No Privacy Among Spies:

Assessing the Functionality and Insecurity of Consumer Android Spyware Apps

Enze “Alex” Liu, Sumanth Rao, Sam Havron, Grant Ho,

Stefan Savage, Geoffrey M. Voelker, Damon McCoy

A real story of tech-enabled stalking

"He's tracking [everything]. Whatever I do, he sees that…"

(Survivor of Intimate Partner Violence)

Reference: Freed et al. Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. CSCW 2019

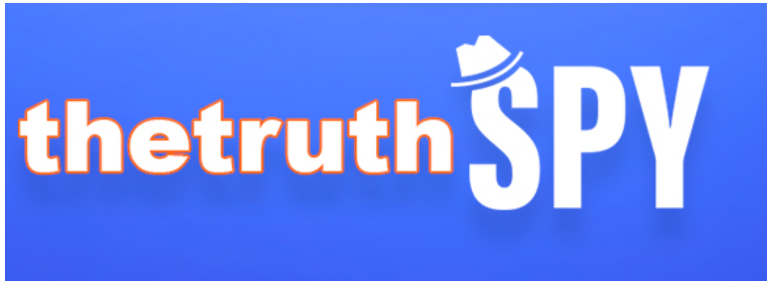
Tech-enabled stalking is on the rise

Hundreds of Apps Can Empower Stalkers to Track Their Victims

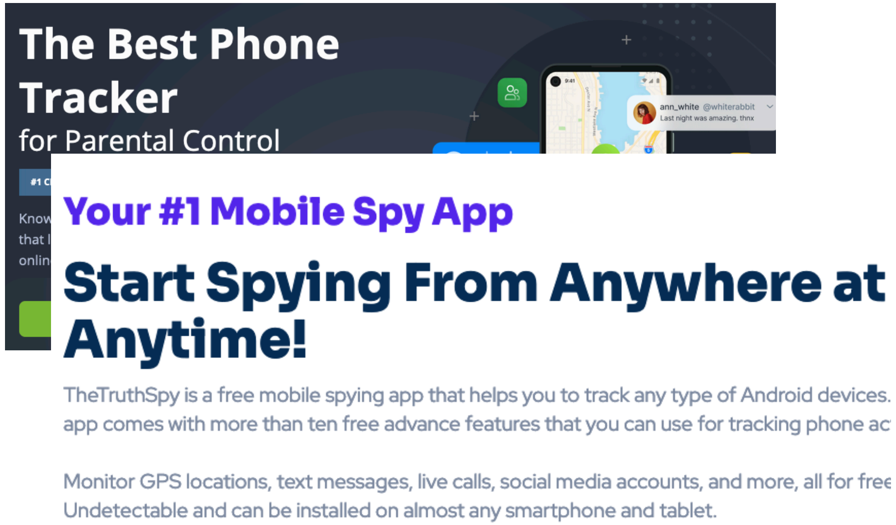
51% Increase in the Use of Online Spying and Stalking Apps During Lockdown

Consumer spyware apps

https://www.prnewswire.com/news-releases/51-increase-in-the-use-of-online-spying-and-stalking-apps-during-lockdown-301090012.html



Consumer spyware apps



The Best Phone Tracker
for Parental Control

#1 C

Know
that I
onlin

ann_white @whiterabbit
Last night was amazing. thnx

Your #1 Mobile Spy App

Start Spying From Anywhere at Anytime!

TheTruthSpy is a free mobile spying app that helps you to track any type of Android devices. app comes with more than ten free advance features that you can use for tracking phone ac

Monitor GPS locations, text messages, live calls, social media accounts, and more, all for free Undetectable and can be installed on almost any smartphone and tablet.

Sent / Received SMS

iMessage

Facebook Messenger

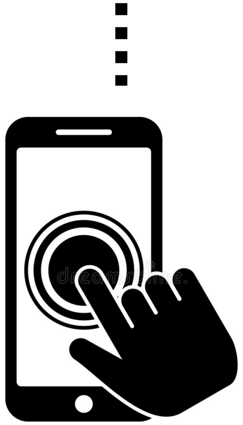
How?

Instagram

Snapchat

Android Keylogger

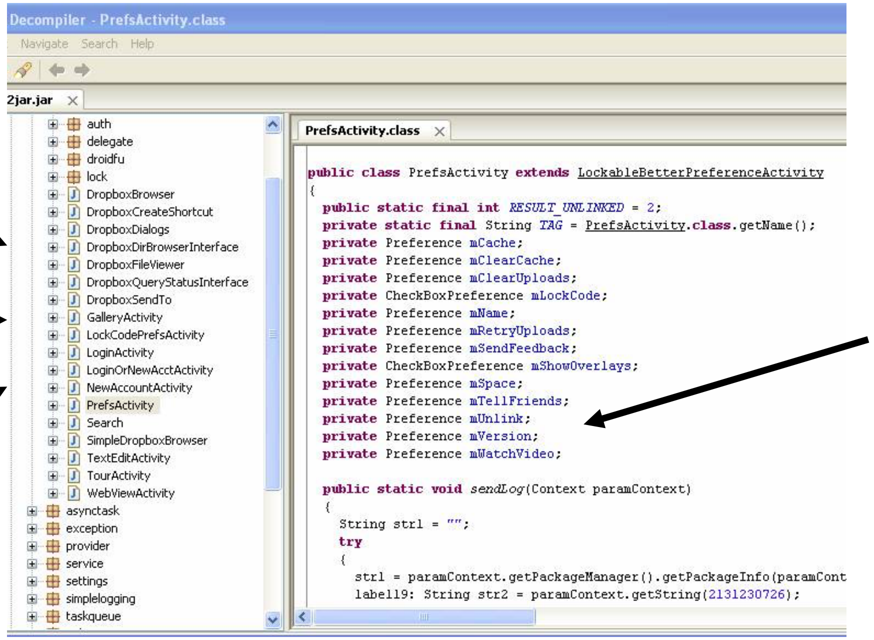
Download TheTruthSpy APK File



Methodology: reverse engineering

Decompilation

Source Files
(.apk files)



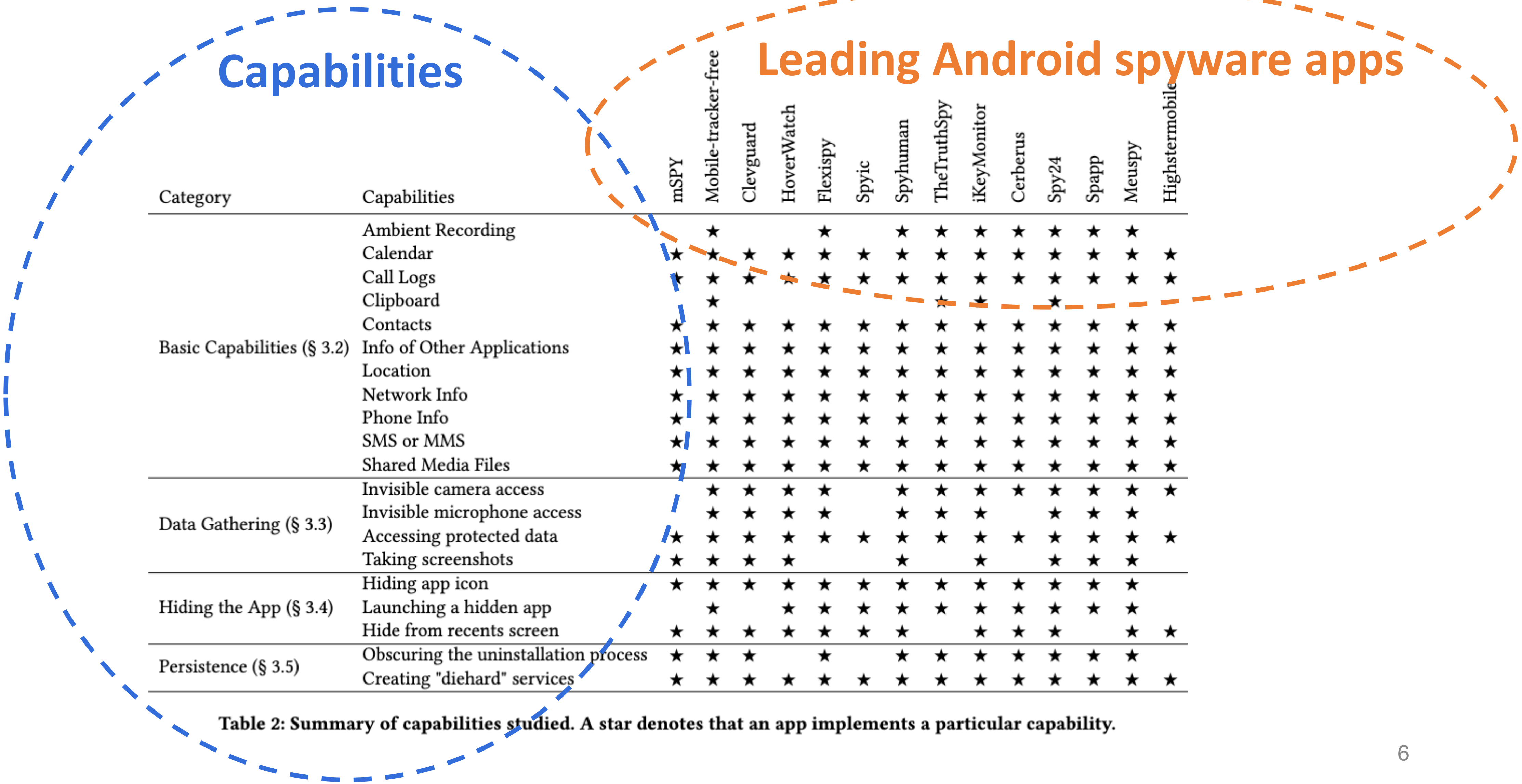
```
public class PrefsActivity extends LockableBetterPreferenceActivity
{
  public static final int RESULT_UNLINKED = 2;
  private static final String TAG = PrefsActivity.class.getName();
  private Preference mCache;
  private Preference mClearCache;
  private Preference mClearUploads;
  private CheckBoxPreference mLockCode;
  private Preference mName;
  private Preference mRetryUploads;
  private Preference mSendFeedback;
  private CheckBoxPreference mShowOverlays;
  private Preference mSpace;
  private Preference mTellFriends;
  private Preference mUnlink;
  private Preference mVersion;
  private Preference mWatchVideo;

  public static void sendLog(Context paramContext)
  {
    String str1 = "";
    try
    {
      str1 = paramContext.getPackageManager().getPackageInfo(paramCont
      label19: String str2 = paramContext.getString(2131230726);
```

Java Files

API Use

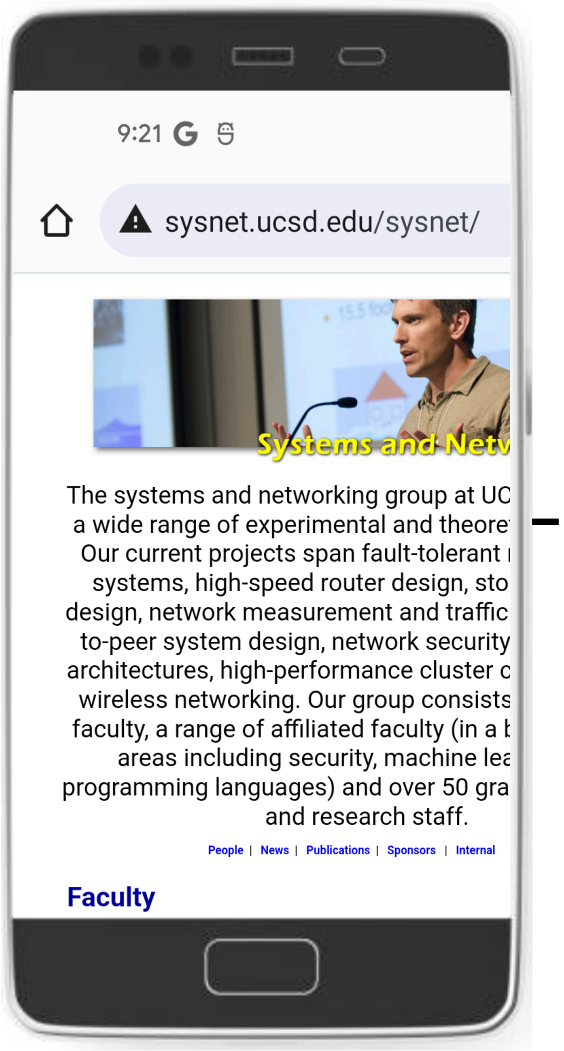
An in-depth analysis of technical capabilities


Capabilities
Leading Android spyware apps

Category	Capabilities	mSPY	Mobile-tracker-free	Clevguard	HoverWatch	Flexispy	Spyic	Spyhuman	TheTruthSpy	iKeyMonitor	Cerberus	Spy24	Spapp	Meuspy	Highstermobile
Basic Capabilities (§ 3.2)	Ambient Recording		★			★		★	★	★	★	★	★	★	
	Calendar	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Call Logs	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Clipboard		★						★	★		★			
	Contacts	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Info of Other Applications	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Location	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Network Info	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Phone Info	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	SMS or MMS	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Shared Media Files	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Data Gathering (§ 3.3)	Invisible camera access		★	★	★	★		★	★	★	★	★	★	★	★
	Invisible microphone access		★	★	★	★		★	★	★		★	★	★	
	Accessing protected data	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Taking screenshots	★	★	★	★			★		★		★	★	★	
Hiding the App (§ 3.4)	Hiding app icon	★	★	★	★	★	★	★	★	★	★	★	★	★	
	Launching a hidden app		★		★	★	★	★	★	★	★	★	★	★	
	Hide from recents screen	★	★	★	★	★	★	★		★	★	★		★	★
Persistence (§ 3.5)	Obscuring the uninstallation process	★	★	★		★		★	★	★	★	★	★	★	
	Creating "diehard" services	★	★	★	★	★	★	★	★	★	★	★	★	★	★

Table 2: Summary of capabilities studied. A star denotes that an app implements a particular capability.

Vignette #1: invisible camera access



9:21 G

sysnet.ucsd.edu/sysnet/

The systems and networking group at UC
a wide range of experimental and theore
Our current projects span fault-tolerant
systems, high-speed router design, sto
design, network measurement and traffic
to-peer system design, network security
architectures, high-performance cluster c
wireless networking. Our group consists
faculty, a range of affiliated faculty (in a b
areas including security, machine lea
programming languages) and over 50 gra
and research staff.

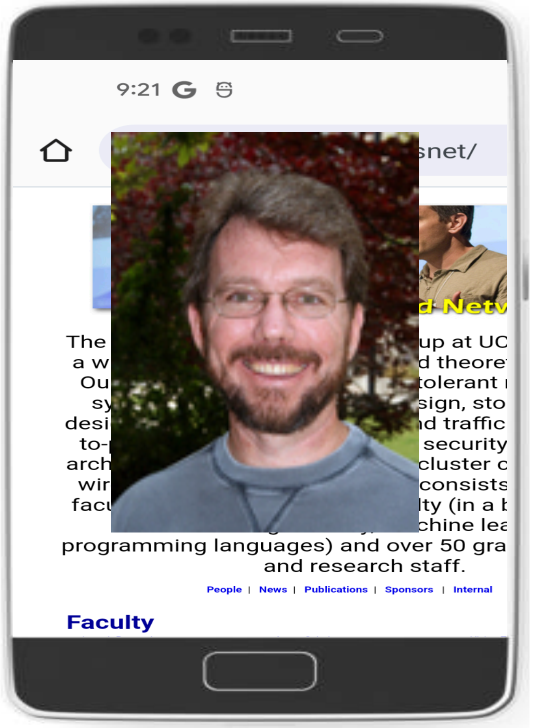
People | News | Publications | Sponsors | Internal

Faculty

Vignette #1: invisible camera access – via 1x1 preview

Normal app:

* Show a preview to the user



9:21

snet/

d Netv

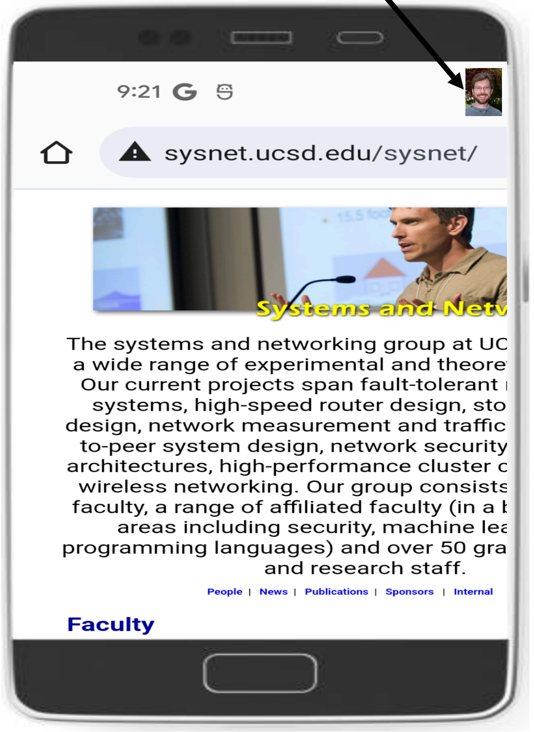
The up at UC
a w d theore
Ou tolerant
sy sign, sto
desi d traffic
to- security
arch cluster c
wir consists
fac ty (in a b
chine lea
programming languages) and over 50 gra
and research staff.

People | News | Publications | Sponsors | Internal

Faculty

Spyware app:

* A preview of size 1x1 (invisible)!



9:21

sysnet.ucsd.edu/sysnet/

Systems and Netv

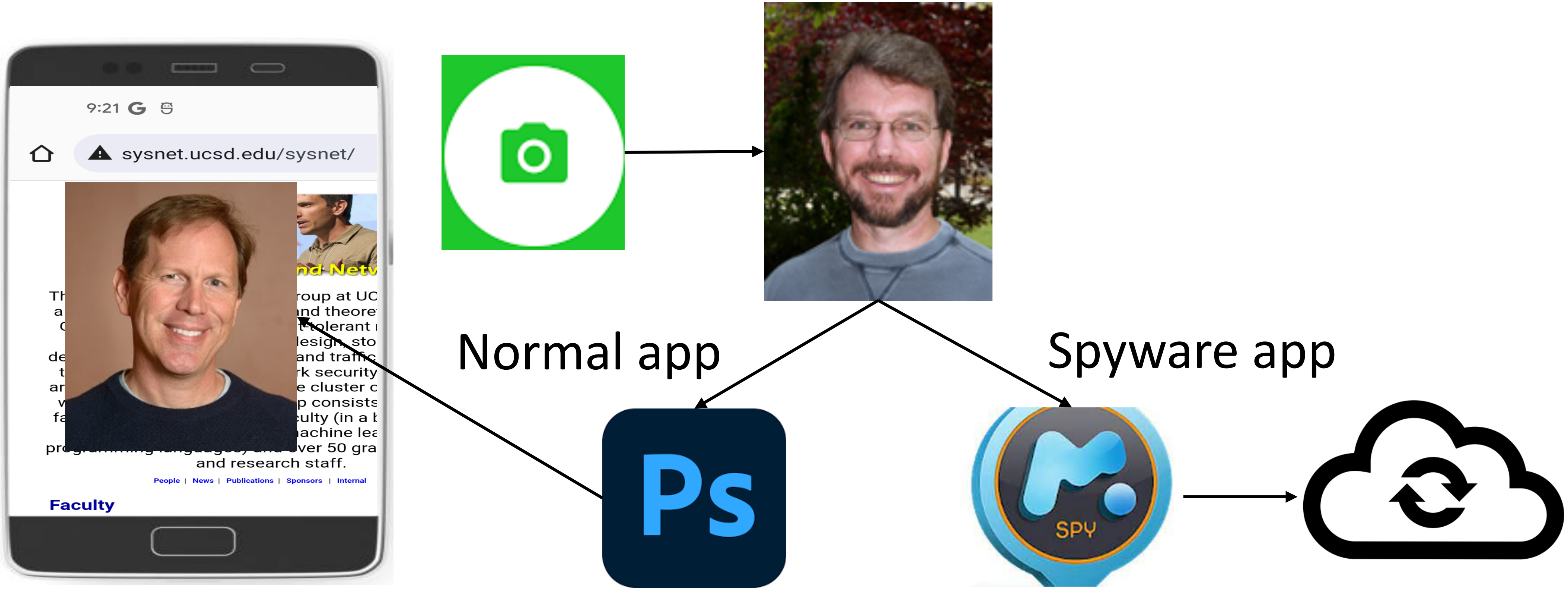
The systems and networking group at UC
a wide range of experimental and theore
Our current projects span fault-tolerant
systems, high-speed router design, sto
design, network measurement and traffic
to-peer system design, network security
architectures, high-performance cluster c
wireless networking. Our group consists
faculty, a range of affiliated faculty (in a b
areas including security, machine lea
programming languages) and over 50 gra
and research staff.

People | News | Publications | Sponsors | Internal

Faculty

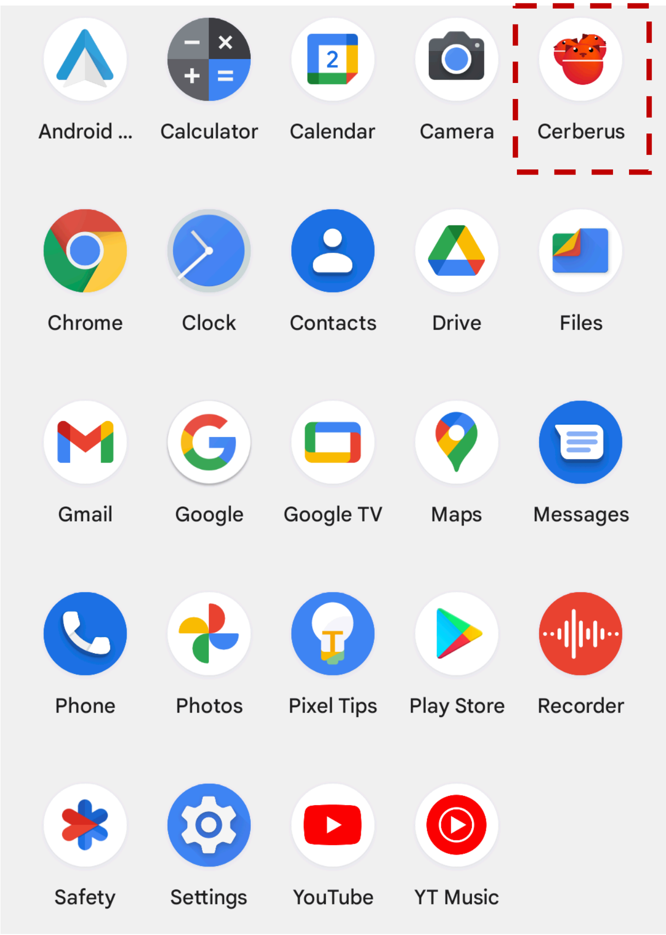
Vignette #1: invisible camera access - via raw frames

- Apps can capture raw frames from the camera

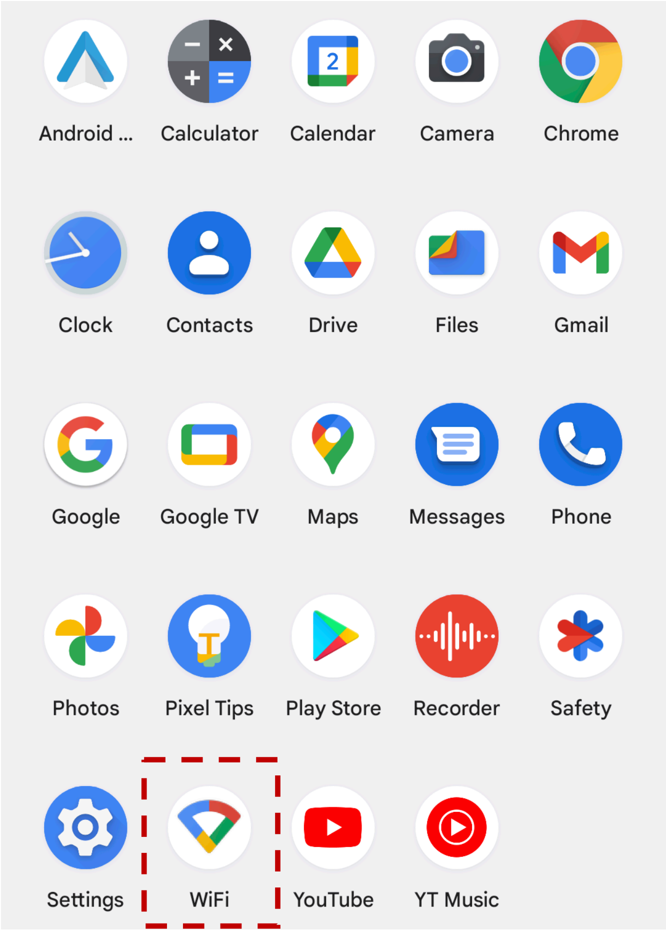


Vignette #2: hiding app icons

Pre-setup:



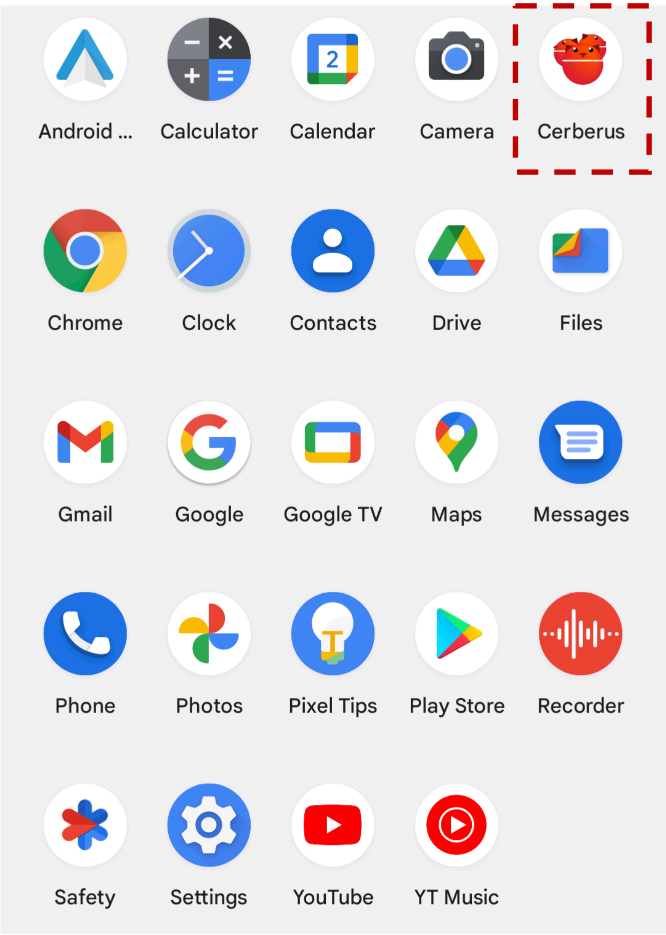
Post:



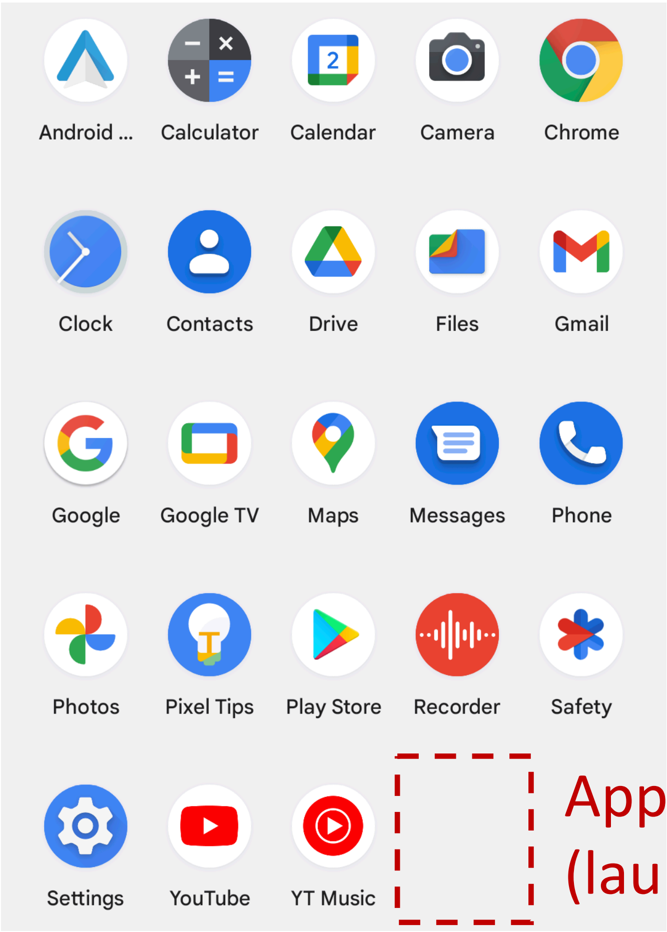
Innocuous Icon

Vignette #2: hiding app icons

Pre-setup:



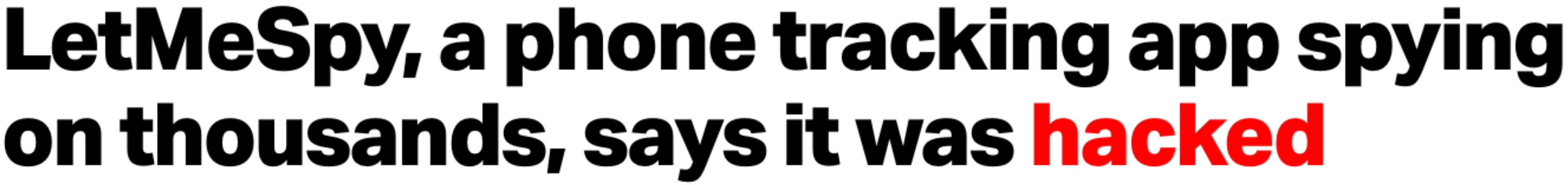
Post:



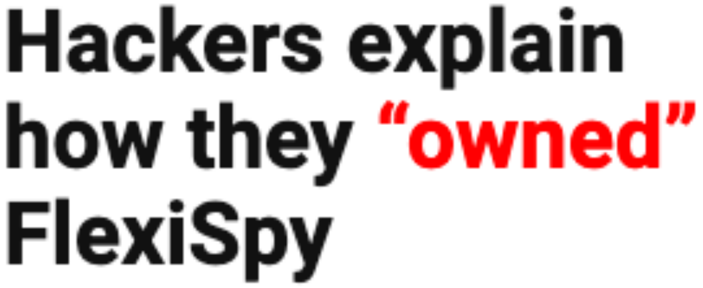
App w/ no icon
(launcher activity)

Takeaway: spyware apps are technically sophisticated

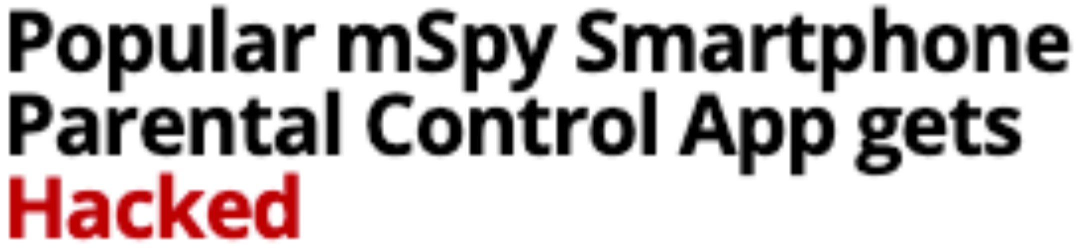
But ironically, they are not very secure



LetMeSpy, a phone tracking app spying on thousands, says it was hacked



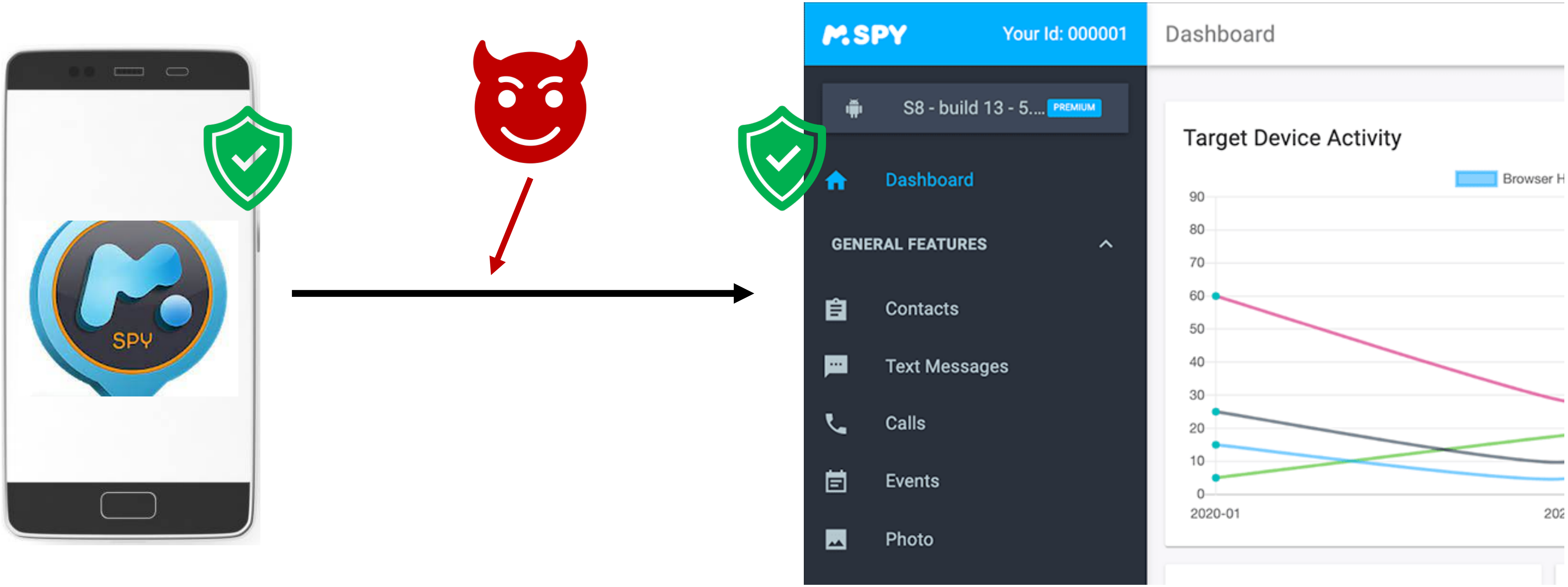
Hackers explain how they "owned" FlexiSpy



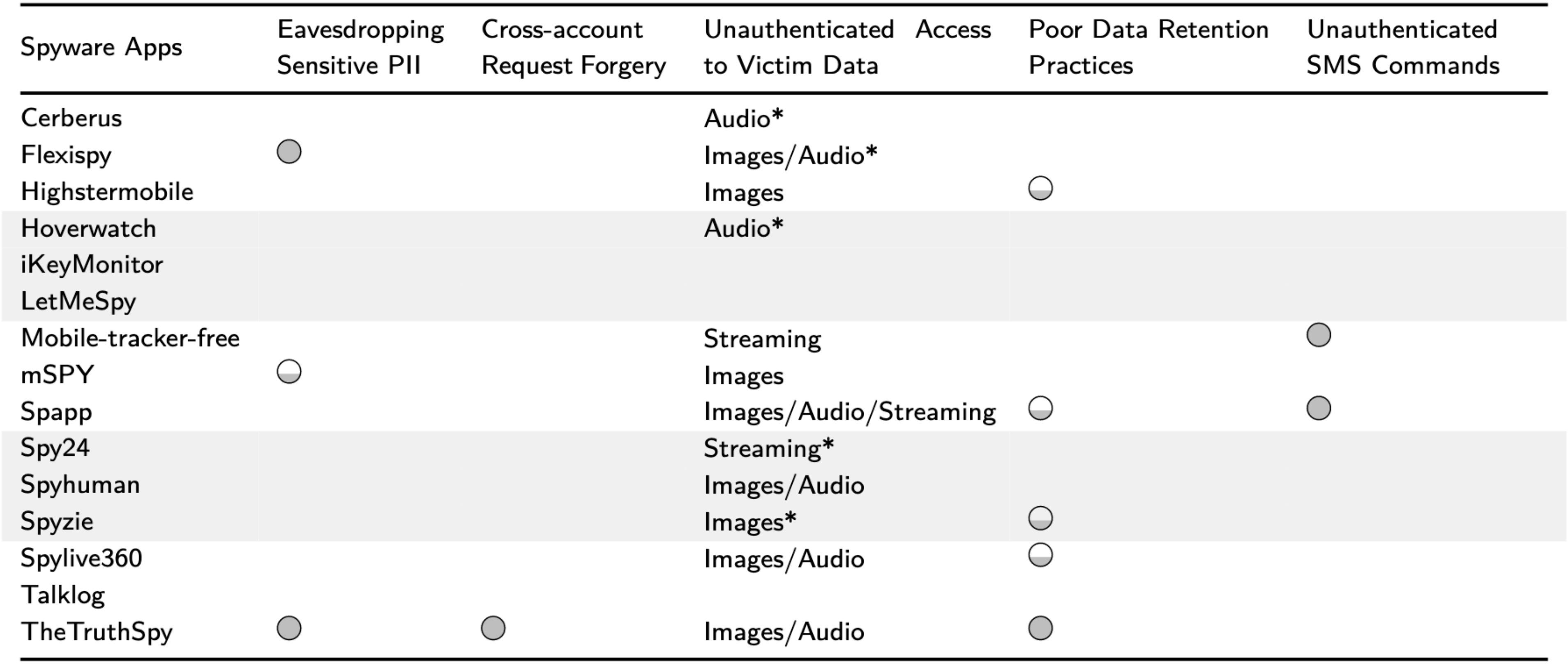
Popular mSpy Smartphone Parental Control App gets Hacked

What are the measures taken by spyware apps to protect user data?

Methodology: an end-to-end approach



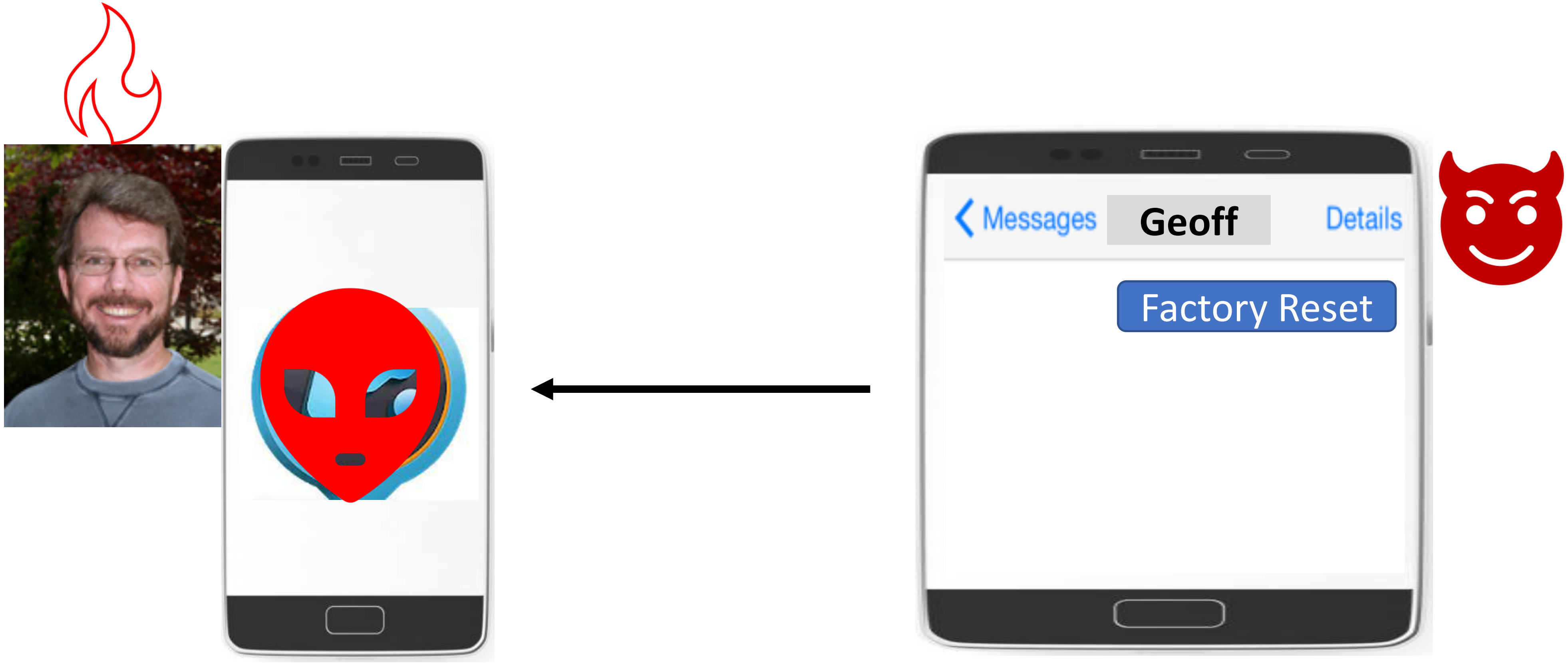
Results: a range of privacy deficiencies



Spyware Apps	Eavesdropping Sensitive PII	Cross-account Request Forgery	Unauthenticated Access to Victim Data	Poor Data Retention Practices	Unauthenticated SMS Commands
Cerberus			Audio*		
Flexispy	●		Images/Audio*		
Highstermobile			Images	◒	
Hoverwatch			Audio*		
iKeyMonitor					
LetMeSpy					
Mobile-tracker-free			Streaming		●
mSPY	◒		Images		
Spapp			Images/Audio/Streaming	◒	●
Spy24			Streaming*		
Spyhuman			Images/Audio		
Spyzie			Images*	◒	
Spylive360			Images/Audio	◒	
Talklog					
TheTruthSpy	●	●	Images/Audio	●	

Table 3. Systematization of commodity spyware vulnerabilities. (Circles denote the severity level of the insecurity. ◒ indicates at least one instance of the insecurity; ● indicates all app functionality is insecure; * indicates URLs are temporary and expire.)

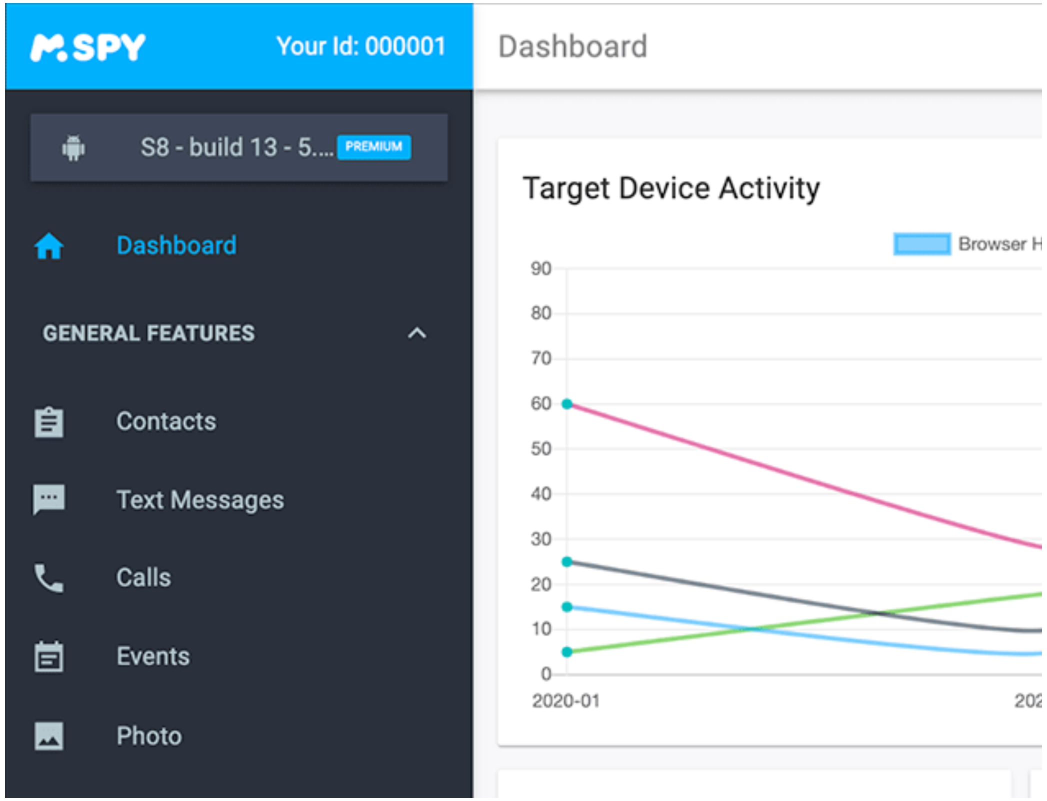
Vignette #1: unauthenticated SMS commands



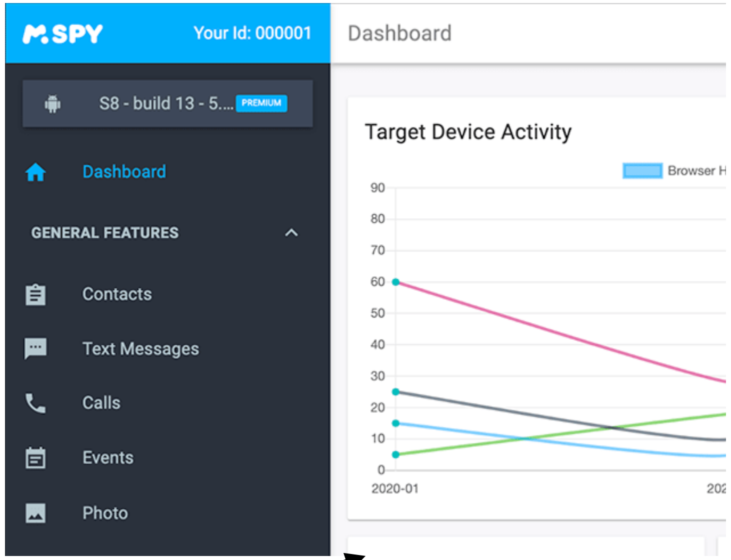
Factory Reset

Vignette #2: transmitting data in plaintext

Username: victim@gmail.com
Password: xxxxxxx
Called Alice at midnight

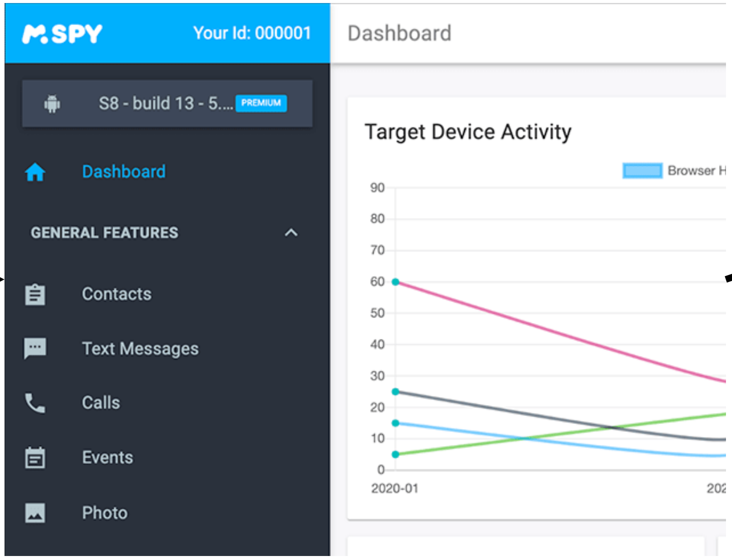


Vignette #3: cross-account request forgery



Your Id: 000001

Create an account



Your Id: 000001

Replacing the attacker’s account id with the victim’s account id

Takeaway: no enough effort in securing sensitive user data

Disclosed to all vendors yet received no response ☹

Summary

- Contribution #1: in-depth analysis of consumer Android spyware apps
  - Studied the spying capabilities of 14 leading spyware apps
  - Documented the creative ways of using APIs
  - Including previously unknown approaches
- Contribution #2: security analysis on user data protection
  - Identified a range of privacy deficiencies

✉ e7liu@ucsd.edu

💻 e7liu.github.io