Security Group

The main activity of the Trustworthy and Secure Future Internet group is the definition of models, methodologies and tools concerning security for the information and communication technologies and for the Future Generation Internet. The dynamic and heterogeneous topology of networks requires adaptive security mechanisms, and the distributed nature requires the definition of mechanisms to manage the trust relations between the parties involved in the interactions. The main application environment are the Future Internet, the Virtual Communities, such as Social Networks, and the distributed environments such as Grid and Cloud.

People

Researchers and Technologists
Paolo Mori (Team Leader)
Fabio Martinelli
Ilaria Matteucci
Marinella Petrocchi
Paolo Santi
Anna Vaccarelli
PostDocs
Gianpiero Costantino
Aliaksandr Lazouski
Charles Morisset
Daniele Sgandurra
Artsiom Yautsiukhin
Ph.D. Students
Peter Drabik
Leanid Krautsevich
Developer
Luca Wiegand
Alessio Lunardelli
Financial administration
Lucia Ghelardi
External Consultants
Luca Bechelli
Associate Researchers from Academia
Stefano Bistarelli
Pierpaolo Degano
Roberto Di Pietro

Areas of Research

Access and Usage Control: mediating the access to valuable and critical resources through effective security mechanisms able to enforce security policies while the access is in progress.

Formal analysis of security protocols and systems: methods, techniques and tools for the rigorous analysis and verification of security.

Parental Control: offering control mechanisms able to safeguard the minors from possible misusage of the modern technology.

Trust Management: automatizing the evaluation of the trustworthiness of the parties involved in e-transactions or interactions.

Cloud Security: defining protection mechanisms to enhance security in virtualized environment.

Mobile System Security: facing the new threats deriving from the spreading usage of current and next generation mobile and wireless devices all over the world.

Risk Management: supporting the design and implementation of systems requiring security assurances, in order to efficiently reduce the risks related to the development process.

Security in Social Computing: supporting secure computations carried out by groups of people and in social networks.

Training activities

- International School on Foundations of Security Analysis and Design (FOSAD)
- Master in Web Technologies (in cooperation with the University of Pisa)

http://security.iit.cnr.it/

Main Collaborations

- Assosecurity (Torino)
- British Telecom
- CSP ScRL (Torino)
- DoCoMo Eurolabs
- ERCIM
- HP
- Infocamere ScPA (Padova),
- ISP del Registro del ccTLD"it"
- Regione Toscana (Firenze), Comune di Livorno,
- SAP
- Thales
- Univ. di Pisa
- Univ. di Trento
- Univ. of Malaga (Spain)
- VPtech (Roma)

Main Research Projects

NESSoS: The Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSoS) aims at constituting and integrating a long lasting research community on engineering secure software-based services and systems. The NESSoS approach is based on addressing security concerns from the very beginning in system analysis and design, thus contributing to reduce the amount of system and service vulnerabilities and enabling the systematic treatment of security needs through the engineering process.

CONNECT: The CONNECT project aims at dropping the interoperability barrier by adopting a revolutionary approach to the seamless networking of digital systems, that is, synthesizing on the fly the connectors via which networked systems communicate. CONNECT enables the dynamic synthesis of CONNECTors by introducing a formal foundation for connectors, which allows learning, reasoning about and adapting the interaction behavior of networked systems.

CONTRAIL: The goal of the CONTRAIL project is to design, develop and promote an integrated approach for Cloud federation. The CONTRAIL platform will provide services for federating IaaS Clouds, and both Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) on top of federated Clouds. The CONTRAIL platform will include an enhanced security support tailored for the Cloud Federation requirements.

ANIKETOS: In the Future Internet, applications may be composed of multiple services from many different providers, and the end user may have little in the way of guarantee that a particular service will actually offer the security claimed. ANIKETOS will help establish and maintain trustworthiness and secure behaviour in a constantly changing service environment. The project will align existing and develop new technology, methods, tools and security services that support the design-time creation and run-time dynamic behaviour of composite services, addressing service developers, service providers and service end users.

VISITO: The project is aimed at realizing technologies able to offer an interactive and customized advanced tour guide service to visit the cities of art in Tuscany through mobile devices. During the city tour, the mobile device is used to get detailed information about what the user is watching, and when taking pictures of monuments, places and other objects, the user can share it on the VISITO platform with his description.

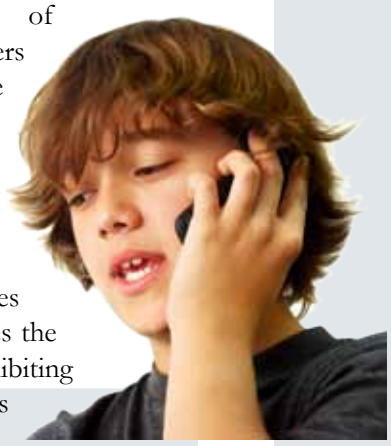
OpenInFSE: implementation of an Infrastructure for the interoperability of the local Electronic Health Record solutions adopted in the Italian regions, exploiting the public communication infrastructure named: “Sistema Pubblico di Connettività (SPC)”.

Research communities

- Coordinator of the Interdepartmental Security Project of CNR
- Co-chairs of the platform SERIT (Security Research in Italy)
- Coordinator of the NESSoS security community

Software tools/applications achieved

iCareMobile is a Parental Control system that enhances significantly the protection of underage users exploiting mobile phones. iCareMobile protects children from unwanted contacts as, for example, the reception of multimedia messages or phone calls from unknown people, prevents the reception of images and videos for adults, and regulates the usage of the phone, such as prohibiting the execution of certain applications in the school hours.



Istituto di Informatica e Telematica