Abstract

Cyber-physical systems are becoming increasingly advanced and complex. At the same time, following an opposite trend, traditional approaches to manage their security and safety are progressively becoming obsolete and unusable. Facing distributed systems, made up of heterogeneous components, which often open up a large attack surface and have low computational capabilities, flexible and dynamic solutions are needed, i.e., solutions able to react quickly to changes in the network or to contrast incoming cyber attacks.

Cybersecurity has become crucial, especially since these systems are also safety-critical. A compromise of their security, as well as undefined behaviours due to faults or cyber attacks, can cause great damage, with potential loss of human lives.

Since manual approaches to handle such systems are unoptimised, error-prone, and time-consuming, the only possible solution, in this context, is to automate the process of network management of the security functions required to protect these systems. On the other hand, as a further requirement, automated solutions must be reliable and allow for formal verification. Any adopted automatic process must, in fact, be rigorous and deterministic.

In this thesis work, we set ourselves this goal. Specifically, the aim has been to identify formal methods and techniques to be used in the process of automating cybersecurity management and security verification in Cyber-Physical Systems.

On the one hand, this work proposes new mechanisms to formally model the key security functions of a network. A correct formalisation, for example, of the traffic that can flow in the network or of the main network security policies and functions, is fundamental and can be used to solve network related management tasks such as allocation, configuration, and verification of necessary security solutions. We followed this approach and we proposed new formal models for solving two policy-based management tasks, well known in the literature: (i) the problem of automatically

configuring security functions (such as firewalls and packet filters) to meet some requirements expressed at a high level by the network administrator, and (ii) the analysis and automatic resolution of anomalies affecting a firewall policy.

On the other hand, we also focused on applying formal methods to verify state of the art security protocols for cyber physiscal systems. We started with protocols in two specific cyber physical domains, Vehicle-to-Everything (V2X) communications and Internet of Things (IoT) networks, and we formally built abstract models to assess their security. Precisely, we formally verified whether they actually satisfy the expected security properties or some attacks are possible against their design. This was done using automatic tools such as Proverif and Tamarin.