PhD in Computer and Control Engineering

Research Title: Improving the dependability and resilience to cyberattacks of next generation computer networks

SESSION: SUMMER 2019

Funded by	DAUIN

Supervisor	Riccardo Sisto - riccardo.sisto@polito.it

Contact	http://netgroup.polito.it

Context of the research activity	The increasing pervasiveness of computer systems has led to the proliferation of distributed safety-critical systems connected to the internet. Smart Grids, autonomous driving vehicles, IoT smart devices, and Industry 4.0 are just examples of this trend. Ensuring dependability and resilience to cyberattacks of these distributed systems is as important as challenging. The upcoming evolution of the networks towards 5G/IoT and the higher flexibility and dynamicity made possible by virtualization and Software-Defined Networking (SDN) bring new security threats and challenges, but at the same time offer new opportunities for protection, by enabling fast dynamic reconfiguration in response to cyberattacks. In order to fully exploit such new opportunities, it is necessary to automate the network reconfiguration process as much as possible. In fact, the traditional approach of manual network management is not compatible with the need of fast real-time reconfigurations, especially because each change in network configuration has to be followed by a verification of the correct network behavior, traditionally done by time-consuming manual tests. Achieving a high level of automation while providing at the same time a high assurance that network security policies are correctly enforced is an open research challenge. On the one hand, some researchers have started developing automated security policy refinement processes. On the other hand, other researchers (including our research group) have proposed automated network verification techniques based on formal approaches. However, an

	efficient way of combining the two techniques together is not yet available, because network verification has the disadvantage that, if a policy violation is found, a correction of the error (e.g. a change in the configuration of network components) has to be found manually. In rapidly evolving systems, such as the ones based on NFV and SDN, where network reconfigurations can be triggered frequently and automatically, manual steps are undesirable because they can limit the potential dynamics of these networks.

Objectives	The main objective of the proposed research is to advance the state of the art in the techniques for reaction to cyberattacks in virtualized networks, by providing mechanisms for automated, fast, and provably correct policy-based reconfiguration of virtualized networks. Formal methods will be exploited to achieve correctness by construction, rather than a-posteriori verification. The main challenge is how to formally model next-generation networks, their components, and policies, in such a way that the models are accurate enough, and at the same time amenable to fully automated and computationally tractable approaches for ensuring safety and security by construction. The candidate will explore a correctness-by-construction approach, alternative to formal verification, but based on formal models of network components similar to the ones used for formal verification. Instead of just checking that the behavior of a fully defined model satisfies some policies (verification), some aspects of the model (e.g. the configurations of some network components) are left open, and a solution that assigns these open values is searched (formal correctness by construction). In order to achieve this goal, Satisfiability Modulo Theories (SMT) solvers will be considered. These tools are good candidates for this purpose because they are very efficient in determining if a set of logical formulas is satisfiable or not, and if it is, they can also efficiently find assignments of free variables that make the logical formulas true. The main idea to be explored in the research is to exploit an SMT solver as backend for building a tool that can automatically and quickly synthesize correct-by-construction configurations of NFV- and SDN-based networks that implement given policies. This implies finding ways of encoding the correct construction problem of such networks as an SMT problem that can be solved efficiently enough. The candidate will exploit the experience already gained by the Netgroup with SMT solvers for fast formal verification of NFV-based networks. Till now, no researcher has yet tried this approach (the previously proposed solutions for automatic reconfiguration of networks use non-formal approaches or specially crafted algorithms and heuristics, and are limited to the configuration of just one type of function, e.g. firewall). If successful, this innovative approach can have high impact, because it can improve the level of automation in re-configuring next generation networks and at the same time provide the high assurance levels required by safety-critical distributed systems.

Skills and competencies for the development of the activity	In order to successfully develop the proposed activity, the candidate should have a strong background in computer networking, a good knowledge of network security, and good programming skills. Some knowledge of formal methods can be useful, but it is not required: the candidate can acquire this knowledge and related skills as part of the PhD Program, by exploiting specialized courses.