Token-Based Vehicular Security System (TVSS): Scalable, Secure, Low-Latency Public Key Infrastructure For Connected Vehicles

Tech ID: 33613 / UC Case 2023-9AH-0

FULL DESCRIPTION

Background

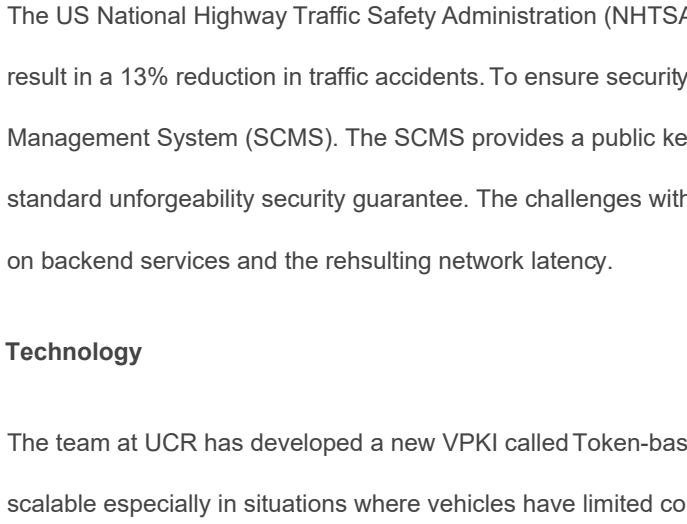
The US National Highway Traffic Safety Administration (NHTSA) estimates that vehicle-to-vehicle (V2V) communication, if implemented can result in a 13% reduction in traffic accidents. To ensure security, the US Department of Transportation adopted the Secure Certificate Management System (SCMS). The SCMS provides a public key infrastructure (PKI) for vehicles to authenticate themselves which promises a standard unforgeability security guarantee. The challenges with existing vehicular public key infrastructure (VPKI) designs is the heavy reliance on backend services and the rehsulting network latency.

Technology

The team at UCR has developed a new VPKI called Token-based Vehicular Security System (TVSS) that is designed to be more efficient and scalable especially in situations where vehicles have limited connection time to roadside units (RSUs). The way TVSS works is:

- Token Generation - Vehicles obtain a batch of tokens from the Certificate Authority (CA). Each token is valid only for a short period of time. The tokens are used to anonymously request pseudonym certificates (PCs) from RSUs.
- PC Provisioning - When a vehicle needs a new PC, it presents a token to the RSU. The RSU verifies the token for validity before issuing a PC to the vehicle. The PC is only valid for a specific geographic region and time window.
- Revocation - If a vehicle misbehaves, the system can revoke its credentials and revoked tokens and PCs are distributed to the relevant RSUs and vehicles in the area.

Images



Overview of the all the protocols of TVSS

CONTACT

Venkata S. Krishnamurty
venkata.krishnamurty@ucr.edu
tel: .

OTHER INFORMATION

KEYWORDS

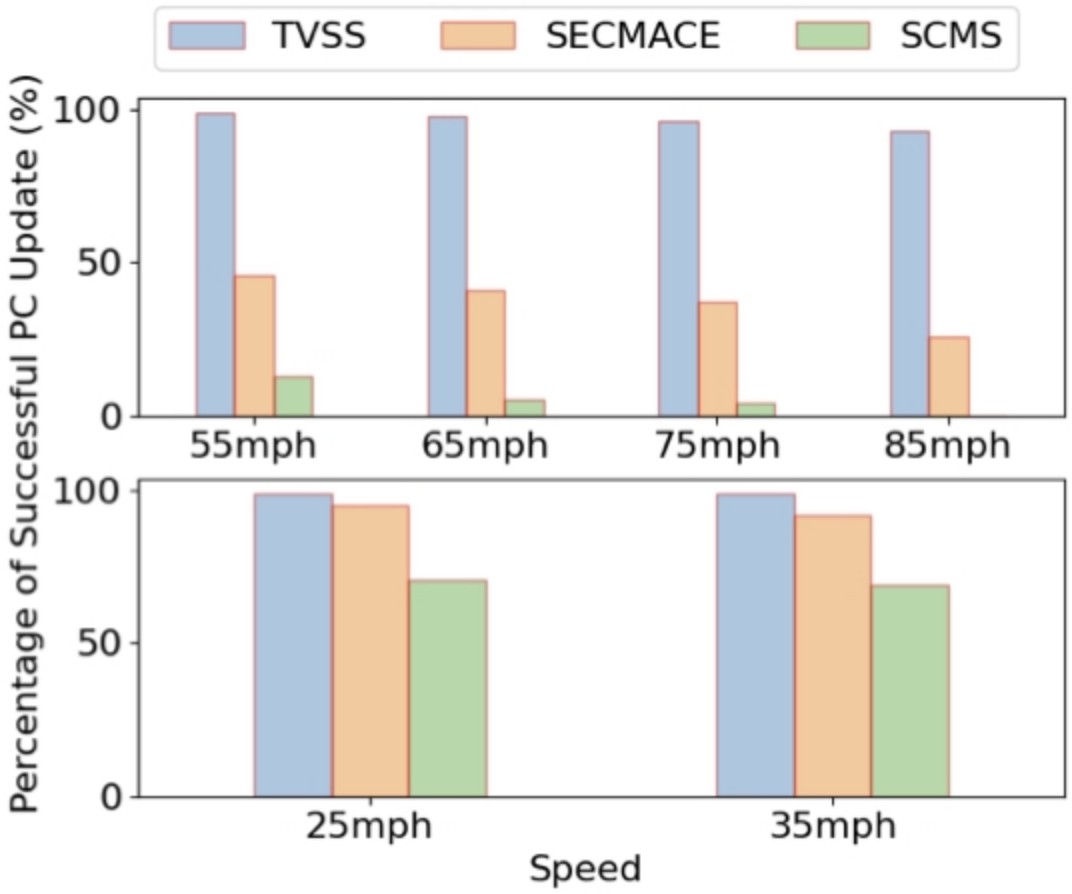
vehicular public key infrastructure, VPKI, IoT, vehicular networks, security, privacy, edge computing, connected vehicles, V2X, dsrc

CATEGORIZED AS

- **Communications**
  - Internet
  - Wireless
- **Computer**
  - Security
- **Security and Defense**
  - Cyber security
- **Transportation**
  - Automotive

RELATED CASES

2023-9AH-0



Comparison of the success ratio of vehicles refreshing a PC - via all VPKIs.

ADVANTAGES

Low latency PC generation - Since TVSS pushes the PC generation to the RSU, it significantly reduces latency. This is specially important in scenarios where vehicles have short connection times with RSUs such as at highway speeds.

Efficient revocation - TVSS uses a localized revocation which significantly reduces the amount of data that needs to be communicated. This localized mechanism provides a 13X reduction in total communication size compared to other systems.

Enhanced privacy - TVSS uses short-lived tokens and localized PCs which enhances privacy by limiting the window for potential vehicle tracking. Additionally, tracking a vehicle's movement over a longer period becomes more difficult.

Simplified Architecture - By moving the computational burden to the edge, i.e., the RSU, TVSS simplifies the system architecture thereby reducing costs without compromising security.

APPLICATIONS

- Smart infrastructure
- Connected vehicles - vehicle to everything (V2X)

STATE OF DEVELOPMENT

The prototype system has been built and tested. The architecture and its capabilities have been tested and demonstrated in field experiments.

RELATED MATERIALS

- Token-based Vehicular Security System (TVSS): Scalable, Secure, Low-latency Public Key Infrastructure for Connected Vehicles

PATENT STATUS

Patent Pending

200 University Office Building,

Riverside,CA 92521

otc@ucr.edu

research.ucr.edu/