



I N S P I R E

EC Grant Agreement n. 225553

The INSPIRE project

Salvatore D'Antonio

University of Naples "Parthenope"

Consorzio Interuniversitario Nazionale per l'Informatica (CINI)

INSPIRE Final Workshop

Rome, January 21, 2011



Setting up the scene



I N S P I R E

EC Grant Agreement n. 225553

- Supervisory Control And Data Acquisition (SCADA) systems are rapidly moving from closed solutions towards IP-based integrated frameworks made of Commercial Off-The-Shelf (COTS) components and using shared networks and standard communication protocols
- This technological trend is bringing many advantages:
 - The availability of a large base of standard and well-known protocols
 - The possibility of using shared and interconnected networks to support distributed SCADA systems
 - The deployment of IP-based services and applications on top of SCADA systems

Cybersecurity in CIs

- Communication networks are the main channel for attacking CIs
- Securing this channel requires deep understanding of a whole variety of inter-related issues

The complexity of cybersecurity – 1

- The simplest definition of cyber security is “security of the cyberspace”, which immediately brings forward the complexity of the problem
- Cyberspace is a domain that lacks a single and clearly delimited frontier
- The interconnections with other infrastructures, above all the communication infrastructure, are numerous

The complexity of cybersecurity – 2

- The initial impact of threats can be local but the spreading of threats can be virtually unlimited
- Users include, potentially, all individuals, organizations and “intelligent” machines

- **Spring 2000**
 - A former employee of an Australian industrial software company used a radio transmitter to remotely hack into the controls of a sewage treatment system at Maroochy Shire, Queensland, and release approximately 264,000 gallons of raw sewage into nearby rivers
- **December 2000**
 - Electric power servers are hijacked to host and play games
- **June 2001**
 - Cal-ISO (California Independent System Operator, <http://www.caiso.com/>) is attacked and compromised for 17 Days
- **January 2003**
 - FirstEnergy (<http://www.firstenergycorp.com/index.html>) hit by Slammer worm. The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant, and disabled a safety monitoring system for nearly five hours

- February 2006
 - Idaho National Laboratory (FERC/D.O.E. has demonstrated attack methods against SCADA systems at a SANS conference)
- January 2008
 - CIA: Hackers to Blame for Power Outages. Hackers literally turned out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments before disrupting the power
<http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/01/18/national/w122440S64.DTL>
- April 2009
 - Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system,
<http://www.reuters.com/article/topNews/idUSTRE53729120090408>
- July 2010
 - Stuxnet worm designed to steal industrial secrets and disrupt operations has infected the SCADA systems of 14 plants. Stuxnet is a working – and fearsome – prototype of a cyber-weapon. [Kaspersky Lab]



Challenges and opportunities



I N S P I R E

EC Grant Agreement n. 225553

- The World Economic Forum estimated in 2008 that there is a 10 to 20% probability of a major CII breakdown in the next 10 years, with a potential global economic cost of approximately 250 billion US\$.
- Awareness of the need to protect CIs
- Cooperation among academia, industry, public bodies in order to achieve a common consensus on CIP priorities
- From political support to policies, from policies to funding for research, different opportunities

- 2007 EC Communication “Towards a general policy on the fight against cyber crime”
 - the setting up of a central EU cyber crime contact point;
 - the support of research in fight against cyber crime;
 - concrete public-private projects;
 - the raising of awareness;
- 2009 EC communication “Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience” on CIIP

- *Preparedness and prevention*, by creating a European Public-Private Partnership for Resilience and a European Forum of Member States to share information and good policy
- *Detection and response*, by supporting the development and deployment of a European Information Sharing and Alert System (Early Warning)

- *Mitigation and recovery*, through the development by Member States of national contingency plans
- *International and EU wide cooperation*, by driving a Europe-wide debate to define EU priorities for the long term resilience and stability of the Internet, possibly leveraging strategic cooperation with third countries



The European context



I N S P I R E

EC Grant Agreement n. 225553

- The EC communication on the Digital Agenda and its impact on the research programmes
- The European Programme for Critical Infrastructure Protection – EPCIP and its 2008 directive focused on Energy and Transport



The European context



I N S P I R E

EC Grant Agreement n. 225553

- Operations of Agencies such as REA, ENISA, Frontex
- The effective interworking of CERTs (Computer Emergency Response Team) and CSIRTs (Computer Security and Incident Response Team), at prevention and at response levels



The European context



I N S P I R E

EC Grant Agreement n. 225553

- The FP7 supporting security, trust and critical infrastructure research (DG ENTR, DG INFSO, DG HOME);
- The CIP-PSP pilot deployments



INSPIRE overview



EC Grant Agreement n. 225553

I N S P I R E

- Two-year small or medium-scale focused research project (STREP)
- Work programme topic addressed
 - Objective ICT-SEC-2007.1.7: Critical Infrastructure Protection (CIP)
- Start date:
 - November 1, 2008
- End date:
 - January 31, 2011

ACADEMY

- Consorzio Interuniversitario Nazionale per l'Informatica (Coordinator) (ITA)
- Technical University of Darmstadt (GER)

INDUSTRY

- SELEX-Sistemi Integrati (ITA)
- Thales Communications (FRA)
- ITTI (SME) (POL)
- S21Sec Information Security labs (SME) (SPA)
- KITE Solutions (SME) (ITA)
- Centre for European Security Strategies (GER)



Objectives – 1

- To analyze vulnerabilities which affect SCADA systems
- To design an architectural framework for SCADA systems monitoring, diagnosis and remediation
- To develop diagnosis and recovery techniques, suited for SCADA systems
- To implement traffic engineering algorithms to provide SCADA traffic with quantitative guarantees

Objectives – 2

- To design and develop a component-based framework for security assessment of SCADA systems
- To define a roadmap for improving the protection of CIs
- To link European CIP research to major US initiatives



INSPIRE-INCO



I N S P I R E

EC Grant Agreement n. 225553

- An international cooperation has been set up between INSPIRE and the NSF-supported project “GridStat” (www.gridstat.net) in the area of power grid protection
- GridStat is a novel publish-subscribe, QoS-managed middleware framework that has been designed to enhance the resilience of electric power grid’s communication network



INSPIRE-INCO in a nutshell



I N S P I R E

EC Grant Agreement n. 225553

- Proposal: 248737
- Acronym: INSPIRE-International (I Cooperation)
- Program: FP7
- Call: FP7-ICT-2009-4
- Funding scheme: Small or medium-scale focused research project -STREP - CP-FP-INFISO
- Duration: 15 months (October 1, 2009 – December 31, 2010, 2010)
- Activity: ICT-4-9.2 - Supplements to support International Cooperation between ongoing projects



The Consortium



I N S P I R E

EC Grant Agreement n. 225553

- **Europe (INSPIRE):**
 - CINI, Consorzio Interuniversitario Nazionale per l'Informatica - Coordinator (Italy)
 - TUD, Technical University of Darmstadt (Germany)
 - ITTI, ITTI Sp.zo.o. (Poland)

<http://www.inspire-strep.eu/>
- **US (GridStat):**
 - WSU, Washington State University (USA)

<http://www.gridstat.net/>



The funding scheme



EC Grant Agreement n. 225553

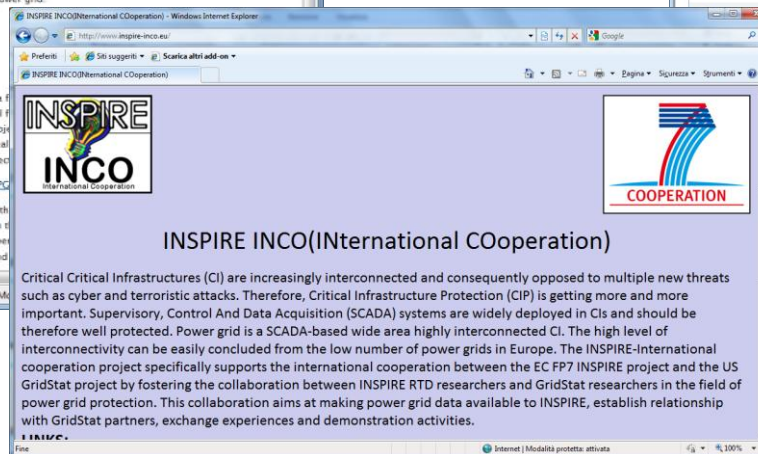
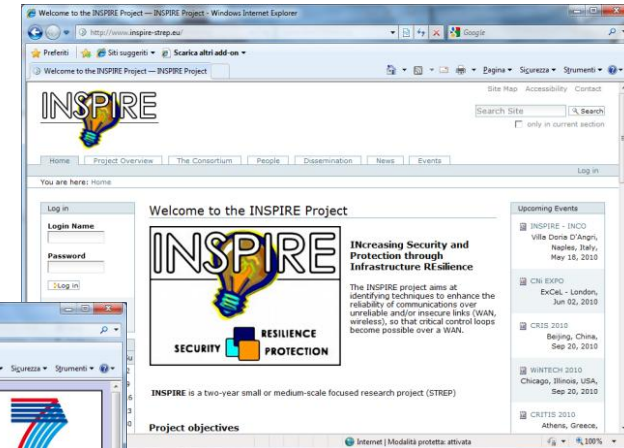
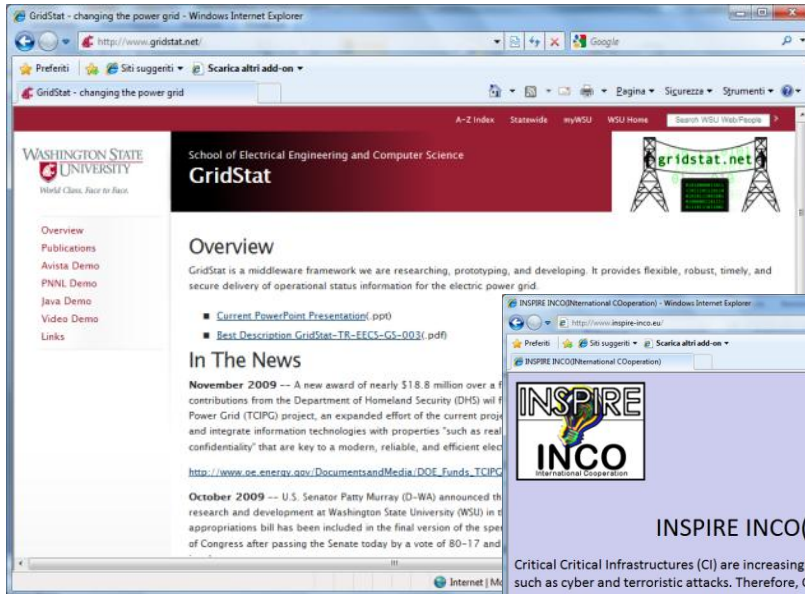
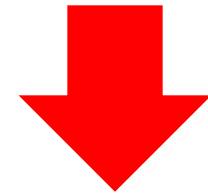
INSPIRE

**Funding for International
Cooperation:
Extension to NSF Grant
0326006**

**Funding for
Research:
EC Grant 225553**



**Funding for
Mobility:
EC Grant
248737**



Objectives -1

- To investigate the use of INSPIRE-developed policy-based management approaches with GridStat's management plane
- To investigate the use of INSPIRE-developed mechanisms for reliable delivery of control messages for the power grid, and how GridStat-developed ones can help complement those in INSPIRE
- To investigate the use of INSPIRE-developed real-time and distributed security framework in GridStat, and the use of GridStat-developed trust management system Hestia in INSPIRE

Objectives - 2

- To investigate how INSPIRE-developed techniques for diagnosis and recovery can be used to help GridStat and NASPInet recover from accidental and malicious failures
- To provide access to field data from real setups (particularly important for EU researchers)
- To share data and knowledge
- To explore the potentials of the emerging Synchro-Phasor* technology in Europe

* aka **Phasor Measurement Unit (PMU)**



More info



I N S P I R E

EC Grant Agreement n. 225553

<http://www.inspire-strep.eu>
info@inspire-strep.eu

Coordinator:

Salvatore D'Antonio

salvatore.dantonio@uniparthenope.it



I N S P I R E

EC Grant Agreement n. 225553

Thanks for your attention!