DVa: Extracting Victims and Abuse Vectors from Android Accessibility Malware

Haichuan (Ken) Xu, Mingxuan Yao, Runze Zhang, Mohamed Moustafa Dawoud, Jeman Park, Brendan Saltaformaggio

Haichuan (Ken) Xu
haichuanxu@gatech.edu
https://haichuanxuken.github.io

Georgia Tech

Android's Accessibility (a11y) Service

Exception to Android's app-isolated sandbox design

a11y service

GOAL

Enhance usability

TECHNIQUE

Alternative input

Read screen

EXAMPLE

Benign a11y utility apps
- Text-to-Speech
- Voice control
- Gesture recognition

Attack device via GUI

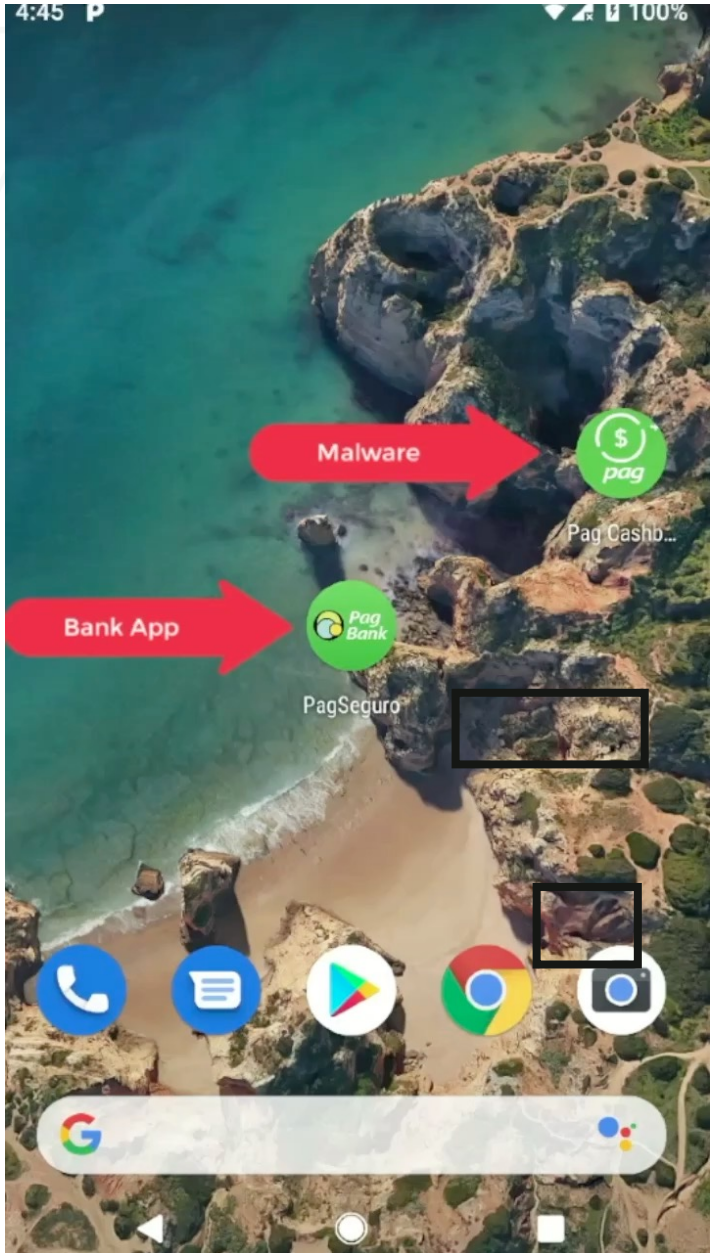
Eavesdrop

Automated GUI actions without consent

a11y Malware
- Target other apps (victims)
- Victim app manipulation (abuse vectors)
- Harder to remove (persistence mechanisms)

Georgia Tech

a11y Malware Stealing Money from Users' Mobile Banking Accounts



→ Malware clicks "Show Balance" button

→ Overlay screen hides:
Instead, the malware (Impersonating as Pag Cashback app)
1. Click "Initiate Transaction" button

→ 2. Enter attacker's account number

→ Pag Bank app (Brazilian banking app)
3. Enter available balance

→ User clicks continue
4. Click "Send Money" button

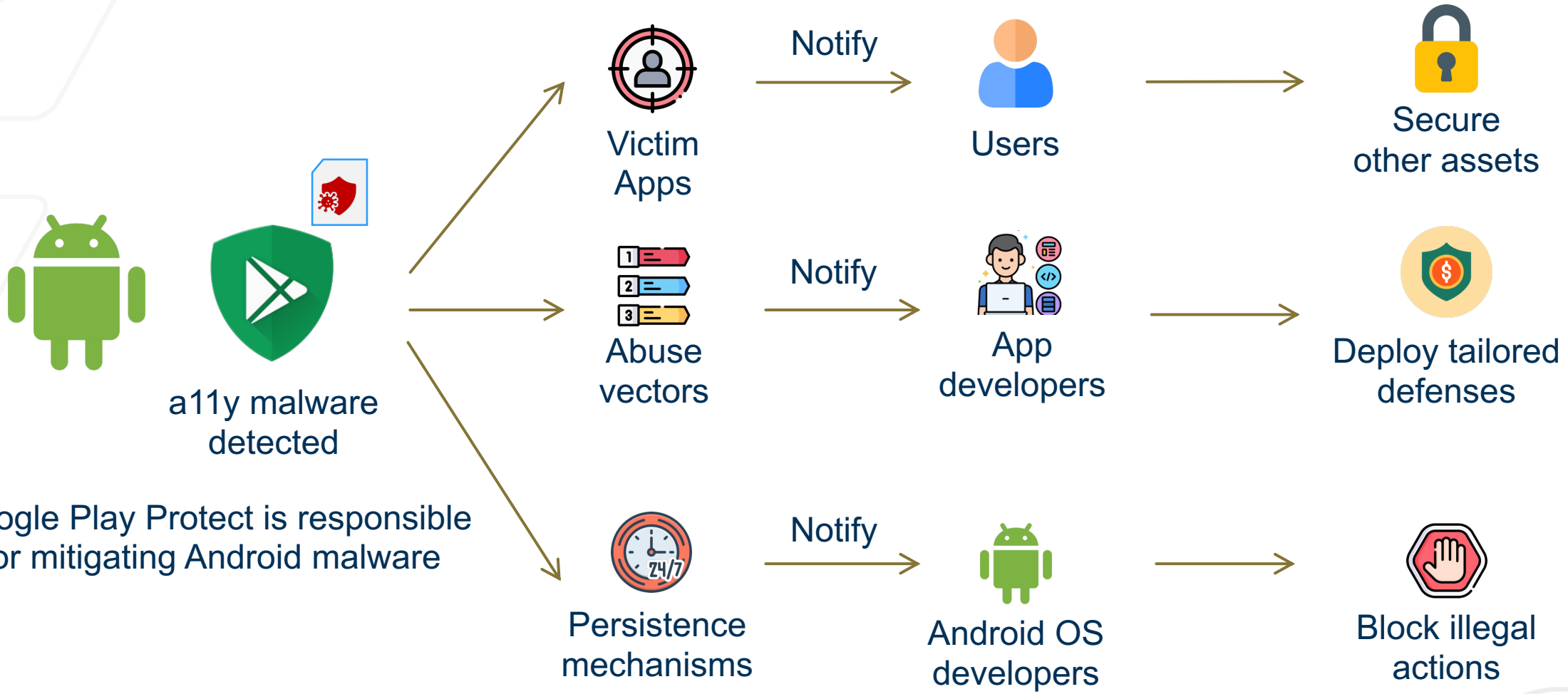
→ User clicks "OK"

→ "Grant accessibility permission to get cashback"

→ "Open Pag Bank for Synchronization"

Georgia Tech

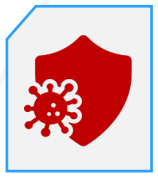
An Ideal Mitigation of Android a11y Malware



Google Play Protect is responsible for mitigating Android malware

Georgia Tech

Challenges to Mitigate Android a11y Malware



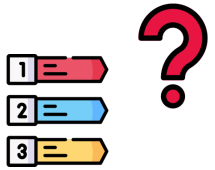
a11y malware

Encoded victim app search
(e.g., one-way hash)

Victim
Apps

Decoding impossible without victim environment

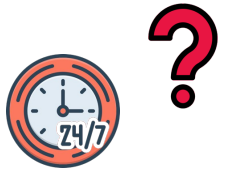
Dynamic abuse
code loading



Abuse
vectors

Absence of abuse code

Trigger-based
execution



Persistence
mechanisms

Incomplete extraction

Georgia Tech

Key Insight: a11y Abuse Is a Double-Edge Sword

Malware's usage of a11y APIs solves our challenges!

a11y malware do this:

This enables us to:

Eavesdrop victim apps → Simulate victim app actions → Reveal targeted victim apps

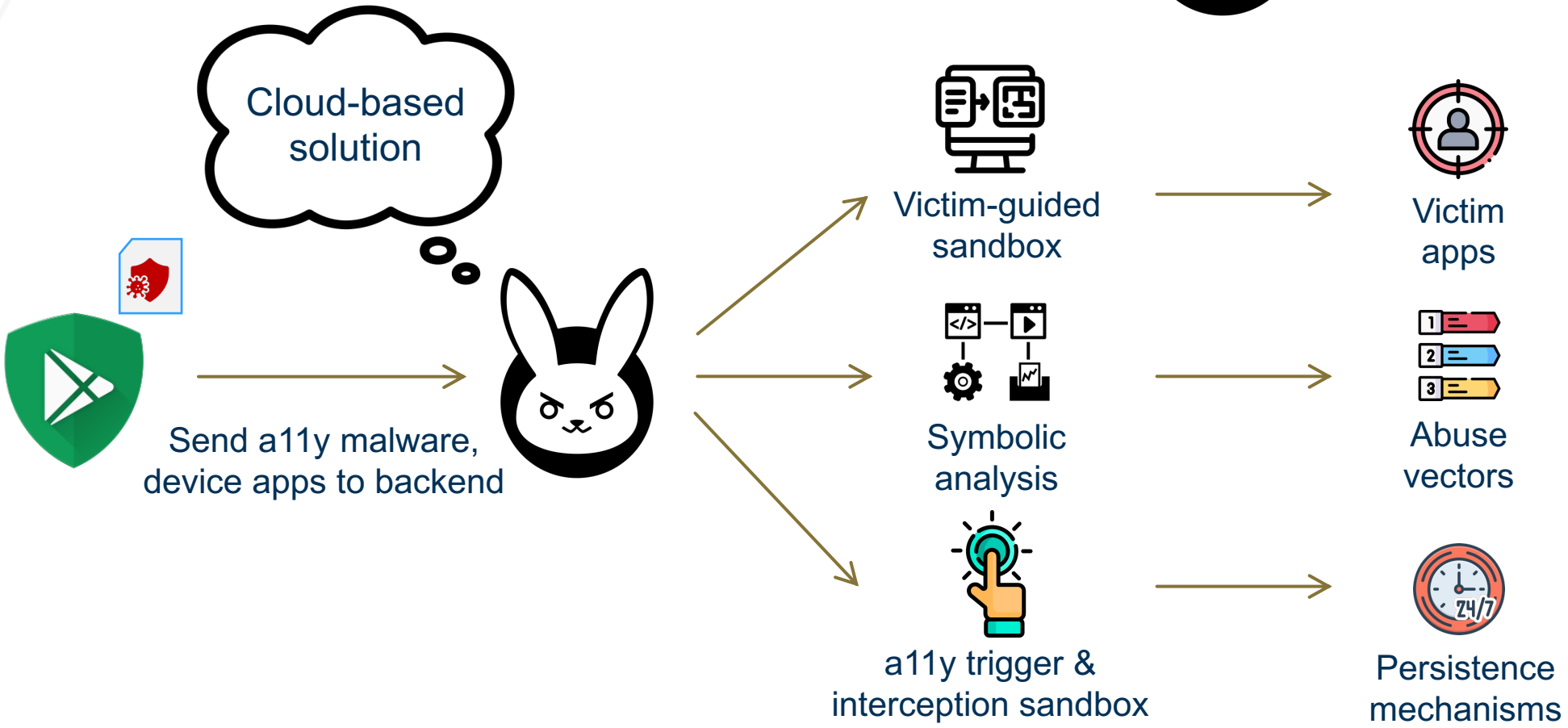
Conduct GUI actions → Symbolic analysis → Model abuse behaviors

Disrupt device control GUI → Trigger and intercept → Infer persistence mechanisms

Georgia Tech

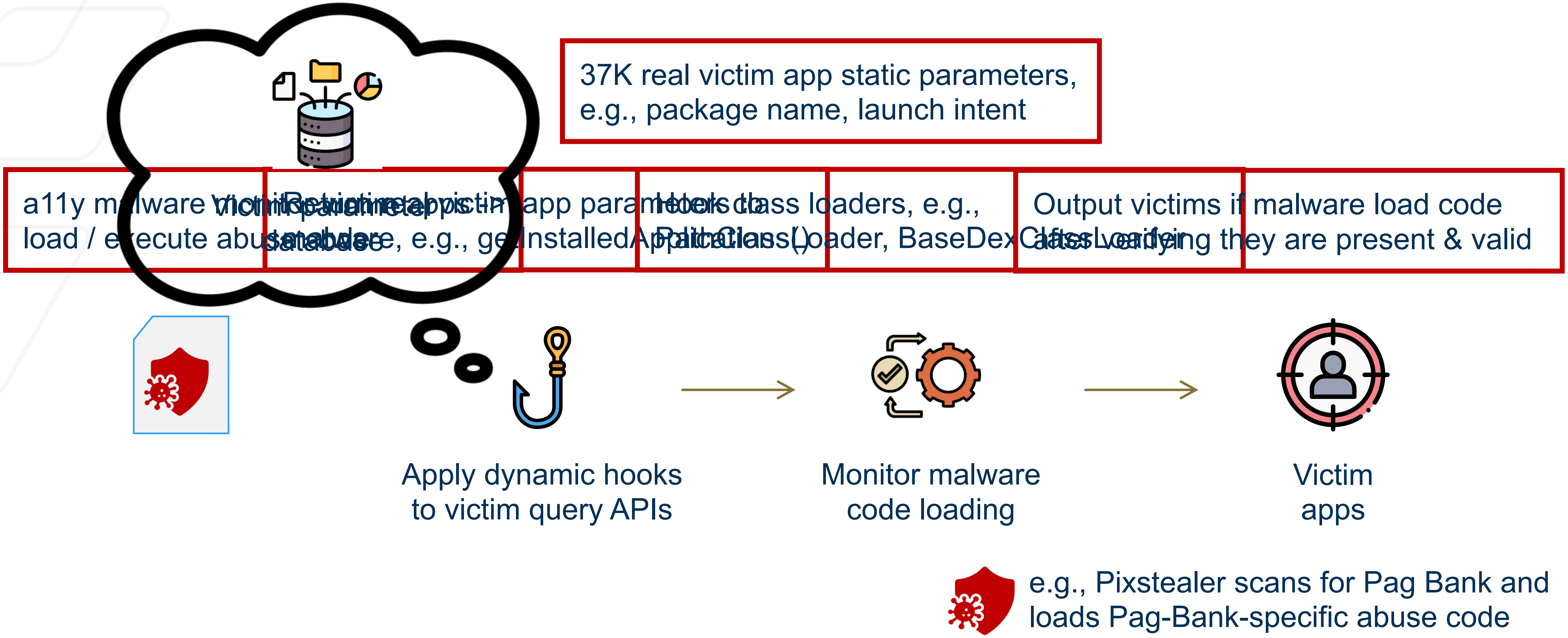
To Help Google Play Protect: Design Of DVa*

* **D**etector of **V**ictim-specific **a**11y Abuse



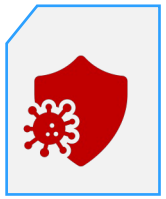
Georgia Tech

Component 1: Victim-Guided Sandbox



Component 1: Victim-Guided Sandbox

a11y malware queries victim apps conduct tailored a11y actions	Broadcast victim a11y events	WINDOW_STATE_CHANGED	Record malware's a11y actions to mimic victim app initiation	Output malware's a11y actions	Output victims if malware conduct GUI actions after seeing the a11y events	



Broadcast victim a11y events

Monitor malware GUI actions

Victim apps

e.g., Pixstealer targets Pag Bank because it use a11y to click “Show Balance” after Pag Bank starts

Georgia Tech

Component 2: Abuse-Vector-Guided Symbolic Analysis

Model API sequences, data-flows of real-world malware abuse vectors

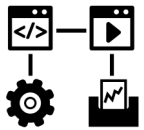
Abuse Vectors
Auto Transactions
Steal Credentials
Steal Authentication Codes
Manipulate Notifications
USSD Codes
Fake Calls
Ransom Screens

Conduct automated GUI actions, e.g., inject clicks, fill text

Log screens / eavesdrop text inputs

Confirm API sequence and data-flow, record execution context

Output malware's abuse vectors targeting each victim app



Symbolic analysis

Victim app attribution

Victim-specific abuse vectors

e.g., Pixstealer targets Pag Bank by conducting auto transactions and stealing credentials

Georgia Tech

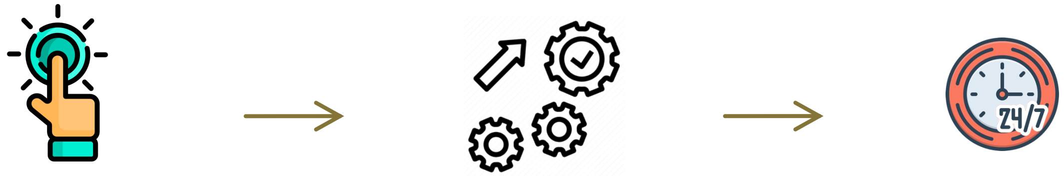
Component 3: a11y Trigger & Interception Sandbox

Model triggers and behaviors of real-world a11y persistence mechanisms

Return home whenever user enters device's app settings / Reinforce Google Play Protect in malware info screen

Send Intents to navigate to persistence mechanisms' trigger screens / Intercept malware actions, e.g., return to home screen / Check consistency: mechanisms if trigger and a11y behaviors match

Persistence Mechanisms
Disable Device Protections
Prevent Info Lookup/Uninstall
Prevent a11y Permission Revocation
Escalate Privileges
Uninstall Other Apps
Disable Power Options



Apply triggers → Capture a11y behaviors → Persistence mechanisms

e.g., Pixstealer persists by preventing users from revoking its granted a11y permission

Georgia Tech

Large-Scale Evaluation

Dataset:
- 9,850 a11y malware
- 197 malware families
- 37K victim app database

Run time:
DVa average run time 110s,
no frontend overhead

Netskope, cloud security solutions,
identify & mitigate malware threats

Seek to fortify their defenses
against mobile malware attacks

Large-Scale Evaluation

Dataset:
- 9,850 a11y malware
- 197 malware families
- 37K victim app database

Run time:
DVa average run time 110s, no frontend overhead

Findings:
- Most abused: steal credentials and automatic transactions
- 83% a11y malware target banking apps
- 70% a11y malware target authentication apps
- 74% victims are banking apps, 7% are cryptocurrency apps

Victim App Types	Top-2 Abuse Vectors	# Malware	# Family	# Victim
Banking	Steal Credentials Auto Transactions	3,579	55	159
Cryptocurrency	Steal Credentials Auto Transactions	1,130	23	16
Shopping	Steal Credentials Auto Transactions	257	5	13
Social Media	Auto Transactions Steal Credentials	539	17	11
Transportation	Steal Credentials Auto Transactions	45	2	6
Authentication	Steal Credentials Steal Notifications	3,022	52	5
Communication	Auto Transactions Steal Credentials	1,374	34	5
Total	--	4,291	65	215

Georgia Tech

Large-Scale Evaluation

DVa extracted:

- 7 categories of a11y-enabled persistence mechanisms
- 92% malware prevent users from uninstalling malware, revoking a11y permission

More intrusive behaviors are less observed:

- 19% malware prevent users from powering off / restarting device
- 2% malware escalate to admin privilege

Family	# Mal.	Disable Anti Virus	Prevent Uninstall	Prevent Perm. Rev.	Escal. Priv.	Admin	Uninstall Others	Disable Power
Spynote	1,421	1,278	1,397	1,378	1,281	0	1,071	0
Hqwar	1,400	1,291	1,270	1,306	1,183	0	989	1,277
Bianlian	545	523	539	521	0	0	0	0
Spymax	461	429	446	451	384	0	351	0
Anubis	449	413	443	443	0	0	278	0
Fakecalls	351	319	290	303	323	0	0	0
Cerberus	349	244	305	305	0	0	102	0
Androlua	298	278	242	238	256	0	108	0
Mobtes	245	214	227	219	0	0	210	220
Mobtool	212	168	188	194	0	0	0	0
Others	4,119	3,584	3,677	3,744	1,277	157	979	355
Total	**9,850**	**8,741**	**9,024**	**9,102**	**4,704**	**157**	**4,088**	**1,852**

Georgia Tech

Much More in the Paper!

- 2FA stealer analysis
- a11y ransomware analysis
- Victim app developers' proactive defense
- More highlights!

DVa: Extracting Victims and Abuse Vectors from Android Accessibility Malware

H. Xu, M. Yao, R. Zhang, M. M. Dawoud, J. Park, B. Saltaformaggio

USENIX Security, 2024

Many Thanks! netskope

Try DVa! @ https://github.com/CyFI-Lab-Public/DVa

Thank you!
Questions?

Haichuan (Ken) Xu
haichuanxu@gatech.edu
https://haichuanxuken.github.io

Georgia Tech Cyber Forensics Innovation Lab

Georgia Tech