Liveness is Not Enough: Enhancing Fingerprint Authentication with Behavioral Biometrics to Defeat Puppet Attacks

Cong Wu¹,², Kun He¹, Jing Chen¹,², Ziming Zhao⁴, Ruiying Du¹,³

¹ Wuhan University, China
² Shenzhen Institute of Wuhan University, China
³ Collaborative Innovation Center of Geospatial Tech., China
⁴ Rochester Institute of Technology, USA
The Prevailing Fingerprint Authentication


Photo: https://www.fingerprints.com/
Attacks on Fingerprint Authentication

ISO/IEC 30107-1:2016
Information technology — Biometric presentation attack detection — Part 1: Framework

New research used 3D printing technology to bypass fingerprint scanners, and tested it against Apple, Samsung and Microsoft mobile products.

New research has found that it's possible to use 3D printing technology to create "fake fingerprints" that can bypass most fingerprint scanners used by popular devices. But, creating the attack remains costly and time-consuming.

Researchers with Cisco Talos created different threat models that use 3D printing technology, and then tested them on mobile devices (including the iPhone 8 and Samsung S10), laptops (including the Samsung Note 9, Lenovo Yoga and HP Pavilion X360) and smart devices (such as a smart padlock).

For decades, the use of fingerprints to authenticate users to computers, networks, and restricted areas was mostly limited to large and well-resourced organizations that used specialized and expensive equipment. That all changed in 2013 when Apple introduced TouchID. Within a few years, fingerprint-based validation became available to the masses as computer, phone, and lock manufacturers added sensors that gave users an alternative to passwords when unlocking the devices.

Although hackers managed to defeat TouchID with a fake fingerprint less than 48 hours after the technology was rolled out in the iPhone 5, fingerprint-based authentication over the past few years has become much harder to defeating. Today, fingerprints
Puppet Attack

Child uses sleeping mom's fingerprints to buy Pokemon gifts

When you want to buy $250 worth of Pokemon presents, desperate times call for desperate measures.

Alfred Ng 17  Dec. 27, 2016 6:25 a.m. PT

I got drunk last night and got robbed because I was using Touch ID :-(

Hi guys,

not looking to blame anyone but thought I'd share my tale of sorrow here...

Long story short, I was at a party last night and I passed out after some heavy drinking. I woke up this morning and walked to an ATM machine wanting to get some cash out for a cab. To my amazement, the transaction was declined. So I whipped out my shiny new iPhone 6, fired up 1Password, placed my thumb for the TouchID, and logged in to my online banking website.
Puppet Attack

Child uses sleeping mom's fingerprints to buy Pokemon gifts

When you want to buy $250 worth of Pokemon presents, desperate times call for desperate measures.

Existing liveness detection methods all fail in defeating puppet attacks.
Our Approach

Complement fingerprint authentication with fingertip-touch behavioral characteristics
Data capture
System Overview

Data capture

Behavior characterizing
System Overview

Data capture

Behavior characterizing

Feature extraction
System Overview

Data capture

Behavior characterizing

Feature extraction

Model training / Authentication
## Table 1: Time- and frequency-domain features and their normalized fisher’s scores.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Feature</th>
<th>Description</th>
<th>Normalized Fisher Score of $(a_x, a_y, a_z, a'_x, \phi, \theta, \psi)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Mean</td>
<td>The mean of the time series.</td>
<td>$(0.45, 0.01, 0.22, 0.68, 0.86, 0.84, 0.84)$</td>
</tr>
<tr>
<td></td>
<td>Standard deviation</td>
<td>The standard deviation of the time series.</td>
<td>$(0.24, 0.56, 0.31, 0.41, 0.58, 0.32, 0.74)$</td>
</tr>
<tr>
<td></td>
<td>Relative standard deviation</td>
<td>The extent of variability in relation to its mean.</td>
<td>$(0.34, 0.15, 0.12, 0.56, 0.71, 0.64, 0.82)$</td>
</tr>
<tr>
<td></td>
<td>Sum of absolute differences</td>
<td>The sum over the absolute value of consecutive changes in the time series.</td>
<td>$(0.32, 0.27, 0.72, 0.52, 0.53, 0.72, 0.78)$</td>
</tr>
<tr>
<td></td>
<td>Absolute energy</td>
<td>The absolute energy of the time series.</td>
<td>$(0.63, 0.98, 0.85, 0.57, 0.72, 0.57, 0.37)$</td>
</tr>
<tr>
<td></td>
<td>Autocorrelation</td>
<td>The autocorrelation of the time series.</td>
<td>$(0.00, 0.14, 0.15, 0.21, 0.94, 0.62, 0.64)$</td>
</tr>
<tr>
<td></td>
<td>Spectral centroid</td>
<td>The center of mass of the spectrum is located.</td>
<td>$(0.34, 0.21, 0.38, 0.12, 0.78, 0.98, 0.78)$</td>
</tr>
<tr>
<td></td>
<td>Spectral spread</td>
<td>The average spread of the spectrum in relation to its centroid.</td>
<td>$(0.66, 0.36, 0.32, 0.78, 0.46, 0.82, 0.96)$</td>
</tr>
<tr>
<td>Frequency</td>
<td>Spectral skewness</td>
<td>The measurement of the asymmetry of the probability distribution of a real-valued random variable about its mean.</td>
<td>$(0.85, 0.45, 0.58, 0.84, 0.56, 0.85, 1.00)$</td>
</tr>
<tr>
<td></td>
<td>Spectral kurtosis</td>
<td>The shape of a probability distribution.</td>
<td>$(0.34, 0.17, 0.70, 0.86, 0.62, 0.51, 0.42)$</td>
</tr>
<tr>
<td></td>
<td>Power spectral density</td>
<td>Average of distribution of power into frequency components.</td>
<td>$(0.90, 0.71, 0.86, 0.26, 0.85, 0.68, 0.82)$</td>
</tr>
<tr>
<td></td>
<td>Spectral entropy</td>
<td>The complexity of the signal in the frequency domain.</td>
<td>$(0.94, 0.32, 0.82, 0.21, 0.96, 0.82, 0.89)$</td>
</tr>
</tbody>
</table>
Figure 3: Characterized fingertip-touch behaviors of three users under STFT. From left to right, spectrograms of $a_1$, $a_2$, $a_3$, $a'$, $\theta$, $\phi$, $\psi$. 

CNN-based Features (CNF)
CNN-based Features (CNF)

Input: psd matrices

Output

N Layers

Step 1. Pretrain the CNN
Step 2. Use first N-1 layers as the feature extractor
One-class Classifier

\[ r_{XY} = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \bar{X})^2} \sqrt{\sum_{i=1}^{n}(Y_i - \bar{Y})^2}} \]

Pearson coefficient-based similarity comparison (PCC)

\[
\min_{R, \alpha} R^2 + C \sum_{i=1}^{n} \zeta_i \\
\text{s.t. } \|x_i - a\|^2 \leq R^2 + \zeta_i, i = 1, \ldots, n \\
\zeta_i \geq 0, i = 1, \ldots, n
\]

One-class support vector machine (OCSVM)

Local outlier factor (LOF)

Isolation forest (IF)
Data Collection

Table 3: Summary of the compiled datasets

<table>
<thead>
<tr>
<th>Dataset</th>
<th>Week of Collection</th>
<th># of Subjects / Attackers</th>
<th>Postures</th>
<th>Device</th>
<th># of Data Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1, 8, and 9‡</td>
<td>90</td>
<td>Sitting, standing, lying, walking, running</td>
<td>OnePlus3</td>
<td>63,000</td>
</tr>
<tr>
<td>2A</td>
<td>2, 3, 5, 7</td>
<td>24, 24, 22, 21</td>
<td>Sitting</td>
<td>OnePlus3</td>
<td>18,200</td>
</tr>
<tr>
<td>2B</td>
<td>10, 11, 12, 13</td>
<td>62, 61, 59, 53</td>
<td>Sitting</td>
<td>OnePlus3</td>
<td>47,000</td>
</tr>
<tr>
<td>3</td>
<td>Added Aug. 2019</td>
<td>64</td>
<td>Sitting</td>
<td>Xperia XZ1, Oneplus5, Vivo X21</td>
<td>3,200</td>
</tr>
<tr>
<td>4A</td>
<td>2, 10, and 11‡</td>
<td>15</td>
<td>Sitting</td>
<td>OnePlus3</td>
<td>3,600</td>
</tr>
<tr>
<td>4B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3,600</td>
</tr>
<tr>
<td>4C</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3,600</td>
</tr>
</tbody>
</table>

Datasets

- 90 subjects in the data collection.
- Compiled three datasets in different postures, periods, and devices.
- Compiled one attack dataset by considering three attacks with 15 subjects as adversaries.
Reliability Evaluation

(a) Time- and frequency-domain features  
(b) CNN-based features  
(c) The union of two feature sets

Figure 5: ROC curves of different feature sets under different one-class classifiers.

(a) Time- and frequency-domain features  
(b) CNN-based features  
(c) The union of two feature sets

Figure 6: BAC under different classifiers and different feature sets at varying training set sizes.
Reliability Evaluation

Finding: CNF+LOF achieves almost the best performance with the lowest FAR.
Evaluation of Presentation Attacks

<table>
<thead>
<tr>
<th>Attack</th>
<th>FAR</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARA</td>
<td>0.08/0.06</td>
<td>-0.29/0.15</td>
</tr>
<tr>
<td>PA</td>
<td>0.12/0.08</td>
<td>-0.62/0.13</td>
</tr>
<tr>
<td>MA</td>
<td>0.25/0.14</td>
<td>-0.37/0.10</td>
</tr>
</tbody>
</table>

Mean/standard deviation of FAR and prediction score under attacks.

- **FAR** and kernel density of prediction score under attacks.
Behavior variability with time elapsing?
Thank you!

Contact: Cong Wu, cnacwu@whu.edu.cn