ON THE SECURITY OF LOCATION DETERMINATION AND VERIFICATION METHODS FOR WIRELESS NETWORKS

Günther Lackner
Institute for Applied Information Processing and Communications, Inffeldgasse 16a, Graz, Austria

Keywords: Wireless Networks, Location Awareness, Access Control, Location Determination, Location Verification.

Abstract: Location awareness in wireless networks could improve existing security systems. Access control or intrusion detection mechanisms would greatly benefit if reliable location information of connected devices was available. This article describes and classifies relevant location determination and location verification approaches.Further on, it validates their applicability, performance and security properties in the aspect of their possible integration into security relevant systems.

1 INTRODUCTION

The nature of radio propagation makes it possible to attack wireless networks from outside the established perimeter protection such as building security. As a result, the general approach is to secure these infrastructures by cryptographic measures and therefore all state-of-the-art wireless computer network technologies provide strong cryptographic mechanisms.

As history shows, attackers can fool many of these concepts by simply bypassing them. Passwords and digital certificates could be stolen or lost and legitimate users may be tricked by social engineering techniques into revealing their authentication credentials. As a consequence, wireless network security should not rely solely on cryptographic measures.

The introduction of *location awareness* into wireless intrusion prevention systems could bring existing building access restrictions into play. The network may then deny or limit connections to clients which are not in legitimate locations. Potential attackers would need to intrude the perimeter or spoof their location to gain full access to the infrastructure.

2 LOCATION DETERMINATION METHODS

Location determination in wireless networks has found a number of fields of application in recent years. Besides security related topics, context-aware computing in general is highly dependent upon location information. Especially in indoor environments or areas with a high density of elevated buildings classic positioning systems like GPS are not reliable. Alternative methods need to take their place.

2.1 Client or Infrastructure based Methods

2.1.1 Client based Methods

This class of methods is characterized by the fact, that the location determination process is carried out fully by the device being located. The work load of data collection and position computation is handled by the device alone and presents no additional burden for the network infrastructure. This property promises good scalability and a decent base for many kinds of location based services. However, mobile devices with limited power and computational resources could be disadvantaged by this architecture. Many client-based positioning solutions are based on an agent-server architecture. An autonomous agent is installed on all participating clients. Its purpose is to collect necessary data as signal strength values or time measurements and compute the current location of the client by using this information.

Advantages. The computational load can be spread over the clients and does not burden the infrastructure. This scenario finds application in ad-hoc networks like wireless sensor networks which are often based on trust level models (Fernandez-Gago et al., 2007).

Lackner G..
ON THE SECURITY OF LOCATION DETERMINATION AND VERIFICATION METHODS FOR WIRELESS NETWORKS.
DOI: 10.5220/0003496302630268
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2011), pages 263-268
ISBN: 978-989-8425-71-3

Disadvantages. As the client is responsible for the location determination it is easy to spoof the result. As this describes client only methods, the infrastructure is not allowed to participate in the process and provide for example location verification.

Comments. From a security point of view, these methods do have a significant weakness as they rely on the collaboration of the client who could be malicious. As attackers are usually not cooperative, these methods are not suitable to be part of a robust security solution (Kraxberger et al., 2010).

2.1.2 Infrastructure based Methods

In contrast to *client based methods*, *infrastructure-based approaches* work without any collaboration and generally even without any notice by the connected clients. Besides the favorable conditions for mobile devices these methods do have a good suitability to be part of a network security architecture (Kraxberger et al., 2010).

Advantages. The network infrastructure alone is responsible for determining the clients location. No collaboration and computational power by the client is needed. This is an important advantage if low power mobile devices are included in the scenario.

Disadvantages. By using infrastructure based methods, the system cannot use additional information provided by the clients, such as GPS signals or scene related data such as the proximity to signal beacons. This could result in a decrease of performance and flexibility.

Comments. The just described approach is generally more suited to be implemented in security related architectures than client based ones. It is considered robust against attacks by malicious clients as the overall security mainly relies on the used physical location-determination method.

Hybrid Methods. Hybrid methods generally rely on collaboration between the client and the infrastructure. The location determination process may be carried out by the client and the infrastructure is able to verify the client's position claim by some means. This process is called location verification and will be discussed in Section 3.

Advantages. The burden of collecting data and computing the location can be shared between the client and the infrastructure. Hybrid methods generally provide more flexibility than client or infrastructure based approaches.

Disadvantages. Due to the required information provided by the client, hybrid methods may be less robust against attacks than infrastructure based methods.

Comments. Hybrid methods can combine the advantages of infrastructure and client based approaches. The slight rise in complexity provides a gain in flexibility by preserving a high degree of security.

2.2 Triangulation or Trilateration

Lateration and angulation are geometrical techniques based on measured signal and communication properties. The accuracy of this data is vital to carry out reliable location determination. In indoor environments this accuracy is not only influenced by the precision of the used hardware, but also by radio propagation properties such as *multipath propagation* and a low probability for availability of *line-of-sight*.

2.2.1 Triangulation

As the name *triangulation* hints, this concept is based on the geometric properties of the triangle. By determining the *Direction of Arrival* of a signal, from at least two different points of view (in two dimensional space), which are not located on a straight line to the target, one can calculate an intersection an thus locate the source of this signal.

Advantages. Triangulation based methods are very robust against all kinds of location attacks. The location determination can easily be carried out in real time and without any a priori measurements or computations.

Disadvantages. The main disadvantage is the need of directional antennas to determine the direction of the client's signal. In non-line-of-sight scenarios, RF signal propagation features as multipath propagation, can seriously downgrade the performance.

Comments. If the determination process is carried out by the infrastructure, triangulation methods prove very robust against all kinds of location attacks (Capkun and Hubaux, 2006). Due to their need for directional antennas, they turn out to be cost intensive.

2.2.2 Trilateration

Similar to triangulation, the concept of *trilateration* is also based on the geometric properties of the triangle.

Instead of determining the angles between the source and the observation points, one measures the distance between them. This approach requires at least three points for measurement in two-dimensional space.

The process of distance measurement could be based on different wireless communication properties such as *Time of Arrival - TOA* or *Received Signal Strength - RSS*. State-of-the-art IEEE 802.11 hardware only provides a resolution of 1 microsecond in the time-domain. Due to the fact that the RF signal is traveling with light-speed, this resolution cannot be used to carry out distance measurements in the standard range of WiFi networks which is generally below 100 meters. Upcoming technologies as IEEE 802.11n could provide timing resolutions up to 1 nano second and therefore allow precise location determination based on signal traveling times.

Advantages. Trilateration can be based on various communication properties, leaving it a very flexible method. If RSS values are used, generally no special purpose hardware is needed as most wireless devices register the signal strength of incoming transmissions.

Disadvantages. If attackers use amplifiers or directional antennas they can easily spoof their location if no countermeasures, such as anomaly detection, are applied. Since multiple sensors at different locations are needed for RSS trilateration, it is not suitable for client based implementations. Similar to triangulation, signal distortions like multipath propagation can downgrade the performance of this method, as they disrupt the proportionality of signal strength and distance.

Comments. Trilateration techniques are very flexible as they can be based on various signaling and communication features. As generally no special purpose hardware is needed, they can be implemented at a low cost. If lateration methods are implemented without any additional security improvements, they are easy to deceive and not appropriate for security related applications.

2.3 Scene Analysis

RF-based *Scene Analysis* can be seen as a kind of *Location Fingerprinting* where various communication and signal features of certain locations or areas are collected and combined. These combined datasets need to be collected and stored in a system *a priori*. To determine one's location, it is necessary to collect these same features, combine them in the exact same way and try to match or approximate the outcome with the formerly created datasets (Liu et al., 2007). A common example of these RF features is the usage of received signal strength (RSS) values and process them into a map.

Advantages. Very robust against attacks with directional antennas and signal amplifiers. Generally no special hardware is needed. No complex computations are needed for the location determination process.

Disadvantages. RSS maps are needed for each sensor device. They have to be created a priori and require frequent recalibrations.

Comments. RSS based scene analysis can be seen as an advancement of simple trilateration as it proves more resistant against signal distortions if more RSS maps are superposed. Anomaly detection mechanisms can easily be deployed, checking the plausibility of RSS values. This is a powerful tool against directed antennas and signal amplifiers. Nevertheless, this method is not sufficiently robust against location attacks.

2.4 Proximity based

Proximity based techniques are the most basic approaches in location determination. They provide relative location information in a symbolic manner. *Landmarks* with well known coordinates, like base stations of the wireless network, represent points in a virtual grid over the environment. The distance between these *landmarks* represent the resolution of the location determination process based on this network. *Proximity based* techniques are simple to implement and can be integrated with different types of physical media such as infrared radiation (IR), bluetooth, ultrasound and radio frequency identification (RFID). An example is the deployment of IR beacons in every room of a building. These beacons could transmit their ID which is only receivable within their deployment area.

Advantages. This approach is generally very easy to implement if existing network infrastructure is used for cell identification. IR and ultrasound are usually delimited by room boundaries allowing these approaches to reach precision on the room level.

Disadvantages. Infrastructure has to be deployed finely grained for higher precision. The distribution of the base stations define the resolution of the location determination.

Comments. Proximity based methods can be based on low cost hardware such as IR, ultrasound or Bluetooth beacons, allowing their cheap implementation. In order to be part of a security relevant system, they need to be combined with a location verification approach.

An alternative application for proximity based systems are *public WLAN-based positioning systems* (WPS). WPS uses existing wireless access-points and a database holding their geodetic positions. A client reports all currently received SSIDs to the system which uses a *multiple nearest-neighbor* approach to interpolate the possible position of the client.

3 LOCATION VERIFICATION

A major concept in this field is the *verification of location claims*. It is described best by an example: A certain *device R* claims to be located in a certain *area A*. This area can be a single room or even a building. Every device located in this very area should be granted access to a specific resource whereas devices that are out of its boundaries must not get access. The network infrastructure provides a *verifier v*. An entity that is able to validate the claim of R according to the *in-region verification problem* (Sastry et al., 2003).

Location verification can be used to extend location determination methods and improve the security and reliability. In some cases it may work without requiring a dedicated location determination method and be the base for a security related system. The next sections present popular research and implementations in the field of location verification.

3.1 Distance-bounding Protocols

Stefan Brands and David Chaum proposed the first solution to the problem of *verifying the distance of a prover to a verifier* (Brands and Chaum, 1993) in 1994 by presenting the *distance bounding protocol*. It is based on the timing delay between sending out a challenge and receiving back the corresponding response. In the following, Srdjan Čapkun et al. (Capkun et al., 2003) extended the protocol to SECTOR, a mutual authentication protocol using distance bounding. As vulnerabilities to this protocol have been discovered, Dave Singelee and Bart Preneel of the K.U. Leuven presented modifications to render it secure against the so called *terrorist fraud attacks*(Singelee and Preneel, 2005). Another solutions, similar to the approach of Singelee and Preneel has been published by Laurent Bussard (Bussard, 2004). In 2006, it was again Srdjan Čapkun, this time with Jean-Pierre Hubaux (Capkun and Hubaux, 2006), who advanced this distance-bounding location verification by pairing it with multilateration. They assume that an increasing number of verifiers also increases the trustworthiness of a location claim as an attacker needs to trick all verifiers at the same time and with coherent spoofs. In 2010, Rasmussen and Čapkun demonstrated a practical implementation of a distance bounding protocol (Rasmussen, 2010). The implementation used custom hardware with sub-nanosecond processing delay, and provided a precision of approximately 15cm.

Advantages. The distance bounding protocols measure the propagation delay of radio waves. Since these waves travel at the speed of light, an attacker is not able to mount a distance reduction attack. Furthermore, some of the proposed protocols cryptographically bind the distance bound to the prover , so that even man-in-the-middle attacks are unfeasible.

Disadvantages. Distance bounding protocols are extremely sensitive to processing delays. A processing delay of 1ns adds approximately 30cm to the distance bound. A practical implementation of such a protocol thus requires extremely fast hardware.

Comments. Distance bounding protocols are robust against distance reduction attacks. However, such protocols require fast hardware, so they may not be suitable for implementation in current network deployments. As an example, the 802.11 standard with the a/b/g amendments has a time resolution of 1μs, which corresponds to a distance error of approximately 300m.

3.2 The Echo Protocol

Naveen Sastry et al. (Sastry et al., 2003) from the University of California, Berkeley developed the *Echo Protocol* in 2003. The *Echo Protocol* is extremely lightweight, and it does not require time synchronization, cryptography or very precise clocks. It is well suited for use in small, cheap, mobile devices. The location determination process requires RF and ultrasound transceivers. The protocol is similar to the RF based distance bounding protocol, the difference is that the response from the prover to the verifier is transmitted as ultrasound rather than RF. Since ultrasound travels at a much slower speed than light, this approach allows for a higher degree of precision when the processing time makes RF based protocols unreliable. The *Echo Protocol* is

vulnerable to distance reduction attacks if the attacker is able to connect to an ultrasound transceiver, e.g. a speakerphone, inside the controlled area. Using a speed of light physical medium, e.g. RF, to connect to an ultrasound transceiver inside the controlled area violates one of the fundamental assumptions of the *Echo Protocol*.

Advantages. The *Echo Protocol* requires no pre-established trust relationship between the prover and verifier. It is extremely lightweight, and thus suitable for devices that are not able to meet the stringent processing time demands of the RF based distance bounding protocol.

Disadvantages. The *Echo Protocol* requires ultrasound transceivers in both the provers and verifiers. The protocol is vulnerable to distance reduction attacks.

Comments. One avenue of future research could be to determine if the microphones and loudspeakers in laptops, PDAs and mobile phones could be used as (ultra)sound transceivers.

3.3 Proximity-proving Protocol

Brent Waters and Edward Felten (Waters and Felten, 2003b) developed a protocol to determine the proximity of wireless devices by measuring signal round-trip times, including party identification based on X.509 certificates and a PKI. Waters et al. presume that the *location claimer* and *location verifier* are temper-proof devices. This approach has been improved by the authors and published in (Waters and Felten, 2003a).

Advantages. The method offers certificate based authentication which provides the whole power of PKI systems including their established capabilities and implementations. Further on, it proves resistant against severe distance-reduction attacks due the use of triangulation for location determination.

Disadvantages. The main disadvantage of this approach is the need for special, temper-proof hardware. Further on, it depends on the availability of a PKI and involves multiple parties in the verification process.

Comments. Waters and Felten were the first to develop a location verification system based on wireless networks that offers integrity and privacy. They incorporated authentication and identification in a round-trip-time based distance bounding approach. However, the requirement for tamper-proof devices and a PKI limits the flexibility and practicability.

3.4 The Secure Location Verification Proof Gathering Protocol (SLVPGP)

Michelle Graham and David Gray from Dublin City University propose a location verification approach based on distance-bounding protocols by Brand and Chaum (Brands and Chaum, 1993). They believe that enlisting the aid of neighboring devices provides the basis of such a method. Their solution allows a *claimant* to make a location claim, and then have this claim verified by an independent *proof provider*. They state that using this approach, a verifier can determine if a location claim is possible and by selecting suitable proof providers one can limit the size of the area in which the claimant can be located. They extend the original protocol by security measures and rely on tamper proof devices to keep the devices cryptographic keys. (Graham, 2009)(Graham and Gray, 2009)

Advantages. SLVPGP does not mandatorily require any network infrastructure as other participants of the network can act as dedicated *proof-providers*. Even the required central authentication authority could be deployed on a node in the ad-hoc network. This offers a high degree on flexibility and allows the deployment in wireless sensor networks.

Disadvantages. The main disadvantage of this method is the need for temper-proof devices to hold the cryptographic keys required for authentication purposes.

Comments. The SLVPG protocol can be seen as a variation of Walters and Feltons Proximity-Proving Protocol. As their location proof is gathered from neighboring devices, a large-scale environment with multiple participants is required. Their approach is very suitable for ad-hoc networks as mobile sensor networks but is limited by the need of tamper-proof devices.

4 CONCLUSIONS AND FUTURE TRENDS

Our conclusion on location determination approaches is, that most of the current solutions are not suit-

able for usage in security related systems. Either their lack of precision is not tolerable or they are too easy to deceive. Only triangulation based on signal-runtime measurements theoretically provides a satisfactory degree of reliability and security.

About location verification solutions we need to state, that at least some of these approaches are fit for application and provide a high degree of security. In particular cases, location aware access regulation systems could use one of the location verification methods described in this article, without a dedicated precise location determination method. For all other applications, hybrid approaches are needed. They could be composed of multiple location determination methods, strengthened by location verification.

A number of security policies, guidelines and frameworks capable of addressing location awareness already exist. Unfortunately, localization tools and techniques are not technically mature.

One may assume that location determination and verification will be addressed in future wireless LAN standards, and therefore the hardware limitations for location determination and verification methods will be overcome. As precise locations are the foundation of location aware access regulation systems, this fact will seriously improve their development and performance.

REFERENCES

Brands, S. and Chaum, D. (1993). Distance-Bounding Protocols (Extended Abstract). In Helleseth, T., editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Technique*, pages 344–359. Lecture Notes in Computer Science 765.

Bussard, L. (2004). *Trust Establishment Protocols for Communicating Devices*. Phd thesis, Eurecom-ENST.

Capkun, S., Buttyán, L., and Hubaux, J.-P. (2003). SECTOR: secure tracking of node encounters in multi-hop wireless networks. In *ACM Workshop on Security of Ad Hoc and Sensor Networks (SANS)*, pages 21–32, Washington. ACM.

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

Fernandez-Gago, M. C., Roman, R., and Lopez, J. (2007). *A Survey on the Applicability of Trust Management Systems forWireless Sensor Networks*. IEEE.

Graham, M. (2009). Poster Abstract : A System for Secure Verification of Location Claims. *Mobile Computing and Communications Review*, 12(2):47–49.

Graham, M. and Gray, D. (2009). Protecting Privacy and Securing the Gathering of Location Proofs The Secure Location Verification Proof Gathering Protocol. *Security and Privacy in Mobile Information and Communication Systems*, pages 160–171.

Kraxberger, S., Lackner, G., and Payer, U. (2010). WLAN Location Determination without Active Client Collaboration. In ACM, editor, *IWCMC '10: Proceedings of the 2010 International Conference on Wireless Communications and Mobile Computing*, pages 1188–1192. ACM.

Liu, H., Darabi, H., Banerjee, P., and Liu, J. (2007). Survey of Wireless Indoor Positioning Techniques and Systems. *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, 37(6):1067–1080.

Rasmussen, K. (2010). Realization of RF Distance Bounding. In *Proceedings of the 19th USENIX Security Symposium, 13 pages. USENIX*.

Sastry, N., Shankar, U., and Wagner, D. (2003). Secure Verification of Location Claims. In *Proceedings of the Fourth International Conference on Web Information Systems Engineering WiSE'03*, pages 1–10.

Singelee, D. and Preneel, B. (2005). Location verification using secure distance bounding protocols. *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.*, pages 834–840.

Waters, B. and Felten, E. (2003a). Proving the Location of Tamper-Resistant Devices. Technical report, Department of Computer Science Princeton University.

Waters, B. and Felten, E. (2003b). Secure, private proofs of location.