Projeto de Formatura – Turmas 2018

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema:

Mecanismos para emissão de certificados com privacidade em redes veiculares

MOTIVAÇÃO

Ao longo das últimas décadas, temos observado o avanço no desenvolvimento de carros inteligentes e autônomos. Para que esses veículos possam melhorar a segurança em rodovias, é necessária a comunicação entre dispositivos, através da troca de mensagens básicas de segurança.

As mensagens enviadas devem ser assinadas para garantir autenticidade e irretratabilidade ao usuário. No entanto, utilizar um único certificado permitiria o rastreio do veículo. Devem ser utilizados pseudônimos, além de outros mecanismos, para garantir a **privacidade** do veículo. Dentre os estudos recentes, a solução *Security Credential Management System* (SCMS) [1] é a principal candidata à padronização nos Estados Unidos e destaca-se pelo foco dado à privacidade e eficiência no processo de emissão de certificados.

OBJETIVO E ESPECIFICAÇÃO

O objetivo deste trabalho é analisar a adequabilidade do sistema SCMS e demonstrar as vantagens oferecidas pelo modelo através de um protótipo. O protótipo desenvolvido possui três modos de operação, que permitem visualizar a importância de cada procedimento realizado pelo SCMS.

- **1º modo de operação:** Apresenta-se um modelo de emissão de certificados tradicional, sem privacidade, no qual a entidade emissora sabe a quem se destina o certificado. Entidades: veículo e *Pseudonym Certificate Authority* (PCA).
- **2º modo de operação:** O sistema SCMS é aplicado parcialmente e garante-se a privacidade do usuário, mas alguns mecanismos de otimização de desempenho não são utilizados. A garantia de privacidade é feita através da clara divisão entre as entidades, de forma que nenhuma possua informações o suficiente sobre o veículo para rastreá-lo. Entidades: o veículo, PCA e *Registration Authority* (RA).
- **3º modo de operação:** Representa o sistema SCMS completo, com eficiência na emissão de certificados. Uma única requisição do veículo dá origem a *N* certificados, todos com garantia de privacidade. Entidades: o veículo, PCA, RA e duas instâncias da *Linkage Authority* (LA).

O protótipo foi desenvolvido em Python e foi feita a interface com a biblioteca criptográfica RELIC Toolkit [2], escrita em C. A exibição dos dados é feita através de uma interface Web. Cada entidade deu origem a um sistema isolado, com seu próprio banco de dados.

OPERAÇÕES DO SISTEMA SCMS

Dentre as operações realizadas no sistema SCMS, destaca-se:

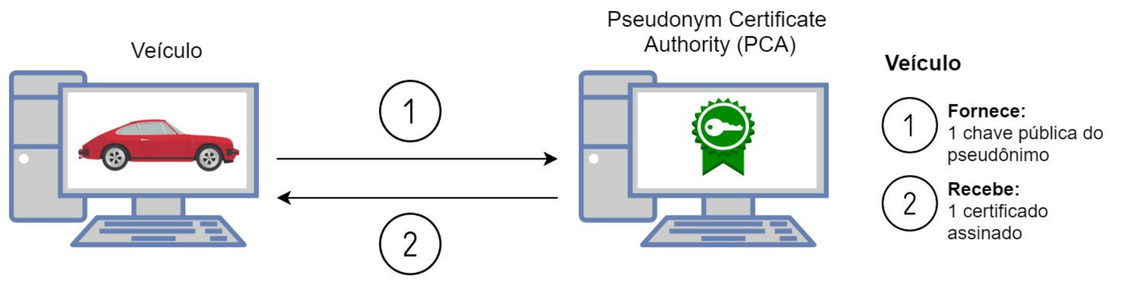
- Expansão de chaves borboletas
- Encadeamento de certificados

Integrante: Giuliana Baratto Barone

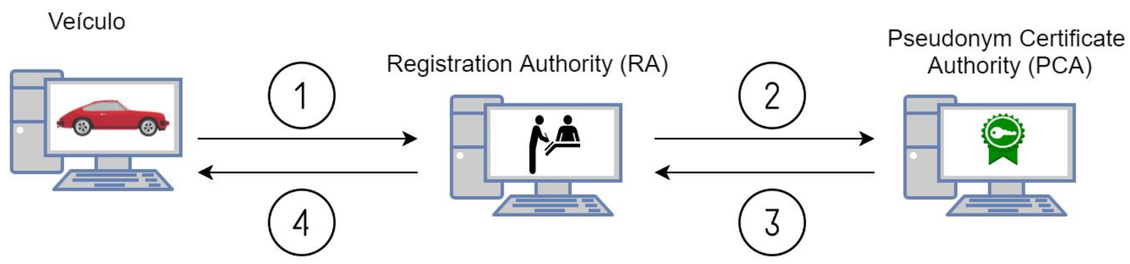
Professor Orientador: Prof. Dr. Marcos Antonio Simplicio Junior

ARQUITETURA DO PROTÓTIPO

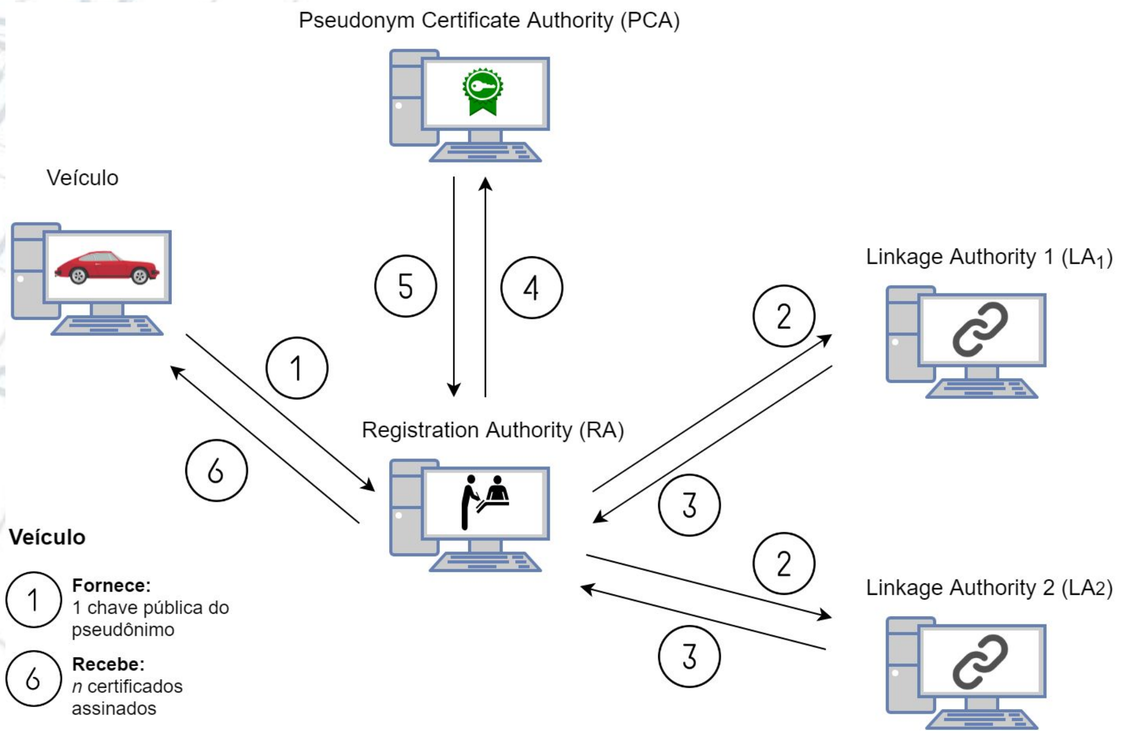
- 1º modo de operação:



- 2º modo de operação:



- 3º modo de operação:



CONCLUSÕES

- No 1º modo de operação, observa-se a completa falta de privacidade do usuário. Este problema é resolvido no 2º modo de operação, com a inserção da entidade RA.
- No 2º modo de operação, o custo para obter um lote de certificados é alto, já que cada certificado representa uma requisição à RA. Este problema é resolvido no 3º modo de operação, com a expansão de chaves borboletas. A obtenção de *N* certificados com uma única requisição diminuiu o processamento no veículo, que é um dispositivo com menor poder computacional. Melhora-se assim a eficiência do sistema como um todo.

REFERÊNCIAS

[1] William Whyte, André Weimerskirch, Virendra Kumar, and Thorsten Hehn. A security credential management system for V2V communications. *InVehicular Networking Conference (VNC), 2013 IEEE*, pages 1–8. IEEE, 2013

[2] D. F. Aranha and C. P. L. Gouvêa. RELIC is an Efficient LIbrary for Cryptography. *https://github.com/relic-toolkit/relic*.