Demo: Efficient and Timely Revocation of V2X Credentials

Gianluca Scopelliti*†, Christoph Baumann*, Fritz Alder†, Eddy Truyen†, Jan Tobias Mühlberg‡†
*Ericsson Security Research, Sweden; †DistriNet, KU Leuven, Belgium; ‡Université Libre de Bruxelles, Belgium
gianluca.scopelliti@ericsson.com

***Abstract*—We present an interactive visual demo of our novel revocation scheme for V2X credentials, which is the first to guarantee an upper bound on revocation time in the presence of strong network attackers. The demo allows users to inspect the network state with a number virtual vehicles, attackers, and events such as network delays and service disruption.**

I. Introduction

State-of-the-art credential management systems for Vehicle-to-Everything (V2X) proposed in industry standards leverage *pseudonymous* identities to protect the privacy of vehicles and their passengers [1], [2]. However, as highlighted by recent surveys [4], [5], such systems present several limitations with respect to *revocation*, i.e., the capability to punish malicious or misbehaving actors after misbehavior connected to a participant's pseudonym is detected. To address these challenges, we have designed a novel revocation scheme based on self-revocation [3]. Our scheme provides a formally-verified design that guarantees an upper bound on revocation time and ensures scalability even with a large numbers of vehicles and attackers in the network. In this interactive demo, we present a proof-of-concept implementation of our scheme applied to a simulated V2X scenario.

II. Scheme Overview

In a typical V2X scenario [1], [2], vehicles exchange information with each other to provide functionalities such as collision avoidance or assisted/autonomous driving. These messages are authenticated using pseudonymous credentials (*pseudonyms* in short), which are issued by the V2X infrastructure to vehicles upon successful authentication and authorization, and are rotated periodically to prevent long-term tracking of vehicles. Misbehaviour detection mechanisms are employed to detect and report misbehaving pseudonyms, which are then *revoked* to preserve road safety.

In our revocation scheme [3], a Revocation Authority (RA) is responsible for distributing periodic messages called heartbeats (HBs). Such messages have a two-fold purpose: First, they carry timing information that is used by vehicles to obtain a common notion of time, which can then provide freshness information to network messages. Second, HBs contain a list of pseudonyms to be revoked. Vehicles receiving a HB first synchronize their local notion of time with the one included in the message, and then check if any of their pseudonyms is included in the HB. If so, they perform *self-revocation* of their credentials. In case malicious vehicles attempt to avert revocation, e.g., by dropping HBs, they will eventually become unable to communicate because their local time will not advance beyond the last HB received. To make this scheme work, we require a Trusted Component (TC) in each vehicle. This TC is responsible for the management of credentials.

III. Demo Description & Conclusions

We have developed a proof-of-concept implementation of our scheme in a simulated V2X scenario running on Kubernetes. The demo consists of a number of virtual vehicles that exchange messages with each other on a small edge area. Attackers in the network can spread malicious information, affecting nearby vehicles. The demo also simulates a number of real-world events such as network delays and interruptions. The code is open source and available on Github[1].

The demo is made interactive by means of a web application where users, who play the role of a system administrator, can monitor the state of the network and trigger revocation requests. The application shows the state of the simulation at each time step (i.e., each second), and users can go back and forth in time to inspect the state of the network. The application also shows the content of HB messages sent by the RA, as well as revocation times for pseudonyms.

This proof-of-concept demo shows the effectiveness of our revocation scheme in a simulated but realistic V2X scenario.

References

[1] B. Brecht, D. Therriault, A. Weimerskirch, W. Whyte, V. Kumar, T. Hehn, and R. Goudy, "A Security Credential Management System for V2X Communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3850–3871, 2018.

[2] ETSI, "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management," European Telecommunications Standard Institute (ETSI), Technical Specification (TS) TS 102 941, 11 2022, version 2.2.1.

[3] G. Scopelliti, C. Baumann, F. Alder, E. Truyen, and J. T. Mühlberg, "Efficient and timely revocation of v2x credentials," in *Proceedings of the 2024 Network and Distributed System Security (NDSS) Symposium*, ser. NDSS'24. Internet Society, 2024.

[4] Q. Wang, D. Gao, and D. Chen, "Certificate Revocation Schemes in Vehicular Networks: A Survey," *IEEE Access*, vol. 8, pp. 26 223–26 234, 2020.

[5] T. Yoshizawa, D. Singelée, J. T. Mühlberg, S. Delbruel, A. Taherkordi, D. Hughes, and B. Preneel, "A Survey of Security and Privacy Issues in V2X Communication Systems," *ACM Comp. Surv.*, Aug. 2022.

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.25002
www.ndss-symposium.org

[1] https://github.com/EricssonResearch/v2x-self-revocation