Quantifying Risks to Data Assets Using Formal Metrics in Embedded System Design

Maria Vasilevskaya and Simin Nadjm-Tehrani

Dept. of Computer and Information Science, Linköping University, Sweden
e-mail:[maria.vasilevskaya, simin.nadjm-tehrani]@liu.se

May 12, 2015

Abstract

This work addresses quantifying security risks associated with data assets within design models of embedded systems. Attack and system behaviours are modelled as time-dependent probabilistic processes. The presence of the time dimension allows accounting for dynamic aspects of potential attacks and a considered system: the probability of a successful attack may change as time progresses; and a system may possess different valuable data assets as its execution unfolds. For system modelling, we employ semi-Markov chains that are a powerful tool to capture system dynamics. For attack modelling, we adapt prominent formalisms of attack trees and attack graphs. These models are used to analyse and quantify two important attributes of security: confidentiality and integrity. In particular, likelihood/consequence-based measures of confidentiality and integrity losses are proposed to characterise security risks to data assets. Identifying these risks in embedded systems is especially relevant in order to be able trading them off for other criteria, e.g. resource footprints. In our method, we consider attack and system behaviours as two separate models that are later elegantly combined for security analysis. This promotes knowledge reuse and avoids adding extra complexity in the system design process. We demonstrate the effectiveness of the proposed method and metrics on real smart metering devices.