Detecting iPhone Security Compromise in Simulated Stalking Scenarios: Strategies and Obstacles

Andrea Gallardo, Hanseul Kim, Tianying Li
Lujo Bauer, Lorrie Cranor
Widespread Problems: Intimate partner violence & Stalking

- 1 in 3 women 15-49 years old, who have ever been in romantic relationship, experience intimate partner violence (IPV)*

- Digital technologies increasingly used to spy on, stalk, and harass intimate partners and stalking victims

Spyware & stalkerware are profitable apps…

Excellent Tracking 🌟🌟🌟🌟🌟
06/17/2022
Excellent. They did a great job giving me access to my husband's phone after three kids I never thought he'd have any reason to cheat on me but I was totally wrong. He suddenly...

Wouldn't Recommend It
08/30/2017
Downloaded this on my wife’s iPhone 7. At 1st I downloaded the lite version which was ok for gps, but that's about it, paid around $10 for the app.
... but legitimate apps can be used for stalking

Location Tracking

iCloud Account
How to help detect compromises?

4 simulated stalking scenarios

  Location sharing

  Suspected spyware

  iCloud compromise

  Jailbreak detection
How to help detect compromises?

4 simulated stalking scenarios

- Location sharing
- Suspected spyware
- iCloud compromise
- Jailbreak detection

18 remote semi-structured interviews with participants acting as friends or coworkers
**Challenge:** Could you guide us through how you would confirm whether someone is tracking your coworker’s location?
Scenario 1: Location sharing

Results: Most participants knew to search Location Services and that Google Maps was using the device’s location, but…
Challenge: Could you guide us through how you would confirm whether someone is tracking your coworker’s location?

Results: Most participants knew to search Location Services and that Google Maps was using the device’s location, but…

… no one searched within the Google Maps app.
Scenario 1: Location sharing

“It was just too much **jumping around** …”
Scenario 1: Location sharing

“It was just too much jumping around …”

“To go in the app itself, not just the iPhone, but the app settings, that’s tricky, so I had a little bit of issue to find that, but I mean, it was all there.”
Scenario 3: iCloud compromise

Challenge: Photos and iMessages are disappearing, and new ones are appearing.

What are some steps you could take to figure out whether someone can see your friend’s photos and messages?
Scenario 3: iCloud compromise

Results: 50% of participants could not find the iCloud devices list
Scenario 3: iCloud compromise

Results: 50% of participants could not find the iCloud devices list
Results: 50% of participants could not find the iCloud devices list

“I think I knew generally to look under iCloud, but I just didn’t know the full screen.”
Scenario 3: iCloud compromise

**Results:** Most participants found it easy to remove from account
How to help detect compromises?

4 simulated stalking scenarios

- Location sharing
- Suspected spyware
- iCloud compromise
- Jailbreak detection
Location sharing recommendation: Make it clear that location is being shared with another user

- Provide users with persistent, immediate indicators for transmitting location to another user

  - Google’s developer policy:

Stalkerware

Code that collects and/or transmits personal or sensitive user data from a device without adequate notice or consent and doesn't display a persistent notification that this is happening.
Location sharing recommendation: Make it clear that location is being shared with another user

▸ Provide users with persistent, immediate indicators for transmitting location to another user

▸ Generate less predictable notifications for an abuser

▸ Require authentication to users to start sharing with someone
Cloud access recommendation: Let users know who / what devices can access their cloud account

- Add indicators of devices in settings
- Make list of devices more immediately visible
“Detecting iPhone Security Compromise in Simulated Stalking Scenarios: Strategies and Obstacles”

- Difficult to detect when iPhone was transmitting information
  - Inability to locate relevant options
  - Lack of immediately visible indicators
- IPV and stalking threat model needs to be considered in design

Andy Gallardo agallar2@andrew.cmu.edu,
Hanseul Kim hanseulkim96@gmail.com,
Tianying Li, Lujo Bauer, Lorrie Cranor