The Practical Application of IFAA Standard

Ant Financial Technical Manager  Alan Zhi Xin
The challenge and opportunity for Internet Authentication
Challenge of biometric authentication
IFAA Introduction
The open and empower of IFAA
The status and future of IFAA
The challenges to traditional authentication

Methodology
- password
- message
- bank card verification
- security question

Potential Risks
- password leak
- account enumeration attack
- unreachable
- trojan horse
- high-cost
- information leak
- information leak
Biometric authentication is the status-of-art

- What you know: easy to forget, account enum attack, trojan horse, high-frequent interrupt
- What you have: not easy to take by hands
- Who are you: low-frequent interrupt
Security Analysis for Biometric Authentication Stack

Original biometric information should never leave user’s device (Privacy Protection and Law)

The storage and matching of biometric data are facing threats.

Biometric input (e.g., fingerprint)

Senor

Feature Abstraction

Template generation

verify

Enrolment

Original template

read

Result

App

Sign the verification result and other related

Server

Trojan horse hijack

Template leak

Trojan horse hijack

Trojan horse hijack

Trojan horse hijack
TEE-based Device Security Capability

- Secure Isolation
- Secure Storage
- Secure Boot
- Secure Crypto
- Secure Location
- Secure Camera

...
Mission: provide secure and easy-to-use identity authentication service that can be accessed everywhere in Internet

- June 2015, Ant Financial, Alibaba, Huawei, SAMSUNG, ZTE, CAICT together announce IFAA.
- Uniform the whole industry chain steps to develop new and easy-to-use authentication solutions.
- Now, have 160 members (until 2018.2). Cover most of the OEMs in China: Huawei, Oppo, Vivo, Xiaomi, SAMSUNG, Meizu, ZTE, Lenovo, Gionee, Smarita etc.; Chip vendors include Qualcomm, MTK, Intel, Spreadtrum, ARM etc., and sensor vendors, secure OS vendors, standard organizations, test and certificate organizations.
The status of IFAA protocol application

- **190M+** Fingerprint payment register user (Alipay)
- **230+** Device models
- **OEM** 36 Brands
- **700M+** IFAA-enabled Android devices
- **35%+** The fingerprint payment rate (Alipay)
A brief introduction to IFAA Architecture

- Two-side secure channel based on TEE/SE capabilities.
- Preinstalled crypto keys in TEE before the devices delivered to users.
- Easy to adapt multiple biometric authentications.
Now, IFAA is open to all applications

- High device coverage: 36 OEM brands.
- High security protocol: two-side secure channel based on TEE
- High stability: used in Alipay payment scenario for almost 3 years
The applications supported by IFAA

Bank
- Pudong development bank

Third-party payment
- Suning Finance

E-commerce
- Suning Commerce

CA
- Shanghai CA
The status and future of IFAA

Current IFAA
• Fingerprint Authentication
• TEE-based Device Security
• Support most of the fingerprint devices in China market
• Set up sample apps
• Smart phone, watch and Bracelet

The Future of IFAA
• Multiple Biometric
• TEE, SE, MCU
• Support global devices
• Empower all kinds of apps
• IoT
Thank You

Contact by
xinzhi.xz@antfin.com
+86 18501648085

#HKG18
HKG18 keynotes and videos on: connect.linaro.org
For further information: www.linaro.org