View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by International Journal of Science Engineering and Advance Technology (IJSEAT)

IJSEAT International Journal of Science Engineering and Advance Technology

Spatial Temporal Provenance For Generating Location Proofs In Distributed Setting

1M.Lakshmi Sravani, 2S V Krishna Reddy
1(P.G.STUDENT) M.Tech in CSE, 2 Assistant Professor in CSE
Dept. computer science and engineering
Kakinada Institute of Engineering and Technology, for Women,Korangi, AP, INDIA

ABSTRACT:
We propose a STP proof conspire named Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP). STAMP goes for guaranteeing the uprightness and non-transferability of the STP proofs, with the capacity of ensuring clients' protection. The majority of the current STP evidence plans depend on remote framework (e.g., WiFi APs) to make proofs for portable clients. Notwithstanding, it may not be attainable for a wide range of uses, e.g., STP pros for the green commuting and combat zone cases unquestionably can't be gotten from wireless APs.

KEYWORDS: collusion detection, verifiers, decentralized protocol.

I. INTRODUCTION:

We plan our framework with a goal of securing clients' obscurity and area protection. No gatherings other than verifiers could see both a client's personality and STP data (verifiers require both character and STP data with a specific end goal to perform confirmation and give administrations). Clients are given the adaptability to pick the area granularity level that is uncovered to the verifier. We look at two sorts of plot assaults: (1) A client who is at a proposed area takes on the appearance of another conniving client B and acquires STP proofs for B. This assault has never been tended to in any current STP verification plans. (2) Colluding clients commonly produce counterfeit STP proofs for each other. There have been endeavors to address this kind of conspiracy. In any case, existing arrangements experience the ill effects of high computational cost and low versatility. Especially, the last agreement situation is in actuality the testing Terrorist Fraud assault [8], which is a basic issue for our focused on framework, however none of the current frameworks has tended to it.

LITERATURE SURVEY:

[1],An explanation gives confirmation of a man's past area and can be basic in demonstrating ones blamelessness. A plausible excuse includes two gatherings: the proprietor, who profits by the justification, and the corroborator, who affirms for the proprietor. As cell phones end up plainly pervasive, they can figure out where we are and what we are doing, and enable us to build up confirmation of our area as they to go with us on our day by day exercises. Existing area based administrations like Google Latitude would already be able to track and record everything we might do, yet these frameworks expect us to uncover our character when recording our area. This leaves our protection in danger, and requires a put stock in outsider to keep up our area data.

[2],we display the principal symmetric key based separation jumping convention that is likewise impervious to purported psychological oppressor misrepresentation, a variation of mafia extortion. Separation bouncing conventions require a correspondence channel that can trade single bits with greatly low inertness. This capricious correspondence prerequisite has incited Hancke and Kuhn to attest in a current distribution that ultra wide band (UWB) radio is important to accomplish a helpful separation bouncing determination for RF security gadgets (contactless keen cards, RFID labels and so forth). We investigate this statement and present an option, novel correspondence approach that use the wonders of side channel spillage to convey a low inertness channel. Our proposition is equipped for distinguishing modern hand-off assaults without turning to the significant cost and intricacy of UWB radio.

PROBLEM DEFINITION

The greater part of the current STP evidence plans depend on remote foundation (e.g., WiFi APs) to make proofs for versatile clients. Be that as it may, it may not be plausible for a wide range of uses, e.g., STP proofs for the green driving and front line illustrations surely can't be gotten from remote APs.

A large portion of the current plans require various trusted or semi-trusted outsiders.

PROPOSED APPROACH

STAMP requires just a solitary semi-trusted outsider which can be installed in a Certificate Authority (CA).

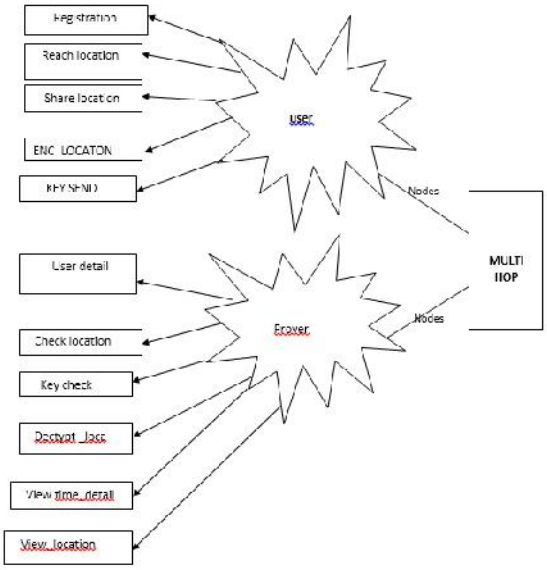
We outline our framework with a target of ensuring clients' namelessness and area security.

No gatherings other than verifiers could see both a client's character and STP data (verifiers require both personality and STP data keeping in mind the end goal to perform check and give administrations).

STAMP requires low computational overhead.

A security examination is exhibited to demonstrate STAMP accomplishes the security and protection targets.

SYSTEM BLOCK DIAGRAM:



PROPOSED METHODOLOGY:

PROVER:

Prover needs to uncover the two his/her personalities and STP data so as to get administrations from a verifier, the prover does not really believe the verifier totally. At the point when a prover tries to assert his/her area at a specific time to a verifier, he/she ought not be committed to uncover his/her most exact area to the verifier.

WITNESS:

A witness who gets a chooses in the event that he/she acknowledges the demand. On the off chance that the demand is acknowledged, the witness sends a back to the prover, after which, the two gatherings begin the execution of the separation bouncing phase of the Bussard-Bagga convention. This empowers the observer to realize that the gathering who is asking for a STP confirmation is inside a specific range. Be that as it may, the witness has no real way to check if the gathering has the private key which in truth compares to the conferred personality.

VERIFIER:

At the point when a prover experiences a verifier (the recurrence of such experiences is particular to the application situations) and he/she plans to make a claim about his/her past STP to the verifier, the STP claim and confirmation stage happens between the prover and the verifier. A piece of the check work must be finished by CA

CERTIFICATE AUTHORITY (CA):

Clients have one of a kind open/private key sets, which are set up amid the client enrollment with CA and put away on clients' close to home gadgets. There are solid motivators for individuals not to give their security away totally, even to their families or companions, so we accept a client never gives his/her cell phone or private key to another party.

ALGORITHM:

NEW ENHANCED STAMP PROTOCOL:

INPUT:M,KPUB,KPRI,H,C,EK

STEP1: STP proof generation phase is the process of the prover getting an STP proof from one witness.

STEP2: STP proof collection event may consist of multiple STP proof generations.

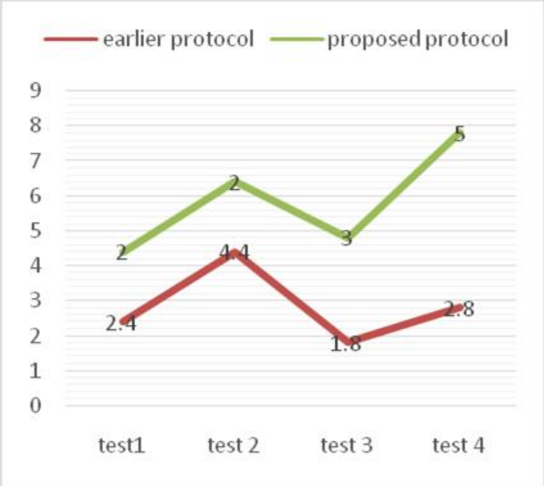
STEP3: The prover finally stores the STP proofs he/she collected in the mobile device.

STEP4: a prover encounters a verifier and he/she intends to make a claim about his/her past STP to the verifier.

STEP5: STP claim and verification phase takes place between the prover and the verifier.

STEP6: communication between the verifier and CA happens in the middle of the STP claim and verification phase.

RESULTS:



The results shows the proposed approach demonstrations effective performance in terms of security and communication as well as computation overhead compared to earlier procedure.

EXTENSION WORK:

We propose a client characterized protection grid framework called dynamic network framework to give security saving preview and nonstop LBS. The fundamental thought is to put a semitrusted outsider, named question server, between the client and the specialist co-op. QS Only should be semi-trusted on the grounds that it won't gather/store or even approach any client area data.

CONCLUSION:

Trustworthiness and non-transferability of area confirmations and area protection of clients are the fundamental outline objectives of STAMP. Our security examination demonstrates that STAMP accomplishes the security and protection targets.

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.

[15] I. Damgård, “Commitment schemes and zero-knowledge protocols,” in Proc. Lectures Data Security, 1999, pp. 63–86.

PROFILES

M. Lakshmi Sravaniis a student of Kakinada Institute of Engineering and Technologyfor Women, Korangi,. Currently, she is pursuing her M.Tech, specializing in CSE department.

Mr. S V KRISHNA REDDY, isan efficient teacher,He is working as an Assistant Professor in Department of C.S.E, Kakinada Institute of Engineering and Technology(KIET-W), korangi, Kakinada. He has 7 years of teaching experience. He has supported many students to publish many papers in both National & International Journals. His area of Interest includesDBMS, Data mining and data warehousing, mobile computing, uml&dp, Data structures, Design and analysis of algorithms.