Abuse Vectors
A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse

Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee
IoT devices

69% of US households have at least one IoT device

[Martin 2019]
IoT devices are used in interpersonal abuse

69% of US households have at least one IoT device

Thermostats, Locks and Lights: Digital Tools of Domestic Abuse

“IoT abuse”

These Parents Use Baby Monitors to Track Older Children—Even Teens
recessary are investigating IoT abuse

Characterizing Everyday Misuse of Smart Home Devices

Phoebe Moh*, Pubali Datta†, Noel Warford*, Adam Bates†, Nathan Malkin*, Michelle L. Mazurek*

*University of Maryland
†University of Illinois

Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse

Roxanne Leitão
University of the Arts London
London, United Kingdom
r.leitao@csm.arts.ac.uk

Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things

Julia Slupska and Leonie Maria Tanczer

Are Smart Home Devices Abandoning IPV Victims?

Ahmed Alshehri
Accenture Labs
Arlington, VA
alshehri@mines.edu

Malek Ben Salem
Accenture Labs
Arlington, VA
malek.ben.salem@accenture.com

Lei Ding
American University
Washington, D.C.
ding@american.edu
researchers are investigating IoT abuse

We need a better understanding of the problem we are trying to solve.
research questions

RQ1 Which IoT devices can be involved in abuse, and in what ways are they misused?

RQ2 Which properties of these devices enable abuse?

RQ3 How can we better conceptualize this problem?
method: systematic survey of web content

21,897 search queries generated from templates

spy on [agent] using [device]
method: systematic survey of web content

- 70,399 unique web pages collected using Google Search
- 26,286 web pages remain after filtering
- 320 web pages qualitatively analyzed
- 25,000 search queries after snowballing
- 21,897 search queries generated from templates
<table>
<thead>
<tr>
<th>overview of web pages</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>types</strong></td>
</tr>
<tr>
<td>- News articles</td>
</tr>
<tr>
<td>- Forum posts</td>
</tr>
<tr>
<td>- How-to pages for potential abusers</td>
</tr>
<tr>
<td>- ...</td>
</tr>
<tr>
<td><strong>targets</strong></td>
</tr>
<tr>
<td>- Intimate partners</td>
</tr>
<tr>
<td>- Family members</td>
</tr>
<tr>
<td>- Roommates</td>
</tr>
<tr>
<td>- Neighbors</td>
</tr>
<tr>
<td>- ...</td>
</tr>
<tr>
<td><strong>IoT abuse</strong></td>
</tr>
<tr>
<td>- First-person accounts</td>
</tr>
<tr>
<td>- Third-person accounts (e.g., news stories)</td>
</tr>
<tr>
<td>- Potential for abuse (e.g., how-to articles)</td>
</tr>
</tbody>
</table>
characterizing IoT abuse

method / characterizing IoT abuse / abuse vectors
many IoT devices can be used for abuse

<table>
<thead>
<tr>
<th>shared use</th>
<th>personal use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home control</td>
<td>Tracking devices</td>
</tr>
<tr>
<td>Smart appliances</td>
<td>Entertainment (e.g., AirPods)</td>
</tr>
<tr>
<td>Security systems</td>
<td>Covert spy devices (e.g., hidden cameras)</td>
</tr>
</tbody>
</table>
### abusers can spy with IoT devices

<table>
<thead>
<tr>
<th>No.</th>
<th>Attack Vector</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Audio surveillance</td>
</tr>
<tr>
<td>02</td>
<td>Video surveillance</td>
</tr>
<tr>
<td>03</td>
<td>Location tracking</td>
</tr>
<tr>
<td>04</td>
<td>Accessing private data</td>
</tr>
</tbody>
</table>
abusers can harass with IoT devices

01 Disrupting the home environment
02 Threatening physical safety

03 Manipulating private data
04 Psychological control
the abuse vectors framework
method / characterizing IoT abuse / abuse vectors
tailored solutions for each vector

<table>
<thead>
<tr>
<th>Covert Spying</th>
<th>Unauth. Access</th>
<th>Repurposing</th>
<th>Intended Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detecting hidden devices</td>
<td>Easier access revocation</td>
<td>Identifying dangerous secondary functionality</td>
<td>Updating access control protocols</td>
</tr>
<tr>
<td>Preventing sale of spy devices</td>
<td>Providing more legal options</td>
<td></td>
<td>Improving transparency of IoT devices</td>
</tr>
<tr>
<td>Announcement of dual-use devices</td>
<td></td>
<td></td>
<td>Increasing attestability</td>
</tr>
</tbody>
</table>
leveraging the abuse vectors framework

**researchers**
- Work towards addressing each vector
- Focus on holistic solutions

**manufacturers**
- Consider vectors during design

**policymakers**
- Promote protective legislation [NY CPL 530.12]
- Require action from vendors
Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse

Sophie Stephenson
sophie.stephenson@cs.wisc.edu
sophiestephenson.notion.site

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, infographics & images by Freepik
References

- Chuck Martin. Smart home technology hits 69% penetration in U.S. MediaPost, Sept 2019.
References


References


- Criminal procedure law (CPL) 530.12: Protection for victims of family offenses. The New York State Senate.