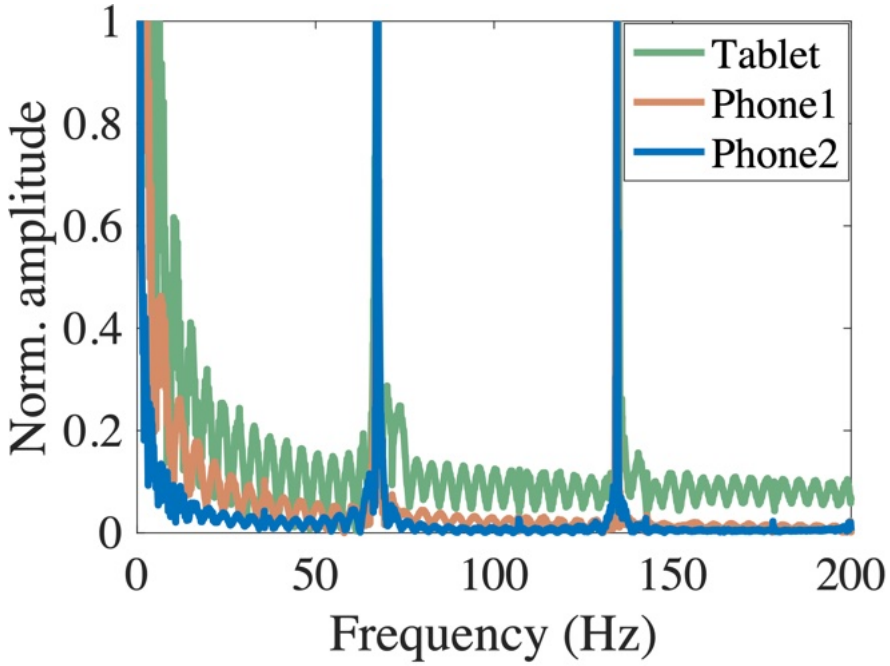


Compare two source sequences of press/release

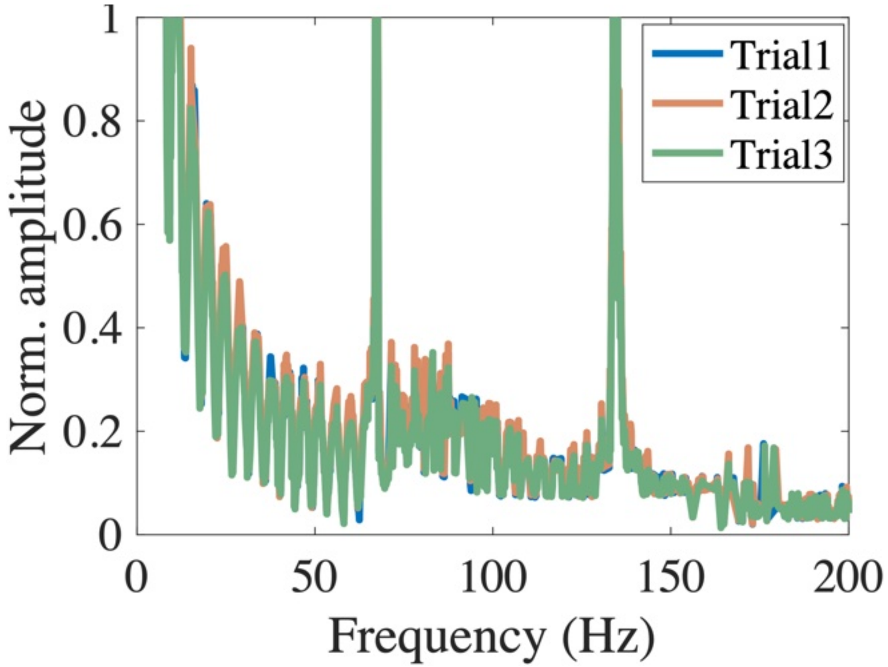
Handling the malicious adversary

- Terminal fingerprinting

Different for different terminals

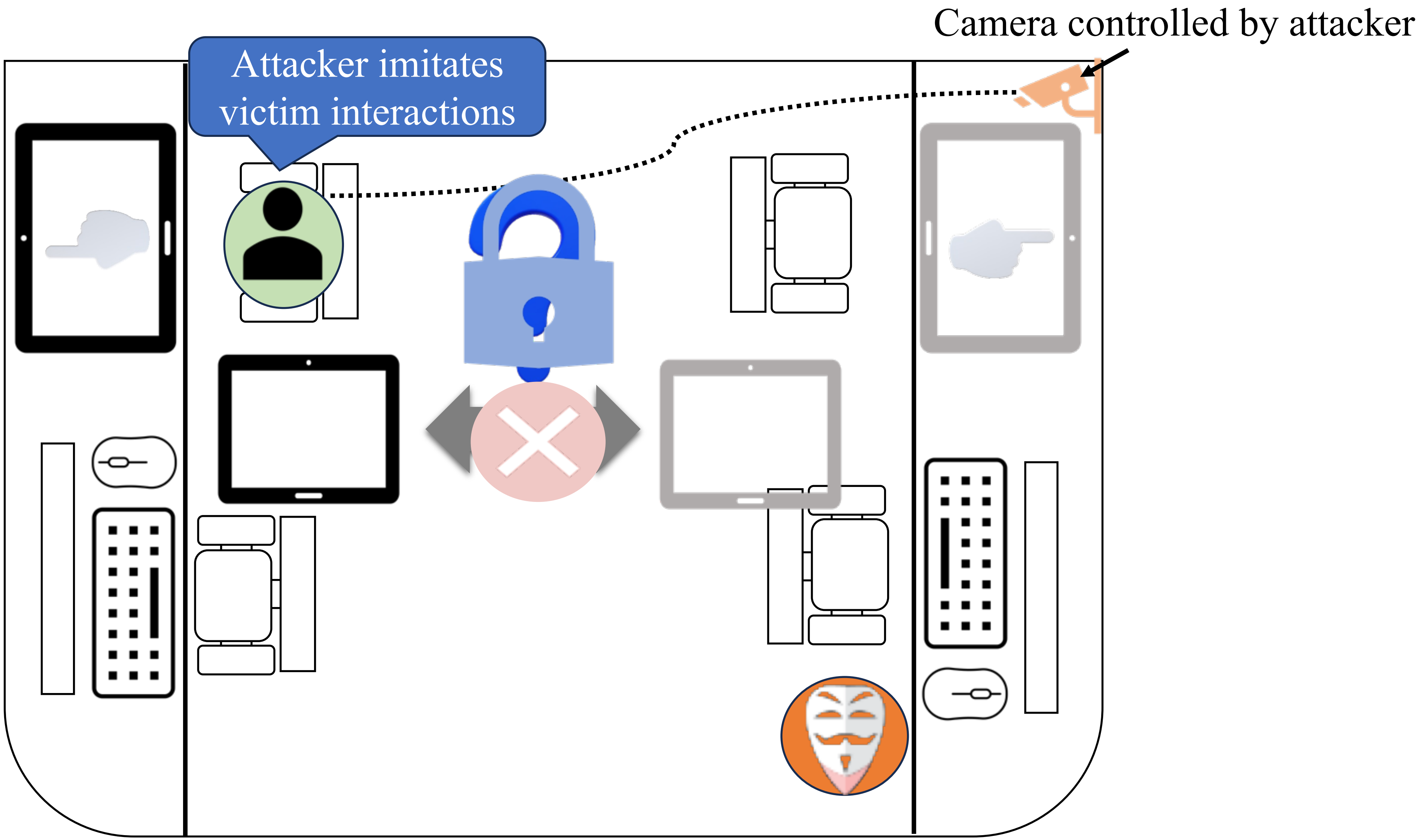


Same for same terminal

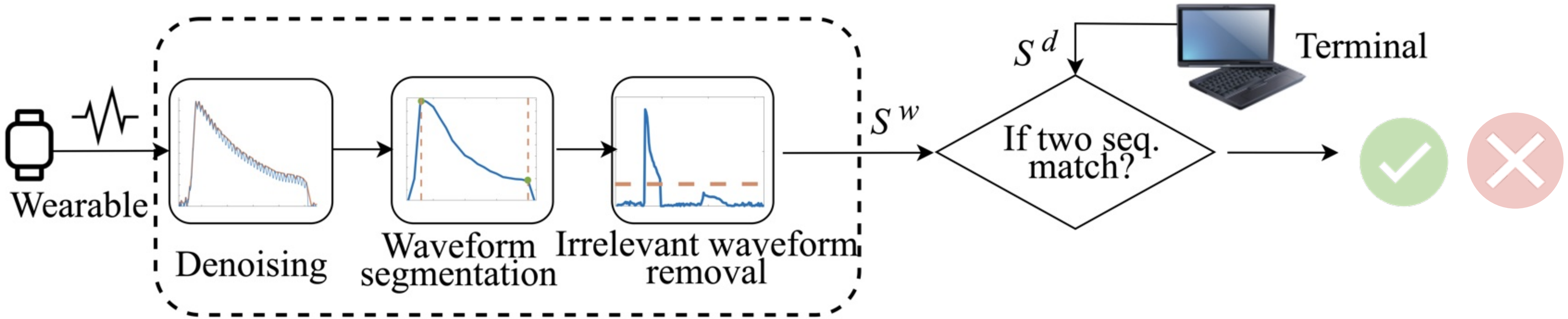


- Leverage terminal's fingerprint as an additional layer of defense

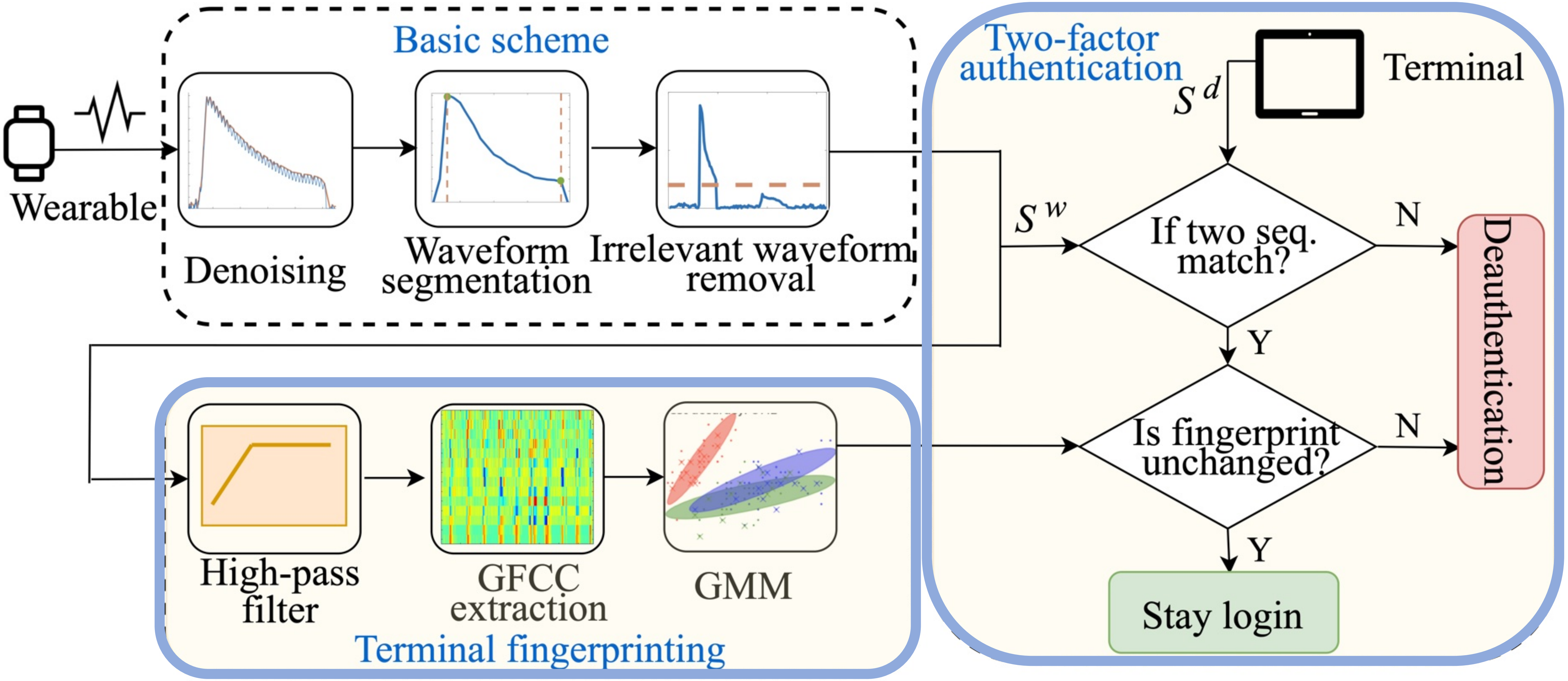
Handling the malicious adversary



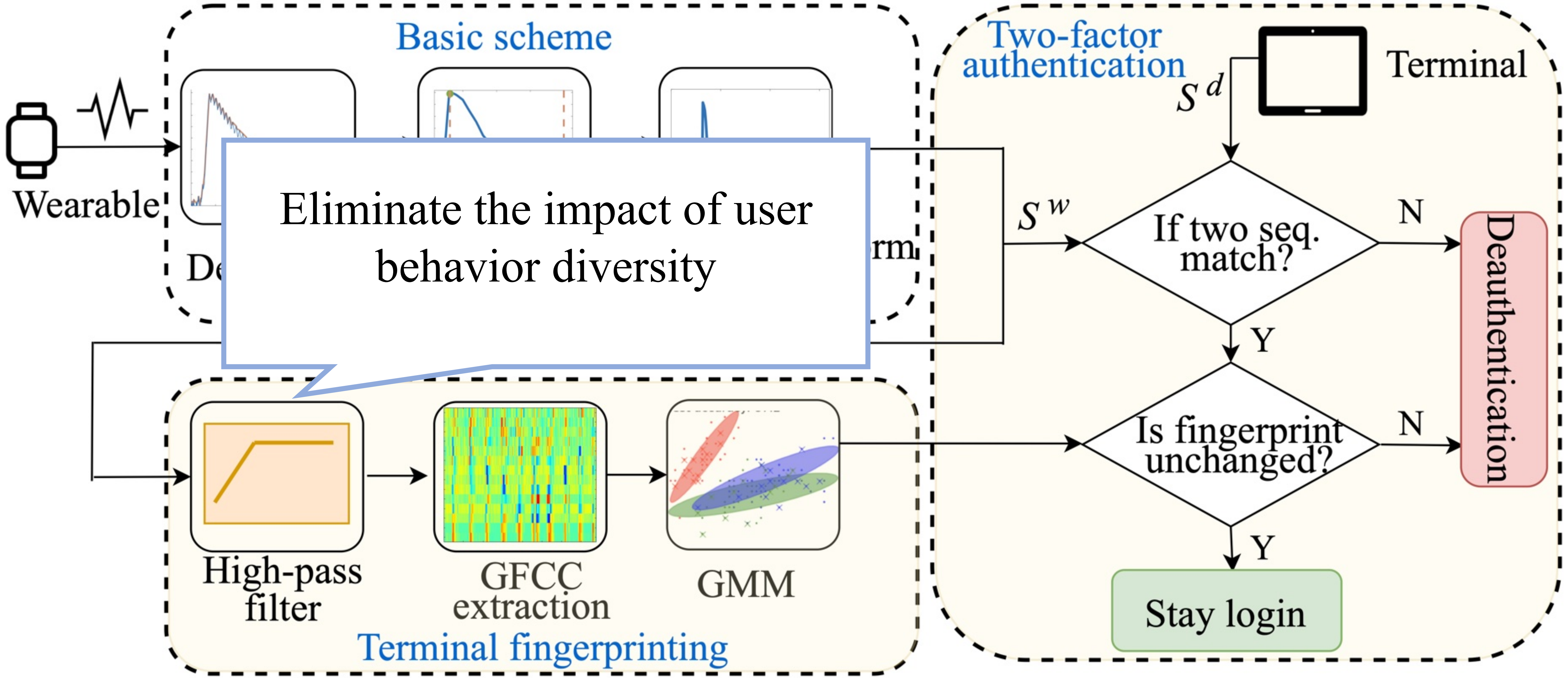
Basic pipeline



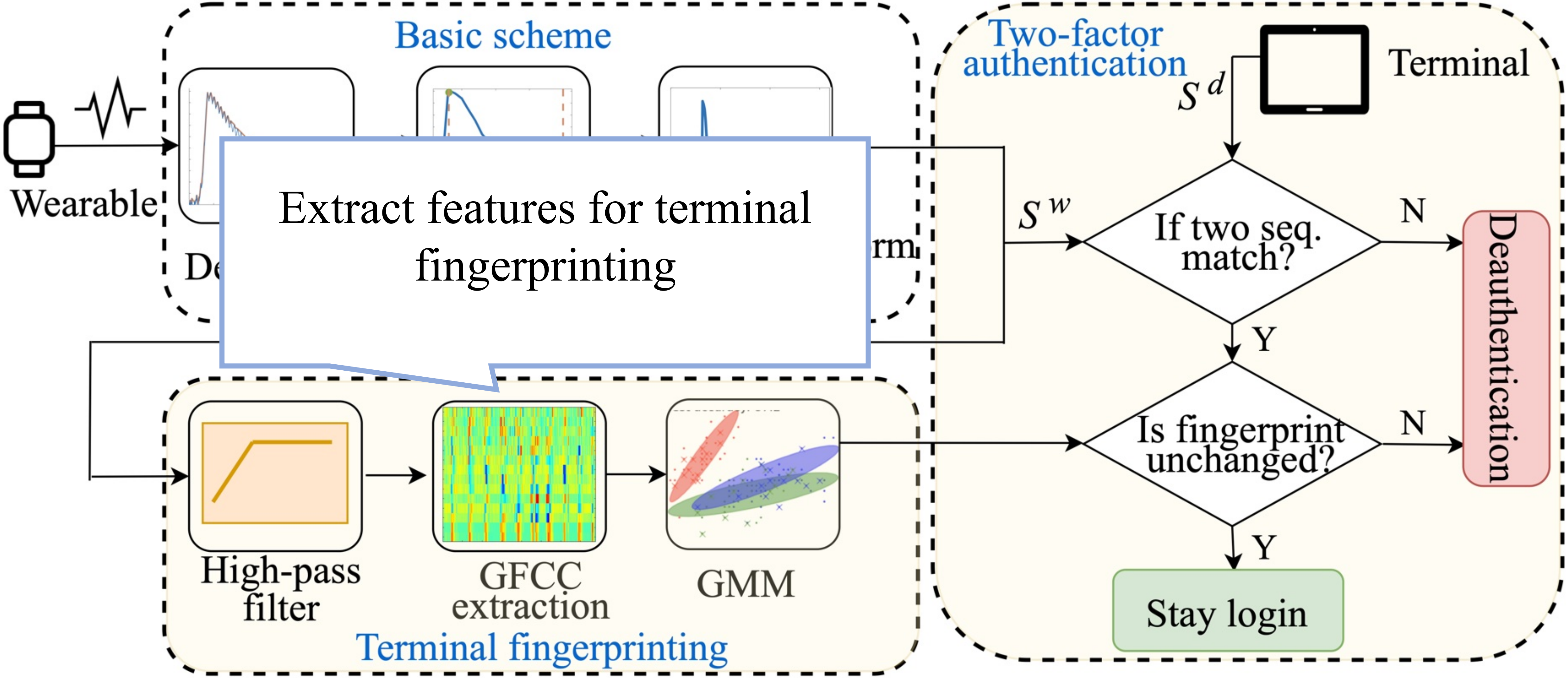
Modified pipeline



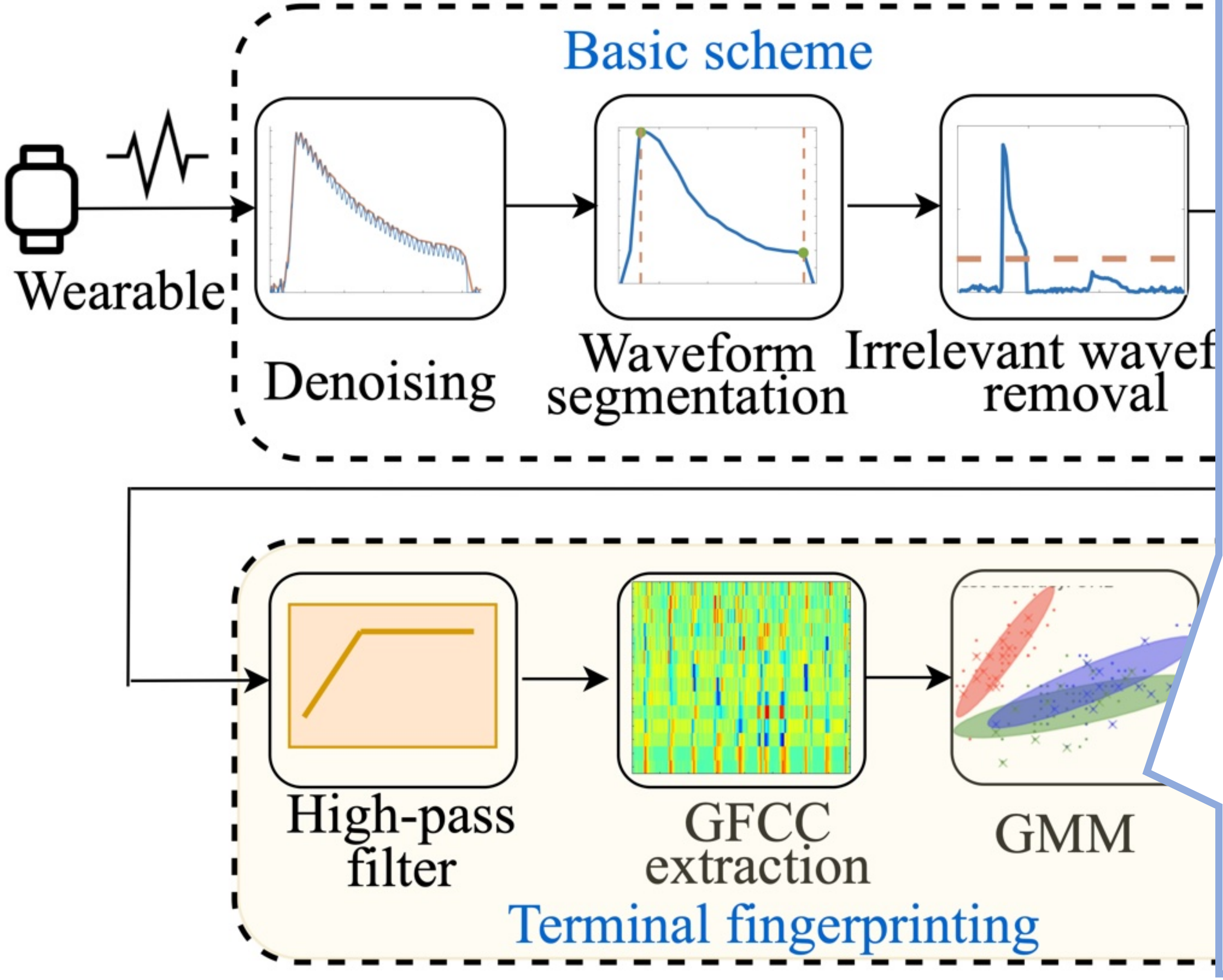
Modified pipeline



Modified pipeline



Modified pipeline

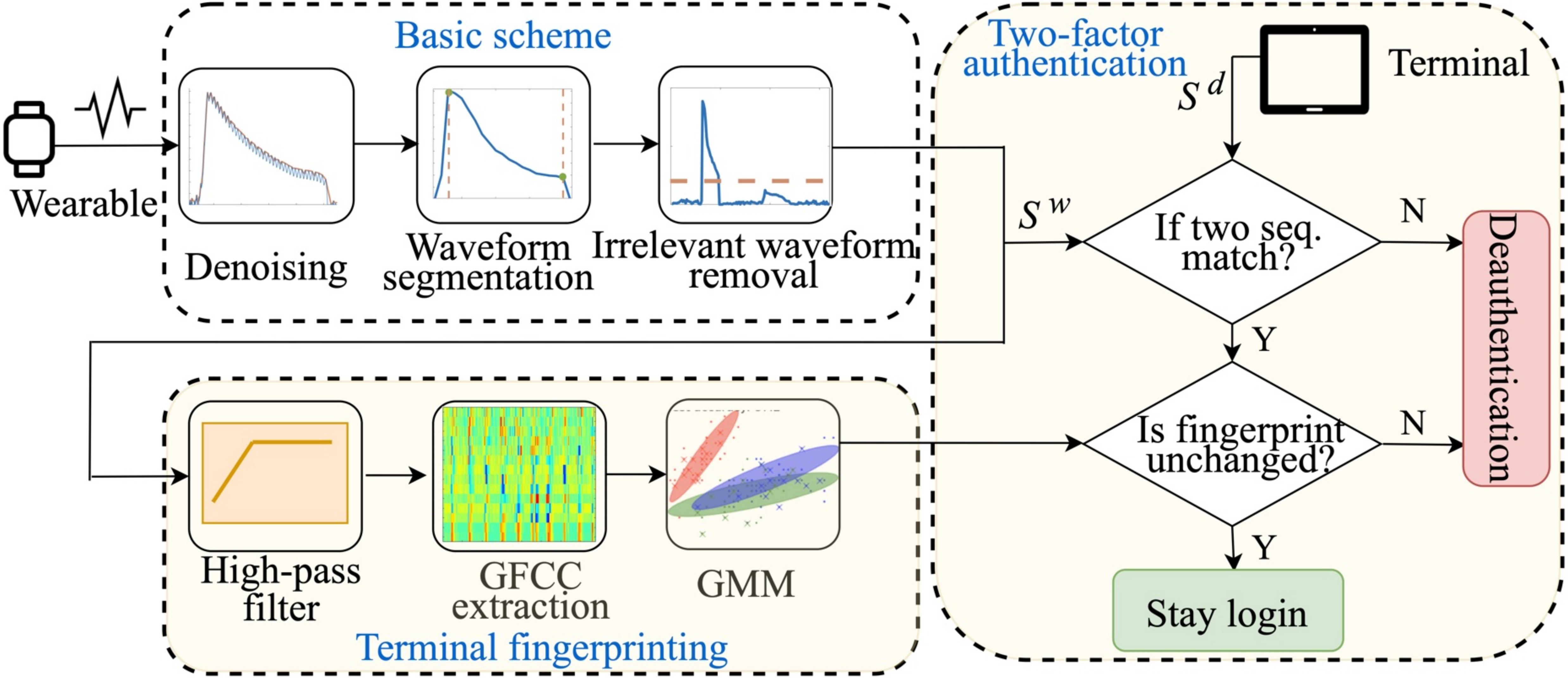


- Utilize set of GFCC features to test for hypothesis:
  - λ_{hyp} = features from original terminal
  - $\lambda_{\overline{hyp}}$ = features not from original terminal
- $\log p(X|\lambda) = \sum_{t=1}^{T} \frac{1}{T} \log p\,(x_t|\,\lambda)$
- $\Gamma(x) =$

$$log \frac{p(x|\lambda_{hyp})}{p(x|\lambda_{\overline{hyp}})} \begin{cases} \geq \theta, accept\ \lambda_{hyp} \\ < \theta, reject\ \lambda_{hyp} \end{cases}$$

- Decision threshold: θ

Modified pipeline



Evaluations

- Experimental setup:
  - Prototype wearable
  - Android tablet
- System Performance
- System Parameters
- Comparison to prior works
- User perception

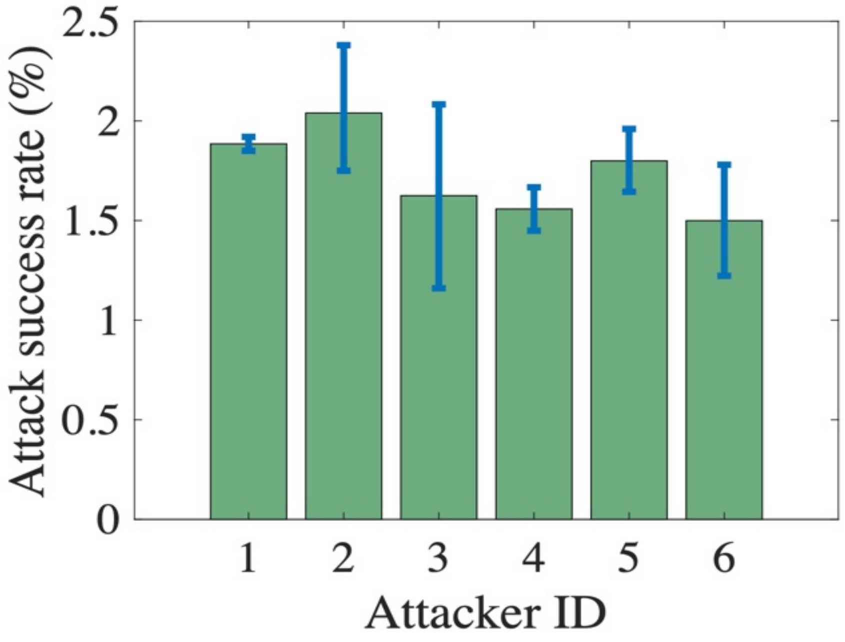
✓ Security

✓ Usability

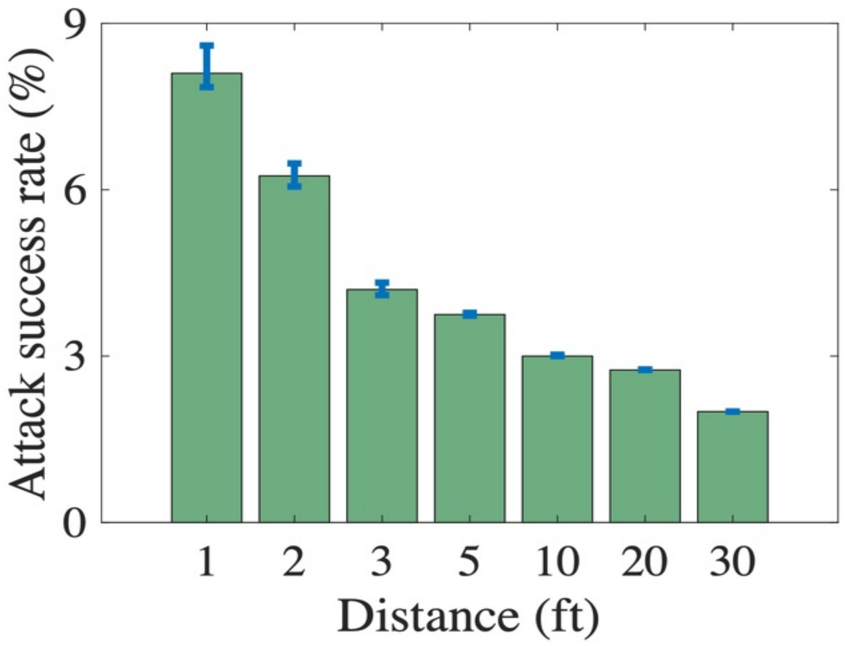
System performance

Robustness against adversaries:

- Innocent adversary



- Malicious adversary



- Practical performance against innocent adversary
- Attack success rate decreases with distance for malicious adversary

Ablation study

Schemes	Malicious adversary							Innocent adversary
Distance (ft)	1	2	3	5	10	20	30	n/a
Without TF(%)	33	30	27	25	16.5	12	10	3
With TF(%)	8.5	6.2	4.2	3.7	3	2.7	2.6	2.4

- Terminal fingerprinting has significant impact on performance

Comparison to prior works

	Our scheme				ZEBRA			
Window size	2	3	4	5	5	7	9	11
FAR (%)	1.5	2.8	4.3	4.7	27.5	25	22.5	21
FRR (%)	11.2	7.5	4.5	3.9	6	4.5	3	2.8

- Better performance, more applicable to wearables than state-of-the-art
- ZEBRA: Use IMU-wearable and two source comparison
  - Disadvantages

**Mare et al., ZEBRA: Zero-effort bilateral recurring authentication. In 2014 IEEE Symposium on Security and Privacy*

Comparison to prior works

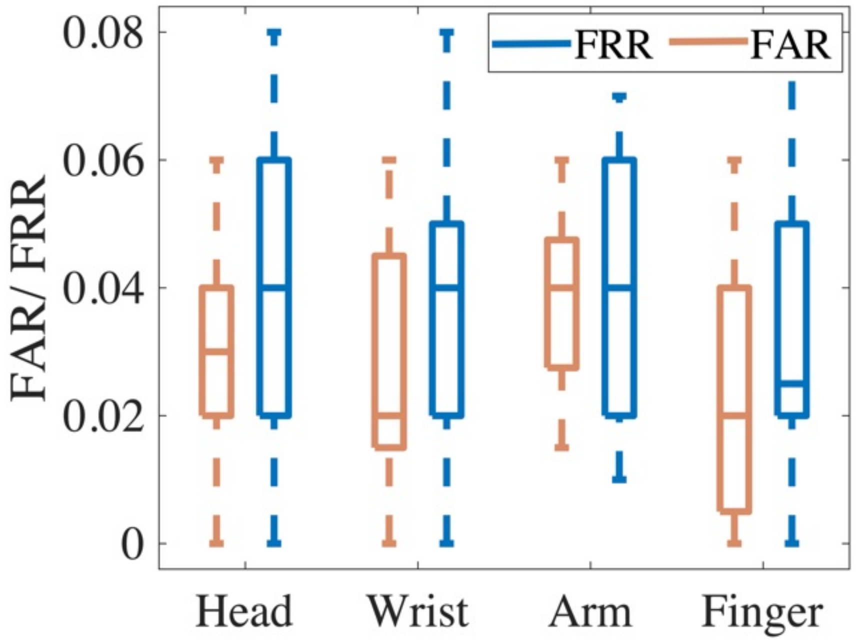
Detection efficiency:

Schemes	Eberz et al. [12]	Our scheme	ZEBRA [29]	Zhang et al. [63]	Segundo et al. [40]
Time (s)	≈40	4.3	≈8	≈125	1

- Practically considerable performance

Different scenarios

- Body locations



- Skin condition

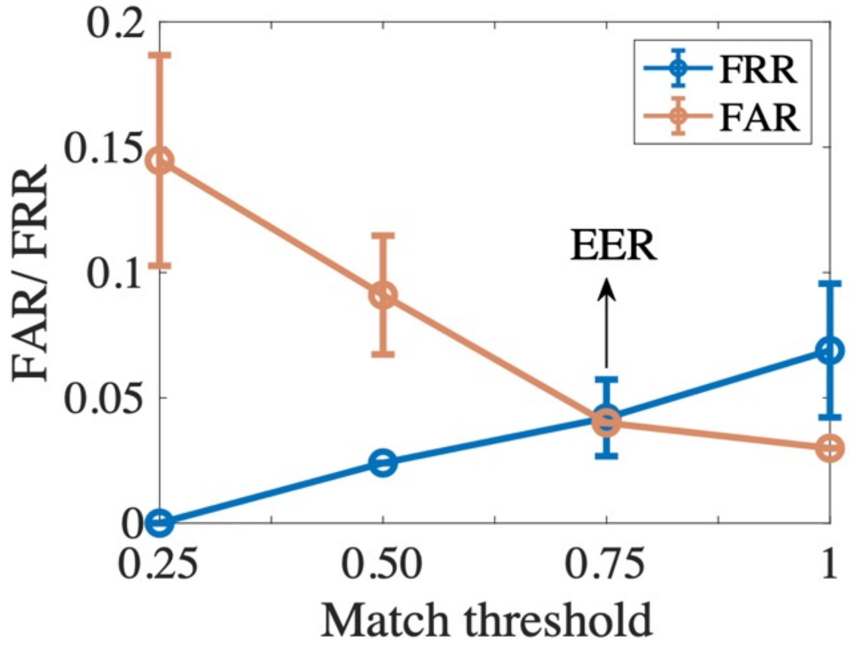
Skin condition	Dry	Moderately wet	Soaked
FAR(%)	3	3.84	7.82
FRR(%)	3.5	8.33	21.6

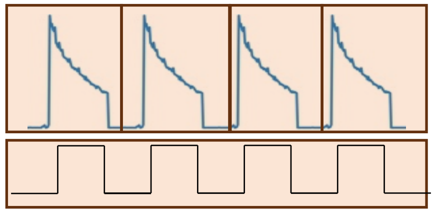
- Similar performance across different body locations
- Practical performance with varying skin conditions

Evaluations

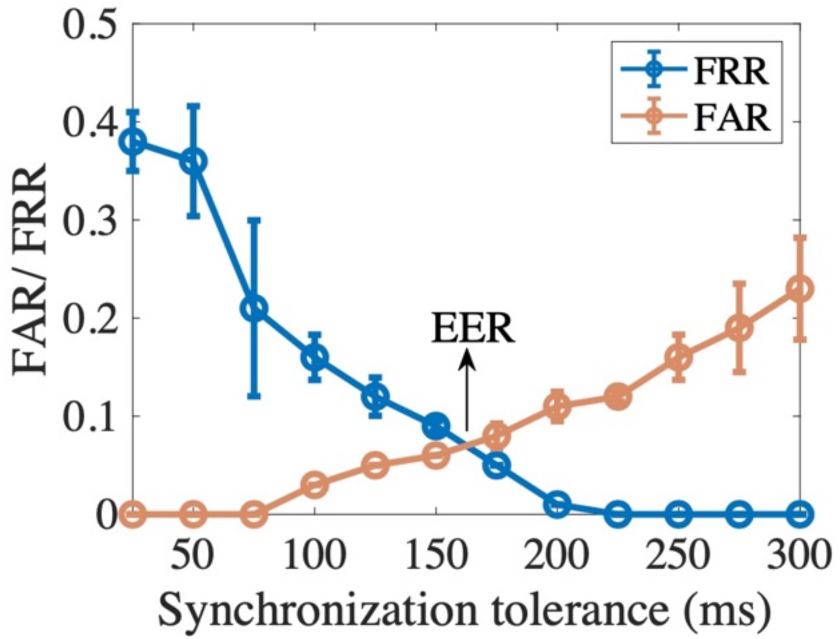
System parameters:

- Match threshold





- Synchronization tolerance



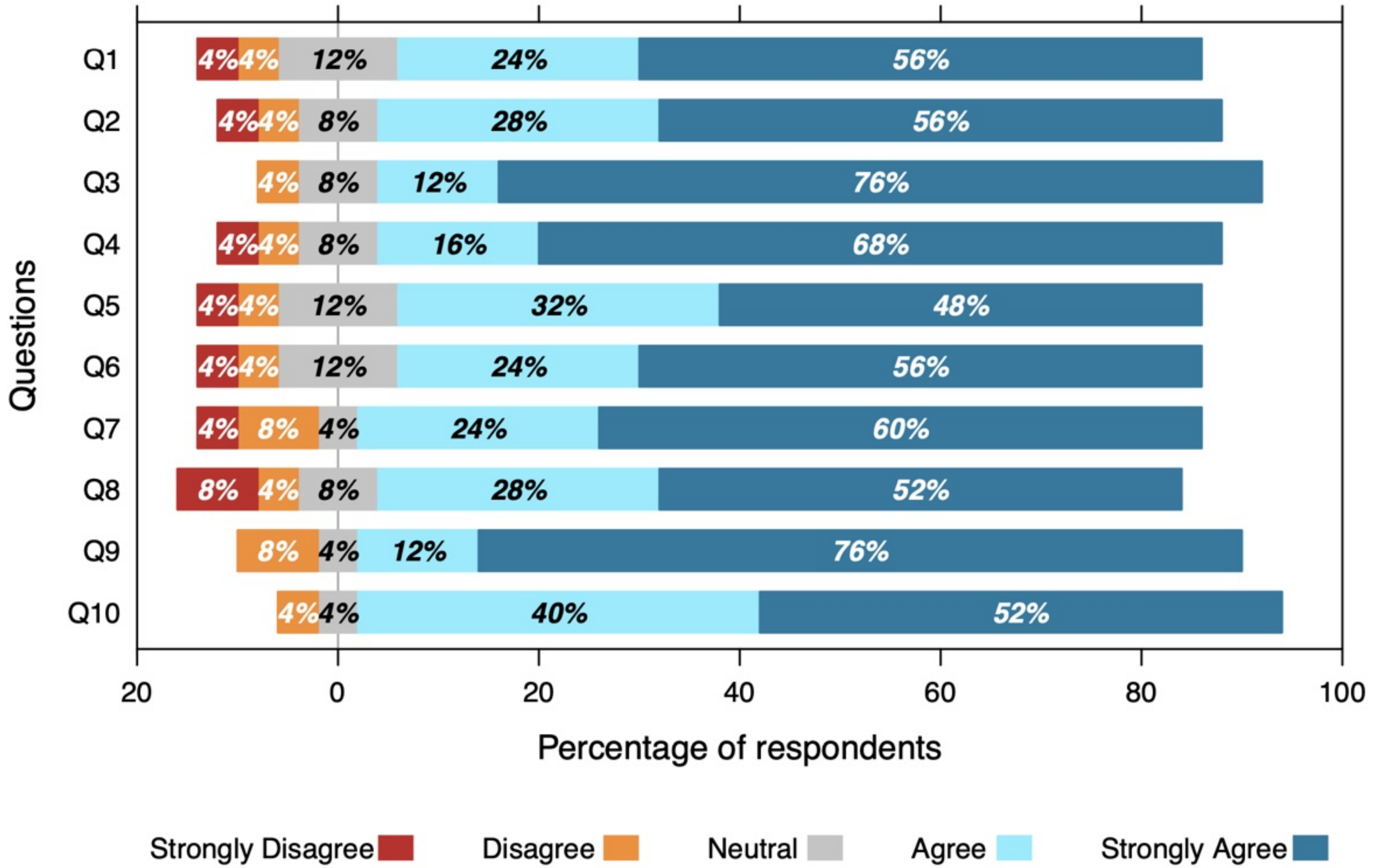
User study

Closed questionnaire:

- Q1 :I would like to adopt the proposed continuous authentication scheme for daily usage.
- Q2 :The proposed scheme requires no effort from me.
- Q3 : The system is easy to use.
- Q4 : The system performance is consistent.
- Q5 : I would not be less worried about temporarily leaving my working terminal unattended with the proposed scheme implemented.
- Q6 : The proposed scheme is more secure compared to the current session timeout approach.
- Q7 : The operation is easy to learn.
- Q8 : The scheme would not disrupt my regular activities on the terminal.
- Q9 : The scheme is more convenient than the session timeout approach.
- Q10: The system is reasonably fast and unobtrusive.

User study

Survey Results:



Well perceived by users and willing to adopt in daily life

Conclusion

- ✓ We investigate the feasibility of leveraging a new form of signal, human-induced electric potential, for two-factor continuous authentication.
- ✓ We developed a wearable prototype for the two-factor continuous authentication scheme to handle various adversaries.
- ✓ We prove via extensive experiments that our scheme outperforms state-of-the-art methods and is well received among users.

Thank You!

Check out our research/group:

MobiSec