Government Degree College::Khairatabad

A.Y. 2021-22

Student Study Projects

Department of Computer Science & Applications

Government Degree College::Khairatabad

Student Study Projects

Project Report
On
“WORAL: A Witness Oriented Secure Location Provenance Framework for Mobile Devices”

By

114019405326 - R. NIKHIL
114019405341 - S. SWATHI
114019405236 - M. NAVEEN KUMAR
114019405187 - K. SAI TEJA REDDY
114019405127 - G. ALEKHYA

Under the supervision of
G. Radhika

Department of Computer Science & Applications

Table of Contents

SYNOPSIS

TITLE:

WORAL: A Witness Oriented Secure Location Provenance Framework for Mobile Devices

ABSTRACT:

Location-based services allow mobile device users to access various services based on the users' current physical location information. Path-critical applications, such as supply chain verification, require a chronological ordering of location proofs. It is a significant challenge in distributed and user-centric architectures for users to prove their presence and the path of traveling a privacy-protected and secure manner. So far, proposed schemes for secure location proofs are mostly subject to tampering, not resistant to collusion attacks, do not offer preservation of the provenance, and are not flexible enough for users to prove their provenance of location proofs. In this paper, we present WORAL, a complete ready-to-deploy framework for generating and validating witness oriented asserted location provenance records. The WORAL framework is based on the asserted location proof protocol and the OTIT model for generating secure location provenance on the mobile devices. WORAL allows user-centric, collusion resistant, tamper-evident, privacy protected, verifiable, and provenance preserving location proofs for mobile devices. This paper presents the schematic development, feasibility of usage, comparative advantage over similar protocols, and implementation of WORAL for android device users including a Google Glass-based client for enhanced usability.

I. INTRODUCTION

Mobile devices have enhanced the use of location-based services (LBS) using the geographical locations of the devices. LBS use location tags, such as in social networks, shopping coupons, traffic alerts, and travel logs. However, LBS dependent on location proofs collected by the user have more interesting features and applications. An auditor can later verify the claim of presence with respect to the user's identity, the location in question, and the time when the user was present at that location. However, untrustworthy location reporting has implications ranging from trivial cases, such as, cheating in social-games to national security issues.

Self-reported location presence using Global Positioning System (GPS) coordinates, cell triangulation in mobile phones, and IP address tracking are all susceptible to manipulated and false location claims. Continuous tracking of users by service providers including third-party applications violates the users' privacy, allows traceable identities, and makes the users 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. Buggy and insecure implementations aggravate the situation even further.

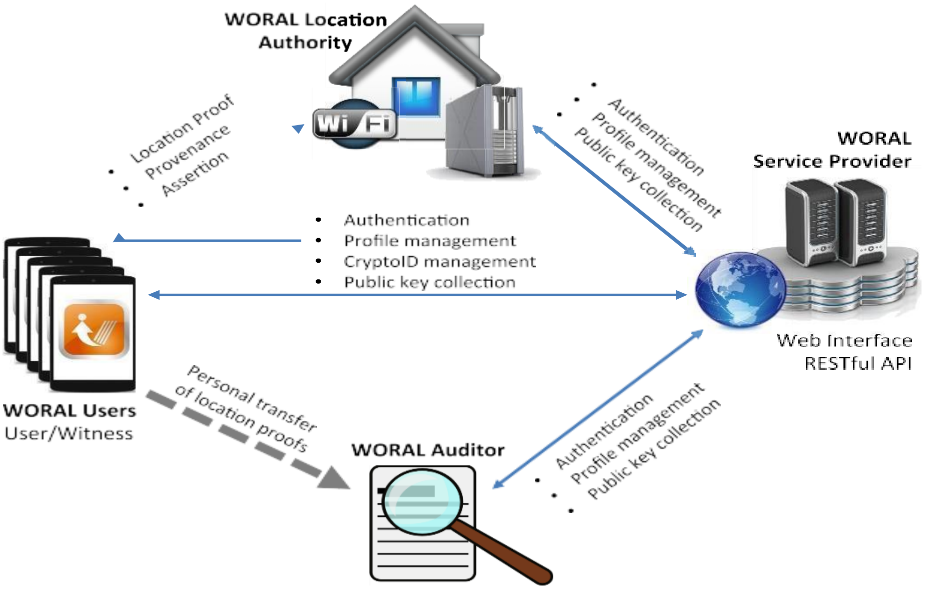
Provenance of information is important for tracing the authenticity of the data back to its source. The provenance of location is a crucial requirement in path critical scenarios. A valid claim of travel path needs to be verified in terms of the location provenance. The integrity of a product may be highly justified by the supply chain and the inter- mediate locations which the product travels through. Provenance for location is a continuous process and is required to be preserved as the user travels around collecting location proofs. Unlike general data items, the sequence in which the locations are traveled needs to be preserved in chronological order within the provenance chain. As a result, location provenance portrays a greater challenge than that for general data items. There have been numerous proposals for allowing user initiated location proof generation.

A localization authority covering the area utilizes some secure distance-bounding mechanism to ensure the user's presence when the user requests for a location proof. However, existing mechanisms overlook collusion attacks as well as the provenance of the location proofs. Related works thus far have not considered third- party endorsement and the chronological ordering for secure location proofs together, which makes the schemes vulnerable to collusion attacks and tampering with the order of the proofs. The following illustrates the practicality of a secure and asserted location provenance framework.

In this Project, we present the Witness Oriented Asserted Location provenance (WORAL) framework. The system is based on the Asserted Location Proof (ALP) protocol and incorporates the OTIT model for secure location provenance. The WORAL framework is a complete suite of production-ready applications, featuring a web-based service provider, a desktop-based location authority server, an Android-based user app, a Google Glass-based client, anda desktop-based auditor.

II. WORAL ARCHITECTURE

Four entities are involved in the WORAL framework: the WORAL mobile device users (user/witness), the *LA*, auditor, and the *SP*. In the secure asserted location provenance protocol, a user *U* visits a site *S*, which is maintained by an *LA*. Additionally, there are a number of witness devices *W*, which are registered with the *LA*, and are willing to serve in asserting the location provenance items. The *SP* is the only centralized entity in the WORAL architecture, which is responsible to manage the accounts of the other three entities, provide authentication, and distribute public keys. Figure 1 depicts the overview of the proposed architecture.



A. DEPENDENCIES ON SERVICE PROVIDER

1) ACCOUNT CREATION AND AUTHENTICATION

In the WORAL framework, users, witnesses, *LA*s, and auditors need to create an account with the *SP* using a unique identification criteria. Such systems can include the Social Security Number, passport number, driving license, trade license, or anything else which unambiguously identifies the person or the organization. While setting up the account, each entity needs to provide a unique username/password, which is later used as login credentials for all the entities.

As the *LA* and auditor need to be authorized entities, there is an account verification stage for these two entities. The *SP* verifies the *LA* and auditor account requests and sends them a service code. *LA*s and auditors cannot access their accounts until the accounts are activated using the service code received from the *SP*.

2) CRYPTOID AND KEY DISTRIBUTION

The *SP* is responsible for providing access to public keys in different stages of the protocol. There are two different approaches to generate the private-public key pair for *LA*s and for users (user/witness).

An *LA* needs to provide a human readable unique identity (location-ID) at the time of account creation. Once the account gets activated, the *SP* generates a private-public key- pair, which is identified by the location-ID. *LA*s need to collect the private key and store it on the local server. Upon receiving a request for the public key for a particular *LA* (location-ID), the *SP* sends the appropriate public key to the requestor.

Privacy is crucial for users (user/witness) to ensure non- traceable provenance against an attacker. In WORAL, we use a cryptographic identity (Crypto-ID) for users. The Crypto- ID hides the actual identity of user/witness within the location provenance records. A user can create multiple Crypto-IDs for WORAL and the user can choose a different one at different times on the mobile device while requesting the location proof. Hence, an external attacker cannot track the location of user/witness from a list of location provenance records. Users (user/witness) can generate a Crypto-ID on the mobile device and a private-public key pair will be created and saved for the

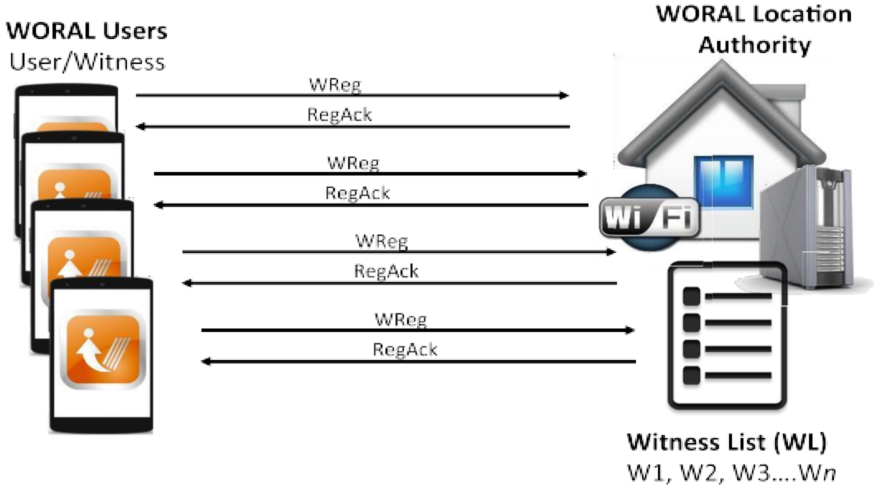
B. LOCATION AUTHORITY DISCOVERY

The user and witness need the IP address of the *LA* to establish TCP connection with the *LA*. They also require the unique location-ID to access public key of the *LA*. The IP and identifier is made available to the user and witnessthrough the *LA* discovery protocol using broadcast messages.

When a user or witness needs the *LA*'s information, it broadcasts a UDP packet to a specific port requesting the information of *LA*. The *LA* always listens for new UDP broadcast packets. If the packet matches with some certain criteria (in our case, request for *LA*'s information), the *LA* sends a UDP packet as a response that contains its location ID. After receiving the response sent by the *LA*, the user/witness can extract the identity and IP address of the *LA* from the received UDP packet.

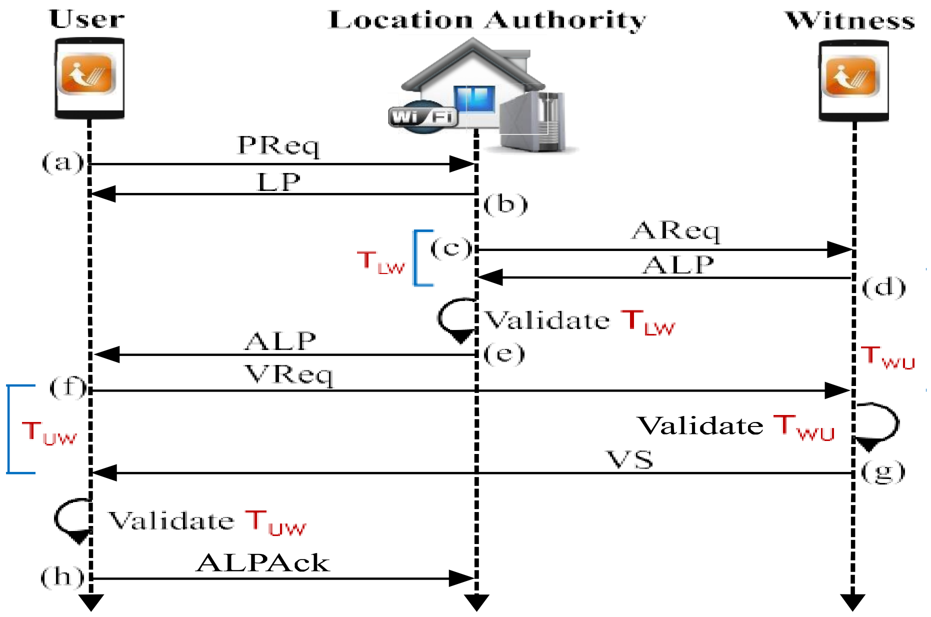
C. WITNESS REGISTRATION

The *LA* needs to maintain a list of available co-located WORAL mobile users who are interested to serve as witnesses. The registration process is shown in Figure. A WORAL mobile user expresses his willingness to serve asa witness by sending a witness registration message *WReg* to the *LA* and is defined as:



A. SECURE LOCATION PROVENANCE PROTOCOL

The sequence of interaction among the entities for creating an asserted location proof with provenance preservation is illustrated in Figure and described as follows:



III. ANALYSIS

The protocol design and performance evaluation was per- formed and presented in details in the Asserted Location Proof paper. The performance evaluation and comparison for the different provenance models were presented in OTIT. This section presents a discussion on the proposed protocol including a comparison to other similar technologies.

A. COLLUSION ATTACKS

We define the following symbols: honest and malicious users U *and* $\bar{U}$; honest and malicious location authorities L and $\bar{L}$; honest and malicious witnesses W and $\bar{W}$. The eight different combinations and corresponding possible collusion attacks are presented in Table. WORAL enforces mutual communication and detection of any colluded fake proof generation. A security analysis of WORAL for each collusion model is presented as follows:

TABLE 1. Collusion models and corresponding threats.

Notation	Attack(s)
U L W	No collusion
U L W	False proof, reordering, DoS, proof switch, relay attack
U L W	DoS, implication
U L W	False endorsement, privacy
U $\bar{L}\bar{W}$	Implication, relay attack, replay attack
U L W	False endorsement, relay attack, Sybil attack [52]
$\bar{U}\bar{L}$ W	False location proofs, relay attack, replay attack
$\bar{U}\bar{L}\bar{W}$	False proofs.

B. *SYSTEM* VULNERABILITY *ANALYSIS*

Someone willing to share the private keys in public-key cryptography, or a general internet user willing to publicly share the secret password, does not allow any system to be secure. As a result, it is not very useful to discuss any situation where all the given entities are malicious. Increasing the number of entities in a system also increases the number of attack surfaces. Any two-entity based location proof protocol has four different collusion combinations. A two-party protocol will have at least one combination which the system will be vulnerable to, where both the parties are malicious. As shown in Table 2, the combination of a malicious location authority $\bar{L}$ and a malicious user $\bar{U}$ will make the protocol invalid. Therefore, any such a protocol is 25% vulnerable in the best-case.

C. SECURE PROVENANCE GENERATION

Next, we present the security lemmas and propositions for secure location provenance schemes.
Lemma 1: A location proof is a securely generated data item for user U, which validly verifies the presence of user U at location L_i, where i {1, 2, . . . , n}.
Lemma 2: A location provenance chain C is a record of location proofs for locations L_i, where i {1, 2, . . . , n }, and presence at each location L is verified using a location proof Proof(L) for that location.

TABLE 3. Comparison of location proof provenance approaches:hash chains (HC), block-hash chains (BC), bloom filter (BF), shadow hash chain (SH), multi-link hashing (MH), and RSA chaining (RC) [2].

Properties	HC	BC	BF	SH	MH	RC
P1	✓	✓	✓	✓	✓	✓
P2	✓	✓	✓	✓	✓	✓
P3	✓	✓	✓	✓	✓	✓
P4	✓	✓	✓	✓	✓	✓

P5				✓		✓
P6			✓			
P7						✓
P8		✓	✓		✓	

D. EVALUATION OF PROTOCOL CHARACTERISTICS

Different models have tried to solve the location proof problem from different perspectives. A comparison of these characteristics for different location proof models is presented in Table 4. The comparison is based on the most important characteristics for location provenance schemes and is summarized as follows:

TABLE 4. Comparative evaluation of protocol characteristics: *proactive location proof* (PLP) [14], *APPLAUS* [45], *STAMP* [46],and the proposed *WORAL* protocol.

Features	PLP	APPLAUS	STAMP	WORAL
Time to generate proof (sec)	$\leq$ 0.5 (10-20m)	$\leq$ 10 (10m)	3 (10-20m)	$\leq$ 1 (10-20m)
Max. distance tested (m)	N/A	10	20	40
Proof size (bits)	$\approx$ 1000	N/A	$\approx$ 1300	$\approx$ 2000
Number of entities involved	2	Multiple	Multiple	3
Malicious LA	No	Partial	Partial	Yes
Vulnerability (%)	75	$\geq$ 75	$\geq$ 75	12.5
Collusion detection rate (%)	N/A	90	90 ($\bar{U}-\bar{W}$), 100 ($\bar{U}-\bar{U}$)	100

1) TIME TO GENERATE PROOF

Time to complete the whole location proof generation process is a very crucial factor in terms of usability and feasibility. The user might stay at some point for a very short period of time. Moreover, the users, and especially the witnesses might lose interest in using any such system if it takes a longer time for completion. Since the time increases with the distance among users and witnesses, we have provided the distance information along with the time to generate the proof.

2) MAXIMUM DISTANCE TESTED

Based on the underlying technology being used in the proto- col, the maximum distance supported by the system may vary. For example, the maximum possible distance covered by APPLAUS [45] is only 10 meters, since it uses Bluetooth technology. For other protocols, we have provided the maximum distance for which the system has been simulated for testing.

3) PROOF SIZE

Since the location proofs are being generated by mobile devices, the reasonable size of the proof is important for ensuring efficient computation and storage operations.

4) NUMBER OF ENTITIES INVOLVED

Increased number of entities increases the validity of the proof. But it comes with several trade-offs. Models involving more entities normally require more time. Moreover, it also increases the dimension of threats.

5) MALICIOUS LA

This is a crucial consideration in terms of secure design. Most models inherently assume that the LA can never be malicious. Though location authorities are a bit more reliable than the volatile nature of the user and witness, it is still a very strong assumption, and is not considered in our design.

6) VULNERABILITY

We have tried to generate a vulnerability matrix for all given models. For any given model, the vulnerability percentage implies the number of scenarios where generation of invalid proofs is possible. For example, in case of the 2-entity proactive location proof protocol (PLP) [14], there are 4 possible scenarios (UW, $U\bar{W}$, $\bar{U}W$, $\bar{U}\bar{W}$). This protocol guarantees the creation of valid proofs only when both U and W are trusted (UW), and thus having 75% of vulnerability. Since STAMP [46] and APPLAUS [45] can have any number of entities, the exact number of possible scenarios is not fixed and the percentage of vulnerability will vary based on the number of entities involved. If we consider 2 entities, the percentage of vulnerability will be 75% (works for 1 out of 4 possible scenarios); considering 3 entities, it will be 87.5% (works for 1 out of 8 possible scenarios), and so on.

7) COLLUSION DETECTION RATE

Theoretical proof or simulation results are used to illustrate the detection rate in case of different types of collusions, given that an attack has already been executed. In general, a higher detection rate implies a better security model. In summary, vulnerability implies the possibility of attack on a given scenario, while the collusion detection rate signifies the chances of successful detection of the given attack.

8) SYSTEM *OVERHEAD FOR LOCATION AUTHORITY*

We evaluated the system overhead while running the WORAL LA server. The LA server was deployed on a dual- core Intel Q9550 2.83GHz desktop PC with 4GB RAM and Ubuntu operating system. We performed the system performance evaluation using Sysbench[1] version 0.4.10, a cross-platform and multi-threaded benchmark tool for evaluating CPU performance.

For calculating the relative performance overhead, we first measured the CPU performance without the LA server running. Subsequently, we measured the CPU performance with the LA server running, and varying the number of consecutive proof requests made to the LA. The relative ratio for the different conditions for the approximate measurements (95 percentile) is shown in Figure 4. The average overhead ratio for all the conditions was at **0.045**, and the maximum value is seen to beat **0.075**. As it can be seen, the *LA* server accounts for a nominal overhead ratio and does not have many changes with the increase of the number of concurrent requests. The results imply that the LA is not a major resource-consuming process and can be handled in regular desktop machines. We posit that the LA can therefore be easily deployed by small businesses and shops, most of whom already own their local computer to run the surveillance system, billing system, etc.

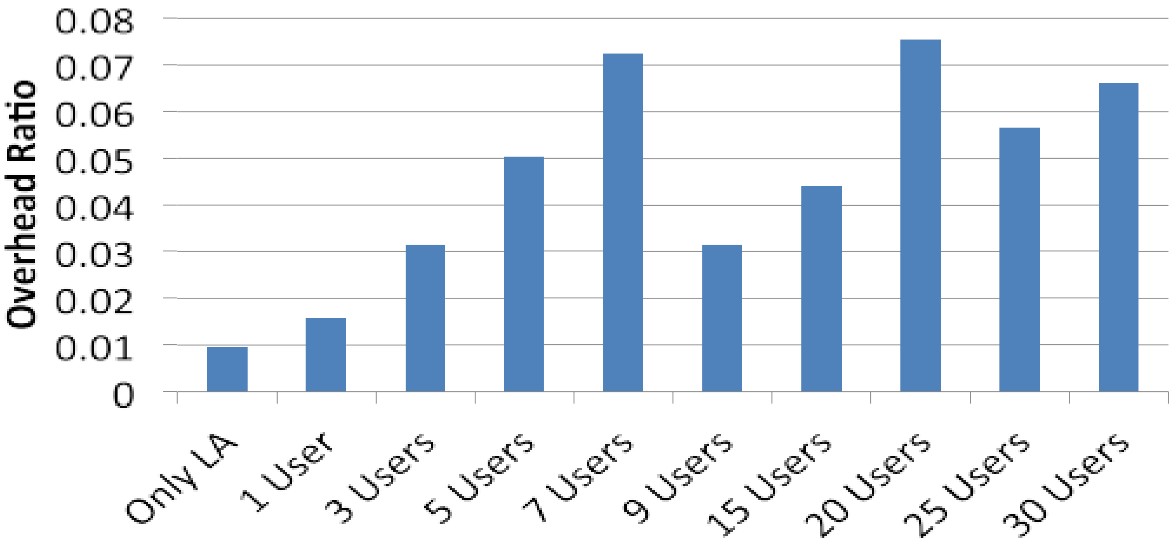


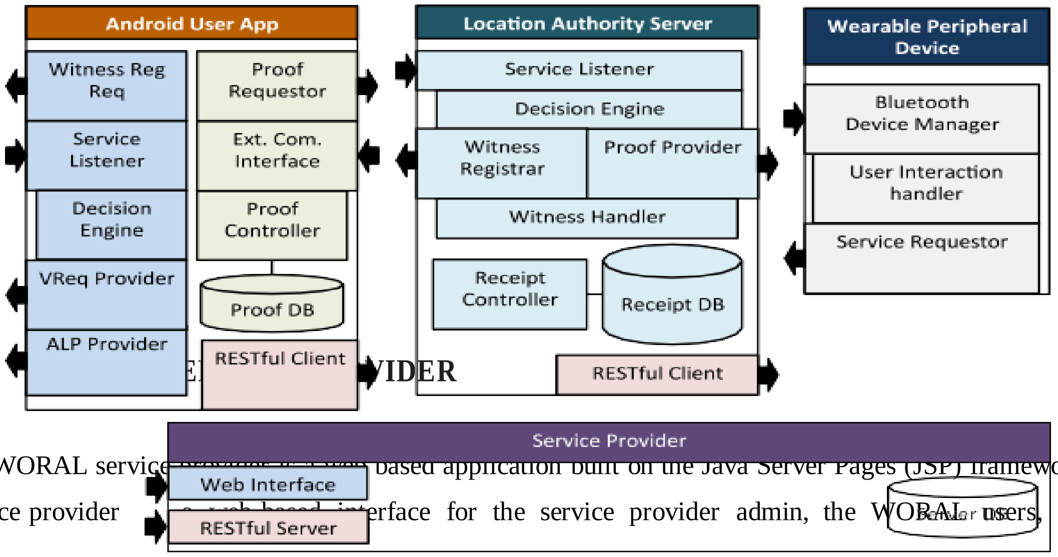
FIGURE 4. **Approximate (95 percentile) system overhead ratio.**

IV. IMPLEMENTATION

In this section, we present the implementation for a *ready-to-deploy* WORAL framework based on the proposed schematic description for the secure location provenance protocol.

A. COMPONENT *ARCHITECTURE*

The component architecture of the WORAL framework is shown in Figure. The inward and outward arrows show the components which are in listening mode for accepting messages or are responsible for sending a message. We used the RSA (2048 bit) for generating signatures and for allencryption and decryption of the packets. Additionally, we used the SHA-2 hash function with digest sizes 256 and 512 for generating the hash messages in the protocol and for storing private information on the databases (e.g. passwords, PIN) respectively.



B. SERVICE PROVIDER

The WORAL service provider is a web based application built on the Java Server Pages (JSP) framework. The Service provider has a web-based interface for the service provider admin, the WORAL users, Location Authorities and auditors.

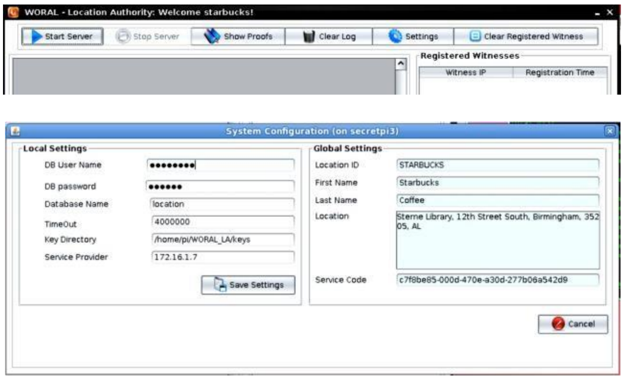
TABLE 5. WORAL service provider web UI services.

Entities	Services
Admin	No registration required (activated via configuration script of web application), Dashboard, View used/unused service codes, Generate new service codes, View registered users/location authorities/auditors, View active inactive location authorities/auditors
User	Registration, Dashboard, View profile settings, View available crypto-IDs, Enable/Disable witness feature, Change password, Update/Save profile, Auto-sync with mobile app

Location Authority	Registration, Dashboard, Profile activation, View profile settings, Profile Activation, Private-key generated during activation, Download private-key, Change password
Auditor	Registration, Dashboard, Profile activation, View profile settings, Profile Activation, Change password

TABLE 6. WORAL service provider RESTful services.

URL *https://ip:8443/woral*	**Parameters**
/Authenticate	*username, password*
Desc: User mobile app, location authority, and auditor uses to login. **Response:** Success or failure (with reason).	
/UserProfile	*username, password*
Desc: User invokes to load profile from server. **Response:** Current user profile in XML.	
/UserProfileUpdate	*username, password, isWitness, provenanceScheme*
Desc: User invokes to sync profile with server after updating on mobile device. **Response:** Success or failure (with reason).	
/LAProfile	*username, password*
Desc: LA invokes to load profile from server. **Response:** Current LA profile in XML.	
/CryptoIDList	*username, password*
Desc: User mobile app uses to download generated crypto-IDs. **Response:** Username and list of crypto-IDs in XML	
/PublicKey	*crypto-ID or location-ID*
Desc: User app, location authority, and auditor uses to collect public keys of users or location authorities. **Response:** Username, modulus, and exponent in XML.	
/PublicKeyUpload	*username, password, crypto-ID, key modulus, key exponent*
Desc: Users generate crypto-ID on the mobile app and uploads the public key. **Response:** Success or failure (with reason).	



DB User Name ●●●●●●●●●

DB password ●●●●●●

Database Name location

TimeOut 4000000

Key Directory /home/pi/WORAL_LA/keys

Service Provider 172.16.1.7

Location ID STARBUCKS

First Name Starbucks

Last Name Coffee

Location Sterne Library, 12th Street South, Birmingham, 35205, AL

Service Code c7f8be85-000d-470e-a30d-277b06a542d9

FIGURE 6. Location authority application panels. (a) Top controlbar. (b) Settings tab.

C. WORAL LOCATION AUTHORITY

The LA server is a Java-based application communicating with the service provider and the user app. logs in and displays the service window. The control tabs on the top of the window is illustratedin Figure 6a. The operator can use the buttons to start and stop the server, and view the current list oflocation proof receipts. The ongoing messages for the protocol are displayed on the logging window. The LA can also use the setting tab to update the local settings, illustrated in Figure 6b. The global settings are downloaded from the SP and are not modifiable once a LA is verified and activated. The local settings are set and saved on the local machine running the LA service. Additionally, we have created a *plug-n-play* LA using Model-B Raspberry P is with 512 MB RAM, along with a customized Raspian image. The simulation test-bed for WORAL using five *plug-n- play* Raspberry Pi LAs is shown in Figure 7.

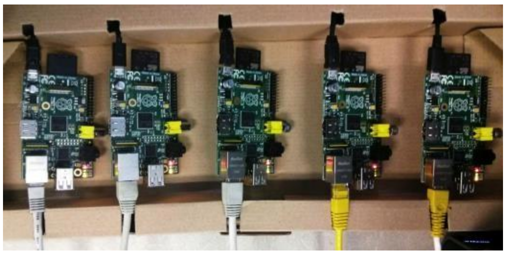
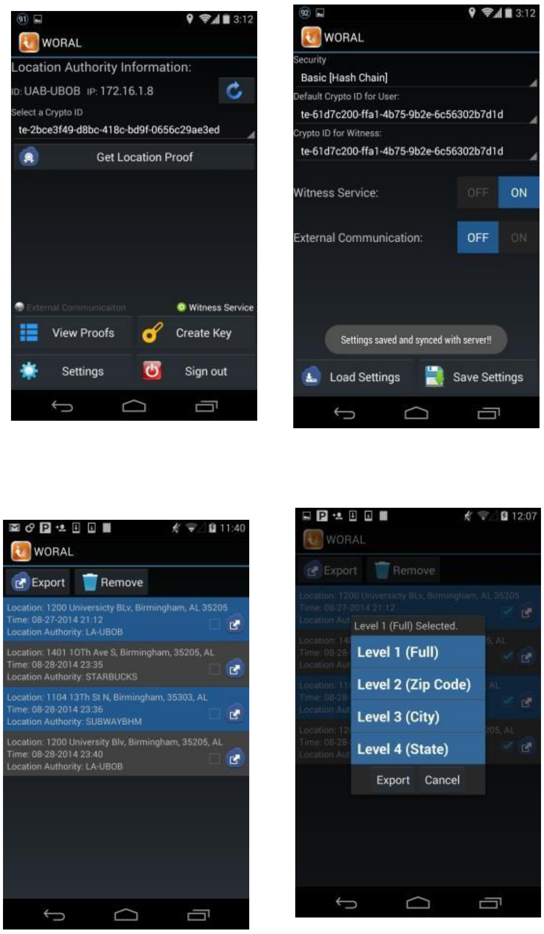


FIGURE 7. *Plug-n-Play* location authorities using raspberry Pi-s.

A. WORAL USERS

The WORAL Android user application is used for both requesting location proofs as well as for asserting other users' location proofs as a witness. The home screen after the user logs in is illustrated in Figure 8a. The home screen allows the user to select a crypto-ID for the current location proof request or generate new crypto-ID keys, and update/modify the settings. The settings screen for the user app is shown in Figure 8b. In the settings mode allows the user to select the

Background witness service features, as well as the external communication feature for wearable peripheral devices. The settings are automatically synced with the service provider. The list of currently collected proofs canbe viewed as shown in Figure 8c. Additionally, the user can selectively or collectively export or delete the proofs. The exported proofs have the desired level of granularity of information as selected by the users and is shown in Figure 8d. The exported proofs are saved as a text file on the mobile device, which can then be sent personally to the auditor by the user (e.g. email, file trans- fer). We have tested our application on LG Nexus 4, Samsung Galaxy Nexus, Samsung Galaxy S4, Motorola XT875, HTC 1X, HTC Evo 4G, and Motorola Moto G phones with Android version 2.3 and higher.



WORAL

Location Authority Information:

ID: UAB-UBOB IP: 172.16.1.8

Select a Crypto ID

te-2bce3f49-d8bc-418c-bd9f-0656c29ae3ed

○ External Communicaiton ● Witness Service

WORAL

Security

Basic [Hash Chain]

Default Crypto ID for User:

te-61d7c200-ffa1-4b75-9b2e-6c56302b7d1d

Crypto ID for Witness:

te-61d7c200-ffa1-4b75-9b2e-6c56302b7d1d

Witness Service: OFF [✓ ON]

External Communication: [✓ OFF] ON

Settings saved and synced with server!!

WORAL

Location: 1200 Universicty BLv, Birmingham, AL 35205
Time: 08-27-2014 21:12
Location Authority: LA-UBOB

Location: 1401 1OTh Ave S, Birmingham, 35205, AL
Time: 08-28-2014 23:35
Location Authority: STARBUCKS

Location: 1104 13Th St N, Birmingham, 35303, AL
Time: 08-28-2014 23:36
Location Authority: SUBWAYBHM

Location: 1200 University Blv, Birmingham, 35205, AL
Time: 08-28-2014 23:40
Location Authority: LA-UBOB

WORAL

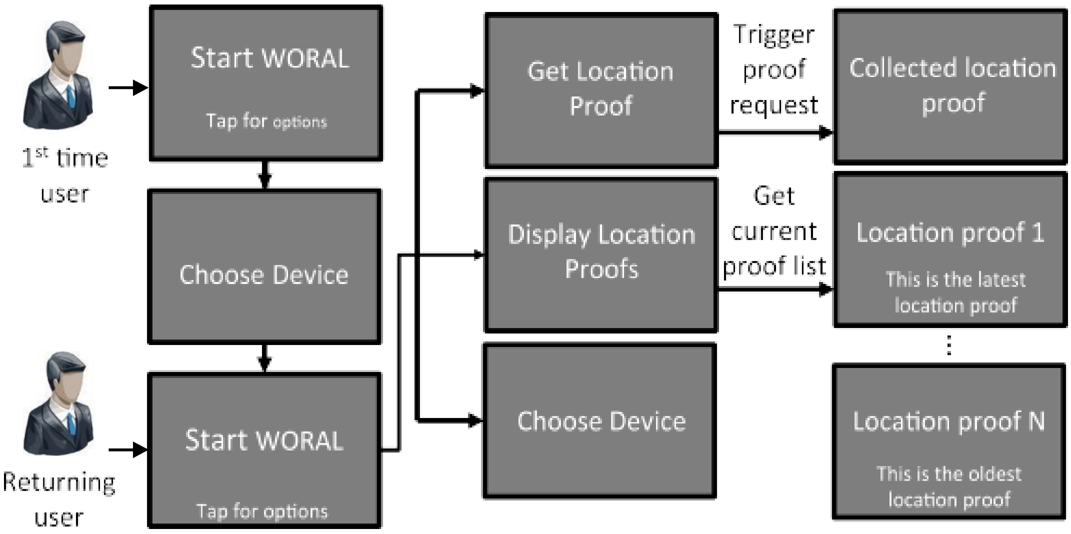
Level 1 (Full) Selected.

Level 1 (Full)
Level 2 (Zip Code)
Level 3 (City)
Level 4 (State)

FIGURE 8. **Android user application. (a) Home screen. (b) Settings. (c) Proof list. (d) Export proofs.**

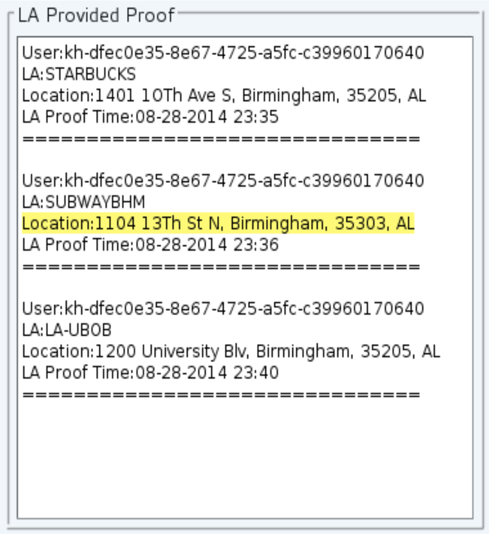
A. WORAL WEARABLE DEVICE EXTENSION

Wearable peripheral devices, such as the Google Glass, are ubiquitous devices with networking capability. Such devices allow seamless interaction and privacy of display for the users. We extended our WORAL framework by implementing a Google Glass based interface for the WORAL Android user app. The wearable device extension greatly enhances the usability of the system by allowing a user to non-intrusively interact with the WORAL framework without any physical operation on the mobile device. The glassware communicates with the WORAL app running on the paired Android phone over Bluetooth. The user can switch on the *external communication* feature on the mobile app to be able to use the WORAL Google Glass extension. The UI flow for the Google Glass is illustrated in Figure 9. Current implementation allows a user wearing the Google Glass to request for location proofs and display the list of currently available location proofs from the mobile device.



A. WORAL AUDITOR

The WORAL auditor is a standalone Java desktop application communicating with the service provider. The user presentsan exported proof (or list of proofs) and the auditor imports the file to verify the location proof(s) and their provenance. Two of the panels from the auditor window, for the *LA* provided information and for the witness assertion, is shownin Figure 10a and Figure 10b respectively. Any mismatchedinformation is marked on the corresponding panels, as seen from Figures 10a and 10b. It therefore depends on the auditorto either accept or reject the location provenance claim by theuser.

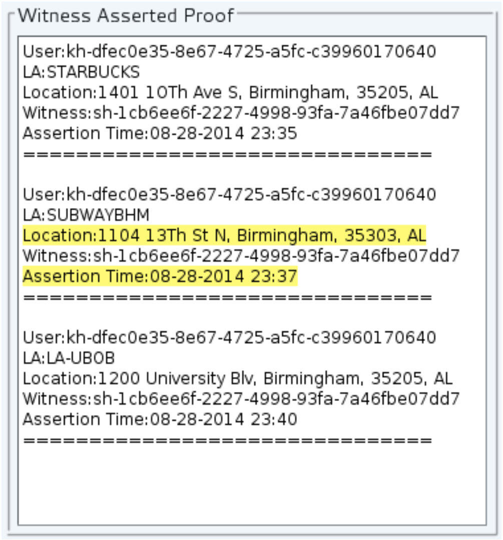


LA Provided Proof

```
User:kh-dfec0e35-8e67-4725-a5fc-c39960170640
LA:STARBUCKS
Location:1401 10Th Ave S, Birmingham, 35205, AL
LA Proof Time:08-28-2014 23:35
================================

User:kh-dfec0e35-8e67-4725-a5fc-c39960170640
LA:SUBWAYBHM
Location:1104 13Th St N, Birmingham, 35303, AL
LA Proof Time:08-28-2014 23:36
================================

User:kh-dfec0e35-8e67-4725-a5fc-c39960170640
LA:LA-UBOB
Location:1200 University Blv, Birmingham, 35205, AL
LA Proof Time:08-28-2014 23:40
================================
```



Witness Asserted Proof

```
User:kh-dfec0e35-8e67-4725-a5fc-c39960170640
LA:STARBUCKS
Location:1401 10Th Ave S, Birmingham, 35205, AL
Witness:sh-1cb6ee6f-2227-4998-93fa-7a46fbe07dd7
Assertion Time:08-28-2014 23:35
================================

User:kh-dfec0e35-8e67-4725-a5fc-c39960170640
LA:SUBWAYBHM
Location:1104 13Th St N, Birmingham, 35303, AL
Witness:sh-1cb6ee6f-2227-4998-93fa-7a46fbe07dd7
Assertion Time:08-28-2014 23:37
================================

User:kh-dfec0e35-8e67-4725-a5fc-c39960170640
LA:LA-UBOB
Location:1200 University Blv, Birmingham, 35205, AL
Witness:sh-1cb6ee6f-2227-4998-93fa-7a46fbe07dd7
Assertion Time:08-28-2014 23:40
================================
```

CONCLUSION

Evolving location-based services have created a need for secure and trustworthy location provenance mechanisms. Collection and verification of location proofs and the preservation of the chronological order has significant real life applications. In this project, we introduce WORAL, a ready- to-deploy framework for secure, witness-oriented, and provenance preserving location proofs. WORAL allows generating secure and tamper-evident location provenance items from a given location authority, which have been assertedby a spatio-temporally co-located witness. WORAL is based on the Asserted Location Proof protocol and is enhanced with provenance preservation based on the OTIT model. The WORAL framework features a web-based service provider, desktop-based location authority server, an Android-based user application including a Google Glass client for the mobile app, and an auditor application for location provenance validation.

REFERENCES

[1] R. Khan, S. Zawoad, M. M. Haque, and R. Hasan, '''Who, when, and where?' Location proof assertion for mobile devices,'' in *Proc. 28th Annu. IFIP DBSec*, Jul. 2014, pp. 146–162.

[2] R. Khan, S. Zawoad, M. M. Haque, and R. Hasan, ''OTIT: Towards secure provenance modeling for location proofs,'' in *Proc. ASIACCS*, 2014,pp. 87–98.

[3] S. Saroiu and A. Wolman, ''Enabling new mobile applications with loca- tion proofs,'' in *Proc. HotMobile*, 2009, pp. 1–6.

[4] J. VanGrove. (Apr. 2010). *Foursquare Cracks Down on Cheaters*. [Online]. Available: http://mashable.com/2010/04/07/foursquare-cheaters/

[5] I. Maduako. (Jul. 2012). *Wanna Hack a Drone? Possible With Geo-Location Spoofing!* [Online]. Available: http://geoawesomeness. com/?p=893

[6] N. O. Tippenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, ''iPhone and iPod location spoofing: Attacks on public WLAN-based positioning systems,'' System Security Group, ETH Zürich Univ., Zürich, Switzerland, Tech. Rep. 599, Apr. 2008.

[7] A. J. Blumberg and P. Eckersley. (Aug. 2009). *On Locational Privacy, and How to Avoid Losing it Forever*. [Online]. Available: https://www.eff.org/wp/locational-privacy

[8] J. McDermott. (Jul. 2013). *Foursquare Selling Its Location Data Through Ad Targeting Firm Turn*. [Online]. Available: http://adage.com/article/ digital/foursquare-selling-data-ad-targeting-firm-turn/243398/

[9] Y. L. Simmhan, B. Plale, and D. Gannon, ''A survey of data provenance in e-science,'' *ACM SIGMOD Rec.*, vol. 34, no. 3, pp. 31–36, Sep. 2005.

[10] R. Hasan, R. Sion, and M. Winslett, ''The case of the fake Picasso: Preventing history forgery with secure provenance,'' in *Proc. 7th Conf. FAST*, 2009, pp. 1–12.

[11] R. Khan, M. Haque, and R. Hasan, ''A secure location proof generation scheme for supply chain integrity preservation,'' in *Proc. HST*, 2013,pp. 446–450.