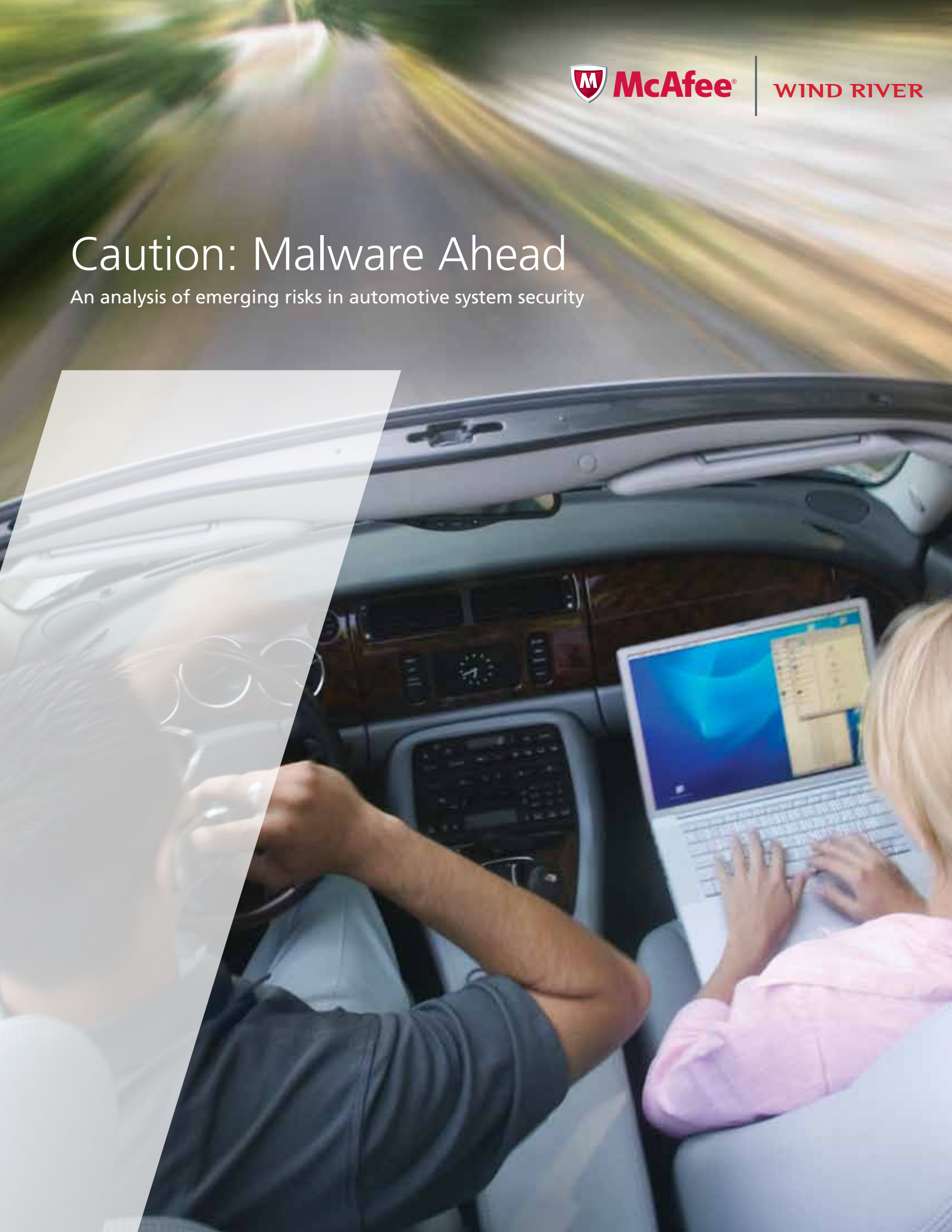


McAfee | WIND RIVER

Caution: Malware Ahead

An analysis of emerging risks in automotive system security

Caution: Malware Ahead

CONTENTS

Introduction

We are living in a world of incredible modern conveniences. Computer chips, embedded in all aspects of our daily lives, have made it possible to have access to all kinds of information when and where we need it. Through Internet protocols, these once dumb devices can now communicate with you and with each other in amazing, unprecedented ways.

According to Ericsson, there will be 50 billion IP-connected devices by 2020, up from 1 billion just a year ago. These are not just the omnipresent gadgets everyone is familiar with. The bulk of the 50 billion IP devices expected by later this decade will be embedded devices. These are often single-purpose devices such as cash registers, airport check-in kiosks, medical devices, access card readers, manufacturing equipment, programmable logic controllers, industrial control systems, and much more that is now being connected. As history has proven, security is an afterthought for most manufacturers. All these devices need proper security and management that is built in from day one.

Previously, embedded devices were essentially a one-way information feed—data was sent from the device from a purely diagnostic perspective (all almost universally out-of-band), but there was no pushing of data in-band. Additionally, these devices typically did very little to influence our lives. Now, policies and tasks can be pushed onto the device and data captured and reported back to one central console. And embedded systems have become a part of the very quality of our lives in automobile electronics, appliances, water and power systems, and the like. This phenomenon has exploded the threat scope for these devices, and security technologies, such as whitelisting and configuration control, combined with global threat intelligence gathered from millions of nodes, are becoming more than a nice to have—they are becoming a "must." These solutions are the first step toward providing complete security on embedded systems.

As embedded devices get on the network, security administrators want to know if they have the appropriate level of security. They want to control different policies on those devices through the same console that they use to control computers.

At McAfee, we are committed to securing embedded devices and the world beyond PCs. As such, we're partnering with Wind River and content experts in a variety of fields to analyze the security of embedded systems and provide sector-specific recommendations for securing these systems and keeping customers, as well as the general public, safe. This report focuses on embedded systems in automobiles and is the first in a series of reports on embedded device security. We hope you find it informative and useful.

Stuart McClure
Senior Vice President
and General Manager
McAfee

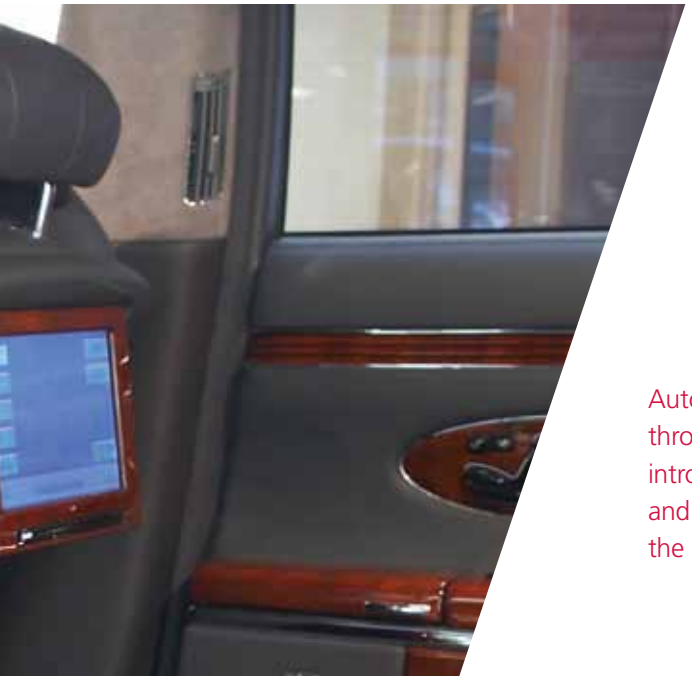
Embedded Devices in Automobiles

The automobile industry is continually adding features and packages that add more conveniences and the ability to personalize the driving experience. Consumers want to be continually connected, even in their cars, which is motivating automobile manufacturers to add more integration between cars and personalized devices such as smartphones and tablets.

New cars have the ability to be remotely started by a mobile phone, using a connection from the car and a request to start it from the key holder, through cellular network services or the Internet. This is just one example of how cars have become increasingly computerized and connected, both in the engine compartment and the dashboard console. As the popularity of these personalized connected systems increases, so does the need for security.

Convenience that was once measured by features like the dual-passenger climate control, heated seats, or the number of cup holders is now being delivered not only through good design, but also through specialized embedded technology. Personalized systems such as Bluetooth, GPS navigation systems, in-vehicle infotainment (IVI), and online help systems have become commonplace. Automakers distinguish their models through electronics, and the trend of introducing embedded microcontrollers and communication capabilities is on the rise.

These embedded devices are used in almost all areas of vehicles, including airbags, the radio, power seats, anti-lock braking system, electronic stability control, autonomous cruise control, communication system, and in-vehicle communication.



Automakers distinguish their models through electronics, and the trend of introducing embedded microcontrollers and communication capabilities is on the rise.

Numerous automakers offer cell phone-based communication, for example, GM's OnStar, Ford's SYNC, BMW's Assist, Lexus' Enform, Toyota's Safety Connect, and Mercedes' mbrace. Some car makers are also including Wi-Fi hot spots in their vehicles that provide Internet access to the passengers' devices.

What's interesting is that many of these embedded systems may also coordinate communication among themselves to bring the next level of personalization. These include:

- Unlocking the vehicle with a specific remote key will automatically adjust the power seats and mirrors for a given driver
- When traveling at higher speeds, the volume of an automobile's sound system automatically increases so the passenger can continue to listen clearly
- Based on a specific driver, the automobile can be throttled to keep the vehicle from driving over a set speed limit

Today, we're seeing bold new experiments, including Google's autopiloted cars and smart roads with sensors that report on traffic conditions and vehicle speeds. Experiments like these show the ongoing possibilities with coordinated, connected communication from all of the multifaceted systems within the automobile.

But there is a concern that as the industry advances, there has been little done to ensure the security of these systems. The first remote keyless entry systems did not implement any security and were easily compromised: a regular learning universal remote control for consumer electronics was able to record the key signal and replay it at a later time. And here's another security lesson from the past—in the early 1980s, car theft reached a high as car thieves bypassed the ignition lock by shorting the electric link to start the engine and drive the car away. By the late 1980s, cryptographic mechanisms were implemented to prevent such attacks.

Car Hacks Exposed

As more and more digital technology is introduced into automobiles, the threat of malicious software and hardware manipulation increases. There are many examples of research-based hacks that show the potential threats and depth of compromise that expose the consumer.

Last year, researchers of the University of California, San Diego, and the University of Washington demonstrated that critical safety components of a vehicle can be hacked if physical access to the vehicle's electronic components inside the passenger cabin is available. The proof-of-concept software, which they dubbed "CarShark," was developed using homemade software and a standard computer port. The scientists figured out how to hack into a modern car using a laptop. Recently, the same research team extended the scenario to remotely mount attacks via Bluetooth. This demonstration supports the need to consider the future security implications of embedded devices in cars and conveniences such as mobile phones, GPS, and Bluetooth.

Another attack was presented by researchers of the University of South Carolina and Rutgers University. Modern vehicles are mandatorily equipped with a tire pressure monitoring system. Radio frequency identification (RFID) tags are used within the tires to provide sensor data over wireless short-distance communication to the vehicle. The researchers showed that an attack can be mounted to track a vehicle and compromise passengers' privacy by tracking the RFID tags using powerful long-distance readers at around 40 meters. While no actual exploit in the field is known, and it is not yet understood if and to what extent this attack poses a threat for passengers' privacy, it is something that should be monitored.

Going one step further is to combine the CarShark attack and weaknesses of Bluetooth implementation in cars. Once the attacker guesses the Bluetooth PIN, the attacker could mount the CarShark attack. Other wireless devices like web-based vehicle-immobilization systems that can remotely disable a car could be manipulated in these situations as well. The immobilization system is meant to be a theft deterrent but could be used maliciously to disable cars belonging to unsuspecting owners.[1]

1 http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html

" Making automotive services more secure than comparable Internet services is really a challenge but is necessary. The automotive world will also have to harmonize the lifecycles of IT-security and automotive security components in the car."

—Winfried Stephan, Senior Consultant
T-Systems ICT Security Consulting and Engineering

There was another recent situation in Texas where it was reported that 100 vehicles were disabled from a remote disable system.[2] The system had been installed by the car dealership, however, was maliciously manipulated by a disgruntled former employee who remotely disabled the cars and wreaked havoc by setting off the car horns.

Security concerns stem from embedded systems integrated into these automobiles and also extend to aftermarket solutions. Recently, a provider of aftermarket GPS navigation systems was recording driver behavior and selling it to Dutch police to use the data to target speeding vehicles.[3]

There are also new tools, like Viper Smart Security, that use Internet mapping capabilities so owners can track their cars' whereabouts as well as a Facebook function that can be configured to send out instant updates on the car's activity. This could easily be used to gain access to the passengers' whereabouts, schedule, and routine. The security concern here is not with the automobile itself, but the correlation between tracking and social media that opens the question of consumer privacy. Based on gathering this information via Facebook updates, the details could be sold or used for other malicious activity against the individual.

Security testing and white hat hacking are ways to better understand the possible threat vectors and emerging exploits. One penetration tester, hired by a US-based municipal government, determined that several IP addresses used by the city's police department connected directly into a Linux device carried in police cruisers. Using little more than FTP and telnet commands, he then tapped into a digital video recorder (DVR) used to record and stream audio and video captured from gear mounted on the vehicle's dashboard. He was able not only to tap the live feeds coming from the two separate cameras mounted on the cruiser, but also to control the hard drive of the DVR.

Using default passwords that were hardcoded into the DVR's FTP server and disclosed in the support manuals he found with an Internet search, he was easily able to upload, download, and delete files that stored months' worth of video feeds.[4] In this situation, basic security could have prevented these results. Gathering the knowledge to hack into the recording system is one flaw but not ensuring that strong unique passwords were changed allowed the ability to manipulate and delete valuable evidence.

2 http://www.pcworld.com/article/191856/exemployee_wreaks_havoc_on_100_cars_wirelessly.html

3 http://www.npr.org/blogs/thetwo-way/2011/04/28/135809709/dutch-police-used-tomtoms-gps-data-to-target-speeders?sc=17&f=1019

4 http://www.theregister.co.uk/2011/05/03/cop_car_hacking

"Vehicles of all price segments are equipped with several electronic units, which in the near future, will boast dramatically increased computing performance and interfaces. Each interface serves as a motivator and means for an attacker to access the vehicle. We can expect new challenges to protecting the changing interface of embedded systems in cars. Vehicle makers have to solve the conflict of implementing security mechanism without losing customers acceptance. I expect a new chapter of car security in the next two car generations."

—Stefan Goss, Professor of Automative Technology
Ostfalia University of Applied Sciences

Infotainment and Networking Systems

The infotainment system is attractive for attackers, as it promises to be an area that closely integrates with an individual's personalized preferences or data. When that happens, there is the opportunity for financial gain for the right information at the right time. Infotainment systems often run standard software for embedded devices that is widely available, whereas other embedded units in a vehicle run mainly proprietary or specialized software.

Application stores, Internet access, or remote connected consumer devices could allow malware to be downloaded on the in-vehicle infotainment (IVI) system. IVI software platforms developed for worldwide use and standards such as GENIVI,[5] influence the architectures for better compatibility and integration. When these software standards are followed, it becomes increasingly important to protect against attacks and manipulation. Infotainment systems and cellular connection networks need to have security designed and incorporated into the development process.

As the growth of embedded systems and amount of code continues to grow to support the consumer demand for these systems, manufacturers now have a model that lets them upgrade or provide premium functions more readily.

Frost and Sullivan estimates that cars will require 200 million to 300 million lines of software code in the near future. The increasing feature set, interconnectedness with other embedded systems, and cellular networking or Internet connectivity can also introduce security flaws that may become exploitable.

A June 2011 article in the *San Jose Mercury News* examined the many ways that manufacturers are using electronics to increase comfort and safety and to gain a competitive edge. From luxury cars like BMWs to high-end electric cars like Tesla to everyday, affordable Fords, automobiles increasingly are coming with Internet-connected features to inform, entertain, and protect the driver.

5 http://www.genivi.org/

"Security will soon become an enabling technology for almost all innovations in cars. Most people would rather have malicious software running on their laptop than inside their car braking system. Thus, incorporating strong security solutions will give manufacturers a competitive advantage."

—Professor Christof Paar, University of Bochum, Germany, and University of Massachusetts Amherst, US

Consumer Considerations

- Which systems connect to the Internet or cellular network, and how are they secured?
- Is there a connection between the navigation system, GPS, and the car's critical electric systems?
- How is the Bluetooth system secured?
- What amount of personal data is uploaded to GPS, and is it being stored somewhere?
- Is there reporting via diagnostics on the system available to ascertain if it has been tampered with?
- Is there any local storage that saves or pulls information from my connected "smart" devices?
- In the event of a resell of the automobile, is there a way to reset all of the infotainment and integrated communication systems back to factory settings to ensure the removal of personalized settings or data?
- What is the manufacturer or cellular network provider's responsibility in the event that secured communications have been compromised?

The New Rules of the Road

The future is not as far away as we think. In June 2011, the Nevada legislature passed a law authorizing executives at the state's department of motor vehicles to begin coming up with a set of rules of the road for autonomous, or self-driving, vehicles.[6] Imagine taking a taxi in Las Vegas, and there is no driver—just a computer at the wheel. This may be the first step toward getting autonomous cars on the nation's roads.

Long gone are the days when the moving parts were just mechanical. We are now in the age of computer chips and systems that provide greater efficiencies in today's vehicles. Expanding beyond engine performance, the ever-growing number of embedded systems and integrated communications in modern automobiles have provided the convenience and personalization that consumers crave. But 10 years from now, will these same systems continue to hold consumer confidence, or will they quickly become another avenue for malware and breach of privacy data?

6 http://www.computerworld.com/s/article/9217967/Nevada_paves_way_to_getting_robotic_cars_on_the_road

Contributors

Stuart McClure, Senior Vice President and General Manager, McAfee

Stuart McClure oversees the McAfee Risk and Compliance product line, including sales, engineering, product management, product marketing, strategy, quality assurance, and customer support. Prior to McAfee, McClure was executive director of security services for Kaiser Permanente, a $34-billion health-care organization. He later served as senior vice president of global threats and research at McAfee, where he led an elite global security threats team and was founder, president, and chief technology officer of Foundstone, Inc. (now McAfee Foundstone).

Widely recognized for his extensive and in-depth knowledge of security, McClure is today one of the industry's leading authorities in information security. He co-authored *Hacking Exposed: Network Security Secrets & Solutions,* which has been translated into more than 30 languages and is considered one of the definitive computer security books. A widely published and acclaimed security visionary, McClure has more than 22 years of technology and executive leadership with profound technical, operational, and financial experience.

André Weimerskirch, Ph.D., Chief Executive Officer and President, ESCRYPT Inc.

Andre Weimerskirch, Ph.D., is chief executive officer (CEO), and president of US-based ESCRYPT Inc. and is in charge of the company's international activities. From 2004 to 2007, he held the position of chief technology officer (CTO) of ESCRYPT GmbH. He studied business information technology and mathematics at Darmstadt Technical University before receiving his Master of Science degree in computer science at Worcester Polytechnic Institute, US. He then received his Ph.D. from Ruhr-University of Bochum in applied data security. Since then, Weimerskirch has been involved in numerous industry projects focused on embedded data security and privacy, both in the US and Europe. He has published numerous articles in academic and industrial workshops and has contributed to several industry standards in the field of automotive data security. He is one of the main players in defining the security and privacy mechanisms for inter-vehicle communication in the US and Europe.

Marko Wolf, Ph.D., ESCRYPT GmbH, Germany

Marko Wolf, Ph.D., is senior security engineer at ESCRYPT GmbH, where he is focused primarily on embedded security and automotive security. He studied electrical engineering and computer engineering at the University of Bochum (Germany) and at Purdue University. After receiving his Master's of Science degree in 2003, he started his Ph.D. in trusted computing and vehicular IT security. Wolf completed his Ph.D. in 2008, with the first comprehensive work about vehicular IT security engineering. He is editor/author of the books *Embedded Security in Cars* (Springer, 2006) and *Security Engineering for Vehicular IT Systems* (Vieweg+Teubner, 2009), serves as program chair of the international "Embedded Security in Cars (ESCAR)" workshop series, and has published more than 30 IT security articles.

Professor Christof Paar, University of Bochum, Germany, and University of Massachusetts Amherst, US

Christof Paar is the Chair for Embedded Security at the electrical engineering department of the University of Bochum and is adjunct professor at the University of Massachusetts at Amherst. He is one of the leading international experts in industrial IT security. From 1994 to 2001 Paar led the Cryptography and Information Security Labs at Worcester Polytechnic Institute, US. He co-founded the Cryptographic Hardware and Embedded Systems (CHES) conference, the leading global event for applied IT security. Paar has extensive research and development experience with European and US companies. He is a board and advisory board member of several security companies and has rich experience with technology start-ups. Paar published more than 150 peer-reviewed publications in applied IT security and holds several patents.

Winfried Stephan, Senior Consultant, T-Systems ICT Security Consulting and Engineering

Winfried Stephan has been working in the field of security analysis and consulting for 15 years with T-Systems ICT Security Consulting and Engineering. He has spent 37 years in cryptography applications. He has spent the last 15 working on projects for the development and implementation of an immobilizer system and other automotive services.

Stefan Goss, Ph.D., Ostfalia University of Applied Sciences

Stefan Goss, Ph.D., has worked in the field of automotive electronics for 25 years. He was global head of development for telematics and instrumentations at Volkswagen from 2002 to 2007 and then global head of development automotive on-board diagnoses from 2007 to 2011 before becoming professor of automotive technology at Ostfalia University of Applied Sciences 2011.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

http://www.mcafee.com

McAfee
2821 Mission College Blvd.
Santa Clara, CA 95054
888 847 8766
www.mcafee.com