Location-Leaking in Mobile Augmented Reality

Gabriel Meyer-Lee; Swarthmore College
Jiacheng Shang, Jie Wu; Temple University
Outline

▷ Motivation and Context
▷ Attack Model
▷ Analysis and Results
▷ Conclusions
Motivation and Context

The emergence of mobile augmented reality and the unaddressed security and privacy concerns.
Mobile Augmented Reality

- Interactive virtual content situated in the real world.
  - Broader term “mixed reality”
- Location-based AR ties virtual content to geophysical location
- Projected to reach $85-90 billion by 2022
  - Mostly games
AR Security/Privacy

Table 2. Security and privacy challenges for AR technologies. We categorize these challenges by two axes: challenges related to output, input, and data access, as arise in single applications, multi-application systems, and multiple interacting systems.

<table>
<thead>
<tr>
<th></th>
<th>Single Application</th>
<th>Multiple Applications</th>
<th>Multiple Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Output</strong></td>
<td>Deception attacks</td>
<td>Handling conflicts</td>
<td>Conflicting views</td>
</tr>
<tr>
<td></td>
<td>Overload attacks</td>
<td>Clickjacking</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trusted path to reality</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Input</strong></td>
<td>Input validation</td>
<td>Resolving focus</td>
<td>Aggregate input</td>
</tr>
<tr>
<td><strong>Data Access</strong></td>
<td>Access control for sensor data</td>
<td>Cross-app sharing</td>
<td>Cross-system sharing</td>
</tr>
<tr>
<td></td>
<td>Bystander privacy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figures from Roesner (2014), de Guzman (2018)
Network Traffic Analysis

▷ Web sites are vulnerable to side-channel attacks because as a byproduct of common web design practices
  ○ Low-entropy inputs
  ○ Stateful communications
  ○ Significant traffic distinction
▷ All of these are also applicable to the design of mobile AR applications
▷ Website Fingerprinting ➔ Location Fingerprinting
The Attack

Side-channel attack to reveal user’s location through network traffic analysis
Overview of the attack

▷ Three separate sets of digital content
▷ User downloads content when within visible radius
▷ User’s network traffic is monitored
▷ User is located based on their network traffic patterns

Model of the side-channel attack
Monitoring network traffic

▷ Network sniffing
  ○ Typical method for network traffic analysis attack
  ○ Applicable to mobile user in urban center or university campus, but requires access point coverage

▷ Spyware on Device
  ○ Coarseness of user permissions makes over-permissioning inevitable
  ○ Most Android users do not pay attention to or comprehend permissions
WallaMe

Digital graffiti AR app available for iOS and Android
Users post walls for other users to discover the art on
Scenario One: Non-overlapping duplicates
Scenario One: Non-overlapping duplicates
Scenario Two:
Overlapping, distinct
Analysis and Results

CNN-based data processing pipeline and classification accuracy
Analysis

- Past WF algorithms have utilized SVM, kNN, random forest
- We require an algorithm that supports:
  - Near real time location updates, allowing an online attack.
  - No reliance on sequential pattern of input location-encoded data
- Our method:
  - Window network download data to 60s
  - Manually label location regions of recorded data
  - Train 1D CNN
CNN Design

Input Data

Convolutional Filters

Hidden Layers

Convolutional Filters

Hidden Layers

Fully-connected Layer

Output Classification

(60 x 1)

(30 x 10)

(10 x 5)

(31 x 10)

(5 x 5)

(51 x 5)

(5 x 5)

(47 x 5)

(27 x 5)

(20 x 1)

(4 x 1) or (8x1)
Results

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Test Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>93.8%</td>
</tr>
<tr>
<td>2</td>
<td>87.6%</td>
</tr>
</tbody>
</table>

Scenario 1 Confusion Matrix

Scenario 2 Confusion Matrix
Moving Frame Error

<table>
<thead>
<tr>
<th></th>
<th>Scenario 1</th>
<th>Scenario 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw Accuracy</td>
<td>93.8%</td>
<td>87.6%</td>
</tr>
<tr>
<td>Error due to moving frame</td>
<td>56.3%</td>
<td>58.2%</td>
</tr>
<tr>
<td>Accuracy excl moving frame</td>
<td>97.3%</td>
<td>94.8%</td>
</tr>
</tbody>
</table>
Conclusion

Potential avenues for mitigation and final conclusion
Mitigation

▷ Irregular user behavior
▷ Secure app design
  ○ Padding
  ○ Probabilistic location loading
Conclusion

▷ You don’t have to worry about playing Pokemon Go for now
▷ Network traffic patterns in AR apps can in fact leak location information
▷ Future AR developers must include network privacy breaches among the risks they account for