
International Federation for Information Processing

TC-11	**Security and Privacy Protec**

Working Group (11.14) on Secure Engineering

Authors (in alphabetical order):

Jorge Cuellar, SIEMENS, Jorge.Cuellar@siemens.com

Wouter Joosen, KU Leuven, wouter.joosen@CS.KULEUVEN.BE

Javier Lopez, University of Malaga, jlm@lcc.uma.es

Fabio Martinelli, CNR-IIT, Fabio.Martinelli@iit.cnr.it

Fabio Massacci, University of Trento, fabio.massacci@unitn.it

Aljosa Pasic, ATOS, aljosa.pasic@ATOSRESEARCH.EU

Introduction

The Information and Communication Technology (ICT) landscape is continuously changing. We are now witnessing the emergence and consolidation of unprecedented models for service-oriented computing (SOC): Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These models have the potential to better adhere to an economy of scale and have already shown their commercial value fostered by key players in the field. Nevertheless, those new models present change of control on the applications that will run on an infrastructure not under the direct control of the business service provider. For business critical applications this could be difficult to be accepted, when not appropriately managed and secured. These issues are of an urgent practical relevance, not only for academia, but also for industry and governmental organizations. New Internet services will have

to be provided in the near future, and security breaches in these services may lead to large financial loss and damaged reputation.

There thus the need and opportunity to organize, integrate and optimize the research on engineering secure services and related software systems to deal effectively with this increased challenge is pertinent and well recognized by the research community and by the industrial one.

Aims / goals

(What does the working group address, what does it want to achieve)

The Working Group 11.14 aims to provide a forum for cross-disciplinary investigation of “secure engineering” with attention also at the software-services and system aspects. The working group will bring together researchers with an interest in several area of computer science, including, security, security engineering, service engineering, software engineering, formal methods and related fields. The WG will leverage on the experience and community developed by the NESSoS Network of Excellence (www.nessos-project.eu) on Engineering Secure Future Internet Software Services and Systems.

We can list the main aims as:

- **The creation of a long lasting research community on engineering secure services and software systems.**
- **Maintaining a research roadmap in the area of secure service engineering.**
- **Maintaining a workbench for secure service engineering tools.**
- **Contribution to education, training, dissemination.**
- **Reduction of gap between industry and research best practices.**

Scope

(What are the groups of people the working group focuses on, what are the boundaries of the work area)

The main membership will most likely be specialized researchers, both from universities and corporate laboratories. Government organizations and IFIP member societies and their members will be the main users of the results of the group.

Working Group 11.14 has a link to the area of other groups, both inside and outside IFIP (as

the ERCIM WG on security and trust management) and the group will seek actively for close cooperation with these groups.

Scope of the working group (*can be revised according to IFIP WGs interests*):

- Security requirements engineering
- Emphasis on identity, privacy and trust
- Requirements languages for managing legislative constraints and socio-technical and economic aspects
- Conflicts resolution between security requirements and other requirements
- Privacy requirements engineering

- Secure Service Architectures and Design
- Reasoning about security in multi-concern design models
- Security design patterns
- Support for model-driven security dynamic adaptation
- Integrate security modelling in domain-specific modelling languages

- Security support in programming environments
- Service creation
- Security support for service creation (by composing services or by programming new services from scratch)

- Service execution

- Security enforcement at runtime

- Middleware
- Monitoring of business compositions

- Secure service programming
- Adherence to programming principles and best practices
- Verifiable concurrency

- Platform support for security enforcement
- Secure cross-domain interactions
- Finely grained execution monitoring
- Supporting security assurance for FI services

- Service composition and adaptation
- Evolution of security contracts during the whole life of software
- Trustworhty market of composable services
- Assessing risk of a service composition
- Test-bed for comparing service adaptation by contract approaches

- Runtime verification and enforcement
- Run-time monitoring of data flow
- Usage control properties monitoring

- Risk and Cost-aware Secure Service Development
- Risk and cost analysis process: towards incremental and iterative process through Secure Service Development
- Risk composition and aggregation
- Risk and cost evolution
- Risk validation and integration
- Applying formal methods to risk management
- Runtime re-configurability of security based on risk management

- Security assurance for services
- Early assurance
- Step-wise refinement of security (from policies down to mechanisms)
- Formal verification of security policies models
- Certification and audit frameworks for scenarios involving outsourcing of services

- Implementation assurance
- Secure programming
- Security testing and debugging
- Penetration testing (specially model-based penetration testing)
- Automatic generation of test for web applications

- Debugging

-
-
- Secured session management for web service security

- Quantitative security for assurance
- Formal security metrics
- Metrics for privacy and isolation in cloud computing
- Validation and comparison frameworks for security metrics
- Compositional calculation in service-oriented systems

Products / activities

(What are the products and activities the working group will deliver)

The WG will proceed on the main goals we considered above and will extensively support, maintain, manage, etc.

- **The creation of a long lasting research community on engineering secure service and software systems.** A set of collaboration tools including a web site, mailing list etc, will be set up. We will continue to support a series of events as conferences/workshops/schools as NESSoS did in the past (more than 10 till now).

- **Maintenance of a research roadmap in secure service engineering.** We will keep operative the research roadmap available through the on-line access to the NESSoS web site. As identified in the roadmap the focus is also in Future Internet services as cloud, e-health, SmartGrids.

- **Maintaining a workbench for secure service engineering tools** The WG will deliver white papers, research roadmap etc. In addition the NESSoS service developments environment will be maintained accessible (currently more than 20 tools are integrated).

- **Contribution to education, training, dissemination.** The WG will support a set of initiatives as PhD schools, open challenges, training events for practitioners, aiming at inspiring and affecting a common program of education and training for researchers and practitioners.

- **The reduction of the gap between industrial best practices and research.** The WG will maintain active connections with main industries in the area and a specific sub-WG is planned.

Workplan

- Past events / achievements / products

(first time after one year of formal existence of the working group)

- Planned events /achievements / products supported by the WG
- Produce white papers in secure service engineering
- Maintain a research roadmap in the area
- Fostering cooperative project proposals (National and International)
- Consultation services for industry, etc..

The WG plans to have several events, achievements and activities. Still it can leverage on the successfully series of NESSoS results (see www.nessos-project.eu). In addition, being the WG based on several disciplines it will be often performed also in cooperation with other organizations/interest groups/etc.. In particular we do wish to continue to: · Co-organize conferences/workshops/schools/open challenges o ESSoS (the main sponsored event), QASA, FOSAD summer school, …

The main keywords will be inclusiveness, openness and cooperation with all the relevant scientific communities. In particular, the new WG aims at cooperating with all the other IFIP WGs, including 11.8 and all the TC2 WGs with whom share several point of interest in order to generate fruitful synergies.

Membership

(Membership rules, annual changes, officers)

- Membership rules

Members of the Working Group are expected to be qualified researchers and/or professionals engaged in the field.

Members are expected to participate actively in Working Group activities. At a minimum, active participation means presenting a paper or taking an active role in the organization of a meeting at least once every three years (i.e., a three-year period of inactivity is taken to indicate that the member is no longer actively interested in this technical area and can be cause for removing the member from the membership list).

- Changes

(first time after one year of formal existence of the working group)

- Officers for the first three-year term, Sep. 2013 – Aug. 2016

Chair: Fabio Martinelli (CNR)

Vice-chairs: Wouter Joosen (KU Leuven), Fabio Massacci (University of Trento)

Secretary: Javier Lopez (University of Malaga)

Liaison with Industry: Aljosa Pasic (ATOS), Jorge Cuellar (Siemens)

Founding Members

Name
Country
E-mail
Martin Abadi
US
abadi@CS.STANFORD.EDU
Mohammed Achemlal
FR
mohammed.achemlal@ORANGE-FTGROUP.COM

Alessandro Aldini

IT

alessandro.aldini@uniurb.it

David Basin

CH

basin@inf.ethz.ch

Benoit Baudry

FR

Benoit.Baudry@INRIA.FR

Lujo Bauer

US

lbauer@cmu.edu

Antonia Bertolino

IT

antonia.bertolino@isti.cnr.it

Colin Boyd

NO

c.boyd@qut.edu.au

Mike Burmester

US

burmester@cs.fsu.edu

Manuel Clavel

ES

manuel.clavel@IMDEA.ORG

Jorge Cuellar

DE

Jorge.Cuellar@siemens.com

Lieven Desmet

BE

Lieven.Desmet@cs.kuleuven.be

Marina Egea

ES

marina.egea@atos.net

Sandro Etalle

NL

s.etalle@tue.nl

Carmen Fernandez Gago

ES

mcgago@LCC.UMA.ES

Eduardo Fernandez

US

ed@cse.fau.edu

Roberto Giacobazzi

IT

rgiacobazzi@gmail.com

Paolo Giorgini

IT

paolo.giorgini@unitn.it

Adrian Gheorghe

US

AGheorgh@ODU.EDU

Maritta Heisel

DE

maritta.heisel@uni-duisburg-essen.de

Paola Inverardi

IT

inverard@di.univaq.it

Valerie Issarny

FR

Valerie.ISSARNY@inria.fr

Somesh Jha

US

jha@cs.wisc.edu

Wouter Joosen

BE

wouter.joosen@CS.KULEUVEN.BE

Jan Jürjens

DE

jan.jurjens@cs.tu-dortmund.de

Sokratis Katsikas

GR

ska@unipi.gr

Khaled Khan

QA

k.khan@qu.edu.qa

Nora Koch

DE

kochn@pst.ifi.lmu.de

Yves Le Traon

LU

Yves.LeTraon@uni.lu

Ben Livshits

US

livshits@microsoft.com

Javier Lopez

ES

jlm@lcc.uma.es

Zakaria Maamar

AE

Zakaria.Maamar@zu.ac.ae

Heiko Mantel

DE

mantel@cs.tu-darmstadt.de

Eda Marchetti

IT

eda.marchetti@isti.cnr.it

Fabio Martinelli

IT

Fabio.Martinelli@iit.cnr.it

Fabio Massacci

IT

fabio.massacci@unitn.it

Gary McGraw

US

gem@cigital.com

Catherine Meadows

US

meadows@itd.nrl.navy.mil

Ron van der Meyden

AU

meyden@cse.unsw.edu.au