IVORIWATCH: EXPLORING TRANSPARENT INTEGRITY VERIFICATION OF REMOTE USER INPUT LEVERAGING WEARABLES

Prakash Shrestha*
University of Florida, USA

Zengrui Lui and Nitesh Saxena
University of Alabama at Birmingham, USA

* Work done at UAB
Web-Configurable Computing Paradigm

Banking transactions

Email
Web-Configurable Computing Paradigm

- Banking transactions
- Email
- Cardiac Pacemaker
- Blood Pressure Sensors

Medical Devices
Web-Configurable Computing Paradigm

- Banking transactions
- Email
- Cardiac Pacemaker
- Blood Pressure Sensors
- Medical Devices

Smart Home System
(e.g., security cameras, voice assistant speaker)
Web-Configurable Computing Paradigm

Banking transactions

Email

Cardiac Pacemaker

Blood pressure

Blood Pressure Sensors

Medical Devices

Smart Home System
(e.g., security cameras, voice assistant speaker)

Manipulated input from the (compromised) host machine can lead to severe consequences, including financial loss, damage of reputation, security breach, and even put human lives in danger.
An instance of input manipulation attack

Banking Trojans, e.g., ZeusVM

The integrity of user-input (or requests) from a client machine should be checked.
An instance of input manipulation attack

Banking Trojans, e.g., ZeusVM

Compromised Host

User Phone
(confirmation SMS)

The integrity of user-Input (or requests) from a client machine should be checked.
Our Scheme: IvoriWatch

• A transparent integrity verification mechanism for the web
• **Goal:** verify whether the input (or the request) received at the remote server has been modified.
• Based on wrist-worn wearable device
  • e.g., smartwatch, bracelet
  • Typically equipped with motion sensors (accelerometer & gyroscope)
• **Contributions**
  • Introduced a Novel Input-Integrity Verification Scheme – IvoriWatch
  • Designed and Implemented IvoriWatch
  • Evaluated in Benign and Adversarial Settings

**IvoriWatch:** Integrity Verification Of Remote Input with Watch
Our Scheme: IvoriWatch
Our Scheme: IvoriWatch

Input and its timestamps.

Input

Motion Sensor Data

IvoriWatch: Integrity Verification Of Remote Input with Watch
Our Scheme: IvoriWatch

IvoriWatch: Integrity Verification Of Remote Input with Watch
Adversarial Model

- Victim’s terminal (or the client machine) has been remotely compromised
- Wrist-wearable is safe (not compromised)

1. User-Present
   - Victim provides input to the remote server using the compromised client
   - Adversary (or malware) attempts to manipulate the user-provided input

2. User-Away
   - User forgets to log out his web-account or software application
   - Utilizing the opportunity, remote adversary attempts to supply its fabricated input
   - No clue about the remote victim’s activities
   - Consider various scenarios
     - Using terminal
     - Using phone
     - Writing
     - Walking
     - Miscellaneous
IvoriWatch Working Principle

Keyboard Region Division

Left region (L)       Right region (R)
IvoriWatch Working Principle

Keyboard Region Division

Left region (L)  Right region (R)

System parameters
Window size: 10
Threshold: 70%

System output for current input
Matches: 13/16 (≥ 70%)
Legit Input

Actual input sequence (Terminal)
R L R L R L L L R R L R R R R

Predicted input sequence (Watch)
R L L L R L R L L R R L R R R R
Key-Region Predictor

- Several statistical features are extracted from motion sensor data
- Infers the location of the key, i.e., left (L) or right (R)
- Consists of a well-trained RandomForest classifier

List of features used in IvoriWatch

<table>
<thead>
<tr>
<th>Minimum</th>
<th>Median Absolute Deviation</th>
<th>Kurtosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum</td>
<td>Inter-quartile range</td>
<td>Skewness</td>
</tr>
<tr>
<td>Mean</td>
<td>Power</td>
<td>Peak-to-peak amplitude</td>
</tr>
<tr>
<td>Median</td>
<td>Energy</td>
<td>Peak-magnitude-to-rms-ratio</td>
</tr>
<tr>
<td>Variance</td>
<td>Spectral Entropy</td>
<td>Median frequency</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>Autocorrelation</td>
<td>Peak counts</td>
</tr>
</tbody>
</table>
Experiment

- Participants: 20 student users
  - 13 males and 7 females
  - Age ranges between 20-35
  - All were touch typists

*The Practice Test: [https://thepracticetest.com](https://thepracticetest.com)
Experiment

- Participants: 20 student users
  - 13 males and 7 females
  - Age ranges between 20-35
  - All were touch typists
- Leveraged “The Practice Test”* website that offers online typing lessons
- Each user typed for 10 minutes while wearing watches on both hands.
- 20 user sessions resulted 20 samples in total

*The Practice Test: [https://thepracticetest.com](https://thepracticetest.com)
Experiment

• Participants: 20 student users
  • 13 males and 7 females
  • Age ranges between 20-35
  • All were touch typists

• Leveraged “The Practice Test”* website that offers online typing lessons
• Each user typed for 10 minutes while wearing watches on both hands.
• 20 user sessions resulted 20 samples in total

• Motion-data for User-Away setting
  • randomly selected two participants.
  • five different regular activities - walking, writing, using-phone, using-terminal, and miscellaneous

*The Practice Test: https://thepracticetest.com
Evaluation Preliminaries

• Considered three different settings
  • Left-Hand
  • Right-Hand
  • Both-Hands -- exploratory
• Input
  • must be at least a word of five characters
  • can be a combination of words with variable character length
• Each word from input and corresponding motion data from wrist-wearables was separated
• `n’ (where 1<=n<=10) consecutive words were combined in a sliding window fashion to form variable lengths input
Evaluation Preliminaries

• Employ Leave-One-Subject-Out (LOSO) cross-validation approach
  • For input-texts from a given user, predictor was built using samples from all other users
  • Resulted in a user-agnostic prediction model
Evaluation Preliminaries

• Employ Leave-One-Subject-Out (LOSO) cross-validation approach
  • For input-texts from a given user, predictor was built using samples from all other users
  • Resulted in a user-agnostic prediction model

• Evaluation Metrics
  • False Negative Rate (FNR)
  • False Positive Rate (FPR)
  • Equal Error Rate (EER)
User-Presence: Performance of IvoriWatch

<table>
<thead>
<tr>
<th>Setting</th>
<th>EER ($\theta$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left-Hand</td>
<td>0.15 ($\theta = 0.61$)</td>
</tr>
</tbody>
</table>

![Graph showing FPR/FNR vs. Similarity Threshold ($\theta$) with EER at 0.15 ($\theta = 0.61$) for Left-Hand setting.]
User-Presence: Performance of IvoriWatch

![Graph showing FPR and FNR for different similarity thresholds.]

**Setting** | **EER (θ)**
---|---
Left-Hand | 0.15 (θ = 0.61)
Right-Hand | 0.23 (θ = 0.58)
User-Presence: Performance of IvoriWatch

<table>
<thead>
<tr>
<th>Setting</th>
<th>EER (θ)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left-Hand</td>
<td>0.15 (θ = 0.61)</td>
</tr>
<tr>
<td>Right-Hand</td>
<td>0.23 (θ = 0.58)</td>
</tr>
<tr>
<td>Both-Hands</td>
<td>0.13 (θ = 0.62)</td>
</tr>
</tbody>
</table>

Both-Hands
User-Away: Performance of IvoriWatch

Left-Hand and Both-Hands

Right-Hand

EER = 0.15 (0.61)

EER = 0.14 (0.60)
Impact of Text Length

Similar trend was found in Left-Hand and Right-Hand settings.
Conclusion, Limitations, and Future Works

• Introduced IvoriWatch
  • a transparent integrity verification system
  • for remote user-input
  • based on wrist-wearables
• Can identify legitimate input and detect manipulated input with minimal errors
Conclusion, Limitations, and Future Works

• Introduced IvoriWatch
  • a transparent integrity verification system
  • for remote user-input
  • based on wrist-wearables

• Can identify legitimate input and detect manipulated input with minimal errors

• Improving the performance by using wrist-wearables with a higher sampling rate

• Evaluation with a large and diverse pool of participants.

• Extension for other personal devices, e.g., laptop mobile phones, tablets
Thank You!