Guaranteeing the Authenticity of Location Information

A comprehensive definition of location authentication and a review of its threats and possible solutions help provide a better understanding of this young security requirement.

Ana Isabel González-Tablas Ferreres, Benjamín Ramos Álvarez, and Arturo Ribagorda Garnacho
Universidad Carlos III de Madrid

New and enhanced location-determination technologies have allowed ubiquitous computing applications to better exploit location information. In particular, these technologies have improved location-based services, such as emergency and navigation services, tracking and monitoring systems, and location-based billing services. They also apply to more specific contexts—for example, in sensor networks, location information is often crucial for node tracking and packet routing.

This increasing use of location information has driven researchers to analyze its specific security requirements.[1] The most important requirements relate to privacy and trust, including authenticity and attestation. Here, we focus on authenticating location information, which is necessary when using such information to grant access to a service or to generate evidence such as a certificate guaranteeing an entity's location at some point in time. It's also useful for accountable tracking of nodes and billing of mobile services. More important, for some services—such as emergency related services—failing to guarantee location information can have fatal consequences.

Location authentication is still a relatively young security property. Stefan Brands and David Chaum first addressed location authentication in 1994,[2] followed by Dorothy Denning and Peter MacDoran in 1996.[3] Researchers have since increased their efforts to understand location authentication, proposing several solutions for different contexts. Despite the recent advances, we still need a clearer picture of this property. Here, we extend a survey we published in 2005[4] to provide a more comprehensive definition of location authentication and to describe its main threats in different scenarios. We also give an overview of proposed mechanisms for fulfilling this requirement, taking into account not only location verification but also the related problem of secure location determination.

Location determination

We start with a brief overview of location determination because of its obvious importance to location authentication. One main approach to location determination is to use an object's internal measurements, such as inertial navigation or odometry techniques. However, the more common approach in ubiquitous computing is to use a reference system that exploits triangulation, proximity, or scene-analysis techniques.[5]

Typically, reference-based location determination considers the exchange of signals between a *target node* (the one being located) and a set

Published by the IEEE CS ■ 1536-1268/08/$25.00 © 2008 IEEE

of *reference nodes*. Reference nodes are part of a location-determination infrastructure, and they usually either know their location because it's fixed or can easily determine it.

Reference-based location determination uses either *range-dependent* or *range-independent* techniques. Range-dependent techniques measure specific properties of the exchanged signals—properties that depend on the distance between the nodes. Usually, these techniques rely on the signal's angle of arrival, the received signal strength (RSS), and the propagation time. Range-independent techniques don't measure signal property; they use other characteristics to determine proximity. For example, they might receive information that the reference nodes (beacons) have broadcast, count the number of hops a message must go through, or identify their location through physical contact with other nodes.

Reference-based location determination also relies on a wireless communication network that's either infrastructure-based (for example, based on a satellite, cellular, or RFID system) or ad hoc (for example, based on sensor networks). Additionally, it considers the number of reference nodes involved and the kind of signal used (mainly radio and infrared electromagnetic signals or ultrasound signals). Finally, reference-based location determination also considers who estimates the location. In *terminal-based* schemes, the target node computes its own location, and in *infrastructure-based* schemes, other nodes, mainly reference nodes, compute the node's location. Moreover, it could consider who collects the data for computing the location in addition to who performs the computation, but this is less common.

Location authentication

Authentication is widely known in its two major facets. *Entity authentication* helps corroborate the veracity of a claimed or presumed party's identity. *Data-origin authentication* verifies a message's source.[6] Location authentication assures the truthfulness of the claimed or presumed location information.

The location-authentication schemes we address here use reference-based location determination, so they consider the located node's information to establish its truthfulness. Reference nodes are also involved in location-authentication schemes, and sometimes a central authority (which might or might not be a reference node) is involved as well.

Because location authentication is a novel security service, the academic community has yet to agree on a common definition. In 2001, Tim Kindberg and Kan Zhang proposed a theoretical framework for context authentication using context-constrained channels.[7] They defined location authentication as the process in which an entity claims its location and that location is verified. However, the concept has since evolved to also include secure location determination.

Because location authentication is a novel security service, the academic community has yet to agree on a common definition.

Location verification

Researchers now commonly refer to Kindberg and Zhang's definition of location authentication as *location verification*,[8] emphasizing that the goal is to verify a claimant node's location. In our setting, the claimant is the target node, and one or more reference nodes or a central authority play the verifier role.

Researchers are addressing different variants of the location-verification problem, using three approaches:

- *Distance bounding*. This verifies that the claimant's distance from a certain verifier has an upper bound (that is, the claimant is closer to the verifier than some distance).
- *In region*. In this approach, the protocols, which are usually built on distance-bounding schemes, verify that the claimant is inside a certain delimited region.
- *Absolute location*. Here, the protocols—also built on distance-bounding schemes, generally in combination with triangulation techniques—must verify the nodes' absolute location.

These approaches can use range-dependent or range-independent techniques and are usually infrastructure based. (We distinguish between infrastructure- and terminal-based schemes according to which entity or entities perform the location authentication, not the location estimation.)

Secure location determination

Secure location determination aims to not only determine a target node's location but also provide some guarantee about the location estimation's authenticity. Secure location determination thus addresses the authenticity of location information but emphasizes that the location information is unknown before the execution of the location-determination protocol.

Secure-location-determination protocols can be infrastructure or terminal based, as well as range dependent or range independent. The settings for some infrastructure-based location-determination protocols are similar to those of absolute-location-verification protocols, except that the location information is known or presumed beforehand.

Redefining location authentication

Taking into account location verification and secure location determination, we propose the following

TABLE 1
Range-dependent location verification and determination.

Location-authentication property	Approach	Proposal	Location-determination technique	No. of reference nodes	Network or system support	Signal used
Location verification (infrastructure-based)	Distance bound	Distance-bounding protocols[2]	ToA* (round trip)	1	Contactless access-control cards	Signals with light-propagation speed
		Secure and private proofs of location—proximity- proving protocol[9]	ToA (round trip)	1	Wireless local area network	Radio
		Distance-bounding proof of knowledge[10]	ToA (round trip)	1	Contact-based devices	Optical or electrical
		RFID distance-bounding protocol[11]	ToA (round trip)	1	RFID tokens such as contactless smartcards	Radio (ultra-wideband communication
		Symmetric key-based distance-bounding protocol[12]	ToA (round trip)	1	RFID tokens such as contactless smartcards	Heat and electro-magnetic emanations (side-channel leakage)
	In region	Secure verification of location claims[13]	ToA (round trip)	Multiple (acceptors)—only one executes the protocol	Sensor and wireless networks	Radio and ultrasound
	Absolute location	Location-based authentication system[3]	Location signatures (specific differential GPS)	Multiple (all in view)	Satellite network (GPS)	Radio
		Secure and private proofs of location—absolute-position verification[9]	ToA (round trip)	Multiple	Wireless local area networks	Radio
		Verifiable multilateration[14]	ToA (round trip)	Multiple	Wireless networks	Radio
Location determination	Infrastructure based	Trusted GNSS† receivers[15]	ToA (one way	Multiple	Satellite network (GNSS)	Radio
		Asymmetric security mechanism for navigation signals[16]	ToA (one way)	Multiple	Satellite network (GNSS)	Radio
		Secure positioning with direct sensor positioning[14]	ToA (round trip)	Multiple	Sensor networks	Radio
	Terminal based	Attack resistant minimum-mean-square location estimation[17]	Compatible techniques (such as RSSI‡)	Multiple	Sensor networks	Radio
		Voting-based location estimation[17]	Compatible techniques (such as RSSI)	Multiple	Sensor networks	Radio
		Robust statistical method for triangulation[18]	Any range-dependent technique	Multiple	Sensor networks	Radio
		Secure positioning in sensor networks[14]	ToA (round trip)	Multiple	Sensor networks	Radio

* Time of arrival, † Global Navigation Satellite System, ‡ Received signal strength indication

TABLE 2
Range-independent location verification and determination.

Location-authentication property	Approach	Proposal	Location-determination technique	No. of reference nodes	Network or system support	Signal used
Location verification (infrastructure based)	Distance bound	Location-authentication protocols[7]	Proximity (in range)	1	Wireless networks	Radio (short-range communication technology)
	In region	Secure location verification using radio broadcast[19]	Proximity (in range)	Multiple (acceptors and rejectors)	Sensor networks	Radio
Location determination	Infrastructure based	Secure localization using transmission-rate variation[20]	Proximity (in range)	Multiple	Sensor networks	Radio
	Terminal based	Secure range-independent localization[21]	Proximity (in range)	Multiple	Sensor networks	Radio
		Secure localization with attack tolerance[22]	Proximity (in range)	Multiple	Sensor networks	Radio

definition (based partly on Alfred J. Menezes, Paul C. van Oorschot, and Scoot A. Vanstone's definition of entity authentication[6]):

> *Location authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of a second party's location in a protocol, and the second party must have participated in the protocol (that is, was active when or immediately before the evidence was acquired).*[4]

Most researchers assume that they can't separate location authentication from entity authentication as we have done. Additionally, some believe they can treat both properties independently,[7] and others view location authentication as an alternative to the traditional entity-authentication proofs based on something you have, know, and are. We assume that location authentication requires entity authentication unless explicitly stated otherwise. However, authenticating a device's location doesn't make any guarantees about the user who is controlling that device, and even the information is guaranteed only during the location authentication process.

Tables 1 and 2 provide an overview of approaches and techniques for range-dependent and -independent location verification and determination.

Underlying location-determination techniques

Most range-dependent location-authentication protocols are built on time-based location determination techniques; the rest use RSS techniques. Time-based techniques estimate the distance between two nodes using a signal with a relatively constant propagation speed to transmit messages. Then, the time a message sent by one node takes to reach the other node (one-way time) is measured, or the time for the first node to receive a response to its message from the other node (round-trip time) is measured. The total latency usually includes the nodes' processing time, though it's considered negligible in most cases. Satellite-based systems also use differential techniques (differential GPS) to enhance location-estimation precision by mitigating undesirable deviations in the satellite signals (these deviations are estimated by nodes that know their own location).

RSS-based techniques use a signal that's altered depending on its travelled distance. Some location-authentication settings use RSS indication, which estimates distance directly from the attenuation.

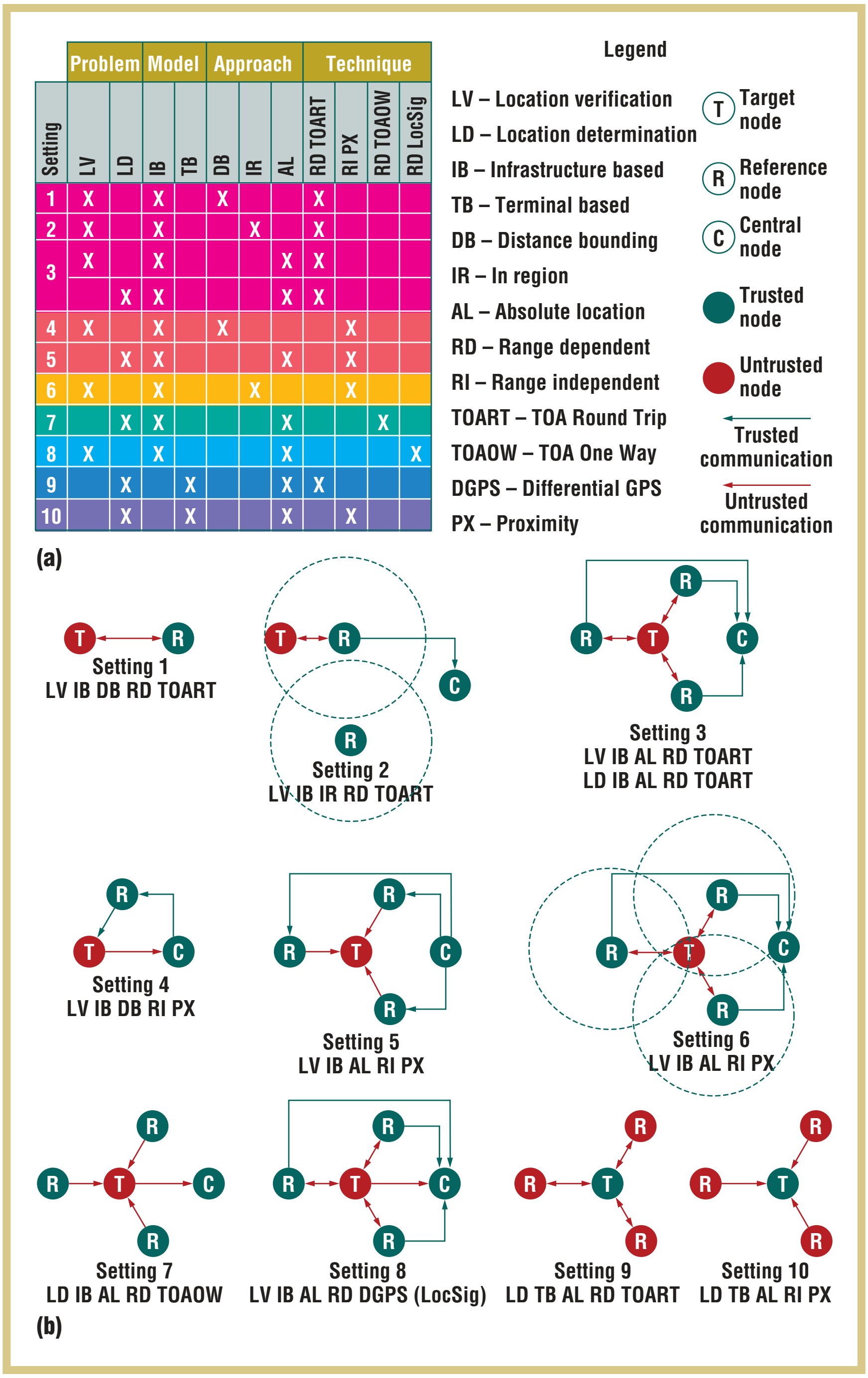
Most range-independent location-authentication schemes use proximity-based techniques, which assume that if a node broadcasts a message, only other nodes close to the transmitting node (within its range) will receive the message.

In all these techniques, when three or more reference nodes are involved, triangulation can be applied to estimate an absolute position. Figure 1 shows an overview of the location-authentication settings we've identified according to their underlying location-estimation technique.

Location-authentication threat models

Only a few location-authentication schemes have been industrially deployed,[3,15] so the threat models researchers have addressed are somewhat theoretical. After analyzing most location-authentication schemes, we've identified two different threat models. The first applies to infrastructure-based location-authentication schemes; the second one to terminal-based schemes.

Both models usually consider the attacker to be an active adversary. The attacker can capture, record, intercept, replay, or insert any message in the communication medium using any kind of signal. We call the



	Problem		Model		Approach			Technique			
Setting	LV	LD	IB	TB	DB	IR	AL	RD TOART	RI PX	RD TOAOW	RD LocSig
1	X		X		X			X			
2	X		X			X		X			
3	X		X				X	X			
		X	X				X	X			
4	X		X		X				X		
5		X	X				X		X		
6	X		X			X			X		
7		X	X				X			X	
8	X		X				X				X
9		X		X			X	X			
10		X		X			X		X		

Legend

LV – Location verification
LD – Location determination
IB – Infrastructure based
TB – Terminal based
DB – Distance bounding
IR – In region
AL – Absolute location
RD – Range dependent
RI – Range independent
TOART – TOA Round Trip
TOAOW – TOA One Way
DGPS – Differential GPS
PX – Proximity

T Target node
R Reference node
C Central node
● Trusted node
● Untrusted node
← Trusted communication
← Untrusted communication

Figure 1. An overview of location-authentication settings. The overview shows (a) the problem they address, the model they follow, and the approach and technique used and (b) a diagram of each setting, identifying the nodes involved and the trustworthiness of these elements. (The colors in the table indicate similarities between the schemes or settings.)

adversary *external* if the nodes under the attacker's control can't authenticate correctly to other nodes in the system. Otherwise, the adversary is *internal*, in which case the adversary will control one or more fraudulent nodes (malicious or compromised).

The difference between malicious and compromised nodes is that we assume that the attacker can't manipulate malicious nodes to access the information used for entity authentication (because it's stored and processed in a tamper-resistant module, for example). However, with compromised nodes, the adversary will have access to the secret keys or authentication information.

The model for infrastructure-based schemes

In infrastructure-based schemes, the adversary's goal is to make reference nodes incorrectly verify or determine the target node's location at some point in time. This goal includes several threats that result if one or more of the elements in the tuple (*id*, *l*, *t*) is incorrectly verified or computed—where *id* stands for node identification, *l* for location, and *t* for time.

For example, the adversary might try to make a verifier believe that a node identified as *id* is at a different location *l* than it really is by using a node *id* placed at *l*. Then the verifiers might think that a different node *id* is at *l*. Infrastructure-based schemes assume that the reference nodes can be trusted and that they usually can communicate securely with a central authority.

The model for terminal-based schemes

In terminal-based schemes, the adversary's goal is for the target node to incorrectly compute its own location at some moment. In this case, we assume that the reference nodes are either malicious or compromised.

Attacks and solutions

Researchers are addressing a set of known attacks for various location-authentication settings. Most attacks target the location information, although others target the time of the location authentication or the located node's identity. Here, we briefly describe the attacks (see Table 3) and analyze

TABLE 3
An analysis of the attacks that might be undertaken in each location-authentication setting. (The colors indicate similarities between the schemes or settings.)

Attack	1	2	3	4	5	6	7	8	9	10
Impersonation	X	X	X	X	X	X	X	X		
Distance fraud	X	X		X		X				
Absolute-location fraud			X		X		X	X		
Time fraud				X	X		X	X		
Mafia fraud 0	X	X	X	X	X	X	X	X	X	X
Mafia fraud 1				X	X		X	X		
Terrorist fraud 0	X	X	X	X	X	X	X	X	X	X
Terrorist fraud 1				X	X		X	X		
Device cloning	X	X	X	X	X	X	X	X		
Report manipulation				X	X		X	X		
Signal and data manipulation							X	X	X	X
Signal and data synthesis							X	X	X	X
Sybil attack									X	X

how existing location-authentication schemes address them.

Impersonation

An external node E or a malicious node T* might try to impersonate an honest node T to make the reference nodes R or the central node C believe that T is at target location l when actually E or T* is located there.

To prevent this attack, the scheme must authenticate the target node during the protocol execution.

Distance fraud

An attacker controlling a malicious target node T* might try to manipulate the device or make it so that it no longer follows the protocol's rules and thus makes the verifiers believe that T* is closer to them than it really is. In schemes based on round-trip time of arrival (ToA), the adversary might undertake this attack by sending the response in advance or manipulating the device's clock speed. In schemes based on proximity techniques, the adversary might try to guess or reuse the token broadcast by the reference nodes or manipulate the device so that it has a more sensitive receiver or a more powerful transmitter.

Fast challenge-response protocols can prevent this attack in round-trip-TOA-based schemes.[2,9–12] Jolyon Clulow and his colleagues also suggest a set of principles to consider when choosing communication protocols and data-coding formats.[23] To avoid a node manipulating its processing time, some researchers suggest tamper-resistant hardware.[9] Others propose making processing times negligible compared to propagation time using specific hardware,[10] and yet others tighten the conditions of the protocol according to the processing time the claimant node declares.[13] For proximity-based schemes, to avoid token reuse or guessing, tokens should be unpredictable and bound to a single, specific location.[7,20]

Absolute-location fraud

An attacker controlling a malicious node T* might try to fake the verification or determination of its absolute location by manipulating the device or make it so that it no longer follows the protocol's rules. Then, reference nodes or the central node might believe that T* is in a different location than it is. In schemes based on multi-lateration, the adversary might undertake this attack by making some of the reference nodes (falsely) believe that the adversary is farther away than it really is. Distance-bounding protocols don't aim to prevent this action. In other cases, the adversary might try to manipulate the node to generate fake reports about its location or manipulate the captured signals.

This attack is prevented in round-trip-TOA-based techniques if the target node is within the polygon or polyhedron formed by the involved reference nodes.[14] In proximity-based schemes, tokens should be unrelated to the distance they address. This hinders malicious nodes from selecting a coherent set of tokens that result in a false location estimation.[20] Other schemes require tamper-resistant devices to prevent target nodes from manipulating signals received from reference nodes or creating fake reports.[15]

Time fraud

In some settings, a malicious node T*

might try to make the reference nodes believe it's at some location it actually left a while ago. In proximity-based schemes, the adversary might undertake this attack by trying to reuse previously received tokens at the target location.

In proximity-based schemes, tokens should be different each time.[7,20] Denning and MacDoran propose a similar mechanism to guarantee freshness and location authentication,[3] while others rely on tamper resistance.[15]

Mafia fraud

In the classic version of this attack, adapted to location-authentication schemes (*mafia fraud* 0), the adversary places one or more malicious nodes T* (or R* in terminal-based schemes) acting as a proxy between honest reference nodes and an honest node T. The malicious node T* is placed at the target location l while T isn't. The adversary's goal is to make the reference or central nodes (the node T itself in terminal-based schemes) believe that T is at l. This attack is also called a wormhole attack.

When the target node interacts with a central node in addition to reference nodes, the mafia fraud attack can be made in a second way (*mafia fraud* 1). In this case, the malicious node T* is placed between the honest node T and the central node C. T is at the target location l while T* isn't. The adversary's goal now is to make the central node believe that T* is at l.

Avoiding this attack in round-trip-TOA-based schemes requires using signals propagating at a speed that the adversary can't exceed (signals whose propagation speed is close to light speed).[8,10,14]

One way to mitigate the attack in proximity-based schemes is to control the access to the tokens by encrypting them with a key shared with the intended (honest) target node. Matthew Pirreti and his colleagues propose a similar mechanism that uses cluster keys shared only between the nodes close to the reference nodes.[22] Other researchers suggest the careful design of reference-node deployment combined with specific requirements such as the use of rejector nodes[19] or sectorized antennas.[21] In another mechanism, the reference nodes use high-bandwidth signals[3] or the target node performs noncryptographic validations to detect whether the signal has been relayed.[15]

Terrorist fraud

This set of attacks (*terrorist fraud* 0 and 1) is similar to mafia fraud attacks except that all participating nodes are malicious. So, the node that was honest in mafia fraud attacks now colludes with the other malicious nodes if there's some authentication operation is involved.

To avoid this attack, the message that the target node sends must be bound to itself (using message authentication, for example) and its contents protected to avoid an adversary reusing them (such as through encryption).[15]

Device cloning

If the adversary controls and has cloned a compromised node, it's easy to make reference or central nodes believe that the node exists at a fake location.

This attack is difficult to prevent, but tamper resistance and device-fingerprinting techniques can help.

Report manipulation

The infrastructure-based schemes that have the target node reporting information to a central node might suffer from this attack. The adversary might try to manipulate the report that an honest target node T sends to make the central node believe T is at an incorrect location.

Message authentication mechanisms can help prevent this attack.

Signal and data synthesis

An adversary might try to impersonate reference nodes to subvert location authentication protocols. This attack is easy to undertake using current public GPS signals.

To prevent this attack, a target node should be able to authenticate the signals received from reference nodes—or at least the data they carry.[15]

Signal and data manipulation

In satellite-based schemes, the signal's ToA is very important. An attacker might manipulate the signals and the data they carry to selectively delay the signals' ToA to an honest target node, which will therefore incorrectly estimate the target node's location.

Message authentication mechanisms sometimes detect of this kind of attack. However, satellite-based systems must include more specific mechanisms that can detect attacks that selectively delay the signal or manipulate its deviations.[15,16]

Sybil attack

In this attack, the adversary controls several compromised reference nodes R*, which collude to broadcast or send erroneous information to make the target node T determine T's location incorrectly.

Once reference nodes have been compromised, target nodes can mitigate this attack using mechanisms that try to detect the fraudulent reference nodes to eliminate their influence in the location estimation.[14,17,18]

Practical issues

Analyzing how the proposed solutions mitigate the threats to location authentication is insufficient; we must also analyze the difficulty and cost of implementing the mechanisms in the context of a particular application to assess its suitability.

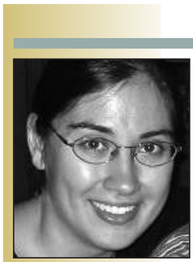
Generally, proximity-based schemes are more affordable[7,19,21,22] and, if designed carefully, might stop an attacker that has reasonable capabilities. Other affordable and interesting schemes are those that don't aim to prevent attacks at all cost but let the target node compute its location successfully with certain guarantees, given that the number of fraudulent nodes is limited.[17,18]

The stronger schemes are usually more expensive to implement[10,11,14,16] and might be adequate only for high-security applications. When analyzing the risk, you need to consider the adversaries' resources and the differing contexts. For example, a weak adversary might be able to undertake attacks (for example, mafia fraud and signal synthesis attacks) in certain contexts but might require numerous resources to overcome other attacks.

Location authentication will receive increasing attention in ubiquitous computing. As we've learned, proposals designed for different contexts converge, and designing and implementing location-authentication mechanisms isn't easy. On the one hand, range-dependent time-based mechanisms are generally more secure against powerful adversaries, but they usually impose hardware and software requirements that aren't always easy to fulfil. On the other hand, robust statistical methods allow the provision of some guarantees to range-independent schemes without the strict hardware and software requirements. Although we focused on how the schemes address location authentication, we now must further study other parameters such as privacy guarantees, efficiency, hardware and synchronization requirements, and resilience to communication errors.

Several big challenges lie ahead for location-authentication researchers—mainly, building competitive commercial implementations of the mechanisms that can withstand attacks at an affordable cost. We must also develop formal methods for analyzing the mechanisms used to provide security guarantees.[24] We'll also need to integrate the authentication of a user's proximity to the located devices to improve the integrity of existing or new mechanisms used in this field. P

the AUTHORS



Ana Isabel González-Tablas Ferreres is an assistant professor in the Computer Science Department at Universidad Carlos III de Madrid. Her main research interests are security and privacy for location-based services and digital signature applications. González-Tablas Ferreres received her PhD in computer science from Universidad Carlos III de Madrid. She's a member of the IEEE and ACM. Contact her at aigonzal@inf.uc3m.es.

Benjamín Ramos Álvarez is assistant professor in the Computer Science Department at Universidad Carlos III de Madrid. His research focuses on non-repudiation issues of electronic signatures. Ramos Álvarez received his PhD in computer science from Universidad Carlos III de Madrid. Contact him at benja1@inf.uc3m.es.

Arturo Ribagorda Garnacho is full professor and head of the Computer Science Department at Universidad Carlos III de Madrid. His research focuses on the security of information and communications technologies and related legal issues. Ribagorda Garnacho received his PhD in computer science from the Universidad Politécnica de Madrid. Contact him at arturo@inf.uc3m.es.

ACKNOWLEDGMENTS

The authors are funded by a research grant of the Research General Directory from the Ministry of Education and Science in Spain under contract SEG2004-02604.

REFERENCES

1. C.A. Patterson, R.R. Muntz, and C.M. Pancake, "Challenges in Location-Aware Computing," *IEEE Pervasive Computing*, vol. 2, no. 2, 2003, pp. 80–89.
2. S. Brands and D. Chaum, "Distance-Bounding Protocols," *Proc. Workshop Theory and Application of Cryptographic Techniques on Advances in Cryptology*, Springer, 1994, pp. 344–359.
3. D.E. Denning and P.F. MacDoran, "Location-Based Authentication: Grounding Cyberspace for Better Security," *Internet Besieged: Countering Cyberspace Scofflaws,* ACM Press/Addison-Wesley, 1998.
4. A.I. González-Tablas et al., "Survey on Location Authentication Protocols and Spatial-Temporal Attestation Services," *Proc. IFIP Int'l Symp. Network-Centric Ubiquitous Systems*, Springer, 2005, pp. 797–806.
5. J. Hightower and G. Borriello, "Location Systems for Ubiquitous Computing," *Computer*, vol. 34, no. 8, 2001, pp. 57–66.
6. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 2001.
7. T. Kindberg and K. Zhang, *Context Authentication Using Constrained Channels*, HP Labs Tech., 2001.
8. D. Singelee and B. Preneel, "Location Verification Using Secure Distance Bounding Protocols," *Proc. IEEE Int'l Conf. Mobile Ad-hoc and Sensor Systems*, IEEE CS Press, 2005, pp. 834–840.
9. B.R. Waters and E.W. Felten, *Proving the Location of Tamper-Resistant Devices*, tech. report TR-667-03, Computer Science Dept., Princeton Univ., 2003.
10. L. Bussard, "Trust Establishment Protocols for Communicating Devices," doctoral dissertation, Institut Eurécom Télécom Paris, 2004.
11. G. Hancke and M.G. Kuhn, "An RFID Distance Bounding Protocol," *Proc. First Int'l Conf. Security and Privacy for Emerging Areas in Comm. Networks*, IEEE CS Press, 2005, pp. 67–73.
12. J. Reid et al., "Detecting Relay Attacks with Timing-Based Protocols," *Proc. 2nd ACM Symp. Information, Computer and Comm. Security*, ACM Press, 2007, pp. 204–213.
13. N. Sastry et al., "Secure Verification of Location Claims," *Proc. 2003 ACM*

Workshop on Wireless Security, ACM Press, 2003, pp. 1–10.

14. S. Čapkun and J.P. Hubaux, "Securing Positioning in Wireless Networks," *IEEE J. Selected Areas in Comm.*, vol. 24, no. 2, 2006, pp. 221–232.

15. C. Wullems, O. Pozzobon, and K. Kubik, "Trust Your Receiver? Enhancing Location Security," *GPS World*, Oct. 2004, pp. 23–30.

16. M. Kuhn, "An Asymmetric Security Mechanism for Navigation Signals," *Proc. 6th Information and Hiding Workshop*, Springer, 2004, pp. 239–252.

17. D. Liu, P. Ning, and W.K. Du, "Attack-Resistant Location Estimation in Sensor Networks," *Proc. 4th Int'l Conf. Information Processing in Sensor Networks*, IEEE Press, 2005, pp. 99–106.

18. Z. Li et al., "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," *Proc. 4th Int'l Conf. Information Processing in Sensor Networks*, IEEE Press, 2005, pp. 91–98.

19. A. Vora and M. Nesterenko, "Secure Location Verification Using Radio Broadcast," *IEEE Trans. Dependable and Secure Computing*, vol. 3, no. 4, 2006, pp. 377–385.

20. F. Anjum, S. Pandey, and P. Agrawal, "Secure Localization in Sensor Networks Using Transmission Range Variation," *Proc. IEEE Int'l Conf. Mobile Ad-hoc and Sensor Systems*, IEEE Press, 2005.

21. L. Lazos and R. Poovendran, "SeRLoc: Robust Localization for Wireless Sensor Networks," *Proc. ACM Workshop Wireless Security*, ACM Press, 2004, pp. 21–30.

22. M. Pirreti et al., *SLAT: Secure Localization with Attack Tolerance*, tech. report NAS-TR-0024-2005, Network and Security Research Center, Dept. of Computer Science and Eng., Pennsylvania State Univ., 2005.

23. J. Clulow et al., "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks," *Proc. Security and Privacy in Ad-Hoc and Sensor Networks Third European Workshop*, Springer, 2006, pp. 83–97.

24. C. Meadows et al., "Distance Bounding Protocols: Authentication Logic Analysis and Collusion Attacks," *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*, Springer, 2007, pp. 279–298.