AFRL-RI-RS-TR-2015-183

SECURE LOCATION PROVENANCE FOR MOBILE DEVICES

UNIVERSITY OF ALABAMA AT BIRMINGHAM

JULY 2015

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2015-183 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /
DAVID M. CLIMEK
Work Unit Manager

/ S /
WARREN H. DEBANY, JR.
Technical Advisor, Information
Exploitation and Operations Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
JULY 2015	FINAL TECHNICAL REPORT	AUG 2012 – FEB 2015

4. TITLE AND SUBTITLE

SECURE LOCATION PROVENANCE FOR MOBILE DEVICES

5a. CONTRACT NUMBER
FA8750-12-2-0254

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
69220K

6. AUTHOR(S)
Ragib Hasan
Rasib Khan
Shams Zawoad
Munirul Haque

5d. PROJECT NUMBER
DHS2

5e. TASK NUMBER
UA

5f. WORK UNIT NUMBER
LA

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
University of Alabama at Birmingham
701 S 20th St
Birmingham AL 35294-0001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory/RIGA
525 Brooks Road
Rome NY 13441-4505

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSOR/MONITOR'S REPORT NUMBER
AFRL-RI-RS-TR-2015-183

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. 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 travel in 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 project, we focused our research on secure location provenance techniques for mobile devices. We created WORAL, a complete ready-to-deploy framework for generating and validating witness oriented asserted location provenance records. The WORAL framework is based a secure asserted location proof protocol and location provenance preservation methods for generating secure location provenance chains on mobile devices. WORAL allows user-centric, collusion resistant, tamper-evident, privacy protected, verifiable, and provenance preserving location proofs for mobile devices. The report presents the schematic development, experiments and results, and implementation of WORAL for Android device users including a wearable device based client for enhanced usability.

15. SUBJECT TERMS
Location Assertion; Location Proof; Location Provenance; Location Security; Mobile Devices, Witness Endorsement; WORAL

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**DAVID M. CLIMEK**
U	U	U	UU	26	19b. TELEPHONE NUMBER (*Include area code*) **N/A**

TABLE OF CONTENTS

LIST OF FIGURES

SUMMARY

This document includes the final project report on “Secure Location Provenance for Mobile Devices” initiated in August 2012 for duration of two and half years. The research and development of the project was performed at the Secure and Trustworthy Computing Lab (SECRETLab) in the Department of Computer and Information Sciences at the University of Alabama at Birmingham. The final target of the project was to deliver a complete solution for secure, user-centric, verifiable, and tamper-evident location provenance for a distributed architecture based on mobile devices. This report presents the final and complete technical report on the methods and phases of research, experimental results and discussion, and the implementation details of a read-to-deploy product developed from the research outcomes.

1. INTRODUCTION

1.1 Motivation

Mobile devices have enhanced the use of location-based services (LBS) using the geographical locations of the devices [3]. 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 [4], to national security issues [5].

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 [6]. 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 [7]. The service providers may also sell the location data of their users taking advantage of the small-text in the service agreements [8]. 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 [9, 10]. 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 intermediate locations, which the product travels through [11]. 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 [2].

1.2 Background

There have been numerous proposals for allowing user initiated location proof generation [3, 12–15]. 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 [16–18]. 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 [3, 6, 7, 12–25].

1.3 Research Scope Definition

Based on our research, we present the **W**itness **OR**iented **A**sserted **L**ocation provenance (WORAL) framework to allow secure location provenance for mobile devices. The system is based on the Asserted Location Proof (ALP) protocol [1] and incorporates the OTIT model for secure location provenance [2]. 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, and a desktop-based auditor.

1.4 Applications of Research Outcome

Assertion oriented location provenance schemes can be effectively used in a variety of real-life scenarios. Our solution emphasizes the device's presence, and can be a highly applicable technology for equipment handling businesses. At present, most high-end devices come with networking features and

built-in memory. Hence, these expensive devices could easily be monitored for presence at their particular locations. The concept of location provenance and witnesses can also be applied to other domains, such as in preserving the integrity of supply chain information for different products and services [11]. An interesting application can be made at organizations that have traveling clientele or employees. Travelers can collect the asserted location provenance items on their mobile devices. Later, they can utilize the proofs to simplify subsequent processes, such as, travel expense claims and itinerary management, in a secure and reliable fashion.

The whole mechanism of asserted proofing could be utilized in a reversed witness oriented application. Instead of a user presenting the proofs as evidence of presence, witnesses can present notarized records as a proof of specific users visiting a certain location. Taking the example of insurance agents, construction site inspectors, and relief workers, the presence of these people are more concerned in their respective fields of action. Witnesses at the particular sites can provide their endorsements as proof of visit for the agents on the field.

Extending the concept of locations and asserted proof of presence, social networks and such community-oriented platforms have opportunities for implementing such schemes as well. A secure proof of presence with provenance preservation can be employed to form ad-hoc social networks and community networks. Therefore, a secure, automated, and non-intrusive location proof generation scheme fits perfectly as the underlying mechanism for all such LBS.

2. METHODS, ASSUMPTIONS, AND PROCEDURES

2.1 Terminologies

We have introduced certain terminologies in the description of our models and for designing the WORAL architecture. The Service Provider SP is the trusted entity providing the secure location provenance service to mobile users, based on decentralized and certified location authorities and verified auditors. A User U is an entity who visits a location and uses a mobile device to request and store location provenance records. A Site S is a physical region with a valid address within a finite area under the coverage of one location authority. A Location Authority LA is a stationary entity, certified by the SP, identified using a unique identifier, and is responsible for providing location provenance records for a particular site. A Witness W is a spacio-temporally co- located mobile user who has volunteered to assert a location provenance record for the presence of another mobile device user at the given location. A Witness List WL provides the listing of all registered witnesses under the coverage of the location authority at a given time. A Crypto-Id CID is a cryptographic identity for the user (who is also a witness), used in all phases of the protocol, ensuring privacy of the entities participating in the process. A Location Proof LP is a token of evidence received by a user when visiting a specific site, and an Asserted Proof AP is a location proof LP asserted by a valid witness using his Crypto-ID. Location Provenance is the guarantee of the chronological ordering of the asserted location proofs in a tamper-evident chain of records based on a particular Provenance Scheme PS. Finally, an Auditor is an SP verified authority who is presented with a chain of asserted location proofs and confirms the legitimacy of the user's claim of presence at the particular site and the order of visits.

2.2 Witnesses and Assertions

In real-life, two parties considering each other as untrustworthy necessitate the involvement of a witness. A witness provides a notarization of a statement between two parties. The endorsed statement implies a greater truth value of the content and is then redistributed among the two parties.

We utilize the same concept to create location proofs and have the proof asserted by a co-located witness. In this context, a witness is a spatiotemporally co-located entity with the user and the location authority. A witness will assert proofs only when willing to do so and can de-register as a witness at any time. In a commercially deployed scenario, the incentive of the witness can be based on awarded 'points' depending on valid assertions. The 'points' would add to the trust value of a witness and may be redeemed for membership benefits from the service provider. The assertions may also be used by the witness to prove co-location with the user.

2.3 Threat Model

The threat model for WORAL is based on the previously described entities and is described as follows:

- The location information within the asserted location proof corresponds to a particular identity of a user and an adversary should not be able to create a location proof for a location that the user has not visited.
- The time at which the particular user visited the given site and collected the asserted location proof should not be modifiable by an attacker to create a proof for a different (local) time than the actual time of visit.
- The identity and location privacy of users and witnesses are protected and an attacker may not create a dossier of users visiting a given location and learn the location history and identities of other users.
- The chronological ordering of the proofs should be preserved and an attacker should not be able to modify the order of proofs in the provenance records.
- The privacy of information within a proof is exposed according to the desire of the user and an attacker or auditor should not be able to view any private information not intended to be exposed by the user.
- A user intending to expose a subset of the location provenance records should not be revealing more than what is required for the desired segment of the chain.
- A malicious user should not be able to hide a temporary off-track movement from the claimed location provenance.
- A malicious user may want to overload the auditor with a high computational requirement for the secure location provenance verification process.

Next, we describe the attacker capabilities for our threat model based on the contexts, assumptions, functionality, and possible intents for each of the entities.

- Unlike previous works [3, 14, 15], we do not consider the location authorities as trustworthy. We assume that the location authorities as well as the requesting and witnessing user present at the site and participating in the proof generation protocol can all be malicious.
- Users, location authorities, and witnesses can collude with one another, driven by social, monetary, or any other form of illicit mutual benefits.
- After a proof is collected for a particular site, the user can delete or tamper with location proof and provenance records which are saved on the device.
- The location authority or the user can create a puppet witness to produce false asserted proofs or relay the assertion requests to a remote witness who is not co- located at the given site at the time of visit.
- Users, LA, and witnesses, each own a public/private key- pair, which has been signed by the SP at the time the entities register for the service, and no entity shares their private keys at any point.

- We assume that a three-way (all-party) collusion scenario does not exist as it is highly unlikely all three participants will be fraud at a given scenario.
- We expect that mobile devices are non-shareable private properties and the physical security of the phone depends on the user himself.
- Attacks such as MAC address fingerprinting are prevented via known techniques such as MAC address cloning [50].
- According to the description of the protocol, we assume the presence of at least one witness at the given site who is willing to provide an assertion.

2.4 System Model

We assume that mobile devices carried by users are capable of communicating with other devices and LAs over WiFi networks. The devices have local storage for storing the provenance items. The user has full access to the storage and computation of the device, can run an application on the device, and can delete, modify, or insert any content in the data stored on the device. The user, LA, and witness can access each others' public key from the SP.

The LA is a fixed server with higher computation and storage capability than a mobile device. A location runs a WiFi network, and the LA is directly connected to the network. Any user interested to receive an asserted location provenance record obtains the address of the LA from the site via network broadcasts. Similarly, a user can obtain the address of the location authority, and register as an interested witness. The location authority periodically updates the available witness list. When required, the location authority chooses a witness from the list at random and sends a request to the selected witness to assert a location proof.

Upon completion of a schematic communication between the entities, the user obtains a provenance preserving location proof from the LA, which has been asserted by a witness, and is stored on the user's device. At a later time, the user presents location proofs as a claim of presence for certain locations and the path of travel. The auditor uses the location-ID and the yielded assertion to validate the claim of presence and the chronological order of the proofs.

2.5 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. Communications between LA and mobile users are done over TCP. All messages are signed using the private key of respective entities and verified using the public key. Signature of an entity E for a message M is refereed as SE (M). An entity can receive the public key of another entity from the SP. All communications with the SP occur through the public network using REST [51] and HTTPS.

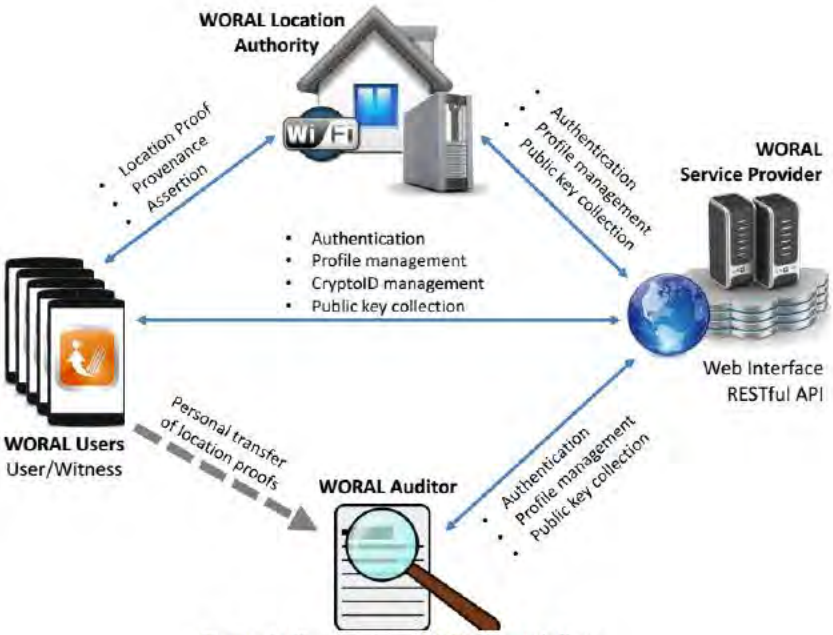


Figure 1: Overview of WORAL work flow

The different steps and phases of the protocol have been designed, such that, to ensure the location proof is resistant to collusion attacks and the provenance of the location proofs is preserved. Hence, we designed WORAL based on the secure location proof collection scheme presented in [1] and is enhanced using secure location provenance schemes presented in [2]. In the following subsections, we present the different components and work flows of the framework.

2.6 Secure Location Provenance Protocol

The sequence of interaction among the entities for creating an asserted location proof with provenance

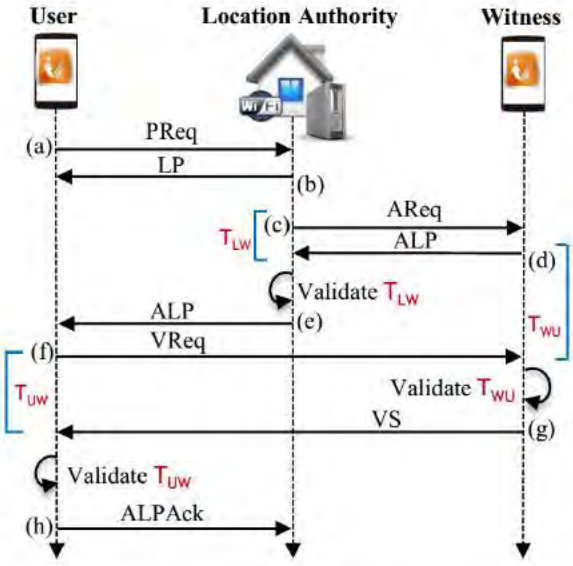


Figure 2: Sequence diagram for WORAL protocol

preservation is illustrated in Figure 2 and described as follows:

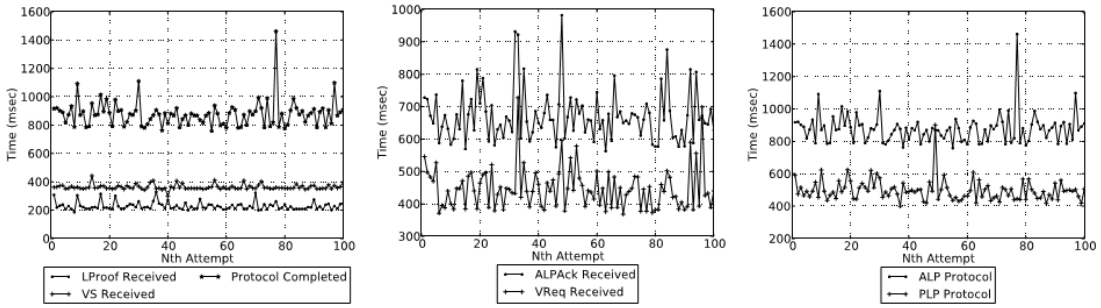
a) **Location proof request:** The user obtains the identity of the LA and sends a location proof request PReq to the LA.
b) **Location proof generation:** The LA generates the location proof LP as shown in Expression 4 and sends the LP to the user.
c) **Proof assertion request:** The LA randomly selects a witness W from the WL and then sends an assertion request AReq to the selected W, where AReq = LP.
d) **Asserted message creation:** The witness W verifies the information in the AReq message. Upon successful verification of all the information, the asserted location proof ALP.
e) **Assertion verification and relay:** The LA receives and verifies the ALP for the assertion provided by the W. The LA also verifies the time lapse between sending an assertion request AReq and receiving the asserted location proof ALP. This time difference is referred as T_{LW} in Figure 2. The LA enforces a maximum threshold for the T_{LW} to detect any proxy forwarding delay by the witness. The process of identifying the appropriate value for the T_{LW} is presented in [1]. Upon successful verification, the LA relays the ALP to the user U.
f) **Verification request:** Once U has received both the LP and the ALP, he directly communicates with W, and sends a verification request VReq.
g) **Verification response:** W receives the VReq from U and checks to see if the assertion has been tampered or not. W calculates the difference between the time available in the ALP, with the current time on the witness' device.
h) **Location proof receipt:** After receiving the VS from W, the user verifies the time difference between the time in the VReq and the current time on the user's device when it receives VS. In Figure 2, this time difference is referred as T_{UW} . A maximum threshold for the T_{UW} ensures that W is not proxying the assertion and the verification requests. U then creates an acknowledgement ALPAck.

The user then stores the proof information on his device for the specific site S and hence, completes the secure location provenance protocol. Subsequently, the LA stores the receipts for the location proofs sent from the users. The LA maintains a publicly visible list of these tickets. At every epoch, it publishes the current state of this list along with a signature. The purpose of this publicly available list is to prevent back-dating and future-dating attacks.

2.7 Proof and Provenance Verification

When the location of U at a certain time is in question, U needs to send the location proofs stored in her device to an SP verified auditor. An exported proof by U from the mobile device contains the following items: plain text proof, LA-signed proof, and witness-signed proof.

Granularity of the location that appears in the exported proof is based on U's selection. As U has control over the stored information, a malicious user can try to tamper with the plain-text information. However, even when the user has colluded with the LA or the witness, the user cannot the change both the signatures. While verifying the location proofs provided by the user, the auditor compares the plain-text information with the information that is signed by the LA and the W. Any discrepancies, with the signed information can be easily detected by an auditor.



(a) User Application (b) Witness & Location Authority (c) Comparison between ALP & PLP

Figure 3: Protocol performance evaluation

An auditor also checks the provenance and chronological order when multiple location proofs have been presented. First, the $LProv_{new}$ is extracted from each proof. Next, depending on the selected provenance scheme P S, the auditor will run the appropriate provenance verification algorithm, which are presented in [2], and verify the location provenance claimed by the user U.

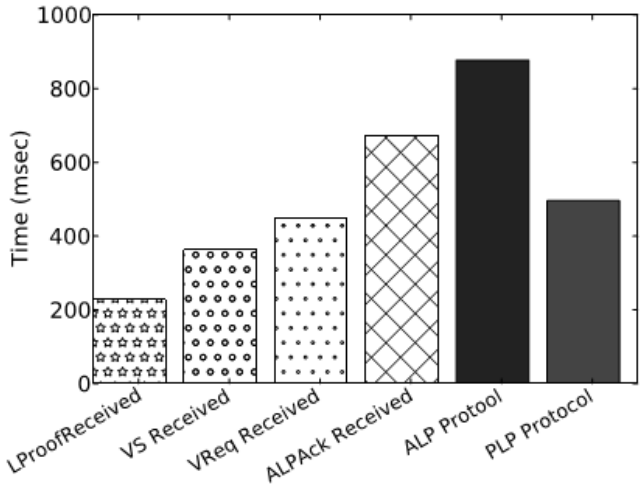


Figure 4: Average times required for different phases of the protocol

3. RESULTS, ANALYSIS, AND DISCUSSION

3.1 Performance Analysis

We evaluated the performance of three important steps of the protocol from the user application. We recorded the timestamps at different phases of the protocol for 100 complete execution cycles. Initially, we recorded the time lapsed after sending a proof request PReq to the location authority L, and eventually receiving a location proof LP. We denote this as LProof Received time. Subsequently, we recorded the time elapsed between sending the verification request VReq and receiving the verification statement VS from the witness W, which is denoted here as VS Received time. Finally, we measured the time required to complete the whole protocol. Figure 3a represents the time required for each step and figure 4 illustrates the average time required for the individual steps.

In our proposed scheme, the mean time for LProof Received and VS Received were 228 milliseconds and 362 milliseconds respectively. Although the computation needed for generating the location proof LP and the verification statement VS is similar (generating the packet then signing it), the VS Received time is higher than the LProof Received time. This behavior is natural, as the witness's device has less computation power than the location authority's device. In the protocol, the location authority L forwards the asserted location proof ALP to the user U. In the end, the location authority L receives the acknowledgement ALPAck receipt from the user U. We measured the time required between these two steps. The time measurement is noted as ALPAck Received on figure 3b, which depicts this processing delay for all iterations. Additionally, the average time required for ALPAck Received is shown in figure 4.

To perform a comparative analysis of our proposed protocol (Asserted Location Proof or ALP protocol), we selected another secure location proof protocol, namely 'Proactive Location Proof' or PLP protocol, proposed by Luo et al. in [14]. Both the protocols were compared based on their time of completion for receiving the location proof. Figure 3c illustrates the time required to complete each protocol. The average processing time for the ALP protocol is 877 milliseconds, whereas that of the PLP protocol is 496 milliseconds. Given the fact that we have more phases in our protocol including numerous encryption and decryption operations, the ALP should be taking a longer processing time. However, the comparison demonstrates that the processing time for ALP is still comparable to rather simplistic models like PLP. Additionally, the other protocols so far have neither considered collusion attacks nor the presence of malicious location authorities.

The results above show some overhead processing in our proposed protocol. However, it provides an extra level of security by getting the assertion from the witness, hence adding to the trust value of such location proofs. The completion time for the protocol is still less than 1 second, which is a reasonable latency for practical usage. Addition of the witness increases the attack surface for the protocol. Nonetheless, we have also proved that our proposed protocol is resilient to all combinations of collusion attacks.

3.2 Threshold Adjustment for Attack Identification

The next phase of the work included a variable-distance setup for the protocol. The recorded times were used to justify the values for T_{LW}, T_{UW}, and T_{WU}. We placed the user U, witness W, and the location authority LA at varying distances and recorded the time measurements for each of the times.

The recorded times show that the time intervals tend to increase as the distance between the entities is increased. Additionally, we observed that the previously set values for the thresholds do not suffice the purpose of determining the proxy attacks in each of the cases. Therefore, the next phase for adjusting the threshold included performing a relay attack using a proxy witness and user. Subsequently, we utilized the measurements from the relay attack to adjust our threshold values using a sliding threshold model.

The values of the thresholds have been determined using relay attacks. We executed a relay attack using a proxy to forward messages between two networks. In the first case, we utilized a proxy to relay packets to a remote network to a witness which is not spatially co-located with user and location authority. We calculated the time lapse between sending VReq and receiving VS for this attack scenario. The recorded T_{LW}'s and T_{UW}'s for both trusted and proxy witnesses are shown in figure 5a and figure 5b respectively. Next, we performed a similar experiment using a user proxy. The proxy was present to relay the packets to the user on the remote network. The recorded T_{WU}'s for both the trusted and proxy users are shown in figure 5c.

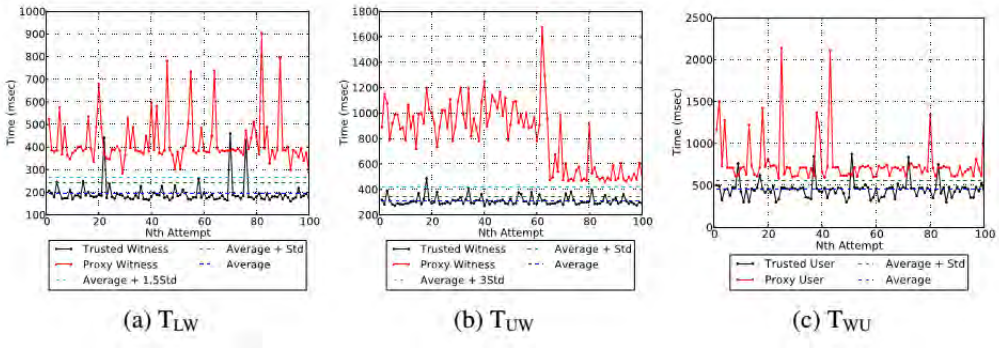


Figure 5: Attack identification using time thresholds

We utilized a sliding threshold model to determine optimal values for T_{LW}, T_{UW}, and T_{WU}. Initially, we started with a minimum value to specify the optimal threshold, and observed the percentage of attacks successfully identified. Additionally, we also calculated the percentage of false alarms when the threshold is set at the given value. For determining an optimal T_{UW}, we set the initial threshold at [Mean (μ) + Standard Deviation (τ)]. The threshold for T_{UW} was thus at 552.46 milliseconds, and the corresponding attack identification and false alarm was found to be at 100% and 6% respectively.

The threshold was set at different incremental values to reduce the false alarm rate in the protocol. The next experimental threshold was set at [μ + 1:3τ], where the attack identification was still at 100%, while the false alarm had dropped to 14%. With a gradual increase of the threshold, we saw no decrease in the percentage of attacks identified, but the false alarm rate reduced to 5% by the time we reached [μ + 2τ]. With T UW set at [μ + 3τ], the attack identification was still 100% but the false alarms has reduced to only 1%. As we increased the threshold beyond [μ + 3τ], we observed the false alarm rate reduced to the point where it was still 1%, and the percentage of attack identification had started to drop. At this point, the sliding threshold was thus fixed at [μ + 3τ] for T_{UW}. The values from our simulation have been summarized in figure 6.

Threshold	Step	Value	(%)Attack Detection	(%)False Alarm
T_{WU}	$\mu + \sigma$	**552.46**	100	6
	$\mu + 1.3\sigma$	583.50	99	6
	$\mu + 1.5\sigma$	604.20	93	6
	$\mu + 1.7\sigma$	624.89	73	5
T_{LW}	$\mu + \sigma$	240.8	100	6
	$\mu + 1.3\sigma$	255.14	100	4
	$\mu + 1.5\sigma$	**264.7**	100	3
	$\mu + 1.8\sigma$	279.04	100	3
	$\mu + 2\sigma$	286.5	98	3
T_{UW}	$\mu + \sigma$	346	100	15
	$\mu + 1.5\sigma$	363.5	100	10
	$\mu + 1.8\sigma$	374	100	8
	$\mu + 2\sigma$	381	100	5
	$\mu + 2.3\sigma$	391.5	100	3
	$\mu + 2.5\sigma$	398.5	100	2
	$\mu + 3\sigma$	**416.01**	100	1
	$\mu + 3.5\sigma$	433.51	100	1
	$\mu + 4.3\sigma$	461.51	98	1

Figure 6: Justification of threshold values

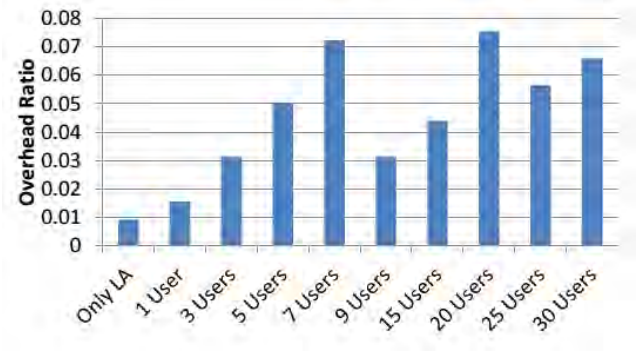


Figure 7: Approximate (95 Percentile) System Overhead Ratio

We applied the same sliding threshold model to determine the threshold values for T_{LW} and T_{WU} respectively. Upon similar experimental evaluations as above, the optimal threshold for T_{LW} has thus been set at [μ + 1:5τ], with a value of 264.7 milliseconds. The corresponding attack identification and false alarm rates are 100% and 3% respectively. Similarly, the optimal threshold for T_{WU} has been found to be at [μ + τ] with a value of 552.46 milliseconds. The corresponding attack identification and false alarm rates are 100% and 6% respectively. The results from the sliding threshold model for T_{LW} and T_{WU} are presented in figure 6.

3.3 System Overhead

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 7. The average overhead ratio for all the conditions was at 0.045, and the maximum value is seen to be at 0.075. As it can be seen, the LA server accounts for a nominal overhead ratio and does not have much change 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.

3.4 Secure Provenance

We proposed 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 $i \in \{1, 2, \ldots, n\}$.

Lemma 2: A location provenance chain C is a record of location proofs for locations L_i, where $i \in \{1, 2, \ldots, n\}$, and presence at each location L is verified using a location proof Proof(L) for that location.

Therefore, using Lemma 1 and Lemma 2, we can say that if a user U presents a provenance chain C, which has Proof(L) as one of the elements, this securely verifies the claim that the user U was present at

Properties	HC	BC	BF	SH	MH	RC
P1	✓	✓	✓	✓	✓	✓
P2	✓	✓	✓	✓	✓	✓
P3	✓	✓	✓	✓	✓	✓
P4	✓	✓	✓	✓	✓	✓
P5	✗	✗	✗	✓	✗	✓
P6	✗	✗	✓	✗	✗	✗
P7	✗	✗	✗	✗	✗	✓
P8	✗	✓	✓	✗	✓	✗

Figure 8: 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]

location L. Using the above lemmas, we put forward the following 8 propositions for secure location provenance:

- P1: Chronology
- P2: Order preservation
- P3: Verifiability
- P4: Tamper evidence
- P5: Privacy preservation
- P6: Selective in-sequence privacy
- P7: Privacy protected chronology
- P8: Convenience and derivability

Additionally, we adopted and created 6 different schemes for secure location provenance. Therefore, given the above security propositions for secure location provenance, Figure 8 summarizes the different properties and features for each of the eight different provenance schemes supported in WORAL [2]. The formal proofs for the security of these propositions for each of the provenance schemes are presented in [2].

3.5 Collusion Attacks

We define the following symbols: honest and malicious users U and $\overline{U}$, honest and malicious location authorities L and $\overline{L}$, honest and malicious witnesses W and $\overline{W}$. 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 [1].

- **[ULW]** All honest entities do not have the threat of generating false location proofs.
- **[$\overline{U}$LW]** $\overline{U}$ can request for false location proofs which will not be signed or endorsed by L and W. A proxy forwarding delay for a relay attack can be detected in step (g) of the protocol and the endorsement will be rejected by W.
- **[U$\overline{L}$W]** $\overline{L}$ cannot create a false proof and will never have the final receipt from the U. Additionally, W will not assert a location proof unless it can detect U's presence. W will not endorse a proof if the timestamp from $\overline{L}$ differs a lot from its own current system time. Any illegitimate information by the $\overline{L}$ will force U or the witness W to forfeit the WORAL protocol.
- **[UL$\overline{W}$]** $\overline{W}$ alone cannot do any harm, other than denial of service (DoS) and privacy violation of U. However, the many-to-one Crypto-IDs of U does not allow $\overline{W}$ to reveal U's linkable identity. A falsely asserted location proof will be discarded by L in step (e) of the WORAL protocol.

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

Figure 9: Service provider UI services

- **[U$\bar{L}\bar{W}$]** $\bar{L}$ and $\bar{W}$ cannot create false location proofs for U if U never participated in a proof protocol. $\bar{L}$ and $\bar{W}$ can give a user a backdated or a future dated timestamp. $\bar{L}$ can also store an old proof to launch a replay attack. However, U can discard the proof by not sending the final receipt in step (h). A relay attack can also be identified by U between step (f) and step (h).
- **[$\bar{U}$L$\bar{W}$]** $\bar{U}$ and $\bar{W}$ cannot create falsely asserted location proofs if L is honest. The L also doesn't allow U and $\bar{W}$ to be the same entities, and hence preventing a Sybil attack [52]. The SP enforces a centralized registration system and prevents a user from having multiple profiles on the same device. L can also identify a relay attack with a proxy U in step (h), and that of a proxy $\bar{W}$ in step (c).
- **[$\bar{U}\bar{L}$W]** $\bar{U}$ and $\bar{L}$ can collude to create a false proof with backdated or future-dated timestamp and launch a relay or replay attack. However, W will not endorse a false proof and can detect a relay attack in step (f).
- **[$\bar{U}\,\bar{L}\bar{W}$]** All-way collusion is not considered in WORAL. However, backdated and future-dated attacks can still be prevented if an auditor checks the published accumulator by the LA for the given epoch. A post-dating attack can be possible if L does not publish the future-dated proof created falsely by $\bar{U}$, $\bar{L}$, and $\bar{W}$.

We claim that any distributed security protocol without centralized monitoring requires at least one entity to be valid. The successful completion of any security protocol is protected against the legitimate entity, which plays the role of the situational verifier. Nonetheless, an auditor may impose a stricter proof model involving asserted location proof statements from multiple closely located location authorities to verify the actual presence of the user [1].

4. IMPLEMENTATION AND TECHNOLOGY TRANSITION

4.1 WORAL Service Provider

The WORAL service provider is a web based application built on the JavaServer Pages (JSP) framework. The service provider has a web-based interface for the service provider admin, the WORAL users, location authorities, and auditors. The summary of the service offered over the web interface is presented in figure 9. The service provider also exposes a set of RESTful APIs [51] for the Android application, and the Java desktop applications for location authority and auditor. Both the web interface and the RESTful APIs are exclusively available via HTTPS. The service provider can be configured for flexible backend database servers via the configuration script.

4.2 WORAL Location Authority

The LA server is a Java-based application communicating with the service provider and the user app. The application logs in and displays the service window. The control tabs on the top of the window is illustrated in Figure 10a. The operator can use the buttons to start and stop the server, and view the current list of location 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 10b. 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 Pi-s with 512 MB RAM, along with a customized Raspian image.

4.3 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

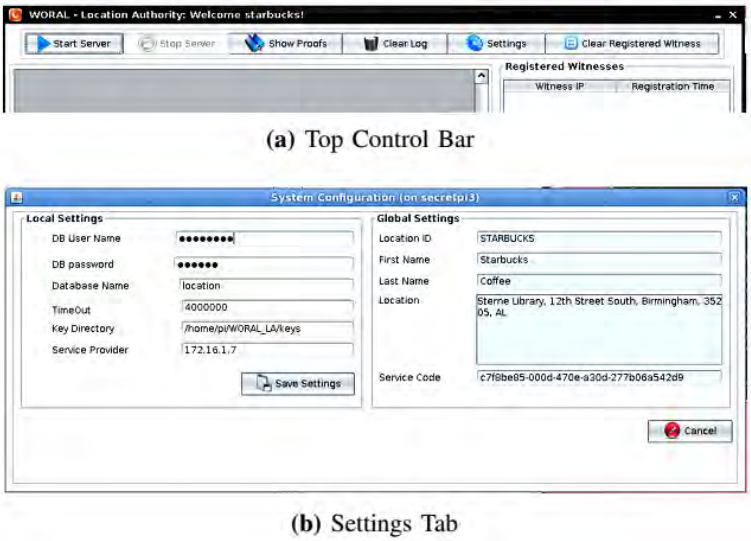
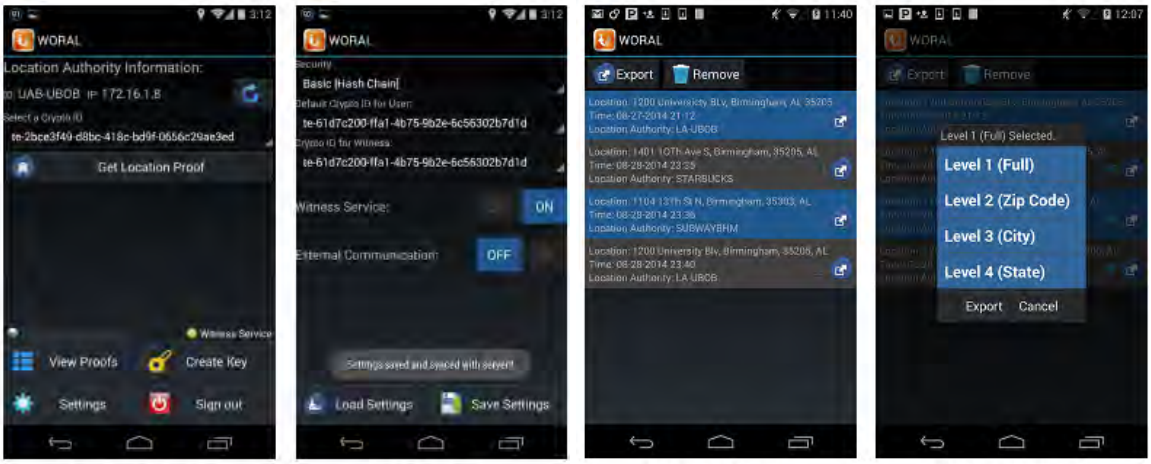


Figure 10: Location authority application panels

11a. 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 11b. 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 can be viewed as shown in Figure 11c. 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 11d. 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 transfer). 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.



(a) Home Screen (b) Settings (c) Proof List (d) Export Proofs

Figure 11: Android user application

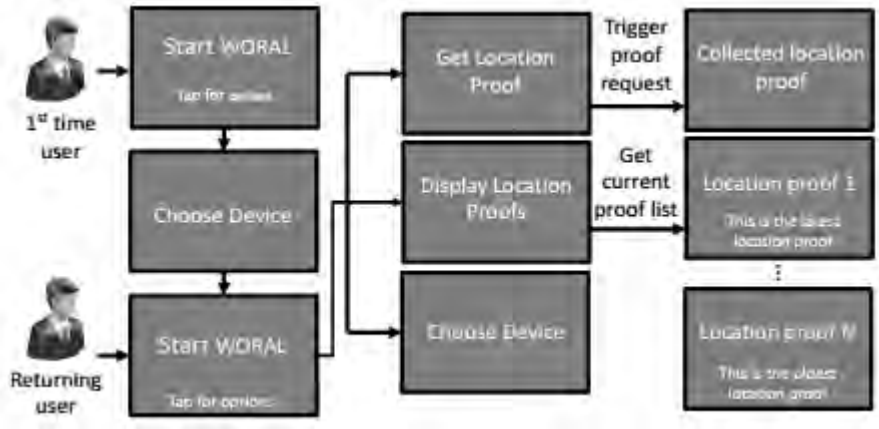


Figure 12: Google Glass/Watch application user flow

4.4 WORAL Wearable Device Extension

Wearable peripheral devices, such as the Google Glass and Google watch, 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 and watch 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 application 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 or watch extension. The UI flow for the Google Glass/watch is illustrated in Figure 12. Current implementation allows a user wearing the Google Glass or watch to request for location proofs and display the list of currently available location proofs from the mobile device.

4.5 WORAL Auditor

The WORAL auditor is a standalone Java desktop application communicating with the service provider. The user presents an exported proof (or list of proofs) and the auditor imports the file to verify the

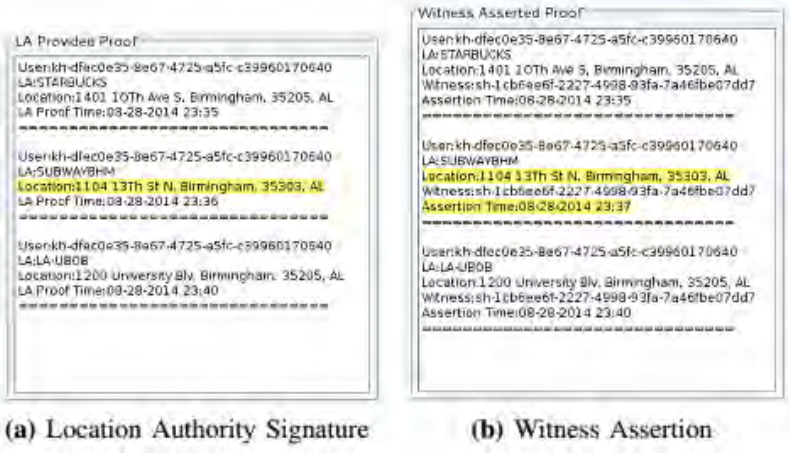


Figure 13: Auditor service panels

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 shown in Figure 13a and Figure 13b respectively. Any mismatched information is marked on the corresponding panels, as seen from Figures 13a and 13b. It therefore depends on the auditor to either accept or reject the location provenance claim by the user.

4.6 Technology Rollout

We had created a video animation for WORAL and had designed a publicity flyer. The animated WORAL video has been uploaded publicly on YouTube, and can be found online in the following URL: https://www.youtube.com/watch?v=mqMI-681LiI

In terms of commercial licensing, we have successfully filed an IPD with the University of Alabama Research Foundation (UABRF). We have also finalized the procedure for a US Provisional Patent filing via UABRF. The provisional patent information is provided below:

Title: Methods for Providing Witness Oriented Secure Location Provenance Framework for Mobile Devices
Date: 04/15/2015
Patent number: U0012-301059

4.7 Information Dissemination

The following publications were made with respect to the research performed under this project:

1. Rasib Khan, Shams Zawoad, Md. Haque, and Ragib Hasan, "**OTIT: Towards Secure Provenance Modeling for Location Proofs**", in Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS), Kyoto, Japan, June 2014.
2. Rasib Khan, Shams Zawoad, Md. Haque, and Ragib Hasan, **"Who, When, and Where? Location Proof Assertion for Mobile Devices"**, DBSEC 2014 Vienna, Austria, July 14-16, 2014.
3. Rasib Khan, Md Munirul Haque, and Ragib Hasan, "**Modeling a Secure Supply Chain Integrity Preservation System**", In Proceedings of IEEE International Conference on Technologies for Homeland Security, Waltham, MA, November, 2013.

4. Ragib Hasan, Rasib Khan, Shams Zawoad, Md Haque, **"WORAL: A Witness Oriented Secure Location Provenance Framework for Mobile Devices"**, IEEE Transactions on Emerging Topics in Computing (TETC) SI on Cyber Security, 2015.

5. CONCLUSIONS

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 paper, 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 asserted by a spatio-temporally co-located witness. WORAL is based on the Asserted Location Proof protocol [1], and is enhanced with provenance preservation based on the OTIT model [2]. 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.

6. REFERENCES

[1] R. Khan, S. Zawoad, M. Haque, and R. Hasan, "Who, When, and Where? Location Proof Assertion for Mobile Devices," in Proc. of DBSec. IFIP, July 2014.

[2] R. Khan, S. Zawoad, M. Haque, and R. Hasan, "OTIT: Towards secure provenance modeling for location proofs," in Proc. of ASIACCS. ACM, 2014.

[3] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in Proc. of HotMobile, 2009, pp. 1–6.

[4] J. VanGrove, "Foursquare cracks down on cheaters." Online at http:

//mashable.com/2010/04/07/foursquare-cheaters/, April 2010.

[5] I. Maduako, "Wanna hack a drone? possible with geo-location spoofing!" Online at http://geoawesomeness.com/?p=893, July 2012.

[6] N. O. Tippenhauer, K. B. Rasmussen, C. Popper, and S. Capkun, "iPhone and iPod location spoofing: Attacks on public WLAN-based positioning systems," SysSec Tech. Rep., ETH Zurich, April, 2008.

[7] A. J. Blumberg and P. Eckersley, "On locational privacy, and how to avoid losing it forever," Online at https://www.eff.org/wp/ locational-privacy, August 2009.

[8] J. McDermott, "Foursquare selling its location data through ad targeting firm turn," Online at http://adage.com/article/digital/ foursquare-selling- data-ad- targeting-firm- turn/243398/, July 2013.

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

[10] R. Hasan, R. Sion, and M. Winslett, "The case of the fake Picasso: Preventing history forgery with secure provenance," in Proc. of FAST. USENIX Association, 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. of HST. MA, USA: IEEE, 2013, pp. 446–450.

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

[13] P. Gilbert, L. P. Cox, J. Jung, and D. Wetherall, “Toward trustworthy mobile sensing,” in Proc. of HotMobile. ACM, 2010, pp. 31–36.

[14] W. Luo and U. Hengartner, “Proving your location without giving up your privacy,” in Proc. of HotMobile, 2010, pp. 7–12.

[15] B. R. Waters and E. W. Felten, “Secure, private proofs of location,” Technical report TR-667-03, Princeton University, January 2003.

[16] S. Brands and D. Chaum, “Distance-bounding protocols,” in Proc. of EUROCRYPT. Springer-Verlag New York, Inc., 1994, pp. 344–359.

[17] J. T. Chiang, J. J. Haas, and Y.-C. Hu, “Secure and precise location verification using distance bounding and simultaneous multilateration,” in Proc. of WiSec. ACM, 2009, pp. 181–192.

[18] K. B. Rasmussen and S. Cˇ apkun, “Realization of RF distance bounding,” in Proc. of USENIX Security. USENIX Association, Aug 2010.

[19] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, “Location privacy via private proximity testing,” in Proc. of NDSS, Feb 2011.

[20] P. Traynor, J. Schiffman, T. La Porta, P. McDaniel, and A. Ghosh, “Constructing secure localization systems with adjustable granularity using commodity hardware,” in Proc. of GLOBECOM, Dec 2010.

[21] J. Brassil, R. Netravali, S. Haber, P. Manadhata, and P. Rao, “Authenticating a mobile device’s location using voice signatures,” in Proc. of WiMob. IEEE, Oct 2012, pp. 458 –465.

[22] G. Ananthanarayanan, M. Haridasan, I. Mohomed, D. Terry, and C. A. Thekkath, “StarTrack: a framework for enabling track-based applications,” in Proc. of MobiSys, Jun 2009, pp. 207–220.

[23] A. Zugenmaier, M. Kreutzer, and M. Kabatnik, “Enhancing applications with approved location stamps,” in Proc. of Intelligent Network Workshop. IEEE, 2001, p. 140.

[24] A. I. Gonza´lez-Tablas, B. Ramos, and A. Ribagorda, “Path-stamps: A proposal for enhancing security of location tracking applications,” in Proc. of Ubiquitous Mobile Information and Collaboration Systems Workshop. Citeseer, 2003.

[25] J. Manweiler, R. Scudellari, and L. P. Cox, “SMILE: encounter-based trust for mobile social services,” in Proc. of CCS. ACM, Nov 2009, pp. 246–255.

[26] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, “Supporting location-based conditions in access control policies,” in Proc. of ASIACCS. ACM, 2006, pp. 212–222.

[27] K. El Defrawy and G. Tsudik, “Alarm: Anonymous location- aided routing in suspicious manets,” IEEE Transactions on Mobile Computing, vol. 10, no. 9, pp. 1345–1358, Sept 2011.

[28] K. El Defrawy and G. Tsudik, “Privacy-preserving location-based on-demand routing in MANETs,” IEEE Journal on Selected Areas in Communications, vol. 29, no. 10, pp. 1926–1934, Dec 2011.

[29] P. Enge and P. Misra, “Special issue on global positioning system,” Proc. of the IEEE, vol. 87, no. 1, pp. 3 –15, Jan. 1999.

[30] E. Gabber and A. Wool, “How to prove where you are: tracking the location of customer equipment,” in Proc. of CCS. ACM, 1998, pp. 142–149.

[31] D. E. Denning and P. F. MacDoran, “Location-based authentication: Grounding cyberspace for better security,” Computer Fraud & Security, vol. 1996, no. 2, pp. 12–16, 1996.

[32] K. Bauer, D. McCoy, E. Anderson, M. Breitenbach, G. Grudic, D. Grunwald, and D. Sicker, “The directional attack on wireless localization: how to spoof your location with a tin can,” in Proc. of GLOBECOM. IEEE Press, 2009, pp. 4125–4130.

[33] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. di Vimercati, and P. Samarati, “Location privacy protection through obfuscation-based techniques,” in Proc. of DBSec. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 47–60.

[34] C. R. Dunne, T. Candebat, and D. Gray, “A three-party architecture and protocol that supports users with multiple identities for use with location based services,” in Proc. of ICPS. ACM, Jul 2008, pp. 1–10.

[35] M. Gruteser and D. Grunwald, “Anonymous usage of location-based services through spatial and temporal cloaking,” in Proc. of MobiSys. ACM, May 2003, pp. 31–42.

[36] S. Capkun and J. Hubaux, “Secure positioning of wireless devices with application to sensor networks,” in Proc. of INFOCOM, vol. 3. IEEE, Mar 2005, pp. 1917–1928.

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

[38] S. Capkun, M. Cagalj, G. Karame, and N. Tippenhauer, “Integrity regions: Authentication through presence in wireless networks,” IEEE Transactions on Mobile Computing, vol. 9, no. 11, pp. 1608–1621, Nov 2010.

[39] Aruba Networks, Inc., “Dedicated air monitors? you decide.” Online at http://www.arubanetworks.com/technology/tech- briefs/ dedicated-air- monitors/, 2006.

[40] S. Pandey, F. Anjum, B. Kim, and P. Agrawal, “A low-cost robust localization scheme for wlan,” in Proc. of WICON. ACM, Aug 2006, p. 17.

[41] P. Tao, A. Rudys, A. Ladd, and D. Wallach, “Wireless lan location- sensing for security applications,” Computing Reviews, vol. 45, no. 8, pp. 489–490, 2004.

[42] M. Youssef, A. Youssef, C. Rieger, U. Shankar, and A. Agrawala, “Pinpoint: An asynchronous time-based location determination system,” in Proc of MobiSys. ACM, Jun 2006, pp. 165–176.

[43] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, “Location- based trust for mobile user-generated content: applications, challenges and implementations,” in Proc. of HotMobile. ACM, Feb 2008, pp. 60–64.

[44] S. Saroiu and A. Wolman, “I am a sensor, and i approve this message,” in Proc. of HotMobile, 2010, pp. 37–42.

[45] Z. Zhu and G. Cao, “Toward privacy preserving and collusion resistance in a location proof updating system,” IEEE Transactions on Mobile Computing, vol. 12, no. 1, pp. 51–64, 2013.

[46] X. Wang, J. Zhu, A. Pande, A. Raghuramu, P. Mohapatra, T. Abdelza- her, and R. Ganti, “STAMP: Ad Hoc Spatial-Temporal Provenance Assurance for Mobile Users,” in Proc. of ICNP, Gottingen, Germany, Oct 2013.

[47] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, “Provenance-aware storage systems,” in Proc. of USENIX ATC. USENIX Association, May 2006, pp. 43–56.

[48] D. Bhagwat, L. Chiticariu, W.-C. Tan, and G. Vijayvargiya, “An annotation management system for relational databases,” The VLDB Journal, vol. 14, pp. 373–396, 2005.

[49] I. Souilah, A. Francalanza, and V. Sassone, “A formal model of provenance in distributed systems,” in Proc. of TaPP. USENIX Association, Feb 2009, pp. 1–11.

[50] I. Martinovic, F. Zdarsky, A. Bachorek, C. Jung, and J. Schmitt, “Phishing in the wireless: Implementation and analysis,” in Proc. of IFIP SEC, 2007, pp. 145–156.

[51] L. Richardson and S. Ruby, RESTful web services. O’Reilly Media, Inc., 2008.

[52] J. Douceur, “The Sybil attack,” Peer-to-peer Systems, pp. 251–260, 2002.

ACRONYMS

ALP	Asserted Location Proof
ALPAck	Asserted Location Proof Acknowledgement
AReq	Assertion Request
BC	Block-Hash Chain
BF	Bloom Filter
C	Location Provenance Chain
CID	Cryptographic Identifier
DoS	Denial-of-Service
GPS	Global Positioning System
HC	Hash Chain
LA	Location Authority
LBS	Location-based Service
LP	Location Proof
LProv	Location Provenance
MAC	Media Access Control (Address)
MH	Multi-Link Hash Chain
Mu (μ)	Average
PLP	Proactive Location Proof
PReq	Proof Request
Proof(L)	Proof for location L
PS	Provenance Scheme
RC	RSA (Cryptosystem) Chaining
REST	Representational State Transfer
S	Site (Location)
$S_E(M)$	Signature by entity E on message M
SH	Shadow-Hash Chain
Sigma (σ)	Standard Deviation
SP	Service Provider
T_{LW}	Time for message sent/received by Location Authority to/from Witness
T_{UW}	Time for message sent/received by User to/from Witness
T_{WU}	Time for message sent/received by Witness to/from User
U	User
VReq	Verification Request
VS	Verification Statement
W	Witness
WORAL	Witness Oriented Asserted Location proof