To Swipe or Not to Swipe: A Challenge for Your Fingers

Yulong Zhang
Senior Software Research Engineer
FireEye Labs

Tao Wei
Senior Manager, Advanced Research
FireEye Labs
Functionalities Using Fingerprints

- Authentication
  - System screen unlock
  - Login in FIDO alliances’ services

- Authorization
  - iTunes/App store pay
  - Apple Pay
  - Transaction authorization using FIDO
Risk: Fingerprints Never Expire

- Password leaked? Fine, you can easily replace it with a new one.
- Fingerprint leaked? Well, it is leaked for the rest of your life.
- Moreover, it is associated with your identity record, immigration history, etc.
Existing Optical Attacks

- Fingerprints can be stolen from its owner if a person touched any object with a polished surface like glass or a smartphone screen.
- Fingerprints can even be extracted from a waving hands photo.
- Attackers can spoof fingerprints accordingly using electrically conductive materials.

System Attacks against Fingerprints?!

This talk will show attacks on Android devices:

- Confused Authorization Attack
  - Bypass pay authorizations protected by fingerprints
- Fingerprint DB Manipulating
- Fingerprint Sensor Spying Attack
  - Collect fingerprints through malware
Outline

◆ Design of Android Fingerprint Frameworks
  ◆ Fingerprint Recognition
  ◆ Mobile Fingerprint Frameworks

◆ System Attacks against Fingerprints
  ◆ Confused Authorization Attack
  ◆ Fingerprint DB Manipulating
  ◆ Fingerprint Sensor Spying Attack

◆ Takeaways
Outline

- Design of Android Fingerprint Frameworks
  - Fingerprint Recognition
  - Mobile Fingerprint Frameworks
- System Attacks against Fingerprints
  - Confused Authorization Attack
  - Fingerprint DB Manipulating
  - Fingerprint Sensor Spying Attack
- Takeaways
Fingerprint Recognition
Fingerprint Recognition: Minutiae Extraction

Figures from J. Feng and A. Jain, Fingerprint Reconstruction: From Minutiae to Phase
IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 33, NO. 2, FEBRUARY 2011
Fingerprint Recognition: Minutiae Matching
Mobile Fingerprint Frameworks
Fingerprint Framework without TrustZone

- Java
- App
- Fingerprint Service
- Encrypted Fingerprint (Feature) DB
- Native
- Native Fingerprint Libraries
- User Space
- Fingerprint Sensor Driver
- Kernel Space
- Hardware

FireEye™ RSA Conference 2015
Threat: Rooting Attacks

Attackers can steal your fingerprints either from memory or from storage!
How to Defend against Rooting Attacks?

TrustZone

- Separate the system to the Normal World, and the Secure World
- Contain potential compromises in the Normal World
Rooting Attackers Cannot Access Fingerprints in TrustZone
Fingerprint Authorization Framework with TrustZone

App → Fingerprint Service → TrustZone Daemon

User Space

Kernel Space

Secure Key Store

Fingerprint Trustlet

TrustZone Driver

SPI Driver

TrustZone Microkernel

Monitor

Hardware
FIDO Alliance
Outline

- Design of Android Fingerprint Frameworks
  - Fingerprint Recognition
  - Mobile Fingerprint Frameworks

- System Attacks against Fingerprints
  - Confused Authorization Attack
  - Fingerprint DB Manipulating
  - Fingerprint Sensor Spying Attack

- Takeaways
Confused Authorization Attack
Confused Authorization Attack

Authentication
◆ Who you are (Passport)

Authorization
◆ What you can do (Visa)

Figures from Wikipedia
Authenticating
Authorizing
Authorizing: Context!

Figures from dailytech.com
To Swipe or Not To Swipe, without A Context?

Figures from dailytech.com
What are your fingerprints?

OR

OR

FireEye™
Confused Authorization Attack

- Do you ever have a second thought when you swipe to unlock the device?

It can enable background attacker to steal your money from your PayPal account!!!
Confused Authorization Attack
Confused Authorization Attack

Question

How can I testify what’s happening behind the finger swiping?

You can’t tell...

What’s the difference of swiping to unlock the device with swiping to authorize a transaction?

You can’t tell...
Confused Authorization Attack

- Applications often mistakenly treat authorization as authentication, and fail to provide context proofs for authorization.

- Without proper context proof, the attacker can mislead the victim to authorize a malicious transaction by disguising it as an authentication or another transaction.
Protections

- Long term: unlike authentication, authorization needs trusted contexts
  - The modules in TrustZone (trustlets) should provide such supports
  - The current FIDO framework doesn’t support it yet.

- Short term:
  - Upgrade your system to the latest version to fix all the known vulnerabilities.
  - Only install popular apps from Google Play on your phone with fingerprint sensors.
Fingerprint DB Manipulating
Fingerprint Settings

How can you attest that only 3 fingerprints were registered?
Fingerprint Framework

App → Fingerprint Service → TrustZone Daemon

User Space

Kernel Space

Hardware

Encrypted Fingerprint (Feature) DB → Secure Key Store → Fingerprint Trustlet

SPI Driver → Monitor → TrustZone Microkernel → TrustZone Driver

TrustZone Driver
Fingerprint DB Manipulating

App → Fingerprint Service → TrustZone Daemon

User Space

Encrypted Fingerprint (Feature) DB

Kernel Space

Secure Key Store → Fingerprint Trustlet → Monitor

TrustZone Driver

TrustZone Microkernel

Hardware

User Space

SPI Driver

Hardware
Fingerprint DB Manipulating

**SETTNGS**

Fingerprint manager
3 fingerprints are registered.
Fingerprint DB Manipulating

- TrustZone just scans a fingerprint and matches it against encrypted fingerprints fed from the normal world
  - It knows nothing about the number of fingerprints stored by the normal world
- An attacker can tamper the normal world framework to stealthily pre-embed special fingerprint blob (maybe fake)
  - So he/she can unlock the device or authorize other operations
  - Leave no explicit traces
Fingerprint Sensor Spying Attack
Fingerprint Framework with TrustZone

- App
  - Fingerprint Service
    - TrustZone Daemon
      - TrustZone Driver
        - Monitor
          - TrustZone Microkernel
            - SPI Driver
              - Secure Key Store
                - Fingerprint Trustlet
                  - Encrypted Fingerprint (Feature) DB
                    - User Space
                      - Kernel Space
                        - Hardware

# RSAC
FireEye
RSA Conference 2015
How about the isolation of fingerprint sensor devices?

- **App**
  - Fingerprint Service
  - TrustZone Daemon

- **Kernel Space**
  - TrustZone Driver
  - Monitor
  - TrustZone Microkernel

- **User Space**
  - Encrypted Fingerprint (Feature) DB
  - Secure Key Store
  - Fingerprint Trustlet
  - SPI Driver

- **Hardware**
  - Fingerprint Service
  - TrustZone Daemon

- **FireEye**

---

#RSAC

RSA Conference 2015
One Fingerprint Framework with TrustZone

- App
- Fingerprint Service
- Encrypted Fingerprint (Feature) DB
- TrustZone Daemon
- Secure Key Store
- Fingerprint Trustlet
- SPI Driver
- TrustZone Driver
- Monitor
- TrustZone Microkernel

User Space
Kernel Space
Hardware
Malware can read directly from the sensor
Fingerprint Sensor Spying Attack

Demo!

- While it is a really big challenge to reverse-engineer all the fingerprint operations, we made it.
Protections

¢ Long term:
  ¢ Isolate fingerprint sensors securely

¢ Short term:
  ¢ Upgrade your system to the latest version to fix all the known vulnerabilities
  ¢ Only install popular apps from Google Play on your phone with fingerprint sensors
Conclusions
Key Takeaways

- Mobile devices with fingerprint sensors are more and more popular
- But they still have severe security challenges, such as
  - Confused Authorization Attacks
  - Rooted kernel in normal world
  - TrustZone security flaws
- Such security flaws can lead fingerprint leakages
- Industry should pay more attention to audit existing design and implementations of fingerprint frameworks
Recommendations I

- Stick to mobile device vendors with timely patching/upgrading to the latest version (e.g. Android Lollipop), and always keep your device up to date.
- Always install popular apps from reliable sources.
- Enterprise/government users should seek for professional services to get protections against advanced targeted attacks.
Recommendations II

- Mobile device vendors should improve the security design of the fingerprint auth framework
  - Improved recognition algorithm against fake fingerprint attacks
  - Better protection of both fingerprint data and the devices
  - Differentiating authorization with authentication

- The existing fingerprint auth standard should be further improved to provide more detailed and secured guidelines for developers to follow

- Given a security standard, vendors still need professional security vetting/audits to enforce secure implementations
Q & A

Yulong Zhang, Zhaofeng Chen, Hui Xue, Tao Wei

FireEye Inc.