SSID's and Social Networks

Michael Ballantyne
University of Utah

Maria Jenkins
University of Utah

Priyanka Parekh
University of Utah

Abstract

Some Wi-Fi network clients transmit a list of networks they've previously connected to when scanning for networks to join, and many users are not aware that this data is broadcasted and can be easily monitored. We hope to make users aware that this data can reveal information about locations they spend time and their social connections. We captured Wi-Fi probe requests from a sample of wireless clients and analyzed the social network implied in the data for privacy risks. We found that Apple laptops revealed the most, while most mobile devices and computers running Linux no longer share private data in probe requests. The data suggests that while some computers no longer reveal previous network associations, large scale data from the remaining clients could present a significant privacy risk. Even at small scale the list of network associations is a possible tool for Wi-Fi client fingerprinting. Our work concurs with other recent studies showing that network associations can be used to fingerprint Wi-Fi clients or link users to certain political organizations or other groups based on the names of the networks. To encourage users to be more security conscious we provided participants with a personalized interactive social network graph showing how their network associations relate them to other participants. We include results from a survey conducted to understand participants' reactions to this data.

1 Introduction

Laptops broadcast the list of Wi-Fi networks(SSID's) that a user has ever connected to. The list of SSID's is broadcasted when your laptop is probing for a Wi-Fi access point. A large majority of users are unaware that this data is broadcasted and can be monitored. Previously cell phones broadcasted this data as well. People are surprised that their location data is being broadcasted. The fact that this data is being broadcasted raises some privacy concerns.

2 Study Procedures

To conduct this study we had to take into consideration the security and privacy of our participants so as to minimize harm but still collect meaningful data. We took precautionary measures to protect the anonymity of our users and

of the data we collected and anonymity in displaying the results for our participants. To minimize harm we took precautionary measures to protect the data and privacy of our users.

2.1 Data Collection

We collected data from consenting participants.

2.2 Survey

2.3 Social Network Analysis

3 Results

4 Related Work

There has been a fair amount of related work in this area, however most of the work was targeted at cell phones and not laptops. Cell phones have stopped broadcasting the SSID list when probing for Wi-Fi connections.

Chang et al sought to discover user relationships from observing the similarity of SSID lists between users, they took into account physical proximity and spatio-temporal behavior. They looked at the similarities of SSID lists being broadcasted from cell phones before cell phones disabled this feature. They found that spatio-temporal data had more social connections.

Barbera et al used social network analysis on datasets of Wi-Fi probes from cell phones in public areas. They

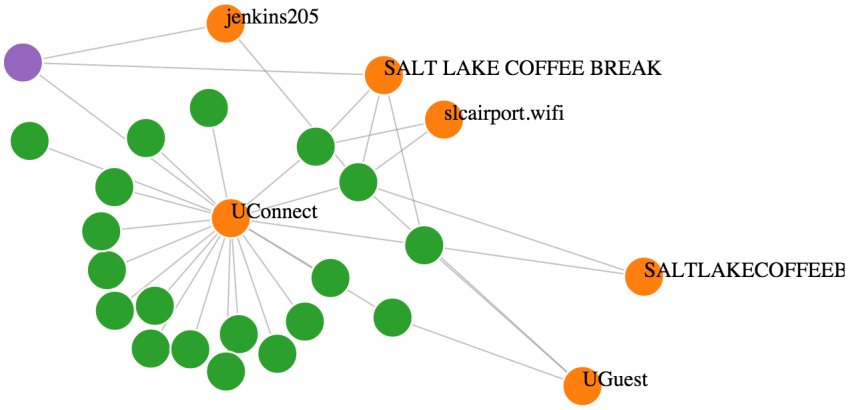

Figure 1: Social Network Graph

found that data matched typical properties of social networks. They also mentioned what devices broadcast the SSID list when probing for a connection.

Desmond et al discussed an alternative approach to fingerprinting that defeats MAC address randomization and the absence of an SSID list by timing the intervals between Wi-Fi probes, but requires hours of continuous data to perform adequately.

Cunche et al present a mechanism to detect links between people by fingerprinting devices by exploiting the fact the SSID lists are broadcasted in plain text when probing for WI-FI connections. They take a very quantitative approach and are able to gather a large dataset. This work demonstrates a privacy breach allowed by the 802.11 probe requests and raises awareness that initiative should be taken to increase privacy in terms of Access point discovery.

5 Conclusion