A MODEL FOR SAFE AND SECURE EXECUTION OF DOWNLOADED VEHICLE APPLICATIONS[1]

Phu H. Phung*, Dennis Kengo Nilsson†

*Department of Computer Science and Engineering
Chalmers University of Technology, Sweden
phu.phung@chalmers.se
† Syncron Japan
dennis.nilsson@gmail.com

ABSTRACT

Existing secure protocols and code signing mechanisms for vehicle systems to download and install software over the air certify only the origin and the integrity of software; thus, they do not address errors that might not be detected in the development process and cannot ensure that the downloaded software do not contain malicious code. In this paper, we identify such possible threats by developing a threat model for the vehicle software architecture. We propose countermeasures against the threats by preventing or modifying inappropriate behavior caused by, e.g., malicious or poorly designed applications. We propose a model to deploy the approach which is based on modifying the application at the wireless gateway in the vehicle before being installed. As a result, security policies are embedded into the application and intercepts security relevant execution events. Thus, the execution of downloaded vehicle applications is monitored to ensure the safety and security for the vehicle system and to detect potential cyber attacks.

[1] *In Proceedings of the 2010 IET Road Transport Information and Control Conference (RTIC'10), London, UK*