ZVEI: Die Elektroindustrie

Position Paper

Cyber Security Challenges in a Changing Automotive Industry

August 2016

German Electrical and Electronic Manufacturers' Association

The objective of this paper is to increase management awareness about the nature of the challenges which the automotive industry faces as it moves towards large- scale deployment of automated and eventually autonomous, networked vehicles.

New features and business models come with new threats and challenges

The automotive industry faces increasingly complex and dynamic product development and vehicle operation environment challenges. The advent of autonomous vehicles systems coupled with the promise of networked vehicles offers opportunities for new business models that deliver customer value in ways the industry is only starting to explore. Every new business opportunity is accompanied by new business risks – in this case many of these new business risks are related to threats to security from cyber-space.

While the prospect of new business opportunities and new revenue streams are enticing, customer goodwill is based primarily based on customer trust in the brands that deliver customer value. The networked nature of the future mobility offerings makes automotive solution providers especially vulnerable to damage to customer trust, and therefore to the brand itself, from cyber-based attacks.

Today's cyber-attacks target financial companies, government organizations, defence, avionics and energy suppliers as well as large technology companies and political groups. As with these industries, the threats to networked mobility solutions will derive from a multitude of sources including organized cyber criminals, activists/hacktivists, terrorists and even state-sponsored cyber-attacks. Together these represent a multidimensional and growing challenge for security and safety of the automotive supply-chain, the vehicle itself, its occupants and associated networks.

Shift the focus from a pure development to a product lifecycle perspective

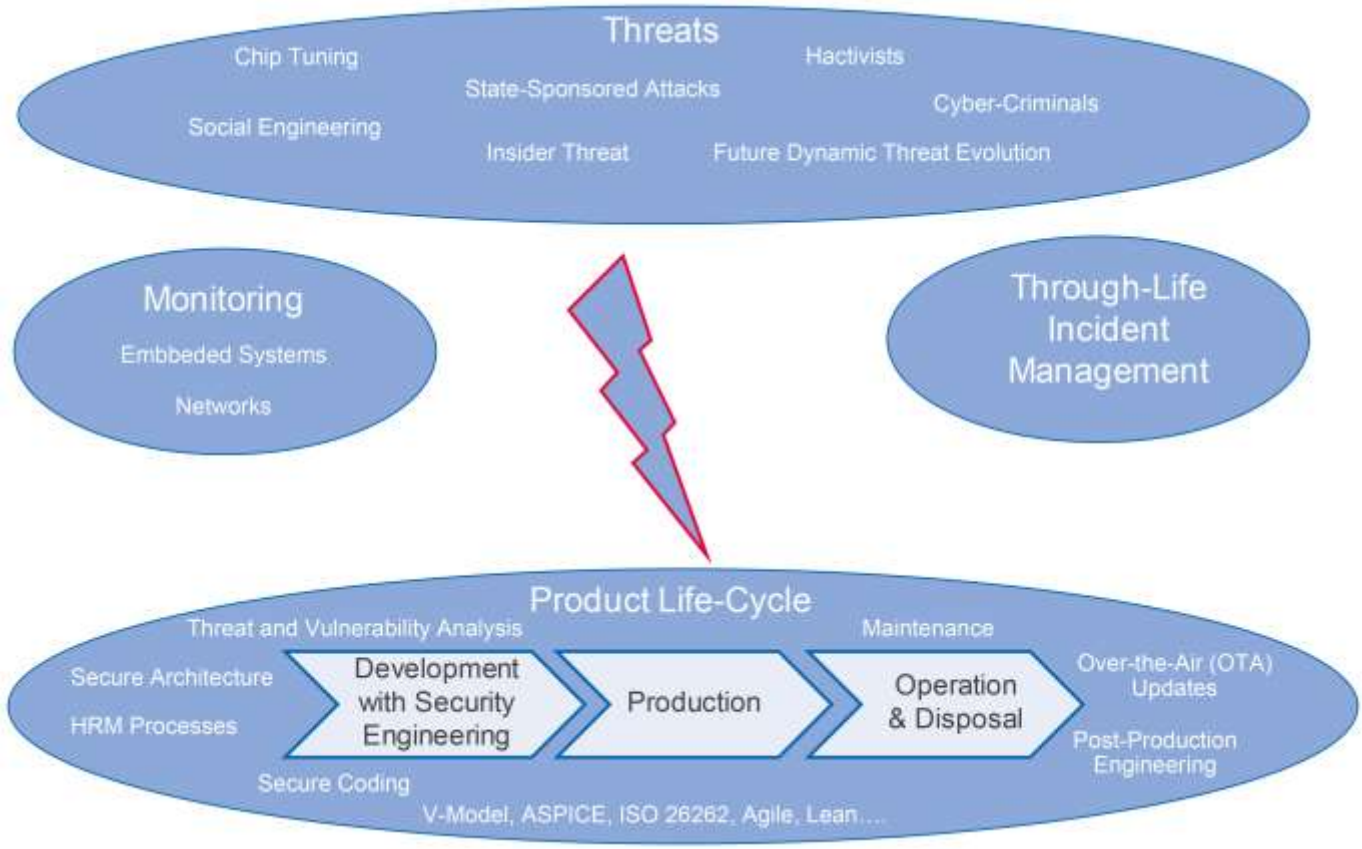
The current automotive industry focus on embedded systems security will be inadequate in the face of the threats which networked mobility solutions will need to address. The response to the future security threat will need to be expanded to address social as well as technical aspects of the threat spectrum. These social aspects include defence against social engineering and insider threat throughout the entire product life-cycle and not just in the product development cycle. Thus cyber-security for networked mobility systems will need to address through-life security management, from initial innovations through to system retirement and disposal. In particular, network traffic monitoring and incident monitoring in the entire complex system environment, including incident detection in all components and rapid incident response processes, will become mandatory. Over-The-Air (OTA) updates will become obligatory in order to support timely responses to future attacks. This makes the engineering challenge for cyber security inherently more dynamic and complex compared to the engineering challenge for safety related development.

Operational processes are a major building block of security strategies

Cyber security challenges in post-production operational environments will become a major focus of cyber security defence in the future. This is a new paradigm for organizations that are used to safety-based approaches where threats can be identified and addressed in the development process before production starts. Threats in cyber-space cannot only be identified effectively in the design process, so operational processes need to be designed to have capabilities that enable adequate and timely responses to dynamic threats scenarios over the operational life-time of the vehicle and the networks it operates in. The automotive industry does not have the organizational functions or capabilities required to do this today.

Embedded and backend security must be considered hand in hand

In the future we can envision attack scenarios where the networks upon which mobility solutions rely are themselves the target of attack, rather than the embedded systems, vehicle data, or automobile occupant data in the individual vehicles. The monitoring and defence of these networks is unlikely to be in the power of single OEMs if the potential of the networked vehicles and mobility solutions are to be realised. Cross-industry collaboration and related business models will need to be established to be effective in responding to these network-focused attacks. These types of attacks may even fall in the realm of attacks on critical infrastructure, which will therefore inevitably bring government regulation to these networks.



Organizations and processes must evolve to handle threat scenarios over the complete lifecycle

Management in the automotive industry needs to prepare their organization to address these new challenges. A key future capability of the automotive organizations will be the ability to maintain acceptable performance levels for mobility solutions while under constant attack from dynamically evolving threat scenarios. Achieving the requisite levels of performance will require adding new and expanded skill sets, including a greater collaboration capability across industries to defend automotive related cyber-space and ultimately the organizations own reputation.

ZVEI - German Electrical and Electronic Manufacturers' Association

The 'ZVEI - German Electrical and Electronic Manufacturers' Association' promotes the industry's joint economic, technological and environmental policy interests on a national, European and global level. The ZVEI represents more than 1,600 companies, mostly small and medium-sized enterprises (SMEs). The sector has 841,000 employees in Germany plus 665,000 employees all over the world. In 2013 the turnover was approximately Euro 167 billion.

The electrical and electronics industry is the most innovative and the second largest industry sector in Germany. Every third innovation in Germany´s manufacturing sector stems from solutions of this sector. 20 percent of all industrial R&D spending come from this industry.

ZVEI - German Electrical and Electronic Manufacturers' Association
Platform Automotive
Lyoner Strasse 9
60528 Frankfurt am Main, Germany
Telephone: +49 69 6302-276
Fax: +49 69 6302-407
E-mail: zvei-be@zvei.org
www.zvei.org

Contact:
Dr. Stefan Gutschling