POSTER: Privacy Preservation through Uniformity

Mohammad Khodaei
Networked Systems Security Group
KTH, Stockholm, Sweden
khodaei@kth.se

Hamid Noroozi
Networked Systems Security Group
KTH, Stockholm, Sweden
hnoroozi@kth.se

Panos Papadimitratos
Networked Systems Security Group
KTH, Stockholm, Sweden
papadim@kth.se

ABSTRACT

Inter-vehicle communications disclose rich information about vehicle whereabouts. Pseudonymous authentication secures communication while enhancing user privacy thanks to a set of anonymized certificates, termed *pseudonyms*. Vehicles switch the pseudonyms (and the corresponding private key) frequently; we term this *pseudonym transition* process. However, exactly because vehicles can in principle change their pseudonyms asynchronously, an adversary that eavesdrops (pseudonymously) signed messages, could link pseudonyms based on the times of pseudonym transition processes. In this poster, we show how one can link pseudonyms of a given vehicle by simply looking at the timing information of pseudonym transition processes. We also propose *"mix-zone everywhere"*: time-aligned pseudonyms are issued for all vehicles to facilitate *synchronous* pseudonym update; as a result, all vehicles update their pseudonyms simultaneously, thus achieving higher user privacy protection.

KEYWORDS

VC, VPKI, Security, Privacy, Pseudonym Transition, Linkability

1 INTRODUCTION

In Vehicular Communication (VC) systems, vehicles disseminate spatio-temporal information frequently, e.g., location and velocity. In order to ensure message integrity, authenticity, and maintaining non-repudiation while preserving user privacy, pseudonymous authentication was proposed: each vehicle is provided with a set of short-lived anonymous certificates, termed *pseudonyms*, and it switches from one pseudonym to another to protect user privacy.

Due to the openness of the wireless communication, an observer could eavesdrop VC, towards inferring user-sensitive information. Even though pseudonymous authentication is a promising approach, an adversary, eavesdropping all traffic in an area, could link successive pseudonymously authenticated messages; more precisely, an attacker could link successive Cooperative Awareness Messages (CAMs) by attempting to *synthetically* link the corresponding pseudonym with the same identifier, or *semantically* link the message using for example time, location, and velocity [1, 15].

There are different strategies for *pseudonym change*, i.e., how to change from the currently used (or expired) pseudonym to a new one. Cooperative pseudonym updates, e.g., mix-zone based schemes [4, 11], suggest changing pseudonyms at appropriate times and places, e.g., at intersections. However, such schemes could enhance user privacy if the region is unobservable by an adversary. Moreover, some of these approaches could significantly affect the operation of safety applications, e.g., when being silent near an intersection [1, 3]; thus, their practicality may be questioned. Beyond these approaches, an *honest-but-curious* Vehicular Public-Key Infrastructure (VPKI) entity (in collusion with vehicle communication observers) could simply link the pseudonyms and correlate to the actual identity of a vehicle [10].[1]

The common denominator among the majority of the proposals in the literature [13] is that vehicles change their pseudonyms asynchronously, e.g., changing pseudonym every 5 minutes [14]. This could enable an adversary, who eavesdrops the communication, to link two successive pseudonyms belonging to a given vehicle [6--9]. In this poster, we show how one can link pseudonyms, and thus pseudonymously signed messages, only based on the timing of pseudonym changes[2].

2 TRACKING APPROACH

Adversarial model: We extend the general adversary model in secure vehicular communications [12] to include VPKI entities that are *honest-but-curious*, i.e., entities complying with security protocols and policies but motivated to profile users. We assume a passive adversary that can receive all CAMs. Deploying a global passive adversary with unlimited coverage is not practical, thus we assume a more practical set up: Roadside Units (RSUs), as *honest-but-curious* system entities, capture messages within their coverage range and aggregate the information. RSUs could be deployed by other authorities than the VPKI ones; thus, they might be tempted to infer sensitive information.

Timing inference attack: An adversary frequently captures pseudonym serial numbers from the received beacons every system parameter τ, e.g., $\tau = 1$ sec. A matrix A is also created where $A[x, y] = A[y, x]$ is the probability of pseudonym x and pseudonym y belonging to the same vehicle's pseudonym pool. By comparing the pseudonym serial numbers at subsequent time snapshots, e.g., τ^i with τ^{i+1}, the attacker can draw a probabilistic conclusion regarding which pseudonyms could be related to each other. He could also draw a deterministic conclusion on which pseudonyms do not belong to a vehicle's pseudonym pool, i.e., for each pseudonym at time snapshot τ^i, there exists exactly one *distinct* vehicle broadcasting a CAM, signed under a private key corresponding to the aforementioned pseudonym. Simply put, if there are N pseudonyms at time snapshot τ^i, they belong to N distinct vehicles.

Fig 1 shows an example of the pseudonym change process from the perspective of a passive adversary. At τ^0, pseudonym E and at τ^1 pseudonyms E and C appeared. This means E and C do not belong to the same vehicle. At τ^2, pseudonyms C, G, and H appeared. The deterministic conclusion is that C, G, and H belong to different, distinct vehicles. The probabilistic conclusion is that E might be linked either to G or H, or none (i.e., E left the VC system).

[1]Note that connecting such anonymous location profiles to real identities of vehicle owners is the final step, e.g., tracing their commutes and identify home/work locations [5], or full de-anonymization of vehicles by honest-but-curious VPKI entities.
[2]Note that we only rely on the times of pseudonym changes to link pseudonyms.

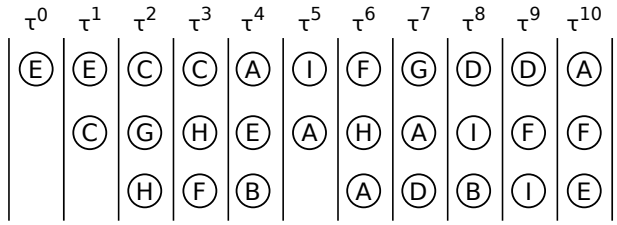

Figure 1: Pseudonym transition (an adversary's viewpoint).

The matrix A would be augmented whenever a new pseudonym is observed, and the relations are updated. For example, considering τ^1 and τ^2, the deterministic conclusion yields A[E,C] = A[C,G] = A[C,H] = A[G,H] = 0, which never be updated during the course of analysis. The probabilistic conclusion results in A[E,G] = A[E,H] = $\frac{1}{3}$. We propose a conventional method to increase the weight of a link, by accumulating the probabilities over time snapshots. Note that a probabilistic conclusion is calculated only considering two consecutive snapshots. For instance, at τ^3 and τ^4, the probability of E being linked to H is $\frac{1}{4}$, thus $A[E, H] = \frac{1}{3} + \frac{1}{4}$.

To identify potential linking solutions, we propose a heuristic method to perform an analysis: the matrix A is traversed to find the absolute maximum value. Multiple maximum values lead to multiple solutions. The scheme uses the maximum value as part of the solution and suggests that its indices (are pseudonyms which) belong to the same vehicle. We then traverse the column where the maximum value was found; the scheme suggests that the next maximum value is related to the previously found link. We continue traversing the column until we hit the maximum number of pseudonyms per vehicle.[3] Having removed the previously linked nodes, our scheme continues its traversal for the next linking sets.

To enhance our tracking algorithm, we introduce another metric with respect to the distance between RSUs. More precisely, two pseudonyms are more likely to be linked to each other if they are captured by the same RSU or two adjacent RSUs. Note that a key assumption for our scheme is pseudonym re-usability, which stems from a practical set up, e.g., each vehicle has 20 pseudonyms per week and randomly switches among those every 5 minute [14].

3 EVALUATION

We use a microscopic vehicle mobility datasets, the LuST [2] and we provide each vehicle with 10 pseudonyms and each vehicle switches from one pseudonym to another every 1 minute.[4] We use OMNET++ (www.omnetpp.org) and the Veins framework to simulate this large-scale scenario using SUMO. In our simulation, we placed 100 RSUs in a region (50KM × 50KM) and Vehicle-to-Infrastructure (V2I) communication is IEEE 802.11p.

4 MITIGATION

To mitigate timing-based inferences based on pseudonym changes, we propose that all vehicles be issued with universally common pseudonym lifetime [6--8], i.e., the anonymity set becomes equal to the number of active vehicles in a region. Thus, we achieve the highest level of privacy as the anonymity set is equal to all vehicles. We also show that even a single honest-but-curious VPKI entity cannot link pseudonyms by accessing eavesdropped messages.

5 CONCLUSION AND FUTURE WORK

In this poster, we show how the pseudonym changing processes could harm user privacy through the inference of timing information. As future work, we plan to systematically investigate pseudonym linkability for other pseudonym transition strategies and evaluate the achieved level of privacy protection in comparison with our scheme.

ACKNOWLEDGEMENT

This work has been partially supported by the Swedish Foundation for Strategic Research (SSF).

REFERENCES

[1] L. Buttyán and et al. 2009. SLOW: A Practical Pseudonym Changing Scheme for Location Privacy in VANETs. In *IEEE VNC*. 1--8.
[2] L. Codeca and et al. 2015. Luxembourg SUMO Traffic (LuST) Scenario: 24 Hours of Mobility for Vehicular Networking Research. In *IEEE VNC*. Kyoto, Japan.
[3] S. Eichler. 2007. Strategies for Pseudonym Changes in Vehicular Ad Hoc Networks Depending on Node Mobility. In *IEEE Intelligent Vehicles Symposium*. 541--546.
[4] J. Freudiger and et al. 2007. Mix-zones for Location Privacy in Vehicular Networks. In *Win-ITS*. Vancouver, BC, Canada.
[5] P. Golle and K. Partridge. 2009. On the Anonymity of Home/Work Location Pairs. In *Pervasive computing*. Springer, 390--397.
[6] M. Khodaei and et al. 2016. Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems. In *IoV/VoI*. Paderborn, Germany.
[7] M. Khodaei and et al. 2018. SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems. *IEEE Transactions on Intelligent Transportation Systems* 19, 5 (May 2018), 1430--1444.
[8] M. Khodaei, H. Jin, and P. Papadimitratos. 2014. Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure. In *IEEE VNC*. Paderborn, Germany.
[9] M. Khodaei, A. Messing, and P. Papadimitratos. 2017. RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd. In *IEEE VNC*. Torino, Italy.
[10] M. Khodaei and P. Papadimitratos. 2015. The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems. *IEEE VT Magazine* 10, 4 (Dec. 2015), 63--69.
[11] R. Lu and et al. 2012. Pseudonym Changing at Social Spots: An Effective Strategy for Location privacy in VANETs. *IEEE TVT* 61, 1 (Jan 2012), 86--96.
[12] P. Papadimitratos and et al. 2006. Securing Vehicular Communications-Assumptions, Requirements, and Principles. In *ESCAR*. Berlin, Germany.
[13] J. Petit and et al. 2015. Pseudonym Schemes in Vehicular Networks: A Survey. *IEEE communications surveys & tutorials* 17, 1 (Mar. 2015), 228--255.
[14] W. Whyte, A Weimerskirch, V. Kumar, and T. Hehn. 2013. A Security Credential Management System for V2V Communications. In *IEEE VNC*. Boston, MA.
[15] B. Wiedersheim and e al. 2010. Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change is not Enough. In *IEEE WONS*.

[3]The exact number of pseudonyms per vehicle could be helpful to an adversary.
[4]Note that pseudonym transition every 1 minute seems not to be practical. However, since the average trip duration for this dataset is around 10 minutes, we chose it to be short. As future work, we plan to evaluate our scheme with a more practical setup.