The Spyware Used in Intimate Partner Violence

Rahul Chatterjee, Periwickel Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, Thomas Ristenpart
Paper Overview

• The first in-depth measurement study of the Intimate Partner Surveillance (IPS) spyware ecosystem

• Contributions:
  • Documented IPS-relevant resources via query snowballing
  • Highlighted the role of dual-use apps
  • Investigated developer complicity
  • Showed that existing anti-spyware tools are ineffective

• Conclusion: “there is acute need for the security community to help mitigate the threat”
Background
IPV, IPS, and Spyware

• “Intimate partner violence (IPV) affects roughly one-third of all women and one-sixth of all men in the United States.”

• Key tool in IPS is spyware installed on a survivor’s phone
  • Two types:
    • Overt spyware directly marketed for covert monitoring
    • Dual-use apps designed for legitimate functions but repurposed for IPS

• (Ab)users exploit both to monitor and exert control over their intimate partners, which leads to IPV
Similarities and Differences between an (ab)user and advanced persistent threat

**Similarities**
- Reliance on niche technology
- Commercial-grade, off-the-shelf
- Both seek to exert control/intimidate

**Differences**
- Personal motives
- Physically close to mobile device, probably have access to some extent
- Organization vs individual effort
- APTs can be extremely sophisticated
- Abusers aren’t necessarily sophisticated
- Personal connection and trust
Similarities and differences between a survivor of IPS/IPV and victim of a nation-state attack

**Similarities**
- May never be aware they are targeted
- Both face intimidation/physical harm
- Defenseless

**Differences**
- Personal connection and trust
- With IPV you can get legal intervention
- More mental trauma
- More expensive to recover from a nation-state attack
- IPS-relevant apps have legitimate uses
- Nation-state attacks may have geopolitical consequences
Methodology
Query Snowballing

• Procedure:
  1. Query the recommendation API on all queries in the seed set
  2. Collect the resulting recommendations
  3. Query the new search terms
  4. Repeat until predetermined number of queries reached or until no new recommendations are found

\[
\text{QSNowball}(Q_{\text{init}}, \ell) : \\
Q \leftarrow \emptyset \\
\text{while } |Q_{\text{init}}| > 0 \text{ do} \\
q \leftarrow \text{pop}(Q_{\text{init}}) ; Q \leftarrow Q \cup \{q\} \\
\text{if } |Q| \geq \ell \text{ then return } Q \\
Y \leftarrow \text{recommend}(q) \\
Y' \leftarrow \text{filter}(Y) \setminus Q \\
Q_{\text{init}} \leftarrow Q_{\text{init}} \cup Y' \\
\text{return } Q
\]
Strengths and Limitations of Query Snowballing

**Strengths**
- Explore the unknown
- Simulates how abusers might find IPS apps
- High threshold ensured queries would converge
- Fairly representative

**Limitations**
- May have missed queries
- Dependent on seed set; don’t know how they chose terms
- Focused on English
- Dependent on play store and google search algorithms
Result (a)

Size of Google Play recommendation snowballs each day and size of cumulative set of distinct queries

Total: 675 queries
Result (b)

Number of distinct apps found each day and cumulative number of apps found over time

Total: 9,224 apps
Pruning

• Used a supervised machine learning algorithm (logistic regression) to prune false positives

• Achieved 93% accuracy across both test sets with a 6% false negative rate

• Achieved 0% false negative rate with threshold of 0.3 (setting up potential use as a detection tool)

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Accuracy</th>
<th>TR</th>
<th>TS₁</th>
<th>TS₂</th>
<th>TS₁+₂</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.5</td>
<td>FNR</td>
<td>4</td>
<td>4</td>
<td>11</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>FPR</td>
<td>4</td>
<td>11</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>0.3</td>
<td>FNR</td>
<td>&lt; 1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>FPR</td>
<td>19</td>
<td>25</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>

Fig. 4: Performance (in percent) of LR classifier on training and different test sets for two classification thresholds.
IPS-relevant apps and typical capabilities

<table>
<thead>
<tr>
<th>App types</th>
<th>Description</th>
<th>Examples</th>
<th>Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal tracking</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Find-my-phone</td>
<td>Locate phone remotely</td>
<td>Find my Android</td>
<td>Location tracking, remote locking and wiping</td>
</tr>
<tr>
<td>Anti-theft</td>
<td>Catch the phone thief</td>
<td>Wheres My Droid</td>
<td>Record location, photos &amp; ambient audio; alert on SIM change</td>
</tr>
<tr>
<td>Call recorder</td>
<td>Record incoming / outgoing calls</td>
<td>Call Recorder</td>
<td>Record calls and back them up to a server</td>
</tr>
<tr>
<td>Data syncing</td>
<td>Sync data from phone to other device</td>
<td>mySMS</td>
<td>Sync SMS and call log, media, browser history</td>
</tr>
<tr>
<td>Phone control</td>
<td>Control phone remotely</td>
<td>TrackView</td>
<td>Full control with capabilities exceeding combination of data syncing and anti-theft</td>
</tr>
<tr>
<td><strong>Mutual tracking</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Family tracking</td>
<td>Track location of family members</td>
<td>Family Tracker</td>
<td>Mutual location sharing</td>
</tr>
<tr>
<td>Couple tracking</td>
<td>Consensual sharing of location and more</td>
<td>Couple Tracker</td>
<td>Syncs location, media content, SMS and call logs</td>
</tr>
<tr>
<td>Friends tracking</td>
<td>Track friends if they are in vicinity</td>
<td>Friends Tracker</td>
<td>Like family tracker, and alerts if friend in vicinity</td>
</tr>
<tr>
<td><strong>Subordinate tracking</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employee tracking</td>
<td>Track employees whereabouts</td>
<td>Where’s my Staff</td>
<td>Similar to anti-theft</td>
</tr>
<tr>
<td>Parental control</td>
<td>For parents to monitor their children</td>
<td>MMGuardian</td>
<td>Capabilities very similar to phone control</td>
</tr>
<tr>
<td>Overt spyware</td>
<td>Claims to be spying app</td>
<td>Cerberus, mSpy, HelloSpy</td>
<td>Surrupitious phone monitoring &amp; control</td>
</tr>
</tbody>
</table>

Fig. 5: Different categories of IPS-relevant apps and their typical capabilities.
Developer Complicity

• User Comments:
  • “Love it!!! I’ve been suspecting my gf cheating and this gave me answers really quick kick the curb girl”

• Advertising:
  • “Don’t Be A Sucker Track Your Girlfriend’s iPhone Now: Get It Here: Catch Her Today”

• Customer Support:
  • “Hi, If I use this app to track my husband will he know that I am tracking him? Thanks, Jessie”
Inefficacy of Existing Anti-Spyware

- Identified 147 apps with 50,000+ downloads; found only 40 of them relevant to removing spyware
- Of the 40 relevant apps, 37 were completely ineffective against dual-use apps!!!

<table>
<thead>
<tr>
<th>Anti-spyware tool</th>
<th>D/L (mn)</th>
<th>On-store (276)</th>
<th>Off-store (20)</th>
<th>Benign (100)</th>
</tr>
</thead>
<tbody>
<tr>
<td>360 Security</td>
<td>100</td>
<td>2</td>
<td>80</td>
<td>0</td>
</tr>
<tr>
<td>Anti-virus Dr.Web</td>
<td>100</td>
<td>2</td>
<td>70</td>
<td>0</td>
</tr>
<tr>
<td>Avast Mobile Security 1</td>
<td>100</td>
<td>2</td>
<td>70</td>
<td>0</td>
</tr>
<tr>
<td>AVG Antivirus1,2</td>
<td>100</td>
<td>2</td>
<td>70</td>
<td>0</td>
</tr>
<tr>
<td>DFNDR Security</td>
<td>100</td>
<td>2</td>
<td>85</td>
<td>0</td>
</tr>
<tr>
<td>Lookout Security</td>
<td>100</td>
<td>3</td>
<td>75</td>
<td>0</td>
</tr>
<tr>
<td>ALYac</td>
<td>10</td>
<td>2</td>
<td>70</td>
<td>0</td>
</tr>
<tr>
<td>Antivirus (TrustGo)</td>
<td>10</td>
<td>2</td>
<td>80</td>
<td>0</td>
</tr>
<tr>
<td>Antivirus (TrustLook)</td>
<td>10</td>
<td>2</td>
<td>70</td>
<td>0</td>
</tr>
<tr>
<td>Avira1</td>
<td>10</td>
<td>3</td>
<td>60</td>
<td>0</td>
</tr>
<tr>
<td>Kaspersky1</td>
<td>10</td>
<td>1</td>
<td>85</td>
<td>0</td>
</tr>
<tr>
<td>Malwarebytes2</td>
<td>10</td>
<td>3</td>
<td>85</td>
<td>0</td>
</tr>
<tr>
<td>McAfee Mobile1,2</td>
<td>10</td>
<td>2</td>
<td>90</td>
<td>0</td>
</tr>
<tr>
<td>ESET1</td>
<td>10</td>
<td>1</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>Norton Mobile1,2</td>
<td>10</td>
<td>13</td>
<td>70</td>
<td>2</td>
</tr>
<tr>
<td>Virus Cleaner2</td>
<td>10</td>
<td>2</td>
<td>75</td>
<td>0</td>
</tr>
<tr>
<td>Anti Spy Mobile2</td>
<td>1</td>
<td>47</td>
<td>95</td>
<td>12</td>
</tr>
<tr>
<td>Incognito2</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Anti Spy (skibapps)2</td>
<td>&lt; 1</td>
<td>36</td>
<td>73</td>
<td>10</td>
</tr>
<tr>
<td>Others (average over 21 apps)</td>
<td>1</td>
<td>2</td>
<td>70</td>
<td>0</td>
</tr>
</tbody>
</table>

| Virustotal (3+ AVs)    | N/A      | 7              | 100            | 3            |

1 Apps from popular antivirus providers.
2 Apps among top 10 search results in Play Store for "anti-spyware".

Fig. 6: True positive (third and fourth columns, higher is better) and false positive (final column, lower is better) detection rates (in percentages) of anti-spyware apps available in the Play Store ordered by reported number of downloads (second column). The final row reports on using Virustotal to flag an app if at least three AV engines flag the app.
Prevention
Which entities are best situated to prevent IPS?

- [https://forms.gle/KefJ3nNPHp6DTYQJ6](https://forms.gle/KefJ3nNPHp6DTYQJ6)
- OS Vendors (64%)
  - (see 18)
- Developers (17%)
  - Make apps more transparent
  - Ethics/risk framework
- Government (2%)
  - Policies that outlaw IPS – COPPA for IPV situations
  - Maybe GDPR? – (routing under purview of GDPR)
    - amend to target developer infractions
- Anti-Virus Companies (1%)
  - Sued by adware companies
  - Created new label PUPs
What actions could OS Vendors take to prevent IPS?

• Know what information is being collected / monitored
  • Notifying users when something is on -- sensors
• Intuitive GUI
• Permissions
• Not hide app icon
• Sensor indicators
• Too much bloatware
• Education
• Faraday cage
• Health checks – security + privacy at os level
Scenario

You are collaborating with Professor Li on future work. Which suggestion sounds most promising to you? What direction would you take?
Related Work and Resources


• VOICE: Sexual Violence Prevention & Victim-Survivor Support, https://healthinitiatives.gatech.edu/well-being/voice, 404.385.4464/4451

• CARE: General Health and Well-Being, https://care.gatech.edu/, 404.894.3498