Attack tree construction: an application to the connected vehicle

K. Karray, J-L Danger, S. Guilley, A. El Aabid
Telecom ParisTech
France

Abstract

Remote connectivity of today's and future cars have increased their capabilities of autonomy and safety, but also their attack surface, as reported by many research papers. In the automotive domain, the security has a direct impact on the users safety. Thus, the management of risk is becoming the main concern of automotive manufacturers, especially for the future fully connected and autonomous cars. One possible way to quantify the overall risk of a system is the systematic construction of attack graphs and attack trees. These formalism are presented as one of the possible solutions in the new Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (SAE-J3061). In this paper we propose to use a graph transformation to formally model the car architecture and its state evolution in order to study possible attack paths. The resulting attack trees are then used to estimate the overall risk of the system. Consequently, it becomes possible to study improvements to build a more secure architecture.The proposed method is designed to support the conceptual phase of the vehicle's cyber-physical system. We illustrate the method on a small example to show how it is possible to prove its efficiency.