


Doctoral Dissertation
Doctoral Program in Computer and Control Engineering (31st cycle)

Software Attestation with Static and Dynamic Techniques

Alessio Viticchié

* * * * * *

Supervisors
Prof. Antonio Lioy, Supervisor
Cataldo Basile, Ph.D., Co-supervisor

Doctoral Examination Committee:
Prof. Bjorn De Sutter, Referee, Ghent University
Prof. Stefano Paraboschi, Referee, Università degli Studi di Bergamo
Bart Coppens, Ph.D., Ghent University
Prof. Claudia Raibulet, Università degli Studi di Milano-Bicocca
Prof. Riccardo Sisto, Politecnico di Torino

Politecnico di Torino
17 July 2019

I hereby declare that, the contents and organisation of this dissertation constitute my own original work and does not compromise in any way the rights of third parties, including those relating to the security of personal data.

. . . . . .

Alessio Viticchié

Turin, 17 July 2019

Abstract

The spread of software tools in every field of modern daily life is forcing the need for effective software integrity protection techniques. This kind of protection is becoming necessary in order to avoid economic threats for producers and security threats for users. Software protection is particularly needed when applications run in untrusted environments (e.g. mobile devices or personal computers). Indeed, it is non-trivial to ensure application security when the attacker controls the entire execution environment. This scenario has recently defined the new class of attacks: Man-At-The-End (MATE). The application of protection techniques against these attacks could be challenging for developers because they often have limited knowledge in software protection. Furthermore, protections techniques presented in literature have critical limitations when applied in MATE scenarios (e.g. not effective enough, not practical or too complex to be applied). As a final issue, modern systems are very diverse, and their configurations are highly varied. Consequently, software protection techniques must be independent of any underlying configuration in order to suit modern systems. Hence, it is worth to investigate new software protection techniques and automatic methods to apply them to general applications.

This thesis presents *Software Attestation* as a valuable integrity monitoring technique. This work aims at defining the general model of the protection methodology in order to provide a reference architecture and workflow. From the general, abstract model, this work defines the specific versions of the protection as model instantiations that select particular software aspects as assets to protect, on which integrity evidence is computed. Hence, this thesis investigates *Static* and *Dynamic* software attestation as interesting instantiations of the general model. Both these two flavours of attestation are investigated starting by defining the requirements, then proposing possible implementations and finally performing the validation of the requirements and the security analysis. All this discussion aims at providing a comprehensive study about the practical applicability of the protection model. Finally, the dissertation aims at demonstrating that the software attestation model is valid for protection and can be used to achieve more complex and robust protection methodologies by combining it with other methods. Furthermore, this thesis underlines the issues that may come from the actual instantiation of the software attestation model. Hence, the discussion wants to present, once more, that threats generate from practical specifications even when models are theoretically robust.