Poster: Privacy Implications of BSSID based Location Services

Muhammad Naveed*, XiaoFeng Wang†, Carl Gunter*
*University of Illinois at Urbana-Champaign
†Indiana University at Bloomington
Email: naveed2@illinois.edu, xw7@indiana.edu, cgunter@illinois.edu

***Abstract*—In this work we show the threats to location privacy of an Android user from popular wireless Basic Service Set Identifier (BSSID) based location services. Our approach uses a combination of techniques an attacker can use to infer the location of a user. Firstly, we describe how an Android app (even with zero permissions) can stealthily steal the BSSIDs from a phone. Secondly, we were able to reverse-engineer the mobile-app to server protocol interaction of a popular BSSID based location service, allowing the attacker to get the location of any chosen BSSID. We make this BSSID to location lookup software available at [1]. We have a demo [3], which shows a malicious app (with zero permissions) stealing the BSSID of the wireless network and transmitting the same to the attacker, allowing the attacker to accurately locate the location of the user. Using our technique attacker can easily steal complete database of the BSSID to geolocation mappings.**

I. Introduction

Wireless access points (APs) are everywhere. We found that even in a small town, wireless AP density varies from 5 to 130. Almost all APs broadcast beacons for the Wi-Fi enabled devices to discover them. The broadcast beacons announce the Basic Service Set Identifier (BSSID) of the AP. BSSID is the MAC address of the wireless interface and is unique for every interface. APs have small range, thus BSSID can be easily mapped to the approximate GPS location, allowing geo-location of the AP with high accuracy.

Many companies have huge BSSID to geo-location mapping databases with countrywide coverage. Some companies (e.g. Skyhook Wireless) drove through out the country to build their databases. Navizon (a famous location service provider) provides apps for Android and iOS with geo-location capabilities that are similar to, or even better than GPS. GPS has poor reception at some places, such as indoors and near high-rise buildings, so many systems use BSSID for better geo-location.

iPhone and iPad can locate you even if GPS is turned off or not available because Apple uses BSSID based location services [4]. These BSSID based location services provide location information for devices that don't have GPS or when GPS signals are weak. BSSID based location services have huge databases that map BSSID of WiFi Access Points (AP) to their GPS coordinates, which are then used to give correct location information. Google used to provide a rate limited BSSID based location service with Google Gears API. Similarly Skyhook Wireless used to have a free API to provide this type of single BSSID queries. Both Google and Skyhook don't provide this service anymore. Collection of BSSID information is very bad for location privacy. SlyFi [5] proposes a new wireless protocol that obfuscates all the identifiable link layer information, but all the wireless networks deployed today use IEEE802.11. In this study we show how to get location from BSSID using a private database. Previously proposed techniques [6] get this information by changing the BSSID of the AP near the phone to the target BSSID (victim) that needs to be located. An app on the phone will be able to locate the victim because it will receive beacons with this new BSSID. This approach doesn't scale to stealing the entire BSSID based location database, because of the need for extensive human interaction. Our approach is different from earlier approaches because we can essentially steal the entire database of this sensitive information.

These services provide very accurate location information based on multiple BSSIDs. In fact, they are capable of locating with high accuracy even with single BSSID. Location is considered very private information and its leakage can impact people's life style. In this poster and demo, we show the huge privacy risk associated with BSSID based location services.

Harvesting BSSIDs is not very hard. A malicious program running on a Wi-Fi equipped device can record and then send all the BSSIDs seen by the wireless interface to the attacker. Smartphones are even more dangerous because an attacker can continuously get BSSIDs from the phone while the victim is moving and can track her. In this work, we focus on smartphones but the technique is general and can be extended to PCs and other devices as long as the attacker can get the MAC address of the AP.

We used Navizon location service to demonstrate our attack. We analyzed Navizon protocol using Man In the Middle (MITM) proxy and decrypted the SSL traffic. We analyzed the decrypted traffic in Wireshark and simulated the Navizon protocol on the computer using a Python script. Attacker can feed the simulator with any arbitrary BSSID and can get the location associated with it, if it is present in the location service database.

We notice that the Navizon service doesn't place any checks on requests. We didn't notice any rate limitation in place by Navizon, while doing experiments. For legal reasons, we didn't tried to steal the complete database, but our technique is capable of stealing the complete database and any average hacker can do the same.

Navizon extensive coverage can be seen at http://www.navizon.com/navizon_coverage_wifi.htm [2]. We collected data from many places and we were able to locate hospitals, restaurants, train stations, bus stations,

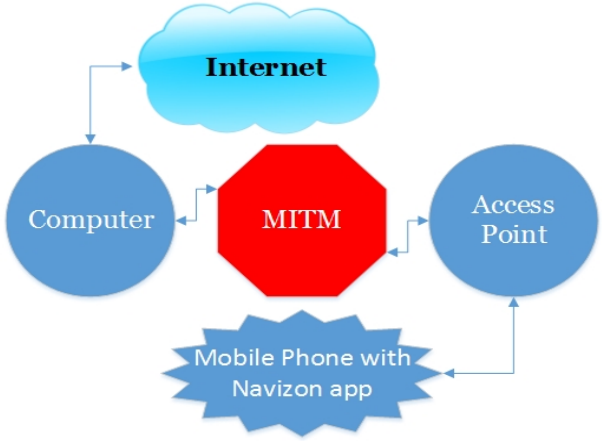

Fig. 1: Understanding Navizon Protocol

airports and many other places. Some of the places we located are shown in Table I. All the results were obtained using single BSSID queries.

Following sections explain the experimental details:

A. Stealing BSSID using Android Apps with Zero Permissions

We analyzed the Android's `procfs` and discovered that BSSID (MAC address) of the AP to which the phone is connected is stored in `/proc/net/arp`. This file is publicly available and can be read even by a zero permission app. Given the fact that most users have their Wi-Fi radio in auto-connect mode, it's very easy to steal this information. As shown in the video demo [3], our zero permission app can steal the BSSID and send it to an attacker controlled web server by using the phone's web browser. To make our attack stealthy, we invoke the browser only when the screen is turned off.

B. Understanding the Navizon Protocol

Navizon's Android app uses SSL to communicate with the server. To analyze the protocol we decrypted the traffic using the setup shown in Figure 1. Phone running Navizon app and computer running Man In The Middle (MITM) proxy are connected to the AP. AP is configured such that it forwards all packets it receives from the phone to the computer and computer forwards reply packets back to the phone using AP. So, phone is accessing Internet through computer running MITM. MITM changes the SSL certificate on the fly with a new certificate with a known key. Now, the communication between Navizon app and server can be decrypted and analyzed using Wireshark.

C. Demo

Our poster will be accompanied with a demo showing the attack. We will collect real time data at the time of demo and show the location on Google maps. We will also collect BSSID data from other places and show that how it can be used to locate people on Google maps.

TABLE I: Places located using single BSSID queries

Location **(All in Champaign-Urbana, IL)**	**Total BSSIDs Collected**	**Working BSSIDs**	**Error**
My home	5	4	0 ft
Carle Hospital	74	2	59 ft
Provena Hospital	57	4	528 ft
Subway	6	4	3 ft
Starbucks	43	3	6 ft
Illinois Terminal (Train/Bus Station)	14	10	0 ft
Korean Church	82	3	150 ft
UIUC Bookstore	34	2	289 ft

ACKNOWLEDGEMENTS

We thank Xiaoyong Zhou and Dongjing He for writing the Android app for the demo. We also thank Ravinder Shankesi, Vincent Bindschadler and Anupam Das for their useful comments.

REFERENCES

[1] Navizon simulator. http://cryptoonline.com/naveed/code/, 2013.

[2] Navizon wifi coverage map. http://www.navizon.com/navizon_coverage_wifi.htm, 2013.

[3] Stealth attack demo. http://youtu.be/UHt4BdMZ90M, 2013.

[4] Jefferson Graham. Jobs, iphone have skyhook pointed in right direction. http://usatoday30.usatoday.com/tech/products/2008-01-22-skyhook_N.htm, 2008.

[5] Ben Greenstein, Damon McCoy, Jeffrey Pang, Tadayoshi Kohno, Srinivasan Seshan, and David Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In *Proceedings of the 6th international conference on Mobile systems, applications, and services*, MobiSys '08, pages 40–53, New York, NY, USA, 2008. ACM.

[6] Nils Ole Tippenhauer, Kasper Bonne Rasmussen, Christina Pöpper, and Srdjan Čapkun. Attacks on public wlan-based positioning systems. In *Proceedings of the 7th international conference on Mobile systems, applications, and services*, MobiSys '09, pages 29–40, New York, NY, USA, 2009. ACM.