Press Release

Vienna, 03/06/2019

AUSTRIAN EXPERTISE FOR EUROPEAN CYBERSECURITY IN THE AUTOMOTIVE MARKET

Sparx Services CE and AIT launch new cybersecurity management system for the automotive sector

In February 2019 the EU launched a cybersecurity initiative designed to strengthen Europe in this critical sector. Already this has resulted in the launch of an Austrian product, THREATGET, jointly developed by the AIT Austrian Institute of Technology and Sparx Services CE. It helps developers identify threats at an early stage, allowing them to quickly assess the associated risks.

With the introduction of the new European security guideline according to ECE level (UNECE WP29; valid in the EU and partly in Asia), in future vehicle manufacturers will be required to verify the cybersecurity of their vehicle systems before their products can obtain type approval. From now on, manufacturers must prove every three years that they have applied a certified cybersecurity management system which covers all stages ranging from vehicle engineering through to documentation. Using the cybersecurity management system, manufacturers must test the cybersecurity of all vehicle types, identify and document potential threats, address security-critical problems and suggest solutions, and finally demonstrably verify that these problems have been solved.

THREATGET permits ECE conformity

This cybersecurity verification requires a modern tool which, for the first time, allows manufacturers to test their systems for ECE compliance. Peter Lieber, the founder of Sparx Services CE: “We have been working with AIT on this solution for two years and are proud that we can launch it on the market so quickly. THREATGET offers IT system designers effective support for security procedures designed to prevent potential cyber attacks, or threats.” The two partners contribute highly complementary areas of expertise to the project: AIT develops cutting-edge AI technologies for application in a critical market segment, and for years has been perfecting the THREATGET technology, while Sparx Services CE has extensive knowledge of model-based system development using the Enterprise Architect modelling platform. Helmut Leopold, Head of Center for Digital Safety & Security at AIT: “For the first time it is now possible to consider safety and security requirements as early as the system design phase. This offers European companies a considerable competitive advantage in an area of increasing importance.”

Set against the background of a strongly growing security engineering industry, THREATGET is targeted at vehicle manufacturers, as well as all companies involved in analysing vehicle architectures and systems in order to issue certification (e.g. the technical inspection association TÜV), as well as those working in the automotive training sector.

Artificial intelligence as a means of managing complexity

The database of potential threats and suggested solutions included in THREATGET is currently being updated and maintained as part of applied research and development activities. Users are provided with a list of potential problems and associated solutions for their specific system model (e.g. vehicle platform) which can then be implemented by a security engineer. This manually updated catalogue is complemented with updates of additional threat catalogues which, for example, are compiled by computer emergency response teams (CERT). In future, these external threat catalogues will be updated into the THREATGET catalogue automatically, using artificial intelligence (AI) algorithms. AI thus helps in managing the complexity of our increasingly networked systems. THREATGET ensures that in future the same basic security principle can be guaranteed for all manufacturers. Furthermore, manufacturers of special vehicles (e.g. for the security sector) will also be able to build on this basic principle, at the same time manually expanding specific security levels and rules in their own vehicle systems.

The global market for cybersecurity solutions is strongly growing because legal regulations are finally becoming compulsory and the attraction as targets for criminal activity is also growing. In contrast to other countries, Europe is clearly positioning itself as a market with a high degree of security awareness. “The framework conditions for our solution in the EU are very good. That’s why we want to quickly inform the market about our product, and exploit the competitive edge we have created,” Lieber concludes.

Further information: https://www.threatget.com (website will be online shortly) and https://cybersecurity.sparxservices.eu/.

Contact:

Dipl.-Ing. Rüdiger Maier, M.A.
Leitung Presse- und Öffentlichkeitsarbeit
Sparx Services CE / 4biz.at Consulting GmbH
Tel.: +43-1-9072627-204
ruediger.maier@4biz.at

Mag. (FH) Michael W. Mürling
Marketing and Communications
AIT Austrian Institute of Technology
Center for Digital Safety & Security
T +43 (0)50550-4126
michael.muerling@ait.ac.at I www.ait.ac.at

Mag. Michael H. Hlava
Head of Corporate and Marketing Communications
AIT Austrian Institute of Technology
T +43 (0)50550-4014
michael.hlava@ait.ac.at I www.ait.ac.at

Picture 1:
Helmut Leopold (left) and Peter Lieber (right) are pleased about the market launch of their joint product THREATGET - Picture: Wolfgang Franz

Figure 1:
This figure shows the data flow between different internal units in a vehicle. You can see the units "Radar" and "Camera" collecting data from the external environment. These are then processed by "Sensor Data Fusion and Decision Making Methods". The data is transmitted to a telematics system that controls the tracking of the vehicle. The telematics interacts with the central "Vehicle Control" to control the speed of the vehicle either by "Brakes" or by "Acceleration". Infotainment" connects to the telematics unit to provide the driver with information. All graphics: AIT

Figure 2:
THREATGET scans all elements and connectors in the model and identifies potential threats to the security mechanism. The example identifies 46 potential threats. THREATGET then summarizes all detected threats into one user interface. This interface has the following meaning:
Threats List: details of all detected potential threats
Threats Reference: A screenshot image of the source of detected threats.
Threat Severity: Evaluates the danger of detected threats to determine both impact and probability based on the parameters.

Figure 3:
THREATGET performs a risk assessment to calculate the risk level of all detected threats. These risk levels can be assigned via the THREATGET risk matrix.

About Sparx Services Central Europe

We are experts in planning, designing and implementing active Enterprise Architecture Management (EAM) systems based on Enterprise Architect (Sparx Systems). As an experienced sparring partner, we provide expert support to organisations in software-intensive industries. Our focus is on ensuring effective implementation, transparency and individuality for the EAM projects of our customers and their consultant ecosystem.
We use established technologies and open standards (Archimate, TOGAF, BPMN, …), best practices und current market challenges such as cyber security modelling. We also include the latest research findings (e.g. Threatget) of the Austrian Institute of Technology (AIT) to make security by design a reality. THREATGET offers effective guidance for system designers, allowing them to design security measures into the system in order to protect it against potential cyber attacks (“threats”). THREATGET automatically analyses cybersecurity threats and system vulnerabilities and suggests appropriate solutions.
https://cybersecurity.sparxservices.eu/

About AIT

The AIT Austrian Institute of Technology is Austria’s largest non-university research institution. With its eight Centers, AIT regards itself as a highly specialised research and development partner

for industry. In the context of comprehensive and global networking and digitalisation the Center for Digital Safety & Security is developing modern information and communication technologies (ICT) and systems in order to establish secure and reliable critical infrastructure. The Dependable Systems Engineering group at AIT has a long-standing history in addressing the interdependencies of safety, security and reliability and is developing new methods and tools to ensure comprehensive system security. AIT experts are also helping to shape future industry standards by contributing to, for example, ISO TC 22 (Automotive), ISO TC 299 (Robotics), IEC TC 56 (Dependability), IEC TC 62 (Medical), IEC TC 65 (Industrial Control), and AIOTI WG03 (M2M). The group also makes this accumulated experience and expertise available to customers through training and consulting.