Securing Smartphone Based ITS

Vasileios Manolopoulos, Panos Papadimitratos, Sha Tao, Ana Rusu
KTH Royal Institute of Technology
Stockholm, Sweden

Abstract—**GPS-equipped smartphones present several advantages for data acquisition in Intelligent Transportation Systems (ITS), compared to solutions that require a new communication infrastructure. However, there are still significant challenges to meet before deployment. Traffic information and location samples must be collected in a secure manner, to not jeopardize the system operation. Equally important, users must be assured about their privacy, notably the protection of information on their whereabouts. To address this two-fold problem, we propose extending the Generic Bootstrapping Architecture (GBA) with anonymous authentication. Identity and location information are protected and separated, and location samples cannot be linked to each other and to any specific user. Thus, our scheme protects users even in the case of a compromised ITS server. Initial evaluation results indicate the feasibility of our approach with off-the-self mobile platforms.**

I. Introduction

Smartphones and portable personal devices, especially those integrating GPS receivers, have become common practice nowadays. Moreover, cellular networks offer very broad coverage. As a result, scores of new location-based applications and services have emerged. In fact, leveraging the smartphone capabilities and the dense infrastructure can be highly advantageous for Intelligent Transportation Systems (ITS) and traffic management applications: each smartphone could provide location samples to a traffic management server, and then provide its user with traffic information.

Smartphone-based ITS can have dramatically lower cost than traditional ones: they have no need for special in-car hardware, and they could reach fast high penetration rates. Major application platforms, Apple's iPhone and Google's Android, provide friendly development environments for prototyping. Moreover, features such as online digital maps or phonetic route guidance could be easily added. Finally, any driver with a relatively modern smartphone would be able to join the system.

However, there are significant challenges to meet before deploying such a solution. On the one hand, obtaining location samples and traffic information must be secure. Otherwise, the traffic management server could receive forged location samples. Or, the mobile client could get corrupted traffic information responses. At the same time, the privacy of the system users cannot be at stake: No one would like to have information on his/her whereabouts, exactly what the mobile clients regularly send to the traffic management server, disclosed. Tracing an individual could lead to identification and even damages (e.g., PleaseRobMe [1]).

Existing commercial solutions ([2], [3]) rely on password based authentication and they provide a statement that they remove the user's identification from all contributed location samples; they pledge no private information disclosure unless this is required by the authorities.

Our goal is to provide strong security, authenticating the individual contributions of the clients. We also want to provide privacy by design, notably by making location updates anonymous and unlinkable. In particular, we want to deprive the traffic management server from any chance to trace and identify users. In the rest of the discussion, for simplicity, we term this the ITS server.

The contribution of this paper is a practical approach to achieve this goal. The novelty of our proposal lies in that: we leverage traditional authentication services by cellular infrastructures, we augment those with anonymous authentication, and we keep the ITS service separate from the mobile operator.

Users contribute encrypted, in an end-to-end manner, data to the ITS server, being anonymously authenticated. This keeps their data (location updates) confidential and unlinkable. Thus, the mobile operator cannot access such detailed location information; that is, more detailed than what mobile operators are already entrusted to maintain (they can determine roughly the whereabouts of any hand-held in their network). More specifically, our proposed architecture augments the Generic Bootstrapping Architecture (GBA), standardized by the 3GPP [4], by anonymous authentication.

In the rest of this paper, Sec. II describes the system architecture and the security requirements, Sec. III surveys related work, and Sec. IV presents our proposed architecture and its basic components. Early implementation results, in Sec. V, support the practicality of our solutions. We conclude with a brief discussion of future work.

II. System Architecture

A. Features

The proposed architecture is shown in Fig. 1. The main components of the system are the smartphones carried by each participating driver and the ITS server. A smartphone application calculates the position, using GPS or network assisted positioning such as Assisted-GPS, and it sends location updates to the main server. The server is responsible for

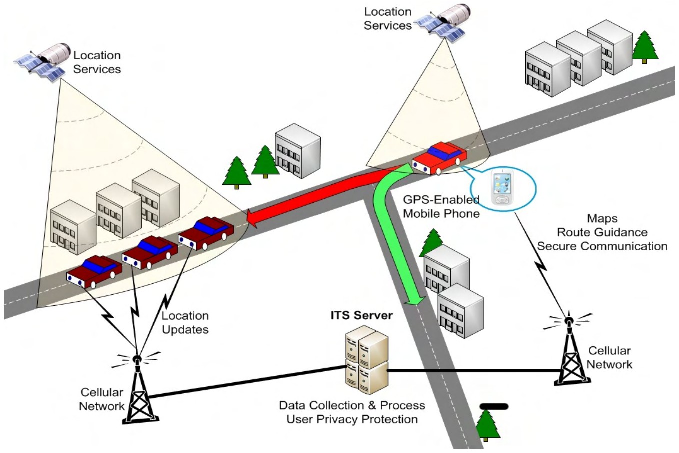

Figure 1. System Overview.

accumulating the data, for processing them and for providing feedback to the mobile client. The communication between the mobile application and the ITS server is done through the cellular network the device subscribes to. Based on the updates it receives, the ITS server reconstructs a traffic model and it calculates, in real-time, the proper feedback for guiding drivers. The updated traffic information sent by the server during the journey is presented on the device's screen on top of a map.

B. *Security requirements*

Besides the obvious benefits of smartphone-based ITS, its security and the privacy of its users are paramount. System faults, resulting for example in sending false guidance information, can deteriorate or even cause traffic congestion; or, worse even, cause road accidents. Thus, it is necessary to secure the ITS system, to ensure it provides reliable information to drivers. Equally important, sensitive user information, e.g., their identity, must not be disclosed. Towards these goals, we state the following requirements:

- **Authentication**: Entities the system must be authenticated (in particular, user smartphones and the ITS server)
- **Confidentiality**: Sensitive user information must be kept confidential.
- **Message Integrity**: Messages must be protected from alteration and the receiver must corroborate the sender (but not necessarily identify it).
- **Access Control**: Only legitimate users must be able to report their locations to the ITS server and get feedback (traffic information, instructions, etc.).
- **Anonymity**: The ITS related actions of the mobile clients must not reveal their identity.
- **Unlinkability**: The ITS server or any outsider should not be able to link two or more location updates (samples) by the same client.
- **Accountability**: In case of misbehavior, an authority should be able to disclose the identity of a client/user, and possibly revoke his/her right to be part of the system.

III. RELATED WORK

The use of mobile devices for gathering traffic information is not a new concept; several works indicate the feasibility of an ITS based only on location samples gathered by mobile phones. An early work [5] describes an analytical method for evaluating real-time ITS based on data collected from GPS devices in probe vehicles: a 3-5% of penetration in the traffic flow is enough for adequate traffic estimation. Recent experiments [6] with a system implemented solely on mobile phones show encouraging results for the feasibility and the accuracy of the traffic estimation (compared to that obtained by fixed sensors): a 2-3% penetration of mobile phones running the application in the total car flow suffices for accurate estimation of the average speed. Moreover, commercial navigation applications already integrate location samples from mobile phones in their algorithms for route guidance [2].

However, security and privacy of similar traffic systems remain open challenges and research is conducted in several projects. Successive location updates by a smartphone, even without any identifier, contain spatial and temporal correlation that can be used as indirect identifiers. These can be exploited to reconstruct user paths with tracking techniques [7]. Then traces can be processed and matched in order to infer frequently visited places, e.g., home or workplace, and finally reveal the user identity. To mitigate such threats, several solutions using cloaking techniques [8] or privacy preserving sampling techniques [9] have been proposed. These solutions are complementary to our proposal. In this paper we do not consider this kind of threat against the dataset of location samples. Rather, our goal is to guarantee the anonymity of the location samples and protect the system security.

Relevant research in security is conducted for vehicular communication systems [25]. Multiple short-term anonymized certificates, termed pseudonyms, can provide authentication while enhancing location privacy. These certificates are used for a short time and then have to be changed [10]. Group signatures are also proposed, in order to reduce the overhead of pseudonym management. As they are significantly costlier (in terms of communication and computation overhead) than classic public key cryptography, special care must be taken for the overall secure vehicular communications system design [12]. Group signatures are also used in credentials systems such as Idemix [11] that provide anonymity for authenticated transactions to services. In our proposed architecture we will use group signatures; based on initial implementation results (Sec. V), their cost can be undertaken by our system.

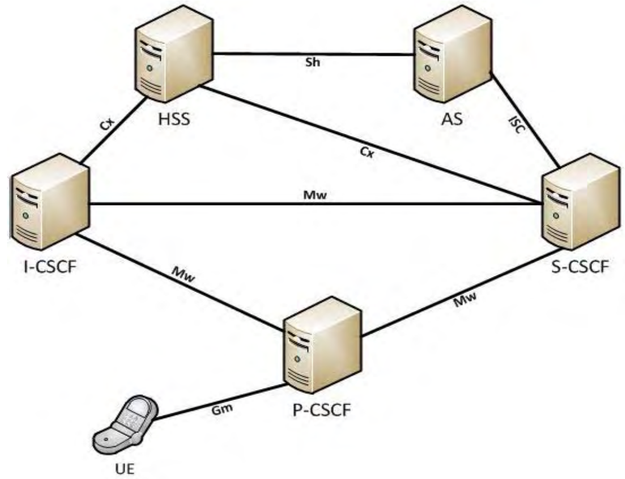

Figure 2. IP Multimedia Subsystem (IMS).

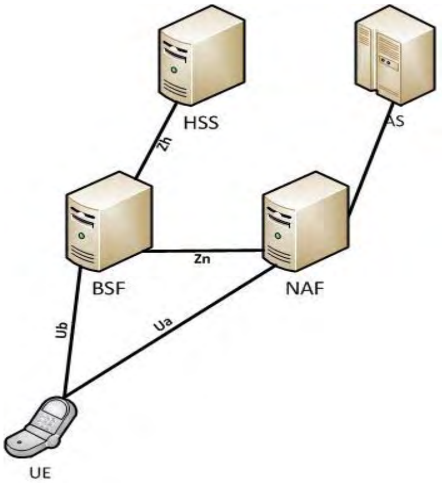

Figure 3. Generic Bootstrapping Architecture(GBA).

IV. ANONYMOUS AUTHENTICATION ARCHITECTURE

Our system collects data provided only by cellular phones. Thus, based on our security requirements (Sec. II.B.), we leverage the security features of cellular 3G/4G network architecture. As much trust is already put on the mobile operator, which can roughly determine a subscriber's location using network-based techniques, we base the authentication of our system on the mobile operator. The IP Multimedia Subsystem (IMS) framework, the Generic Authentication Architecture (GAA) [13] and the Generic Bootstrapping Architecture (GBA) [4], all proposed by 3GPP, provide the means towards that. Security on these networks relies on the Subscriber Identity mode (SIM) card and a shared key between the subscriber and the mobile operator.

In order to prevent the mobile operator from accessing to the user location updates and to address privacy requirements (anonymity, unlinkability), we propose the integration of group signatures in the GBA. In the following subsections, we describe the core IMS architecture, the GBA, the used group signatures scheme, and the proposed design.

A. *IP Multimedia Subsystem (IMS)*

IMS is the key element in the 3G/4G architecture that makes possible ubiquitous cellular access to all kinds of Internet services [14]. It was originally proposed with the vision to merge cellular networks with the Internet. Several procedures have been standardized under the scope of IMS regarding security of services, authentication and authorization [13], [4].

Fig. 2 presents the core components of the IMS. Communications are based on internet standards, namely the SIP protocol for signaling and control of the sessions (Mw, Gm interfaces) and the DIAMETER protocol (Cx, Sh interface) for AAA (Authentication, Authorization and Accounting). Therefore, the main entities in IMS are SIP servers termed Call/Session Control Functions (CSCFs). The CSCFs handle SIP signaling are categorized as follows:

- P-CSCF (Proxy-CSCF): The P-CSCF can be seen as the first access point to the IMS. It acts as an inbound/outbound SIP proxy server [14].
- S-CSCF (Serving-CSCF): The S-CSCF is a SIP Server that is the center of the IMS signaling procedures. It handles registration, routing, maintenance of sessions and enforcement of mobile operator's policy.
- I-CSCF (Interrogating-CSCF): The I-CSCF is a SIP proxy that provides routing information for SIP request/answers. It is used mainly to assign an S-CSCF to a user based on capabilities received from the HSS.

The AS (Application Server) is also a SIP entity that hosts additional services for the users; it can be on the mobile operator's side or from a third-party company. The HSS (Home Subscriber Server) is the main database of the IMS holding information about security (authentication and authorization) and user information regarding access to particular services.

B. *Generic Bootstrapping Architecture (GBA)*

In GBA, there are four main components of the authentication process, illustrated in Fig. 3: the application client, called UE (User Equipment) in the GBA context, the service application NAF (Network Application Function), the BSF (Bootstrapping Server Function), and the HSS (Home Subscriber System). The message flow is shown in Fig. 4. The UE contacts the NAF and issues a request for service access. Then the NAF informs the client application that GBA authentication is required. The UE contacts the BSF, an entity responsible to communicate with the HSS of the mobile operator. The UE sends its user-id to the BSF; with this user-id, the BSF gets the corresponding mobile client profile regarding its security settings and an Authentication Vector (AV) from the HSS. The authentication vector consists of a random number (RAND), an authentication token (AUTN), an expected response (XRES), a cipher key (CK) and an integrity key (IK). Next, the BSF forwards only the RAND and the AUTN to the UE. These two items are needed in order to run the 3G Authentication and Key Agreement (AKA) protocol. The UE first checks the AUTN to verify that the challenge originates from an authorized network. The UE runs the AKA

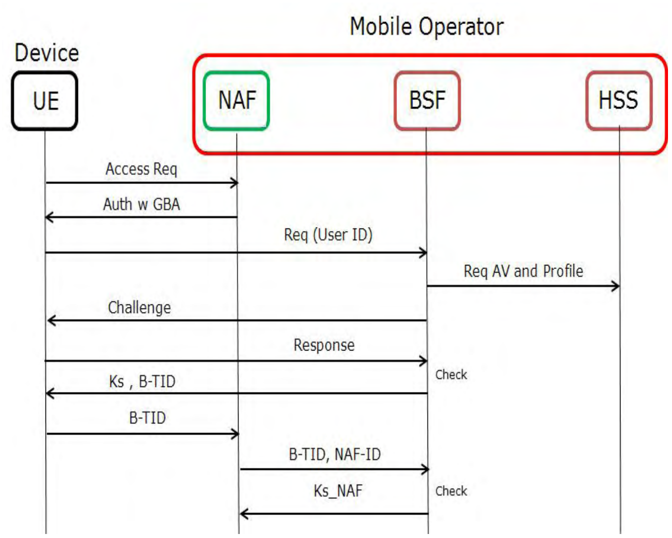

Figure 4. GBA Message Flow.

algorithm in its ISIM/USIM card and using the pre-shared key stored on the card it calculates the CK, IK and RES. The result of the procedure is that now both BSF and UE share the same session keys CK and IK. The UE calculates a Digest AKA response using RES and sends this response back to the BSF, which in turn verifies it. If the response is correct the BSF calculates the session key, Ks, by concatenating CK and IK, and it responds to the UE, indicating the success of the procedure (200OK), the key lifetime and a Bootstrapping Transaction Identifier (B-TID) to be used later by the UE. The UE also calculates the Ks concatenating CK and IK. At this point, the UE is authenticated by the BSF and they share a common secret key. Next, the UE sends an application request to the NAF along with its B-TID. The NAF contacts the BSF sending the NAF-ID and it gets the key material Ks_NAF in a reply from the BSF; the Ks_NAF is to be used for the communication with the UE. The UE derives the same key Ks_NAF based on the Ks.

After completing this procedure, the UE is authenticated by the NAF and a secure communication channel between them can be established using the Ks_NAF. The B-TID can be considered as a temporary identifier of the UE that cannot reveal any identity information of the subscriber and thus provide anonymity. However, unlinkability would not be achieved. For that, the UE would need to be configured to obtain a new B-TID each time it had a new location update to send. To overcome this obstacle, we propose the integration of group signatures.

C. Group Signatures

Group signatures, originally proposed in [15], provide anonymous authentication for an entity in a group. In our case, the group would be all the drivers (their smartphones) participating in the ITS. The basic advantage is that the verifying party (the ITS server) can validate the integrity of the update and that it originated from a legitimate member. But it remains unable to link signatures by the same user (mobile device) or to identify the user within the group. Thus, anonymity and unlinkability are achieved. Accountability is provided by the group manager, which can open a given signature and disclose the signer under special circumstances (e.g., criminal investigation).

With various group signature schemes in the literature, a scheme running on smartphones has to be efficient and produce short signatures, to keep computational and communication overhead low. In this work, we use the BBS scheme described in [16]; it generates short signatures and it does not require bilinear pair computations for the signing operation (in other words, it keeps the computation lower for the more constrained mobile client).

The scheme has four main functions:

- *Keygen*: It produces the keys for the system, namely the user private keys, **gsk**, the group manager private key, **gmsk,** and the group public key, **gpk**.
- *Sign*: It takes as inputs a message **m**, the **gpk** and a user's **gsk[i]**; it produces group signature **σ**.
- *Verify*: It takes as inputs a message **m**, the **gpk** and a signature **σ**; it verifies if **σ** is a valid signature on **m**.
- *Open*: It takes as inputs a message **m**, the **gpk**, a signature **σ** and **gmsk**; it identifies the user that issued the signature **σ**.

An interesting feature of the BBS scheme is that several values for the computation of a signature can be pre-computed; this can reduce the time needed for signing (necessary for each location update sent to the ITS server by the mobile client).

D. GBA With Group Signatures

Our architecture is shown in Fig. 5. The proposed addition to the GBA architecture is the integration of the Group Signatures Center (GSC) on the NAF. These two entities could reside on different physical servers, in which case they communicate via a standard secure channel (e.g. using TLS). Nonetheless, as they are both controlled by the mobile operator and reside in its network, we assume for simplicity in the rest of the discussion they run on the same machine.

The traffic application running on the smartphone executes first the GBA protocol between NAF and BSF as described in Sec. III. B. At the end of this procedure, UE and NAF have ended up sharing a common key Ks_NAF and the user is authenticated. The last step is for the NAF to request the GUSS (GBA User Security Settings) from the BSF. The GUSS contains information regarding the specific user and his/her authorization. GUSS specifies whether the user is a legitimate for the traffic system. If so, the NAF proceeds with having the user's private key **(gsk[i])** created by the GSC. The **gsk[i]** and the group public key **(gpk)** are sent to the UE through the secure channel already established between NAF and UE. The procedure on how to establish a secure channel with TLS and mutual authentication between UE and NAF is described in [17]. At this point, the UE is ready to start communicating with the ITS server.

To verify a legitimate user, the traffic server needs to get the **gpk**. It can communicate directly with NAF and the GSC to

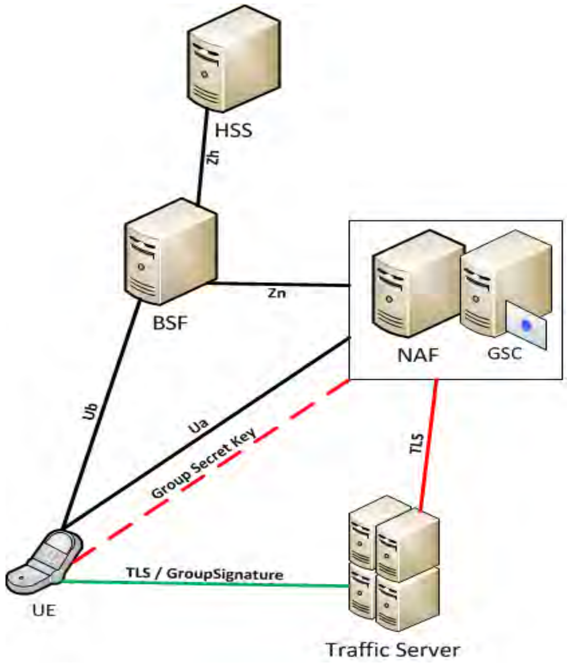

Figure 5. Proposed Architecture.

acquire the latest **gpk**. There are no special security or privacy considerations for this part besides the authentication of the NAF to the traffic server. This is required for the traffic server to be sure that it uses the correct **gpk**.

The interface of the traffic server used to accept location samples is protected with standard TLS and the traffic server must possess a valid certificate from a trusted authority. This is for the UE to authenticate the legitimate traffic server in order to be sure that it sends its location report and receives the traffic information from a trusted party. Then, for each location information packet that the UE sends, it creates a hash of the message and computes the digital signature σ using the **gpk** and his/her **gsk[i]**. Finally, it submits the message σ to the traffic server through the TLS channel established before. The server can verify the signature using the **gpk** that has been acquired from the NAF and based on that accept the message or terminate the connection.

To identify a user/client in case of misbehavior or at the request of authorities, the mobile operator and the traffic service provider must cooperate. Using the group manager's secret key (**gmsk**), the mobile operator can open the group signatures in question, provided by the ITS server, and the user can be identified. To revoke a user i from the system, the **gpk** and the unrevoked users' **gsk[j]**, for j ≠ i, must be changed. The GSC publishes a Revocation List (RL) with the private keys of the revoked users and it notifies the ITS server and the users that a new RL is available. The ITS server contacts the GSC directly to get the required parameters and the remaining users have to re-execute their authentication procedure. Then, they proceed on calculating the new keys using the procedure specified in [16].

The major advantage of our design is that authentication is separated from the location information. Authentication along with unlinkability and anonymity of location samples is achieved. Even a misbehaving ITS server or an outsider getting access to the accumulated data cannot connect the location information to a specific user, thanks to the group signature properties. Successive location updates would be linked only as long as the UE used the same TLS connection to the ITS server. However, in a real case scenario, we mandate that every time the application starts, a new connection be established with the ITS server. On the other hand, the mobile operator has access to the identity information of the user, but it cannot retrieve location data the user submits to the ITS service: those are sent directly to the ITS server through a TLS channel protected with the ITS server's public key.

V. Implementation

To evaluate our proposed solution, a full working test-bed of the IMS architecture is required. There is one open source implementation of the IMS [18] but, unfortunately, it does not support the GBA architecture. Therefore, we began by implementing the BBS scheme on an Android device in order to validate the feasibility of creating group signatures on such devices with low computational power. For our implementation, we used the Java Pairing Based Cryptography Library (jPBC) [19], a Java port of the PBC library [20] that provides the mathematical tools for pairing based operations. To initialize the scheme we use the Type A curve generator of the library with the default parameters (160 bit long group order r and 512 bit long base field q) offering 80 bits of security [21]. The size of the signature is 510 bytes. To reduce computation delays, we use the pre-computation of variables suggested in [16]. Table I presents the time (in sec) needed for one successful sign/verify operation on different Android phones we experimented with. We should note that verification on the client side is not needed, but it is presented here for completeness. Verification on the server side could be an issue, depending on the volume of signatures to be verified (proportional to number of active users). However, batch verification solutions can be applied in this case to enhance performance [22].

As expected, computation delays depend on the CPU of each smartphone. The X10i and HTC Google Nexus One have a 1 GHz Scorpion CPU while the two other ones a 600 MHz ARM 11 CPU. Although delays appear relatively high for this initial implementation, our application can be supported by smart phones. With penetration rates between 3%-5% and depending on the type of road, location sampling every 10 sec is sufficient for providing adequate traffic information [5]. To reduce overhead, calculating a signature on multiple location updates might also be an option, with the mobile client sending to the ITS server less frequently (e.g., once per minute). This approach would be dependent on the level of unlinkability of location samples needed (those bundled remain anonymous yet would be trivially linked).

TABLE I. Sign/Verify Delays (Sec)

	X10i	HTC Google Nexus One	X10i mini	HTC Legend
BBS sign	4,107	4,103	8,736	9,545
BBS verify	6,635	7,787	15,905	15,808

VI. Discussion And Conclusions

The security of the system and the privacy of its participants are two major challenges towards smartphone-based ITS. Our approach addresses these challenges by separating the authentication from the location data gathering system. Authentication for each user leverages the GBA architecture of the IMS. Then, anonymous authentication is used to access and provide data to the ITS server.

One drawback of the implemented group signature scheme is that when a user is revoked the legitimate users have to recalculate their keys. Group signatures schemes with verifier local revocation can be an alternative [12]. Furthermore, anonymous authentication in general introduces the problem of Sybil attacks against the ITS server: a misbehaving device could produce and sign multiple spurious location updates and send them to the ITS server. Due to their unlinkability, the server cannot link them to the misbehaving client and detect the abuse. Traditional approaches with pseudonyms can overcome this threat, using with certificates with non-overlapping validity [10] and one pseudonym used for each location update/sample. This variant of the pseudonym solution may have increase management cost (e.g. for preloading sufficiently many pseudonyms), but it may very well be practical due to low computational costs and the very low rates of updates for the considered traffic management application (e.g., compared to safety applications). Alternatively, the signing procedure could be controlled by a secure hardware module (e.g., SIM card) [10] or group signatures with limited number of valid signing actions [24] could be used.

Our approach enables the integration of these different cryptographic primitives to provide anonymous authentication and it leverages the mobile operator as a trusted third party. While traditional public key cryptography is easy to use on smartphones, we implemented a specific group signatures scheme, as a proof of concept to ascertain the feasibility of this type of anonymous authentication on smartphones.

In follow-up work, we plan to present a full-blown comparison of different alternatives for anonymous authentication implemented on smartphones. Moreover, their effect on the performance of a complete ITS will be evaluated, under different configurations of the system. The final target of our work is the implementation of a prototype ITS based on smartphones, integrating the security features described here.

Acknowledgment

The authors would like to thank the Swedish Foundation for Strategic Research (SSF) for funding this project.

References

[1] “Please Rob Me.” http://pleaserobme.com, accessed on 20-5-2011

[2] “TomTom.” http://www.tomtom.com, accessed on 20-5-2011

[3] “Foursquare.” http://foursquare.com, accessed on 20-5-2011

[4] 3GPP TS 33.220 “Generic Authentication Architecture (GAA); Generic bootstrapping architecture (Release 9),” 2009

[5] M. Ferman, D. Blumenfeld, and X. Dai, “An Analytical Evaluation of a Real-Time Traffic Information System Using Probe Vehicles,” Journal of Intelligent Transportation Systems, vol. 9, pp. 23-34, Mar. 2005

[6] J.C. Herrera, D.B. Work, R. Herring, X. J. Ban, Q. Jacobson, and A.M. Bayen, “Evaluation of traffic data obtained via GPS-enabled mobile phones: The Mobile Century field experiment,” Transportation Research Part C: Emerging Technologies, vol. 18, pp. 568-583, Aug. 2010

[7] J. Krumm, “Inference Attacks on Location Tracks,” Pervasive Computing, vol. 4480, pp. 127–143, 2007

[8] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, “Preserving privacy in gps traces via uncertainty-aware path cloaking,” Proceedings of the 14th ACM conference on Computer and communications security, 2007

[9] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.C. Herrera, A.M. Bayen, M. Annavaram, and Q. Jacobson, “Virtual trip lines for distributed privacy-preserving traffic monitoring,” Proceedings of the 6th International Conference on Mobile Systems, Applications and Services, 2008

[10] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure Vehicular Communication Systems: Design and Architecture,” IEEE Communications Magazine, Vol. 46, No. 11, pp. 100-109, Nov. 2008

[11] “Idemix,” http://www.zurich.ibm.com/~pbi/identityMixer_gettingStarted/, accessed on 20-5-2011

[12] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, “On the Performance of Secure Vehicular Communication Systems,” IEEE Transactions on Dependable and Secure Computing, 2011, to appear

[13] 3GPP TR 33.919 “3G Security; Generic Authentication Architecture (GAA); System description (Release 9),” 2009

[14] G. Camarillo and M.A. Garcia-Martin, “The 3G IP Multimedia Subsystem (IMS)”, Wiley, 2006

[15] D. Chaum and E. Van Heyst, “Group signatures,” Advances in Cryptology – EUROCRYPT’91

[16] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” Advances in Cryptology – CRYPTO 2004

[17] 3GPP TS 33.222 “Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS) (Release 10),” 2010.

[18] “OpenIMSCore,” http://www.openimscore.org/, accessed on 20-5-2011

[19] “Java Pairing-Based Cryptography Library (jPBC)” http://gas.dia.unisa.it/projects/jpbc/, accessed on 20-5-2011

[20] “Pairing-Based Cryptography Library.” http://crypto.stanford.edu/pbc/, accessed on 20-5-2011

[21] N. Koblitz and A. Menezes, “Pairing-based cryptography at high security levels,” Cryptography and Coding, vol. 3796, pp. 13–36, 2005

[22] A. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, “Practical short signature batch verification,” Proceedings of Cryptographers’ Track, RSA Conference, 2009

[23] D. Boneh and H. Shacham, “Group signatures with verifier-local revocation,” Proceedings of the 11th ACM Conference on Computer and Communications security, 2004

[24] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich, “How to win the clonewars: Efficient periodic n-times anonymous authentication,” Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006

[25] P. Papadimitratos, A. de La Fortelle, K. Evensen, R. Brignolo, and S. Cosenza, “Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation,” IEEE Communications Magazine, Vol. 11, No. 1, pp. 84-95, November 2009