RESISTO
RESIlience enhancement and risk control platform for communication infraSTructure Operators

WORKSHOP/TUTORIAL:

"Physical and cyber threats: the new challenges for TLC Critical Infrastructures"

DATE: May 19th, 2019 | **VENUE:** Valencia – Spain Universitat Politècnica de València (UPV)

WORKSHOP CHAIR AND CO-CHAIR

Federica Battisti | Roma Tre University

participates to two european projects, ATENA (Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over critical infrAstructures) and RESISTO (RESIlience enhancement and risk control platform for communication infrastructure Operators). Both projects deal with the protection of critical infrastructures from cyber attacks and natural disaster, with a specific focus on the interaction among the considered infrastructures.

➢ *federica.battisti@uniroma3.it*

Publications related to the topic of the workshop are:

• F. Adamsky, M. Aubigny, F. Battisti, et al., "Integrated Protection of Industrial Control Systems from Cyber attacks: the ATENA Approach", in International Journal of Critical Infrastructure Protection, Elsevier, Volume 21, June 2018, Pages 72-82.

• F. Battisti, G. Bernieri, M. Carli, M. Lopardo, and F. Pascucci, "Detecting integrity attacks in IoT-based Cyber Physical Systems: a case study on Hydra testbed", Proc. of the Global Internet of Things Summit (GIoTS), 4-7 June, 2018, Bilbao, Spain.

• R. Copeland, S. Ahvar, N. Crespi, M. Copeland, R. Durand, J.-M. Duquerrois, F. Paganelli, F. Battisti, A. Neri, "Technology Assessment for Mission-Critical Services on Automotive Virtual Edge Communicator (AVEC)", Proc. 21st Conference on Innovation in Clouds, Internet and Networks (ICIN), 20-22 February, 2018, Paris, France.

• F. Battisti, M. Carli, F. Pascucci, "Securing Cyber Physical Systems from injection attacks by exploiting random sequences", Proc. 13th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 9-11 October, 2017, Rome, Italy.

Federica Pascucci | Roma Tre University

participates in several EU project about critical infrastructure protection: MICIE (Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures), CockpitCI (Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures), FACIES (online identification of Failure and Attack on interdependent Critical InfrastructurES), URANIUM (Unified Risk Assessment Negotiation via Interoperability Using Multi-sensor data), ATENA (Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over critical infrAstructures) and RESISTO (RESIlience enhancement and risk control platform for communication infraSTructure Operators). The projects address the protection of the critical infrastructure by developing risk assessment tools to prevent and limit faults and failures and by considering the interdependence among infrastructures.

➢ ***federica.pascucci@uniroma3.it***

Publications related to the topic of the workshop are:

• Faramondi, L., Setola, R., Panzieri, S., Pascucci, F., Oliva, G., "Finding critical nodes in infrastructure networks", (2018) International Journal of Critical Infrastructure Protection, 20, pp. 3-15.

• Faramondi, L., Oliva, G., Panzieri, S., Pascucci, F., Schlueter, M., Munetomo, M., Setola, R.,"Network Structural Vulnerability: A Multiobjective Attacker Perspective", (2018) IEEE Transactions on Systems, Man, and Cybernetics: Systems, Article in Press.

• Bernieri, G., Etchevés Miciolino, E., Pascucci, F., Setola, R.,"Monitoring system reaction in cyber-physical testbed under cyber-attacks", (2017) Computers and Electrical Engineering, 59, pp. 86-98.

• Miciolino, E.E., Setola, R., Bernieri, G., Panzieri, S., Pascucci, F., Polycarpou, M.M.,"Fault diagnosis and network anomaly detection in water infrastructures", (2017) IEEE Design and Test, 34 (4), art. no. 7878551, pp. 44-51.

• Miciolino, E.E., Bernieri, G., Pascucci, F., Setola, R.,"Communications network analysis in a SCADA system testbed under cyber-attacks", (2016) 2015 23rd Telecommunications Forum, TELFOR 2015, art. no. 7377479, pp. 341-344.