iPhone and iPod Location Spoofing

Attacks on Public WLAN-based Positioning Systems

iPhone and iPod Location Spoofing: Attacks on Public WLAN-based Positioning Systems

Nils Ole Tippenhauer, Kasper Bonne Rasmussen, Christina Pöpper and Srdjan Čapkun
Department of Computer Science
ETH Zurich
8092 Zurich, Switzerland
{tinils, kasperr, poepperc, capkuns}@inf.ethz.ch

ABSTRACT

In this work, we study the security of public WLAN-based positioning systems. Specifically, we investigate the Skyhook positioning system [41], available on PCs and used on a number of mobile platforms, including Apple's iPod touch and iPhone [1]. We demonstrate that this system is vulnerable to location spoofing and location database manipulation attacks. We further discuss approaches for securing Skyhook and similar WLAN-based positioning systems.

1. INTRODUCTION

In the last decade, researchers have proposed a number of WLAN positioning techniques for (local area) wireless networks [5,9,19,50]. The applications of these techniques are broad and range from improving networking functions (i.e., position-based routing) to enabling location-related applications (e.g., access control, data harvesting).

WLAN positioning systems are now being commercialized and are being used as a substitution and/or complement to the Global Positioning System [15]. One such system is the Wi-Fi positioning system (WPS) from Skyhook [41], available for PCs (as a plugin) and on a number of mobile platforms, including the Apple iPod touch and iPhone [1] as well as on Nokia mobile phones based on Symbian [4]. The Skyhook WPS relies on existing WLAN access points for localization of devices that have 802.11a/b/g wireless interfaces – in WPS, a mobile device collects information about all visible WLAN access points in its vicinity, obtains their locations from the Skyhook location database, and determines its own position by aggregating this information. The position estimate can then be directly used by a mapping application like Google maps or can be combined with other sources of location information, such as those from GSM stations or GPS. Positioning systems by Mexens [26] and the Fraunhofer institute [13] have a similar mode of operation. We call these systems *public WLAN-based positioning systems*, since they rely on public WLAN access points which are not under control of the service operator that provides the positioning service.

In this work, we analyze the security of public WLAN-based positioning systems. Using the example of the Skyhook WPS, we demonstrate that such positioning systems are vulnerable to location spoofing attacks: by jamming and replaying localization signals, an attacker can convince a device that it is at a position which is different from its actual physical position. We further show that, given that it uses access point location information provided by the users, the Skyhook WPS is also vulnerable to database manipulation attacks, which can equally be used for location spoofing. We further discuss possible approaches for securing public positioning systems and show their potential advantages and drawbacks, given the constraints of the application scenarios in which they are used.

By demonstrating these attacks, we show the limitations of Skyhook and similar positioning systems, in terms of the guarantees that they provide and the applications that they can be used for. Given the relative simplicity of the attacks and the availability of the equipment used to perform the attacks, we conclude that, without appropriate modifications, these positioning systems cannot be used in security- and safety-critical applications.

To the best of our knowledge, this work is the first that analyzes the security of public WLAN positioning systems and the first that demonstrates the implementation of location spoofing attacks in WLAN networks. Equally, we are unaware of any prior work that discusses location database manipulation attacks.

The structure of the paper is as follows. Background on public WLAN-based positioning is given in Section 2. Location spoofing attacks are presented in Section 3. Database manipulation attacks are described in Section 4. Solutions for securing public WLAN-based positioning systems are discussed in Section 5. Related work is described in Section 6. In Section 7, we conclude the paper.

2. BACKGROUND: WLAN POSITIONING SYSTEMS

WLAN-based positioning systems include range-based systems, which rely on RSS (Received Signal Strength) measurements, and range-free systems, which rely on localization beacons. Both types of systems make use of WLAN access points (AP) as localization stations which typically broadcast service announcement beacons from fixed known locations. Based on the reception of these beacons, devices compute their positions. In range-based systems [5, 14, 16, 31, 34], the localized node (LN) records the signals received from access points, measures their RSS values, converts them into ranges, and estimates its own positions using the measured ranges. In range-free systems, the LN registers which APs are in its reception range, and based on this information, estimates its position. In most proposed WLAN-based positioning systems, the APs are controlled by the authority that operates the system. Typically, range-free and range-based WLAN positioning systems achieve a positioning accuracy in the order of meters, and if they rely on location fingerprinting, they can achieve accuracy in the order of tens of centimeters [5, 31, 34].

Skyhook's Wi-Fi Positioning System (WPS) is a metropolitan area public positioning system; it is a software-only system and requires a LN solely to have a WLAN-capable card and an internet connection. Skyhook's WPS differs from existing WLAN positioning systems in that it does not maintain its own AP infrastructure; instead, it relies on the existing commercial, public, and private access points. In WPS, the operator (Skyhook) first creates a location lookup table (LLT), which contains data samples taken from different locations. For each location, the Medium Access Control (MAC) addresses of all visible access points are stored. This lookup table can then be queried by the software on the LN. Since obtaining information about available access points in an area can be a work-intensive process (that needs to be constantly updated due to the dynamics of the WLAN networks), WPS also allows users to enter (on-line) locations and MAC addresses of their access points and of access points that they observe in their vicinity. As we will discuss later, Skyhook also leverages on information obtained from location requests to update its WLAN location database (LLT).

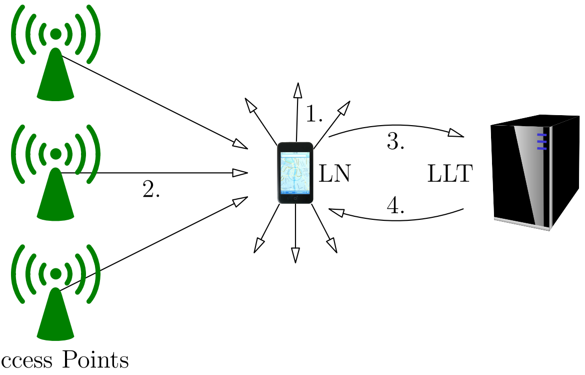


Figure 1: The Skyhook localization process. 1. The LN broadcasts a probe request frame. 2. APs reply with a response beacon frame. 3. The LN queries the LLT server. 4. The server returns data about observed APs. 5. The LN computes its location.

WPS localization can be divided into five phases, as shown in Figure 1. In phase 1, the LN scans all WLAN (802.11a/b/g) channels for access points by broadcasting a probe request frame on all channels.[1] In phase 2, the APs in range reply to the LN with network announcement beacon frames containing, among other parameters, their MAC addresses. After having detected these beacons and recorded their corresponding signal strengths, the LN sends the recorded MACs to the Skyhook LLT (phase 3); this step requires that the LN has an (internet) connection to the LLT. In phase 4, the server compares the reported MACs to its stored data and provides the LN with locations of the access points. In phase 5, the LN computes its position based on the received access point location information using a non-disclosed algorithm[2]. Note that by sending information about its neighboring access points to the WPS database, the LN also allows Skyhook to update its database.

3. LOCATION SPOOFING

In this section, we analyze the security of the Skyhook WPS and we show attacks on its positioning. We demonstrate that the Skyhook WPS is vulnerable to attacks in which signal insertions, replays, and/or jamming allow an attacker to either prevent the localization or to convince a device that it is at a position which is different from its actual physical position (location spoofing). Our attacks are composed of two actions: (1) impersonation of access points (from one location to another) and (2) elimination of signals sent by legitimate access points. Since rogue access points can forge their MAC addresses and can transmit at arbitrary power levels, access point impersonation can be easily done in WPS. Equally, since WLAN signals are easy to jam, signals from legitimate access points can be eliminated, thus enabling location spoofing.

In what follows we will demonstrate location spoof-

[1] Although Skyhook [41] reports that WPS uses passive network scanning, the implementation of WPS on our iPod touch device performs *active* network scanning. If only passive scanning is used, phase 1 is redundant.

[2] We were not able to find the description of the Skyhook's position computation algorithm in the open literature.

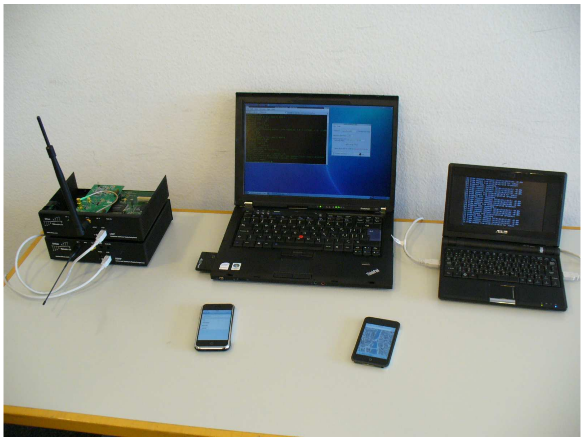


Figure 2: Equipment used in our experiment. The iPod and iPhone are the LNs, the laptops are used to impersonate access points (APs), and the software radios are used to jam legitimate APs.

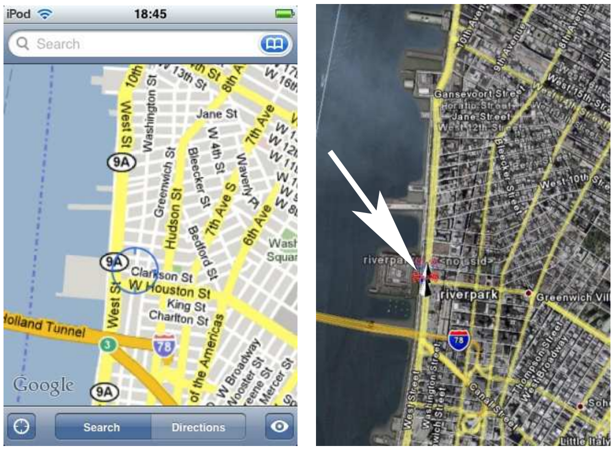
ing attacks in three scenarios, (i) the LN is not in the range of legitimate APs (AP impersonation), (ii) the LN is in the range of legitimate APs and uses only WLAN-based localization (AP replacement) and (iii) the LN is in the range of legitimate APs and uses a hybrid WLAN/GSM-based localization system. Further we will show that the same attacks can be performed on Skyhook's Loki browser plugin on a standard PC.

3.1 Equipment

In our experiments, we used the following equipment. For positioning, we used the Apple iPhone and iPod touch [1] devices with the WPS-enabled Google maps application and a Laptop device with an installed Skyhook's Loki browser plugin [41]. To perform the attacks, the attacker needs devices that impersonate legitimate access points as well as devices that eliminate legitimate access point signals. For access point impersonation, we used two laptops running Ubuntu Linux configured as wireless access points; these devices were transmitting on channels which were not occupied by existing access points, and they were configured such that they could modify the MAC addresses of their Wi-Fi interfaces, their network names (SSID), and signal strengths. To eliminate signals from legitimate access points we jammed these signals, using a software radio platform (USRPs [11] with daughterboards for the 2.4 GHz band). Our equipment is shown in Figure 2.

3.2 AP impersonation

First, we performed an attack which we call *access point impersonation* attack. The idea of an AP impersonation attack is to report remote access points to the attacked device, which will then compute a location that is in the proximity of the remote APs. This attack exploits the fact that the WPS localization relies on (easily replayed) AP MAC addresses for their identification; AP MAC addresses are public since they are contained in the network announcement beacons.



(a) (b)

Figure 3: Location spoofing attack. (a) Location in New York City (circle in the center) displayed by an iPod physically located in Europe (caused by an AP impersonation/replacement attack) (b) Physical location of impersonated APs (indicated by the arrow and displayed using Google Earth [3]).

To execute the AP impersonation attack, we used a Laptop with a WLAN card, running a program that impersonates APs and that we have written for this purpose. Our program waits for probe requests sent by the LN (iPhone or iPod) and replies to these requests with custom-made beacon responses, that correspond to the beacon responses from impersonated remote APs. Each beacon response $\hat{r}_i$ contains a MAC$_i$ address that is equal to the MAC address of the spoofed network i; the beacon also contains an SSID$_i$, that is not necessarily equal to the one of the spoofed network. We note that network SSIDs are not used by the WPS to identify the APs, but helped us to distinguish the impersonated from legitimate APs. All other parameters in the beacon responses were set to their default values (e.g., signal strength was set to 17 dBm). This setup enabled us to impersonate an almost arbitrary number of access points in the vicinity of the LN.

In our experiment, we chose to impersonate four geographically mutually close access points located in New York City, and we set their SSIDs to: NY_1, NY_2, NY_3, NY_4. In order to find the MAC addresses corresponding to these access points, we used the WiGLE database [53], which provides information about worldwide wireless networks.

We first performed this experiment in an environment without WLAN coverage, i.e., no legitimate APs were

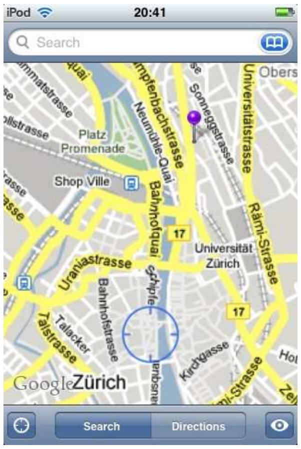


Figure 4: Location spoofing attack. Location displayed by the iPod in city downtown (marked by a circle) at about 1 km distance from the iPod's actual position (marked by a pin) at university campus (caused by an AP impersonation/replacement attack).

visible to the iPod at its physical location at the time of localization. After impersonating the APs using our program, the localization process on the iPod resulted in a location in New York City, while the device was physically located in Europe; this is shown in Figure 3. The displayed location was close to the position of the spoofed access points. We then successfully performed a more fine-grained spoofing attack and modified the displayed location of an iPod such that it displayed a position in the city center of our city, approx 1 km from its actual position (at the university campus). This is shown on Figure 4. Beyond succeeding in performing the AP impersonation attack, we learned that at least some of the access points that we impersonated are registered in the Skyhook database (LLT).

We then performed the same attack in an area covered by public APs. We impersonated wireless networks with MAC addresses of access points that are contained in the Skyhook database, but are located far (New York) from the actual physical location of the device. As a result, the WPS algorithm failed since the LN (iPod) registered access points at locations which are physically too far apart and was thus not able to resolve its own position. Although, in this scenario, the location spoofing attack failed, it unveiled a simple denial-of-service (DoS) attack on WPS localization. To perform this DoS attack, the attacker only needs to impersonate an AP which is in the Skyhook database and is located far from the actual physical location of the localized device.

In the following section, we show how to successfully spoof a location of a device even if it resides in an area covered by public (legitimate) APs.

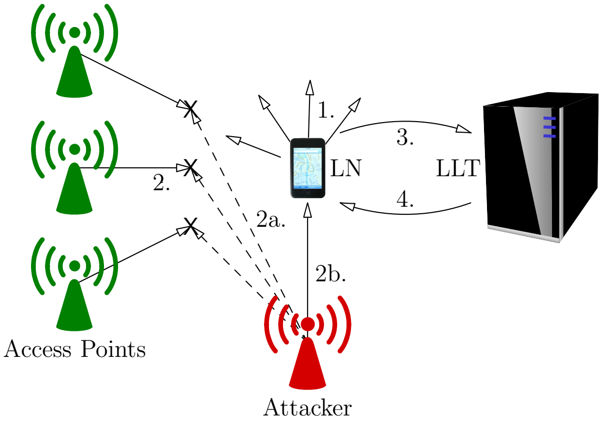


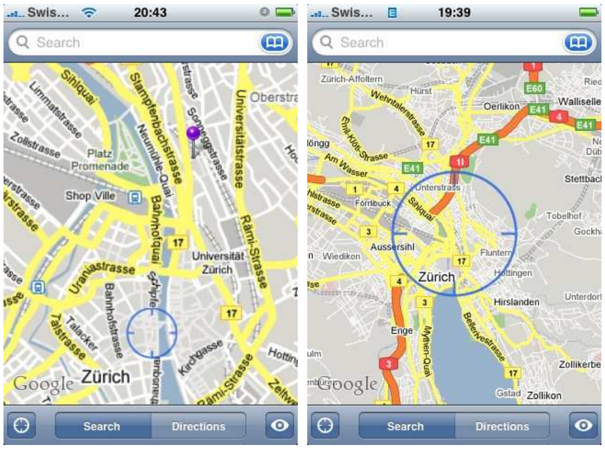
Figure 5: AP replacement attack. The beacons of legitimate APs are jammed (2a) and the attacker sends spoofed beacon responses to the LN (2b). The LN processes the spoofed beacons as they are legitimate and displays an incorrect position.

3.3 AP replacement

Nowadays, most urban and suburban regions as well as other popular areas are covered by a large number of legitimate APs and will – with increasing probability – be categorized by Skyhook. In order for the AP impersonation attack to succeed despite the presence of known APs, we need to eliminate the announcement beacons sent by the legitimate APs and replace them with our impersonated AP beacons. We call this an *AP replacement* attack and it can be considered as a more comprehensive form of the AP impersonation attack.

The idea behind the AP replacement attack is shown in Figure 5. In this attack, we use standard wireless tools to detect the channels on which the legitimate APs are transmitting their beacons and then launch a physical-layer jamming attack to disable the reception of those beacons on the identified channels. Simultaneously, we insert signals from impersonated APs on non-jammed channels. The jamming is not noticed by the user because the simple user interface on the iPod does not provide enough information to detect ongoing jamming. We also note that instead of physical-layer jamming, an attacker could use MAC layer jamming or signal overshadowing, which would result in the same effect (i.e., the elimination of legitimate AP signals).

In our attack setup, the legitimate access points were transmitting on WLAN channels 6, 10, and 11. We used software-defined radios (USRPs [2], see Figure 2) to emit uniform noise on those channels, which blocked the communication between legitimate APs and the iPod. By using physical-layer jamming, we had full control over the transmission power and bandwidth of the jamming signals and could easily elude the 802.11 protocol standard. We then announced the impersonated net-



(a) (b)

Figure 6: Attack on iPhone WLAN/GSM localization. (a) Location displayed by the iPhone in the city center (marked by a circle) at about 1 km distance from the iPhone's actual position (marked by a pin) at university campus (caused by an AP impersonation/replacement attack). (b) Location displayed by the iPhone when spoofing failed. The attacker's target location was in New York City, far from the location that the iPhone's GSM localization computed (in Europe). The attack thus failed and the iPhone displayed the location computed using GSM localization (marked by a circle).

works using channel 2 (up to 13 channels are available in 802.11 in total).

Equally as in the AP impersonation attack, (see Figures 3(a) and 4), the AP replacement caused the iPod to report an incorrect location (in New York city or in the city downtown), chosen by the attacker.

3.4 Location Spoofing Attacks on Hybrid WLAN/GSM Localization Systems

The attacks described in Sections 3.2 and 3.3 were performed on an iPod touch device. Regarding localization, the iPhone differs from the iPod in the sense that it applies a hybrid localization technique, which combines WLAN and GSM base station localization. In the iPhone, GSM-based localization provides a rough position estimate, while WLAN localization provides the device with a fine-grained position estimate.

GSM, the second source of location information, can be used to detect displaced (impersonated) locations in the WPS process and enables the devices to fall back to GSM localization. As our experiments showed, if the position that the device computes using WPS is too far away from the position that it obtains using GSM information, the iPhone will only display the position computed using GSM (i.e., it ignores the WPS position). This is shown on Figure 6b.

However, since the GSM localization is significantly less accurate than WPS localization, using the attack described in Section 3.3, we were still able to displace the iPhone within its GSM localization accuracy (in our test, within 1 km distance). The result of this attack can be seen in Figure 6a; the figure shows the real physical location of the device (marked by a pin) and the location displayed by the iPhone (marked by a circle). This result is similar to the one obtained for iPod location spoofing (Figure 4).

In order to spoof the position of an iPhone to different cities or countries, the attacker either needs to disable the GSM signal reception (e.g., using widely available GSM jammers) or spoof GSM base stations, which has been shown to be feasible for GSM [28] and even for UMTS networks [27]. Attacks using GSM base station spoofing or jamming were not part of our experiments.

3.5 PC location spoofing

We further tested the same attacks on a Laptop with an installation of Skyhook's Loki browser plugin [41]. This plugin is installed into the browser like a toolbar and is able to provide web sites with location information. We repeated the above described location spoofing attack (AP impersonation and replacement) and the results we got on the Laptop were identical to the ones reported by iPod touch.

Thus, if users rely on Loki to provide their web applications with location information, this can be misused by the attacker and possibly lead to a wider system or data compromise, since the attacker can fully control the location that Loki provides to the application.

One can further imagine a web service that provides information to the user only if the user is at a given location. Given the attacks that are described, Loki cannot be used for location verification, since even the user could spoof his own location to get access to the service (e.g., pretending to be in New York, while being in Europe). By using the attacks that we described, Loki results could be equally modified in a number of other ways, including by the manipulation of input that the plugin gets from the networking interfaces.

4. LOCATION DATABASE MANIPULATION

AP location/MAC data enters the Skyhook database in one of three ways: (1) The database is extended and updated by vehicle-based signal scanning and data collection performed by the company, (2) new access points can be inserted online by the users, and (3) Skyhook incorporates data that was submitted by the user in localization queries in order to improve the accuracy of its reference database. As we show in what follows, Skyhook's WPS database (LLT) is not resistant to targeted

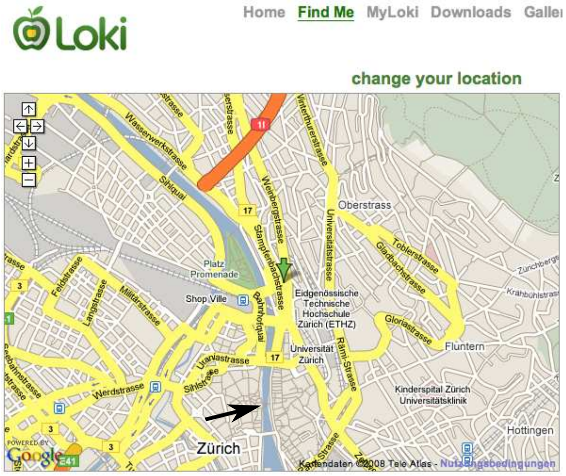


Figure 7: Data corruption in the LLT (using Loki). The lower (black) arrow displays the original location D of AP_k in the LTT. The upper (green) arrow shows the new location U, after impersonating an access point with AP_k's MAC.

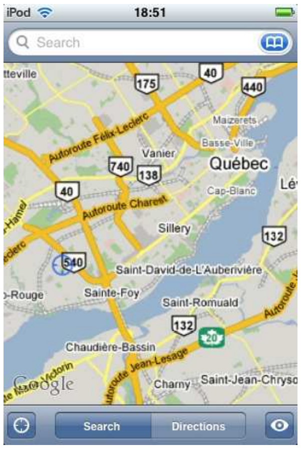


Figure 8: Reverse AP location lookup in the LLT. Using a spoofed access point and modifying its MAC address resulted in a localization in Québec, Canada, though being physically located in Europe.

location database manipulation attacks, although Skyhook tries to counteract this threat by applying error-detection and error-correction methods (surveying the age and consistency of data and executing periodic rescans of outdated areas [41]).

In database manipulation attacks, the attacker tries to actively interfere with the database underlying the localization process by inserting wrong data and/or by modifying existing entries, e.g., by changing the recorded positions of access points to remote positions. Consequently, the attacker may not only change the result of an individual localization, but influence many localizations that all use the common database (in this case, the LLT).

4.1 Injection of false data

Here we show how we successfully inserted false location information for an access point into the Skyhook LLT. During the location spoofing experiments described in Section 3, access point AP_k was used to provide internet access over WLAN to the iPod in order to enable the communication between the iPod and Skyhook's database. The MAC of AP_k was, before the experiments, unknown to Skyhook.

When we spoofed the location of the iPod (located at campus, location U), the iPod reported to Skyhook not only the impersonated APs (from the location D, at city downtown), but also the MAC of the AP_k (located at U) that it used for its internet connection. As a consequence, the MAC address of AP_k got added by WPS to the LLT database with location at D, although being physically located approx. 1 km away (at U).

Subsequent tests in which the iPod was connected only to AP_k, showed that the iPod displayed a location at D, confirming that, in the LLT database, AP_k has a position in the city downtown (D), while being located at university campus (U), approx 1 km away.

This attack is a direct consequence of Skyhook WPS mode of operation, in which the LLT database is not being updated only by company employees and on-line users, but also through the localization requests that the users send when they want to determine their positions.

4.2 Corruption of existing data

A more severe form of the data manipulation attack is the virtual relocation of access points that have already been categorized in the database. To demonstrate this, we used the access point AP_k that was previously injected at the location in city downtown (position D). To change the location of AP_k in LLT, we set up a second access point using AP_k's MAC at our university campus (position U) and kept it active over a longer time (several days). All localizations executed by users in this area were now also submitting AP_k's MAC when localizing themselves - however this time for the new position U. As a consequence, Skyhook started to resolve the old location of AP_k to the new position U, assuming that the majority of the reported MAC addresses define the correct location. Consequently, the access point AP_k was moved in the LLT database from location D to its new position U, as shown in Figure 7. As before, we verified this result by localizing a device using only AP_k.

Because this database manipulation attack is in fact conducted involuntarily by all users using the WPS service in range of AP_k, this attack is hard to detect by the service provider (Skyhook). Although we acknowledge that this manipulation attack only succeeds in settings where the localization service is triggered (much) more often at the new location than at the old one, this attack represents a powerful threat to the correctness of the LTT database and may affect the results of the localization service for many users and at many locations.

4.3 Reverse Location Lookups

Using our attack equipment from Section 3, we are able to find the exact positions of any AP recorded in the LTT with known MAC address, but unknown position. Although this does not manipulate the database contents, it still represents an undesired function of WPS revealing (confidential) positions of access points; here we assume that Skyhook wants to maintain the confidentiality of the AP MAC-AP location bindings.

We performed a *reverse AP location lookup* by changing the MAC address (switching two bits) of one of the spoofed access points in the downtown area which we used in the prior attacks. The position resulting from an iPod localization using this access point was Québec, Canada, as shown in Figure 8. Since manufacturers often assign MAC addresses linearly to their products, this also allows us, e.g., to look up the locations of access points from one production charge.

4.4 Conclusion

From the above analysis and attacks, we can only conclude that WLAN localization systems that use the data originating from clients to update their database – either explicitly by manual insertions or implicitly during the localization process – are susceptible to *database manipulation* attacks. More research is needed to provide mechanisms that would protect public (cooperative) WLAN localization systems from such manipulation attacks.

5. DISCUSSION: SECURING PUBLIC WLAN-BASED LOCALIZATION

In this section, we discuss possible solutions for securing public WLAN-based localization systems. The solution space can be divided into solutions for secure data acquisition (i.e., preventing the acquisition of false data) and into calibration of already acquired data in the database (i.e., detection and elimination of false data). Data calibration is required to detect and thwart database manipulation attacks; Skyhook performs data calibration by surveying the age and consistency of data and by periodic scans of outdated areas. In the following, we focus on the technically more challenging solutions for achieving authentication and location verification during the data acquisition.

The first observation we make is that the localization beacons of WLAN access points can be easily forged and replayed. Traditional authentication mechanisms would not help much here, because they would require software modifications at the access points, which are not under the control of the service provider (Skyhook). Furthermore, even if appropriate modifications would be made to the access points and AP beacons would be properly authenticated, WPS would still be vulnerable to jamming and wormhole-based [20] signal relay attacks [23, 47]. To prevent relay (wormhole) attacks, the access points and the localized nodes (LNs) would therefore need to mutually authenticate their communication and would either need to be tightly time synchronized, or use challenge-response protocols with accurate (i.e., *ns*) time measurements [6]; both would require significant hardware and software modifications to both the access points and the LNs.

Given that such modifications of access points and LNs are not feasible in public WLAN positioning systems, authentication of access point beacons needs to be done in a manner that does not require any pre-shared cryptographic material between the APs and the LNs. For this, we propose to use unique AP characteristics such as their *traffic* or *signal fingerprints*. These fingerprints should be difficult to forge and easy to measure (by the LNs); if they are not, APs could be impersonated in the same manner as in the WPS system that uses (easily forgeable) MACs as device identifiers. Equally, traffic and signal fingerprints of APs need to be chosen such that they are unique or mutually distinguishable with high probability. Since access points do not cooperate in fingerprint extraction with the LNs or with the system provider, the fingerprints also need to be easily measurable by the provider to build the LLT database and by the LN for AP identification.

Assuming that such AP fingerprints can be measured by the LNs, our fingerprint-enhanced WPS would therefore work in the following manner. The service provider measures the fingerprint data of the APs using appropriate software and/or hardware, and stores it in the LLT along with the MAC addresses and RSS values for each access point; as a side effect, manual user input, which represents a source of false information, would be precluded. During the localization, the fingerprint-enhanced LNs measure the fingerprint data from the surrounding APs and report this data along with the MAC addresses and signal strengths to the service provider that, in turn, compares it to the data in the LLT. Based on a probabilistic analysis, the service provider returns the location information which is then used by the LN to compute its position. If the analysis fails, i.e., if the fingerprint data does not correspond to the stored data up to a pre-defined degree, possibly indicating an attack, no location information is returned. Alternatively the most likely position could be returned along with a warning that the location could not be verified. This could be presented to the user as, say, a red circle instead of a blue.

Recently, a number of results have emerged that show how unique characteristics of WLAN access points and of other wireless devices can be measured. One way of identifying access points is by collecting data specific to their configuration or model. The feasibility of this approach was recently discussed in [7]. This approach does neither require hardware modification of the LN device nor changes on the scanned access points, but instead relies on characteristic behavior of different AP models on malformed 802.11 frames. Although this does not completely prevent location-spoofing attacks, it makes them more difficult since the attacker has to extract AP device specific data in order to compose adequately forged response frames. This would require his prior physical presence at the access point whose location is to be spoofed. In [36, 44], the authors discuss signal fingerprints based on physical characteristics of individual device radios. The process of collecting these fingerprints requires specialized hardware which would have to be added to the LN devices. Signal fingerprints would prevent attacks by attackers using off-the-shelf hardware, but would not prevent a sophisticated attack by an attacker that samples and replays the signals on the physical layer. Spoofing fingerprints based on physical characteristics of the transmitted signal requires a high frequency sampling oscilloscope with a sample frequency at least as high as the fingerprinting hardware in the LNs. In addition, an attacker would need an arbitrary waveform generator capable of reconstructing the sampled signal without adding any distortion or noise. This is very hard because the oscilloscope, waveform generator, and controlling computer all have finite dynamic ranges, i.e., they can only represent the captured signal in steps. These hardware requirements make signal fingerprints much harder to forge than behavioral fingerprints. The usability of the fingerprint-enhanced WPS stimulates further research on identifying nonforgeable and easily measurable AP fingerprints.

Another technique for detecting and preventing location spoofing in WPS is by geo-locating the IP address of the AP that is used to query the location database. Although this information is relatively coarse and can be spoofed using IP tunneling, it can be used to make simple location spoofing attacks at larger distances (e.g., to different countries) more difficult.

6. RELATED WORK

In the last decade, a number of outdoor localization systems for mobile devices were proposed and implemented, based on satellite communication (GPS [15]), cellular networks (GSM), Wi-Fi networks or specialized platforms [5, 9, 12, 19, 35, 50, 51]. These techniques differ in terms of accuracy, reliability, and hardware requirement. Positioning techniques were also extended and used for positioning in wireless ad-hoc networks [8, 10, 29, 30, 39, 46].

Later security analysis has shown many of these systems or underlying technologies to be vulnerable to attacks [27, 28, 32, 33, 52]. Proposals followed that aim at securing GPS [21]. Furthermore, several proposals have been made to improve the security in WLAN-based localization. However, all of these solutions require the cooperation of the APs [32–34, 42].

To secure systems not based on WLAN, several secure ranging and secure localization systems were proposed in the open literature. The first secure ranging protocol was described in [6]; this protocol was later applied to a wireless scenario and extended to provide mutual authentication in [45]. To allow more resource constrained devices to perform secure ranging in noisy environments, Hancke and Kuhn proposed an alternative protocol in [17]. This paper also discussed possible implementations of secure ranging in hardware. An authenticated ranging protocol for wireless devices was proposed in [49]. Attacks on possible implementations of secure ranging protocols were discussed in [18].

A system for secure localization was proposed in [38], based on ultrasonic and radio wireless communications; this system is limited by the use of ultrasonic signal, which requires that no attackers are present in the area of interest as demonstrated in [40]. Kuhn [21] proposed an asymmetric security mechanism for navigation signals, based on hidden message spreading codes. Čapkun and Hubaux [47, 48] propose a secure localization technique called verifiable multilateration, based on secure ranging, which further enables a local infrastructure to verify positions of the localized devices. Authenticated ranging and secure localization (verifiable multilateration) were implemented in [43]. In [49], Čapkun et al. propose a location verification scheme based on hidden and mobile base stations.

Lazos et al. [22] proposed a technique for secure positioning of a network of sensors based on directional antennas. Lazos et al. [23] propose an extension of this technique that copes with jamming and replays of localization signals. In [37], the authors propose and implement a system for broadcast localization and time-synchronization, based on navigation signal encoding, that prevents signal replay and time-shift attacks. Li et al. [24] and Liu et al. [25] propose statistical methods for securing localization in wireless sensor networks.

To the best of our knowledge, this work is the first that analyzes the security of public WLAN positioning systems and the first that demonstrates the implementation of location spoofing attacks in WLAN networks. Equally, we are unaware of any prior work that discusses location database manipulation attacks.

7. CONCLUSION

In this work, we studied the security of public WLAN-based positioning systems. Specifically, we investigated the Skyhook positioning system [41], available for PCs and used on a number of mobile platforms, including Apple's iPod touch and iPhone [1]. We demonstrated that this system is vulnerable to location spoofing and location database manipulation attacks. By demonstrating these attacks, we showed the limitations of Skyhook and similar public WLAN-based positioning systems, in terms of the guarantees that they provide and the applications that they can be used for. Given the relative simplicity of the described attacks, we conclude that, without appropriate modifications, these positioning system cannot be used in security- and safety-critical applications. We further discussed approaches for securing public WLAN positioning systems and we call for more research on the development of usable and secure public positioning solutions, based e.g., on access point signal fingerprints.

8. REFERENCES

[1] Apple Inc. http://www.apple.com.

[2] GNU Radio: The gnu software radio. http://gnuradio.org/trac.

[3] Google earth. http://earth.google.com.

[4] Loki Mobile applet for Nokia phones using Symbian. http://loki.com/download/mobile.

[5] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building RF-Based User Location and Tracking System. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, volume 2, pages 775–784, 2000.

[6] S. Brands and D. Chaum. Distance-bounding protocols. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology (EUROCRYPT)*, pages 344–359. Springer, 1994.

[7] S. Bratus, C. Cornelius, D. Peebles, and D. Kotz. Active behavioral fingerprinting of wireless devices. In *Proceedings of the ACM Conference on Wireless Security (WiSeC)*, 2008.

[8] N. Bulusu, J. Heidemann, and D. Estrin. GPS-less low cost outdoor localization for very small devices. *IEEE Personal Communications Magazine*, 7(5):28–34, October 2000.

[9] P. Castro, P. Chiu, T. Kremenek, and R. Muntz. A Probabilistic Room Location Service for Wireless Networked Environments. In *Proceedings of the International Conference Atlanta Ubiquitous Computing (Ubicomp)*, volume 2201. Springer-Verlag Heidelberg, September 2001.

[10] L. Doherty, K. Pister, and L. El Ghaoui. Convex position estimation in wireless sensor networks. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, April 2001.

[11] Ettus. Universal software radio peripheral (USRP). http://www.ettus.com.

[12] R.J. Fontana, E. Richley, and J. Barney. Commercialization of an ultra wideband precision asset location system. *Ultra Wideband Systems and Technologies, 2003 IEEE Conference on*, pages 369–373, 2003.

[13] Fraunhofer IIS. Press release, autonomous WLAN positioning system. http://www.fraunhofer.de/EN/press/pi/2008/01/Presseinformation14012008.jsp, 2008.

[14] S. Ganu, A. Krishnakumar, and P. Krishnan. Infrastructure-based location estimation in WLAN networks. In *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, march 2004.

[15] I. Getting. The Global Positioning System. *IEEE Spectrum*, December 1993.

[16] Y. Gwon, R. Jain, and T. Kawahara. Robust indoor location estimation of stationary and mobile users. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, march 2004.

[17] G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. In *Proceedings of IEEE Conference on Security and Privacy in Communication Networks (SecureComm)*, pages 67–73. IEEE Computer Society, 2005.

[18] G. Hancke and M. Kuhn. Attacks on 'Time-of-Flight' Distance Bounding Channels. In *Proceedings of the ACM Conference on Wireless Security (WiSeC)*. ACM, 2008.

[19] J. Hightower, G. Boriello, and R. Want. SpotON: An indoor 3D Location Sensing Technology Based on RF Signal Strength. Technical Report 2000-02-02, University of Washington, 2000.

[20] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, San Francisco, USA, April 2003.

[21] M. Kuhn. An asymmetric security mechanism for navigation signals. In *Proceedings of the Information Hiding Workshop*, 2004.

[22] L. Lazos and R. Poovendran. SeRLoc: secure range-independent localization for wireless sensor networks. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, pages 21–30. ACM, 2004.

[23] L. Lazos, R. Poovendran, and S. Čapkun. ROPE: robust position estimation in wireless sensor networks. In *Proceedings of the symposium on Information processing in sensor networks (IPSN)*. IEEE Press, 2005.

[24] Z. Li, W. Trappe, Y. Zhang, and B. Nath. Robust Statistical Methods for Securing Wireless

Localization in Sensor Networks. In *Proceedings of the symposium on Information processing in sensor networks (IPSN)*, 2005.

[25] D. Liu, P. Ning, and W. Du. Attack-Resistant Location Estimation in Sensor Networks. In *Proceedings of the symposium on Information processing in sensor networks (IPSN)*, 2005.

[26] Mexens LLC. Navizon virtual GPS service. http://www.navizon.com.

[27] U. Meyer and S. Wetzel. A man-in-the-middle attack on UMTS. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, pages 90–97, 2004.

[28] C. Mitchell. The security of the GSM air interface protocol. Technical report, Technical Report RHUL-MA-2001-3, Royal Holloway University of London, 2001.

[29] D. Moore, J. Leonard, D. Rus, and S. Teller. Robust distributed network localization with noisy range measurements. In *Proceedings of the ACM Conference on Networked Sensor Systems (SenSys)*, pages 50–61. ACM Press, 2004.

[30] D. Niculescu and B. Nath. Ad hoc positioning system (APS) using AoA. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, San Francisco, USA, April 2003.

[31] S. Pandey and P. Agrawal. A survey on localization techniques for wireless networks. *Journal of the Chinese Institute of Engineers*, 29(7):1125–1148, 2006.

[32] S. Pandey, F. Anjum, and P. Agrawal. *TRaVarSeL–Transmission Range Variation based Secure Localization*, pages 215–236. 2007.

[33] S. Pandey, F. Anjum, B. Kim, and P. Agrawal. A low-cost robust localization scheme for WLAN. In *Proceedings of the International Workshop on Wireless Internet*, New York, NY, USA, 2006. ACM.

[34] S. Pandey, B. Kim, F. Anjum, and P. Agrawal. Client assisted location data acquisition scheme for secure enterprise wireless networks. *Wireless Communications and Networking Conference, 2005 IEEE*, 2:1174–1179 Vol. 2, 13-17 March 2005.

[35] N. B. Priyantha, A. Chakraborty, and H. Balakrishnan. The Cricket location-support system. In *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, pages 32–43. ACM Press, 2000.

[36] K. B. Rasmussen and S. Čapkun. Implications of radio fingerprinting on the security of sensor networks. In *Proceedings of IEEE Conference on Security and Privacy in Communication Networks (SecureComm)*, 2007.

[37] K. B. Rasmussen, S. Čapkun, and M. Čagalj. SecNav: secure broadcast localization and time synchronization in wireless networks. In *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, pages 310–313. ACM, 2007.

[38] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, pages 1–10. ACM, 2003.

[39] A. Savvides, C.-C. Han, and M. B. Strivastava. Dynamic fine-grained localization in Ad-Hoc networks of sensors. In *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*, pages 166–179. ACM Press, 2001.

[40] S. Sedihpour, S. Čapkun, S. Ganeriwal, and M. Srivastava. Implementation of Attacks on Ultrasonic Ranging Systems, demo at ACM SENSYS'05, 2005.

[41] Inc. Skyhook. . http://www.skyhookwireless.com.

[42] P. Tao, A. Rudys, A. M. Ladd, and D. S. Wallach. Wireless lan location-sensing for security applications. In *Proceedings of the ACM Workshop on Wireless Security (WiSe)*, pages 11–20, 2003.

[43] N. O. Tippenhauer and S. Čapkun. UWB-based Secure Ranging and Localization. Technical Report 586, ETH Zurich, January 2008.

[44] O. Ureten and N. Serinken. Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering*, 32(1):27–33, 2007.

[45] S. Čapkun, L. Buttyan, and J.-P. Hubaux. Sector: Secure tracking of node encounters in multi-hop wireless networks. In *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, October 2003.

[46] S. Čapkun, M. Hamdi, and J.-P. Hubaux. GPS-free Positioning in Mobile Ad-Hoc Networks. *Cluster Computing*, 5(2), April 2002.

[47] S. Čapkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, volume 3, pages 1917–1928, 2005.

[48] S. Čapkun and J.-P. Hubaux. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):221–232, February 2006.

[49] S. Čapkun, M. Čagalj, and M. Srivastava. Secure localization with hidden and mobile base stations. In *Proceedings of the IEEE Conference on Computer Communications (InfoCom)*, pages 1–10, April 2006.

[50] R. Want, A. Hopper, V. Falcao, and J. Gibbons. The Active Badge Location system. *ACM Transactions on Information Systems*, 10(1), 1992.

[51] A. Ward, A. Jones, and A. Hopper. A New Location Technique for the Active Office. *IEEE Personal Communications*, 4(5), October 1997.

[52] J. S. Warner and R. G. Johnston. Think GPS Cargo Tracking = High Security? Think Again. *Technical report, Los Alamos National Laboratory*, 2003.

[53] WiGLE. Wireless Geographic Logging Engine. http://wigle.net/.