International Journal of Research
Available at https://journals.pen2print.org/index.php/ijr/

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 03
March 2019

Secure Location Sharing Using STAMP

Mr. P.Feridoz Khan & M.Santhi Priya

#1 Asst. Professor,Dept of CSE, PBR Visvodaya Institute Of Technology And Science,Kavali,India

#2Studnet,Dept of Master of Computer Application (MCA), PBR Visvodaya Institute Of Technology And Science ,Kavali,India

ABSTRACT:

Location-based services square measure quickly changing into vastly in style. Additionally to services supported users' current location, several potential services believe users' location history, or their spatial-temporal place of origin. Malicious users might idle their spatial-temporal place of origin while not a rigorously designed security system for users to prove their past locations. during this paper, we present the SpatialTemporal provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and nontransferability of the location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. Our prototype implementation on the Android platform shows that STAMP is low-cost in terms of computational and storage resources. Extensive simulation experiments show that our entropy-based trust model is able to achieve high collusion detection accuracy

Keywords: Location Proof, Spatial-Temporal Provenance, Trust, Privacy

I.INTRODUCTION

With the pervasiveness of smart phones, Location Based Services (LBS) have received considerable attention and become more popular and vital recently. However, the use of LBS also poses a potential threat to user's location privacy. In this project, we present an efficient and privacy-preserving location-based query solution, called APPLAUS and LOCATEme. Specifically, to achieve privacy-preserving spatial range query, we propose the first predicate-only encryption scheme for inner product range (Pseudonym object PO), which can be used to detect whether a position is within a given circular area in a privacy-preserving way. To reduce query latency, we further design a privacy-preserving index structure in LOCATEme. Detailed security analysis confirms the security properties of LOCATEme. In particular, for a mobile LBS user using an Android phone, around 1.9 s is needed to generate a query, and it also only requires a commodity workstation.

Today's location-sensitive service relies on user's mobile device to determine its location and send the location to the application. This approach allows the user to cheat by having his device transmit a fake location, which might enable the user to access a restricted resource erroneously or provide bogus alibis. To address this issue, we propose a privacy preserving location proof updating system (APPLAUS) in which co-located Bluetooth enabled mobile devices mutually generate location proofs, and update to a location proof server.

To develop periodically changed pseudonyms that can be used by the mobile devices to protect source location privacy from each other, and from the untrusted location proof server. We also develop user-centric location privacy model in which individual users generate their location privacy preserving pseudonym objects in real-time and decide whether and when to accept a location proof exchange request based on their location privacy levels. The main objective is to provide privacy preserving location proof updates for all Location Based Services (LBS), existing and new ones. LOCATEme can be implemented with the existing network

infrastructure and the current mobile devices, and can be easily deployed in Bluetooth enabled mobile devices with little computation or power cost.

2.LITERATURE SURVEY

1)A Secure verification of location claims

AUTHORS: N. Sastry, U. Shankar, and D. Wagner,

With the growing prevalence of sensor and wireless networks comes a new demand for location-based access control mechanisms. We introduce the concept of secure location verification, and we show how it can be used for location-based access control. Then, we present the Echo protocol, a simple method for secure location verification. The Echo protocol is extremely lightweight: it does not require time synchronization, cryptography, or very precise clocks. Hence, we believe that it is well suited for use in small, cheap, mobile devices.

2)Location Verification using Secure Distance Bounding Protocols.

AUTHORS: D. Singelee and B. Preneel,

Abstract— Authentication in conventional networks (like the Internet) is usually based upon something you know (e.g., a password), something you have (e.g., a smartcard) or something you are (biometrics). In mobile ad–hoc networks, location information can also be used to authenticate devices and users. We will focus on how a prover can securely show that (s)he is within a certain distance to a verifier. Brands and Chaum proposed the distance bounding protocol as a secure solution for this problem. However, this protocol is vulnerable to a so– called "terrorist fraud attack". In this paper, we will explain how to modify the distance bounding protocol to make it resistant to this kind of attacks. Recently, two other secure distance bounding protocols were published. We will discuss the properties of these protocols and show how to use it as a building block in a location verification scheme.

3)**A privacy-aware location proof architecture AUTHORS:** W. Luo and U. Hengartner,

Recently, there has been a dramatic increase in the number of location-based services, with services like Foursquare or Yelp having hundreds of thousands of users. A user's location is a crucial factor for enabling these services. Many services rely on users to correctly report their location. However, if there is an incentive, users might lie about their location. A location proof architecture enables users to collect proofs for being at a location and services to validate these proofs. It is essential that this proof collection and validation does not violate user privacy. We introduce VeriPlace, a location proof architecture with user privacy as a key design component. In addition, VeriPlace can detect cheating users who collect proofs for places where they are not located. We also present an implementation and a performance evaluation of VeriPlace and its integration with Yelp.

4)Distance-bounding proof of knowledge to avoid real-time attacks, AUTHORS: L. Bussard and W. Bagga

Traditional authentication is based on proving the knowledge of a private key corresponding to a given public key. In some situations, especially in the context of pervasive computing, it is additionally required to verify the physical proximity of the authenticated party in order to avoid a set of real-time attacks. Brands and Chaum proposed distance-bounding .protocols as a way to compute a practical upper bound on the distance between a prover and a verifier during an authentication process. Their protocol prevents frauds where an intruder sits between a legitimate prover and a verifier and succeeds to perform the distance-bounding process. However, frauds where a malicious prover and an intruder collaborate to cheat a verifier have been left as an open issue. In this paper, we provide a solution preventing both types of attacks.

5)Practical and provably-secure commitment schemes from collision-free hashing
AUTHORS: S. Halevi and S. Micali,
We present a very practical string-commitment scheme which is provably secure based solely on collision-free hashing. Our scheme enables a computationally bounded party to commit strings to an unbounded one, and is optimal (within a small constant factor) in terms of interaction, communication, and computation. Our result also proves that constant round statistical zero-knowledge arguments and constant-round computational zero-knowledge proofs for NP exist based on the existence of collision-free hash functions.

3.THE STAMP SCHEME

A. Preliminaries

1) Location Granularity Levels: We assume there are n granularity levels for each location, which can be denoted by $L_1 L_2 \ldots L_n$, where L_1 represents the finest location granularity (e.g., an exact Geo coordinate), and L_n represents the most coarse location granularity (e.g., a city). Hereafter, we refer to location granularity level as *location level* for short. When a location level L_x is known, we assume it is easy to obtain a corresponding higher location level L_y where $y > x$. The semantic representation of location levels are assumed to be standardized throughout the system.

2) Cryptographic Building Blocks: STAMP uses the concept of *commitments* to ensure the privacy of provers. A commit-ment scheme allows one to commit to a message while keeping it hidden to others, with the ability to reveal the committed value later. The original message cannot be changed after it is committed to. A commitment to a message M can be denoted as $C(M,r)$ where r is a nonce used to randomize the commitment so that the receiver cannot reconstruct M, and the commitment can later be verified when the sender reveals both M and r. A number of commitment schemes [14]–[16] have been pro-posed and commonly used. Our system does not require a spe-cific commitment scheme. Any scheme which is perfect binding and computational hiding can be used. In our implementation, we used [14], which is based on one-way hashing.

One-way hash functions have the similar binding and hiding properties as commitment schemes. However, for privacy pro-tection purpose, we do not use hash functions because they are vulnerable to *dictionary* attacks. An adversary who has a full list of possible inputs could run an exhaustive scanning over the list to crack the input of a hash function.

TABLE I

LIST OF NOTATIONS

$M_1 \| M_2$	Concatenation of messages M_1 and M_2
K_u^+	Public key of user u
K_u^-	Private key of user u
$E^K(M)$	Encryption of message M with key K
$H(M)$	One-way hashing of message M
$C(M,r)$	Commitment to message M with nonce r

We assume every user has the ability to generate one -time symmetric keys. All parties have agreed upon a one-way hash function and a commitment scheme. The commitment scheme is implemented based on any pseudo-random generator. All cryp-tographic notations have been summarized in Table I.

3) Distance Bounding: A location proof system needs a prover to be securely localized by the party who provides proofs. A distance bounding protocol serves the purpose. A distance bounding protocol is used for a party to securely verify that another party is within a certain distance [17]. Different types of distance bounding protocols have been studied and proposed. A most popular category is based on *fast-bit-ex-change* : one party sends a challenge bit and another party replies with a response bit and vice versa. By measuring the round-trip time between the challenge and the response, an upper bound on the distance between the two parties can be calculated. This fast-bit-exchange phase is usually repeated a number of times.

One of the most challenging problems in distance bounding is the Terrorist Fraud attack, i.e., the P-P collusion scenario. The Terrorist Fraud attack is hard to defend against because a fast-bit-exchange process demands no processing delay (or at least extremely small processing delay) at the prover end be-tween receiving a challenge bit and replying a response bit [17]. Thus, signing cannot be executed in the middle of a fast-bit-ex-change, which means a hidden communication tunnel between two colluding parties allows them to execute fast-bit-exchange and signing separately. Thereby, one is only certain that the party who executed the fast-bit-exchange is nearby, but the party may not actually possess the private key of the identity who he/she claimed to be.

To the best of our knowledge, three existing distance bounding protocols [9], [18], [19] addressed the Terrorist Fraud attack. The schemes proposed in [18], [19] are based on pre-established shared secrets, and thus does not fit our scheme considering the anonymity requirement between a prover and a witness. The Bussard-Bagga protocol proposed in [9] is based on a zero-knowledge proof technique, and it allows the prover to be authenticated via a private/public key pair. Hence, we adopt the Bussard-Bagga protocol as our distance bounding protocol. The protocol consists of three stages. The first stage is the *preparation* stage, where the prover encrypts his/her private key K^- with a random symmetric key k and gets an encrypted message e. The prover then commits to each bit of e and k, resulting two sequences of bit commitments C_e and C_k . In the second *distance bounding* stage, the prover sends C_e and C_k to the location verifier (or the witness in our context), the location verifier then starts a multi-round fast-bit-exchange. In round i, the prover replies the ith bit of k or e depending on the challenge bit. Since the location verifier never learns both bit values, he/she can never learn about K^- . After the fast-bit-exchange, the location verifier de-commits and verifies the corresponding bit commitments in C_e and C_k (only for the received bits) by asking the prover to provide the nonces used for those commitments. In the third *zero-knowledge proof* stage, the prover convinces the verifier that he/she knows K^- through a zero-knowledge proof. It is not possible for a user to give away the values of k and e, which would mean that K^- is given away. Because of this, the protocol is not vulnerable to the Terrorist Fraud attack. In the scenario we are considering, a witness does not know the identity of a prover, we therefore cannot rely on the witness only to authenticate the prover via the zero -knowledge proof. We integrate the Bussard-Bagga protocol into STAMP by breaking up its execution and have the witness and verifier jointly authenticate the prover. The details are given in Section V-B.

4.RESULTS AND DISCUSSION

Sharing Data To The admin using encryption technique

Viewing sent information by user

5.CONCLUSION

In this projet we have presented STAMP, which aims at providing security and privacy assurance to mobile users' proofs for their past location visits. STAMP relies on mobile devices in vicinity to mutually generate location proofs or uses wireless APs to generate location proofs. Integrity and non-transferability of location proofs and location privacy of users are the main design goals of STAMP. We have specifically dealt with two collusion scenarios: P-P collusion and P-W collusion. To protect against P-P collusions, we integrated the Bussard-Bagga distance bounding protocol into the design of STAMP. To detect P-W collusion, we proposed an entropy-based trust model to evaluate the trust level of claims of the past location visits. Our security analysis shows that STAMP achieves the security and privacy objectives. Our implementation on Android smartphones indicates that low computational and storage resources are required to execute STAMP. Extensive simulation results show that our trust model is able to attain a high balanced accuracy with appropriate choices of system parameters.

REFERENCES

[1]S. Saroiu and A. Wolman, “Enabling new mobile applications with location proofs,” in Proc.

ACM HotMobile, 2009, Art. no. 3.

[2]W. Luo and U. Hengartner, “VeriPlace: A privacy-aware location proof architecture,” in Proc.

ACM GIS, 2010, pp. 23–32.

[3]Z. Zhu and G. Cao, “Towards privacy-preserving and colluding-resistance in location proof updating system,” IEEE Trans. Mobile Comput., vol. 12, no. 1, pp. 51–64, Jan. 2011.

[4]N. Sastry, U. Shankar, and D. Wagner, “Secure verification of location claims,” in Proc. ACM WiSe, 2003, pp. 1–10.

[5]R. Hasan and R. Burns, “Where have you been? secure location provenance for mobile devices,” CoRR 2011.

[6]B. Davis, H. Chen, and M. Franklin, “Privacy preserving alibi systems,” in Proc. ACM ASIACCS, 2012, pp. 34–35.

[7]I. Krontiris, F. Freiling, and T. Dimitriou, “Location privacy in urban sensing networks: Research challenges and directions,” IEEE Wireless Commun., vol. 17, no. 5, pp. 30–35, Oct. 2010.

[8]Y. Desmedt, “Major security problems with the ‘unforgeable’ (feige)- fiat-shamir proofs of identity and how to overcome them,” in Proc. SecuriCom, 1988, pp. 15–17.

[9]L. Bussard and W. Bagga, “Distance-bounding proof of knowledge to avoid real-time attacks,” in Security and Privacy in the Age of Ubiquitous Computing. New York, NY, USA: Springer, 2005.

[10]B. Waters and E. Felten, “Secure, private proofs of location,” Department of Computer Science, Princeton University, Princeton, NJ, USA, Tech. Rep., 2003.

[11]X. Wang et al., “STAMP: Ad hoc spatial-temporal provenance assurance for mobile users,”in Proc. IEEE ICNP, 2013, pp. 1–10.

[12]A. Pfitzmann and M. Köhntopp, “Anonymity, unobservability, and pseudonymity-a proposal for terminology,” in Designing Privacy Enhancing Technologies. New York, NY, USA:Springer, 2001.

[13]Y.-C. Hu, A. Perrig, and D. B. Johnson, “Wormhole attacks in wireless networks,” IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 370–380, Feb. 2006.

[14]S. Halevi and S. Micali, “Practical and provably-secure commitment schemes from collision-free hashing,” in Proc. CRYPTO, 1996, pp. 201–215.

Author’s Profile:

P.FERIDOZ KHAN has received his M.Tech from PBR Visvodaya Institute of Technology & Science Now He is dedicated to teaching field from the last 8 years. He has Guided 5 U.G students. At present he is working as Assistant Professor in PBR Visvodaya Institute of Technology & Science, Kavali, and Andhra Pradesh, India.

M.SANTHI PRIYA, pursuing Master of Computer Application (MCA) from PBR Visvodaya Institute of Technology and Science, Kavali, Nellore (dt),Andhra Pradesh