Abusability of Automation Tools on Intimate Partner Violence

Shirley Zhang, Paul Chung, Jacob VerVelde, Nishant Korapati, Rahul Chatterjee, and Kassem Fawaz

Sinister device hidden in a mum's car exposes dangerous domestic violence trend

The discovery of a sinister device hidden in a woman's car points to a growing dangerous trend that authorities are powerless to stop.

UK MPs warn against growing use of smart tech in domestic abuse

Committee's report says devices including home security systems used to coerce and control victims

TECH

Increasingly common phone act actually a relationship red flag, study reveals

By Rebekah Scanlan, News.com.au

Published Nov. 25, 2024, 9:11 a.m. ET

15 Comments

The Spyware Used in Intimate Partner Violence

Publisher: IEEE Cite This PDF

Rahul Chatterjee ; Periwinkle Doerfler ; Hadas Orgad ; Sam Havron ; Jackeline Palmer ; Diana Freed **All Authors**

Abusive Partner Perspectives on Technology Abuse: Implications for Community-based Violence Prevention

Author: Rosanna Frances Bellini | Authors Info & Claims

Tech companies should build products with domestic violence victims in mind, expert says

By Grace Atta | Domestic Violence

Sat 10 Feb 2024

Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review

Michaela M Rogers [1,✉], Colleen Fisher [2], Parveen Ali [3], Peter Allmark [4], Lisa Fontes [5]

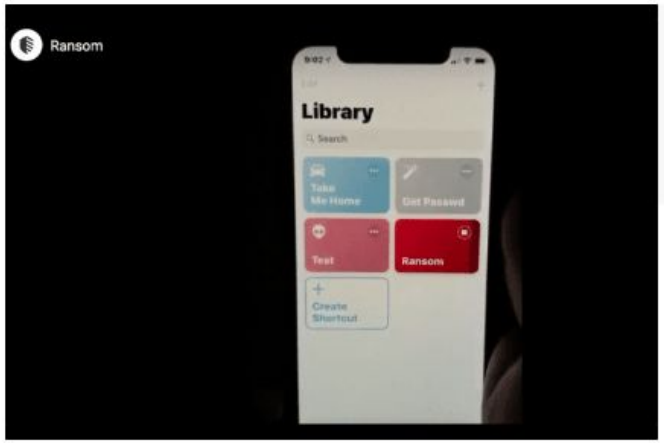
Home › Apple

Apple Cybersecurity

IBM Warns of Apple Siri Shortcut Scareware Risk

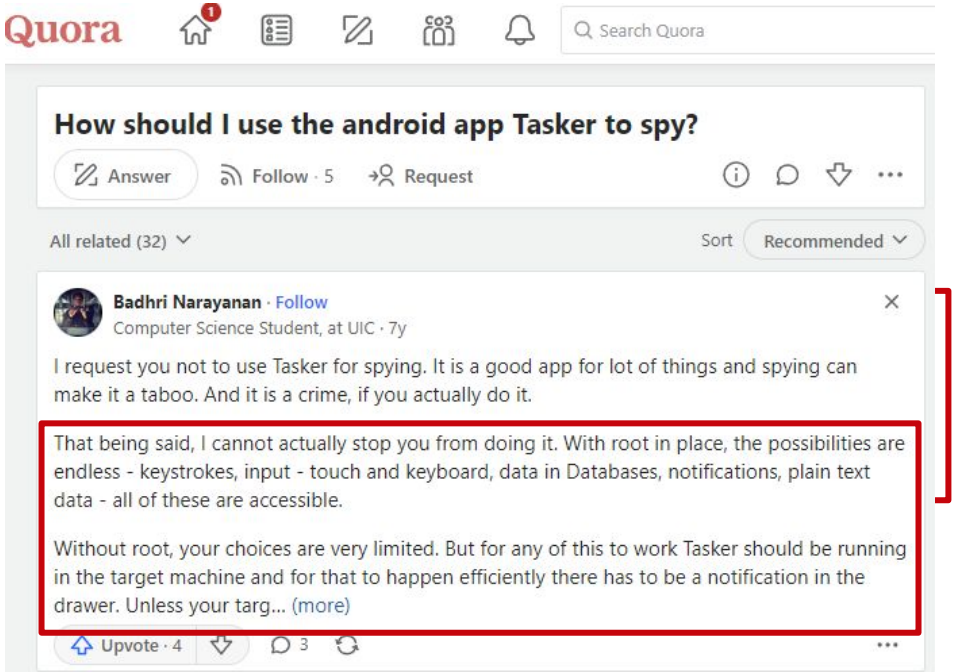
By **Sean Michael Kerner** - January 31, 2019

Share



Apple's Siri voice assistant is intended to help users, but according to new research published by IBM on Jan. 31, attackers could potentially abuse the Siri Shortcuts feature.

Apple introduced Siri Shortcuts with iOS 12, enabling users and developers to use Siri to automate a series of tasks. IBM's X-Force security division discovered that it is possible to use a Siri Shortcut for malicious purposes, including tricking a user into paying a fee to avoid having his or her information stolen in an attack known as scareware. In a proof-of-concept Siri Shortcuts scareware attack developed by IBM, a malicious shortcut is able to read information from an iOS device and then demand a fee from the user, all with the native Siri voice.



- Spy by Reezy
- Just run the command with the voice **"Hey Siri, Spy"** when your phone is in a friend's hands
- The shortcut takes a photo without opening the camera and saves the photo to the gallery
- Enjoy

What is Automation App?

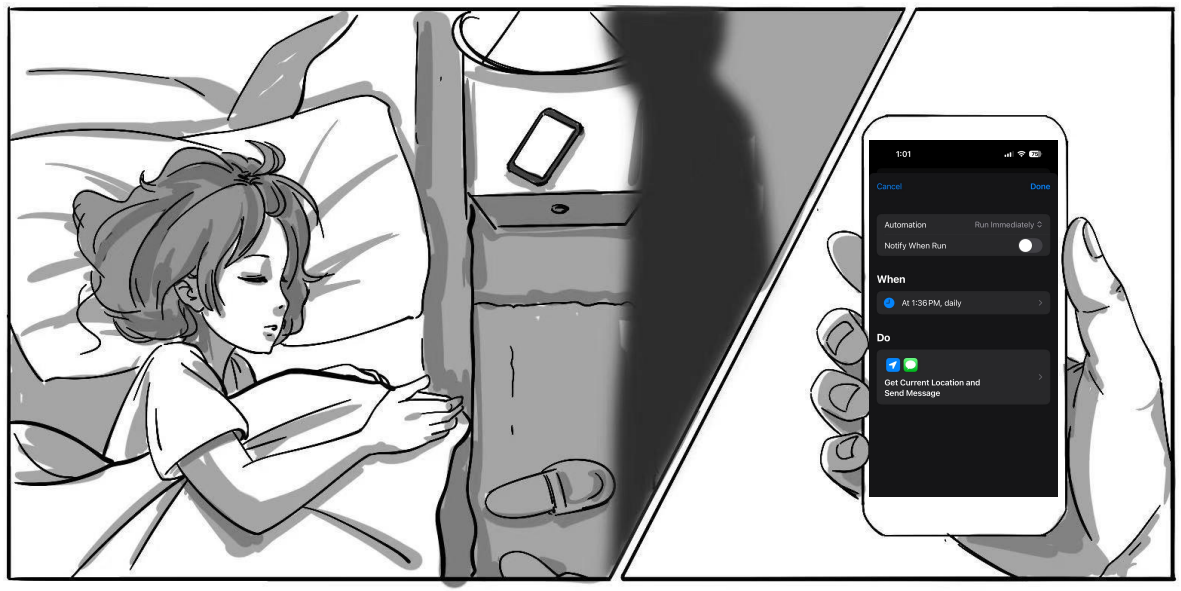
Wednesday 3:00 PM,

“Group meeting in 30 mins!”

Trigger → ***Actions (recipe)***

Intimate Partner Violence (IPV) Threat Model

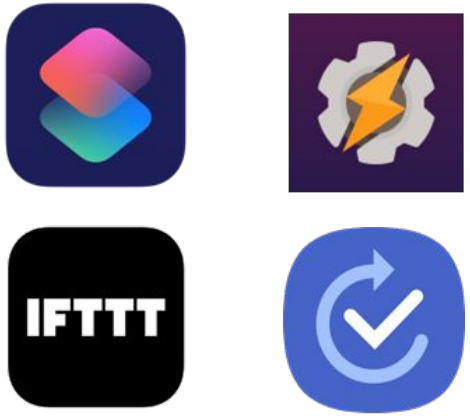
- Have **capability to unlock** (at least once) victim's mobile phone.
- Capable of communicating with the victim in various ways, such as phone calls, texts.



Research Questions

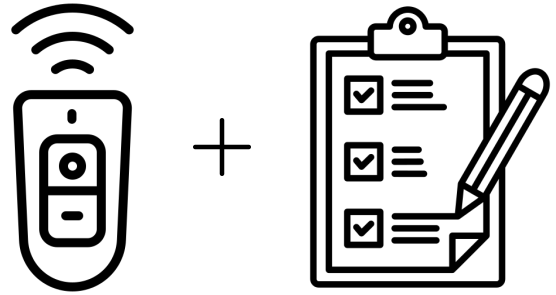
- **RQ1** ⇔ Capability Analysis
  - What are the *capabilities* of popular automation applications?
- **RQ2** ⇔ Attack Showcase
  - What specific *harms* might these capabilities pose to IPV victims?
- **RQ3** ⇔ Detector & Measurement
  - How can abusive automation recipes be *detected* to support affected users?

Capability Analysis



4 Popular
Automation App

UI Step-through



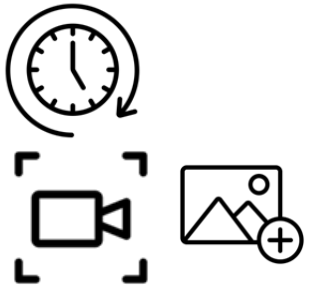
Collect
Triggers + Actions

Capability Analysis – Triggers

Shortcuts and Tasker support all triggers, while IFTTT and Bixby Routine support less user action triggers.

- Internal events
- External events

- Preset time
- User actions



Capability Analysis – Actions

Both Tasker and Shortcut support Turing-complete logic, while Bixby Routines limited to one-shot if-this-then-that.

- Device control 
- Flow control 

- Data management 
- Communication 

RQ1: What are their capabilities?

Having high privilege, and are capable of collecting, exfiltrating sensitive information from the phone.

Furthermore, they can manipulate the device hardware/software functionality.

Device control
Flow control
Data management
Communication

Attack Showcase

Automation apps can easily achieve…

- Surveillance — When  Collect  Send 
- Impersonation — When  Send  To third party
- Overloading — Repeat 100 times, perform 
- Lockout/Control — When  Do  ; Send myself 

Attack Showcase

We utilized Shortcut to capture the last image on victim's device, send that to a server of the attacker through HTTP.

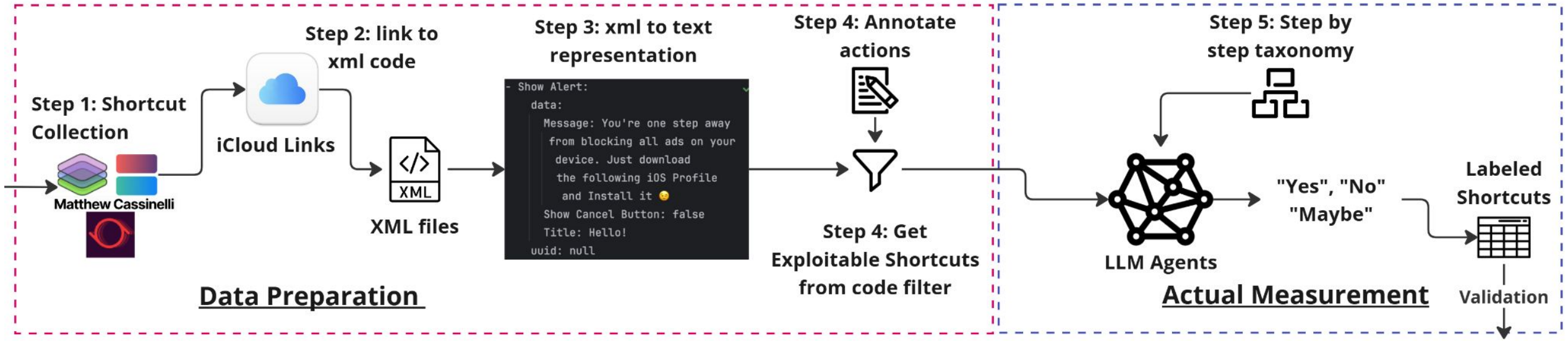
RQ2: What harms could these capabilities cause?

Enable four Tech-Facilitated Attacks: Surveillance, Overloading, Impersonation, Lockout/Control.

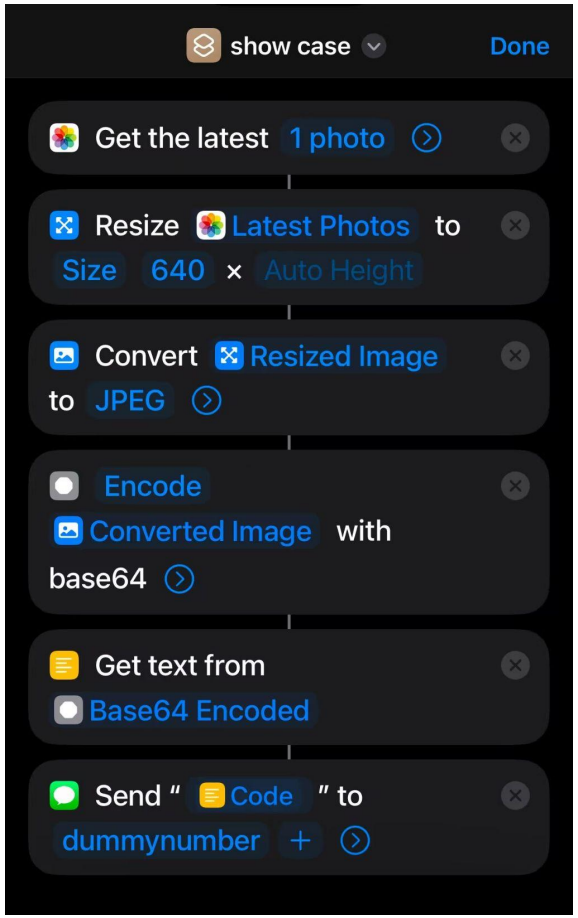
And, it is hard for the victim to trace where the attack came from.

Detector & Measurement – Overview

We evaluated **4** Domains – **12,962** Shortcuts.



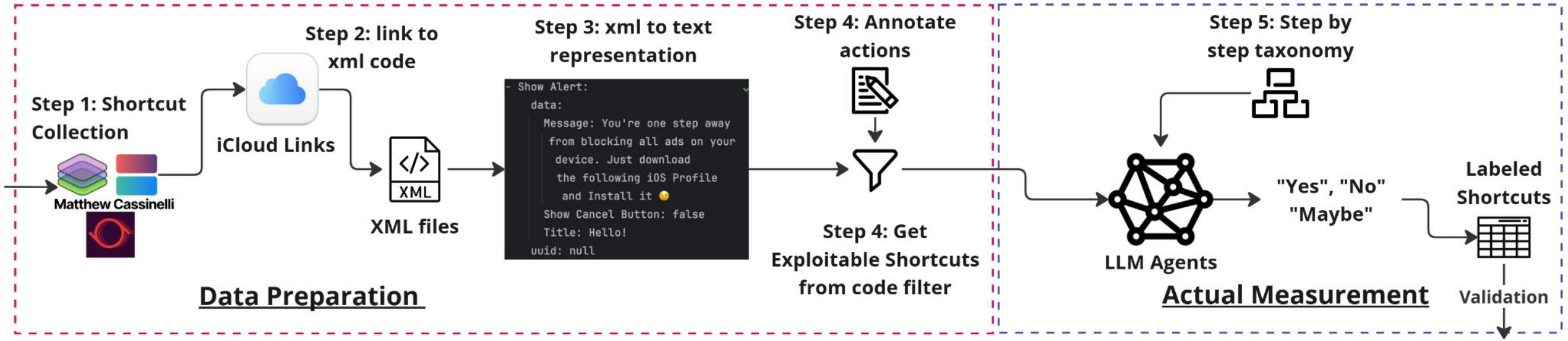
Detector & Measurement – Overview




```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>WFQuickActionSurfaces</key>
        <array/>
        <key>WFWorkflowActions</key>
        <array>
                <dict>
                        <key>WFWorkflowActionIdentifier</key>

<string>is.workflow.actions.getlastphoto</string>
                        <key>WFWorkflowActionParameters</key>
                        <dict>
                                <key>UUID</key>
                                <string>1FC682B0-6069-4C5A-9531-
0AEB1E8FEE62</string>

<key>WFGetLatestPhotosActionIncludeScreenshots</key>
                                <false/>
                        </dict>
                </dict>
                <dict>
                        <key>WFWorkflowActionIdentifier</key>

<string>is.workflow.actions.image.resize</string>
                        <key>WFWorkflowActionParameters</key>
                        <dict>
                                <key>UUID</key>
                                <string>51C3BDE3-42F8-4E7B-8043-
670E8E1AA206</string>
                                <key>WFImage</key>
```

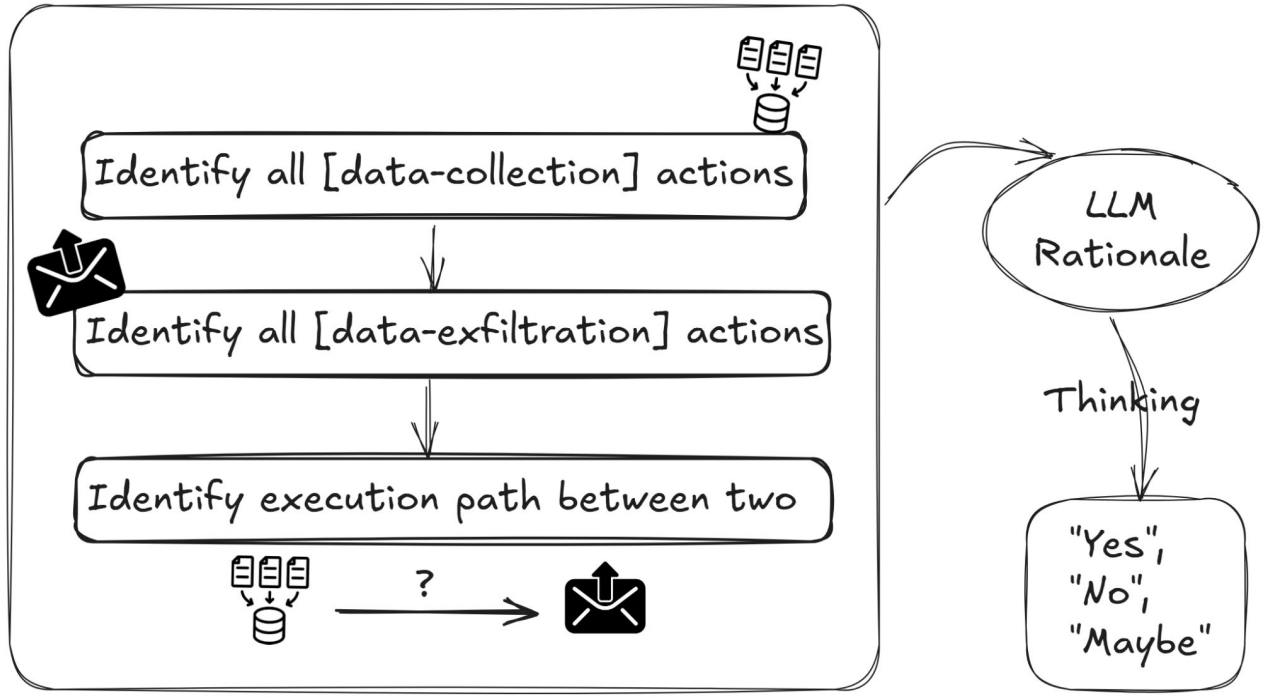
Extract the important information from XML

Detector & Measurement – Overview

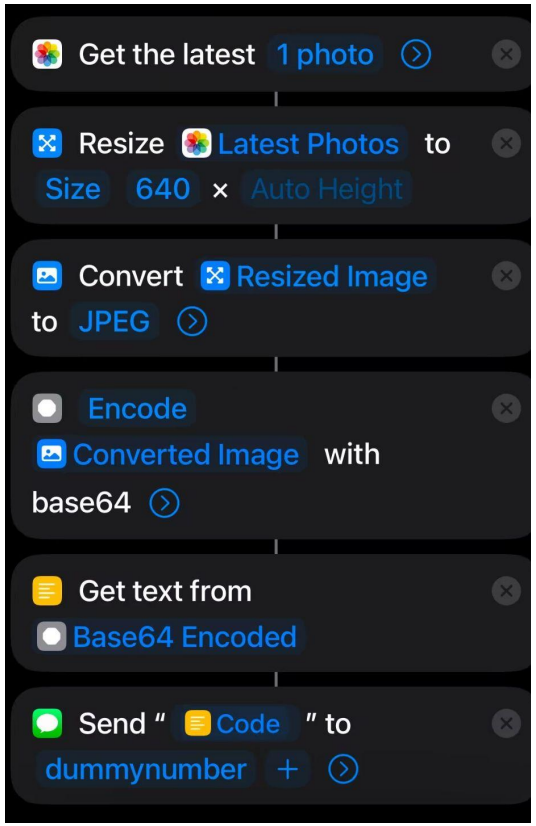


Detector & Measurement – Prompt Design

- **Surveillance**
  - `data-collection` + `data-exfiltration` + `trace-hiding`
- **Impersonation**
  - `data-insertion` + `data-exfiltration`
- **Overloading**
  - Repeatedly `data-exfiltration` / `resource control`
- **Lockout/Control**
  - `resource control`



Detector & Measurement – Prompt Design




```
- Get Last Photos:
    data:
      Get the latest: 1 photo
      Include Screenshots: false
    uuid: 1FC682B0-6069-4C5A-9531-0AEB1E8FEE62
- Resize Image:
    data:
      Height: Auto Height
      Resize:
      - data: Latest Photos (attachment)
        uuid: 1FC682B0-6069-4C5A-9531-0AEB1E8FEE62
      Width: '640'
      to: Size
    uuid: 51C3BDE3-42F8-4E7B-8043-670E8E1AA206
- Convert Image:
    data:
      Convert:
      - data: Resized Image (attachment)
        uuid: 51C3BDE3-42F8-4E7B-8043-670E8E1AA206
      Preserve Metadata: true
      Quality: '70.0'
      to: JPEG
    uuid: B1D088B7-3C3F-4D6F-8115-9AA51E8A49CF
```

```
- Base64 Encode:
    data:
      Encode Mode: Encode
      Line breaks at: Every 76 characters
      input:
      - data: Converted Image (attachment)
        uuid: B1D088B7-3C3F-4D6F-8115-9AA51E8A49CF
    uuid: BD0F2098-22B0-4137-9479-6AE4A154DE42
- Get Text From Input:
    data:
      Custom Output Name: Code
      Get text from:
      - data: Base64 Encoded (attachment)
        uuid: BD0F2098-22B0-4137-9479-6AE4A154DE42
    uuid: 7D60231F-D9D4-4B1C-AE42-EBC229E9201A
- Send Message:
    data:
      Send:
      - data: Code (attachment)
        uuid: 7D60231F-D9D4-4B1C-AE42-EBC229E9201A
      Show When Run: true
      to:
      - dummynumber
    uuid: 80A196B0-1FF3-4A99-8A1C-2B35572E2F7A
```

Detector & Measurement – Results

Lockout/Control exploits represent the highest confirmed threat (5.06%), comparing to Spy and Stalk (0.16%), Overloading (0.5%) and Impersonation (2.62%).

Category	LLM Labeled		
	Yes	No	Maybe
Spy and Stalk	**21 (0.16%)**	244	106
Impersonation	**340 (2.62%)**	4,499	702
Lockout/Control	**656 (5.06%)**	2,227	184
Overloading	**65 (0.5%)**	101	313
Total	**1,014 (7.87%)**	/	/

Detector & Measurement – Reporting Concerns

- We emailed the automation app companies and domain manager.
- Response from Tasker:

  "If the attacker intentionally misuse the app, then notification would not help to alert victims." – when we raise concern about tutorials to turn off the notifications about Tasker.

- Response from Apple:

  "The behavior you reported requires physical access to an unlocked iPhone. Please note that we recommend that users use a strong device passcode to prevent unauthorized access to their device."

RQ3: How can abusive recipes be detected?

We designed a LLM-based detector to examine if a shortcut could be used to conduct 4 IPV attacks.

This detector is open-sourced.

Mitigation

- **Identify**:
  - OS-level monitoring
- **Detect**:
  - LLM-assisted recipe analysis
- **Protect**:
  - Pre-recipe runtime permissions
- **Respond**:
  - Persistent, informative notifications

Thank you!

Acknowledgement

Paper QR Code

Wi-Pi Lab

My website