DESIGN AND DEVELOPMENT OF AN ASSURANCE METHODOLOGY FOR SECURITY CERTIFICATIONS IN HIGHLY DYNAMIC ARCHITECTURES

Matteo Cavagnino – 961707

RELATORE
Prof. Claudio A. Ardagna

CORRELATORE
Dr. Nicola Bena

The advent of increasingly dynamic and distributed systems continuously improves how end-users benefit from online services; the more a system is dynamic, the higher its flexibility and the better the provided service. Therefore, in recent years, ICT systems evolved at a fast pace, moving from static web services to the cloud, edge and finally, Internet of Things (IoT). These architectures granted a better user service thanks to the resources they offer. Moreover, thanks to its flexibility, IoT is rapidly increasing in popularity, counting tens of billions of devices worldwide and even tens of thousands in a single interconnected system. Unfortunately, such extended and pervasive infrastructures come with many cyber-security weaknesses and a general (perceived) lack of trustworthiness. To this day, one of the ways to address this need for trustworthiness is by means of certification, where a component's certificate is exhibited to others to allow the authentication of the same.

A cyber-security certificate is obtained after long, resource-intensive and costly certification processes, mostly executed by third-party authorities, that never really changed after the definition of a limited number of standard ones (e.g. Common Criteria). The issue with traditional schemes is their heavy reliance on the staticity of the certified product; any change in the product's configuration, software or context has a high chance of invalidating the certificate and then requiring to re-execute the certification process from scratch. This issue was alleviated by numerous pieces of research in Cloud and Edge environments but never completely solved, and with IoT, the problem got progressively more evident. The problem with dynamic architectures lies in their dynamicity; a single dynamic system such as Cloud, Edge or IoT may undergo several changes during its life cycle, and such changes might interest any architectural layer. For example, the changes in a system's configuration vary from software security updates and hardware upgrades to deployment context changes (e.g. the physical relocation of a device or machine, which could increase the exposure to threats). In addition, more issues emerge from the most pervasive structures, such as IoT systems, where the deployment environment might change, and the high number of low-power devices deployed that need to handle potentially sensitive data could be easily overwhelmed by a resource-heavy testing process.

This thesis aims to take an important step toward a certification scheme for systems that may undergo a high number of changes during their life cycle; the proposed scheme reduces redundancy, time and resources needed to obtain a certificate.

The work is structured as follows.

1. **Study of the state of the art of certification schemes** to visualise better the background and context considered in this thesis, highlighting the current research focus and, most importantly, gaps; such study mainly focuses on Cloud computing, Edge computing and Internet of Things paradigms;

2. **Definition of the methodology of the proposed certification scheme,** where the main building blocks of the certification process are introduced and thoroughly formalized. Two new certification components are introduced: the *scoring system* and the *trigger* component. We present such components as new core elements of the certification process, aiming to increase automation and reduce the effort needed to re-evaluate a system. Furthermore, the methodology includes revisiting the formal models of the other core components, such as *non-functional properties* and their *attributes*, *evidence collection*, and the released *certificate*. Each component is bound to the others with the use of specific functions to obtain a complete *certification model* ultimately;

3. **Execution of the proposed certification scheme over a real-world-inspired scenario,** where we show each of the scheme's steps and the relative artefacts generated, accurately describing and formalizing the core elements, finally leading to the certificate's release.

The work in this thesis represents a first step toward the definition of a certification scheme for highly dynamic systems by changing how the problem is approached. Regardless, the outcome of this thesis work leaves space for future developments, from the evolution of the major phases of the process to the integration with traditional certification schemes, allowing the proposed solution to operating on systems previously certified with other schemes.