SAE International™

Do Vehicles Need Data Security?

2011-01-0040
Published
04/12/2011

André Weimerskirch
escrypt Inc.

doi:10.4271/2011-01-0040

ABSTRACT

Data security was introduced to vehicles in the 1980's with the electronic theft protection system. Since then data security was also implemented in further electronic systems of vehicles, including theft protection for electronic control units, protection of mileage counter integrity, protection against software manipulation (secure flashing), and secure wireless on-board diagnoses (e.g. via Bluetooth). Vehicles include more and more electronic systems and open communication channels based on public standards, making them vulnerable to a variety of attacks. Security mitigation mechanisms are implemented in software and might be supported by a controller with basic security features.

Recently, research was started to centralize security features in a single dedicated security controller. This security controller implements cryptographic methods and provides tamper resistance. Current and future applications with need for security include vehicular communication, feature activation and pay-on-demand applications as well as digital content protection systems.

In this work we will analyze which degree of implemented security features in a vehicle is reasonable. We will consider both security features based on secure hardware and software mechanisms. We will distinguish applications that protect a financial asset (e.g. theft protection) and safety applications (e.g. future vehicle-to-vehicle wireless communication safety applications). We will evaluate whether there is a threat to safety because of new technologies, and how this threat needs to be mitigated. Finally, we will identify the useful mitigation mechanisms and describe how these need to evolve over time. We will perform the evaluation under the premise of economic security, i.e. always assuming that only economically feasible solutions will be deployed.

INTRODUCTION

Data security was first introduced to vehicles in the 1980's for theft protection systems. In the first step, drivers had to enter a secret passcode via a small input keyboard to unlock the engine control unit and start the vehicle. Then car makers implemented electronic immobilizers that "linked" the vehicle key to a crucial vehicle component (usually the engine control module). The vehicle key was equipped with a small controller that passed a secret string to the engine control module, and the engine only started if the proper secret string was passed. This mechanism is still continuously improved to counter advanced attacks. Car makers also introduced remote vehicle unlock features. The first iteration was poorly designed and the number of stolen vehicles increased; the remote control transmitted a fixed "secret string" and an attacker could eavesdrop and replay it by using a universal learning TV remote control. The car makers learned quickly and introduced sophisticated mechanisms (so called rolling codes). Please note that the electronic immobilizer and remote unlock feature are usually separate systems. Today most car makers switch to standardized mechanisms since proprietary cryptographic algorithms were repeatedly broken (e.g. the proprietary algorithm Keeloq was completely broken in 2008 [2].

Nowadays vehicles are computerized with dozens of microcontrollers and hundreds of megabytes of storage. Many vehicles provide Bluetooth connections for handsfree headsets or for connecting an entertainment device. Bluetooth connections are also used for easy service to replace the diagnoses plug. Vehicles provide Internet access to passengers, and tires report air pressure via a wireless link to the vehicle's internal diagnosis system. It is planned that vehicles will communicate with each other and with road-side access points via Dedicated Short Range Communication (DSRC) to implement cooperative safety applications (e.g. a

heavily abrupt breaking vehicle broadcasts an electronic emergency break light warning message), information applications and commercial applications. It becomes clear that vehicles will become highly connected mobile computing nodes and that for vehicles data security must be carefully considered. This topic made it recently into the news [5, 6]. The authors were able to prove vehicles' security weaknesses by successfully attacking vehicles. For instance, they were able to manipulate the firmware of a vehicle to block a single wheel that could have caused an accident, and they were able to track a vehicle and damage privacy using the US mandatory tire pressure system. Note that an attack to cause harm requires physical access to the vehicle; in case of manipulating the vehicle's firmware, physical access to a communication bus that is connected to the ABS (anti-break system) electronic control module (ECM) is required. However, if physical access is available, an attacker can also cut a break pipe to cause harm. The imminent danger becomes clear though and it might only be a matter of time before serious vulnerabilities become known and before attacks can be mounted via a wireless interface from some distance. Unlike PCs, vehicles do not implement any regular security update mechanisms and vulnerabilities cannot easily be fixed.

The opinions about the necessary degree of security mechanisms (and thus involved implementation cost) widely differ between vehicle makers, security consultants (the author being one), and academic people, and they are often driven by business and personal interest. In the remaining paper, we will perform a risk assessment by identifying assets and attacks, evaluating the risk for the identified attacks, and suggesting reasonable countermeasures. Our objective is to keep cost of countermeasures low since a solution must be commercially feasible or it will be discarded by car makers. Please note that this paper will provide an overview without going into application details and without providing implementation details. The performed process can be repeated for a subset of vehicle system at increased detail level to come up with attractive and feasible countermeasures.

ASSETS AND ATTACKS

Assets include applications and systems that an attacker may find attractive to attack. Assets comprise interfaces, applications, communication systems, and electronic control units (ECUs). We provide an overview of assets and attacks in Table 1. It is possible to broaden the scope (e.g., on the level of overall assets such as “stealing the vehicle”) or to narrow it down (e.g., “perform a reverse-engineering attack to the vehicle key's build-in microcontroller”).

ATTACKER MODEL

We classify attackers based on [1] according to the attacker's capabilities:

- A1. Clever Outsider: A talented engineer and/or cryptographer who does not possess any inside knowledge.
- A2. Knowledgeable Insider: An insider who posses detailed knowledge about the system (security and non-security related) and has access to its specifications.
- A3. Funded Organizations: An organization that has access to substantial resources.
- A4. Funded Organizations with Insider Knowledge: An organization that has access to substantial resources and insider knowledge (e.g. by buying insider knowledge)

Free-riders that apply exploits are not considered in the attacker model since they are beneficiary of a successful attack rather than attackers. However, free riders are dangerous for successful business models.

COMMON COUNTERMEASURES

Today a variety of countermeasures is implemented in vehicles. We assume that these common countermeasures are already implemented in our vehicle target of evaluation. Note that these countermeasures are not implemented in all vehicles and they are not implemented by all car makers. However, since they are implemented by some car makers, we assume that implementing these countermeasures is feasible and attractive, and that it is a matter of time until these countermeasures are implemented in a majority of vehicles. The countermeasures implemented today are listed in Table 2. Note that there are four common security applications: (1) electronic immobilizer, (2) vehicle unlock mechanism, (3) component identification, and (4) secure software download. (1) and (2) are implemented by almost all vehicle manufactures, whereas (3) and (4) can be found in an increasing number of vehicle models. Assets AS5 and AS6 take a special role since they are not implemented yet but are currently designed and standardized, and might be deployed as early as 2015.

RISK OF IDENTIFIED ATTACKS

RISK MODEL

Risk is defined as the product of likelihood and impact. Likelihood is defined as the probability that an attack is successful. It is based on the technical difficulty of an attack and the legal deterrence. Note that the car maker can only directly alter the technical difficulty of an attack to adjust the level of risk. Legal deterrence can be indirectly adjusted via legislation. The impact of an attack is defined by impact to safety, impact to the car maker's financial interests (e.g. if the car maker cannot sell a feature anymore because it is

Table 1. Assets and Attacks

Asset Number	Asset	Attack Number	Attack	Explanation
AS 1	Vehicle theft protection	AT 1	Replace theft protection components	Theft protection schemes include the electronic immobilizer, alarm system, physical security, GPS theft system, etc. We focus on the electronic immobilizer and vehicle unlock mechanisms but include further theft protection mechanisms in the risk analysis.
		AT 2	Flash new firmware to theft protection components	
AS 2	Component theft protection	AT 3	Remove security component	Component theft protection avoids that individual components (e.g. radio and navigation system) are stolen.
		AT 4	Flash new firmware	
AS 3	Internal communication bus	AT 5	Eavesdrop data	ECUs communicate via the internal communication bus (e.g. CAN, FlexRay, MOST, LIN, …). The data might include safety and non-safety relevant information. Access to the internal bus requires physical access to the unlocked vehicle or to a compromised external interface. The internal communication bus might be used to mount further attacks. Access to the communication bus is provided via the diagnosis interface.
		AT 6	Alter and inject data	
AS 4	External wireless interfaces for comfort functions (Bluetooth, tire sensor, …)	AT 7	Eavesdrop data	External wireless interfaces provide easy access to vehicle data and service functions. For instance, Bluetooth can be used to access the vehicle logs, and Bluetooth can also be used to connect a headset. The interface might provide access to the internal communication bus.
		AT 8	Alter and inject data	
AS 5	Wireless cooperative safety applications	AT 9	Eavesdrop data	DSRC based safety systems will decrease traffic fatalities by cooperative one-hop communication between vehicles. Messages will include location, time and vehicle information. Eavesdropping might reduce privacy, and message alteration might endanger safety and/or comfort.
		AT 10	Alter and inject data	
AS 6	Wireless cooperative information and commercial applications	AT 11	Eavesdrop data	DSRC information and commercial applications include vehicle-to-access point communication and vehicle-to-vehicle communication. Messages might be altered to gain an advantage (e.g. provide false information to other vehicles to reroute them and avoid congestion) or messages might be eavesdropped to learn about other vehicles' behavior (privacy).
		AT 12	Alter and inject data	
AS 7	Commercial and infotainment applications (including activation of features for additional payment)	AT 13	Exploit services without paying	It is a common business model to include deactivated features in vehicles, or to implement features and deactivate these after a trial period. Hackers want to activate these features without paying.
AS 8	ECUs	AT 14	Read out firmware	ECU firmware is compromised to save development cost (by competitors) and to alter behavior (e.g. increasing engine power). Alternating ECU firmware is also a popular attack path for several of the above attacks.
		At 15	Alter firmware	
		At 16	Alter hardware	ECU hardware is altered to influence the operation of an ECU. For instance, an odometer can be altered to manipulate the odometer mileage.

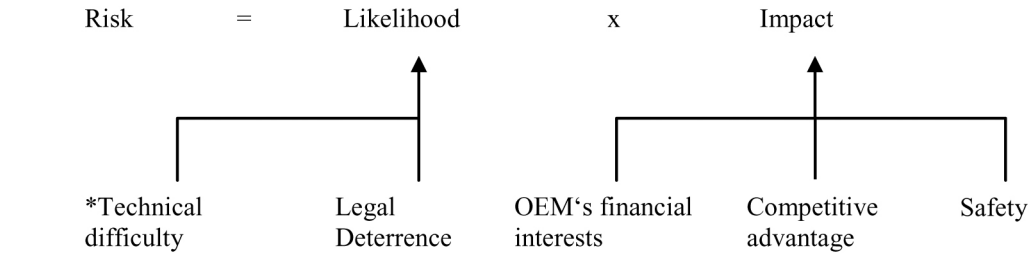
common knowledge how to activate the feature for free), and impact to the car maker's competitive advantage (e.g., if a vehicle model is known to be stolen frequently, insurance premiums will increase and consumers will tend to buy vehicles with lower insurance rates). The definition of risk is summarized in Figure 1.

Table 2. Countermeasures Implemented Today

Asset Number	**Asset**	**Attack Number**	**Attack**	**Countermeasures Implemented Today**
AS 1	Vehicle theft protection	AT 1	Replace theft protection components	*Electronic Immobilizer:* A microcontroller in the vehicle key and one or more ECUs are coupled. The electronic key must proof knowledge of a secret in a challenge-response mechanism to start the vehicle. *Vehicle Unlock*: A microcontroller in the key fob generates so-called rolling codes to unlock the vehicle. The vehicle ECU compares the received code with the expected one. *Component Identification*: All ECUs are coupled together, and replacing a single component will deactivate the vehicle.
		AT 2	Flash new firmware to theft protection components	*Secure Software Download*: Software must be digitally signed by the car maker. The ECU verifies the firmware's digital signature, and only verified firmware can be loaded into an ECU.
AS 2	Component theft protection	AT 3	Remove security component	*Component Identification*, see above
		AT 4	Flash new firmware	*Secure Software Download*, see above
AS 3	Internal communication bus	AT 5	Eavesdrop data	None
		AT 6	Alter and inject data	None
AS 4	External wireless interfaces for comfort functions (Bluetooth, tire sensor, …)	AT 7	Eavesdrop data	Only if they come as part of an implemented standard (e.g. Bluetooth security)
		AT 8	Alter and inject data	Only if they come as part of an implemented standard (e.g. Bluetooth security)
AS 5	Wireless cooperative safety applications	AT 9	Eavesdrop data	Comprehensive countermeasures are currently planned
		AT 10	Alter and inject data	Comprehensive countermeasures are currently planned
AS 6	Wireless cooperative information and commercial applications	AT 11	Eavesdrop data	Comprehensive countermeasures are currently planned
		AT 12	Alter and inject	Comprehensive countermeasures are currently

Table 2 (cont.). Countermeasures Implemented Today

			data	planned
AS 7	Commercial and infotainment applications (including activation of features for additional payment)	AT 13	Exploit services without paying	Car maker specific
AS 8	ECUs	AT 14	Read out firmware	None
		At 15	Alter firmware	*Secure Software Download*, see above
		At 16	Alter hardware	None



* Parameter that can be altered by car maker

Figure 1. Risk Model

In our evaluation, we use units low, medium and high for both the likelihood and impact metric. A *low impact* will affect a single vehicle or a small number of vehicles, and it will impact a vehicle only once and it will not be annoying or dangerous. A *medium impact* affects a larger amount of vehicles, and it might be annoying or uncomfortable for the driver but not dangerous or permanent. A *high impact* affects a significant number of vehicles, and drivers and passengers will clearly notice signs of the attack. Likelihood is defined relatively rather than in absolute terms. An attack of low likelihood is expected to never happen and it will be a surprise if it happens. An attack of high likelihood is expected to happen frequently. An attack of medium likelihood is expected to happen but only infrequently. Table 3 defines the risk levels. For instance, the matrix in Table 3 maps medium impact and low likelihood to a low risk. As a rule of thumb, high risk attacks must be countered, medium risk attacks must be considered individually, and low risk attacks must be monitored.

Table 3. Risk = Likelihood × Impact

Impact → ↓ Likelihood	Low	Medium	High
Low	Low	Low	Medium
Medium	Low	Medium	High
High	Medium	High	High

RISK EVALUATION

We now assign a likelihood and impact to each attack. For ease of presentation, we assign a single likelihood. For a detailed analysis of a subsystem, it is recommended to assign a likelihood for each attacker category. We then calculate the risk following the risk matrix of Table 3 with the impact being the worst case of the three impact sub-categories. The results are displayed in Table 4. Individual entries can certainly be disputed and we focused on relative consistency. We explain the most important entries in the following:

• *AS1*: Vehicles are stolen regularly by overcoming the electronic theft protection mechanisms, but not by towing them, although they are equipped with modern theft

protection systems. It is known that components are replaced or added after physically opening the vehicle (AS 1). A more secure theft protection mechanism provides a competitive advantage because of insurance rate advantages. However, impact is limited since consumers' first focus is not insurance premiums. While the risk is evaluated as medium, it can be reduced by alarm systems and GPS tracking systems. We marked this in brackets.

• *AS2*: Arguments of AS1 can be applied similarly to AS2.

• *AS3*: It is easy to alter and eavesdrop data on the internal communication busses. The impact might be devastating if safety relevant data, e.g. ABS related data, is altered. Physical access to the internal bus is required, however, and in case of a successful attack it is usually easy to detect the manipulation.

• *AS4*: It is assumed here that no countermeasures are implemented. If Bluetooth or another standardized wireless communication protocol is implemented, and if security is turned on, the risk is reduced (in brackets).

• *AS5 and AS6*: The evaluation is based on the current draft of the IEEE 1609.2 standard [3]. Security is considered carefully and risks are well mitigated. The impact is low to medium since the applications will support and notify the driver but will not control the vehicle at the initial deployment stage.

• *AS7*: The likelihood solely depends on the car maker's implemented security features. Since the impact is potentially high, the risk evaluates to either medium or high.

• *AS8*: It is easy to read out firmware but hard to alter it due to the secure software download mechanism. On the other side, altering the hardware, e.g. replacing an ECU or adding another microcontroller, is fairly easy (e.g., this attack is mounted to compromise theft protection mechanisms). The impact is potentially high since safety relevant systems could be manipulated. However, physical access is required to mount the attack, and in case of a successful attack it is easy to detect the manipulation (it is far easier to detect a replaced or added ECU than to identify a manipulated firmware of a genuine ECU).

COUNTERMEASURES

From the previous section, it can be concluded that there are several high risk assets in vehicles. However, it must also be concluded that almost all of these high risk assets can, and are, mitigated by addition protection mechanisms including physical security and GPS theft protection systems. Also it must be noted that manipulation of the ECUs and internal bus has a high risk but can usually detected after an attack (although it is not common practice to search for such traces). The following countermeasures are suggested here for mitigation:

1. Use common countermeasures including (1) electronic immobilizer, (2) vehicle unlock mechanism, (3) component identification, and (4) secure software download.

2. For all wireless interfaces, use standardized protocols in a secure mode. For instance, the attack in [6] is successful because of an unprotected wireless RFID interface of the tire sensors.

3. Consider introducing an integrity check for the internal communication bus systems to lower the risk of Asset AS3. However, this will not significantly reduce the risk potential. Attackers can still tamper with individual ECUs or sensors to alter data that is passed over the communication bus (cf AS8). It increases the technical difficulty for an attack though and will reduce the number of attackers. Protection the communication bus is also a requirement for all further advanced security mechanisms.

4. Introducing microcontrollers with security features (tamper resistance, key storage, cryptographic operations) will avoid that ECUs can be replaced and that firmware can be read or altered (AS8). It will also counter altering of communication (AS3). These mechanisms can then be used to increase the level of remaining applications, including theft protection. However, there are limitations and manipulation will still be possible. Sensors can be manipulated and false data is then introduced at the source (e.g., the tire rotation sensors can be manipulated to report a behavior that will result in a critical reaction). There are R&D efforts in this area but at this time such approaches are commercially unfeasible. Until then, physical security of the vehicle and its components is a limitation for electronic tampering.

5. Countermeasures for AS7 must be considered on an individual basis. It might be commercially attractive to avoid tampering and lost revenue by introducing strong security features including secure tamper resistant hardware. Once such security components are available, they might be used at low additional cost to increase the security level of other applications and thus reduce the risk level overall.

In our risk model of Figure 1 we defined that likelihood is defined by technical difficulty of an attack and legal deterrence. In our consideration so far we only considered the technical difficulty. We showed that there are limitations to security in a commercial environment. In particular, sensors cannot be made tamper resistant at this time. Legal deterrence needs to play a role in a security evaluation since tampering with such systems is comparable to tampering with mechanical parts and will be prosecuted. It is also important to keep in mind that an attacker will always follow the easiest attack path. An attacker that wants to tamper with safety related systems will at some point not aim for electronic systems but for mechanical systems.

Table 4. Risk Evaluation

Asset Number	**Asset**	**Attack Number**	**Attack**	**Likelihood**	**Impact**			**Risk**
					Financial Interest	**Competitive Advantage**	**Safety**	
AS 1	Vehicle theft protection	AT 1	Replace theft protection components	**Medium**	Low	**Medium**	Low	Medium (Low)
		AT 2	Flash new firmware to theft protection components	**Medium**	Low	**Medium**	Low	Medium (Low)
AS 2	Component theft protection	AT 3	Remove security component	**Medium**	Low	**Medium**	Low	Medium (Low)
		AT 4	Flash new firmware	**Medium**	Low	**Medium**	Low	Medium (Low)
AS 3	Internal communication bus	AT 5	Eavesdrop data	**Medium**	Low	Low	**Low**	Low
		AT 6	Alter and inject data	**Medium**	Low	Low	**High**	**High** (tamper evident)
AS 4	External wireless interfaces for comfort functions (Bluetooth, tire sensor, …)	AT 7	Eavesdrop data	**High**	Low	**Medium**	Low	**High** (Medium)
		AT 8	Alter and inject data	**High**	Low	Low	**Low**	Medium (Low)
AS 5	Wireless cooperative safety applications	AT 9	Eavesdrop data	**High**	Low	**Low**	Low	Medium
		AT 10	Alter and inject data	**Low**	Low	**Medium**	Low	Low
AS 6	Wireless cooperative information and commercial applications	AT 11	Eavesdrop data	**Low**	Low	**Medium**	Low	Low
		AT 12	Alter and inject data	**Low**	Low	**Medium**	Low	Low
AS 7	Commercial and infotainment applications (including activation of features for additional payment)	AT 13	Exploit services without paying	Car Maker Specific	**High**	Low	Low	**Medium/High**
AS 8	ECUs	AT 14	Read out firmware	**High**	Low	Low	**Low**	Medium
		At 15	Alter firmware	**Low**	**High**	Medium	**High**	Medium
		At 16	Alter hardware	**Medium**	Low	Low	**High**	**High** (tamper evident)

RELATED WORK

Recently, the first attacks on vehicles were implemented and presented in [5] and [6]. We believe that the shown attacks do not pose a threat to vehicle drivers' safety since they require physical access to the vehicle and considerable knowledge - cutting a brake pipe is probably easier. Potential weaknesses of vehicle electronic were summarized in [7] and [13]. For vehicle-to-vehicle and vehicle-to-infrastructure security, a huge variety of research articles is available. The dominant standard is IEEE 1609.2 [3] and design approaches were summarized in [9]. Mechanisms for secure feature activation were presented in [12] and secure software downloads was analyzed in [10]. Component identification is considered in [11]. Secure architectures and secure hardware is researched and developed in the EVITA project [4] and in the OVERSEE project [8].

CONCLUSIONS

In this article we analyzed the security mechanisms for vehicles. The original question is answered by the evaluation results: data security for vehicles is required and it can be introduced in a commercially attractive manner. It is highly recommended to implement common countermeasures including electronic immobilizer, vehicle unlock system, component identification, and secure software download. It is also highly recommended to use standardized wireless interface security mechanisms and turn on the security features. It is finally recommended to introduce secure communication buses in terms of authentication in the mid-term future.

Manufacturer specific applications with an underlying financial business model might drive introduction of dedicated security solutions including security microcontrollers. These can then be used to increase the security level of remaining applications.

REFERENCES

1. Anderson, R. J., *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, Inc. 2001

2. Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., Shalmani, M. T. M., *On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme*, 28th International Cryptology Conference - CRYPTO 2008, Santa Barbara, CA, USA. August 17-21, 2008.

3. IEEE 1609.2-2006, *Standard for Wireless Access in Vehicular Environments* (*WAVE*)*, Security Services for Applications and Management Messages*, June 2006.

4. EVITA, e-safety vehicle intrusion protected applications, http://evita-project.org/.

5. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., *Experimental Security Analysis of a Modern Automobile*, Proceedings of the 31st IEEE Symposium on Security and Privacy, May 16-19, 2010 (Oakland).

6. Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W., and Seskar, I., *Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study*, in Proceedings of the 19th USENIX Security Symposium, Washington DC, August 11-13, 2010.

7. Lemke, K., Paar, C., Wolf, M. (Editors), *Embedded Security in Cars - Securing Current and Future Automotive IT Applications*, Springer-Verlag, 2006.

8. OVERSEE, Open vehicular secure platform, https://www.oversee-project.com.

9. Weimerskirch, A., Haas, J. J., Hu, Y-C., and Laberteaux, K. P., *Data Security in Vehicular Communications Networks*, VANET - Vehicular Applications and Inter-Networking Technologies, Wiley Blackwell, 2010.

10. Weimerskirch, A., *"Secure Software Flashing,"* SAE Int. J. Passeng. Cars - Electron. Electr. Syst. 2(1):83-86, 2009, doi:10.4271/2009-01-0272.

11. Weimerskirch, André, Paar, Christof, and Wolf, Marko, *Cryptographic Component Identification: Enabler for Secure Inter-vehicular Networks*, 62nd IEEE Vehicular Technology Conference, September 25-28, 2005, Dallas, TX, USA.

12. Schramm, K. and Wolf, M., "Secure Feature Activation," SAE Int. J. Passeng. Cars - Electron. Electr. Syst. 2(1)62-67, 2009, doi:10.4271/2009-01-0262.

13. Wolf, M., Weimerskirch, A., and Wollinger, T., *State-of-the-Art: Embedding Security in Vehicles*, EURASIP Journal on Embedded Systems, Special Issue on Embedded Systems for Intelligent Vehicles, 2007.

CONTACT INFORMATION

Dr. André Weimerskirch
escrypt Inc.
315 E Eisenhower Parkway
Suite 008
Ann Arbor, MI 48108
USA
andre.weimerskirch@escrypt.com

The Engineering Meetings Board has approved this paper for publication. It has successfully completed SAE's peer review process under the supervision of the session organizer. This process requires a minimum of three (3) reviews by industry experts.

ISSN 0148-7191

SAE Customer Service:
Tel: 877-606-7323 (inside USA and Canada)
Tel: 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
SAE Web Address: http://www.sae.org
Printed in USA