POSTER: Security By Mobility in Location and Track Verification

Matthias Schäfer[†] Daniel S. Berger[†] Vincent Lenders[*] Jens Schmitt[†]

[†]University of Kaiserslautern
Germany
{schaefer, berger, jschmitt}@cs.uni-kl.de

[*]armasuisse
Switzerland
vincent.lenders@armasuisse.ch

ABSTRACT

This poster presents the idea of exploiting mobility to improve the security in location and track verification. Unlike traditional approaches which require tight time synchronization or two-way communication, mobility can be used to derive lightweight verification schemes. By ensuring independent movement of the verifiers, our scheme can provide security guarantees even if the verifiers' positions are known to the attacker. We also give an outlook on more general opportunities for mobility-aided security.

1. INTRODUCTION

Location verification seeks to verify claims of users to be at certain positions. Common solutions to this challenge employ triangulation or challenge response techniques to verify the physical origin of a signal. However, the underlying assumptions of time synchronization between verifiers or the presence of a two-way communication channel are not always met in practice. Schäfer et al. [1] have recently demonstrated that these system requirements can be considerably relaxed by exploiting the mobility of verifiers. By verifying a sequence of consecutive location updates (*track verification*) instead of single location claims, they were able to detect location spoofing attacks without time synchronization or dedicated communication.

The security of the scheme of Schäfer et al. assumes that verifiers and attackers are stationary. This assumption, however, can be violated in realistic scenarios. At the same time, the scheme does not fully exploit the potential of mobility. For example, mobile verifiers can provide useful means to further relax requirements such as the minimum required number of messages to detect attacks. In fact, our current research suggests that with mobile verifiers, it is possible to mitigate known problems of the above scheme while at the same time reducing system requirements of existing location verification schemes.

This poster seeks to give an overview of the role of mobility for security in location and track verification. In particular, we study both the challenges and opportunities brought forward by mobile attackers and verifiers.

2. MOBILITY IN SECURITY

Mobility has been recognized to be beneficial for security more than a decade ago. In 2003, Čapkun et al. [2] proposed using mobility to move two nodes into immediate physical vicinity. If nodes are close enough, secure side channels such as the visual contact between users can be used to set up security associations between the nodes.

Five years later, Čapkun et al. [3] presented a scheme which relies on mobile base stations to securely verify claimed positions. Trusted base stations initiate the verification of a node's location by sending a verification request from one position and then move to a second position to receive the response. The first position might be correctly guessed by the attacker by analyzing the request signal. The second position, however, is assumed to be unknown to the attacker. This lack of knowledge prevents location spoofing attacks because the verification is based on the *time difference of arrival* at the different base stations. In order to manipulate the verification, the attacker would have to exactly schedule the response sending times in order to mimic the times of arrival at the different base stations of a legitimate claimer. This would only be possible if the attacker knew the base stations' locations.

Both approaches use mobility *indirectly* in the sense that they employ the mobility of nodes to first establish conditions in the network which then allow for the respective protocols to run securely. Our approach differs by measuring and verifying a direct effect of mobility: the changes in distances between nodes. This way, we are able to design location verification protocols which are secure even when facing an attacker knowing all verifiers' positions. Moreover, we find that these effects can be measured without a need for time synchronization between verifiers. This results in the relaxation of system requirements as mentioned above.

3. MOBILITY-DIFFERENTIATED TOA

Our system consists of a set of verifiers and a prover. The prover broadcasts its position claim periodically with a fixed transmission interval Δ. The verifiers measure the interarrival time $\Delta_{i,j}^{v}$ of received claims. We assume that there is no compromised verifier and that verifiers are able to exchange information securely. We further assume that either a nonempty subset of the verifiers, or the prover, or both are moving during the verification process.

WiSec '15 June 22-26 2015, New York, USA
Copyright is held by the owner/author(s)
ACM 978-1-4503-3623-9/15/06.
http://dx.doi.org/10.1145/2766498.2774988

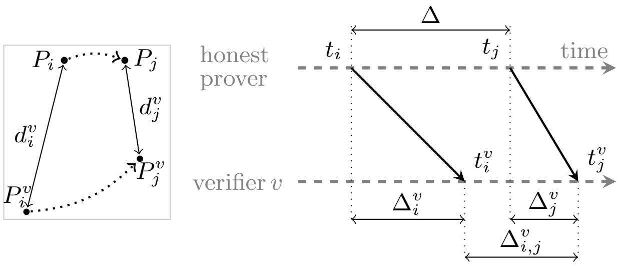

Figure 1: System model. An honest (possibly mobile) prover is broadcasting its position every Δ seconds. Two consecutive claims for positions P_i and P_j are received by a moving verifier v with an interarrival time $\Delta_{i,j}^v$ which differs from Δ by the difference in propagation delays $\Delta_j^v - \Delta_i^v$.

By considering the difference between Δ and $\Delta_{i,j}^v$, that is

$$\Delta - \Delta_{i,j}^v = (t_j - t_i) - (t_j^v - t_i^v) = \Delta_i^v - \Delta_j^v ,$$

we obtain the so called *mobility-differentiated time of arrival* (MDToA). This metric has been first used by Luo et al. [4] to realize a passive self-positioning scheme. Recently, Schäfer et al. [1] proposed to exploit MDToA in the context of secure track verification. The MDToA has the practical advantage that it can be measured without a need for time synchronization or additional communication since only node-local periods and the known fixed transmission interval are used.

It is worth noting that our assumptions generalize the assumptions made in [1]. Another slight difference is that instead of using a fixed transmission interval Δ, [1] broadcast a prover-local time stamp with each location claim to determine the MDToA. Nevertheless, the MDToA can be obtained using both methods. Hence, our results also hold for their track verification scheme. In addition, however, our scheme also allows for *location* verification: the prover is not required to move as long as some of the verifiers are moving.

3.1 Location Verification

The basic idea for our scheme is that verifiers compare the expected MDToA with the measured one (cf. [1]). Each verifier can derive the expected MDToA based on local knowledge (its current and previous positions) and the received location claims. A spoofing attack is detected if at least one verifier detects a deviation.

3.2 Attacker Model

To assess the security of MDToA-based schemes, we consider a mobile and clairvoyant attacker. We assume that the attacker is able to position itself at any location at any point in time. We also assume that the attacker knows all positions of all nodes at all times. In particular, it knows the exact positions of the verifiers at the reception of its location claims already when sending those claims.

As all location verification schemes are based on ToA measurements, MDToA-based schemes are not secure in the presence of a Dolev-Yao attacker. In particular, distributed attackers or attackers sending independent signals to each verifier (e.g. with directional antennas) can choose the time of arrivals arbitrarily; such attackers could spoof any combination of MDToAs at the verifiers including the expected one. Accordingly, we exclude the case of a Dolev-Yao attacker.

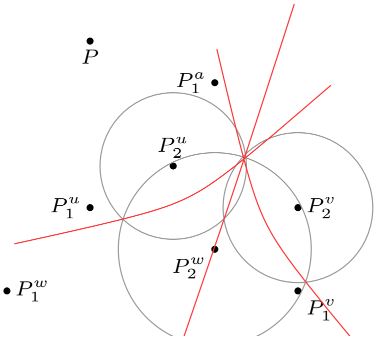

Figure 2: An attacker tries to spoof location P starting at position P_1^a. It sends two location claims to three verifiers u, v, and w. Between the reception of the claims, the verifiers move from $P_1^{u/v/w}$ to $P_2^{u/v/w}$. This way, the attacker's second position is constrained to the red lines' intersection.

The attacker's goal is to claim at least one false location, that is, it claims P while it is at $P^a \neq P$.

3.3 Security

Our preliminary findings suggest that by using a sufficient number of verifiers, any location or track verification scheme based on the MDToA becomes secure. Moreover, the number of verifiers can be reduced in many cases. For instance, if the verifiers avoid certain unfavorable movement patterns, the location verification scheme can be secure with just three verifiers (in two dimensions). Our goal is thus to derive constraints on positioning and timing of attackers and verifiers. An example of such constraints is shown in Figure 2.

4. CONCLUSION

This poster describes how security can benefit from mobility. In particular, we present our preliminary security analysis of MDToA-based location verification schemes. Due to the natural assumption of mobility and its lightweight system requirements, we believe that our insights can bring practical improvements to existing verification schemes.

5. REFERENCES

[1] Matthias Schäfer, Vincent Lenders, and Jens B. Schmitt. Secure track verification. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, May 2015.

[2] Srdjan Čapkun, Jean-Pierre Hubaux, and Levente Buttyán. Mobility helps security in ad hoc networks. In *Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, pages 46–56, 2003.

[3] Srdjan Čapkun, Kasper Rasmussen, Mario Čagalj, and Mani Srivastava. Secure location verification with hidden and mobile base stations. *IEEE Transactions on Mobile Computing*, 7(4):470–483, April 2008.

[4] Jun Luo, Hersh V. Shukla, and Jean-Pierre Hubaux. Non-interactive location surveying for sensor networks with mobility-differentiated toa. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, pages 1–12, April 2006.