Mini-MAC: Raising the Bar for Vehicular Security with a Lightweght Message Authentication Protocol

Jackson Schmandt,[1] Alan T. Sherman,[2] Nilanjan Banerjee[1]
CSEE Department, University of Maryland, Baltimore County (UMBC)
{schmandt, sherman, nilanb}@umbc.edu

February 6, 2016

Abstract

We propose Mini-MAC, a new message authentication protocol that works in existing automotive computer networks without delaying any message or increasing network traffic.

Deployed in many vehicles, the CAN bus is a low-speed network connecting electronic control units, including those that control critical functionality such as braking and acceleration. The CAN bus is extremely vulnerable to malicious actors with bus access, including wireless access. Traditionally, Message Authentication Codes (MACs) help authenticate the sender of a message, and variants prevent message replay attacks; however, standard MACs are unsuitable for use on the CAN bus because of small payload sizes. Restrictions of the CAN bus, including the need not to delay messages or increase bus traffic, severely limit how well this network can be protected.

Mini-MAC is based on a counter-seeded keyed-Hash MAC (HMAC), augmented with message history and truncated to fit available message space. It does not increase bus traffic and incurs a very small performance penalty relative to the provably secure HMAC. It is the first proposal to combine these two tenets for vehicle networks. The message history feature protects against all transient attackers, even if they know the keys. Though the CAN bus cannot be properly secured against a dedicated attacker, Mini-MAC meaningfully raises the bar of vehicular security, enhancing the safety of drivers and others.

Index terms— CAN bus, automotive security, message authentication code, Mini-MAC, vehicle security, applied cryptography.

1 Introduction

At the 2015 Black Hat conference, Miller and Valasek [MV15] gained full control of a new Jeep, including its engine, brakes, and steering, by exploiting vulnerabilities in its computer network and Wi-Fi implementation and by rewriting firmware on a controller connected to the car's entertainment system. This demonstration, and other similar projects [RMM+10, KCR+10, CMK+11, WJL15, FBZ+08], highlight the egregious state of vehicular security, including the lack of authentication of messages sent on the Controller Area Network (CAN).

To strengthen vehicular security in a simple and practical yet meaningful way—without replacing the CAN bus—we propose Mini-MAC, a new variable-length Message Authentication Code (MAC) for the CAN bus that works with small payload sizes without delaying messages. Built on the provably-secure HMAC, Mini-MAC protects against masquerade attacks. Mini-MAC also incorporates a counter and message history to protect against replay attacks; the message history feature protects against all transient attackers (attackers who can access the CAN bus

[1] Mobile Pervasive Sensor System Lab
[2] Cyber Defense Lab