Control Architecture to Provide E2E security in Interconnected Systems: the (new) SHIELD Approach

Andrea Fiaschetti[1], Andrea Morgagni[2], Andrea Lanna[1], Martina Panfili[1], Silvano Mignanti[1], Roberto Cusani[3], Gaetano Scarano[3], Antonio Pietrabissa[1], Vincenzo Suraci[4], Francesco Delli Priscoli[1]

***Abstract*—**Modern Systems are usually obtained as incremental composition of proper (smaller and SMART) subsystems interacting through communication interfaces. Such flexible architecture allows the pervasive provisioning of a wide class of services, ranging from multimedia contents delivery, through monitoring data collection, to command and control functionalities. All these services requires that the adequate level of robustness and security is assured at End-to-End (E2E) level, according to user requirements that may vary depending on the specific context or the involved technologies. A flexible methodology to dynamically control the security level of the service being offered is then needed. In this perspective, the authors propose an innovative control architecture able to assure E2E security potentially in any application, by dynamically adapting to the underlying systems and using its resources to "build the security". In particular, the main novelties of this solution are: i) the possibility of dynamically discovering and composing the available functionalities offered by the environment to satisfy the security needs and ii) the possibility of modelling and measuring the security through innovative technology-independent metrics. The results presented in this paper moves from the solutions identified in the pSHIELD project and enrich them with the innovative advances achieved through the nSHIELD research, still ongoing. Both projects have been funded by ARTEMIS-JU.

***Keywords*—**Dynamic Composability, E2E Security, Common Criteria, Attack surface metrics, Optimization

I. Introduction

TECHNOLOGICAL advances in computational capabilities along with improvement in communication technologies have enriched the market with a new class of SMART devices that can be used in every application domain, ranging from entertainment, trough automotive and manufacturing, to energy or health.

These devices (i.e. sensor nodes, SMART actuators, programmable controllers, small computing platform, etc.) are commonly referred to as Embedded Devices or Embedded Systems (ESs) and their peculiarities are: i) a reduced size, ii) the possibility of implementing specific functionalities with limited resources and iii) the possibility of interconnecting with other devices to create more complex systems.
Leveraging these peculiarities, several industrial domains have started to massively deploy ESs networks to realize a plenty of tasks, no longer limited to a specific functionality but extended up to end-to-end behaviors.

In order to drive the European research towards an improvement of ES technologies, the European Commission, within the Seventh Framework Programme (FP7) has established the ARTEMIS-JU, a technological initiative in charge of defining and promoting a specific roadmap towards clear and focused objectives [1]. One of these objectives is the development of new technologies and/or strategies to address E2E Security in the context of ESs, with particular care to:

- Solutions oriented to systems certification,
- Cost reduction
- Re-use and re-engineering of non-recurring solutions.

In this context the authors, starting from their academic and industrial backgrounds, have conceived the SHIELD Framework ([2]), an architectural paradigm and design methodology able to address security aspects potentially in each and every domain where ESs (or networks of interconnected ESs) are deployed to provide specific services.
As it happens for communication networks, where modular and cognitive architecture are adopted to provide flexible E2E services that dynamically satisfy the desired level of QoS (see [6]), similarly the interconnection of ESs may require the adoption of a modular and cognitive approach to provide E2E security functionalities that dynamically satisfy the desired "security level" form the end-user.

Thus, the main novelty of the presented approach is the possibility of realizing a "known and predictable" E2E security behavior starting from the composition of individual, atomic elements. In spite of this, the main features of the proposed SHIELD framework are:

1 Authors are with the Department of Computer, Control and Management Engineering "A. Ruberti" at "Sapienza" University of Rome, Via Ariosto 25, 00185 Rome, Italy (e-mail: surname@diag.uniroma1.it).

2 Author is with Selex Electronic Systems (Finmeccanica Company), Via Laurentina 760, 00143 Rome, Italy (e-mail andrea.morgagni@selex-es.com)

3 Authors are with the Department of Information, Communication and Electronic Engineering (DIET) at "Sapienza" University of Rome, Via Eudossiana 18, 00184 Rome, Italy (e-mail: name.surname@ uniroma1.it).

4 Author is with Università degli studi e-Campus, Via Isimbardi 10, Novedrate, 22060, Italy (e-mail vincenzo.suraci@uniecampus.it)

- **modularity** and **expandability** (i.e. the possibility of composing elements together),
- **cognitiveness** and **flexibility** (i.e. the possibility of dynamically adapting to the specific context)
- **technology independence** (i.e. the possibility of abstracting the controlled components in order to measure and provide security in any environment).

The basic approach has already been presented in [2] as preliminary result of the pSHIELD research project ([11]); in this paper an improvement with respect to the basic approach is shown, mainly basing on the recent advances achieved in the execution of the nSHIELD project ([12]), which represents the second phase of the SHIELD Roadmap.

In order to describe the SHIELD approach to E2E security, the rest of the paper is structured as follows: in Section 2 the SHIELD methodology (as presented in [2]) is recalled and in Section 3 the SHIELD behavior as a closed-loop control system is depicted in detail. In Section 4 the innovative control approach to assure E2E security is then presented, and in Section 5 an example is provided. Finally in Section 6 conclusions are drawn.

II. The SHIELD Methodology

The main purpose of the SHIELD methodology is to provide an architectural solution and a design paradigm to enable the Composability of atomic (Security) functionalities in Complex Systems.

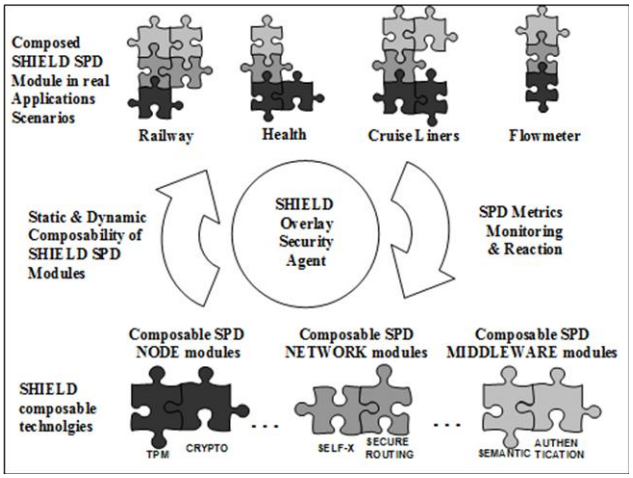

Fig. 1 SHIELD Methodology

A trivial representation is provided in Fig. 1. The *SHIELD modules* can be represented as pieces of a puzzle, which perfectly fits each other thanks to common interfaces. Each module implements a Security technology or a specific Security functionality. As an example, in Fig. 1 at *node level* there are two modules: Trusted Platform Module and Crypto Technology, at *network level* there are two functionalities: self-x algorithms and secure routing, and at *middleware level* there are two other services: semantic management and authentication.

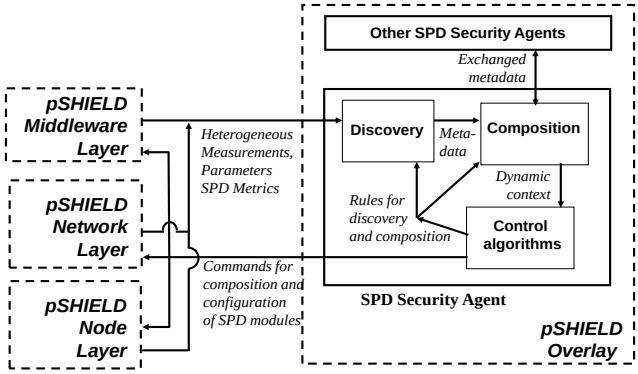

Fig. 2 SHIELD Architecture

These modules, belonging to different SPD layers (node, network or middleware), can be composed (i.e. activated, deactivated or configured) statically or dynamically by the *SHIELD Security Agent*, an innovative software agent (see [4] for details) that collects the information on the system and takes decisions according to proper control algorithms.

This is possible thanks to the development of proper *semantic models* (as outlined in [3] and [5]) that allows the system description in a technology independent way (i.e. machine readable) as well as the definition of *security metrics* that allow the quantification of the security level and consequently the

Thanks to the continuous monitoring performed by the Security Agent, individual SHIELD modules can be dynamically activated and reconfigured once the measured Security metrics do not satisfy the required Security levels, even at run-time.

In addition modularity and technology-independence of the architecture allow a plug&play like behavior, suitable for any kind of application.

In a more structured representation, in Fig. 2 the SHIELD reference architecture is depicted as a control scheme, with the indication of the actors involved in the measurements and commands exchange. The scheme is generically referred to as SPD functionalities, that means Security Privacy and Dependability, since the proposed approach allows to jointly address these peculiarities. However in the prosecution of the paper we will refer only to the "Security" aspects, for which the new metrics and the control algorithms are tailored.

The core of the system, as previously introduced, is the Security Agent: each Agent monitors a set of properly selected measurements and parameters taken from the system (see the arrows labeled as *measurements* in Fig.2). These heterogeneous measurements and parameters are converted by the security agents in *homogeneous/technology-independent) metadata* by extensively using properly selected semantic technologies; the use of homogeneous metadata makes easy the metadata exchange among different security agent (see Fig.2). Each Security Agent, thanks to metadata homogeneity, can aggregate the available metadata, in order to deduce

ISBN: 978-1-61804-237-8

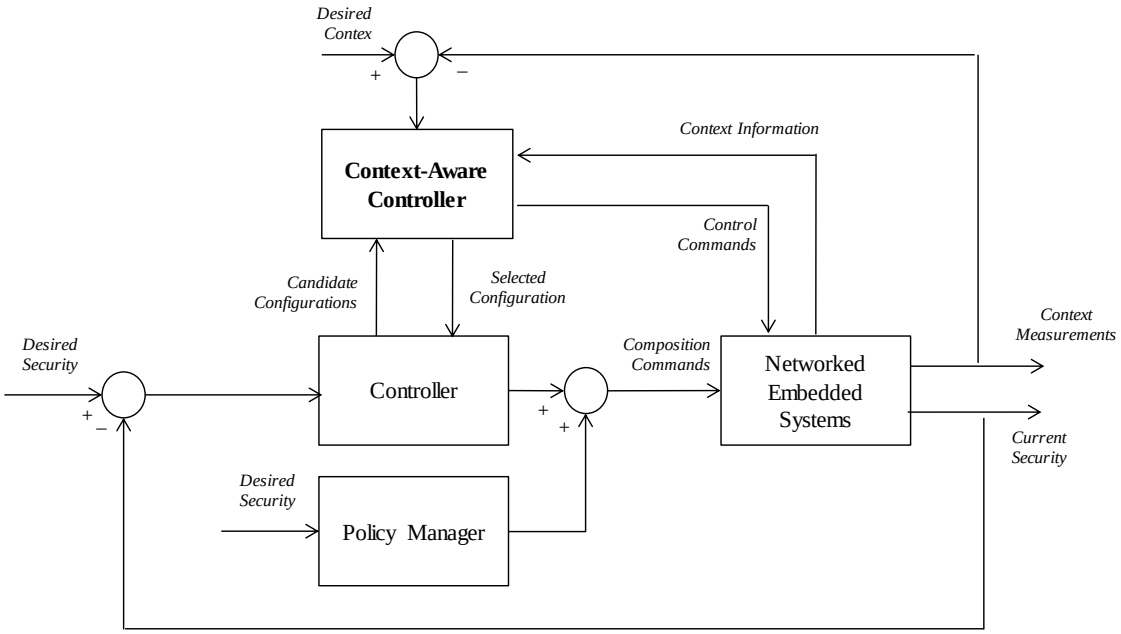

Fig. 3 Composability: a closed-loop view

information which form the so-called *dynamic context* on which the control decisions will be tailored.

Last, but not least, in the security agent runs a set of *control algorithms* which are responsible of dynamically deciding which Security modules have to be composed (i.e. enabled/ disabled/configured) in order to achieve the desired Security level. The decision is driven by the computation of proper technology independent *metrics*, specifically designed for security applications.

In the scope of end-to-end security (the focus subject of this paper), the strength of the SHIELD methodology is that is possible to derive an overall (or E2E) behaviour starting from the atomic behaviors of atomic components and adequately composing them according to proper rules and control algorithms.

On a practical point of view, the SHIELD paradigm allows to deploy small devices (or to use the ones already available), interconnect them and, with the introduction of an intelligent software Agent, dynamically organizing and structuring them so that their capabilities are leveraged to jointly produce the desired effect. As an example, one may be interested in realising the secure monitoring of a train station:

IF the devices deployed in the station (i.e. sensors, cameras, controllers, actuators, etc.) are SHIELD compliant

AND IF at least one SHIELD Security Agent is introduced in this system

THEN it is possible to activate the automatic composition and the system will automatically discover the available devices and the context information, quantify the security level according to the defined metrics, compute a control action and enforce it in the systems to activate/configure the sensors and cameras in the station so that the collected monitoring data are cyphered and made available only to authorized personnel.

This is a trivial example, but is representative of what we call E2E security behaviour: each component is in charge of a specific functionality that is useful to reach the overall objective.

III. THE SHIELD CLOSED-LOOP CONTROL APPROACH

The problem of composing security functionalities can be successfully modelled by leveraging a control theoretic approach (see Fig. 3). Indeed, such kind of model is by far closer to the effective implementation of the SHIELD system.

The *reference signal* is the desired security level, obtained and quantified according to the SHIELD metrics (that will be presented in the following section).

This signal is then used by the *Controller*, that is able to elaborate decision according to proper control algorithms as well as through the interaction with a secondary *Context Controller* that translates ancillary information on the system into constraints and parameters relevant for security purposes. A secondary reference signal may be applied to the system, if, apart from the E2E security behavior, it is also of importance to control other parameters not relevant for security.

In [2] a control algorithm based on Common Criteria composition engine enriched with Hybrid Automata and Model Predictive Control optimization have been proposed as preliminary instantiation of such architecture. This approach has been conceived to be fully in line with the concepts being developed in similar context (e.g. the Future Internet framework [3]) where the limitations coming from the lack of coordination among elements belonging to different layers and/or heterogeneous environments, are addressed through the design of modular controllers and multi-objective procedures.

This solution proved to be valid, but less effective for complex implementations mainly due to the effort needed to translate the "information" into semantic models. The nSHIELD research has then lead to the definition of a new, simpler and more efficient approach, based on these pillars:

- A new metric has been introduced, based on the concept of "attack-surface", that enables an ease abstraction with respect to the underlying technologies.
- The Common Criteria (CC) guidelines have been confirmed, since the satisfaction of security properties must base its foundations on a consolidated standard, and embedded in the new metrics
- The control algorithm has become the translation of the metrics into an optimization problem, whose objective is to find the elements that maximize a target function

IV. Innovative Control Approach to E2E Security

The main novelty of this approach is the definition of "attack surface", i.e. a virtual line that surrounds a system and by which is possible to identify the potential menaces or vulnerabilities that affect the security level. When composing two or more elements, the attack surface is updated and the new menaces/vulnerabilities are updated as well. Once the final shape of the system is achieved, the resulting surface is the starting point to perform control. As anticipated before, the innovative approach to compose atomic functionalities to achieve E2E security, is based on the two most important standards in cyber-security: Common Criteria (CC, [8]) and Open Source Security Testing Methodology Manual (OSSTMM, [9]).

The OSSTMM "is a methodology to test the operational security of physical locations, human interactions, and all forms of communications such as wireless, wired, analog, and digital"[9]. It is based on the concept of *control* that is the mean to influence the impact of threats and their effects when interaction is required. Controls are divided in two categories:

- **Interactive Controls**, which are able to directly influence visibility, access, or trust interactions and this set includes Authentication, Indemnification, Resilience, Subjugation and Continuity
- **Process Controls**, which do not influence the interactions but they are used to create the defensive processes. They are Non-repudiation, Confidentially, Privacy, Integrity and Alarm.

The activation of a single or a multiple control may originate undesirable effects on the attack surface of the system (i.e. the set of interfaces and vulnerabilities that affect the . The OSSTMM models this element through the *Limitation* concept, which denotes the inability of a control to protect a part of the system. The Limitation value is given by the capabilities of the system and the controls in terms of Vulnerability, Weakness, Concern, Exposure and Anomaly. Fig. 4 shows how the Limitations are mapped with respect to the system and the controls.

In the nSHIELD approach hereby presented, we have improved the OSSTMM standard by considering an attack surface described through the Common Criteria. In particular it has been defined the **Damage Effort Ratio** (DER) as the ratio between the "Damage Potential" and the "Effort" values for each interface, thus obtaining a numerical indicator of the damage that can be caused to the system if a malicious access occurs in this interface. This is a way to measure the "surface" without a-priori knowledge about the system.

Category		OpSec	Limitations
Operations		Visibility	Exposure
		Access	Vulnerability
		Trust	
Controls	Class A - Interactive	Authentication	Weakness
		Indemnification	
		Resilience	
		Subjugation	
		Continuity	
	Class B - Process	Non-Repudiation	Concern
		Confidentiality	
		Privacy	
		Integrity	
		Alarm	
			Anomalies

Fig. 4 Limitations effects

As an example, we could consider an interface in which it is possible to access with three different privileges and three different access rights as in Tab. 1: an interface with "root" privilege and "admin" right has DER=1, WHILE an "authenticated"-"authenticated" combination assures a DER=0,67.

Method Privilege	Value	Access Rights	Value
root	4	admin	4
debugger	3	authenticated	3
authenticated	2	anonymous	2

Tab 1.Example of DER

Considering the inclusion of CC in the OSSTMM standard, the control scheme presented in Fig. 3 is instantiated as depicted in Figure 5:

- the main controller is based on an optimization function that tries to minimize the vulnerability of the attack surface by activating functionalities
- The Context Aware controller has become the OSSTMM controller, since it uses context information to provide the list of Interactive/Process Controls that the main controller may put in place to cope with the security needs.

In addition, the influence of Policy Management (that in [2] has been modelled as a disturb) has become a "controllable" input for the context controller, that considers Policies as constraints to the Interactive/Process controls that it can put in place.

.

ISBN: 978-1-61804-237-8

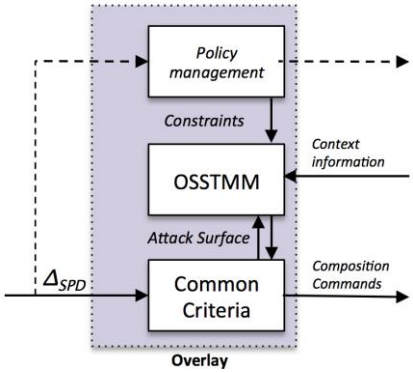

Fig. 5 Innovative Controller

From the mathematical point of view, the main controller solves a typical optimal control problem where the objective function is the minimization of Security value and the constraints is given by the OSSTMM-CC standards and by the policy management system. Higher values of Security cause the activation of more controls and countermeasures; this is the reason why the optimal problem minimizes the Security value. In particular, it minimizes the Δ_{SPD} (i.e. security) value, which is the difference between the desired and actual SPD values.

V. Example of the new SHIELD approach

The example by which the proposed methodology has been tested is an improvement of the one presented in [2] as final demonstration of the pSHIELD project, i.e. the "Monitoring of freight trains transporting hazardous material".

The hypothesized platform is composed by a central unit connected by means of a ciphered wireless network to remote sensors. In this platform the assets to protect are data sent by remote sensors to central unit, where data are recorded inside the central unit itself.

Threats identified for the above scenario are the following:

- Unauthorized disclosure of information stored within or communicated through computers or communications systems;
- Unauthorized modification or destruction of stored information;
- Manipulation of computer or telecommunications services resulting in various violations;
- Propagation of false or misleading information;
- Users lacking guidance or security awareness;
- Data entry or utilization error;
- Faulty access rights management;

Security functionalities (i.e. Controls) that counter the above threats belong to the following categories:

- Authentication;
- Confidentiality;
- Non repudiation;
- Subjugation.

The application of the surface Attach metrics approach does not depend on a thorough knowledge of the theory that generates such an approach, but only by a well-established knowledge that the supplier of the system and/or components of a system must have on security issues.

Starting from the previously evidenced threats, for each of the two components the attack surface value must be computed, according to the guidelines provided in [8] and [9].

The values for the components of the sample scenario are:

- Central unit: 88,75

Constant due to the lack of controls that could be implemented

- Wireless Sensor Network: [84,089 93,340]

Depending on which of the two available controls is activated. In fact it is important to consider that the different choice of key management and Cryptographic operation algorithm change the vulnerability type, so it insert the possibility, changing these algorithm to modify the Security level of the component introducing different states.

In this case the formulation of an Optimization function is not needed, since it is evident that the most robust configuration is the one associated to a 93,340 value for the WSN. However, in case the available controls and their combination is very high, it is sufficient to maximize the Optimization function given by the sum of the atomic security value, within the constraints defined by policies (i.e. mutual inclusion or mutual exclusions of controls).

VI. Conclusions and Future Works

In this paper the innovative results achieved by the nSHIELD project have been presented, as a significant improvement of the proof of concept reported in [2]. In particular it has been shown how it is possible to drive an E2E behavior by acting on the atomic elements; the key idea is to describe each component with a clear and univocally defined metric value that measure the vulnerability of its attack surface (derived as a mix of [8] and [9] guidelines). Then, while composing together several elements, the resulting attack surface is obtained as the result of an optimization problem whose potential solutions are the different controls that the atomic elements can put in place to countermeasure specific menaces. The problem may be solved by exploration or through simple heuristics.

The proposed methodology is currently being intensively tested in industrially relevant scenarios from the avionic and railways domains and the results will be made available in the final nSHIELD project deliverables.

Future works foresee the adaptation of the proposed approach to address also other problems. It could be particularly helpful, for example, in scenarios where the topologies change very often and the E2E behavior is the provisioning of a specific service, like power distribution (see [10]). The main challenge will be the adaptation/tailoring of a proper metric to the new domain, since a good metric is the basis of any SHIELD-like methodology.

ISBN: 978-1-61804-237-8

ACKNOWLEDGMENT

The authors would like to thank the pSHIELD and nSHIELD partners for the significant work performed in these projects to transfer the SHIELD methodology from idea to reality.

REFERENCES

[1] ARTEMIS Strategic Research Agenda, March 2006

[2] Fiaschetti A., Suraci V., Delli Priscoli F. *"The SHIELD Framework: how to control Security, Privacy and Dependability in Complex Systems"*, Proceedings of IEEE Workshop on Complexity in Engineering (COMPENG2012), June 11-13, Aachen, 2012

[3] Fiaschetti A., Suraci V., Delli Priscoli F., Taglialatela A., *"Semantic technologies to model and control the "composability" of complex systems: a case study"*, Book chapter of 'Semantics: Theory, Logic and Role in Programming', Nova Publisher, 2012.

[4] Suraci V., Fiaschetti A., Anzidei G., *"Design and implementation of a service discovery and composition framework for security, privacy and dependability control"*, Future Network & Mobile Summit 2012, July 2012, Berlin, Germany

[5] Fiaschetti A., Lavorato F., Suraci V., Palo A., Taglialatela A., Morgagni A., Baldelli A., Flammini F., *"On the use of semantic technologies to model and control Security, Privacy and Dependability in complex systems"* Proc. Of 30th International Conference on. Computer Safety, Reliability and Security (SAFECOMP'11), Sep. 2011. Naples, Italy.

[6] Castrucci, M., Delli Priscoli, F., Pietrabissa, A., Suraci, V., *"A cognitive future internet architecture"* (2011) Lecture Notes in Computer Science, 6656, pp. 91-102, ISBN: 978-364220897-3, doi: 10.1007/978-3-642-20898-0_7

[7] F. Delli Priscoli, *"A fully cognitive approach for future internet"*, Future Internet, vol. 2, no. 1, pp. 16–29, 2010.

[8] Common Criteria for Information Technology Security Evaluation, v3.1, July 2009

[9] OSSTMM, Open Source Security Testing Methodology Manual

[10] S. Canale, A. Di Giorgio, A. Lanna, A. Mercurio, M. Panfili, and A. Pietrabissa, *"Optimal planning and routing in medium voltage powerline communications networks"*, IEEE Trans. Smart Grid, vol. 4, no. 2, pp. 711–719, 2013.

[11] pSHIELD Technical Annex, June 2010

[12] nSHIELD Technical Annex, September 2011

Andrea Fiaschetti obtained his Ms.C. degree in Control Systems Engineering in 2009 fron the University of Rome "La Sapienza" and his Ph.D. degree in Systems Engineering in 2013 from the same University. His research interest is in the field of control theory applied to security domains, with particular focus on modular and composable architecture. He is also vice-president of the Complex Systems Engineering Committee, within

Andrea Morgagni obtained his Ms.C. degree in Biomedical Engineering in 1996 from "Università Politecnica delle Marche". He is currently employed in Selex Electronic Systems (a Finmeccanica Company), where he works as a Senior Security Evaluator for the Evaluation Facilities accredited by the National Security Authority and OCSI . His main expertise is in the field of Security Metrics and Security Certification process for industrial (civil/military) products, according to the ITSEC and Common Criteria (ISO/IEC 15408) standard guidelines.

Andrea Lanna was born in Velletri (Italy) in 1985. He received the Laurea Triennale and Laurea Magistrale degrees in Control and Systems Engineering from the University of Rome "Sapienza", Italy, in 2009 and 2011, respectively, where he is currently pursuing the Ph.D. degree in Systems Engineering and Operative Research. Since December 2011 he has also been working with research group at Value Up s.r.l., Rome. His main research interests include critical infrastructures protection and the application of control systems theory for renewable energy integration in transmission and distribution network. He is involved in Italian and European Research Projects.

Martina Panfili was born in Ceccano (Italy) in 1982. She obtained the Master Degree in System Engineering in 2010 and the Ph.D in System Engineering in 2014 at the University of Rome "Sapienza". Her main research activities are focused on the application of system and control theory to network resource management and Security in the Embedded Systems context. She has been involved in EU research project (MONET, DLC+VIT4IP, nShield).

Silvano Mignanti received his PhD in System Engineering from the University of Rome "Sapienza", Italy in March 2009. He is collaborating with Sapienza since 2005, working in different European projects, among wihch DAIDALOS I and II, WEIRD, P2PNext, Bravehealth, nSHIELD, DLC+VIT4P. He is also collaborating with the CRAT and the CRMPA consortia. Since 2012 he is researcher at Value Up s.r.l.; since april 2014 he is working with Selex-ES in the Fidelity project.

Roberto Cusani received the "Laurea" degree in Electronic Engineering and the Ph.D. in Communication Systems and Computer Science from the University of Rome "La Sapienza". From 1986 to 1990 he was research engineer at the University of Rome "Tor Vergata", teaching Digital Signal Processing. In 1991 he joined the University of Rome "Sapienza" as Associate Professor of Signal Theory. In 2000 he becomes Full Professor and teaches Information Theory and Coding, and Mobile Communications. From 2004 to 2009 he is the head of the Telecommunication Department (INFOCOM) of the University of Rome "Sapienza". He is author of more than 100 publications in international journals and conferences, of the text-book "Teoria dei Segnali" and of five patents regarding telecommunication applications. He was involved in many research programs, both national and international, and in projects with the industries.

Gaetano Scarano was born in Campobasso (Italy) in 1956. He graduated in Electronic Engineering in 1982 at University of Rome "Sapienza". Since 1991 he is working at the University of Rome "Sapienza" where, at present, he is Full Professor and holds the courses "Signal Theory" and "Image Processing and Transmission". His main research activities are on formal methods and on theory of the images transmission. He is the author of about 100 papers appeared on major international reviews and conferences and of one patents. He was/is the scientific responsible, at the University of Rome "Sapienza", for several projects financed by the Italian Minister of Education (MIUR). He is Associate Editor for IEEE Signal Processing Letters.

Antonio Pietrabissa graduated in Electronic Engineering from the University of Rome "La Sapienza", in 2000, where he received the Ph.D. in System Engineering in 2004. Since 2010, he is Assistant Professor with the Department of Computer, System and Management Engineering of the University of Rome "La Sapienza". He is member of the Technical Committe of the Consortium for the Research in Automation and Telecommunication (CRAT). Since 2000, he has been participating in more than 10 European Union, ESA and National projects on telecommunications. His research focus is the application of system and control theory methodologies to telecommunication networks, with specific interest to the design of resource management protocols (e.g., connection admission control, congestion control, routing, medium access control) for multimedia broadband satellite systems, wireless networks and next-generation

heterogeneous networks. He is author of more than 20 journal papers and more than 40 conference papers on these topics.

Vincenzo Suraci graduated in Computer Engineering with 110/110 cum laude in October 2004 at the University of Rome “Sapienza”. In April 2008 he pursued a Ph.D. in Systems Engineering in the department of Computer Systems Science of University of Rome “Sapienza”. Currently he is researcher at e-Campus and senior project manager at University of Rome “Sapienza”. His main research interest is to develop and to adapt advanced control and operational research theories (reinforcement learning, column generation, hybrid automata, and discrete event systems) to solve challenging and emerging engineering problems in the field of security and dependability.

Francesco Delli Priscoli was born in Rome in 1962. He graduated in Electronic Engineering in 1986 and he received the Ph.D. in system engineering from the University of Rome "La Sapienza" in 1991. From 1986 to 1991 he worked in the "Studies and Experimentation" Department of Telespazio (Rome). Since 1991 he is working at the University of Rome "La Sapienza" where, at present, he is Full Professor and holds the courses "Automatic Controls" and "Control of Communication and Energy Networks". In the framework of his activity, he has mainly researched on resource/service/content management procedures and on cognitive techniques for telecommunication and energy networks, by largely adopting control based methodologies. He is the author of about 180 papers appeared on major international reviews (about 65), on books (about 10) and conferences (about 120) and of five patents. He was/is the scientific responsible, at the University of Rome "La Sapienza", for 31 projects financed by the EU and by the European Space Agency (ESA), as well as for many national projects and co-operations with major industries. His present research interests concern closed-loop multi-agent learning techniques for Quality of Experience (QoE) evaluation and QoE assurance in advanced communication and energy networks, as well as all related networking algorithms.

ISBN: 978-1-61804-237-8