2022UBICOMP



Leakage or Identification: Behavior-irrelevant User Identification Leveraging Leakage Current on Laptops

Dian Ding, Lanqing Yang, Yi-Chao Chen, Guangtao Xue

Shanghai Jiao Tong University



Outline

- Background
- Motivation
- Preliminary
- Challenge and Methodology
- Evaluation
- Conclusion and Future Work

Background

Laptops are indispensable in study, work and entertainment...







Information security is important...







Conventional Methods

4

• Password

• Fingerprint

• Face id





• Voiceprint





Biometrics-based Methods

• Finger



acoustic signal

• Body size



• Mouth







vibration signal





Leakage Current on Laptop

• Background of Leakage Current



• Leakage Current from adapter:



- Advantages of *Leakage Current*:
 - Laptops with metal casings are popular with users and manufacturers.
 - No additional specific sensors and energy consumption required.

Preliminary

• User Identification based on Leakage Current



System Overview



Challenge I — Noisy from Body Electric Potentials

• Noisy signal from **Body Electric Potential** caused by *environmental electric fields*.



Body Electric Potiential from *electric field*

Spectrum of leakage current

Challenge I — Noisy from Body Electric Potentials



Challenge II — Feature Screening

• **Sparsity** of Capacitive Characteristics



- Feature Screening among different users
 - DC-SIS (Distance Correlation Sure Independence Screen) on each frequency

$$dcov^{2}(\mathbf{u},\mathbf{v}) = \int_{R^{d_{u}+d_{v}}} \|\phi_{\mathbf{u},\mathbf{v}}(\mathbf{t},\mathbf{s}) - \phi_{\mathbf{u}}(\mathbf{t})\phi_{\mathbf{v}}(\mathbf{s})\|^{2}\omega(\mathbf{t},\mathbf{s})d\mathbf{t}d\mathbf{s}$$

Challenge III – User Identification



Challenge III – User Identification





• Maximize the differences between different users.

 $d1 + \alpha < d2$ $L = \max(d1 + \alpha - d2, 0)$

Experimental Setup



User: Wear the earphone and touch the metal casing of laptop.Laptop: Connect to the adapter and keep in charge.

Evaluation

• Micro benchmark of *LeakPrint*



Accuracy of legitimate users and attackers



Accuracy with different parameters

Conclusion and Future Work

Conclusion

- Propose a novel user identification system based on leakage current
- Suppress the effects of environmental electric fields
- Address the sparsity of Capacitive Characteristics

Future work

- Hardware: Verify the feasibility of wearable devices to receive the leakage current
- Algorithm: Mine other user information contained in the leakage current





