ATIS-I-0000059

Improving Vehicle Cybersecurity

ICT Industry Experience & Perspectives

Abstract

This whitepaper addresses how the Information and Communication Technology (ICT) industry can share lessons learned to assist the vehicle Original Equipment Manufacturers (OEMs) with improving vehicle cyber security, and how the ICT industry and vehicle OEMs can benefit from working together.

Foreword

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-Internet Protocol (IP) transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer and Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Contents

1. Introduction

The age of connected and self-driving vehicles is bringing unprecedented new innovations and options to transportation and to other sectors. The greatest risks to this exciting future are those posed by cyber intrusion to the vehicle, and if left unaddressed, these threats have the potential to eclipse the bright future inherent in these innovations. The dangers range from access to the owner's, driver's, or passenger's personal and financial information to outright loss of physical control of the connected vehicle.

The Information and Communication Technology (ICT) industry has extensive experience with cybersecurity and is actively working to continually enhance security in its networks and devices. And because of how central the ICT industry is to the "connected world," it is able to offer cyber intrusion detection and prevention functionality to and across many industries and sectors. With the advent of the connected vehicle, the network reaches into new frontiers as it provides the connectivity for advanced applications and data collection. Yet, until now, the ICT industry and automobile original equipment manufacturers (OEMs) have engaged in limited industry-to-industry dialog regarding how to best address and plan for connected vehicle cybersecurity.

The Alliance for Telecommunications Industry Solutions (ATIS) believes that through collaboration, including the sharing of best practices and lessons learned, that the ICT and vehicle OEMs will be able to mitigate the risk of cyber intrusion in the connected vehicle. This is why ATIS identified the need for and began working toward the opportunity of a consistent and coordinated approach to most effectively share the ICT industry's technical knowledge, experience, and perspectives with the automobile OEMs. This dialog and collaborative work will contribute to increased road safety, improved reliability of connected vehicles, enhanced customer experience, and many other benefits to both industries.

ATIS' diverse membership represents the ICT ecosystem – from telecommunications network providers, to equipment and software