CS 525M Mobile and Ubiquitous Computing: The Wi-Fi Privacy Ticker: Improving Awareness & Control of Personal Information Exposure on Wi-Fi

Shengwen Han

Computer Science Dept.
Worcester Polytechnic Institute (WPI)
Abstract

- **Problem:** Unaware of the risk while using Wi-Fi
- **What this paper aims:**
  - Improve their awareness
  - Provide with control—Wi-Fi privacy ticker
    - Display + prevent transmission
- **To verify:** 3-week field study with 17 participants
Why—Easy to get people’s information?

- Public Wi-Fi hotspots which provide little protection
- Provide personal info to use web services
- Freely available tools for eavesdropping
Related Work

- Understanding & behavior on Wi-Fi
- Technologies to improve awareness & control
- Commercial solutions
The Wi-Fi Privacy Ticker

● **Workflow**
  - User provides terms to monitor;
  - System monitors network traffic when using Wi-Fi
  - When it detects that any term is being sent or received in the clear, it is shown on a peripheral “ticker” display and added to an archive
  - User-control
● **The Network Monitor**
  - Hook `NtDeviceIoControlFile`—handle network-related requests
  - For 3-week field study—Internet Explorer and Firefox browsers
**The Control Mechanism—Zapper**

- Implemented in Windows kernel
- Close socket device handle when it detects a highly sensitive term in the socket’s “send” buffer
- Drops connection
To indicate a “zapped” term, the term appears in *Ticker display* with a strikethrough and a balloon tip appears in system tray.

Cannot prevent terms from being received in the clear.
• The Ticker Display
  • Real-time alerts of potential data exposures
  • Scrolling text that moves from right to left
  • Implemented by .NET Windows Presentation Foundation
- Terms:
  - *Watch List* terms—user specifies (a sensitivity level, displayed name)
  - search terms

- Color reflects term’s sensitivity level

- Rules to prioritize display of terms:
  - First detected, first appear (sensitivity level > detection order)
  - time-out of *Ticker display’s* queue—90 seconds
- ‘out’ / ‘in’, times, IP of the server and other details
- Network encryption
  - Open or Closed Network—bright shade
  - Secure Network or VPN—darker shade
• **The Archive**
  - Review past exposures
  - Any detected *Watch List* terms including which were dropped from the queue for time-out reasons
Considerations for Protecting Users’ Data

- User’s Preferences are password-protected
- Particularly sensitive term types are never shown in the clear
- Database in which system stores user's terms remains encrypted
3-Week Field Study

- Study Procedure & Data Collection
  - Survey + data logs
- Participants
  - chosen from company
  - have option of using a VPN
- Participants’ Watch Lists
- 186 unique *Watch List* terms

<table>
<thead>
<tr>
<th>Term Type</th>
<th># of Participants</th>
<th># of Terms per Type</th>
<th># of Terms per Sensitivity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email address</td>
<td>17</td>
<td>28</td>
<td>1 13 14</td>
</tr>
<tr>
<td>Password</td>
<td>16</td>
<td>30</td>
<td>19 9 2</td>
</tr>
<tr>
<td>Social Security #</td>
<td>14</td>
<td>14</td>
<td>10 3 1</td>
</tr>
<tr>
<td>Street address</td>
<td>13</td>
<td>15</td>
<td>2 7 6</td>
</tr>
<tr>
<td>Birth date</td>
<td>12</td>
<td>13</td>
<td>3 5 5</td>
</tr>
<tr>
<td>ZIP Code</td>
<td>12</td>
<td>14</td>
<td>0 1 13</td>
</tr>
<tr>
<td>Last name</td>
<td>11</td>
<td>11</td>
<td>0 5 6</td>
</tr>
<tr>
<td>First name</td>
<td>10</td>
<td>16</td>
<td>0 2 14</td>
</tr>
<tr>
<td>Username</td>
<td>9</td>
<td>13</td>
<td>2 4 7</td>
</tr>
<tr>
<td>Credit Card #</td>
<td>6</td>
<td>11</td>
<td>5 6 0</td>
</tr>
</tbody>
</table>
## Results

- **Watch List Term Exposure**
  - Average of 1,054 unique search terms were detected for each participant
  - Personal data was transmitted with high frequency
  - Many websites sent personal data in the clear

<table>
<thead>
<tr>
<th>Site</th>
<th>% of Total Matches (out of the 353 sites observed)</th>
<th>Email Address</th>
<th>First Name</th>
<th>Last Name</th>
<th>Password</th>
<th>Street Address</th>
<th>Username</th>
<th>ZIP Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web search &amp; portal</td>
<td>22.39%</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Social networking</td>
<td>21.07%</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Sports</td>
<td>16.66%</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Newspaper</td>
<td>6.41%</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Company</td>
<td>3.81%</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Airline</td>
<td>2.83%</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>eCommerce (apparel)</td>
<td>2.53%</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>eCommerce (technology)</td>
<td>2.09%</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>1.35%</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Auction</td>
<td>1.34%</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
### Change in Awareness

<table>
<thead>
<tr>
<th>Statement</th>
<th>Agreement Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>When I am connected to the Internet on a wireless network, I think about</em></td>
<td></td>
</tr>
<tr>
<td>what information I may be exposing to others on the Wi-Fi network*</td>
<td></td>
</tr>
<tr>
<td><em>I am not concerned about others on the Wi-Fi network being able to</em></td>
<td></td>
</tr>
<tr>
<td>see the information that I expose when I use the Internet on Wi-Fi*</td>
<td></td>
</tr>
<tr>
<td><em>Ticker has made me more aware of</em></td>
<td></td>
</tr>
<tr>
<td>what I may be exposing to others on the network</td>
<td></td>
</tr>
<tr>
<td><em>I feel safer about Wi-Fi when the Ticker is running</em></td>
<td></td>
</tr>
</tbody>
</table>

* - Difference between pre- and post-study surveys is significant (p<.01)

- Pay attention to network encryption
- Form more accurate mental models of the circumstances in which data get transmitted
- Positive to Zapper
Change in Behavior

- ≠long-term behavior change
- Upgrade encryption of home wireless network
- Start using VPN
- More careful about types of networks
- Not stay logged in
- Close browser windows more frequently
- Educate friends
Discussion & Future Work

- **Improve the Control Mechanism**
  - pop up a window to ask if dropping connection or proceeding
  - rule-based systems
● Extend the Ticker Concept
  ● Detect transmitting of personal data which is not in *Watch List*
  ● Monitor additional applications
  ● Develop system used by parents to monitor and keep children safe on the Internet
  ● Change or augment user experience
Provide Education

- Educate users about phishing attacks by *PhishGuru* and *Anti-Phishing Phil*
- Making suggestions based on user’s activities
Conclusion

- Wi-Fi Privacy Ticker
- How to help users become more aware of the unencrypted transmission of terms and how to prevent
- Three-week field study with 17 participants verified that participants’ awareness improved and their behavior on Wi-Fi changed
References

Thanks!
Questions?