Continuous Authentication Using Human-Induced Electric Potential

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

ACSAC 2023
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 issue

• Conventional solution: One-time Authentication
  • Limitations
    • Verify only initially
  • One-time authentication is not enough!
Related works

Physiological-based approaches:
- ECG/PPG
- Eye-based

Behavioral-based approaches:
- Gait
- Touch Gesture
- Keystroke

Heart based

Right Atrium

Left Atrium

Right Ventricle

Left Ventricle

VF stage

IR stage

VE stage

Diatole

Systole

AS stage

IC stage
Related works

Other approaches:

Proximity
Sub-meter accuracy issues

Timeout
Not entirely risk-free
A new type of signal: Human-induced electric potential

Leverage human-induced electric potential for continuous authentication

Overview
Feasibility study

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

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
Adversarial model

Malicious adversary: Deliberately access other terminals

Attacker imitates victim interactions

Camera controlled by attacker

Shared workspace
Handling the innocent adversary

Basic scheme:

- **Wearable**
  - Human-induced electric potential captured by wearable

- **Authenticator**
  - Implemented on terminal
  - Two-source interaction sequences match in timing?

- **Terminal**
  - Time sequence generated by terminal OS
Basic scheme

Signal acquisition:

Acquire signal using wearable prototype
Basic scheme

Wearable

Denoising

Refine signal

![Graph](image-url)
**Basic scheme**

- Identify critical time instances

---

**Graphical representation**

- Wearable
- Denoising
- Segmentation

**Waveform**

- **Norm. amplitude**
- **Time (s)**
- Segment
- Press (Touch)
- Release
Basic scheme

Wearable

Denoising → Segmentation → Irrelevant waveforms removal

To remove impact of user movement

![Graph showing denoising and segmentation process]

- Touchscreen interaction
- Threshold
- Body movement

Norm. amplitude vs Time (s)
Compare two source sequences of press/release

But how about malicious adversary?

Basic scheme

Wearable

Terminal

Irrelevant waveforms removal
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

Attacker imitates victim interactions

Camera controlled by attacker
Basic pipeline

Wearable → Denoising → Waveform segmentation → Irrelevant waveform removal → $S^W$ → $S^d$ → If two seq. match? (Terminal) → ✔️ or ✗️
Modified pipeline

Eliminate the impact of user behavior diversity

Wearable

Basic scheme

High-pass filter

GFCC extraction

GMM

Terminal fingerprinting

Two-factor authentication

If two seq. match?

Is fingerprint unchanged?

Y

Stay login

N

Deauthentication

Terminal
Modified pipeline

Extract features for terminal fingerprinting

Wearable

Basic scheme

High-pass filter
GFCC extraction
GMM

Terminal fingerprinting

Two-factor authentication

If two seq. match?

Is fingerprint unchanged?

Stay login

Deauthentication
Utilize set of GFCC features to test for hypothesis:

- \( \lambda_{\text{hyp}} \) = features from original terminal
- \( \lambda_{\text{nonhyp}} \) = features not from original terminal

\[
\log p(X | \lambda) = \sum_{t=1}^{T} \frac{1}{T} \log p(x_t | \lambda)
\]

\[
\Gamma(x) = \log \frac{p(x | \lambda_{\text{hyp}})}{p(x | \lambda_{\text{nonhyp}})} \begin{cases} 
\geq \theta, & \text{accept } \lambda_{\text{hyp}} \\
< \theta, & \text{reject } \lambda_{\text{hyp}}
\end{cases}
\]

Decision threshold: \( \theta \)
Modified pipeline

Wearable → Denoising → Basic scheme → Waveform segmentation → Irrelevant waveform removal → High-pass filter → GFCC extraction → GMM → Terminal fingerprinting

Two-factor authentication

$S^d$ → If two seq. match?

Y → Is fingerprint unchanged?

Y → Stay login

N → Deauthentication

N → Deauthentication
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**

  ![Graph showing attack success rate for innocent adversary.]

- **Malicious adversary**

  ![Graph showing attack success rate for malicious adversary.]

  - Practical performance **against innocent adversary**
  - Attack success rate **decreases** with distance for malicious adversary
## Ablation study

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Malicious adversary</th>
<th>Innocent adversary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distance (ft)</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Without TF(%)</td>
<td>33</td>
<td>30</td>
</tr>
<tr>
<td>With TF(%)</td>
<td>8.5</td>
<td>6.2</td>
</tr>
</tbody>
</table>

- Terminal fingerprinting has **significant impact** on performance
## Comparison to prior works

<table>
<thead>
<tr>
<th>Window size</th>
<th>Our scheme</th>
<th>ZEBRA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 3 4 5 5 7 9 11</td>
<td></td>
</tr>
</tbody>
</table>

| 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 |

- **ZEBRA** uses IMU-wearable compatible source comparisons
- **Disadvantages**

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

Detection efficiency:

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Eberz et al. [12]</th>
<th>Our scheme</th>
<th>ZEBRA [29]</th>
<th>Zhang et al. [63]</th>
<th>Segundo et al. [40]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time (s)</td>
<td>≈40</td>
<td>4.3</td>
<td>≈8</td>
<td>≈125</td>
<td>1</td>
</tr>
</tbody>
</table>

• Practically considerable performance
Different scenarios

- Body locations
- Skin condition

<table>
<thead>
<tr>
<th>Skin condition</th>
<th>Dry</th>
<th>Moderately wet</th>
<th>Soaked</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAR(%)</td>
<td>3</td>
<td>3.84</td>
<td>7.82</td>
</tr>
<tr>
<td>FRR(%)</td>
<td>3.5</td>
<td>8.33</td>
<td>21.6</td>
</tr>
</tbody>
</table>

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

System parameters:

- **Match threshold**
  - Graph showing FAR/FRR vs. Match threshold with EER indicated.

- **Synchronization tolerance**
  - Graph showing FAR/FRR vs. Synchronization tolerance (ms) with EER indicated.
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
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:

MobiSeci

[QR Code]