IGI PUBLISHING

ITJ 4723

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

This paper appears in the publication, International Journal of Digital Crime and Forensics, Volume 1, Issue 2
edited by **Chang-Tsun Li © 2009, IGI Global**

Conducting Forensic Investigations of Cyber Attacks on Automobile In-Vehicle Networks

Dennis K. Nilsson, Chalmers University of Technology, Sweden

Ulf E. Larson, Chalmers University of Technology, Sweden

ABSTRACT

The introduction of a wireless gateway as an entry point to the automobile in-vehicle network reduces the effort of performing diagnostics and firmware updates considerably. Unfortunately, the same gateway also allows cyber attacks to target the unprotected network which currently lacks proper means for detecting and investigating security-related events. In this article, we discuss how to perform a digital forensic investigation of an in-vehicle network. An analysis of the current features of the network is performed, and an attacker model is developed. Based on the attacker model and a set of generally accepted forensic investigation principles, we derive a list of requirements for detection, data collection, and event reconstruction. We then use the Integrated Digital Investigation Process proposed by Carrier and Spafford (2004) as a template to illustrate how our derived requirements affect an investigation. For each phase of the process, we show the benefits of meeting the requirements and the implications of not complying with them. [Article copies are available for purchase from InfoSci-on-Demand.com]

Keywords: *Automobile; Cyber Attacks; Forensics; In-Vehicle Networks; Investigation*

INTRODUCTION

Automobile in-vehicle networks have historically been isolated from attackers as a result of the limited access possibilities. However, due to recent advances in wireless communications combined with a huge economical incentive for the vehicle industry in accessing and updating vehicle firmware over the air, this situation is about to change. The fact that the wireless technology for updating and diagnosing firmware has already been successfully used for several years within the telecommunications industry also indicates that it is possible to adapt it to other areas, including the automotive domain.

The enabling factor is the introduction of a wireless gateway as an entry point to the in-vehicle network, which consists of a set of

Copyright © 2009, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

electronic control units (ECUs). The gateway allows for remote interaction with ECU firmware, even when the vehicle is running. Common administrative functions such as diagnostics and firmware updates could be performed remotely. Thus, vehicle owners do not need to drive to a service station to get their car diagnosed, and new firmware updates can easily be applied to thousands of vehicles simultaneously. Thus, faulty firmware can be diagnosed and replaced faster, and safer vehicle operation can be achieved. Additionally, as discussed by Shavit et al. (2007), the need for costly vehicle recalls is removed since physically interfacing each vehicle through the *on-board diagnostics* (OBD) module is no longer required. Furthermore, as discussed by Moustafa et al. (2006), vehicle-to-vehicle and vehicle-to-infrastructure communication allows vehicles to receive alerts of changing weather conditions and to obtain area information from roadside stations.

However, the new technology also introduces new safety and security issues for the manufacturers to consider. Allowing communication between the unprotected in-vehicle network and one or more external entities introduces a whole new range of threats collectively known as *cyber attacks*. An attacker could, for example, use the firmware update function to inject malicious code into the in-vehicle network while the vehicle is running.

As an illustration, consider a speeding vehicle that drives off a road and crashes with fatal consequences for the driver. This type of incident is normally caused either by the driver himself, or by vehicle malfunction or physical tampering. If the brake line is found to be cut, the cause of the accident is most certainly an act of physical tampering, and a criminal investigation needs to be initiated to bring those responsible to a court of law. Now, consider instead the possibility that the brakes were disabled by a piece of malicious code. If there is no digital evidence available, there would be no means of revealing that a crime was committed, the criminal would walk free, and the cause of the accident would wrongly be determined as vehicle malfunction.

The current in-vehicle network produces data to support the operation and maintenance of the vehicle, and to protect the vehicle from safety-related incidents. However, when an intelligent attacker is introduced, there is a need to produce data that can reveal both the presence of malicious code, and provide evidence that will aid an investigation of a cyber attack.

The aim of this article is to define a set of requirements for conducting a forensic investigation of cyber attacks on automobile in-vehicle networks. In particular, we analyze the current in-vehicle network structure, including node layout and external interfaces. Based on the analysis, we identify and define plausible cyber attack actions and derive a cyber attacker model. We then use the attack actions in combination with a set of in-vehicle specific investigation goals to derive a set of requirements on data and a supporting infrastructure for meeting the goals of the investigation. To illustrate the use of the requirements, we apply the Integrated Digital Investigation Process proposed by Carrier and Spafford (2004) and show how the investigation benefits from meeting the requirements.

This article continues by presenting current methods for conducting forensic investigations in vehicles and motivates the need for in-vehicle network security. It then describes a conceptual in-vehicle network including gateways and external interfaces. Then, an attacker model is defined, followed by a list of design goals and a set of requirements for conducting a digital investigation in vehicle environments. An investigation process which is guided by the requirements is then described. Finally, a discussion of in-vehicle forensics and relevant future work is outlined, together with some concluding remarks.

RELATED WORK

Until now, the center of attention for conducting vehicle forensics has been on physical accident reconstruction, and thus the focus has been on determining the physical condition of the vehicle and the surrounding area. As described

Copyright © 2009, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/conducting-forensic-investigations-cyber-attacks/1597

Related Content

Efficient Anonymous Identity-Based Broadcast Encryption without Random Oracles

Xie Liand Ren Yanli (2014). *International Journal of Digital Crime and Forensics (pp. 40-51).*

www.irma-international.org/article/efficient-anonymous-identity-based-broadcast-encryption-without-random-oracles/120220

Collision Analysis and Improvement of a Parallel Hash Function based on Chaotic Maps with Changeable Parameters

Min Longand Hao Wang (2013). *International Journal of Digital Crime and Forensics (pp. 23-34).*

www.irma-international.org/article/collision-analysis-and-improvement-of-a-parallel-hash-function-based-on-chaotic-maps-with-changeable-parameters/83487

Watermark-Only Security Attack on DM-QIM Watermarking: Vulnerability to Guided Key Guessing

B. R. Matamand David Lowe (2012). *Crime Prevention Technologies and Applications for Advancing Criminal Investigation (pp. 85-106).*

www.irma-international.org/chapter/watermark-only-security-attack-qim/66834

Measuring Crime in and around Public Housing Using GIS

Harold R. Holzman, Robert A. Hyattand Tarl Roger Kudrick (2005). *Geographic Information Systems and Crime Analysis (pp. 311-329).*

www.irma-international.org/chapter/measuring-crime-around-public-housing/18831

An Effective Reversible Watermarking for 2D CAD Engineering Graphics Based on Improved QIM

Fei Pengand Yu-Zhou Lei (2011). *International Journal of Digital Crime and Forensics (pp. 53-69).*

www.irma-international.org/article/effective-reversible-watermarking-cad-engineering/52778