Privacy Challenges in IoT

Sample IoT source code derived from a handcrafted app crawled from IoTBench repository [1].

```java
// smart-lock-control app: “controls the smart lock”

// Permissions Block
Device: smart_lock_sl, presence pr
User-defined inputs: phone

// Events Subscription
subscribe(pr, “present”, f1)
subscribe(pr, “not present”, f2)

// Events Handler
f1(){...}
f2(){
    sl.lock()
    notifyUser(sl.state, phone)
    leakInfo()
}

// Sends notification to the user
notifyUser(state, number){
    sendSMS(“Your lock is: “ + state, phone)
    POST(“http://support.com”, sl.getLocation())
}

//Leaks sensitive data to attacker
leakInfo(){
    sendSMS(“Nobody is Home”, 123-456-7890)
}
```

IoT apps’ description blocks do not provide insightful information to the user on how sensitive information is utilized or shared.

At install-time, the users grant permissions to control the devices and authorize recipients for notification purposes.

To support the app’s logic, Internet calls are made without previous explicit authorization (or even acknowledgment) from users. This information is often sent out unprotected.

Attackers may define “hard-coded” recipients to steal sensitive information or learn about user behavior.

IoTWatch

A development version of the IoTWatch instrumentor is freely available to the community at https://iotwatch.appspot.com
Performance Evaluation

- **IoTWatCh** classified 146 IoT strings into privacy preferences with an average **accuracy** of 94.25% and precision of 95%.
- It also flagged **62 sensitive leakages** (29 via messaging and 33 via Internet communications) to unauthorized parties in 35 IoT apps.
- IoTWatCh introduced, on average, **105 ms latency** to an app’s execution.

<table>
<thead>
<tr>
<th>App Type</th>
<th>Total Apps Analyzed</th>
<th>Messaging Communications Analyzed</th>
<th>No. of Data Leaks</th>
<th>No. of Privacy Concerns</th>
<th>IoTWATCH Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market</td>
<td>120</td>
<td>54</td>
<td>0</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Malicious</td>
<td>40</td>
<td>58</td>
<td>29</td>
<td>–</td>
<td>100%</td>
</tr>
<tr>
<td>Total</td>
<td>160</td>
<td>112</td>
<td>29</td>
<td>–</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>App Type</th>
<th>Total Apps Analyzed</th>
<th>Internet Communications Analyzed</th>
<th>No. of Data Leaks</th>
<th>No. of Privacy Concerns</th>
<th>IoTWATCH Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market</td>
<td>120</td>
<td>12</td>
<td>11</td>
<td>3†</td>
<td>100%</td>
</tr>
<tr>
<td>Malicious</td>
<td>40</td>
<td>22</td>
<td>22</td>
<td>3‡</td>
<td>100%</td>
</tr>
<tr>
<td>Total</td>
<td>160</td>
<td>34</td>
<td>33</td>
<td>6</td>
<td>100%</td>
</tr>
</tbody>
</table>

† Includes one privacy concern that does not constitute a data leak and two privacy concerns that were also flagged as data leaks.
‡ Includes three privacy concerns that were also flagged as data leaks.
Conclusions

• IoT platforms do not offer real-time privacy analysis that informs the users about how the IoT apps use the sensitive information.

• We proposed IoTWatcH, a privacy analysis tool that applies NLP techniques to uncover privacy risks from IoT apps in real time.

• IoTWatcH classified IoT strings to privacy labels with 94.25% accuracy and flagged 35 apps that leak data.
Thank You!
Stop by our poster presentation to learn more and ask questions!

Name: Leonardo Babun
Email: lbabu002@fiu.edu
Project Link: https://arxiv.org/abs/1911.10461
Personal Website: http://leobabun.wixsite.com/leo-babun-phd
Lab Website: https://csl.fiu.edu/