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

Dennis K. Nilsson
dennis.nilsson@ce.chalmers.se

Ulf E. Larson
ulf.larson@chalmers.se

Department of Computer Science and Engineering
Chalmers University of Technology
SE-412 96 Göteborg, Sweden

ABSTRACT

The introduction of the wireless gateway as an entry point to an 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 paper, we discuss the specifics of performing 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 Brian Carrier's Digital Crime Scene Model as a template to illustrate how the requirements affect an investigation. For each phase of the model, we show the benefits of meeting the requirements and the implications of not complying with them.

Categories and Subject Descriptors

H.1 [**Models and Principles**]: Miscellaneous

General Terms

In-vehicle network forensics

Keywords

Forensics, vehicle, in-vehicle, network, investigation, data, requirements

1. INTRODUCTION

Automobile in-vehicle networks have historically been isolated from attackers due to the limited access possibilities, but with the advent of wireless Internet-based connectivity between the vehicle and its surroundings, this is about to change. The introduction of a wireless gateway as an entry point to the in-vehicle network allows for remote interaction with vehicle firmware, even when the vehicle is running. This allows remote diagnostics and thus, vehicle owners do not have to drive to a service station to get their car diagnosed. Moreover, firmware updates can easily be applied to thousands of vehicles simultaneously, instead of interfacing each vehicle through the *on-board diagnostics* (OBD) module, thus removing the need for attaching and detaching cables.

In addition, vehicle-to-vehicle and vehicle-to-roadside communication and inter-vehicle communications systems [11] allow vehicles to alert each other 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 manufacturer to consider; *cyber attacks* on vehicles are introduced. We define cyber attacks as attacks that target the vehicle network. An attacker could, for example, use the firmware update feature to inject malicious code into the vehicle network while the vehicle is running.

As an illustration, consider the case of a speeding vehicle that hits the face of a rock. This incident is either caused by the driver itself, or by vehicle malfunction or physical tampering. If the brake wire 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 the responsible to a court of law. Consider instead the possibility that the brakes were disabled by a piece of malicious code. If there is no digital evidence available, the criminal would walk free, and the cause of the accident would wrongly be determined as malfunction.

The current in-vehicle network produces data necessary for 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 investigation of a cyber attack.

In this paper, we state a set of requirements for digital forensic investigations of cyber attacks on automobile in-vehicle networks. We analyze the current in-vehicle network structure, including node layout and external interfaces. Based on the analysis we derive an attacker model and define attacker actions. We use the actions together with a number of forensically sound design goals based on the five widely accepted investigation goals: *who, what, where, when*

e-Forensics 2008, January 21-23, 2008, Adelaide, Australia.
© 2008 ICST 978-963-9799-19-6.

and *why* [25] 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 Brian Carrier's Digital Crime Scene Model [2] and show how the investigation benefits from meeting the requirements.

The remainder of this paper is outlined as follows. In Section 2, we discuss the current methods for conducting forensic investigations in vehicles. In Section 3, we describe an in-vehicle network including gateways and external interfaces. Section 4 formulates a problem definition and lists the design goals, and Section 5 presents the set of requirements for a digital investigation. Section 6 describes the investigation process, as guided by the requirements, and Section 7 discusses future work. Finally, Section 8 concludes the paper.

2. RELATED WORK

Until present time, the process of conducting vehicle forensics has been centered around physical accident reconstruction and has thus been focusing on determining the physical condition of the vehicle and the surrounding area. The status of brakes, lights and wipers, roadway surfaces, loose material and visibility have been important factors to investigate when revealing the cause of an accident [14]. However, this information does not help against "accidents" caused by cyber attacks.

A more recent solution, introduced in the early 1980's is the *event data recorder*, or EDR [7]. An EDR is a black box which records critical event data, such as vehicle speed, engine speed, acceleration, braking, and seat belt status when certain events, such as airbag-release, occur [7, 28]. The EDR data is however, not fine-grained enough to determine whether the "accident" was caused by a cyber attack, and the data does not raise alerts. To access the EDR data, the OBD interface is used [5, 15].

Both the strictly physical approach and the EDR data records have proved extremely useful for accident investigation; however, for cyber attacks, they are not sufficient. Thus, there is a need for a, finer-grained technique for investigating the causes of vehicle accidents.

In-vehicle forensics is similar to cell phone/PDA forensics in the sense that both areas regard operation on embedded devices with limited processing power and memory. Thus, the general ideas used for conducting cell phone/PDA forensics are expected to be applicable in the in-vehicle environment.

The National Institute of Standards and Technology (NIST) has published some guidelines for cell phone and PDA forensics [12, 13]. The guidelines show how data can be retrieved using various tools and procedures. In [8, 25] ideas for conducting forensics on cell phones and PDAs are presented and two phases are described: acquisition and analysis. In the acquisition phase, a forensic duplication of the cell phone or PDA is acquired using tools, such as Paraben's Device Seizure [16] and Forensic SIM Toolkit [3]. Typically, the internal memory and the external memory card, if present, is copied. In addition, for cell phones, a copy of the SIM card is acquired. In the following phase, analysis, the forensic copy is examined to recover relevant information.

The main ideas for cell phone/PDA forensics, such as acquisition and analysis, are also applicable for in-vehicle forensics. However, while a cell phone or a PDA is a single device, the in-vehicle network consists of a large number of embedded devices and is thus a substantially more complex environment. In addition, the interface and data stored on the embedded devices differ. Thus, we believe that new methods for performing forensic investigations in such environments are required.

3. BACKGROUND

An in-vehicle network has two external interfaces: a wireless interface connecting to the Internet, and the OBD interface for physical access. Through these interfaces, two administrative functions can be accessed: diagnostics and firmware updates. Diagnostics is used for check status on the in-vehicle components, and firmware updates are used to update the components.

3.1 The In-Vehicle Network

The *network* in the vehicle consists of *nodes*, *gateways*, and *buses*. A node is an *Electronic Control Unit*, or ECU, which is connected to the bus. The bus is the shared data transfer media, e.g., copper cables. The buses and the nodes form a network. Data may be transferred from one network to another through a gateway. All messages are broadcast on the bus.

An example ECU configuration contains 1-2 kB RAM, 32-64 kB ROM, and 512 kB flash memory [19, 26]. The ROM memory contains the firmware that is executed on the ECU. Each ECU is responsible for the functionality of a certain area in the vehicle. For example, one ECU is responsible for the head lights system, and one ECU handles the driver door functionality (e.g., lock and window). For more complex functions such as the engine system, a number of ECUs are co-operating. Each ECU also has a RAM data area for parameter storage (e.g., which lights are turned on etc.).

There are different network types in an in-vehicle network [21]: *Controller area network* (CAN), *local interconnect network* (LIN), and *media oriented systems transport* (MOST). CAN is the most common network in a vehicle today. There are often several CAN networks, e.g., powertrain and comfort CAN [22]. LIN is a communication protocol used for non-safety critical sensor/actuator systems where CAN is too expensive or not suitable. Communication in LIN is based on a master-slave architecture, where the master is connected to the CAN bus and relays traffic between the CAN and the LIN networks [23]. The MOST protocol, finally, is used to carry audio and video information. This network often employs a ring topology with optical fiber for sending/receiving data in a master-slave fashion. The master is connected to the CAN bus and relays traffic between the CAN and MOST networks [21]. An example vehicle network is illustrated in Figure 1.

In this paper, we focus on the CAN network since its nodes are responsible for safety-critical functions and is therefore a valuable target for the cyber-attacker.

3.2 Administrative Functions

Two common administrative functions that exist for vehicles are *diagnostics* and *firmware updates*.

Diagnostics is used to affect single data parameters in nodes [24], and is used for reading node status, such as *the passenger door is locked*, or controlling node activity (e.g., *unlock the passenger door*) by writing node status. Diagnostics is usually done through the OBD interface and can be performed either by using specific commands for query-

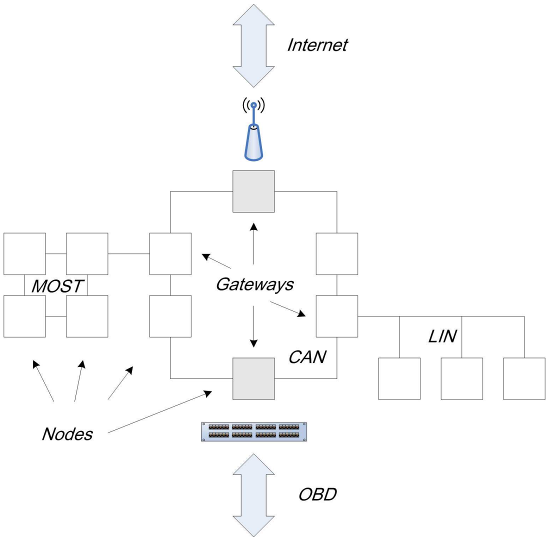

Figure 1: An in-vehicle network consisting of the CAN, LIN, and MOST networks, and two external interfaces.

ing and setting parameter values, or by performing low-level read or write operations on specific memory addresses.

Firmware update is the process of re-flashing the memory of the ECU to install new firmware, e.g., in the case of vehicle functionality problems [10]. The new application binary is transmitted on the bus, and the target ECU flashes the binary to its ROM and reboots.

4. PROBLEM DEFINITION

In this section, we formulate a definition of the problem and the design goals for a complete solution for in-vehicle network digital forensic investigations. In addition, we present the considered attacker model, based on terms presented by Howard and Longstaff [6] in the CERT taxonomy. We define an *event* as an action which is intended to result in a change of state of a selected target. We further define a *security violation* as an event that violates security policy rules, and an *attack* as a series of steps, where one or more events are included, taken by an attacker to violate the security policy.

4.1 Design Goals

To properly perform a digital forensic investigation the necessary data must be present.

- *A method to detect events in the vehicle must be present.* To perform a digital forensic investigation, an alert about a security violating event must have been triggered to provide reason to initiate the forensic investigation.
- *Data to answer the questions who, what, where, when, and why must be produced in the vehicle.* During the forensic investigation, this data must be available in the ECUs for an investigator to extract the necessary information when needed.
- *Information about the current state (e.g., firmware versions) in a vehicle must be available and stored in a secure location.* To detect whether the vehicle has been tampered with, the extracted data must be compared to the original data.

4.2 Attacker Model

In our attacker model, we assume that an attacker can access the in-vehicle network from either the Internet interface or the OBD interface. We further assume that the attacker can perform the actions presented in [6], e.g., inject, modify, and replay messages on the bus as shown in [27]. Moreover, we assume that the attacker can install software, and delete potential logs to hide its presence.

We assume that an attacker after a successful intrusion attempts to either read from, or write data to the ECUs. By reading data, an attacker can attack confidentiality (read secret keys) and privacy (read private driver information). By writing data, an attacker can attack integrity (change functionality of ECUs) and availability (disable ECUs). We therefore focus on intrusion attacks and analyze what methods an attacker can use to read and write data from and to the ECUs.

An attacker that wants to affect the in-vehicle network and the ECUs has three means of doing this. The three actions an attacker can perform are diagnostics requests, low-level requests, and update the node firmware.

- **Sending diagnostics queries (SD)**: An attacker can send read or write requests to get or set certain parameter values in an ECU.
- **Sending low-level requests (SL)**: An attacker can send low-level read or write requests to read or write the byte value of a certain memory address.
- **Performing firmware updates (FU)**: An attacker can update an ECU with new firmware through re-flashing. Thus, an attacker can change the functionality of an ECU to perform malicious acts.

5. REQUIREMENTS FOR A DIGITAL INVESTIGATION

The present vehicle network is primarily designed to support operational safety and maintenance considerations. As discussed earlier, this is not sufficient for protecting against cyber attacks. We use the design goals along with the attacker model to derive a set of requirements for supporting the digital investigation. The set of requirements is divided according to the design goals and are denoted: *Event detection requirements, Forensic data requirements* and *State information requirements.*

5.1 Event Detection Requirements

To detect an event at an early stage it is necessary to introduce a detection mechanism to the in-vehicle network. The event detection requirements address what devices need to be present to detect and alert the appropriate authority that a security violation has been detected.

A model-based detection system [4] maintains a list of allowed communication patterns and alerts when prohibited events occur. Also, the alert data is used together with the event data to aid investigation. In addition, there is a need for a storage device and a device for writing event and alert data to the storage.

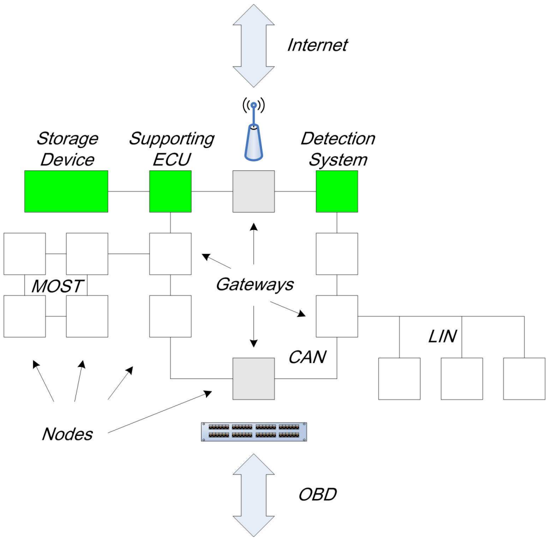

Figure 2: An in-vehicle network with a detection system and storage with supporting ECU devices attached.

Requirement **E1**: A device capable of detecting and providing notifications regarding security violations (events) is installed.

Requirement **E2**: A storage device, along with a supporting ECU which listens to network traffic and writes data to the storage device is installed.

When E1 and E2 are fulfilled, three devices are added to the vehicle network as shown in Figure 2 (dark background). A detection system is added to detect and alert on security violations, and a storage device together with a supporting ECU is placed in the network to contain all the needed logs.

5.2 Forensic Data Requirements

Forensic data requirements address what data needs to be logged for answering the questions raised during the investigation. The goal of a forensic investigation is to provide answers to the questions *who, what, where, when* and *why*, and to be able to reconstruct the state and the events taking place in the system [9]. In order to do this, appropriate data must be captured before and during the event. If the data is insufficient, one or more questions may be left unanswered, or the confidence level of established hypotheses may be lower than with sufficient data. For a forensic investigation it is however difficult to pinpoint single log items that are more interesting than other, since all information *might* actually be useful. For the vehicle network, we use our attacker model to derive appropriate data. The data is grouped according to each forensic goal and attack action. The abbreviations for the attack actions are taken from Section 4.2.

Requirement **D1**: The following data is produced to answer the *who* question.
SD: The identity of the node sending a query.
SL: The identity of the node conducting a low-level operation.
FU: The identity of the node initiating the firmware update.

Requirement **D2**: The following data is produced to answer the *what* question.
SD: The name of the query.
SL: The code of the low-level operation.
FU: The sequence of update command names. Reboot event name.

Requirement **D3**: The following data is produced to answer the *where* question.
SD: The network ID of the sender and receiver of each query.
SL: The network ID of the sender and receiver of each low-level operation.
FU: The network ID of the sender and receiver of the firmware update sequence.

Requirement **D4**: The following data is produced to answer the *when* question.
SD: The time when the query is issued.
SL: The time when the low-level operation is issued.
FU: The time of the start and end of the firmware update sequence of commands, and the time for each individual command.

Requirement **D5**: The following data is produced to answer the *why* question.
SD: The name and value of the query.
SL: The value and target memory address of the low-level operation.
FU: The content of the data in the firmware update sequence.

5.3 State Information Requirements

State information requirements address the data needed by investigators to reconstruct the initial state of the network, and to exclude data that has no significance in an investigation. For this purpose, it is necessary to maintain a description of the a priori state for each network node. This can be achieved by, for example, maintaining a diagnostics laptop that stores an updated list of hashes for all firmware currently installed in the ECUs. This list must be updated each time a firmware update is performed. The list must also be kept in a secure and tamper-resistant location, preferably an offline location.

Requirement **S1**: A list of hashes and the complete current firmware version for all ECUs must be maintained at a secure location.

6. DIGITAL FORENSIC INVESTIGATION OF AN IN-VEHICLE NETWORK

In this section we apply the *Digital Investigation Process Model* proposed by Carrier and Spafford [1, 2] for an example investigation of a vehicle network. Several other models for conducting digital forensics have been proposed, e.g., the U.S. Department of Justice model [20], the model proposed by Prosise et al [17] and the model proposed by Reith et al [18]. We have selected Carrier's model since it connects the physical and the digital crime scene investigations, which is important since both the physical investigation, the EDR records, and the digital investigation may provide complementary evidence when investigating vehicle incidents.

Carrier's proposed model contains the five phases *Readiness, Deployment, Physical crime scene investigation, Digital crime scene investigation* and *Presentation.* We discuss each phase in turn as the investigation proceed, and for each phase, we discuss the actions taken by the investigating organization (e.g., law enforcement, insurance agent, or vehicle manufacturer) in terms of the requirements. We also discuss the implications of not complying with the requirements.

6.1 The Readiness Phase

The readiness phase ensures that the organization is ready to deal with cyber attacks and that the supporting data collection infrastructure is activated so that the relevant data is present when it is needed.
Prerequisites: A list of hashes of the current firmware installed on all ECUs in the in-vehicle network must be accessible according to Requirement S1.
Action: The organization maintains a trained staff of investigators who responds quickly to reported events. In addition, a diagnostics laptop with the latest node firmware versions and hashes, and other diagnostics tools which could interface with both the wireless gateway and the OBD is prepared.
If the prerequisites are not fulfilled: The organization would at best maintain a staff of accident reconstruction investigators, who has to rely on the physical investigation and the EDR data to conduct the investigation.

6.2 The Deployment Phase

The deployment phase provides a means of detecting and confirming that an event has occurred.
Prerequisites: A detection system is present, according to Requirement E1, to indicate that a security violation has occurred.
Action: The organization is alerted from the detection system, either directly over a wireless link or through the vehicle user, who is alerted from the vehicle itself.
If the prerequisites are not fulfilled: The organization relies on either that the event is detected during routine-diagnostics testing in the service station, or that it is detected by the driver when the vehicle is in use.

6.3 The Physical Crime Scene Investigation Phase

The physical investigation phase examines all physical objects on the crime scene.
Prerequisites: None.
Action: A physical investigation of the vehicle is supported by digital evidence collected during the digital investigation. For example, a fingerprint on the OBD connector could be supported by OBD logs showing the time when the OBD was interfaced and what commands were issued.
If the prerequisites are not fulfilled: The same action can be performed as above; however, if no digital evidence is collected during the digital investigation the evidence collected in these two phases cannot be used in conjunction to support the findings of a cyber attack.

6.4 The Digital Crime Scene Investigation Phase

The digital crime scene investigation identifies all digital events that have occurred on the network and examines digital data for evidence.
Prerequisites: Data must be produced in the vehicle network to answer the *who*, *what*, *where*, *when*, and *why* questions regarding the events according to the Requirements D1-D5.

Action: Three steps are performed: *System preservation*, *evidence search*, and *event reconstruction.*

- **System preservation**: System preservation requires isolating a system from its surroundings. This means to guarantee that the wireless gateway does not accept external connections during the investigation. Then, the storage device is disconnected and duplicated so that all firmware updates and all log entries can be analyzed offline.

- **Evidence Search**: Evidence is searched for by reading the event and alert logs from the detection system stored in the storage device, and by comparing the firmware versions on the storage device to the versions stored in the trusted diagnostics laptop. Suspicious firmware versions are reverse engineered to find the differences and the potential causes.

- **Event Reconstruction**: The attacks are reconstructed by using the discovered evidence from the event and alert logs, and the firmware versions.

If the prerequisites are not fulfilled: The digital crime scene investigation phase is impossible to perform without any relevant data.

6.5 The Presentation Phase

The results of the investigation is presented to the appropriate audience after all hypotheses have been tested against the evidence.
Prerequisites: Both the physical and digital investigation must be finished, and hypotheses must have been supported or refuted.
Action: The physical evidence, the evidence from the EDR records and the digital evidence from the network is used to explain what has happened. Correct conclusions regarding both physical and cyber attacks can be supported.
If the prerequisites are not fulfilled: The explanation will have to rely on physical evidence and EDR records only. If a cyber attack has caused the event, erroneous conclusions may be drawn.

7. FUTURE WORK

While a vehicle has several mechanisms, e.g., redundancy and fault tolerance, for detecting and alerting upon safety issues such as loss of braking capacity, security issues is at best marginally addressed. What we see as the most critical item to address is the capability of a vehicle to handle security problems in the same way as safety problems. Today, the only means of detecting security-related events is when they manifest themselves, in other words, when the vehicle starts acting outside specification. Hopefully, this behavior does not manifest itself as loss of braking capacity or other action that potentially has dreadful consequences. Thus, despite the necessity of creating forensically sound data, the immediate attention need to be focused on detection. One way of doing this would be by using a model-based intrusion detection system, which uses models of normal traffic content and behavior, and alerts whenever abnormal events occur.

8. CONCLUSIONS

In this paper, we have presented a set of requirements needed for conducting a digital forensic investigation of a cyber attack on an automobile in-vehicle network. We have analyzed the current in-vehicle network and proposed a set of data that need to be produced during vehicle operation. Moreover, we recognize the need for detection systems and storage devices within the network, and the storage of vehicle state information at a secure location. We have illustrated the significance of the requirements by applying an investigation model and have shown the benefits of fulfilling the requirements, and the implications of not complying with them.

9. ACKNOWLEDGMENTS

The authors would like to thank Dr. Stefan Lindskog of Karlstad University and the anonymous reviewers for valuable suggestions that improved the quality of the paper.

10. REFERENCES

[1] B. D. Carrier and E. H. Spafford. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence*, 2(2), 2003.

[2] B. D. Carrier and E. H. Spafford. An Event-Based Digital Forensic Investigation Framework. In *Proceedings of the 4th Digital Forensic Research Workshop*, 2004.

[3] ForensicSIM Toolkit. http://www.radio-tactics.com/forensic_sim.htm.

[4] T. D. Garvey and T. F. Lunt. Using Models of Intrusions. In *Proceedings of the Third Workshop on Computer Security Incidence Handling*, Herndon, Virginia, 1991.

[5] J. O. Harris and W. C. Wilson. Protocols for the Recovery, Maintenance and Presentation of Motor Vehicle Event Data Recorder Evidence. http://www.harristechnical.com/articles/mvedr.pdf, December 2005.

[6] J. D. Howard and T. A. Longstaff. A Common Language for Computer Security Incidents (SAND98-8667), 1998.

[7] Insurance Institute for Highway Safety. Event Data Recorders. http://www.iihs.org/research/qanda/edr.html, 2006.

[8] K. J. Jones, R. Bejtlich, and C. W. Rose. *Real Digital Forensics. Computer Security and Incident Response*. Addison-Wesley, 2006.

[9] B. A. Kuperman. *A Categorization of Computer Security Monitorings Systems and the Impact on the Design of Audit Sources*. PhD thesis, Purdue University, August 2004.

[10] R. Miucic and M. Shavit. Firmware Update Over The Air (FOTA) for Automotive. In *Proceedings of Asia Pacific Automotive Engineering Conference*, August 2007.

[11] H. Moustafa, G. Bourdon, and Y. Gourhant. Providing Authentication and Access Control in Vehicluar Network Environments. In *Security and Privacy in Dynamic Environments*, IFIP International Federation for Information Processing, 2006.

[12] National Institute of Standards and Technology. Guidelines on PDA Forensics. NIST Special Publication 800-72, 2004.

[13] National Institute of Standards and Technology. Guidelines on Cell Phone Forensics. NIST Special Publication 800-101, 2007.

[14] T. O'Connor. Forensic Reconstruction. http://faculty.ncwc.edu/TOConnor/425/425lect11.htm, June 2001.

[15] W. S. Palmer. Black Box Technology and its Implications for Auto Insurance. www.injurysciences.com/Documents/Claims82002.pdf, August 2002.

[16] Paraben Device Seizure v1.3. http://www.paraben-forensics.com/catalog/product_info.php?cPath=25&products_id=405.

[17] C. Prosise and K. Mandia. *Incident Response: Investigating computer crime*. McGrawHill Osbourne Media, 2001.

[18] M. Reith, C. Carr, and G. Gunsch. An Examination of Digital Forensics Models. *International Journal of Digital Evidence*, 2002.

[19] How to Build a Select Monitor Interface. http://www.alcyone.org.uk/ssm/ecu/index.html.

[20] U.S. Department of Justice. Electronic Crime Scene Investigation: A guide for first responders. Technical report, U.S. Department of Justice, July 2001. Available at: http://www.ncjrs.org.

[21] Vector. Serial Bus Systems in the Automobile: Part 1. Collection of Professional Articles: Issue March, 2007.

[22] Vector. Serial Bus Systems in the Automobile: Part 2. Collection of Professional Articles: Issue March, 2007.

[23] Vector. Serial Bus Systems in the Automobile: Part 3. Collection of Professional Articles: Issue August, 2007.

[24] Vector. Vehicle Diagnostics: The whole story. Collection of Professional Articles: Issue August, 2007.

[25] L. Volonino, R. Anzaldua, and J. Godwin. *Computer Forensics, Principles and Practices*. Prentice Hall, 2007.

[26] Overview of bosch motronic hardware. http://volvospeed.com/obd2/ecu_overview.htm, 2007.

[27] M. Wolf, A. Weimerskirch, and C. Paar. Security in Automotive Bus Systems. In *Workshop on Embedded IT-Security in Cars*, 2004.

[28] P. Zucker. Legal Ramifications for Automobile Black Boxes. http://www.expertlaw.com/library/accidents/auto_black_boxes2.html, June 2003.