GOVERNMENT DEGREE COLLEGE KOLLAPUR ,NAGARKURNOOL(DIST)

DEPARTMENT OF COMPUTER SCIENCE AND APPLICATIONS

JIGNASA PROJECT

ON

WORAL: Oriented Secure Location Framework for Mobile Devices

Witness

STUDENTS: 1) A.POOJITHA 230330174681001,
2) D. ANOOSHA 230330174681003,
3) MUZAHIRENA 230330174751009 ,
4) P. SRILATHA 230330174681007 ,
5) R. JOYTHI 230330174681008,

SUPERVISOR: MD SOFI PASHA

Contents

- Introduction
- Woral Framework
- Woral Architecture
- Witness Registration
- Implementation

Introduction

- 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.
- The system is based on the Asserted Location Proof (ALP) protocol.

WORAL Framework

- Terminologies
- Witnesses and Assertions
- Threat Model
- System Model

Terminologies

- The ***Service Provider*** **SP** is the trusted entity providing the secure location provenance service to mobile users.
- 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.
- A ***Witness*** **W** is a spacio-temporally co- located mobile user.
- A ***Witness List*** **WL** provides the listing of all registered witnesses under the coverage of the location authority at a given time.

- A witness is a spatio-temporally 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.
- 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.

Threat Model

- 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.
- 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.

Threat Model

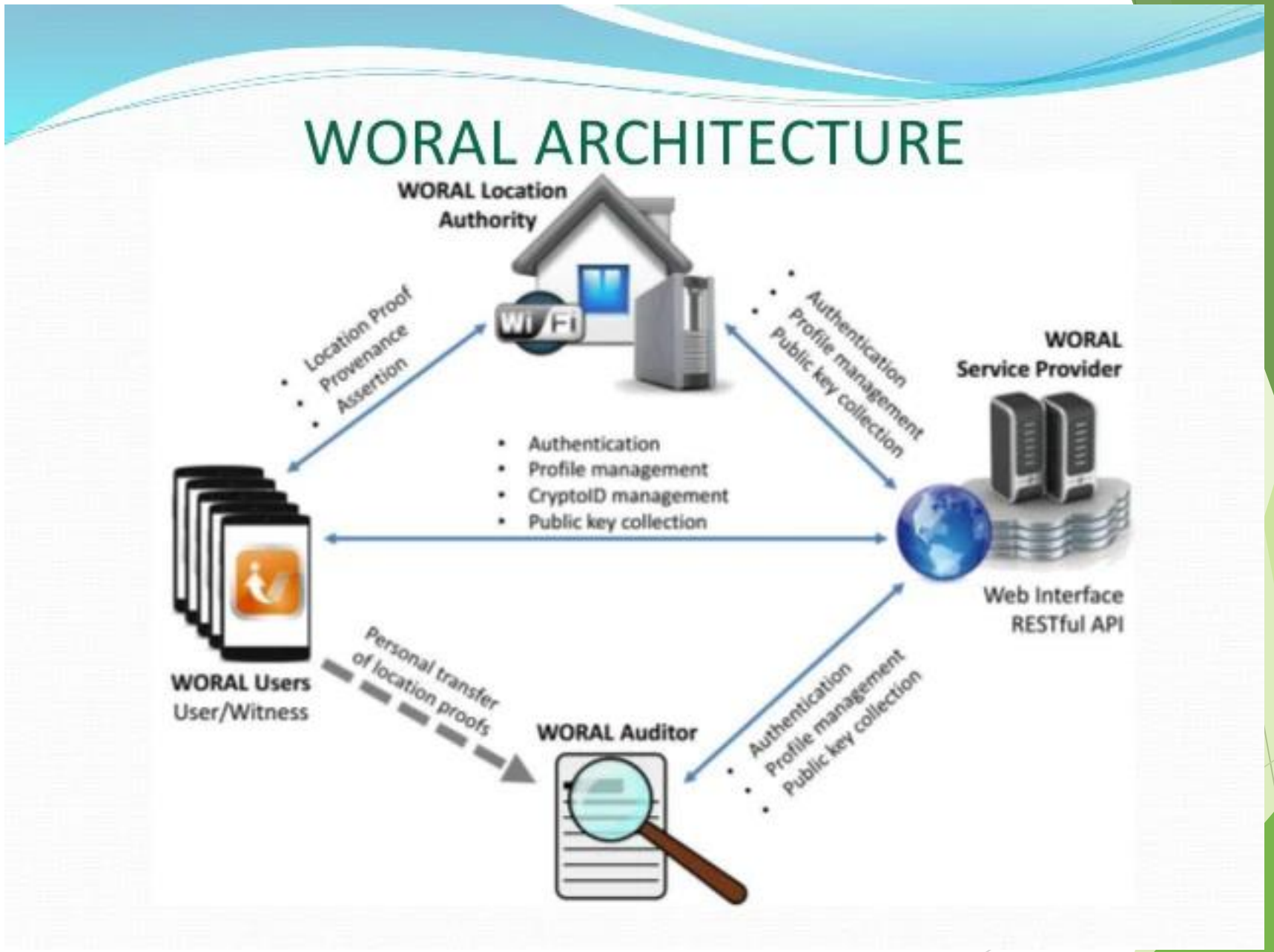
- We expect that mobile devices are non-shareable private properties and the physical security of the phone depends on the user himself.
- Attacks such as MAC address fingerprinting are prevented via known techniques such as MAC address cloning.
- After a proof is collected for a particular site, the user can delete or tamper with location proof and provenance records which are saved on the device.

System Model

- We assume that mobile devices carried by users are capable of communicating with other devices and LAs over Wi-Fi 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 LA is a fixed server with higher computation and storage capability than a mobile device.

- A location runs a Wi-Fi 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.

WORAL ARCHITECTURE



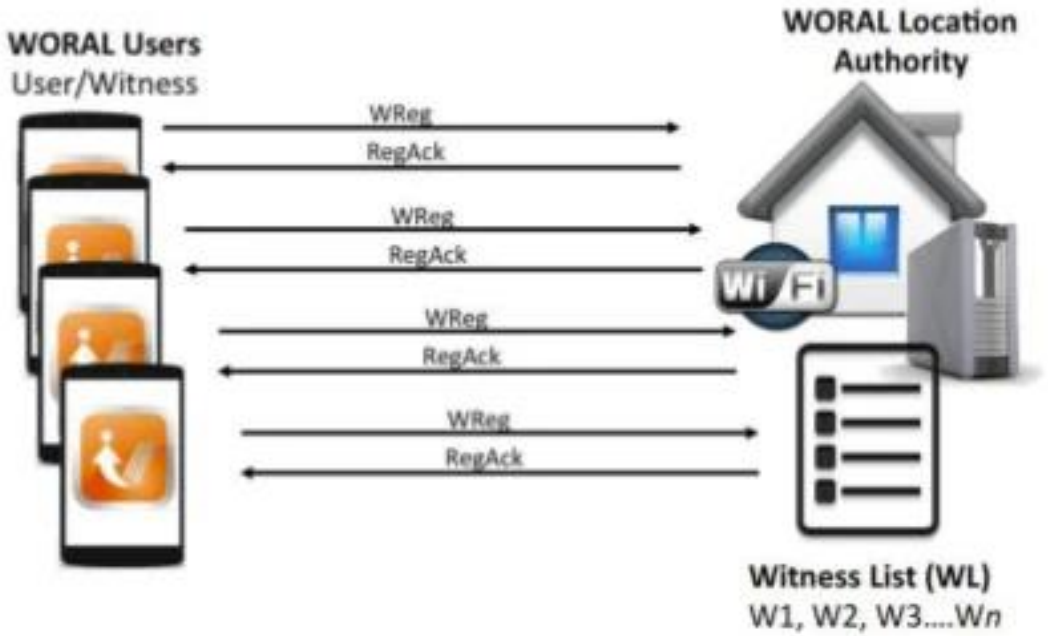
Service Provider

- **Account Creation and Authentication:** In the WORAL framework, users, witnesses, LAs, and auditors need to create an account with the SP using a unique identification criteria such as the Social Security Number, passport number, driving license, trade license, or anything else.
- **CryptoID and Key Distribution:** The SP is responsible for providing access to public keys in different stages of the protocol.

Location Authority

- The user and witness need the IP address of the LA to establish a 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 witness through the LA discovery protocol using broadcast messages

Witness Registration



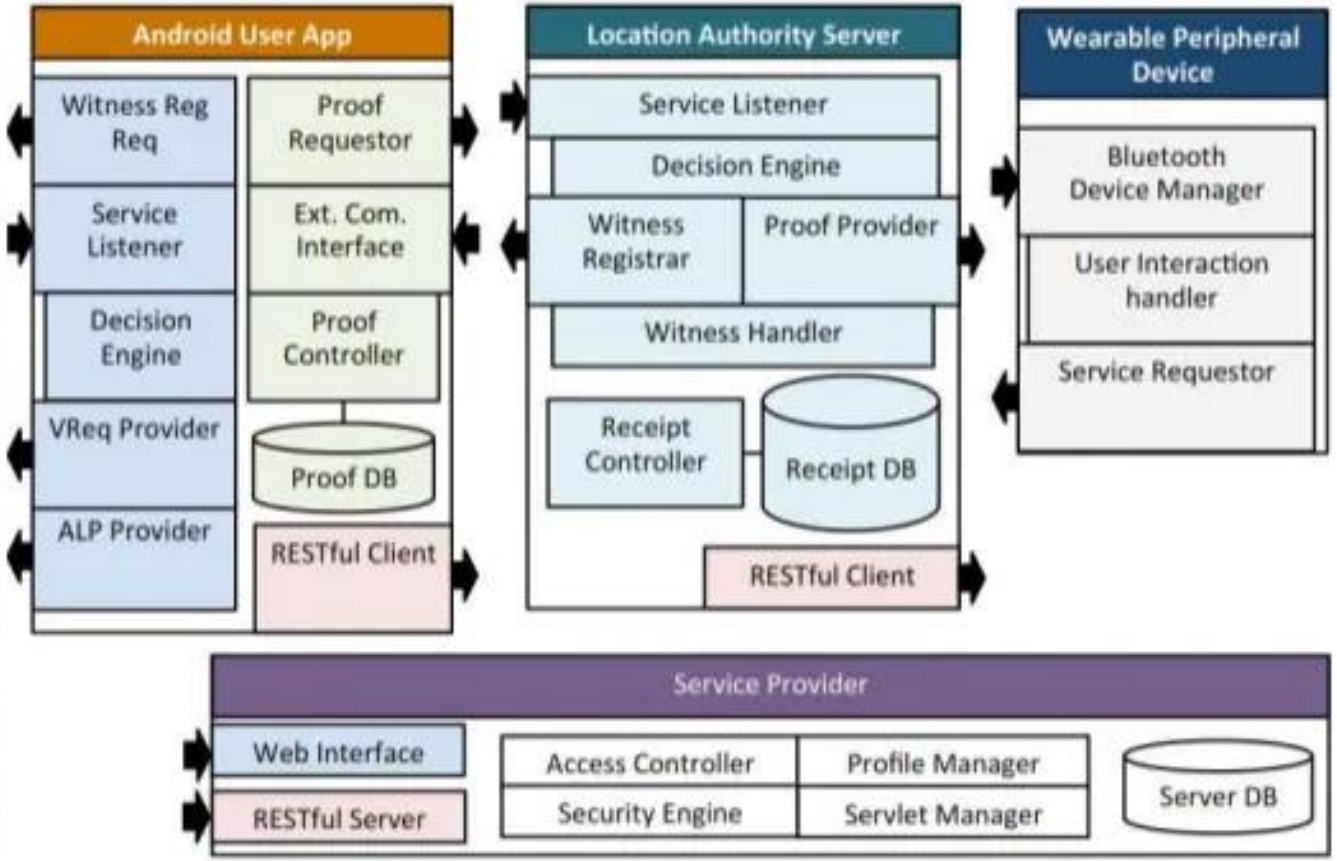
A WORAL mobile user express his willingness to serve as a witness by sending a witness registration message WReg to the LA.

$$W\ Reg = <CID_w, t_w, S_w(CID_w, t_w)>$$

System Overhead for Location Authority

- The LA server was deployed on a dual- core Intel Q9550 2.83GHz desktop PC with 4GB RAM and Ubuntu operating system.

Component Architecture



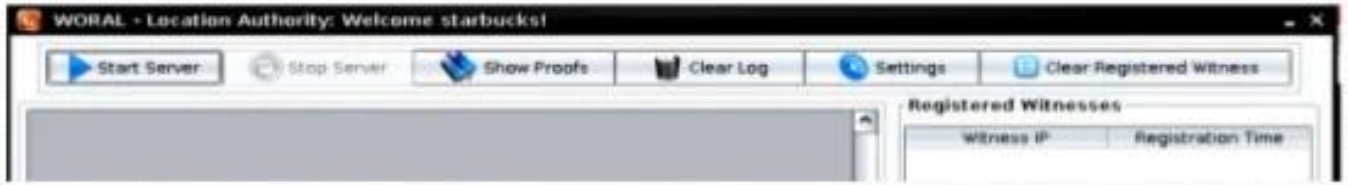
WORAL Service Provider

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

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

WORAL Location Authority

- The LA server is a Java-based application communicating with the service provider and the user app.



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.

Home Screen

Setting

WORAL Users

Proof List

Export Proofs

The application is tested 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 Auditor

The WORAL auditor is a standalone Java desktop application communicating with the service provider.

Conclusion

- 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.
- 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.


THANK
YOU