Secure Location Provenance for Mobile Devices

Cyber Security Division
2012 Principal Investigators’ Meeting

October 11, 2012

Ragib Hasan, Ph.D.
Assistant Professor
University of Alabama at Birmingham
ragib@cis.uab.edu
205-934-8643
Introduction

- **TTA #10: Digital Provenance**

- **Project Title**: Secure Location Provenance for Mobile Devices
- **Project Location**: University of Alabama at Birmingham

- **Our Team**
  - **Lab**: UAB SECRETLab ([http://secret.cis.uab.edu](http://secret.cis.uab.edu))
  - **PI**: Ragib Hasan, Assistant Professor, UAB
  - **Postdoctoral Fellow**: Md. Haque, Ph.D.
  - **Graduate Students**: Shams Zawoad, Rasib Khan
Provenance refers to the history of an object (i.e., the origin and derivation history).

Digital provenance focuses on recording the entire lifecycle of a digital object.

Widely used by scientific computing community, provenance is only recently being used in file systems and databases.
Location Provenance

- **Physical location** is a very important but often overlooked attribute of an object

- **Location history** is very important in real-world security

**Example:**
- Location history of food/medicine
- Location history of people or devices entering secure locations
- Location history of criminal suspects
- Location history for reimbursement processing
Problem Statement:

How can we verify or audit the location provenance/history of a person or a mobile device while respecting privacy?

That is, given a set of claims by a subject of being present in various locations at different times, how do we verify that

- The subject was actually physically present in such locations at the claimed time
- The subject visited the locations in the claimed order

Note: the subject can be a device, data, other objects, or a human.
Technical Approach

Potential Approaches:

- **Tracking by system** (Centralized “Big Brother”-like tracking)
  - Violates privacy
  - Not scalable/feasible at large scale

- **Self-reported locations** (e.g., via GPS)
  - Users can lie about locations
  - Location information can be spoofed

- **Hybrid-approach** (user chooses to get location proofs)
  - A loosely distributed set of location services provide location proofs for a small physical location
Example Scenario

- Alice visits a Starbucks at 3.21 pm

- Bob, the manager of the Starbucks, gives Alice a “proof”, stating that Alice was present at that Starbucks at 3.21 pm

- Alice keeps track of her location proofs, and later can present (a subset of) the proofs to prove her location history
How Location Proof Systems work today

Problem: This works when users and locations do not collude
Limitations of Existing Schemes

Existing location proof schemes:

- Location ensures that user is present (e.g., via Distance bounding)
- Issues a signed proof of presence
- Can prevent users from creating false proofs
- **Do NOT consider collusion** between user and location to create false proofs (fake alibis)
- Not privacy preserving

Location provenance schemes

- Very little research on location provenance schemes
- Need to preserve privacy
Our goals

- Build a **collusion-resistant, high-performance, lightweight** location provenance system

- Use common off-the-shelf mobile devices (i.e., require no special hardware)

- Note: Techniques can be extended to other physical objects as well
Challenges

- **Preventing collusion**
  - Very difficult to prevent all types of collusions between location and users
  - Location proofs can be computed offline, backdated/postdated, or simulated

- **Privacy**
  - How do we prove order of any arbitrary subset (of locations)?

- **Location granularity**
  - How can users get a single location proof, but prove it at different granularities?
Our Approach: Collusion-resistant location proofs

- To make collusions more difficult, introduce the notion of Witnesses.

- In our Witness-endorsed proof model, witnesses who are also present in the same location, endorse location proofs.
  
  - E.g., Charlie says that he is also present in the same Starbucks as Alice, and he endorses the proof Alice got from Bob.
  
  - Very difficult to pull off a location-user collusion unless they can get (independent) witnesses to collude as well.
Our Approach: Privacy-preserving Location Provenance Schemes

- Use novel data structures that allows users to prove the order of any arbitrary subset of locations
- Allow users to prove locations in any granularity via privacy-preserving proofs
- Build verifiable location provenance chains with low overhead
Our Approach

1. Device and Location Provider participates in protocol to ensure presence.

2. Location Provider issues Location Proof.

3. Proof sent to Witness for Endorsement.


5. New location data and proof inserted in location provenance chain.

Mobile Device

Location Service Provider

Co-located Witness
Milestones, Deliverables, and Schedule

Milestones:

▪ Phase 1:
  ▪ Milestone 1: Design of a realistic and practical threat model for location
  ▪ Milestone 2: Design of an attacker model that addresses collusion and other real-life attack scenarios
  ▪ Milestone 3: Design of specifications of proposed system

▪ Phase 2:
  ▪ Milestone 4: Design and analysis of a location proof schema and generation algorithm.
  ▪ Milestone 5: Design of a location provenance schema, provenance generation algorithm, and provenance verification algorithm
Milestones, Deliverables, and Schedule

Milestones

- **Phase 3: Implementation**
  - Milestone 6: Completion of location provenance application and proof server code.

- **Phase 4: Evaluation**
  - Milestone 7: Completion of performance evaluation report.

- **Phase 5: Release**
  - Milestone 8: Completion of open source release of software tools and collaboration with vendors.
Deliverables

- **Publications and Technical reports:**
  - We already have a preliminary version of the threat model and collusion model as a tech report

- **Software and documentation**
  - Mobile app for Android and iPhone
  - Location proof server
  - Location provenance libraries for Android and iPhone
  - Documentation and tutorials on app, code, and system
Technology Transition Plan

- **Software release:**
  - All software developed under this project will be released in open source and will be made available on the project website
  - We will release location provenance server and client apps

- **Collaboration with vendors:**
  - We already have an established relationship with Google’s Mobile platform team
  - We will work with them to develop native location proof support for Android-based phones
Quad Chart

BAA Number: 11-02
Title: Secure Location Provenance for Mobile Devices
Date: July 7, 2011

Officer Name: Dr. Ragib Hasan/University of Alabama at Birmingham

Operational Capability and Goals

1. Trustworthy verification of location data provenance for mobile devices
2. Prevents/detects collusion between different entities
3. Allows users to protect privacy by enabling verification of any arbitrary subsequence of location provenance
4. Solution can be implemented and executed in today's mobile phones and other mobile devices
5. Proposed research matches the goals of the BAA by advancing the state of the art in location history and provenance verification

Proposed Technical Approach:
Leverage ideas from secure file provenance to protect integrity and confidentiality of location data provenance for mobile devices. Develop novel cryptographic constructs to allow privacy-preserving location provenance audits. No technology exists today to audit location provenance.

Tasks:
- Development and evaluation of the threat model, witness-attested model, algorithms for generating collision-resistant, witness-endorsed location proofs
- Design of schemes for verification of chronological order of location proofs
- Implementation of location provenance applications on mobile phone and location proof services
- Performance evaluation of the location proof infrastructure through experiments
- Deployment of production quality application and service software to DHS

Related Works:
Officer Dr. Hasan is the pioneer in securing data provenance for files and built SPROV, an application layer library for secure file provenance

Schedule, Cost, Deliverables, & Contact Info:

Deliverables:
Year 1: System Specification, Model document, Attack Analysis. Proof of concept demonstration
Year 2: Extensive testing and evaluation, production quality prototype construction, deployment, commercialization

Corporate Contact Information: University of Alabama at Birmingham
Technical Point of Contact: Dr. Ragib Hasan, Assistant Professor, Department of Computer and Information Sciences, University of Alabama at Birmingham, 115, 1300 University Blvd, Birmingham, AL 35294
Phone: 205-934-8643 Email: ragib@cis.ua.edu FAX: 205-934-5473
Questions?

Please visit http://secret.cis.uab.edu

Contact:
- Ragib Hasan
- ragib@cis.uab.edu
- 205-934-8643