7-1-2010

Environmental Obfuscation of a Cyber Physical System - Vehicle Example

Jason Madden

Bruce M. McMillin
Missouri University of Science and Technology, ff@mst.edu

Anik Sinha

Recommended Citation

J. Madden et al., "Environmental Obfuscation of a Cyber Physical System - Vehicle Example," *Proceedings of the 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops (COMPSACW)*, Institute of Electrical and Electronics Engineers (IEEE), Jul 2010.
The definitive version is available at https://doi.org/10.1109/COMPSACW.2010.39

2010 34th Annual IEEE Computer Software and Applications Conference Workshops

Environmental Obfuscation of a Cyber Physical System - Vehicle Example

Jason Madden, Bruce McMillin, and Anik Sinha

Missouri University of Science and Technology
Department of Computer Science
Intelligent Systems Center
Rolla, MO 65409
{jlm333,ff,aks3z4}@mst.edu

Abstract

Cyber-Physical Systems (CPSs) are deeply embedded infrastructures that have significant cyber and physical components that interact with each other in complex ways. These interactions can violate a system's security policy, leading to unintended information flow. The physical portion of such systems is inherently observable, and, as such, many methods of preserving confidentiality are not applicable. This fundamental property of CPSs presents new security challenges. To illustrate this, a vehicle composed of an embedded computer system, its operator, and its environment show how information is disclosed to an observer that is watching from the outside.

The example is made of up a vehicle with an automated engine management system (smart cruise control) traveling across some terrain with an observer watching the vehicle. The information that is to be protected is the controller of the vehicle. This model is analyzed using formal models of information flow, namely nondeducibility and noninference. The vehicle's operation, in context with the terrain of the road, discloses information to the observer. Context is important; the same information that was disclosed with one terrain type is hidden with a different terrain.

This problem, its methodology, and results uncover problems, and solutions, based on the theory of information flow, to quantify security in these new types of systems.

***Keywords*-Road Vehicles; Security; Information Flow**

I. Introduction and Motivation

A Cyber-Physical System (CPS) is an emerging term for a system with deeply embedded computation enmeshed with a physical system [1]. Potential CPSs include high-confidence medical devices and systems, traffic control and safety, advanced automotive systems, process control, energy conservation, environmental control, avionics, instrumentation, and critical infrastructure control systems (water and gas resources, for example). These systems share a common vulnerability, since they inherently control a physical system; confidentiality is difficult to secure. Thus, security in such systems must be described within the physical and cyber context of its operation [2].

Automated vehicles within a highway system form an emerging CPS domain with just such security requirements. Vehicles have communication capabilities whose primary goal is to extend the vision of the driver beyond line of sight. Four major groups of applications [3], [4] are those of a) vehicle-to-vehicle traffic, b) vehicle-to infrastructure, c)vehicle-to-home and d)routing based applications. These are classified on the basis of usage and communication patterns into either safety related or comfort-related (commercial) applications (such as location-based services) [5]. These CPS vehicles have emerging requirements for security [6].

Many cyber security mechanisms for vehicle infrastructures are limited to access control and key management schemes to maintain integrity and privacy [7] to support a wide range of security requirements [8]. While some authors downplay privacy as a concern [4] or even as achievable, others stress the need for privacy through anonymity [3], implemented through the use of multiple keys [7]. All of this work restricts itself to authentication schemes and the use of keys to protect the cyber privacy. To address privacy of the driver and confidentiality of the EMS requires development and analysis of a security model within the system context, fundamentally, a driver, in a vehicle, on a road. This is motivated by the need to determine (or hide) if a vehicle is participating in an automated highway system, or is being operated independently; if the vehicle is pretending to operate under

DOI 10.1109/COMPSACW.2010.39

automated control, but is not, it presents a security risk. To address this issue, this paper considers a complement to traditional analysis by analyzing information flow within the operational context as a fundamental security model.

A specific system chosen as a model problem in this paper, representative of these CPSs, is the automotive Engine Management System (EMS). An EMS is composed of a set of microprocessors that take real time input from sensors and provide output to actuators distributed around different components of a vehicle. The most common of these units include transmission control units, traction control, brake control, etc. A Controller Area Network (CAN) is used to communicate between the devices. Composing this system of controllers with a connection to the CAN device allows all the components work together to provide the driver with enhanced safety, ease of control, and timely response of the vehicle [9]. This coordination results in a CPS with confidentiality requirements [10]. While integrity and availability are vital concerns in operation of the EMS, this paper addresses confidentiality of the system within the context of its environment. Knowing the state of the EMS exposes the existence of critical system control of the vehicle. Determining these controls and preventing their proper execution can reveal confidential information about the driver. The vulnerabilities are due to the disclosure of information. Classic models of confidentiality (such as strict secrecy through encryption, for example) are not appropriate for cyber physical systems as they only protect its cyber portion. Inherently, the system discloses confidential information through its physical actions. Two formal information flow properties, noninference, and nondeducibility [11] are particularly appropriate for examining cyber physical systems [12].

The main contribution of this paper is to show how to determine security within the context of the vehicle's operation and show, fundamentally, when security is violated, and when it is preserved. Velocity, terrain, and obstructions form a context to send information from the vehicle's EMS to an outside observer. Coupled with the knowledge of the world, this information is sometimes adequate to gather enough information in order to reveal knowledge about the driver, but under certain contexts, the context, itself, provides obfuscation of system information. Similar analogies and analysis can be made with oil/gas (observing flow in a pipe) [13], aircraft control (observing a physical motion change), or power flow along power lines [12].

The remainder of this paper is organized as follows: Section 2 states the method to conduct CPS analysis and the model problem; Section 3 is the information analysis; and Section 4 re-emphases the significance of the problem.

II. Methodology and Problem Statement

A. Methodology

The inference of confidential information from observable information flow has high potential to cause critical information leakage, therefore, the vehicle's information flow should be carefully analyzed. Existing security models [11] that analyze multi-level security system behavior are used. Specifically, trace-based information flow models are conceptually attractive for CPSs. Informally, a legal trace of a system is a record of its events during its execution. The collection of all legal traces represents possible system behavior. Both high-level and low-level events are present in these traces. By restricting events to only those that are visible to an observer in the low-level security domain (low-level events) or by purging events in the high-level security domain (high-level events) from these traces, two interesting properties result

Nondeducibility Model: a system is considered nondeducibility secure if it is impossible for an observer in the lower-level security domain, through observing visible events, to deduce anything about the sequence of high-level input events. By restricting the observable trace to only those events that are visible, if another trace can always be found with the same high-level events, the system is nondeducibility secure - i.e. a observation in the low-level security domain is compatible with any of the high-level input events [11].

Noninference Model: a system is considered secure if and only if for any legal trace of system events, the trace resulting from a legal trace purged of all high-level events is still a legal trace of the system [11].

Nondeducibility is particularly appropriate for a CPS; for most systems it is clear that some sort of high-level actions are present, but it is enough to obfuscate which particular actions are occurring [11]. Noninference is a stronger property that indicates what is observed could have occurred with, or without, any high-level events. Note that these are weaker than the traditional notion of confidentiality, namely, noninterference, which states that an observation of a trace is exactly the same with or without high-level actions. This latter property is nearly impossible to achieve in CPSs [12].

The methodology for approaching information security for a CPS consists of the following steps:

1) Determine system function
2) Determine security partitions
3) Develop system traces
4) Apply information flow theory

The last two steps are particularly challenging in a CPS as both the cyber and physical semantic meaning must be merged into a single trace/analysis.

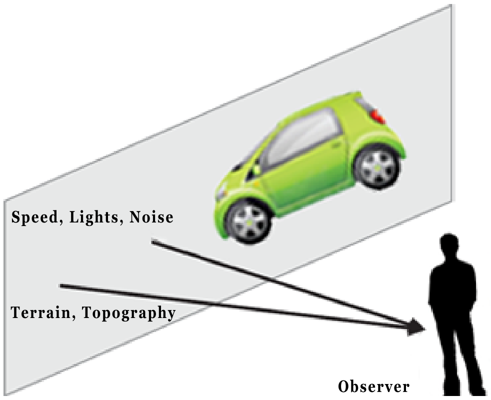

Figure 1. Information flow diagram of an EMS. The observer deduces high-level security domain information from visual cues.

B. Problem Statement

In a vehicle control is maintained either by the EMS or by the driver. For the sake of presentation, the problem is to preserve the confidentiality of the two control types. Confidential information is shown in Table I to analyze the information flow in the EMS.

Table I. Confidential information in EMS

Data	Type	source	Function
Driver		vehicle operator	
Cruise Control	ECU	Automatic control	
Crash Avoidance	ECU	Automatic control	
Control	**Type**	**source**	**Function**
Sensor Information	Digital (CAN)	Sensor Network	Sensor information giving input into the EMS

The EMS is made up of two security levels (shown in Table II). In the high-level security domain, communication is done through a CAN bus and is responsible for the control of the vehicle. In the low-level security domain, the speed information causes implicit communication due to visual queues. The unobstructed view of the vehicle reveals information about the vehicle such as speed, which makes this the implicit communication. The failure of confidentiality occurs when observers from the low-level security domain observe or deduce information from the high-level security domain as depicted in Figure 1.

Table II. Security levels in EMS

Security Level	Security Entities	Reasons
High-Level	EMS	Responsible for aiding the control of the vehicle for the driver
	Driver	Relays input to the EMS by the use of actuators, levers and buttons
Low-Level	Physical	Everything exterior to the vehicle
	Observer	The entity watching information flow

Table III. List of events used in the terrain examples

Notation	Description
l1	Initial speed
l2	Speed reduction
l3	Speed Increase
h1	Driver maintains gas flow
h2	Cruise control maintains speed
h3	Driver increases gas flow
h4	Cruise control increases speed
h5	Driver slows current gas flow
h6	Cruise control decreases speed
h7	Driver resumes original gas flow

III. Analysis of EMS using security models

Using the appropriate security models will show how the EMS can divulge information to the low-level security domain. The following analysis examines the vehicle's operation as a composition of both the driver (manual inputs) and the automated control provided by the EMS over two different types of terrain, flat and hilly 2. The EMS's cruise control is further segmented into three variants:

- **Standard Cruise** This is a typical cruise control of an automobile, it reacts to changes in terrain, but not perfectly, it may speed up or slow down momentarily.
- **Perfect Cruise** This is a cruise control that maintains speed exactly over all terrain. It is not a realistic device, but is included to prove counterexamples.
- **Random Cruise** This is a variant of Standard Cruise with random variability build into it.

Events in Table III are observed at e1 ... e7 in Figure 2 (e2, e3 and e5, e6 differ only the the direction of vehicle travel). Trace analysis is used to develop legal traces of the vehicle in its context and analyzed with respect to two security models.

For each of these proofs, the event that the vehicle changes or maintains velocity is treated as an independent set of traces. If one of the traces fails to hold the property then it fails for the entire scenario.

Theorem 1. *Vehicle operation is nondeducibility secure when traveling up hill for standard and random cruise controls.*

Proof: The EMS is a non-deterministic system which is built from the traces in Table IV: For each trace the first and third events are low-level events and the second event is a high-level input event into the system.

Table IV. Trace list for the Standard Cruise

Scenario	Trace
Traveling Up Hill (e2,e6)	
Maintain Speed	$\{l_1h_3l_1\}$, $\{l_1h_4l_1\}$
Speed Reduction	$\{l_1h_1l_2\}$, $\{l_1h_2l_2\}$, $\{l_1h_5l_2\}$,$\{l_1h_6l_2\}$
Traveling Down Hill (e5, e3)	
Maintains speed	$\{l_1h_5l_1\}$, $\{l_1h_6l_1\}$
Increases speed	$\{l_1h_1l_3\}$, $\{l_1h_2l_3\}$, $\{l_1h_3l_3\}$, $\{l_1h_4l_3\}$
Traveling on Flat Surface (e1,e4,e7)	
Maintains speed	$\{l_1h_1l_1\}$, $\{l_1h_2l_1\}$
Increases speed	$\{l_1h_3l_3\}$
Decreases speed	$\{l_1h_5l_2\}\}$

Table V. Trace list for the Perfect Cruise

Scenario	Trace
Traveling Up Hill (e2,e6)	
Maintain Speed	$\{l_1h_3l_1\}$
Speed Reduction	$\{l_1h_1l_2\}$, $\{l_1h_5l_2\}$
Traveling Down Hill (e5,e3)	
Maintains speed	$\{l_1h_5l_1\}$
Increases speed	$\{l_1h_1l_3\}$, $\{l_1h_3l_3\}$
Traveling on Flat Surface (e1,e4,e7)	
Maintains speed	$\{l_1h_1l_1\}$, $\{l_1h_2l_1\}$
Increases speed	$\{l_1h_3l_3\}$
Decreases speed	$\{l_1h_5l_2\}\}$

Standard Cruise: This scenario is built from the traces in Table IV. The vehicle, as it travels up the hill, is nondeducibility secure because for any trace the low-level output events are identical regardless of the controller of the vehicle. The traces are either l_1l_1 or l_1l_2. There are multiple high-level events that the vehicle either speeds up, slows down, or maintains speed. Because of this fact, there is no high-level event trace that leads to a unique set of low-level output events to the observer.

Perfect Cruise: This scenario is built from the traces in Table V. Because the perfect cruise does not allow for any deviation from the set speed, it is more revealing of the controller of the vehicle. The driver has the ability to change speed or due to a lack of awareness changes speed, this leads to a divulgence of information and violates the nondeducibility property.

Random Cruise: This scenario is built from the traces in Table VI. Traveling up hill the random cruise is able to perform the same actions as a driver, so for each case of the vehicle with a change in velocity or maintenance of the velocity the controller is nondeducibility secure. The random perturbations of the velocity are able to hide the fact that a non-perfect driver reveals the controller of the vehicle. ■

Table VI. Trace list for the Random Cruise

Scenario	Trace
Traveling Up Hill (e2,e6)	
Maintain Speed	$\{l_1h_3l_1\}$, $\{l_1h_4l_1\}$
Speed Reduction	$\{l_1h_1l_2\}$, $\{l_1h_2l_2\}$, $\{l_1h_5l_2\}$,$\{l_1h_6l_2\}$
Traveling Down Hill (e5,e3)	
Maintains speed	$\{l_1h_5l_1\}$, $\{l_1h_6l_1\}$
Increases speed	$\{l_1h_1l_3\}$, $\{l_1h_2l_3\}$, $\{l_1h_3l_3\}$, $\{l_1h_4l_3\}$
Traveling on Flat Surface (e1,e4,e7)	
Maintains speed	$\{l_1h_1l_1\}$, $\{l_1h_2l_1\}$
Increases speed	$\{l_1h_3l_3\}$, $\{l_1h_2l_1\}$
Decreases speed	$\{l_1h_5l_2\}$, $\{l_1h_2l_1\}$

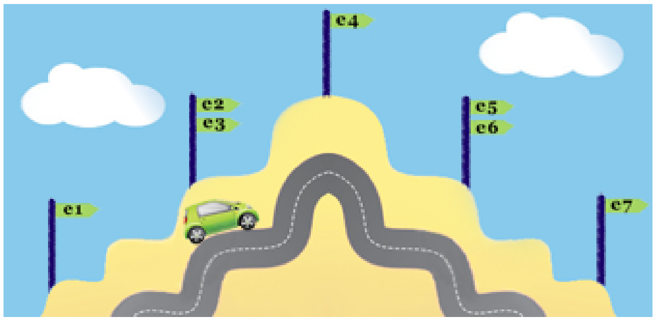

Figure 2. Comparison of how the events are captured on differing terrains.

Theorem 2. *Vehicle operation is nondeducibility secure when traveling down hill for standard and random cruise controls.*

Proof: The EMS is a non-deterministic system and for given low level inputs and controllers there are several representative traces. For each trace the first and third events are low-level events and the second event is a high-level input into the system.

Standard Cruise: This scenario is built from the traces in Table IV. The vehicle, as it travels up the hill, is nondeducibility secure because for any trace the low level outputs are identical regardless of the controller of the vehicle. There are multiple high level actions that the vehicle either speeds up, slows down, or maintains speed. The traces are either l_1l_1 or l_1l_3. Because of this fact, there is no event trace that leads to a unique set of outputs to the observer.

Perfect Cruise: This scenario is built from the traces in Table V. Traveling down hill reveals the controller much in the same way as going up hill. Since it is unreasonable for the vehicle to change its speed while on a perfect cruise control it reveals that the driver is in control of the vehicle. There is a unique trace for any sort of speed variation, so this violates the nondeducibility property.

Random Cruise This scenario is built from the traces in Table VI. The random cruise will vary the speed in such a way that it will average out at the target speed. This is feasible if the cruise has as much control over the vehicle as the perfect cruise but alters the velocity enough to make it reasonable at different discrete events that the velocity can vary. ■

Theorem 3. *Vehicle operation is not nondeducibility secure when traveling across a flat terrain.*

Proof: The EMS is a non-deterministic system represented by a trace of events. For each trace the first and third events are low-level events and the second event is a high-level input into the system.

Standard Cruise: Refer to the traces in Table IV. The vehicle, as it travels across a flat surface, is not nondeducibility secure because for any trace the low level outputs are not always identical. In the case that the vehicle speeds up ($\{l_1 h_3 l_3\}$) or slows down ($\{l_1 h_5 l_2\}$), there is no other way to explain these actions than to say that the driver is operating the vehicle in these cases. A cruise control would not act in this manner.

Perfect Cruise: Refer to the traces in Table V. Traveling across the flat plane with a perfect cruise control is the same case as a standard cruise control.

Random Cruise Refer to the traces in Table VI. The random cruise has the most substantial amount of effect on the case of the flat terrain. For both the standard cruise and the perfect cruise, it is not nondeducibility secure for the reason that it is unreasonable to have any differences of speed from the set velocity. The random cruise adds small changes in velocity to simulate a human driver, implying that they are not perfect. As a result, there is no unique trace for the cases of increasing or decreasing speed showing nondeducibility. ■

Discussion The results from these examples reveal inherent obfuscation even in the presence of observable events. When the low-level output events correlate with a low-level input event at the physical level, the controller of the high-level input events is hidden from the observer. For example, as the vehicle travels up the hill, the event of the vehicle slowing down from its initial velocity can be explainable in two ways; the driver did not maintain the proper amount of gas flow to give the vehicle enough force to make it up the hill or the cruise control could not compensate for the steep grade of the hill. It follows that there is a trace for both the driver and the cruise control that allow the vehicle to slow down while traveling up hill.

Adding a perfect cruise in the system shows how any deviation in speed from the target speed reveals the existence of the driver. Having some variation as added by the random cruise is beneficial to the system as a whole since a human is imperfect as a driver. By the addition of the randomized cruise a simulation of a driver is added into the system, and this addition solves the problem of having unique traces for a given case that is nondeducibility secure. Generally a driver can not maintain a constant speed over all terrains while a perfect cruise control has the ability to do this.

Theorem 4. *Vehicle operation is not noninference secure when traveling down hill or traveling up hill.*

Proof: : The EMS is a non-deterministic system which is built from the following traces: For each trace the first and third events are low-level events and the second event is a high-level input into the system.

Standard Cruise: The vehicle, as it travels down the hill, is noninference secure because for any trace the low-level traces are identical regardless of the controller of the vehicle. After a purge of the high-level events, in the case of maintaining speed the resulting trace is $\{l_1 l_3\}$, while increasing speed the resulting trace is $\{l_1 l_3\}$. In terms of traveling up hill the resulting traces are $\{l_1 l_2\}$, while reducing speed the resulting trace is $\{l_1 l_2\}$. It is not noninference secure with respect to there being a controller when the vehicle is maintaining speed, but this does not reveal who is in control of the vehicle. It is noninference secure in the case that the vehicle is increasing speed while traveling down hill and decreasing speed while traveling up hill when the high level input is purged from the traces.

Perfect Cruise: After purging the high level events with respect to the perfect cruise, it follows much in the same way as the standard cruise. Once the hight level events are purged, the low level trace would result with $\{l_1 l_3\}$ in the down hill trace and $\{l_1 l_2\}$ for the up hill trace. Having a controller violates the noninference property.

Random Cruise Including a random cruise in this environment keeps the vehicle controller noninference secure. There is a controller visible to the observer, but it cannot be inferred whether the control is from the driver or the cruise control. This is caused by there being no unique mappings to an individual controller after the removal of the high level events. ■

Theorem 5. *Vehicle operation is not noninference secure when traveling across a flat surface and increases or decreases speed.*

Proof: : The EMS is a non-deterministic system where for each trace the first and third events are low level events and the second event is a high level input into the system.

Standard Cruise: The vehicle, as it travels along the road, is not noninference secure because for any trace after the purge of the high-level events, the low-level traces are not identical. After a purge of high level events, the resulting trace for the vehicle while maintaining speed is $\{l_1 l_1\}$, the resulting trace from the vehicle increasing speed is $\{l_1 l_2\}$, and finally the resulting trace for the vehicle decreasing speed is $\{l_1 l_3\}$. This rule is violated both in the case that the vehicle increases and maintains speed. The reason is after the controller is removed from the system the vehicle will begin to slow down due to friction and gravity on the vehicle.

Perfect Cruise: In this case the perfect cruise acts the same as the standard cruise.

Random Cruise After the purge of all the high-level events the resulting trace is $\{l_1 l_3\}$. It is noninference secure in terms of the control of the vehicle. ■

Discussion The outcome of this analysis shows another natural obfuscation of high-level events when the low-level events correlate with the physical design of the system. For example, if the vehicle traveling down the hill has a high-level action removed from the trace, it is reasonable for the vehicle to slow down or remain a constant speed. On flat terrain, the control (EMS or human) of the vehicle can be inferred because if the vehicle either speeds up or slows down then it is not the cruise control that is managing the operation of the vehicle.

The perfect cruise does little to improve the results. The random cruise improves the ability to infer which control is active in the system. With its addition, it masks the control by adding additional traces into the system that guarantee that there is no unique mapping of traces at the low-level.

IV. Conclusions and Significance

This paper showed that while CPSs have an inherent information flow leak due to inherent observability, they contain natural information flow obfuscation of their high level events. For the specific example of an EMS system of a vehicle and the driver of an automobile there were some cases in which the EMS in its environment satisfies the properties of noninference and nondeducibility. In order to accomplish this, there was a natural obfuscation of the high-level events due to the context of the physical world and the response of the vehicle. The cases in which the confidentiality of the vehicle and the driver did not satisfy the information flow properties occurred when it was not reasonable for a controller to take some action that was uncharacteristic of the system. The natural obfuscation is significant in the CPS domain because it provides a means to hide information within the context of an inherently observable system.

This analysis involving the EMS and the driver is a common example of many CPSs that use the lowest security level as a medium of information transfer. There is no way to avoid the use of this medium and is significant to the analysis of these infrastructures. Thus, the approach, methods, and security models of this paper quantify security analysis for cyber-physical systems.

Acknowledgment

This work was supported in part by the NSF CSR award CCF-0614633 and the Missouri S&T Intelligent Systems Center

References

[1] E. A. Lee, “Cyber-physical systems - are computing foundations adequate?” in *Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, October 16 - 17, 2006.

[2] V. Srinivasan, J. Stankovic, and K. Whitehouse, “Protecting your daily in-home activity information from a wireless snooping attack,” in *UbiComp ’08*. New York, NY, USA: ACM, 2008, pp. 202–211.

[3] A. Aijaz and et. al., “Attacks on inter-vehicle communication systems - an analysis,” in *(WIT 2006)*, 2006. [Online]. Available: http://www.leinmueller.de/publications/wit2006-AttackModel.pdf

[4] R. Karim, “VANET: Superior System for Content Distribution in Vehicular Network Applications,” Rutgers University, Department of Computer Science, Tech. Rep., 2008.

[5] E. Schoch, F. Kargl, T. Leinmüller, and M. Weber, “Communication patterns in vanets,” *IEEE Communications Magazine*, vol. 46, no. 11, pp. 119–125, November 2008.

[6] K. Plobl, T. Nowey, and C. Mletzko, “Towards a security architecture for vehicular ad hoc networks,” in *ARES ’06*. Washington, DC, USA: IEEE Computer Society, 2006, pp. 374–381.

[7] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure vehicular communication systems: design and architecture,” *Communications Magazine, IEEE*, vol. 46, no. 11, pp. 100–109, november 2008.

[8] A. Kung, “Security Architecture and Mechanisms for V2V / V2I ,” Sevecom, Tech. Rep., 2008.

[9] T. Hoppe, S. Kiltz, and J. Dittmann, “Security threats to automotive can networks - practical examples and selected short-term countermeasures,” in *SAFECOMP*, 2008, pp. 235–248.

[10] D. Nilsson, U. Larson, and E. Jonsson, “Creating a secure infrastructure for wireless diagnostics and software updates in vehicles,” in *SAFECOMP*. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 207–220.

[11] J. McLean, “Security models,” in *Encyclopedia of Software Engineering*, 1994.

[12] H. Tang and B. McMillin, “Analysis of the security of information flow in the Advanced Electric Power Grid using Flexible Alternating Current Transmission System (FACTS),” in *Critical Infrastructure Protection*. Springer, 2008, pp. 43–56.

[13] R. Akella and B. McMillin, “Model-Checking BNDC Properties in Cyber-Physical Systems,” in *COMPSAC ’09*, vol. 1, July 2009, pp. 660–663.