InfinityGauntlet: Expose Smartphone Fingerprint Authentication to Brute-force Attack

Yu Chen
Xuanwu Lab, Tencent

Yang Yu*
Xuanwu Lab, Tencent

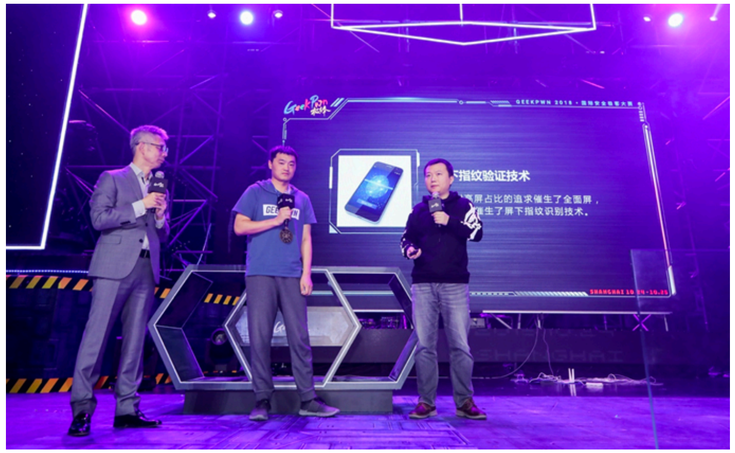
Lidong Zhai
Institute of Information Engineering, Chinese Academy of Sciences, China

Paper

Code

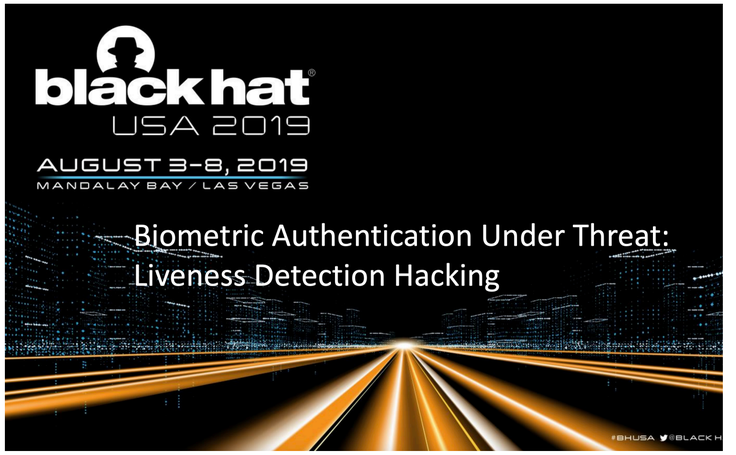
腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB

Motivation



Residual Replay Attack@GeekPwn2018

Presentation Attack@GeekPwn2019



Liveness Detection Bypass@BH-USA2019

Artificial Fingerprint Artifact
+
Latent Fingerprint on Sensing Area

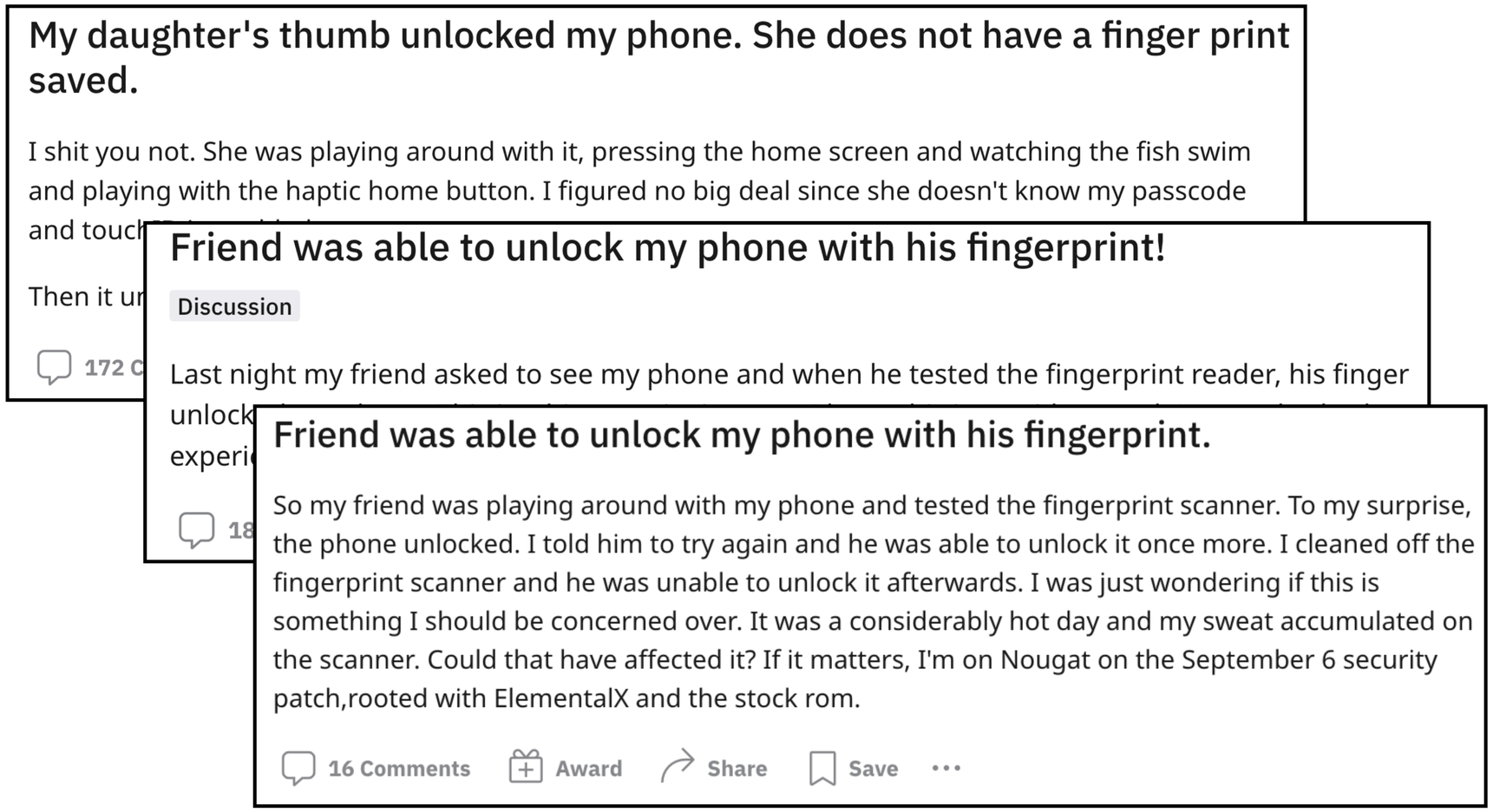
Artificial Fingerprint Artifact
+
Latent Fingerprint on Anywhere

~~Artificial Fingerprint Artifact~~
+
Latent Fingerprint on Anywhere

Can we achieve this ~~Artificial Fingerprint Artifact~~ + ~~Latent Fingerprint on Anywhere~~ **zero-knowledge attack ?**

Latent Fingerprint

Motivation



False Acceptance Rate:

$$\begin{aligned} FAR :&= \Pr\left[\mathrm{M}_{r=1}(\mathrm{S}(f)) = 1\right] \\ &= \Pr\left[\mathrm{R}\left(\mathrm{S}\left(f\right), \mathrm{S}\left(v\right)\right) = 1\right] \end{aligned}$$

False Positive Identification-error Rate:

$$\begin{aligned} FPIR :&= \Pr\left[\mathrm{M}_{r=N}\left(\mathrm{S}\left(f\right)\right) = 1\right] \\ &= \Pr\left[\bigvee_{i=1}^{N} \mathrm{R}\left(\mathrm{S}\left(x\right), \mathrm{S}\left(v_i\right)\right) = 1\right] \\ &\approx 1 - \prod_{i=1}^{N} \Pr\left[\mathrm{R}\left(\mathrm{S}\left(x\right), \mathrm{S}\left(v_i\right)\right) = 0\right] \\ &\approx 1 - \left(1 - FAR\right)^{N} \\ &\approx N \cdot FAR \end{aligned}$$

Collision Rate ~ 10^{-4}

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

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.

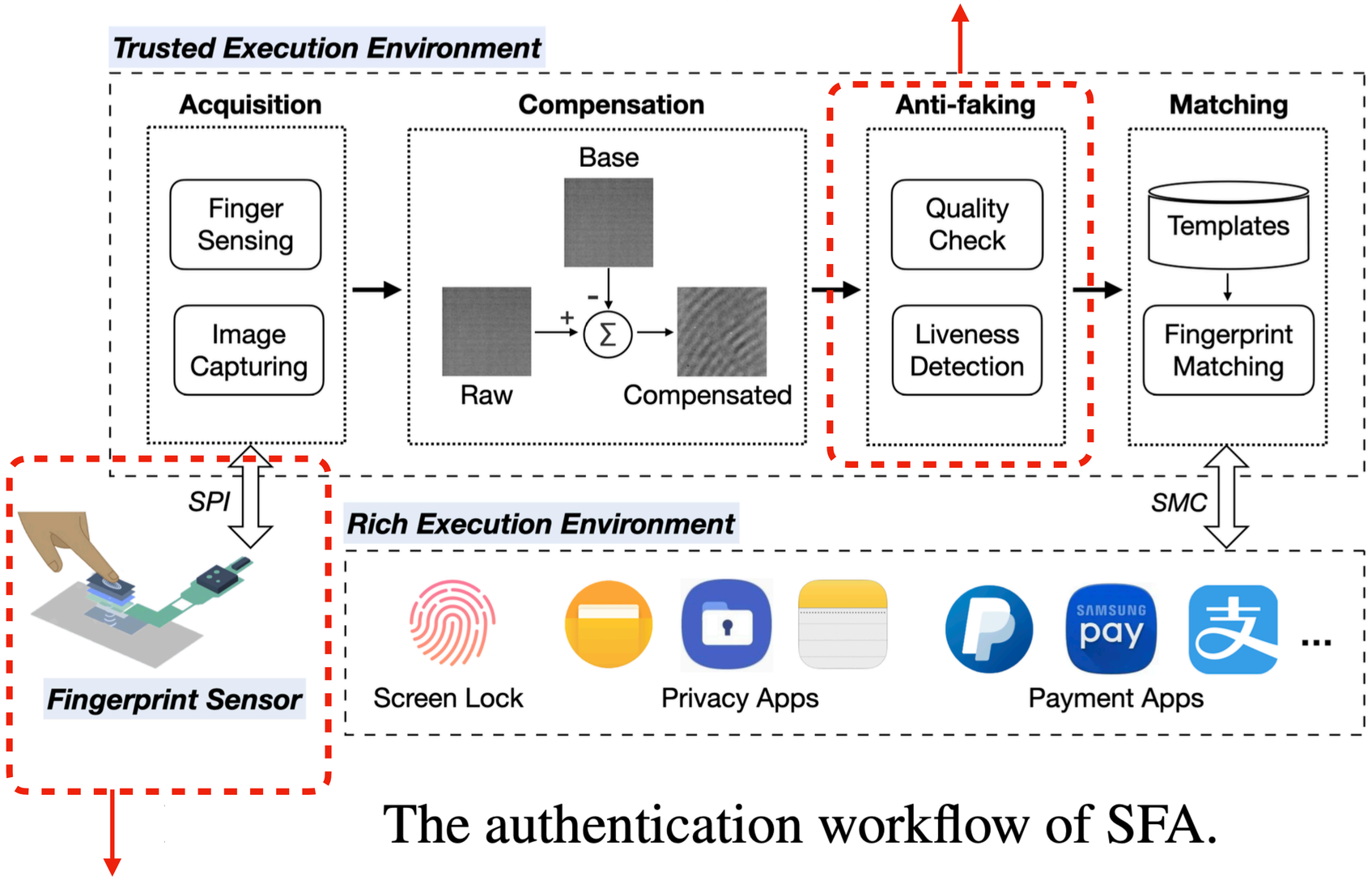
P4: Forbid SFA at least 30 seconds after five consecutive failed SFA attempts.

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

How to bypass the attempt limit?

Challenges 2

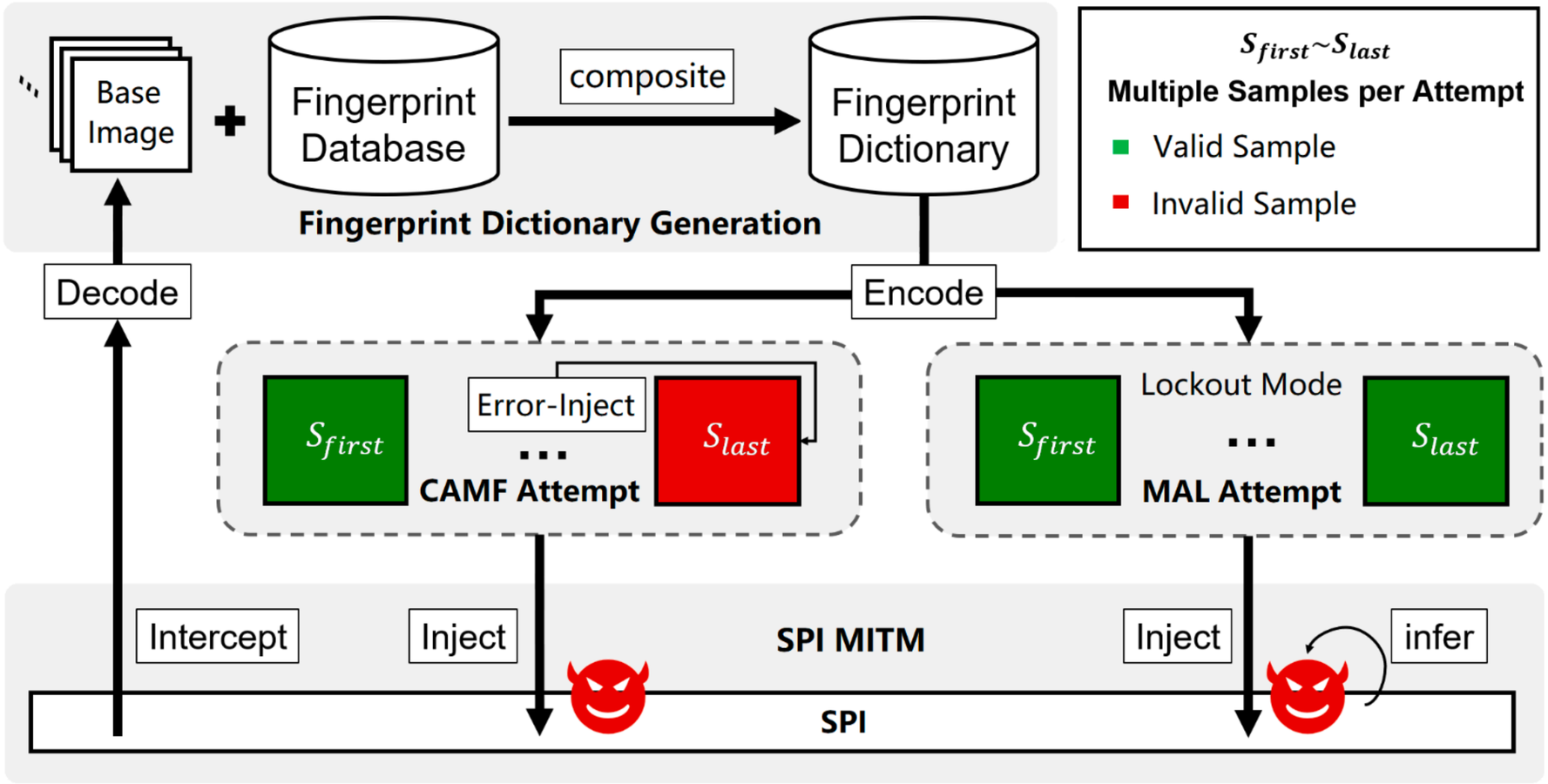
How to bypass quality and liveness detection?



The authentication workflow of SFA.

How to make automatic attempts ?

Attack Overview



Overview of INFINITYGAUNTLET.

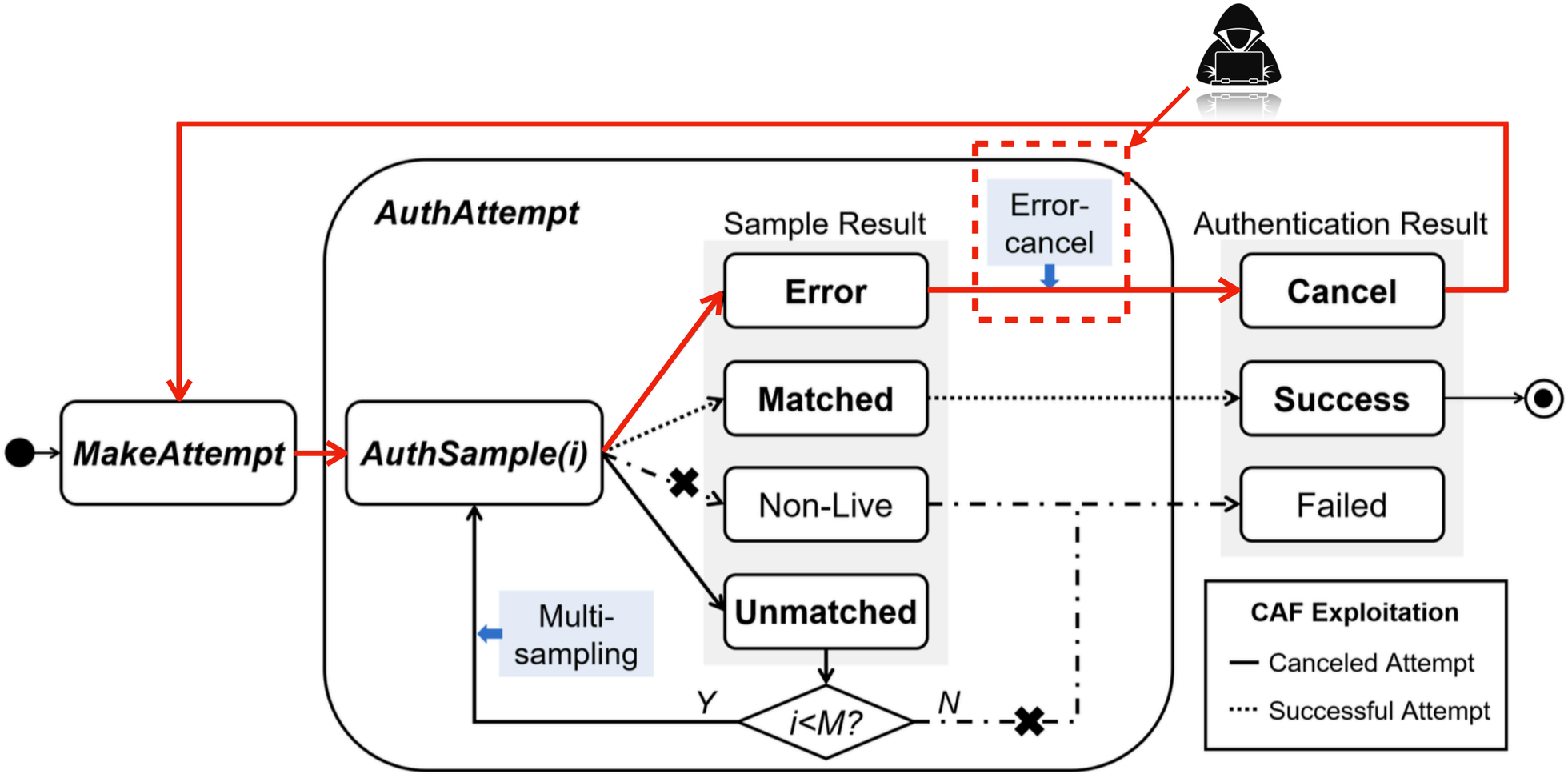
Infinity

CAMF and MAL vulnerabilities

SPI MITM injection
Fingerprint generation

Gauntlet

CAMF (CVE-2022-25820 etc.)

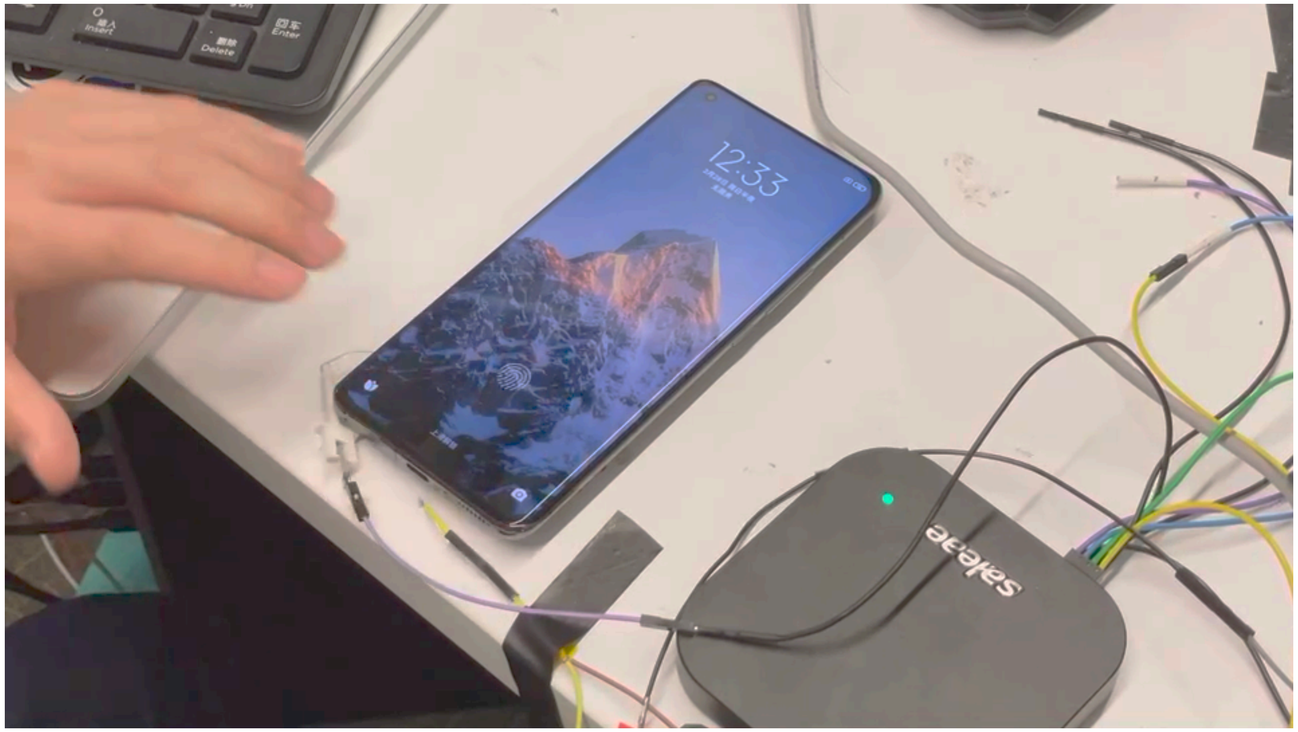


Multi-sampling mechanism and CAMF vulnerability

Affected MFRs :

- Samsung
- Xiaomi
- OnePlus
- OPPO
- Vivo (limited)
- Apple (limited)

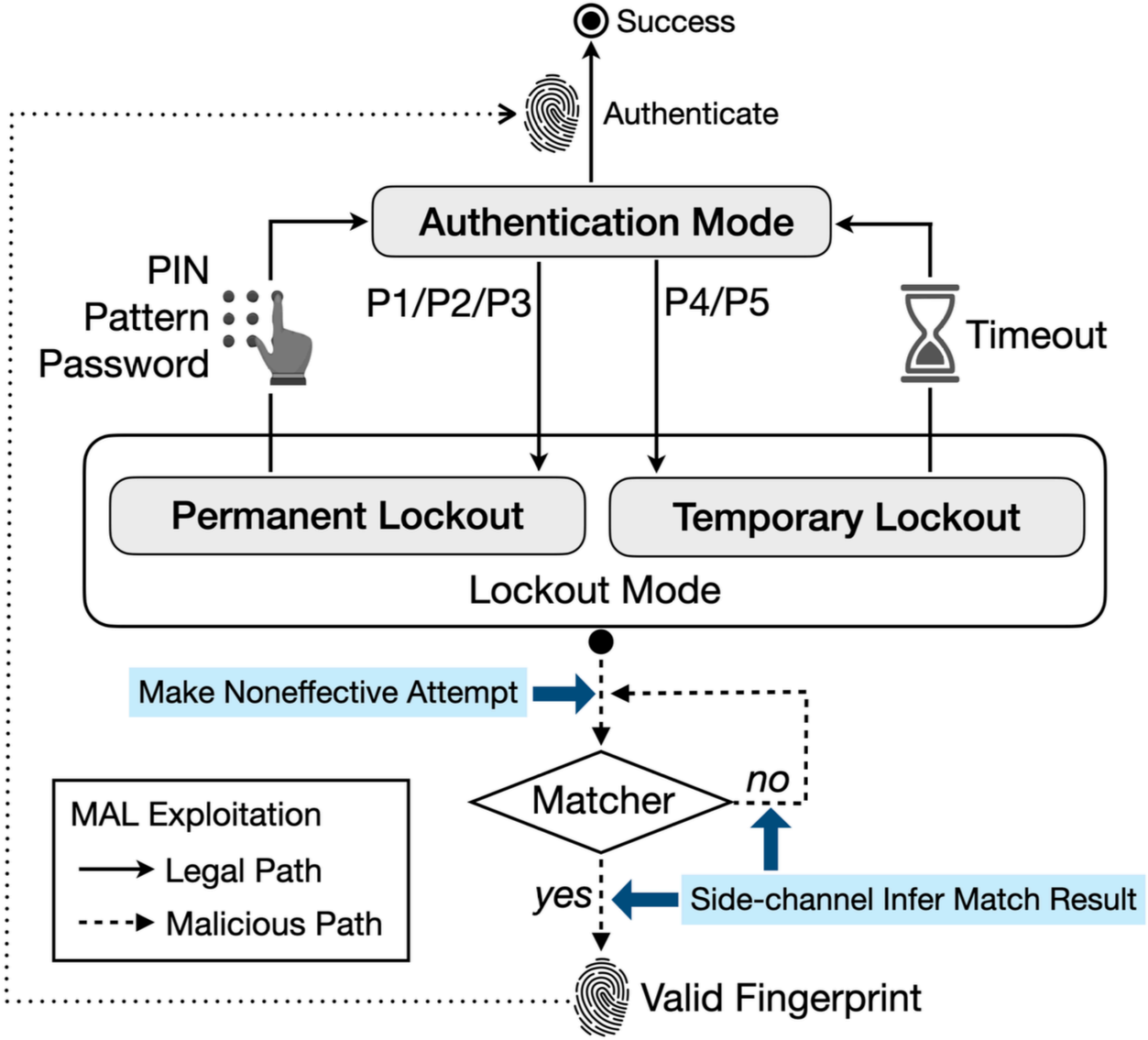
Lift-Too-Fast Error-cancel



Checksum Error-cancel

Different Types of CAMF

MAL (CVE-2021-40006 etc.)



Lockout mode and MAL vulnerability

Step1: let the SFA enter a lockout mode

Step2: Make unlimited noneffective attempts until a matched result is inferred by side-channel

Step3: Replay the successful attempt that contains the valid fingerprint after the lockout mode is exited

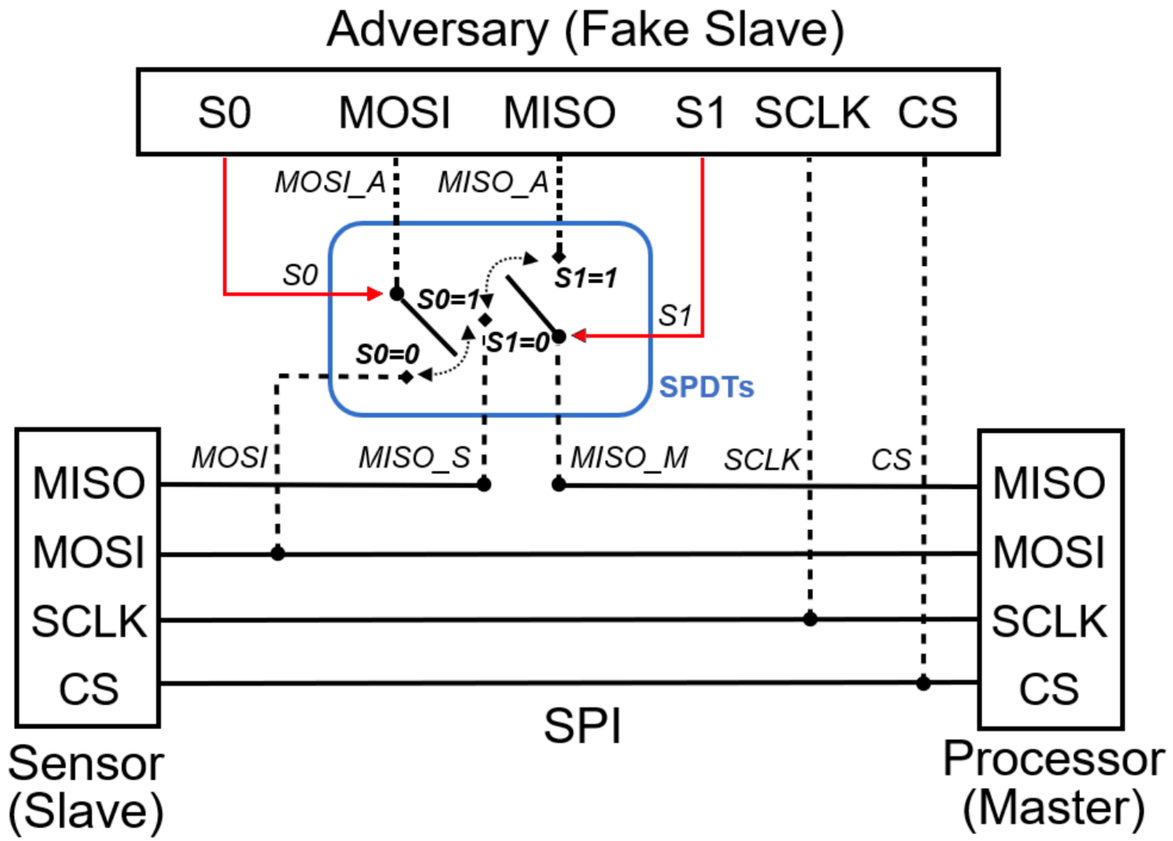
Affected MFRs :

Huawei

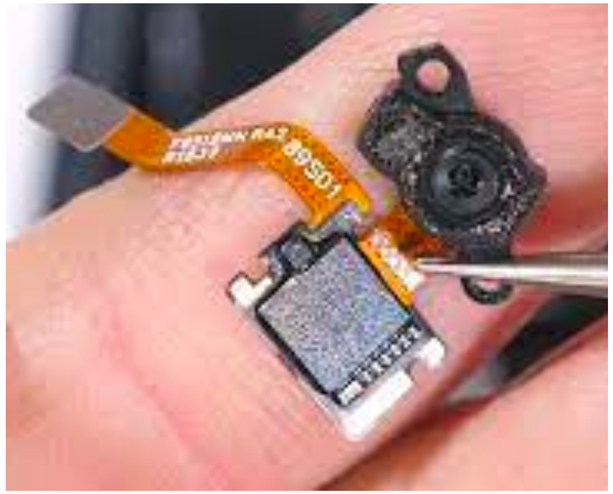
Honor (limited)

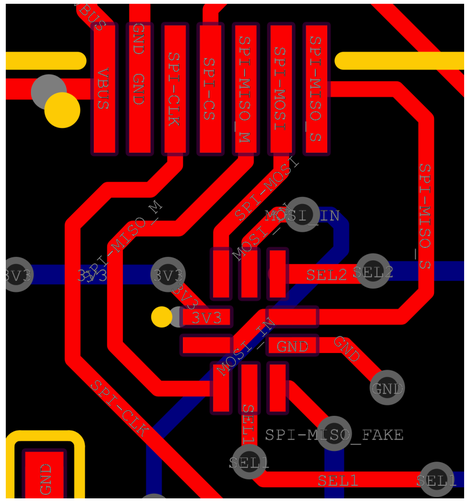
Vivo (limited)

SPI-MITM on Fingerprint Sensor



MITM Attack on SPI

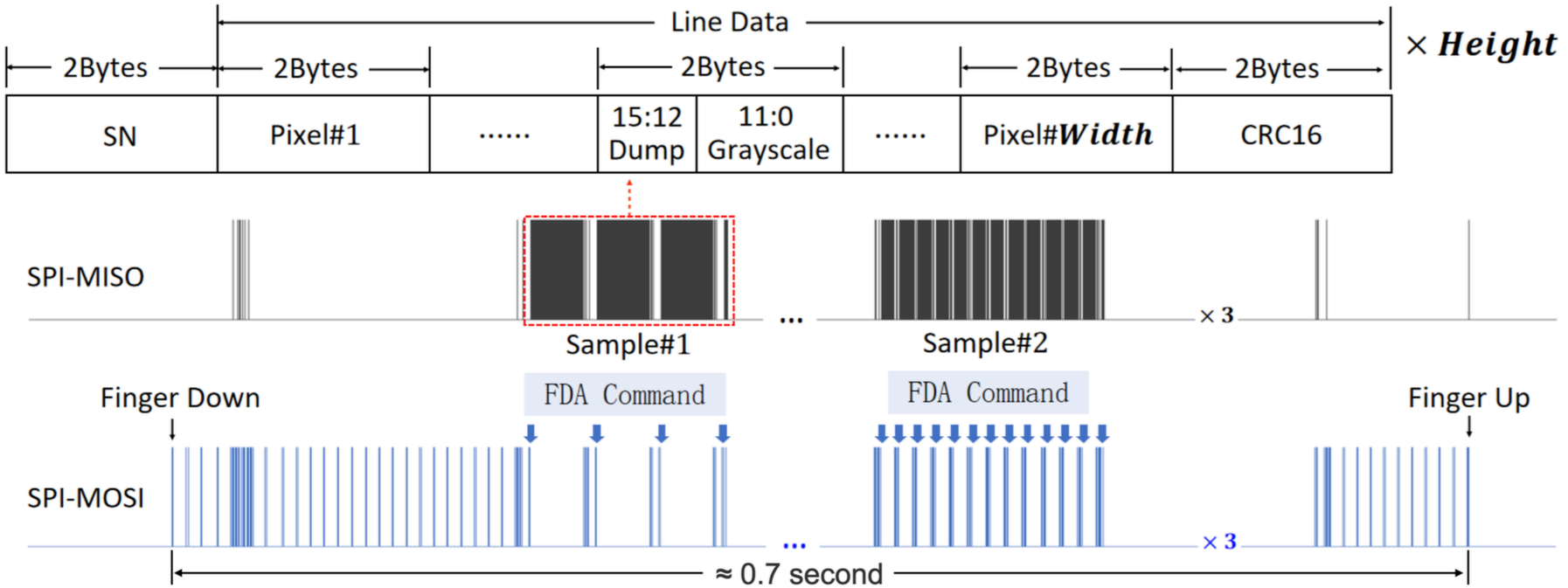


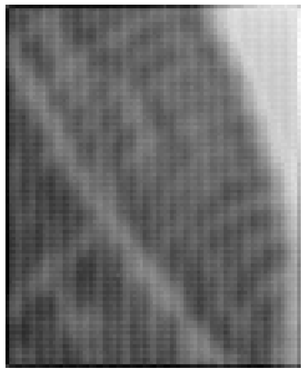


Function of the two SPDT switches.

	State	Function
S0	0	Identify the FDA command from *MOSI*.
	1	Intercept raw image from *MISO_S*.
S1	0	Keep connection from *MISO_S* to *MISO_M*.
	1	Inject raw image from *MISO_A* to *MISO_M*.

Hijacking Fingerprint Images

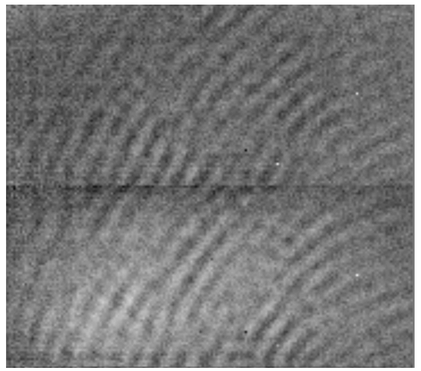




Capacitive

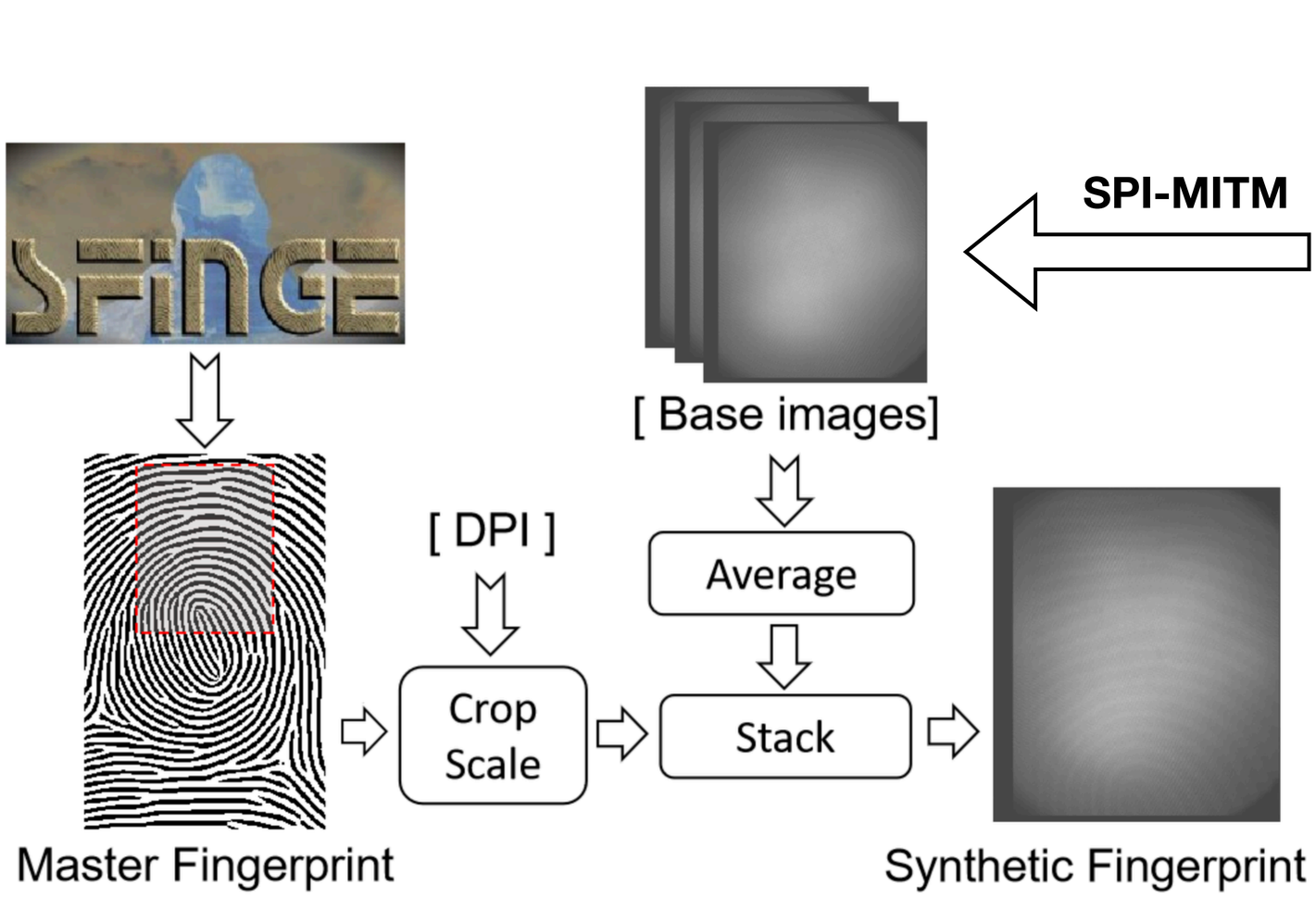
In-display optical

ultra-thin In-display optical

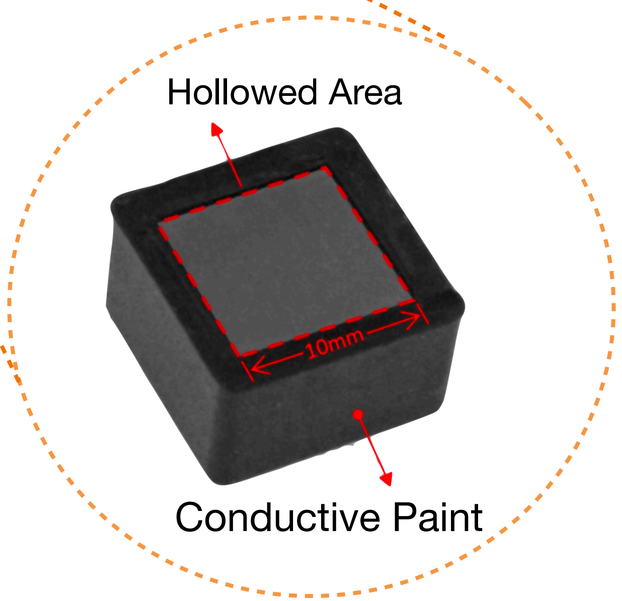


In-display ultrasonic optical

Fingerprint dictionary generation



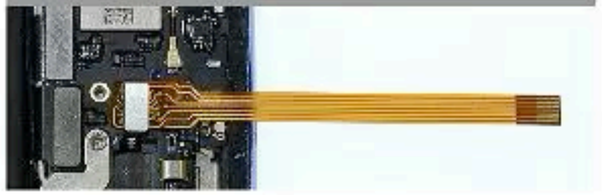
Synthetic fingerprint generation for SFA



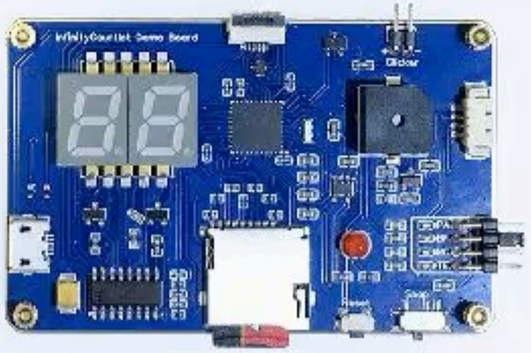
Attack Demonstration

Auto Clicker

FPC Cable



Attacking Board



Tencent Security

Xuanwu Lab

InfinityGauntlet: Expose Smartphone Fingerprint Authentication to Brute-force Attack(Usenix Security23)

Results of brute-force experiments on OnePlus 7P

	Enroll One Finger	Enroll Five Fingers
Success #	9.2[1]	41.9[2]
Failed #	0	0
Time Cost	2.01 hours	0.44 hours

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

Smartphone		Sensor		Vulnerability			Attack		
Manuf./Model	OS/Ver.	Vendor	Type	CAMF	MAL	MITM	Unlock[1]	Payment[2]	Privacy[3]
Samsung Galaxy S20U	Android 11	Qualcomm	Ultrasonic	✔	✘	✔	*FULL*	*FULL*	*FULL*
Samsung Galaxy S10+	Android 9	Qualcomm	Ultrasonic	✔	✘	✔	*FULL*	*FULL*	*FULL*
Xiaomi Mi 11 Ultra	Android 11	Goodix	Optical	✔	✘	✔	*FULL*	*FULL*	*FULL*
OnePlus 7 Pro	Android 11	Goodix	Optical	✔	✘	✔	*FULL*	*FULL*	*FULL*
OnePlus 5T	Android 8	Goodix	Capacitive	✔	✘	✔	*FULL*	*FULL*	*FULL*
Huawei Mate30 Pro	HarmonyOS 2	Goodix	Optical	✘	✔	✔	*FULL*	*FULL*	*FULL*
Huawei P40	HarmonyOS 2	Novatek	Optical	✘	✔	✔	*FULL*	*FULL*	*FULL*
OPPO Reno Ace	Android 10	Goodix	Optical	✔	✘	✔	*FULL*	*FULL*	*FULL*
Honor Magic3	Android 11	Goodix	Optical	✘	✔	✔	*LIMIT/COND*	*FULL*	*FULL*
Vivo X60 Pro	Android 11	Goodix	Optical	◯	✔	✔	*LIMIT/COND*	*FULL*	*LIMIT*
Apple iPhone 7	iOS 14.4.1	AuthenTec	Capacitive	◯	✘	✘	*PA_ONLY*	*PA_ONLY*	*PA_ONLY*
Apple iPhone SE	iOS 14.5.1	AuthenTec	Capacitive	◯	✘	✘	*PA_ONLY*	*PA_ONLY*	*PA_ONLY*
Apple iPhone SE(2nd)	iOS 15.5	AuthenTec	Capacitive	◯	✘	✘	*PA_ONLY*	*PA_ONLY*	*PA_ONLY*

[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