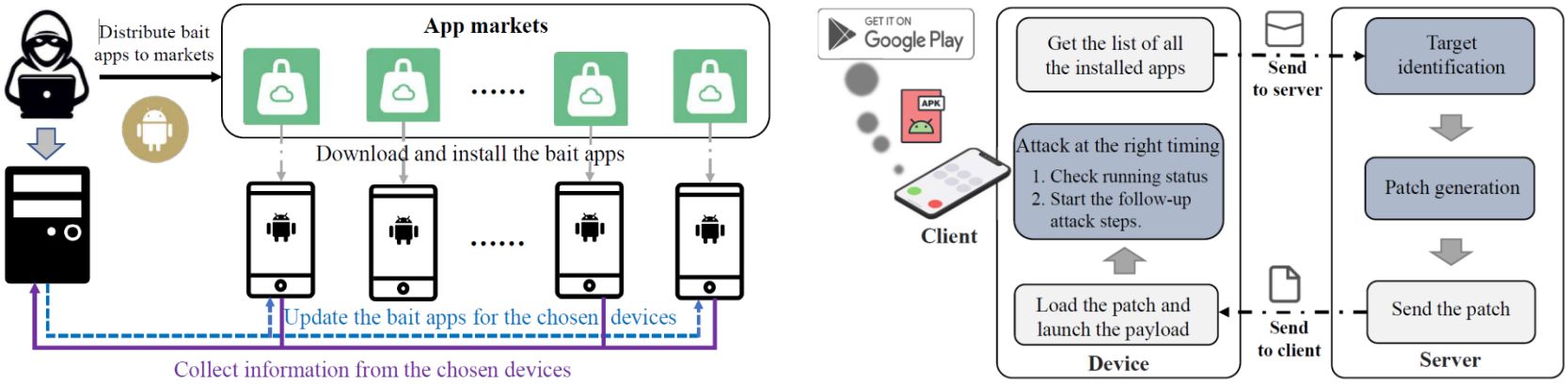
# VenomAttack: Automated and Adaptive Activity Hijacking in Android

**Pu SUN, Sen CHEN, Lingling FAN, Pengfei GAO, Fu SONG, Min YANG**

Frontiers of Computer Science, DOI：10.1007/s11704-021-1126-x

# Problems & Ideas

- Activity hijacking attack in Android :
  - Existing activity hijacking attacks no longer pose an effective security threats in recent Android versions.
  - Existing activity hijacking attacks have no capable of large-scale and automated attacks.
- Ideas: A hotpatch based activity hijacking attack that can bypass all existing defense methods through clever design, and has a large range and automatic attack capability.




VenomAttack scheme and workflow of VenomAttack. Left: the adversary develops some bait apps with different interesting and/or useful functionalities to attract more users and distributes them via app markets (e.g., Google Play Store); Right: workflow of VenomAttack contains three main phases : (1) target identification; (2) patch generation and (3) attack at the right timing.

# Main Contributions

- Contributions:
  - A more practical and powerful attack, VenomAttack, using hotpatch techniques, newly discovered flaw and bug.
  - We conduct extensive experiments and user study, which demonstrate the effectiveness of VenomAttack.
  - We conduct a systematic study of existing activity hijacking attacks under various defense mechanisms.

**Table 4** Results of bypassing state-of-the-art defense mechanisms

| Attacks \ Defense | Offline Analysis Methods | | | | | Android Design Restrictions [12, 32] [20, 33] | Real-time Detection Methods | | |
|---|---|---|---|---|---|---|---|---|---|
| | Lee *et al.* [6] | TICK [9] | CENTAUR [14] | MR-Droid [17] | TDroid [16] | | WindowGuard [15] | ActivityShielder [18] | Activity Hijacking Protector [34] |
| Attack in [8] | ● | ● | ● | ● | ● | ● | ● | ● | ◐ |
| Activity hijacking [3] | ○ | ○ | ○ | ○ | ● | ● | ● | ● | ● |
| Task hijacking [5] | ◐ | ● | ◐ | ◐ | ◐ | Unknown | ● | ● | ◐ |
| ActivityHijacker [4] | ● | ● | ● | ● | ● | ● | ● | ● | ◐ |
| Information stealing attack [9] | ● | ● | ● | ● | ● | ● | ● | ● | ◐ |
| Activity injection [6] | ● | ● | ● | ● | ● | ● | ● | ● | ○ |
| Activity hijacking [10] | ○ | ○ | ○ | ○ | ● | ● | ● | ● | ○ |
| Stranghogg 2.0 [11] | Unknown | Unknown | Unknown | Unknown | ◐ | ● | ○ | ○ | ◐ |
| VenomAttack | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ |

●: Fully detect ◐: Partially detect ○:Unable to detect

Results of various activity hijacking bypassing the defense mechanisms: only VenomAttack can not be detected or restricted by any existing defense method. Other existing attacks are detected or restricted by some defense mechanisms.