Certified Copy? Understanding Security Risks of Wi-Fi Hotspot based Android Data Clone Services

Siqi Ma[1], **Hehao Li**[2], Wenbo Yang[2], Juanru Li[2], Surya Nepal[3], Elisa Bertino[4]

[1] *The University of Queensland, Australia;*

[2] ***Shanghai Jiao Tong University, China;***

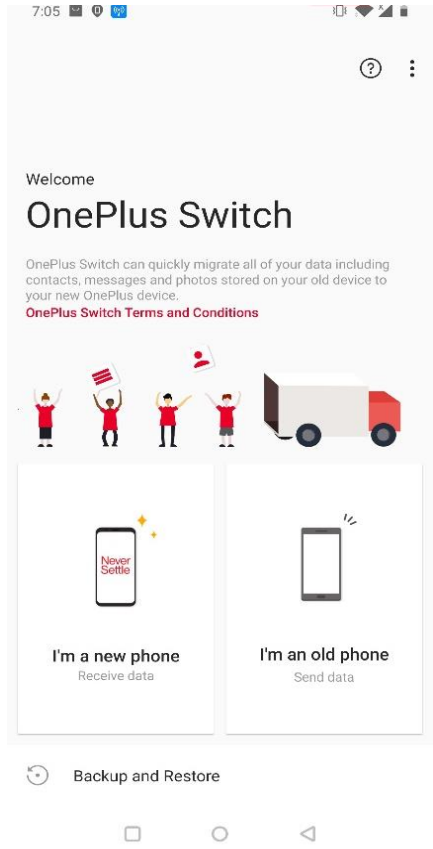
[3] *CSIRO, Australia,*

[4] *Purdue University, USA*

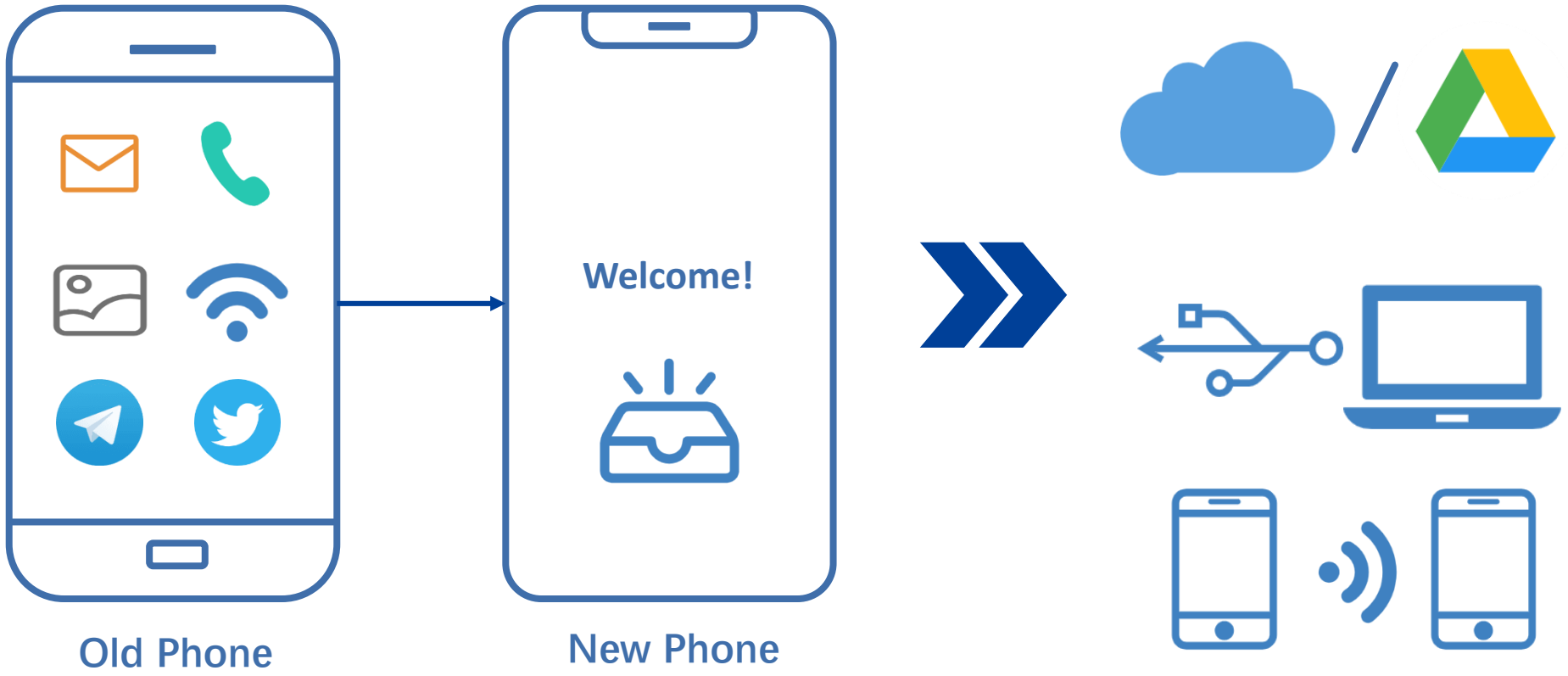
上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

Contents

Motivation: Cloning data from your obsolete phones

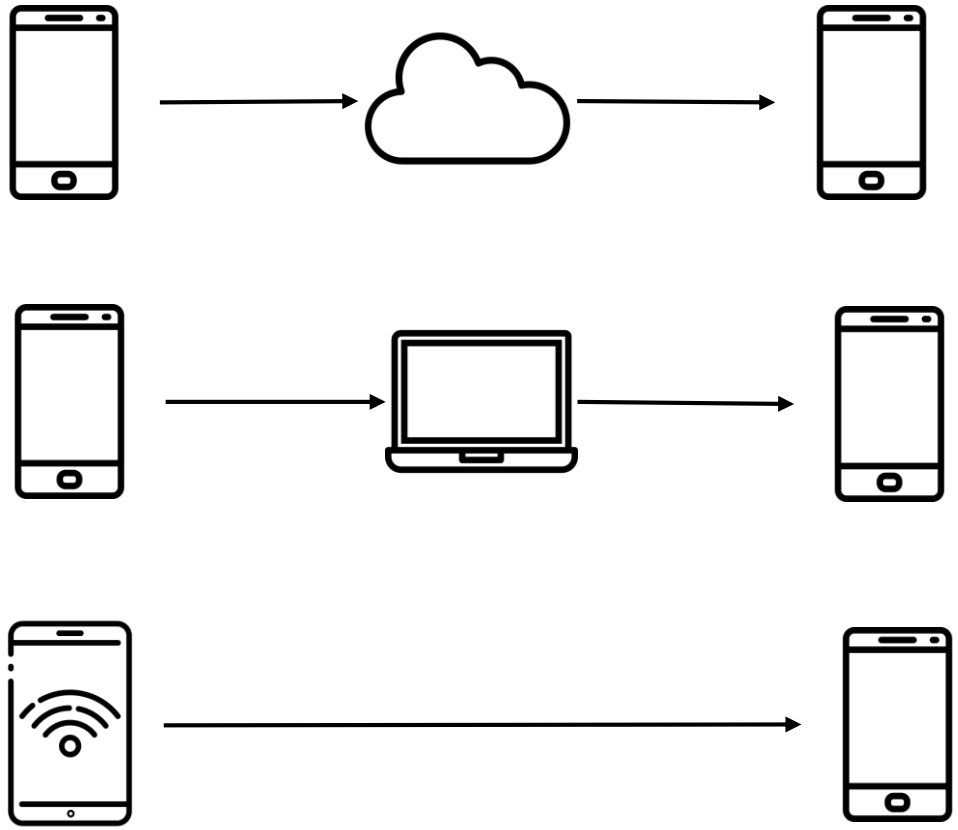


Different Transmission Channels to Clone Data



Three Types of Data Transmission

- **Cloud-based**
  - Remote server as a portal (and thus slow)
  - Charge for extra storage
- **PC-based**
  - Need a USB cable and a computer
- **Wi-Fi hotspot-based（✓）**
  - Privately built WLAN
  - Data transferring with a high speed



Security Threats against Sensitive Data

- Highly Sensitive data are allowed to be cloned!
  - SMS messages
    - Recovering SMS messages **without using default SMS app**
  - App & sandbox data
    - Exporting locally stored app data (e.g., **authentication token**)
    - **Silently app installation**
  - System settings
    - WLAN history
    - Lock screen settings

Contents

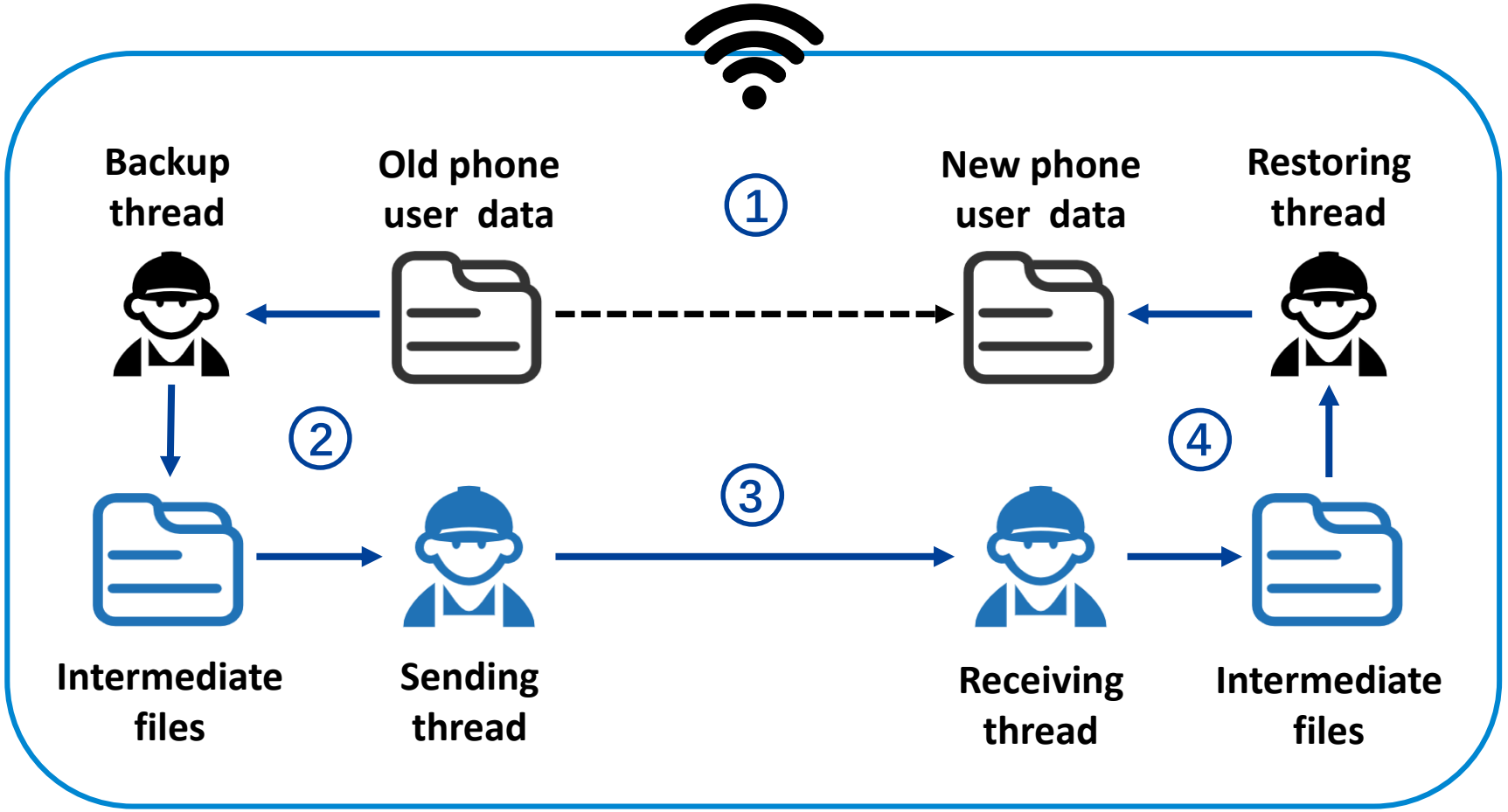
Workflow of Data Clone Service

① Wi-Fi Setup

② Data Export

③ Data Transmission

④ Data Import



Analyzing Wi-Fi Setup

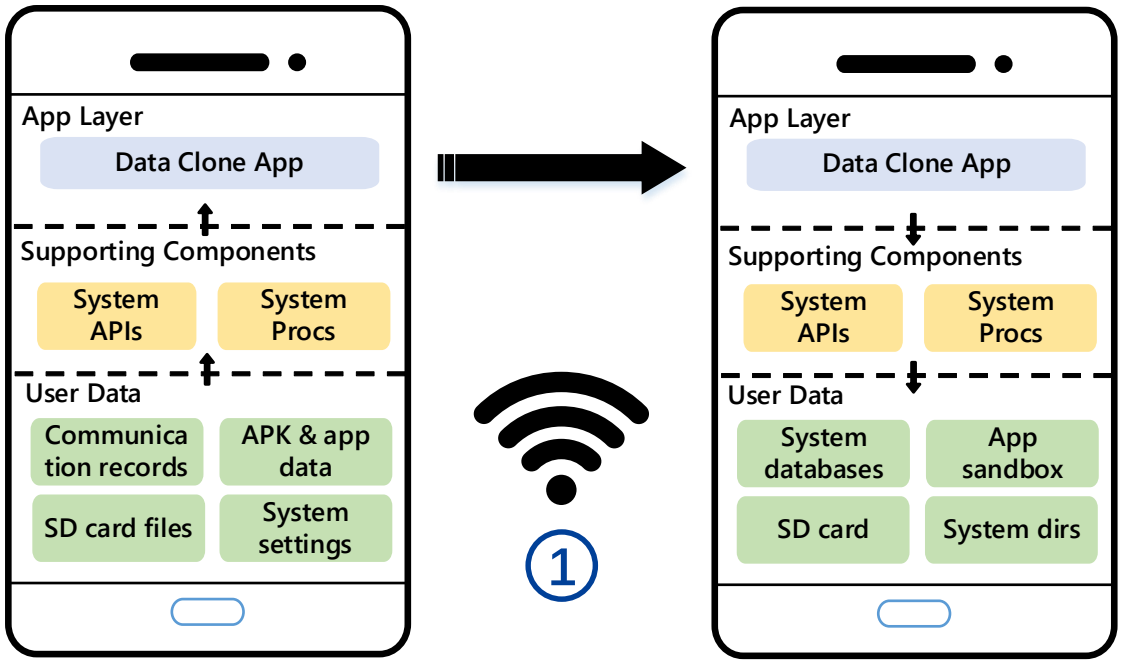
① **Wi-Fi Setup**

- Generation rules of SSID/password
- Connection restriction of Wi-Fi hotspot

② Data Export

③ Data Transmission

④ Data Import



Analyzing Data Export/Import

① Wi-Fi Setup

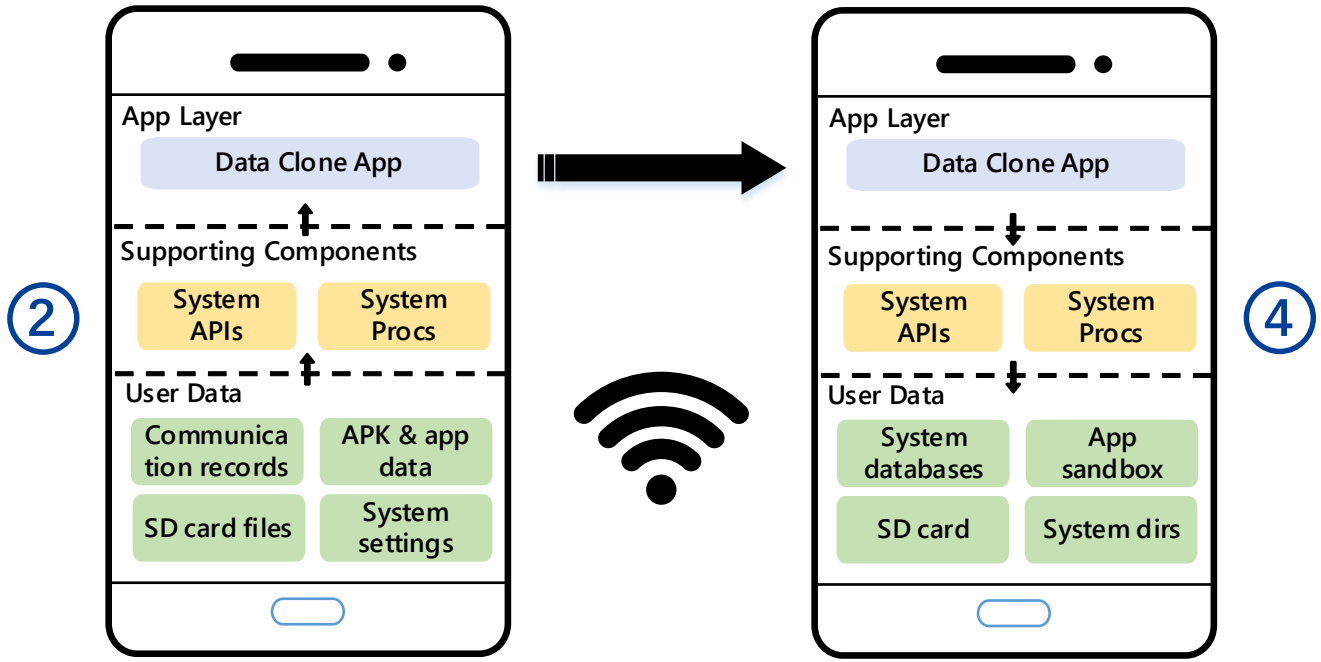
② **Data Export**

- Temporary File I/O operations
- Invoked external system services
- Customized system components

③ Data Transmission

④ **Data Import**

- Similar to data export



Analyzing Data Transmission

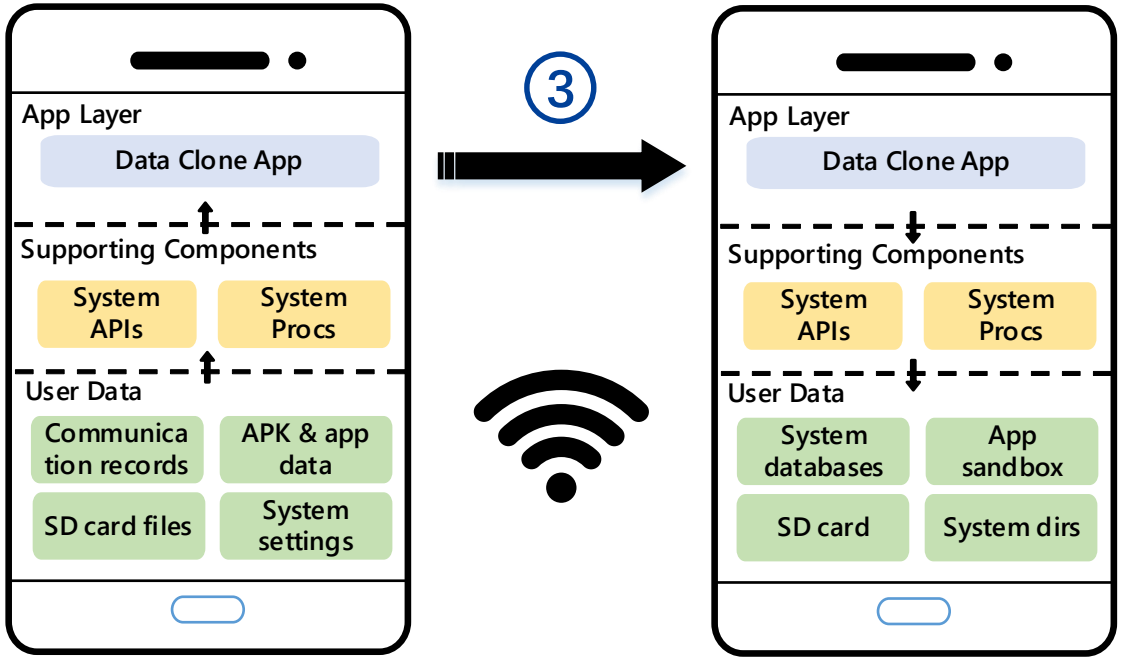
① Wi-Fi Setup

② Data Export

③ **Data Transmission**

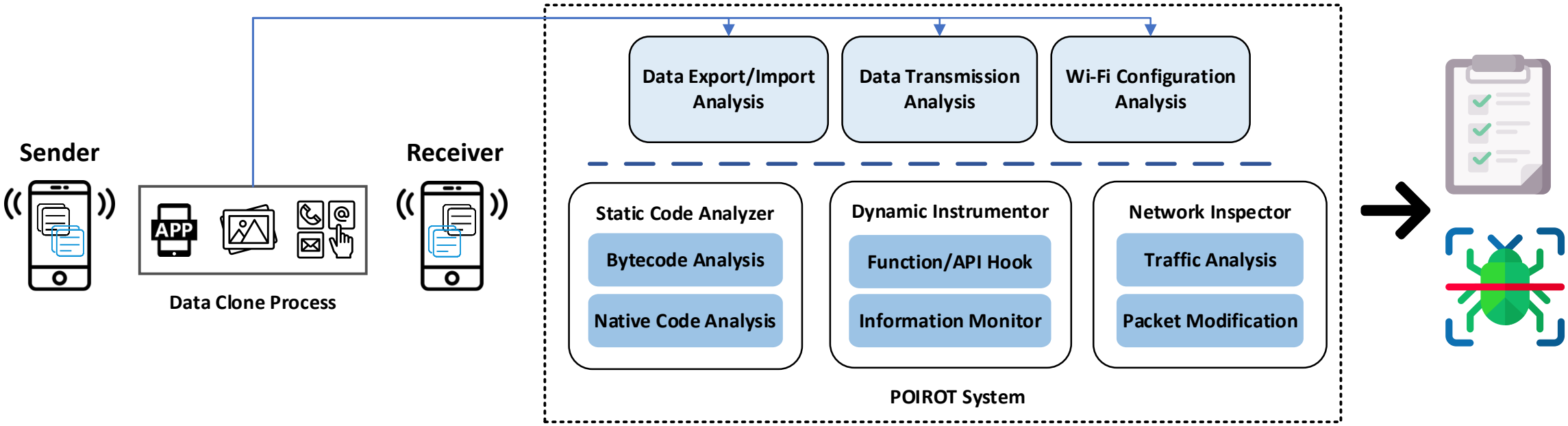
- Network traffics and the used protocols
- Data confidentiality and integrity

④ Data Import



Contents

The **POIROT** Analysis System



Dataset

- Data clone services of **eight** Android manufacturers
  - **Huawei** 
  - **OPPO** 
  - **Vivo** 
  - **Xiaomi** 
  - **Gionee** 
  - **Oneplus** 
  - **Motorola** 
  - **Nokia** 

- Devices made from **2015 to 2019**
- Android versions from **5.0 to 9.0**

Analysis Results

- **7 of 8 data clone services are vulnerable, affecting millions of sold devices**
- Weaknesses in three aspects:
  - Insecure Wi-Fi networks
  - Insecure protocols
  - Insecure files
- Attacks
  - Network-level attacks
  - On-device attack

Data Clone Service	Number of vulnerable devices
Huawei PhoneClone	≥ 100 million
OPPO BackupAndRestore	≥ 70 million
Vivo EasyShare	≥ 70 million
Xiaomi Backup	≥ 50 million
Gionee GdataGhost	≥ 15 million
OnePlus BackupRestore	≥ 4 million
Motorola Migrate	≥ 1 million

Insecure Wi-Fi networks

- **The temporarily built Wi-Fi networks are generally insecure!**
  - Predicated SSIDs
    - Allowing **attackers to detect data clone behaviors**
  - Weak Wi-Fi passwords
    - Allowing **attackers to connect to the WLAN**
  - No restriction of connection devices
    - Allowing **malicious devices to join the session**

Service	Unpredicatable SSID	Secure Wi-Fi Password	Connection Restriction
Gionee	✗	✗	✗
Huawei	✗	✗	✓
Motorola	✗	☹	✗
Nokia	✓	✓	✗
OnePlus	✗	✗	✗
OPPO	✗	☹	✗
Vivo	✗	✗	✗
Xiaomi	✗	✗	✗

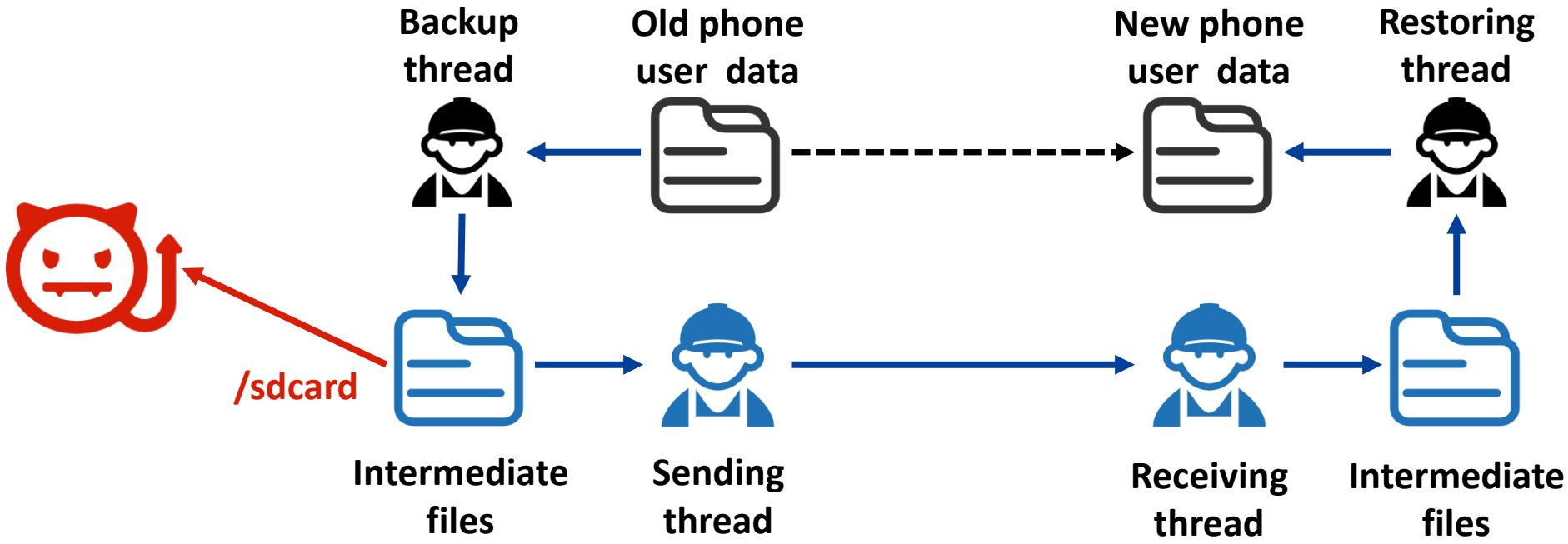
Insecure communication

- **No data clone service** encrypts transferred data
  - **Data Eavesdropping Attack**: *Ginoee, Huawei, Oneplus, OPPO, Vivo, Xiaomi*
- **No data integrity verification**
  - **Data Tampering Attack**: *Ginoee, Oneplus, OPPO, Vivo, Xiaomi*
  - Only *Huawei* and *Xiaomi* employ data checksum (*Xiaomi* however fails to validate it)

Service	Protocol	Service Port	Encrypted Transmission	Integrity Check
Gionee	TCP	5024	✗	✗
Huawei	FTP/TCP	-	✗	✓
Motorola	TCP	6000	✗	✗
Nokia	TCP	8988	✗	✗
OnePlus	TCP	8940	✗	✗
Oppo	TCP	8939	✗	✗
Vivo	HTTP/WebSocket	10178	✗	✗
Vivo	TCP	57383-57386	✗	☹

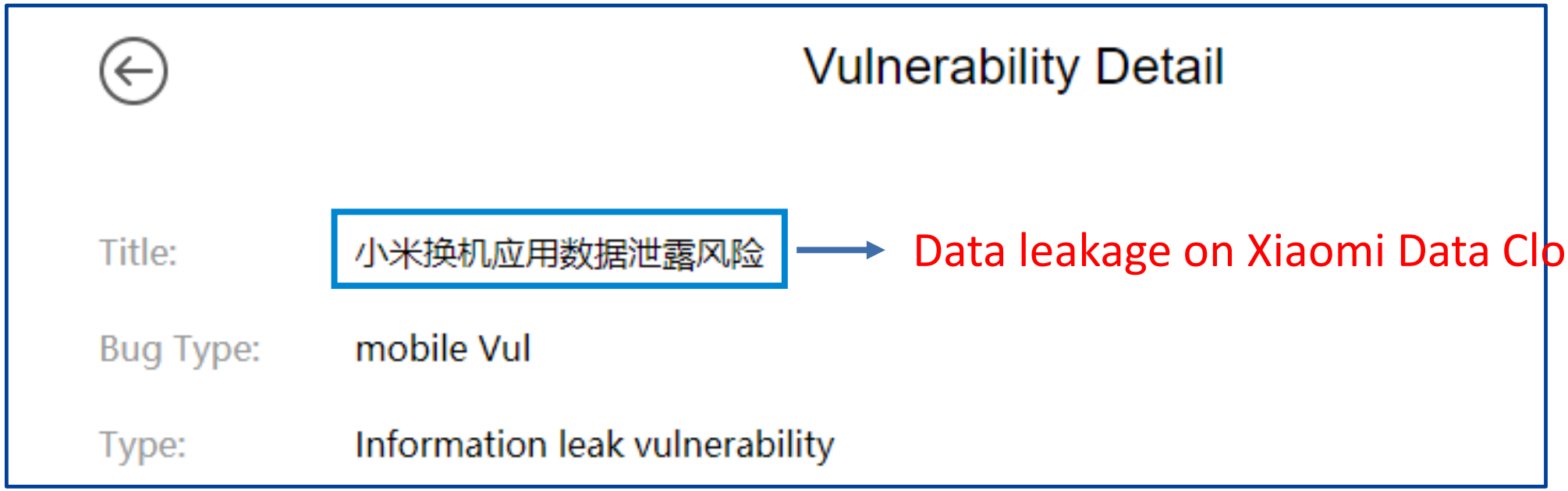
Insecure Files

- Asynchronous data transmission and data export/import
  - Intermediate data **storing on SD card as temporary files**, easy to retrieve
- **On-device data extraction attack**: *Gionee*, *Nokia*, *OnePlus*, *Xiaomi*



Feedbacks and Updates

- Feedbacks from several vendors
  - **Bounty awards received**
- Updated services
  - **OPPO，Vivo，Xiaomi**



Contents

Conclusion

- A comprehensive investigation against **customized Wi-Fi hotspot based data clone services** on Android
- An analysis system, **POIROT**, to help **detect security flaws** in those services
- Finding vulnerabilities in **7/8 investigated data clone services**
  - Vulnerable to **both on-device attack and network-level attacks**
  - Affecting **millions of Android phones in use**
- **We have helped manufacturers to fix those flaws**

Thanks and Questions?