CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS’

Secure Location Provenance for Mobile Devices

University of Alabama at Birmingham

Ragib Hasan

September 16, 2013

Homeland Security

Science and Technology

Team Profile

SECu**RE** and **T**rustworthy computing Lab (**SECRETLab**)

Department of Computer and Information Sciences

University of Alabama at Birmingham, AL, USA

Principal Investigator:	Ragib Hasan, Ph.D. *Assistant Professor, UAB*
Post Doc. Fellow:	Md Munirul Haque, Ph.D.
Ph.D. Students:	Shams Zawoad Rasib Khan, M.Sc.

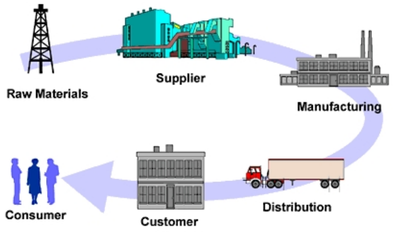
Customer Need

Why do we need Location Proof / Provenance?

Ever wondered where your food comes from, or whether your medicine came through the proper supply channels?

Proof of location history is needed for many applications

- Supply chain integrity preservation
- Secure travel log maintenance
- Alibi preservation for investigation
- Location based benefit claims
- Corporate traveling
- Personal record keeping



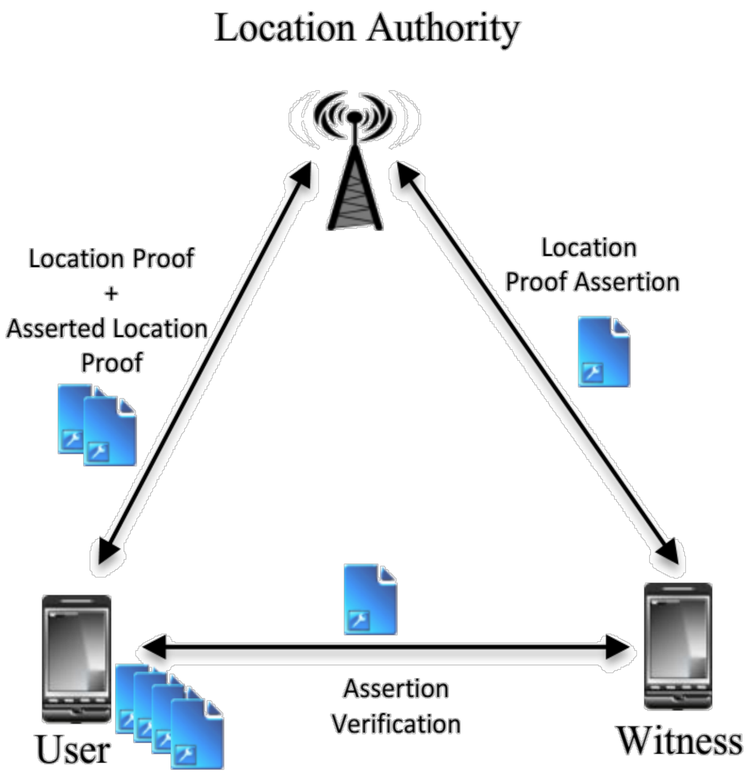
Approach

We present a system for distributed location proofs and provenance for mobile devices, with following properties:

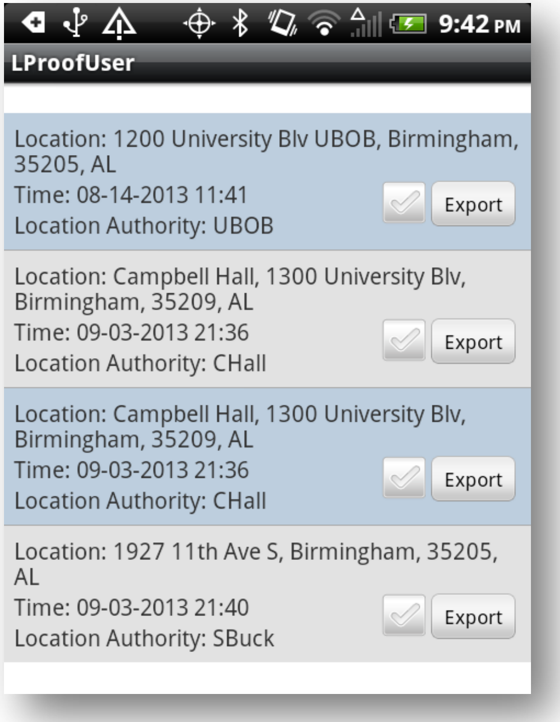
- **Securely generated** location proofs
- **Decentralized** solution for easy deployment
- **User-centric** solution to allow maximum user-control
- **Privacy protection** for user information containment
- **Collusion-resistant** and **tamper-evident** to ensure validity of information
- **Order preserving** provenance records

Approach *(cont.)*

- **Three-party model** for generating location proofs
  - **User** – requests proof
  - **Location Authority** – issues proof
  - **Witness** – endorses proof
- Three-way mutual validation
- Threshold based admission and acceptance
- **Chronological chaining** of proofs
- **Auditor** – validates proof presented by user



Approach *(cont.)*


9:42 PM

LProofUser

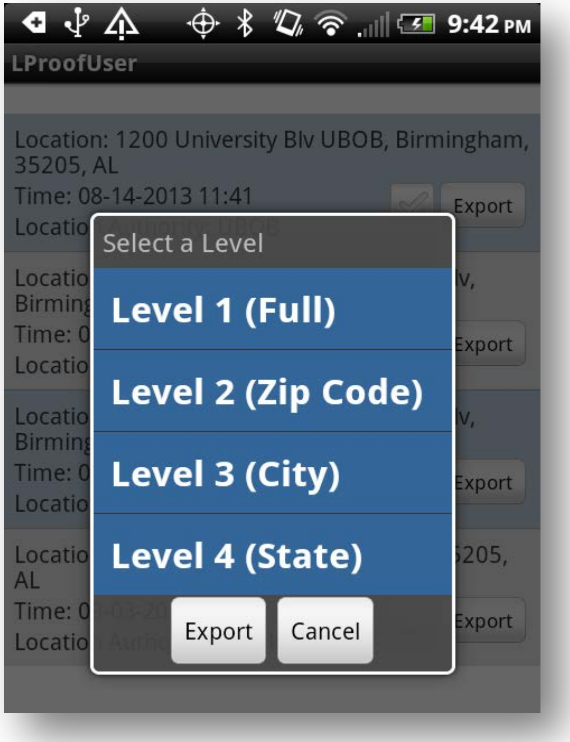
Location: 1200 University Blv UBOB, Birmingham, 35205, AL
Time: 08-14-2013 11:41
Location Authority: UBOB

Location: Campbell Hall, 1300 University Blv, Birmingham, 35209, AL
Time: 09-03-2013 21:36
Location Authority: CHall

Location: Campbell Hall, 1300 University Blv, Birmingham, 35209, AL
Time: 09-03-2013 21:36
Location Authority: CHall

Location: 1927 11th Ave S, Birmingham, 35205, AL
Time: 09-03-2013 21:40
Location Authority: SBuck

List of received location proofs


9:42 PM

LProofUser

Select a Level

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

Export proof for submitting to auditor

Prototype Application Screenshots

Approach *(cont.)*

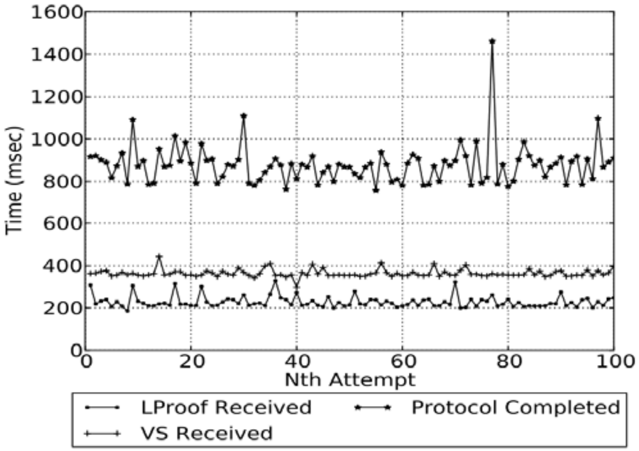
Location Provenance

Location provenance provide a verifiable location chronology for the mobile device.

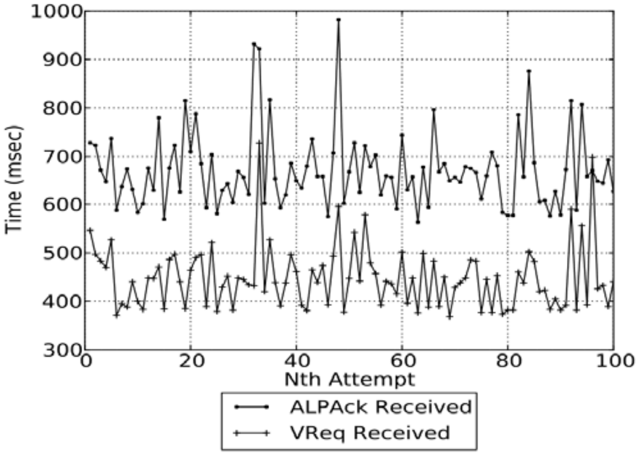
Our location provenance schemes provide the following guarantees:

- False history cannot be implanted by user or anyone else
- Hash-chains protect chronology
- Memory efficiency achieved via Bloom filters
- Users are capable of selectively proving **any arbitrary subset** of their location history, at any chosen granularity. This protects user privacy and allows the user to control what is revealed.

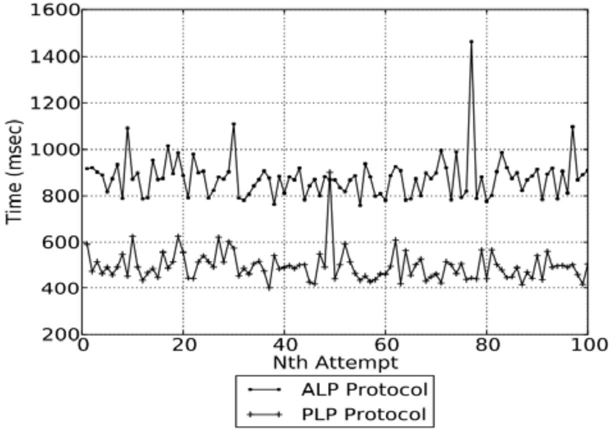
Approach *(cont.)*



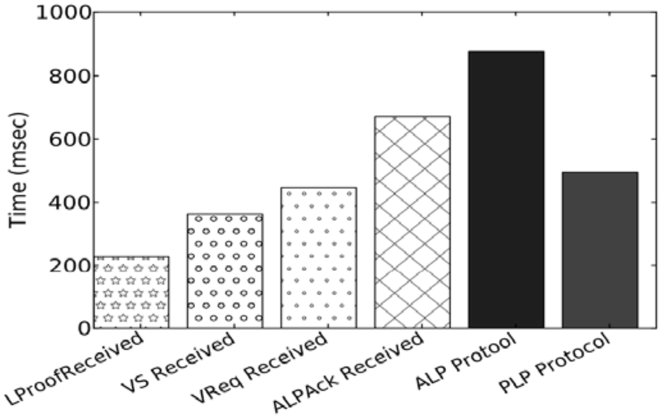
(a) User Application



(b) Witness and Location Authority



(c) Comparison between ALP & PLP



(d) Average Time Required for Different Steps of the Protocol

Benefits

- **Decentralized** model allows easy deployment for location proof generation
- Ownership of proof item and provenance chain is strictly **user-centric**, and Users can protect their privacy as they are **in control** of what gets recorded and revealed.
- More **efficient** than existing location proof systems (proved experimentally)
- Cryptographic ID ensures **privacy**
- Three-way mutual validation ensures the protocol to be **collusion-resistant**
  - (proved theoretically)
- Threshold based admission/acceptance of signatures **detects relay/proxy attacks**
  - (proved through experimental simulation)
- Hash-chains and Bloom filters allow memory efficient **chronological provenance** chains

Competition

Current technologies are

- GPS-based
- Self-reported (e.g. Facebook)
- Automatic provider-oriented reporting (e.g. Google)
- Centralized architecture (e.g. [1] Dunne et al. 2008)

Research Gaps

- **No competitor** supports the unique features we provide (provenance, collusion-resistance, verifiability)

- Current state-of-the art
  - Lacks security (e.g. misreport, masquerade, collude)
  - Lacks control (provider-oriented, privacy issues)
  - Lacks scalability (centralization bottleneck, establishment issues)

- We introduce **new capability** that will advance the state-of-the-art significantly

[1] DUNNE, C. R., C ANDEBAT, T., AND GRAY, D. 2008. A three-party architecture and protocol that supports users with multiple identities for use with location based services. In Proceedings of the 5th International conference on Pervasive services. ICPS '08. ACM, 1–10.

Current Status

- **Completion of Phase 1** (a and b), January 2013
  - System model and goals
  - Attack model and possible attacks
  - Architectural definitions

- **Completion of Phase 2** (a and b), July 2013
  - System Components
  - Proof components
  - Design and security analysis of the scheme
  - Prototype development (please visit demonstration booth)
  - Extended experimental results and evaluation
- Currently in **Phase 3**.

- **Milestones** 1 to 5 have been reached.

- **Privacy Threshold Analysis** has been performed to determine the impact on user privacy. Our project passed the analysis was found to comply with DHS/S&T/PIA-02.

- **Prototypes**: Android applications for users, and location server prototypes have been created and limited testing has been performed.

- **Technical progress reports**: November 2012, January 2013, March 2013, July 2013

Please visit our prototype demo this afternoon.

Next Steps

- **Things to do:**
  - Optimize efficiency for location provenance chain creation and storage
  - Random identity generation for users
  - User-centric granular exposure of information
  - Larger scale testing with many mobile devices
  - Financial modeling and strategic planning for location provenance solution deployment
  - Completion of the final prototype
- **Release plan**: Make the app available on Android App Store/Google Play, and release server code/app code in open source.

Contact Information

- **SECRETLab**
  - Phone: 205.934.8643
  - Fax: 205.934.5473
  - Web: http://secret.cis.uab.edu/

- **PI: Ragib Hasan**
  - Email: ragib@cis.uab.edu
  - Web: http://www.ragibhasan.com/