PREVENTION OF LOCATION-SPOOFING
A Survey on Different Methods to Prevent the Manipulation of Locating-Technologies

Michael Decker
Institute AIFB, University of Karlsruhe (TH), Kaiserstr. 89, 76 128 Karlsruhe, Germany

Keywords: Location-based Services (LBS), Location-Spoofing, Mobile Computing Security, Positioning.

Abstract: There are many different locating technologies to determine a mobile device's current position. Examples for such technologies are the satellite-based Global Positioning System (GPS), the cell-ID method in mobile phone networks or WLAN-based approaches. These technologies are the enabler of so called *Location-based Services* (LBS): LBS are services to be used with mobile handheld-computers like PDAs or smartphones that evaluate a mobile user's position. When locating-technologies are discussed in the LBS community, the focus is often on the accuracy of the calculated location whereas the resistance to manipulation attempts by the possessor of the mobile device or by third-parties is almost never considered. But there are examples of LBS where users or external attackers might have an incentive to manipulate the locating system. This is termed as *location spoofing*. This article presents a survey of different technical approaches to prevent or at least to detect location spoofing.

1 INTRODUCTION

Location-based Services (LBS) are services for mobile handheld-computers which evaluate the location of at least one mobile device during execution. The standard example for LBS is that of a *Point-of-Interest-Finder* (POI-Finder): such a service guides a user to certain type of facility (e.g. restaurants, petrol stations, ATM) in his nearer surrounding.

LBS are enabled by the possibility to determine the location of a mobile device. This is called *locating*. Nowadays many descriptions for locating methods can be found in literature, see Küpper (2007) for an overview. While in the common considered scenarios for LBS like the above mentioned POI-finder it seems to be quite unlikely that someone has an incentive to manipulate the employed locating system there are several evident examples of LBS for which this isn't the case, e.g. location-aware access control, navigation of military vehicles, location-based billing or geo-fencing.

The term *location spoofing* in literature can refer to the manipulation of a locating system by the possessor of the device[1] (internal attack, e.g. Mundt (2005)) or by an third-party attacker, who is technically not involved in the provisioning of the LBS (external attack, e.g. Warner & Johnston (2003)). In the domain of computer science the term *spoofing* usually refers to faking ones identity, e.g. DNS- or IP-spoofing. Spoofing doesn't include the case of a denial-of-service-attack where the determination of the location is just inhibited or *jammed*; such attacks are noticed by the mobile user or the LBS provider as failure of the locating system. During a spoofing attack the mobile user or service provider obtains a faked location statement but isn't aware that the location was faked, so spoofing is more dangerous than just jamming.

The purpose of this article is to give a systematic overview of various approaches to prevent location spoofing that are described in literature. Despite extensive literature research we couldn't find a survey article which covers anti-spoofing techniques from the viewpoint of LBS. To facilitate this presentation of all the anti-spoofing-approaches we developed an appropriate classification scheme.

The remainder of the article at hand is organized as follows: Section 2 is devoted to an explanation of basic terms and the introduction of a classification scheme for anti-spoofing-methods. According to this scheme — we call it the *Anti-Spoofing-Tree* —

[1] the possessor of the device isn't necessarily the legal owner, e.g. if the device was stolen or lost

Decker M. (2009).
PREVENTION OF LOCATION-SPOOFING - A Survey on Different Methods to Prevent the Manipulation of Locating-Technologies.
In *Proceedings of the International Conference on e-Business*, pages 109-114
DOI: 10.5220/0002232601090114

the discussion of the identified basic methods to prevent spoofing from section 3 to section 7 is organized. Since GPS is the most popular used locating system we devote section 8 to discuss how GPS is secured against spoofing. The article ends with the obligatory summary and outlook in section 9.

2 CLASSIFICATION SCHEME AND BASICS TERMS

During our literature research we identified five basic methods for the prevention of location spoofing which can be found at the second level of the classification tree depicted in figure 1: Plausibility checks, tamperproof hardware, location keys, request-response-protocols and radio technology methods. The further subclassifications shown in the figure are covered in the corresponding sections in this paper.

One kind of attack that is relevant for several locating systems is the so called *rerouting attack* (also called *wormhole attack*): the principle is that a signal or message is received at a particular location and then transmitted (maybe using another medium) to another location, where it is emitted. A perfect rerouting attack can only be detected by the latency (time lag) it induces. Another similar attack is the *replay attack*: for such an attack the signal is recorded and replayed (maybe several times) with a deliberate time lag, maybe at a different location.

3 PLAUSIBILITY CHECKS

When performing a plausibility check on the level of the raw messages (e.g. radio signals) of the locating system we have the possibility to check the absolute or the relative signal strength (Warner and Johnston, 2003). The signals emitted by the GPS satellites reach the earth's surface with a strength of just $-160dBW$. An obvious way to perform an external spoofing attack is to employ earthbound artificial satellites (so called *pseudolites*) which broadcast faked GPS signals with a much higher signal level and thus overcast the genuine signals from the satellites. This attacks can be detected by checking the absolute signal strength of the received signals. More sophisticated attacks can only be detected by paying attention to relatively weak increase of the received signal strength. There is another plausibility check method based on the specific features of GPS: for GPS the approximate trajectories of the satellites for the next few months are published in advance over the internet (so called *almanac*). So the GPS receiver should check if the satellites he currently receives at his alleged location conforms to those listed in the almanac.

A plausibility check can also be performed when the locating system already calculated the position of the mobile device based on the received raw messages: In many scenarios there will be several location determinations at different time points so it can be checked if the mobile device moves with a reasonable velocity. The route of the mobile device should also be plausible, e.g. there should be no alleged movements through obstacles like walls or buildings. If available the measurements of appropriate sensors designed for dead reckoning (e.g. accelerometer, odometer, barometer, (gyro)compass or speedometer) can be evaluated and checked for concordance with the alleged movement pattern as reported by the primary locating system.

Plausibility checks at the level of the raw messages are primarily applicable for scenarios where the plausibility check should be performed on the mobile device since the raw signals are usually not forwarded to the backend. Checks of the calculated position can be done on the device and on the backend.
It is also possible to have dedicated stations in a locating system for performing plausibility checks, so called *reference stations*. Reference stations are an optional extension of the locating system. For GPS there are several stations all over the world (e.g. in Colorado Springs (USA) or on Ascension Island). These stations know their own position and calculate their location according to the received locating signals. If a significant deviation is detected, this implies a malfunction of the locating system or a spoofing attack. In this case the operator of the locating system and/or the mobile user have to be warned.

However, an external attacker could emit his spoofing signals in a way that they only affect the mobile device but not the reference station. Therefore in literature the suggestion of hidden reference stations can be found (Capkun et al., 2006), i.e. the locations of the reference stations are kept secret. Since the secret concerning the location of the reference stations might be revealed sooner or later there is further the idea to have mobile reference stations, e.g. motor vehicles equipped with the necessary technical equipment.

4 TAMPERPROOF HARDWARE

From the domain of location-aware digital rights management (DRM) comes the requirement that an end user device should only be able to playback mul-

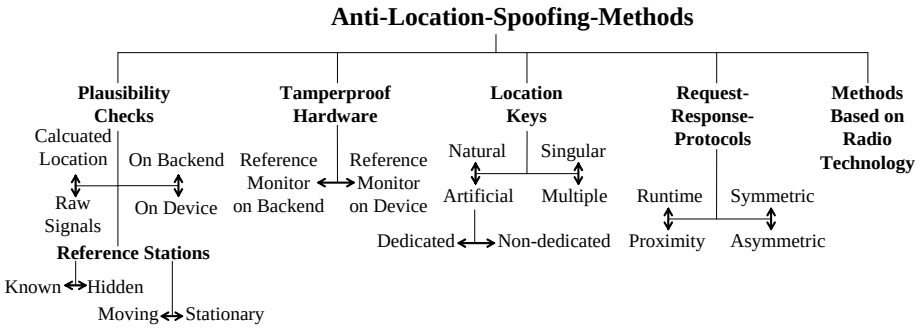

Figure 1: "Anti-Spoofing-Tree": Classification scheme for Anti-Spoofing-Methods.

timedia content (e.g. movies) at particular places (Mundt, 2005). For set-top-boxes for television sets there is even the requirement that the decryption of the broadcasted content should only be possible within the subscriber's private residence but not at public places like restaurants (Gabber and Wool, 1998). In this case the owner of the mobile device is also the potential attacker, so this requires methods for the prevention of internal attacks. This can only be implemented by using a special hardware module that is secured against physical manipulation attempts, so called *tamperproof hardware*. The tamperproof hardware module has to encapsulate the functionalities for locating, for making the decision if at the current location the content should be playbacked or not (the so called *reference monitor*) and the function to decrypt the content.

The system described by Mundt (2005) is based on GPS and also includes a clock that is implemented as tamperproof hardware. He assumes that the signals emitted by the satellites have a time stamp and are digitally signed so the locating module would be able to detect rerouting attacks since rerouting of radio waves leads to an unavoidable time lag. But to detect the time lag caused by rerouting a highly precise clock is necessary, because radio waves travel with light speed so even rerouting over large distances causes a time lag in the order of several milliseconds (e.g. 100 km in $\approx 0,3$ milliseconds). Such highly precise time measurements can only be provided by atomic clocks, but they are too heavy and too expensive so they cannot be integrated into mobile consumer devices. Mundt's system therefore uses a quartz clock that is synchronized with an external time source every couple of hours so it isn't necessary to have a permanent internet connection. For this time synchronization a special cryptographic protocol is used.

For the case that the location information is calculated on the mobile device and then forwarded to the stationary backend of a service provider it can be reasonable to employ tamperproof hardware on the mobile client, too: the tamperproof module in this case not only performs the calculation of the location but also signs the determined location with a private key. With the corresponding public key the service provider then is able to verify the authenticity of the received location information. The private key has to be stored inside the tamperproof module because if an attacker would be able to obtain it he could generate faked location messages with a valid digital signature.

5 LOCATION KEYS

As *location key* we regard information that is only available at particular locations. The mobile user has to forward this information to some backend system as proof that he is actually at the location where he claims to be. This principle is especially suited for cases where the mobile device calculates its location and provides this to the LBS provider but the provider wants to be sure that this calculation wasn't faked.

We distinguish at the first level whether a location key is of either *natural* or *artificial* origin. "Natural" means that the key isn't emitted as result of human activity. For artificial keys we can further distinguish if it is a *dedicated* or a *non-dedicate* key: dedicated keys are generated only for the purpose of the prevention of spoofing while non-dedicated keys are emitted for other purposes and their employment as mean to prevent spoofing is a spin-off effect.

One anti-spoofing system that works with non-dedicated location keys is the so called *CyberLocator* (Denning and MacDoran, 1996). The system was designed to supplement GPS. Using this system the mobile device is equipped with a GPS receiver and thus can determine the position by itself, but it has also to forward the raw signals (radio fingerprint) received from the GPS satellites at the backend. It is not possible to predict the pattern of the raw signals

received at a particular spot on earth's surface at a particular time instant because the signals are affected by many different influences, e.g. by the ionosphere or the weather conditions. The trajectory of the satellites is defined in advance and this information is published in the GPS signals in form of the so called ephemeris and almanac data; however, the actual trajectory of the satellites isn't exactly the one defined in advance and subject to random influences. At the backend the raw signal reported from the mobile device will be compared to those reported by trusted reference stations in the proximity of the alleged location of the mobile device. The authors of the *CyberLocator* paper state that the distance between reference station and mobile device shouldn't be larger than 3.000 kilometres; unfortunately the authors of *CyberLocator* don't explain how they calculated this maximum distance between mobile device and reference station. Also rerouting attacks (see section 2) are considered, i.e. a colluding user that actually stays at the alleged location forwards the received raw signals to the attacker. However, for the *CyberLocator* system it is demanded that the radio fingerprint is forwarded within 5 milliseconds because it is assumed that rerouting would cause additional latency beyond that threshold. It seems quite demanding to meet the maximum latency time of 5 ms even when not performing a rerouting attack, since UMTS-HSPA causes a latency of 150 ms, and even wire-bound internet connections over DSL have a latency of at least 20 ms.

Another system to prevent spoofing is called *Location Aware Access Control* (LAAC) and was devised by Cho and colleagues (2006) . Unlike the *CyberLocator* this system is based on dedicated location keys that are emitted by the base stations of a wireless local area network (WLAN). The location keys are randomly chosen bit sequences which are renewed periodically (e.g. every five seconds). These location keys are reported to the backend system. The mobile device has to combine all the location keys it receives from different base stations within a given timeframe and combine them by using the XOR-function. Afterwards the result of this calculation is then the input for a hash function whose output is the actual location key that has to be transmitted to the backend. Since the backend knows all the current location keys used by the base stations it is able to calculate the hash values like the mobile device to verify the correctness of the received location keys. A further feature of the system is that the radiation angle of the base stations can be controlled by using special antennas. If we have two base stations with a radiation angle of 90° it is possible to arrange these base stations in a way so that the area where the waves of both stations can be received has a rectangular shape. This is an interesting feature to obtain regions that cover the premises of a business like a restaurant, a hotel or a theme park where the currently present customers should be able to access a particular wireless service (e.g. free internet access, special information services). The authors of LAACs don't describe arrangements to prevent rerouting attacks but this has to be interpreted by considering the application scenario that is primarily addressed, namely to restrict free wireless internet access to users staying in a particular area. For rerouting the colluding attackers usually need a fast data transmission connection; however, if this connection is already available there is no need to perform a spoofing attack to gain internet access.

Malaney (2007) proposes a system based for indoor WLANs. The aim of this system is that mobile devices should be able to prove that they are within a building. It is assumed that only authorized people can enter the building (e.g. because there is a gatekeeper) and should have access to the WLAN. The mobile devices have to calculate their position (e.g. based on GPS or a special indoor locating-system) and measure the signal strength of all the WLAN access points they can receive at the current location. These values have to be reported to a central server that makes the decision if the mobile device should get access or not: it is checked if the reported position lies within the building and then if the reported signal strength pattern matches the signal strength pattern for that location. In this scenario the signal strength pattern of the WLAN access points at a particular location can be considered as non-dedicated location key because unauthorized people cannot get into the building to measure the signal strength. There are simulation models to calculate an estimation of a signal strength pattern at a given location; however, to work with these models it is necessary to know the building plan, the locations of the access points and the specific attenuation characteristics of the walls and furniture in the building.

In literature so far no anti-spoofing-approach can be found that is based on natural location keys. However, the cosmic background radiation could act as one because it is receivable at each point of the earth's surface for a given time instant with a specific pattern. A further dimension for the discrimination of location-key methods would be to differentiate between *singular* and *multiple* keys. For singular keys (e.g. CyberLocator) each location key stands for one area while for multiple keys (e.g. Malaney's system) the location keys may overlap for some regions.

6 REQUEST-RESPONSE-PROTOCOLS

The basic principle of request-response-protocols is as follows: the mobile device (prover) receives a request message from a trusted base station (verifier); the message contains a non-predictable random bit sequence (called *nonce*) and the prover has to send a response message that is based on this bit sequence. We distinguish two cases: In **runtime-based protocols** the prover's response message won't arrive in time at the verifier's position if the prover is further away from the prover than alleged because longer distances lead to longer runtimes. If request and response are sent over radio waves it isn't possible to sent a message over a larger distance in the same period of time because radio waves travel at the speed of light ($\approx 3 \times 10^8 m/s$), which constitutes the maximum speed that is possible according to today's knowledge. However, measuring the runtime of radio waves requires extreme precise clocks because the travel time of radio waves for typical application scenarios of locating technologies are very short. In **proximity-based protocols** a prover too far away won't be able to receive the verifier's message because of signal attenuation.

A nice example for a anti-spoofing-system employing a runtime-based request-response-protocol is the one described by Sastry & colleagues (2003): The prover can start the protocol by sending a radio message with his alleged location to the verifier. If the verifier receives this messages and deems itself as responsible for the alleged location he generates a nonce and sends a request message containing this nonce over radio back to the prover; the verifier also starts a precise clock at the time instants he begins to send the request message. When the prover receives the request message he sends back the nonce as response as soon as possible; however, for this way back ultrasonic waves are used instead of radio waves. The verifier will stop the clock when he received the complete response. He verifies that the response indeed contains the nonce and tests if the calculated runtime is small enough for the distance between his location and the alleged location of the prover. The special feature of this protocol is that it uses two different kinds of waves for the transmission of the messages, namely radio waves and ultrasonic waves. This stems from the requirement that the protocol should be robust with regard to particular measurement errors of the messages' roundtrip time, especially the processing time required by the prover to produce the response message. If all the messages would be transmitted over radio these measurement errors would lead to distance inaccuracies that would render the protocol useless for the purpose of prevention location spoofing. That's why ultrasonic waves are used for the transmission of the response message. Ultrasonic waves travel at a velocity that is six orders of magnitude smaller than lightspeed ($331 m/s$), so a measurement error of 0.1 seconds results only in a distance error of ≈ 33 meters, while for radio waves the distance error would be ≈ 30.000 *km* for the same time span. A distance error of 33 meters should be acceptable even for most indoor locating scenarios. Since the speed of ultrasonic waves is relatively low the return way of the nonce is prone to a rerouting attack with an out-of-band-transmission over radio waves; this is why the authors of this protocol opted to use the ultrasonic waves for the response message and not for the request message because in their opinion it requires much more effort to perform a rerouting attack for the response message than for the request message.

Waters & Felten (2003) describe another request-response-protocol for the prevention of location spoofing that is based on runtime measurements. However, in their protocol radio waves are used for all message exchanges. To discern protocols that use one kind of wireless waves from protocols that use different kind of waves we further introduce two further sub-classes of request-response protocols that are mutual exclusive, namely *symmetric* respective *asymmetric* protocols.

An example of a request-response-protocol based on proximity (i.e. without measuring the runtime of signals) can be found in Vora et al. (2006). In their system several verifiers are installed within a particular target region. The system's purpose is to detect mobile clients who falsely claim they are within that target region. To make the system more secure there are so called *rejection verifiers* outside the target region; if one of them receives a signal from a prover the verifier is considered as spoofer.

7 RADIO TECHNOLOGY

There are special approaches concerning the radio technology employed for locating systems that can help to prevent spoofing attacks:

Spreading of Frequence Spectrum. The basic principle of spread spectrum techniques is to transform a narrow-banded signal into a signal with a broader bandwidth. It requires more effort to jam or forward a broadbanded radio signal than a narrow-banded one. Examples for spread spectrum methods are *Frequence Hopping Spread Spectrum* (FHSS) and *Direct Se-*

quence Spread Spectrum (DSSS). A simple form to spread signals is to assign a different frequency to each sender like for GLONASS: in this system each satellite broadcasts on his own frequency.

Manchester-Coding. For an attacker it is usually harder to eliminate a set bit in a radio message than to set an unset bit. Therefore the idea of the so called *Manchester-Coding* is to replace each bit of the original message by two bits. This coding is done in a way that also unset bits are mapped to codewords with set bits, so an attacker who cannot "delete" bits isn't able to alter the navigation message in a consistent way.

Another approach in this class is to use multiple antennas at a station or device to detect if signals are arriving from the wrong direction.

8 ANTI-SPOOFING FOR GPS

All of the nominal 24 satellites of the GPS-system emit signals carrying navigation messages on the same two radio frequencies called $L1$ and $L2$. The navigation messages contain amongst other things the identification number of the satellite that produced the message and parameters to describe the trajectories of the individual satellites. The *code division multiple access (CDMA)* method is used to encode the messages so a receiver is able to obtain the message of a single receiver. For CDMA the messages are encoded using a spread code sequence. The GPS has two types of such code sequences (Küpper, 2007): The Coarse Acquisition Code (C/A-code) is for the *Standard Positioning Service (SPS)*, which can be used by civilian users; it is only broadcasted on the $L1$ frequency. The Precise Code (P-code) is for the *Precise Positioning Service (PPS)* that should only be accessible by military users. It is possible to use a secret Y-key to obtain the P(Y)-code. The P-code is broadcasted on both frequencies and can be considered as symmetric key because for encryption and decryption the same key is used. If someone wants to perform a GPS-spoofing-attack including the PPS he has to know the secret Y-key. This means that the secret key has to be stored in all military GPS receivers that are intended to use the PPS. If only one of this receivers is compromised (e.g. gets lost or is stolen) the whole systems gets prone to spoofing attacks. To prevent this the Y-key is replaced every 24 hours (rekeying). Nowadays techniques are available to benefit from the higher locating accuracy provided by the PPS messages even if the secret Y is not known, e.g. so called *kinematic or codeless receivers*.

9 CONCLUSIONS: SUMMARY AND OUTLOOK

In the article we gave a survey on different methods to prevent the manipulation of location-methods which was based on a classification schema. Since there is a large variety of different attack methods as well as anti-spoofing-methods it is not possible to recommend a single approach for the prevention of location-spoofing; rather the decision for one or more spoofing-prevention-techniques has to be made after an analysis of the respective application scenario and its specific security threats and requirements.

REFERENCES

Capkun, S., Cagalj, M., and Srivastava, M. (2006). Secure localization with hidden and mobile base stations. In *Proceedings of IEEE INFOCOM 2006*, pages 1–10.

Cho, Y., Bao, L., and Goodrich, M. T. (2006). LAAC: A Location-Aware Access Control Protocol. In *Mobile and Ubiquitous Systems*, pages 1–7.

Denning, D. E. and MacDoran, P. F. (1996). Location-Based Authentication. *Computer Fraud & Security*, 1996(2):12–16.

Gabber, E. and Wool, A. (1998). How to prove where you are. In *ACM Conference on Computer and Communications Security*, pages 142–149.

Küpper, A. (2007). *Location-based Services*. John Wiley & Sons, Chichester, U.K.

Malaney, R. A. (2007). Securing Wi-Fi Networks with Position Verification (Extended Version). *International Journal of Security Networks*, 2(1-2):27–36.

Mundt, T. (2005). Location Dependent Digital Rights Management. In *ISCC 2005*, pages 617–622.

Sastry, N., Shankar, U., and Wagner, D. (2003). Secure Verification of Location Claims. In *2nd ACM Workshop on Wireless Security*, pages 1–10, San Diego, USA.

Vora, A. and Nesterenko, M. (2006). Secure Location Verification using Radio Broadcast. *IEEE Transactions on Dependable and Secure Computing*, 3(4):377–385.

Warner, J. S. and Johnston, R. G. (2003). GPS Spoofing Countermeasures. Technical Report LAUR-03-6163, Los Alamos National Laboratory (USA).

Waters, B. R. and Felten, E. W. (2003). Secure, private proofs of location. Technical Report TR-667-03, Princeton University.