InfinityGauntlet: Expose Smartphone Fingerprint Authentication to Brute-force Attack

Yu Chen
Xuanwu Lab, Tencent

Yang Yu*
Xuanwu Lab, Tencent

Lidong Zhai
Institute of Information Engineering, Chinese Academy of Sciences, China
Motivation

- Residual Replay Attack @ GeekPwn 2018
- Presentation Attack @ GeekPwn 2019
- Liveness Detection Bypass @ BH-USA 2019

Artificial Fingerprint Artifact + Latent Fingerprint on Sensing Area

Artificial Fingerprint Artifact + Latent Fingerprint on Anywhere

Artificial Fingerprint Artifact + Latent Fingerprint on Anywhere

Can we achieve this zero-knowledge attack?

Latent Fingerprint on Anywhere
Motivation

My daughter’s thumb unlocked my phone. She does not have a fingerprint saved.

I shit you not. She was playing around with it, pressing the home screen and watching the fish swim and playing with the haptic home button. I figured no big deal since she doesn’t know my passcode and touch ID.

Then it unlocked by itself.

Friend was able to unlock my phone with his fingerprint!

Discussion

Last night my friend asked to see my phone and when he tested the fingerprint reader, his fingerprint unlocked the phone.

Friend was able to unlock my phone with his fingerprint.

So my friend was playing around with my phone and tested the fingerprint scanner. To my surprise, the phone unlocked. I told him to try again and he was able to unlock it once more. I cleaned off the fingerprint scanner and he was unable to unlock it afterwards. I was just wondering if this is something I should be concerned over. It was a considerably hot day and my sweat accumulated on the scanner. Could that have affected it? If it matters, I’m on Nougat on the September 6 security patch, rooted with ElementalX and the stock rom.

Can we achieve the zero-knowledge attack by brute-force?

False Acceptance Rate:

\[ FAR = \Pr[M_{r=1} (S(f)) = 1] \]
\[ = \Pr[R(S(f), S(v)) = 1] \]

False Positive Identification-error Rate:

\[ FPIR = \Pr[M_{r=N} (S(f)) = 1] \]
\[ = \Pr[\bigvee_{i=1}^{N} R(S(x), S(v_i)) = 1] \]
\[ \approx 1 - \prod_{i=1}^{N} \Pr[R(S(x), S(v_i)) = 0] \]
\[ \approx 1 - (1 - FAR)^N \]
\[ \approx N \cdot FAR \]

Collision Rate \( \sim 10^{-4} \)
Challenges 1

**P1:** Forbid SFA and challenge for primary authentication (e.g., PIN, pattern, password) if the number of failed attempts exceeds the attempt limit.

**P2:** Forbid SFA and challenge for the primary authentication once every 72 hours.

**P3:** Forbid SFA and challenge for the primary authentication after smartphone restart.

**P4:** Forbid SFA at least 30 seconds after five consecutive failed SFA attempts.

**P5:** Forbid SFA when the primary authentication is locked out temporarily.

How to bypass the attempt limit?
Challenges 2

How to bypass quality and liveness detection?

The authentication workflow of SFA.

How to make automatic attempts?
Attack Overview

Overview of INFINITYGAUNTLET.
CAMF (CVE-2022-25820 etc.)

Multi-sampling mechanism and CAMF vulnerability

Affected MFRs:
Samsung
Xiaomi
OnePlus
OPPO
Vivo (limited)
Apple (limited)
Lift-Too-Fast Error-cancel

Checksum Error-cancel

Different Types of CAMF
Step 1: Let the SFA enter a lockout mode.

Step 2: Make unlimited noneffective attempts until a matched result is inferred by side-channel.

Step 3: Replay the successful attempt that contains the valid fingerprint after the lockout mode is exited.

Affected MFRs:
- Huawei
- Honor (limited)
- Vivo (limited)
SPI-MITM on Fingerprint Sensor

Adversary (Fake Slave)

<table>
<thead>
<tr>
<th>S0</th>
<th>MOSI</th>
<th>MISO</th>
<th>S1</th>
<th>SCLK</th>
<th>CS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SPDTs

S0 = 0
S1 = 0
S0 = 1
S1 = 1

Function of the two SPDT switches:

<table>
<thead>
<tr>
<th>State</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0</td>
<td>Identify the FDA command from MOSI.</td>
</tr>
<tr>
<td>0</td>
<td>Intercept raw image from MISO_S.</td>
</tr>
<tr>
<td>1</td>
<td>Keep connection from MISO_S to MISO_M.</td>
</tr>
<tr>
<td>S1</td>
<td>Inject raw image from MISO_A to MISO_M.</td>
</tr>
</tbody>
</table>
Hijacking Fingerprint Images

- Capacitive
- In-display optical
- Ultra-thin In-display optical
- In-display ultrasonic optical
Fingerprint dictionary generation

Synthetic fingerprint generation for SFA

Capture base images

Master Fingerprint

[ DPI ]

[ Base images ]

Average

Stack

Synthetic Fingerprint

Hollowed Area

Conductive Paint
Attack Demonstration
InfinityGauntlet: Expose Smartphone Fingerprint Authentication to Brute-force Attack (Usenix Security 23)
Results of brute-force experiments on OnePlus 7P

<table>
<thead>
<tr>
<th>Metric</th>
<th>Enroll One Finger</th>
<th>Enroll Five Fingers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success #</td>
<td>$9.2^1$</td>
<td>$41.9^2$</td>
</tr>
<tr>
<td>Failed #</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Time Cost</td>
<td>2.01 hours</td>
<td>0.44 hours</td>
</tr>
</tbody>
</table>

**Setup:**
- 200,000 synthetic fingerprint
- Enroll One/Five fingers
- Repeat 12 times

**Metric:**
- **Success #**: Average number of successes
- **Failed #**: Average number of attempts that increased the counter
- **Time Cost**: Average time required for one successful attack
# Scalability

<table>
<thead>
<tr>
<th>Smartphone</th>
<th>OS/Ver.</th>
<th>Sensor Vendor</th>
<th>Sensor Type</th>
<th>CAMF</th>
<th>MAL</th>
<th>MITM</th>
<th>Attack</th>
<th>Unlock¹</th>
<th>Payment²</th>
<th>Privacy³</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samsung Galaxy S20U</td>
<td>Android 11</td>
<td>Qualcomm</td>
<td>Ultrasonic</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
</tr>
<tr>
<td>Samsung Galaxy S10+</td>
<td>Android 9</td>
<td>Qualcomm</td>
<td>Ultrasonic</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
</tr>
<tr>
<td>Xiaomi Mi 11 Ultra</td>
<td>Android 11</td>
<td>Goodix</td>
<td>Optical</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
</tr>
<tr>
<td>OnePlus 7 Pro</td>
<td>Android 11</td>
<td>Goodix</td>
<td>Optical</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
</tr>
<tr>
<td>OnePlus 5T</td>
<td>Android 8</td>
<td>Goodix</td>
<td>Capacitive</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
</tr>
<tr>
<td>Huawei Mate30 Pro</td>
<td>HarmonyOS 2</td>
<td>Goodix</td>
<td>Optical</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
</tr>
<tr>
<td>Huawei P40</td>
<td>HarmonyOS 2</td>
<td>Novatek</td>
<td>Optical</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
</tr>
<tr>
<td>OPPO Reno Ace</td>
<td>Android 10</td>
<td>Goodix</td>
<td>Optical</td>
<td>✔</td>
<td>✗</td>
<td>✔</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
</tr>
<tr>
<td>Honor Magic3</td>
<td>Android 11</td>
<td>Goodix</td>
<td>Optical</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>LIMIT/COND FULL</td>
<td>FULL</td>
<td>FULL</td>
<td>FULL</td>
</tr>
<tr>
<td>Vivo X60 Pro</td>
<td>Android 11</td>
<td>Goodix</td>
<td>Optical</td>
<td>✗</td>
<td>✔</td>
<td>✔</td>
<td>LIMIT/COND FULL</td>
<td>FULL</td>
<td>FULL</td>
<td>LIMIT</td>
</tr>
<tr>
<td>Apple iPhone 7</td>
<td>iOS 14.4.1</td>
<td>AuthenTec</td>
<td>Capacitive</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>PA_ONLY</td>
<td>PA_ONLY</td>
<td>PA_ONLY</td>
<td>PA_ONLY</td>
</tr>
<tr>
<td>Apple iPhone SE</td>
<td>iOS 14.5.1</td>
<td>AuthenTec</td>
<td>Capacitive</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>PA_ONLY</td>
<td>PA_ONLY</td>
<td>PA_ONLY</td>
<td>PA_ONLY</td>
</tr>
<tr>
<td>Apple iPhone SE(2nd)</td>
<td>iOS 15.5</td>
<td>AuthenTec</td>
<td>Capacitive</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>PA_ONLY</td>
<td>PA_ONLY</td>
<td>PA_ONLY</td>
<td>PA_ONLY</td>
</tr>
</tbody>
</table>

¹ Unlock: screen unlock.
² Payment: make payments on pre-installed or third-party payment apps, including: Paypal, Alipay, Samsung Pay, Huawei Pay, OPPO Pay, Vivo Pay, and Apple Pay.
³ Privacy: log into pre-installed privacy protection apps, including Secure Folder for Samsung, Hidden Folders for Xiaomi, LockBox for OnePlus, Safe for Huawei and Honour, Private Safe for OPPO, File Safe for Vivo and Notes for Apple.
Vulnerabilities exposure responsibility

We have submitted these vulnerabilities to these seven manufacturers (Huawei, Xiaomi, Honor, Vivo, OPPO, Moto and Samsung), and all have been confirmed, including critical and high ones.

After we submitted these vulnerabilities, Google also raised the security requirements of the “false trial” in the Android compatibility definition document (CDD) to prevent fingerprint brute-force attacks.
Thank you!

If you have any questions, feel free to contact us via email:

alohachen@tencent.com