

Decentralised location proof system

February 23, 2016

Abstract

1 Introduction

2 Previous work

Location proof systems are expected to be accurate and tamper-proof. For this reason, existing solutions have chosen to use a central authority to issue proofs [1, 2, 3].

Hardware techniques [1] operate by supplementing existing WiFi access points with *femtocells* (small cellular antennae that connect to the mobile carrier via the Internet). Location verification over the internet is made possible by determining which femtocell a mobile node is connected to as it transfers data via Wi-Fi. This solution requires investment in additional hardware to supplement existing WiFi access points. It also requires access to mobile providers user database to identify users locations.

Other proof systems [2] deploy software on Wi-Fi access points. Access points taking part in the location proof network become part of a 'group' with a shared group signature. Mobile nodes can request a location proof from an access point, who signs it with the group signature. Access points provide location proofs to nodes without ever learning the node's identity, thus protecting user's privacy. However, due to the systems reliance on the group signature structure, access points become a target for attack. Compromising an access point would allow an attacker to create false location proofs.

[2] considers a number of threats in their architecture:

- **Dishonest users.** A dishonest user tries to obtain location proofs that certify her presence at some place at a particular time even if she was not there. Dishonest users may achieve this goal by colluding with malicious intruders.
- **Malicious intruders.** A malicious intruder is not interested in obtaining location proofs for her own use but offers to help other users to get location proofs on their behalf in exchange for other benefits like money.
- **Curious APs and applications.** A curious AP tries to learn a users identity while the user is acquiring a location proof from the AP. Similarly, a curious application tries to learn more location information from a location proof than it really needs.
- **Malicious applications.** A malicious application obtains location proofs from its users and then tries to take advantage of these proofs to get unauthorised access to other applications.
- **Active and passive eavesdroppers.** An eavesdropper records and maybe modifies communication between users, proof- ssuers, or applications.

Distributed P2P location proof systems also exist [3]. A central authority is used and acts as a certificate authority, issuing a unique ID to each person using the system. Unique identity is proved by users by providing SSN, drivers licence, or passport documents. This removes the threat of a Sybil attack, but makes the central authority a clear target for attack. The system uses three parties to provide location proofs; a mobile user who requests a proof, a fixed location authority, and a mobile user who acts as a witness. The system becomes vulnerable in the case where all three users collude, but is otherwise quite an interesting approach.

[3] also outlines a number of possible attacks on their system:

- **False presence:** A malicious user can create a fake location proof on his own, without being physically present at the location. The fake proof is supposed to resemble an actual proof, which the user could have actually collected from a valid location authority.

- **False timestamping (backdating, future dating):** In a backdating attack, the user and the location authority colludes to create a proof for a past time. Conversely, in future dating, the location authority and a user colludes to generate a proof with a future timestamp.
- **Implication:** A location authority and/or a witnesses can falsely accuse a user of his presence at a certain location. In this case, the malicious location authority and witness colludes to generate a false proof of presence for the user.
- **False assertion:** A user can collude with a witness, and generate a falsely asserted location proof. The truth value in such a fake proof is reinstated with the assertion received from the other user.
- **Denial of presence:** A user can visit a location and at a later time, deny his presence at that location. In such a case, the user actually denies the validity of a certain location proof that has been generated upon his presence at that particular location.
- **Proof switching:** The user is expected to have full access to all storage facilities on his mobile device. Hence, the user utilizes the legitimate proof and manipulates the information to create a false proof for a different location.
- **Relay attack:** A user can use a proxy to relay the requests and collect a location proof. Alternatively, a location authority can maliciously relay assertion requests with the witness not being present at the site.
- **Sybil attack:** A Sybil attack occurs when a single user generates multiple presence and identities [29]. A user can launch a Sybil attack by generating multiple identities representing a user and a witness and provide false endorsements for location proofs.
- **Denial of witnesss presence:** At the time of proof verification, the user can claim the absence of witnesses at the site or falsely claim an assertion to be counterfeit. The user and the location authority may also collude and claim the non-availability of witnesses.
- **Privacy violation:** An attacker may capture an asserted location proof generated for a user, and discover the identity of the user and/or the witness.

'OTIT' [4], a model for designing secure location provenance, can be used to compare existing location proof systems. This model defines the following requirements necessary for designing any secure location provenance scheme: Chronological, Order Preserving, Verifiable, Tamper Evident, Privacy Preserved, Selective In-Sequence Privacy, Privacy Protected Chronology, and Convenience & Derivability.

3 Results

4 Conclusions

References

- [1] J. Brassil, P.K. Manadhata, "Verifying the Location of a Mobile Device User", Proc. of MobiSec 2012, June 2012.
- [2] Luo, W., Hengartner, U., "Proving your Location without giving up your Privacy", Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, HotMobile 2010, Annapolis, Maryland, February 22 - 23, pp. 712. ACM, New York (2010)
- [3] R. Khan, S. Zawoad, M. M. Haque, and R. Hasan, "'Who, When, and Where?' Location Proof Assertion for Mobile Devices", Proceedings of the 28th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy, ser. DBSec. IFIP, July 2014.
- [4] Khan, R., Zawoad, S., Haque, M., Hasan, R. "OTIT: Towards secure provenance modeling for location proofs", Proc. of ASIACCS. ACM (2014)