The Third International Conference on Availability, Reliability and Security

CERTILOC: Implementation of a spatial-temporal certification service compatible with several localization technologies

J.M. de Fuentes, A.I. González-Tablas, A. Ribagorda
Computer Science Department. University Carlos III de Madrid (SPAIN)
jfuentes@inf.uc3m.es, aigonzal@inf.uc3m.es, arturo@inf.uc3m.es

Abstract

Recently researchers are being encouraged to address security and privacy requirements for location information. This work contributes to this area by presenting CERTILOC, a prototype of a spatial-temporal certification service that is interoperable with representative localization technologies (GSM Cell-ID and GPS). Our work is completed with a broad threat analysis on spatial-temporal certification services and an exposition of legal considerations that can be made if used in work scenarios.

Keywords. Certification, localization, legal issues.

1. Introduction

Nowadays a wide range of location estimation technologies are accessible to the general public. The most well-known location estimation technology is the Global Positioning System (GPS), probably followed by the cell-based location information provided by some wireless networks such as mobile phone networks. Supported on their spreading, location-based services are gradually becoming a reality. As a consequence, location information is more and more used everyday. One of the challenges that this situation raises is the development of solutions to provide end-to-end control of location information [1], particularly, the development of mechanisms that guarantee user's privacy and location information's trust.

This work focuses on the problem of digitally certifying the location of an entity at a given time by addressing the implementation of CERTILOC. Our research builds upon the spatial-temporal certification framework developed by González-Tablas, Ramos and Ribagorda [2]. We have designed the system to be compatible with several localization methods, to use existing standards when appropriate and to follow a modular design. Besides the value that a real implementation provides, our work contributes also by analyzing the security of this kind of systems from a broader point of view and its legal implications when used for workforce monitoring scenarios.

Related work. During the last decade some spatial-temporal certification models and mechanisms have been proposed in [3, 4], but none of them addresses their implementation besides that they focus on specific application scenarios. On the other hand, [5] presents a proof of concept implementation of a GPS-enabled device which sends its location data protected with a self generated digital signature. It could be integrated in our system as an alternative localization subsystem.

Paper outline. In Section 2 the main concepts of González-Tablas *et al.* spatial-temporal certification framework are described. Section 3 presents the principal features of the implemented service. Sections 4 and 5 discuss the security analysis and legal implications respectively. Finally, Section 6 summarizes conclusions and lessons learned.

2. Spatial-temporal certification services

Spatial-temporal certification services are defined as *those services that generate, collect, maintain, make available and validate evidences concerning the spatial-temporal information of an entity* [2]. Therefore, evidences generated by these services attest that some entity was located at some place at some moment in time under some specific policy. Such evidence is called Spatial-Temporal Certificate (STC) and it binds certain Spatial-Temporal Information (STI) to some entity. These services find their application in non-repudiation scenarios (e.g., in the tracking of entities and assets such as mobile workers), in location-based billing (e.g., automatic toll collection systems for highway usage) and in security policies enforcing (e.g., an on-line gambling site require to its clients to be located within some geographic area).

The provision of spatial-temporal certification services takes place in several phases in which several entities may participate. First phase is *certificate generation*, in which a requester asks for the generation of a STC for a specific subject to the spatial-temporal evidence generator. This generator issues the STC after obtaining the location information of the subject from a

0-7695-3102-4/08 $25.00 © 2008 IEEE
DOI 10.1109/ARES.2008.146

secure Spatial-Temporal Information Service (STIS). STISs act as location servers but in the model it is assumed that the methods they use to obtain the location information guarantee its authenticity to some extent. Second phase considers the *certificate transfer, storage and retrieval*, so the STC reaches the intended receiver. Third phase is *certificate verification*, which is performed by a spatial-temporal verifier. Fourth phase comprises the *certificate use* (the evidence user makes use of the spatial-temporal evidence to obtain some benefit from a relying party) and fifth phase, which does not always occur, comprises *dispute resolution* (an adjudicator decides if the claimant and the relying party do not agree). For more details on these issues, we refer the reader to the previous work of González-Tablas *et al.* in [2].

3. Description of the system

Our system addresses the first three phases described in the model, as the certificate use phase will depend on the application in which the system may be integrated and the fifth phase usually takes place in legal contexts. The majority of the system's functionalities, grouped in the Spatial-Temporal Certification Authority (STCA), are accessible through a web interface on the main CERTILOC server (see Figure 1) although there is also some functionality offered through the PDA's interface. For the sake of simplicity, in our system, the receiver of the evidence is the same entity that requested its generation. Once a user receives a STC, he may verify it by checking the STCA´s signature.

One of the main characteristics of CERTILOC is that it is designed to be compatible with different localization technologies. Currently the prototype obtains the location information from two spatial-temporal information services, one for GSM devices that uses Cell-ID location method (STIS-GSM) and another for GPS-enabled devices such as PDAs (STIS-GPS). They are the most spread location estimation technologies and are representative of the main current localization methods, network and terminal-based localization respectively. Some remarks have to be made about the design of the GPS-based localization subsystem. Regarding that GPS-enabled devices locate themselves, a PDA module must exist to communicate its location to externals. Additionally, taking advantage of that, we designed this subsystem as a first approach to a distributed spatial-temporal certification service, that is, our self-located devices issue *self-signed STC* (simplified certificates referring to themselves) which are sent to the central service so a proper STC can be issued. For a real distributed service, the device's software and hardware should be reliable enough.

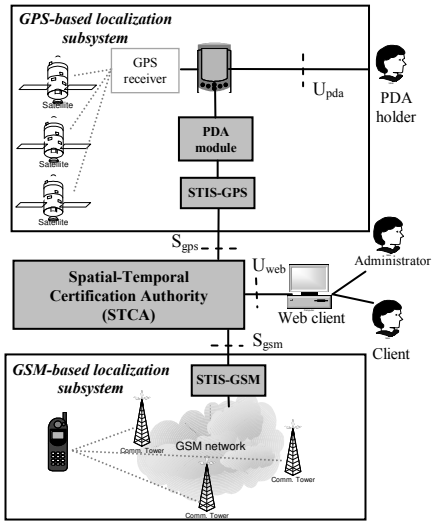

Figure 1. Overview of CERTILOC

The STIS-GSM returns immediately a response to location requests about GSM devices (*immediate requests*). However it cannot be assumed that PDAs will be always accessible to attend to the location requests directed to them. Therefore, our system is designed such that *deferred requests* (location related requests referring to connection limited devices) are served in three phases: first, requests made by users are stored by the STCA in a database shared with the STIS-GPS; second, as soon as the PDA connects to the STIS-GPS, the pending requests are attended and the STIS-GPS stores the self-signed STCs issued by the PDA in the cited database; third, users access a second time to the system to trigger, if possible, the completion of their request. Although we plan to integrate in CERTILOC a policy based privacy management and enforcement mechanism, it is still not implemented.

The following sections of this chapter explain both the design and implementation of CERTILOC. Section 3.1 contains its functionalities. Section 3.2 describes its architecture. On section 3.3, the technologies in use and implementation details are shown. Finally, Section 3.4 focuses on CERTILOC´s timing performance.

3.1 Functionalities

First of all, the prototype can *locate devices*. A client can access the system through the web interface and make a location request. The system then transfers the request to the appropriate STIS and, when the STI is available, it is transferred to the client. If the request affects a connection limited device, the client gets

instead a locator, which allows him to resume his request afterwards if it has been attended.

Furthermore, the system allows clients to *certify devices' location*. The STCA, after having obtained the STI, generates and stores a STC. Again, if it is a connection limited device, the user gets a locator instead. The prototype also allows clients to *manage STC´s lifecycle* (download, remove and consult STCs).

PDA users can *generate voluntary self-signed STCs at any time* through the PDA´s interface. These self STC are afterwards used by the STCA to generate a complete STC. PDA users can also specify some configuration parameters (related to the relationship between the PDA and the STIS-GPS).

Finally, regarding the privacy management and enforcement, it is planned (but not implemented) that any client responsible of a device will be able to manage privacy policies which will specify under which conditions a user would allow the processing of the STI related to devices the user is responsible of.

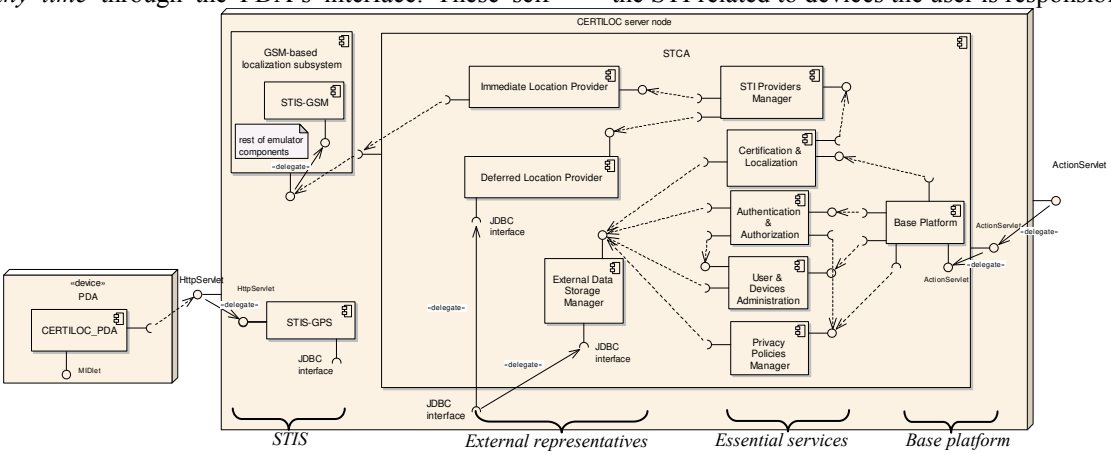

Figure 2. CERTILOC´s deployment diagram.

3.2 System architecture

Figure 2 contains the system's deployment diagram. Logic is distributed in two nodes: CERTILOC server and a PDA. The STCA is the main component deployed on the server. It follows the MVC pattern and is structured in three layers:

- **Base platform.** It receives user actions and makes callings to the essential services.
- **Essential services.** It contains the components in charge of the main functionalities.
- **External representatives.** It contains two STI providers, which are the components that connect to the STIS (one for immediate requests and another for deferred ones).

Besides the STCA, the entire GSM-based localization subsystem and the GPS-STIS are also deployed in CERTILOC server node. The certificates repository and the database shared between the STIS-GPS and the STCA are also placed in the server node.

3.2.1 Dynamic behavior. Following we identify the main processes that take place in each request (*location* or *certification* request).

Users can make an **immediate request** after logging in the system through the web interface (*request generation*). The "certification & localization" module then calls to the "immediate location provider" (*internal STI retrieving*) who transfers the request to the STIS-GSM using the O.M.A Mobile Location Protocol 3.0 (*external STI retrieving*). The immediate location provider contacts with the location network to get the STI which is sent back to the STCA (*STI transference*). The STCA should enforce then the privacy policies defined for the located device (*privacy enforcement*). If the request was for certifying, then the *complete STC generation* process is done and the STC is inserted into the database (*database updating*). The result, STI or STC, is transferred to the user (*system response*).

In case of **deferred requests**, when the client makes the request, it is inserted into the database and a locator is sent to the user (*request insertion*). Periodically, the PDA gets securely connected to the STIS-GPS (*device connection*) using Wi-Fi access and a self-defined protocol with mutual authentication built upon HTTP over SSL. The STIS-GPS looks for unanswered requests in the database (*request retrieving*) and if any, they are securely sent to the device (*request transference*). Then, the PDA, which has been registering periodically its own STI, answers each request building a self-signed STC using the closer in time STI (*request resolution*). Those self-signed STCs are sent to the STIS-GPS (*answering certificate transference*), which validates and inserts

them in the database (*answering certificate insertion*). When the client returns to the system and uses the provided locator (*deferred request resuming*), after privacy policies are checked (*privacy enforcement*), the STI or the STC built upon the referred self-signed STC (*complete STC generation*) are sent to the user.

The PDA holder can **generate at any time voluntary self-signed STCs**. These STCs are preliminary built when the PDA holder orders the certification (*voluntary STC initial generation*) but their signature is generated when they are sent to the STCA within the cited *certificate transference* process.

3.2.2 Security mechanisms. Besides the security mechanisms established in the connections between the STCA and the STISs, user authentication and authorization mechanisms are also integrated in CERTILOC. Regarding user authentication, web interface currently offers a classical user and password access, although the use of X.509 public key certificates is planned. PDA holder authentication is not considered in CERTILOC, mainly because it would lead to a less friendly mobile application. Regarding user authorization, currently the system only checks if the user´s role (client or administrator) is allowed to make the request. In next release, if the action involves spatial-temporal information, the system will check privacy policies established for the affected device.

3.3 Implementation details

The whole prototype has been implemented using Java. The server node runs Ubuntu Linux 6.0.6. Server components are running on several web application servers (Apache Tomcat 5.5.23). The STCA has been implemented using the Struts framework. Related to STC generation, we selected OpenSAML 2.0 (currently under development) and we followed, as much as possible, the SAML based STC structure defined in [2]. With respect to data storage, MySQL 5.0.5 is used.

Regarding the GSM-based localization subsystem, it has been emulated using software provided by Ericsson [8]. Regarding the GPS-based localization subsystem, the STIS-GPS has been built using Java Servlets and the GPS-enabled device is a Nokia N95 supporting J2ME and compliant with the Java Location API (JSR 179). For cryptographic operations, we use the Bouncycastle API version 1.3.7.

3.4 System performance

In this section we present the time yield of the system from the user point of view. We have analyzed system performance differentiating the system operation with the two localization subsystems (GSM and GPS). Table 1 shows the results.

Table 1. Results of time measurements.

Time ID	Process	Mean time
GSM-based localization subsystem		
T_1	Location request	3.13 sec.
T_2	Certification request	3.86 sec.
GPS-based localization subsystem		
T_3	From *device connection* to *answering certificate insertion*	13.53 sec.
T_4	*Voluntary STC initial generation*	3.9 sec.
T_5	*Certificate transference* (for voluntary STC)	4.97 sec.

3.4.1 GSM-based localization subsystem. Table 1 shows the mean time for location (T_1) and certification (T_2) requests related to GSM devices. These results were expected taking into account the complexity of the involved tasks and the available resources to carry out them. The difference between the two times is due to additional processing needed for composing the STC in certification requests.

3.4.2 GPS-based localization subsystem. Table 1 shows time measures for the essential processes related to GPS-enabled devices. Process names used in this section are taken from those identified in section 3.2. Note that neither *request insertion* nor *deferred request resuming* processes have been timed, because they were negligible compared to the rest of times.

First of all, time measurement T_3 represents the time between the PDA gets connected with STIS-GPS for obtaining pending requests, and until its responses are correctly stored in the server database.

In case of voluntary self-signed STC, as said on section 3.2, the process is divided into two parts, and each of them has been timed separately. Time T_4 represents the time in the PDA to create the data structure that will be included in the certificate. Although this process involves connecting with the GPS receiver, it is relatively fast (at least, admissible for the user experience). This data structure is stored until the next connection to the STIS-GPS takes place. Time T_5 shows the length of this connection, during which the stored certificate is retrieved, digitally signed and finally sent to the server. Comparing the times obtained for this technology with the previously one, times are larger in this case although essential tasks are the same (creating data structures, making digital signatures and communicating). This result was expected, because PDAs have fewer resources.

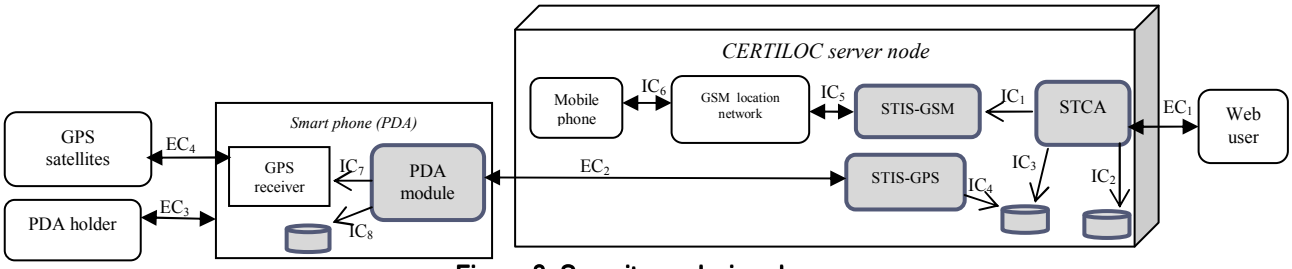

Figure 3. Security analysis scheme

4. Security analysis

CERTILOC´s main security goals are the integrity and confidenciality of STI [9]. In this section we analyze the main threats that CERTILOC must face to. We will use Figure 3 to help in the analysis.

First threat that CERTILOC must face to is *identity spoofing*. In CERTILOC web users access the system through the channel marked as EC_1 and they are forced to log into the system. Once authenticated, user actions take place inside a session whose correctness is checked in every request, avoiding then *privilege escalation attacks*. An attacker may try also to impersonate the STCA in order to access the GSM-based localization subsystem (e.g. to illegally know the location of a device), but this threat is mitigated by the user/password authentication required by the Ericsson MPS SDK software. An attacker may also try to impersonate the STCA or the STIS-GPS in order to access the shared database between them or the STCs database. In CERTILOC this threat is again reduced by requiring user/password authentication to access the mentioned databases. An identity spoofing attack could also be performed for both the PDA and STIS-GPS, one against each other, in channel EC_2. This could allow to obtain the STI in an unauthorized way (if STIS-GPS identity is spoofed), or to provide fake STI (in case of PDA spoofing). For this purpose, an SSL tunnel with server authentication is established. Client (the PDA) authentication is made within our self-designed communication protocol.

Another threat that must be considered is *location spoofing* (i.e. modifications over the STI). This threat could take place wherever any STI is involved. Satellite signals (EC_4) could be intentionally altered, and this cannot be mitigated (at least, with public GPS). Furthermore, the PDA could be manipulated, unless tamper-resistant hardware is used. Besides, the transferred STI from the PDA could also be altered within the communication (EC_2). In our case, additionally to the cited SSL tunnel (which could be enough) the digital signature made for certifying the information also guarantees its integrity. This digital signature is also the mechanism used to alleviate this threat in the databases placed in the server, although it would be advisable to analyze the data introduced by users through the web interface (to prevent SQL injection attacks). It is important to remark that in a real GSM-based localization subsystem it would be also necessary to take measures against this threat.

Other threat to take into account is the *loss of privacy*. This could be achieved in two ways. First, an attacker could try to access to confidential data. In our system, this could be attempted in all databases and in EC_1 and EC_2 channels. To reduce this threat, all accesses to this data are authenticated. In case of the data stored into the PDA, it has been protected by using only internal memory. Nevertheless, it would be desirable to cipher all data storages.The second way to achieve loss of privacy could be an unauthorized use of the obtained STI (regarding that STI is considered a private data when referred to a person). To ease this threat, security policies enforcement and management mechanisms are planned.

The last kind of threat considered is *denial of service*. This could be attempted on PDA (e.g., by sending a great couple of requests), on satellite signals (jamming attacks) or on the server node (by making lots of simultaneous requests). In CERTILOC, only the attack over the PDA is prevented, because the operating system controls the resources consumption.

Including all of the referred measures would not lead to a safe architecture, but to a reasonably defended system against external threats. Nevertheless, insider attacks could be performed.

5. Legal issues in workforce monitoring scenarios

In this section we analyze firstly the authority of an employer to monitor an employee using the system and secondly the legal validity of the STC once generated.

It has to be remarked that when a device is directly or potentially related to someone, its STI is also its holder´s one. This fact is relevant from the legal point of view, because the location information of a person is

considered as personal data, and therefore it must be protected (as dictated by [10], transposed in Spain in [11]). One of the applications of this prototype would be to integrate it in a working scenario, that is, as surveillance or control measure. We address this issue considering the Spanish law, but they can be easily applied to any European country belonging to the European Union as they all have as base the same European Directive [10]. In the Spanish workers statute [12], it is stated that the employer can give devices that can be located to the employees as a tool of working. Nevertheless, if the employer collected the location data of his employees, he should inform them about this collection [11].

In this situation, it is interesting to analyze the legal value of STC as evidence within a judiciary process. Its validity is conditioned to the strength of the digital signature. The digital signature now made by the prototype may be considered as an "*advanced digital signature*" [13]. This kind of signature is not enough to have the same validity as a handwritten one. To achieve this, in addition to the saying until now, the whole prototype should be checked as a "*secure signing device*". This condition should be fulfilled by real systems based on this prototype.

6. Conclusions

The fact that nowadays location information is more and more used promotes researchers to address the challenges that arise for guaranteeing an end-to-end control of this information. The system we have implemented addresses the implementation of a prototype of a spatial-temporal certification service that is based on the model proposed in [2] and is compatible with two localization technologies, GSM Cell-ID and GPS. This kind of practical research has not been commonly addressed, which gives a special value to our work. Our work is not only an implemented prototype, but also a system whose design has focused on dependability. In the system there is a modular division of responsibilities and commonly accepted standards are in use, which make the prototype more flexible. The dependability is also reflected in the integrated security mechanisms, which do not lead to a complete safe architecture but to a reasonably defended system. Furthermore, we analyze also the legal implications of using the system in work scenarios.

Though the prototype is completely functional, we are currently working in the development of a policy-based privacy management and enforcement module and in extending the prototype to locate RFID labels.

The main lesson learned from our work is that it is viable to implement this kind of systems although they have to deal with a great number of complex security threats, some of which can be easily mitigated but others are difficult to prevent.

Acknowledgements

The authors would like to thank J. Carlos Calvo for his collaboration in the implementation. Authors are partly supported by Spanish M.E.C. (SEG2004-02604).

References

[1] C. A. Patterson, R. R. Muntz, and C. M. Pancake, "Challenges in location-aware computing", *IEEE Pervasive Computing*, 2(2):80–89, April 2003.

[2] González-Tablas, A.I, Ramos, B., Ribagorda, A., "Spatial-temporal certification framework and extension of X.509 attribute certificate framework and SAML standard to support spatial-temporal certificates", in Proc. of EuroPKI'07, 2007.

[3] L. Bussard. Trust Establishment Protocols for Communicating Devices. PhD thesis, Institut Eurécom, Télécom Paris, 2004.

[4] A. Zugenmaier, M. Kreutzer, and M. Kabatnik, "Enhancing applications with approved location stamps", in Proc. of IEEE Intelligent Network Workshop, 2001.

[5] Wullems, C.; Pozzobon, O. and Kubik, K., "Trust your receiver? Enhancing location security", *GPS World*, 2004, 15, 23-30.

[6] ITU-T. ITU-T RECOMMENDATION X.509 - Information technology – Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, August 2005.

[7] OASIS. Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) Version 2.0. OASIS Standard, 2005.

[8] Ericsson, MPS SDK 6.0.1, March 2004.

[9] Pfleeger, C. and Pfleeger, S. Security in Computing (3rd edition), Prentice Hall, 2003.

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, July 2002.

[11] Ley Orgánica 15/1999, de 13 de diciembre**,** de Protección de Datos de Carácter Personal, Spain, 1999.

[12] Real Decreto Legislativo 1/1995, de 24 de marzo, Spain, 1995

[13] Ley 59/2003, de 19 de diciembre, Spain, 1999.