ABSTRACT

This habilitation thesis presents the professional activity and the scientific work of the candidate after the defence of his PhD thesis at the Technical University of Cluj-Napoca on the 26th of May 2009, and the title confirmation by the Ministry of Education and Research on the 25th of August 2009. The research activities within the candidate's PhD thesis were focused on the composition of security protocols, on the analysis of multi-protocol attacks, and on the application of these concepts in the design of novel security protocols.

Conversely, the candidate's activities after obtaining his PhD degree in 2009, and starting with 2010 have been focused on the security, resilience, analysis and design of Networked Critical Infrastructures (NCI). The candidate's research interests for this particular field have been cultivated by a 3-year post-doctoral research grant (from Sept. 2010 to Sept. 2013) awarded by the Institute for the Protection and Security of the Citizen (IPSC), Joint Research Centre (JRC) of the European Commission, located in Ispra, Italy.

The research started under this grant is currently continued under a 4-year (March 2014 - March 2018) FP7 Marie Curie project that the candidate was awarded in 2014.

This habilitation thesis presents the candidate's original contributions to improving the security and the resilience of NCI. The presented results have been documented in top peer-reviewed journals (including Communications of the ACM, IEEE Transactions on Emerging Topics in Computing, IEEE Systems Journal, International Journal of Critical Infrastructure Protection, Security and Communication Networks) and in the proceedings of scientific conferences and workshops (including IEEE/IFIP Networking, ADHOC-NOW, IFIP CIP, EuroSec). The habilitation thesis at hand is structured according to the following chapters.

The first chapter summarizes the candidate's contributions and presents the thesis outline.

The second chapter presents a novel cyber-physical *Experimentation Platform for Internet Contingencies* (EPIC) aimed to enable performing security studies on NCI. EPIC is a modern scientific instrument that can provide accurate assessments of the impact that cyber-attacks may have on the cyber and physical dimensions of NCIs. To meet the complexity of today's NCIs, EPIC uses an emulation testbed based on Emulab to recreate the cyber elements of a NCI and software simulators for the physical components. Compared to other testbeds its main advantage is that it can support very accurate, real-time, repeatable and realistic experiments with heterogeneous infrastructures. This powerful scientific instrument can be used to study multiple interdependent infrastructures and provide insights about the propagation of faults and disruptions. The thesis presents several case studies showing how EPIC can be used to explore the impact of cyber-attacks and Information and Communications Technology (ICT) system disruptions on physical processes such as power plants, chemical plants, electricity grids and railway systems.

The third chapter presents a novel Cyber Attack Impact Assessment (CAIA) methodology inspired from the field of System Dynamics. The approach compares the behavior of complex physical processes in the presence and in the absence of accidental or deliberate interventions in

order to evaluate the significance of cyber assets. These interventions may be attributed to cyber attacks, but also to faults and random events. The main advantage of the developed technique is that it is applicable to large-scale, hierarchical, and heterogeneous installations, but most importantly that it may be used to evaluate the impact of disturbances, e.g., cyber attacks, in a wide variety of production systems. Since the technique relies on input data, i.e., one-way communication from physical process to assessment engine, and it leverages measurements that are already available in specific network points, e.g., historian databases, it may be applied in critical production environments where the impact of various control commands may be assessed and quantified in the attempt to identify critical control variables. This is a significant aspect of the presented technique which differentiates it from existing, intrusive methodologies. Furthermore, the output of CAIA can be used by various network planning and risk assessment techniques in order to ensure the implementation of important protection mechanisms of critical system components.

The fourth chapter presents a novel NCI security-aware network design methodology. The approach is formulated as an integer linear programming (ILP) problem that minimizes the costs of the network while taking into account a variety of constraints which are essential prerequisites for the correct functioning and for the security of NCI. The ILP model assumes that traffic between different NCI end-points, e.g., sensors and hardware controllers, is routed across a communication infrastructure in which nodes are installed at locations selected from a set of feasible sites. This selection accounts for the cost of bandwidth, the cost of provisioning nodes and security equipment, as well as the capacity of nodes and of communication links. Furthermore, the ILP model provisions NCI traffic and communicating end-points into security zones and conduits as defined by ISA-62443. Finally, real-time communication constraints enforce that NCI-specific communication requirements are satisfied.

The fifth chapter describes a novel resilient NCI design methodology that accommodates real-time delivery of data packets, reliability of communications, and communications resilience. The network design is formulated as an Integer Linear Programming (ILP) problem that accounts for data flows between different cyber assets, as well as traditional NCI design requirements pertaining to real-time traffic, reliability, and resilience. The technique encompasses a K-resilience configuration factor to enable the deployment of K back-up communication paths for each main communication path. In this respect, for each data flow the technique defines a resilient communication group (RCG), which encompasses the main data flow's communication path as well as all of its associated back-up communication paths. Reliability constraints are adopted from the traditional field of system safety, and are adapted to the present problem through the linear transformations proposed by Chiang et al. in the field of fuzzy logic optimization. The developed ILP problem is experimentally evaluated from several perspectives targeting the impact of costs, resilience, and reliability, on the generated ILP architecture.

Considering that software vulnerabilities constitute significant parts of any attack vector, the candidate developed a novel approach for assessing the software vulnerabilities of NCI services. The sixth chapter presents the developed methodology, which was embedded into an innovative tool called ShoVAT to complement the features exposed by Shodan – one of the most popular Internet service search engines available today. ShoVAT takes the output of traditional Shodan queries and performs an in-depth analysis of service-specific data, e.g., service banners, in order to identify software version numbers, product vendor, product name, etc. By leveraging specially

crafted heuristics ShoVAT rebuilds Common Platform Enumeration (CPE) names for each identified product and it extracts the list of Common Vulnerability Entries (CVE) from National Vulnerability Database (NVD). Since Shodan also provides historical data on indexed services, ShoVAT can explore historically the degree of service exposure, i.e., the number and severity of discovered vulnerabilities.

The seventh chapter presents the candidate's professional and research development plans in the short and in the long-term.