No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps

Enze "Alex" Liu, **Sumanth Rao**, Sam Havron [1], Grant Ho , Stefan Savage , Geoffrey M. Voelker, and Damon McCoy [2]

UC San Diego [1]*Cornell Tech* [2]*New York University*

What are Spyware Apps?

Consumer mobile spyware apps enable abusers to tap victims' phones and stealthily monitor user activities (i.e., phone calls, camera, location, images, e-mail, etc). They are marketed to the general public and used for nefarious means (e.g., cyberstalking). Some characteristics include :

- Transmit collected information over the internet.
- Easy installation and no technical expertise needed.
- Often have poor security hygiene (many incidents)

Figure 1:Potpourri of spyware vendors

Research Questions

- **How do spyware apps achieve their core functionalities?** (e.g., taking pictures without being noticed)
- **What security measures do spyware apps have to protect the sensitive data they collect?**

Key Contributions

- Performed an in-depth technical analysis of the 14 most popular spyware apps targeting Android phones.
- Document how spyware apps achieve their core functionalities through the creative abuse of Android APIs.
- Document the security measures spyware apps have to protect sensitive user data collected.

Results - Spyware Technical Capabilities

Data Gathering: Stealthily collect victim information without being noticed (e.g., covertly access the camera/microphone).

Hiding the App: Keep the existence of the app hidden from the victims (e.g., hiding from Android app launcher, recent app's list).

Persistence: Obscuring the app uninstallation process and restarting even when forcibly stopped.

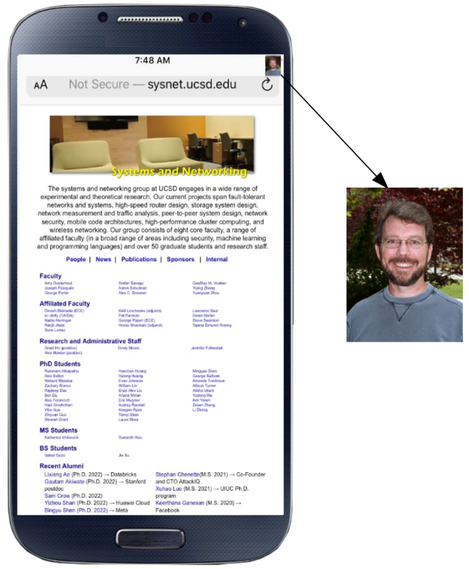

Figure 2:Taking picture without being noticed (through 1x1)

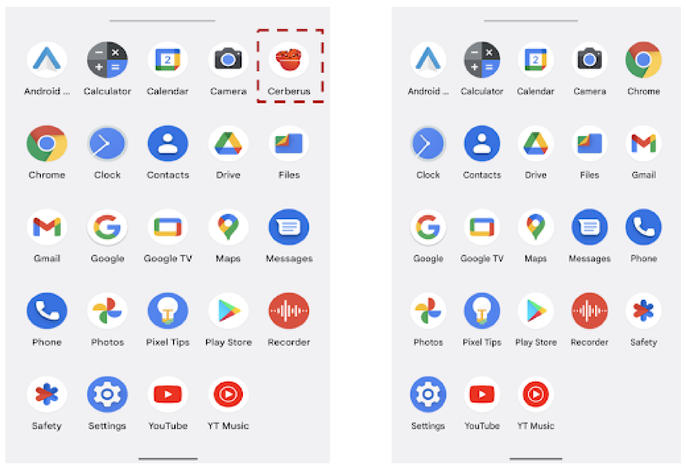

Figure 3:Hiding app icon (through manifest)

Results - Poor Data Hygiene

4/14 (28%) of the spyware apps transmit sensitive user data in plaintext (e.g., usernames, passwords, text messages, call history).

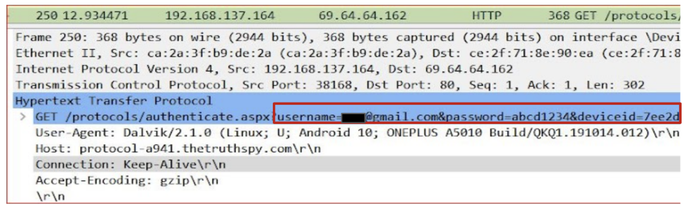

Figure 4: *TheTruthSpy* app leaking user credentials

6/14 (43%) of the apps store their data in public URLs accessible by anyone (e.g., images, audio, videos collected from device).

2/14 (14%) apps execute remote commands initiated by anyone (e.g., locating device, remote wiping).

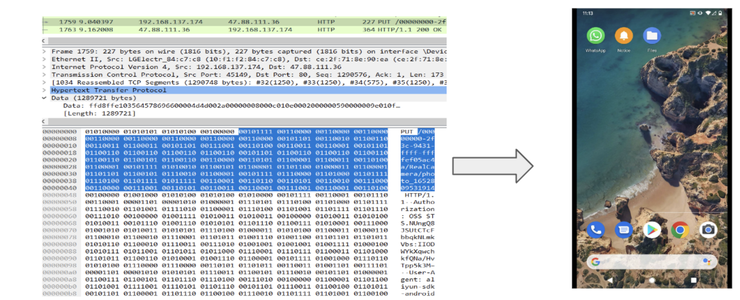

Figure 5:Raw packet data from *Clevguard* app used to reconstruct image

Conclusion

- Creative abuses of Android APIs (e.g., the Accessibility API) exploit the Android threat model.
- The privacy deficiencies we uncover convey the hard truth: these apps prioritize business over protecting user data.
- Highlights the need for a more creative, diverse, and comprehensive set of interventions from industry, government, and the research community.