LOCOPRO - The Location Provenance System

Sudarshan B. Banote	Department of Computer Engineering, Pravara Rural Engineering College,Loni, Savitribai Phule Pune University, Pune
Mahesh S. Barwat	Department of Computer Engineering, Pravara Rural Engineering College,Loni, Savitribai Phule Pune University, Pune
Kaustubh D. Jagtap	Department of Computer Engineering, Pravara Rural Engineering College,Loni, Savitribai Phule Pune University, Pune
Akshay B. Shekade	Department of Computer Engineering, Pravara Rural Engineering College,Loni, Savitribai Phule Pune University, Pune
Prof. M. R. Kharade	Department of Computer Engineering, Pravara Rural Engineering College,Loni, Savitribai Phule Pune University, Pune

Abstract:

Mobile device users use location-based services to access various services with user's current physical location information. Some of its applications e.g. supply chain verification; It particularly requires an ordering of location proofs. It is a significant challenge in some user based architectures for users to prove their presence and the path of travel along with a privacy-protected and insecure manner.

Till now, some schemes for location proofs are generally are not resistant to factors such as tampering, collusion attacks also they do not preserve the provenance. They are not that much flexible for users to prove their provenance of location proofs. In this paper, we present a ready-to-deploy framework for generating and validating witness-oriented asserted location provenance records. This framework is based on the asserted location proof (ALP) protocol for generating secure location provenance on the android devices. This framework allows user-centric, collusion resistant, tamper-evident, privacy protected, verifiable, and provenance preserving location proofs for android devices.

Introduction:

The system is based on the Asserted Location Proof (ALP) protocol for secure location provenance. The proposed framework is a suite of production-ready applications. It is a ready-to-deploy framework for secure, witness-oriented, and provenance preserving location proofs. It generates secure and tamper-evident location provenance items from a given location authority. It is based on the Asserted Location Proof protocol and Features a web-based the service provider, raspberry pi based location authority server, an Android-based user application, and an auditor application for location provenance validation. The system is

applicable in various areas mainly including government sectors, private sectors, Industries; NGO's where the concept of location and asserted proof presence can be used.

Some of the self-reported location presence using Global Positioning System (GPS) coordinates, cell triangulation system in mobile phones, and IP address tracking these all techniques can fall victim to manipulated and false location declaration. Uninterrupted tracking of users by the service providers including third-party applications breaks the privacy of the user, allows traceable identities, and the user becomes defenseless against untrusted service providers. The service providers may also sell the location data of their users taking advantage of the small text in the service agreements. Information provenance is very important for tracing the authenticity of data. The provenance of location is an important requirement in some scenarios
.
In this paper, we use a localization authority which covers the area utilizing the secure distance bounding mechanism for ensuring the user's presence when the user requests for a location proof. Although, some of the existing systems are collusion attack resistant as well as the provenance of the location proofs. But still, related works have not considered third party interruption and the chronological ordering for secure location proofs together, which makes the schemes unsafe to collusion attacks and tampering. The following illustrates the practicality of a secure and asserted location provenance framework.

Suresh is a government servant in an inspection department. He requires to travel to given particular draught hit areas and create a daily report of the status. Unfortunately, Suresh is charged with negligence towards his job when the higher authority claimed that he was not serious about his job and generated fake reports. The inspection report that Suresh presented was discarded for being a false as higher authorities claimed that Suresh did not visit the site. In an alternate scenario, Suresh collects location provenance records as he visits each of the sites, which are asserted by a witness. Therefore, Suresh can then prove his regular visits and the order of visit to each of the sites based on these secure location provenance records
.
In this paper, we present the Location provenance framework using ALP protocol. The system is based on the Asserted Location Proof (ALP) protocol for secure location provenance. This
The framework is a complete suite of production-ready applications. It features a web-based service provider, a raspberry pi-based location authority server, and an Android-based user app also a desktop based auditor.

Applications:

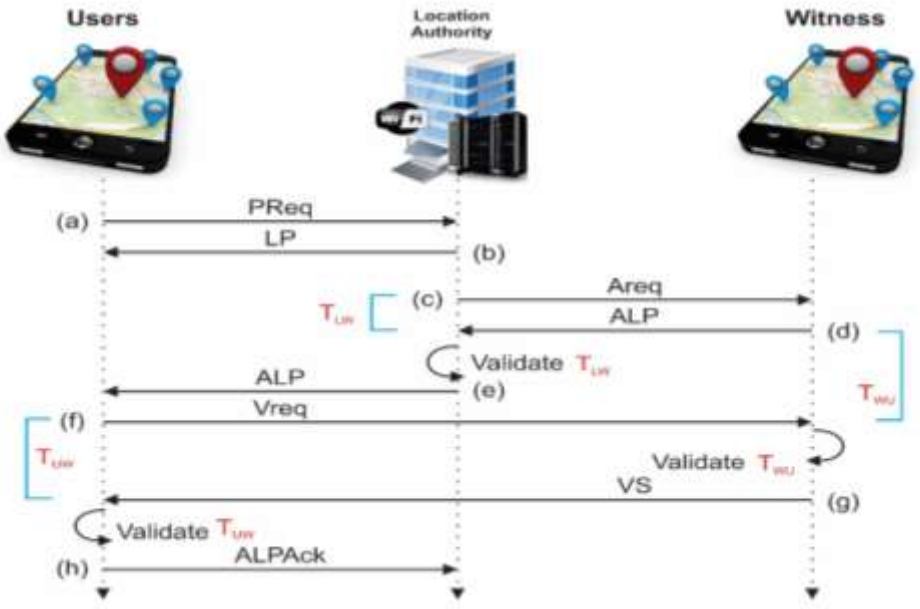
Assertion oriented location provenance schemes will be effectively utilized in a range of real-life situations. Our solution emphasizes the device's presence and can be an extremely applicable technology for instrumentation handling businesses. At present, most high-end devices return with
networking options and intrinsic memory. Hence, these expensive devices may simply be monitored for presence at their specific locations. The concept of location provenance and witnesses will conjointly be applied to different domains, such as in preserving the integrity of offer chain data for various product and services. A fascinating application is often created at

organizations who have traveling business or workers. Travelers can collect the declared location provenance things on their mobile devices. Later, they can utilize the proofs to alter subsequent processes, such as travel expense claims and itinerary management, in a safe and reliable fashion. The whole mechanism of asserted proofing might be utilized during a reversed witness bound application. Instead of a user showing the proofs as evidence of presence, witnesses can give notarized records as a proof of specific users visiting an explicit location. Taking the example of insurance agents, construction site inspectors, and relief workers, the presence of these people area unit a lot of involved in their various fields of action. Witnesses at the particular sites will provide their endorsements as proof of visit for the agents on the field.

Framework Architecture:

Four entities are used in the framework: The Android app mobile device users (user/witness), the *Location authority*, the auditor, and the *Service Provider*. In this asserted location provenance protocol, a user *U* visits a site *S*, which is maintained by a *Location Authority*. Furthermore, there are some of the witness devices indicated by W; they are registered with the *Location Authority*, also they are willing to serve in asserting the location provenance. The *Service Provider* is the only authorized entity in the architecture, it is responsible for managing the accounts of the other entities, it provides authentication and public keys.

The Communications between *Location Authority* and android mobile users are done using TCP. All messages are secured using the private key of respective entities and are verified using the public key. An entity receives the public key of another entity from the *Service Provider*. All communications with the *Service Provider* occur through the public network using HTTPS. The different phases of the protocol have been outlined, such that, to ensure the location proof is unaffected by collusion



Conclusion:

Evolving location-based services have generated a requirement for secure and dependable location provenance mechanisms. Assortment and verification of location proofs and also the preservation of the chronological order has important reality applications. During this paper, we tend to introduce a ready to deploy framework for safe, witness-oriented, and provenance protective location proofs. Our framework permits generating secure and tamper-evident location provenance things from a given location authority, that are supported by a collocated witness. Our framework is predicated on the asserted Location Proof protocol and is increased with provenance preservation. The framework options a web-based service supplier, desktop-based location authority server, associate Android-based user application, associated an auditor application for location validation.

References:

[1] Benjamin Davis, hao chen and Matthew franklin.
Privacy preserving alibi systems, ASIACCS'May 2-4,2012, Seoul, Korea.

[2] Rashib khan, Md Munirul Haque, and Ragib Hasan, Towards supply chain information integrity preservation crossTalk-September/October 2015.

[3] Stefan Saroiu and Alec Wolman's Enabling new mobile application with location proofs, Microsoft Research, February 23-24,2009, Santa Cruz, CA, USA

[4] Rashib khan, Md Munirul Haque, Shams Zawoad, and Ragib Hasan's, WORAL: A witness-oriented secure location provenance framework for mobile devices, 2168-6750 IEEE. VOLUME 4.1. MARCH 2016.