PREEMPTIVE DISSEMINATION DAY

Date: **11th May 2017**
Location: **Vitrociset Spa**, Via Tiburtina 1020, Rome (Italy)

We are pleased to invite you to the "**Dissemination Day**" of PREEMPTIVE, a FP7 European Research Project. PREEMPTIVE proposes innovative solutions to protect critical infrastructure, with specific attention to utilities (energy, water and gas), their industrial networks and their automated control systems.
The main contributions of the project include solutions for enhancing existing methodologies that aim at **ensuring critical infrastructures security**, and **new prevention and detection tools** to protect critical infrastructures from cyber-attacks that can act at different levels (e.g., network, hosts or process).

During the course of the day, we will focus on the critical infrastructure cyber-threats landscape. We will discuss how attackers can damage our critical infrastructures and what solutions the PREEMPTIVE workforce has developed to tackle and defeat attacks that become every day more sophisticate.

We will conclude the day with a panel where key stakeholders (EU research projects executors, end users, people from industry and academy) discuss the main challenges that cyber-security experts are facing today.

With the financial support of FP7 – Seventh Framework Programme Grant agreement no: 607093

AGENDA

Timeslot	Talk Title	Presenter
09.45 – 10.15	An overview of the PREEMPTIVE project	Giorgio Sinibaldi, Vitrociset
10.15 – 11.45	Attack hunting: PREEMPTIVE toolbox for defending critical infrastructure from network, host and process based cyber-attacks.	Elisa Costante, *Security Matters* Xavier Clotet, *Aplicaciones en Informática Avanzada, S.L.* Maurizio Pizzonia, *Università degli studi Roma Tre* Sandro Etalle, *University of Twente* David Lund, *HW Communications* Antonio Ursini, *Vitrociset*
11.45 – 12.00	Coffee Break	
12.00 – 12.45	PREEMPTIVE in action: a demo of attacks and detection	Antonio Ursini, *Vitrociset*
12.45 – 14.00	Lunch	
14.00 – 14.30	On methodologies for critical infrastructure protection	Steffen Pfrang, *Fraunhofer-Gesellschaft*
14.30 – 15.00	The EU Regulatory Framework: The Road Ahead	Laurens Naudts, *KU Leuven, CiTiP*
15.00 – 15.15	Coffee Break	
15.15 – 16.15	Panel Discussion: current and future challenges in cyber-security for critical infrastructures	Speakers from EU research projects, end users, industry and academy
16.15 – 16.30	Take home message and workshop closure	Giorgio Sinibaldi, *Vitrociset*

With the financial support of FP7 – Seventh Framework Programme Grant agreement no: 607093

Talks Abstracts

Morning

09.45 – 10.15: An overview of the PREEMPTIVE project.

The increasing levels of cyber-attacks and advanced persistent threats (APTs) require a new approach to cyber protection. Detecting and preventing intrusion at the early stage of the attack is critical and developing a multi-layered approach to the protection is a key to success. PREEMPTIVE project has developed multi-layered software tools, hardware and firmware solutions and a methodology aimed at protecting critical infrastructures from cyber-treats. In this session, we provide an overview of the PREEMPTIVE platform and its main objectives.

10.15 – 11.45: Attack hunting: PREEMPTIVE toolbox for defending critical infrastructure from network, host and process based cyber-attacks.

Industrial control systems (ICS) monitor and control the physical processes of critical infrastructures like power plants, water, oil and gas distribution systems. In recent times, sophisticated and targeted attacks against owners and operators of ICS across multiple critical infrastructure sectors have increased. As ICS environments differ from traditional IT systems, they also face unique security challenges and therefore require specific solutions to enhance security and mitigate the impacts of cyber-attacks. In this session, we present a suite of solutions developed within PREEMPTIVE that aim at protecting ICS from cyber-attacks that target the communication network, the software infrastructure and the physical process.

12.00 – 12.45: PREEMPTIVE in action: a demo of attacks and detection

In this session, we show how the PREEMPTIVE tools can be integrated in a comprehensive framework and how tools can be deployed in an operational environment such as an energy distribution system. We also show how a cyber-attack can infect a system, what damages it can cause and how effective PREEMPTIVE can be in defending from it.

With the financial support of FP7 – Seventh Framework Programme Grant agreement no: 607093

Afternoon

14.00 – 14.30: On methodologies for critical infrastructure protection

In this session, we will be presenting the findings on methodologies for securing critical infrastructures. We will start from existing standards and best practices and talk about discovered gaps. Then, we will present the PREEMPTIVE methodology, a framework for evaluating and protecting those infrastructures. The talk will be concluded with the lessons learned from performing an evaluation of the methodology in a real site.

14.30 – 15.00: The EU Regulatory Framework: The Road Ahead

How could future legislation help in reducing the vulnerability of critical infrastructures against cyber-attacks? Despite recent positive efforts by the EU legislator, the EU remains vulnerable to cyber incidents. In this presentation, an overview will be given of the legal and technological challenges and gaps still faced by regulators concerning the cyber-security protection of critical infrastructures. Recognizing the cyber-security value-chain, policy recommendations that could improve the overall protection of critical infrastructures will be formulated towards Member States, national authorities, market operators and tool developers.

15.15 – 16.15: Panel Discussion: current and future challenges in cyber-security for critical infrastructures

As cyber-attacks grow in number and sophistication, security for national and international critical infrastructures is increasingly attracting the attention of key stakeholders. The vulnerabilities of legacy SCADA system have been dramatically exposed in recent years, most notably by Stuxnet and Flame. Governments, institutions and industry need to collaborate to address these vulnerabilities and to improve critical infrastructure security readiness in a fast-changing environment where the adoption of new smart technologies (smart meters, IoT, smart devices) comes with increasing security risks. In this session, we bring together a panel of international experts for a discussion of the challenges, responses and next steps regarding cyber security for critical infrastructure.

With the financial support of FP7 – Seventh Framework Programme Grant agreement no: 607093

Who's behind PREEMPTIVE

Vitrociset designs, implements, integrates and manages electronic and IT systems in civil and military sectors for private businesses, public authorities, governmental agencies and international organizations. The company's main fields of activity encompass Defense systems, Critical Infrastructure Information protection, Satellite Technologies, Telecommunications, Transport and Infrastructures.

Security Matters was founded in 2009 to bring to the market SilentDefense, a solution to address industrial cyber security threats and needs. Over the following years, the tireless diligence and tight collaboration with critical infrastructure operators allowed SilentDefense to grow and be refined into the market leading solution it is today. The unique knowledge and expertise of SecurityMatters were recognized by Gartner in 2014, when SecurityMatters became the first company ever nominated as a Cool Vendor for technology and service providers in the OT market. Today, SecurityMatters provides critical infrastructure and industrial automation companies with best-of-class industrial cyber resilience technology that enables quick identification and recovery from threats to operational continuity.

Aplicaciones en Informática Avanzada, S.L. (AIA), founded in 1988, is one of the few Spanish companies working in the Consulting and Engineering of Software and IT Systems that strongly emphasizes innovation. The objective of Grupo AIA is the transformation of information into knowledge, where the customer is considered as a collaborating participant. Grupo AIA's main objective is the production of a real and tangible economic benefit for its clients; this is achieved through innovation using basic science methods, particularly coming from Physics and Artificial Intelligence backgrounds.

The UT University is based in Netherlands. The Distributed and Embedded Security group (DIES) forms the heart of UT's information security research. The group works on data and network security and cybercrime prevention.

With the financial support of FP7 – Seventh Framework Programme Grant agreement no: 607093

The Israel Electric Corporation (IEC) was established in 1923. IEC is a sole integrated electric utility in the State of Israel. IEC generates, transmits and distributes substantially all the electricity in the State of Israel and it is one of the largest industrial companies in Israel. IEC has close relationship with the Government of Israel. IEC is a primary electricity supplier in Israel providing all Israel electricity demand requirements.

Roma Tre (www.uniroma3.it) is the youngest state University in Rome, founded in 1992 as an offspring of Università "La Sapienza", being now the second in size with about 30'000 students and 600 faculty members in eight schools. It has a vast experience in the area of information visualization, Internet analysis, and data security. It collaborates with a number of European research groups, industries, industrial consortia, and governmental entities.

ENCS is a not-for-profit cooperative association of members from government, academia, and industry. ENCS has the mission to improve the resilience of European critical infrastructures. The initial focus of ENCS is on improving the security of Smart metering- , Smart Grids- and Industrial Control Systems infrastructures of Utilities/DSO's in Europe. ENCS works with dedicated resources and with member resources in research & development, testing, monitoring, education &training, and information & knowledge sharing. ENCS is active in the research community, standards organizations, and expert groups.

Harnser Risk Group is an independent provider of security risk advisory services to infrastructure operators and governments in Europe and the Middle East as well as the European Commission and NATO. These include owners and operators of Critical National Infrastructure (CNI) assets, as well as governments seeking to increase resilience across all designated CNI sectors by managing those assets. Harnser has undertaken several empirical studies for the European Commission to aid the implementation of EPCIP.

With the financial support of FP7 – Seventh Framework Programme Grant agreement no: 607093

KU LEUVEN	KU Leuven is the largest Belgian academic institution and one of the oldest European universities. KU Leuven is also a member of the League of European Research Universities (LERU), a group of twenty European research-intensive universities committed to the values of high-quality education in an internationally competitive research environment. The KU Leuven Centre for IT & IP Law (https://www.law.kuleuven.be/citip/en) is a research centre at the Faculty of Law of KU Leuven dedicated to advance and promote legal knowledge about the information society through research and teaching of the highest quality
Fraunhofer	The Fraunhofer-Gesellschaft undertakes applied research of direct utility to private and public enterprise and of wide benefit to society. The Fraunhofer-Gesellschaft is the largest organization for applied research in Europe. The core competences of the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB) in Karlsruhe are in the domains of image interpretation, control systems, and information and communication management.
HWC www.hwcomms.com	HW Communications Ltd (HWC) was founded in 1990. It has traditionally focused on advanced research and development in mobile and wireless communications, which have been implemented as bespoke solutions for external companies and government agencies. More recently, HWC has also targeted the transfer of the technologies developed in the research laboratory into its own range of secure and resilient communication products. HWC's unique breadth of capability spans all layers of the communication stack, allowing for optimum consideration for secure and resilient communication systems.
IREC Institut de Recerca en Energia de Catalunya Catalonia Institute for Energy Research	IREC is a private Foundation with the participation of the Catalan regional government (Generalitatde Catalunya), the Spanish Ministries of Industry and Science & Innovation, the Univ. of Barcelona, the Polytechnic Univ. of Catalonia, the Univ. Rovira Virgili and private companies from the energy sector. The Institute constitutes a research organization committed to carry out, promote, spread, transfer and improve research activities in the energy and environment sectors of knowledge and of their applications. More specifically, it has lines of work in technologies related to micro-grids, electric vehicles, energy storage, efficiency in buildings, bioenergy and biofuels and offshore wind energy. The centre also has an electricity and power electronics area, and design and characterization of materials for energy.

With the financial support of FP7 – Seventh Framework Programme Grant agreement no: 607093

Practical Information

Registration and more information

This workshop is organized as part of the PREEMPTIVE project and as such, no fee is required to participate. Tea/coffee and lunch will be provided on the day. All presentations and discussions will be in English. For registration and more information, please contact Giorgio Sinibaldi, g.sinibaldi@vitrociset.it

Venue and Transportation

The event is held at Vitrociset offices, located in Via Tiburtina 1020, Rome (Italy). From Fiumicino or Ciampino Airport, you can take a taxi (it takes respectively about 1 hour and 40 minutes) or a train to *Termini* train station. From *Termini* central station, take the *Metro B* until the last stop, *Rebibbia* (it takes about 25 minutes). From *Rebibbia* to Vitrociset offices it takes 10 minutes walking: at the exit of the metro station, you need to cross the road (use the subway on the right). Alternatively, you can take bus 437, 443 or 447 and stop at *Tiburtina/Iino Da Parma*. If you wish to come by car, you need to take the "Grande Raccordo Anulare" and exit at *Tiburtina Center* (we suggest avoiding the car: Rome's traffic jams are infamous).

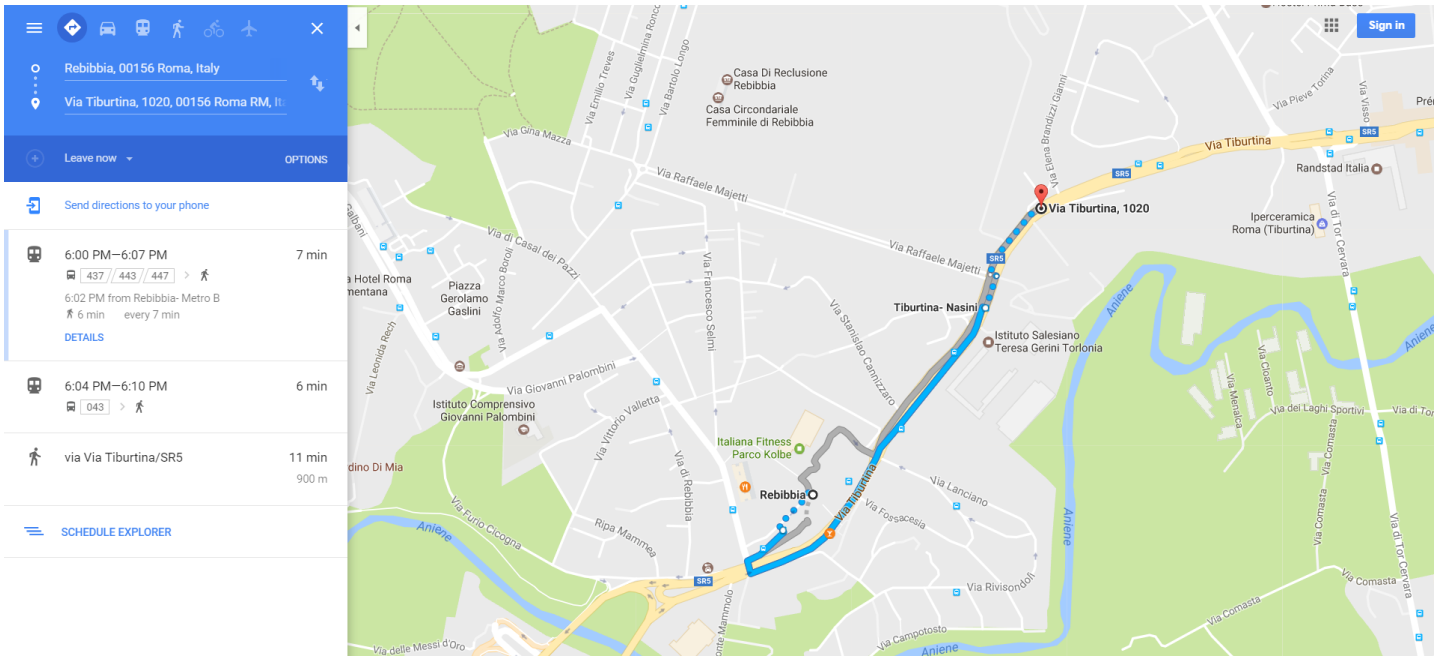

Figure 1: How to reach Vitrociset offices from Rebibbia station

With the financial support of FP7 – Seventh Framework Programme Grant agreement no: 607093