



I N S P I R E

EC Grant Agreement n. 225553

INSPIRE: INcreasing Security and Protection through Infrastructure RESilience

Luigi Romano

University of Naples "Parthenope"

luigi.romano@uniparthenope.it

ICT Fair for Trust & Security Research in the Olomouc Region
14th of May 2009 - Olomouc, Czech Republic



INSPIRE summary



EC Grant Agreement n. 225553

INSPIRE

- Two-year Specific Targeted REsearch Project (STREP)
- Work programme topic addressed
 - Objective ICT-SEC-2007.1.7: Critical Infrastructure Protection (CIP)
- Start date:
 - November 1, 2008
- End date:
 - October 31, 2010



The Consortium



EC Grant Agreement n. 225553

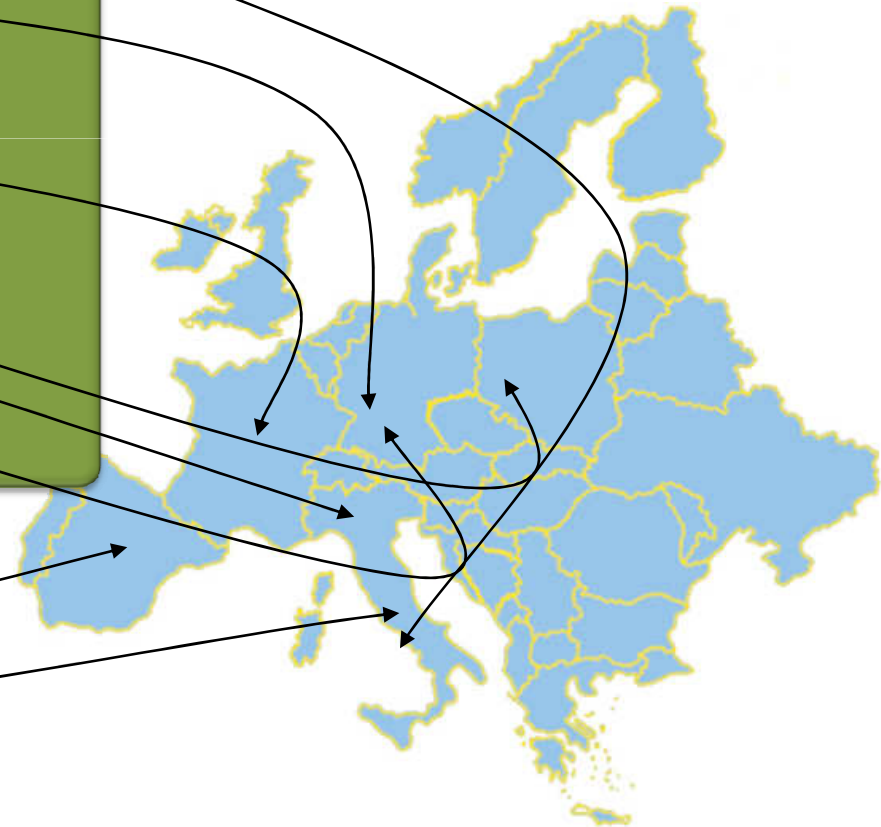
INSPIRE

ACADEMY

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

INDUSTRY

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





Setting up the scene



I N S P I R E

EC Grant Agreement n. 225553

- Evidence is showing that Critical Infrastructures (CIs) are exposed to major security risks
 - Cyber-spies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system [Reuters]
- IT guys of electric utility companies or of the Department of Homeland Security lose a lot of sleep over security exposure of their Supervisory Control And Data Acquisition (SCADA) systems
- The shared communication infrastructure has become an obvious target for disrupting a SCADA network
 - An attacker may exploit a vulnerability of the wireless trunk of a SCADA communication infrastructure to prevent real-time delivery of SCADA messages
 - This would result in the loss of monitoring information or even of the ability to control entire portions of the SCADA system



SCADA security threats

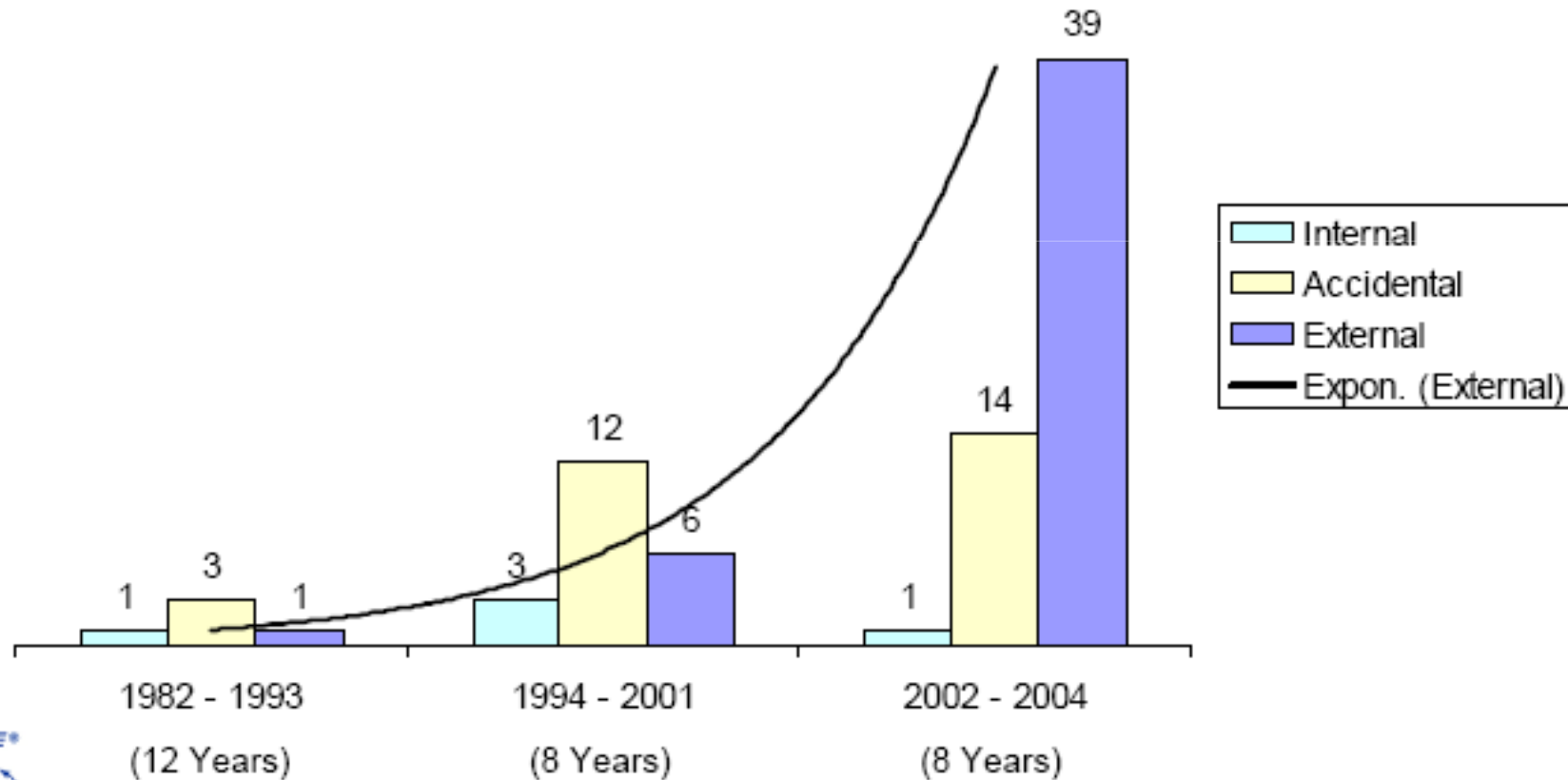


INSPIRE

EC Grant Agreement n. 225553

- **Malware**
 - SCADA systems are vulnerable to worms, viruses, Trojans, and spyware
- **Insiders**
 - This is commonly referred to as the “disgruntled employee” scenario, where a knowledgeable insider may be motivated to damage and/or to corrupt the system
- **Hackers**
 - Outsiders who want to break into SCADA systems because they are attracted by the challenge
- **Cyber Terrorists**
 - A SCADA system is the ideal target of well-funded terrorist groups seeking to cause widespread damage to a large portion of the population

BCIT Industrial Security Incident Database (ISID)



The Myths and Facts behind Cyber Security Risks for Industrial Control Systems , Eric Byres, P. Eng., Justin Lowe



Security attacks to SCADAs – 1/2



INSPIRE

EC Grant Agreement n. 225553

- **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



Security attacks to SCADAs – 2/2



INSPIRE

EC Grant Agreement n. 225553

- 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

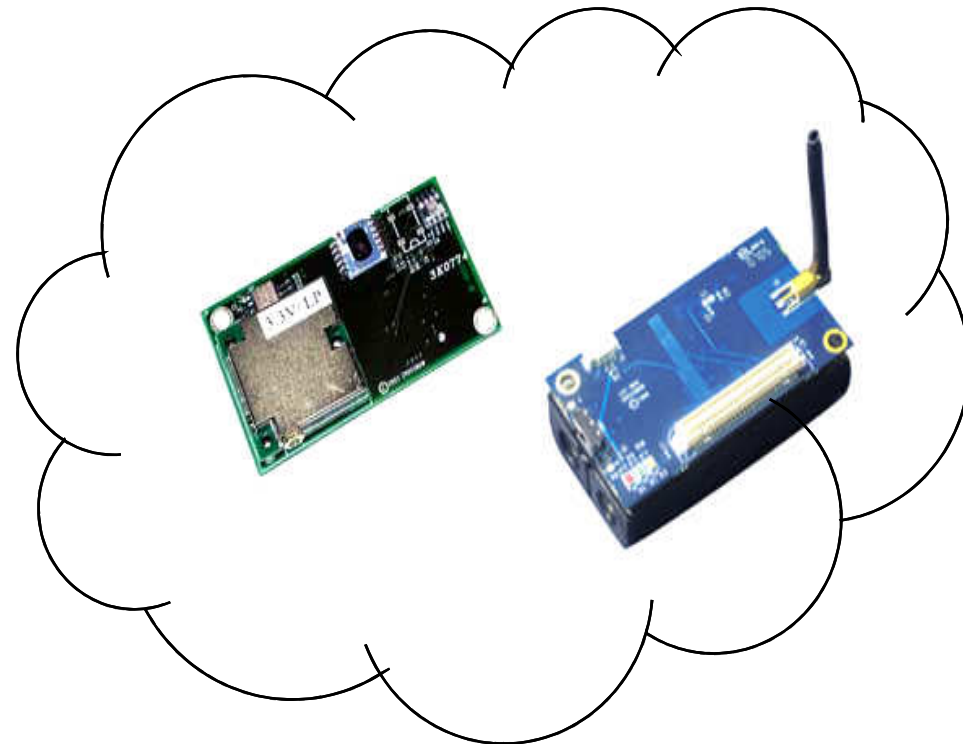
- Cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system,

<http://www.reuters.com/article/topNews/idUSTRE53729120090408>

SCADA Key components

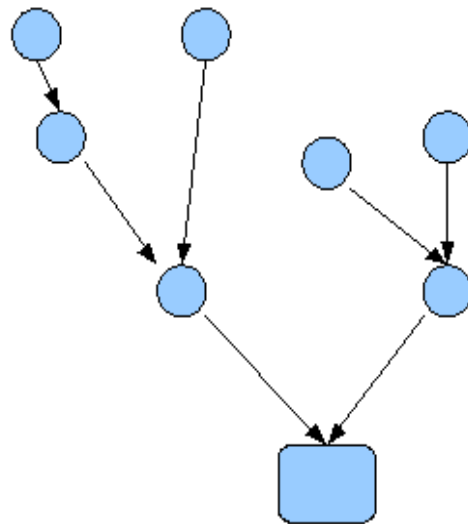


- Embedded Systems
- Wireless Sensor Networks

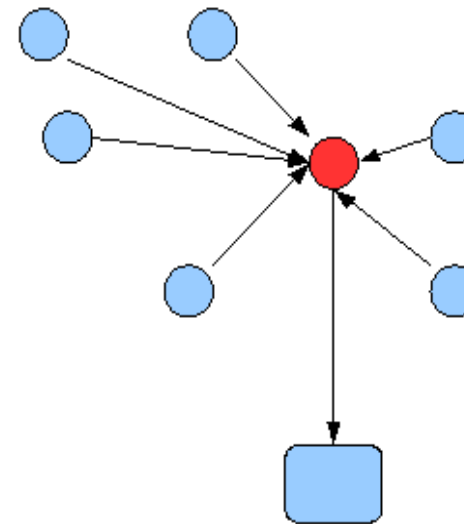


Sink-hole attack

- An intruder attracts network traffic by disseminating malicious routing information
- It then alters and/or selectively filters out individual data flows



Before the attack



After the attack



Objectives – 1/2



I N S P I R E

EC Grant Agreement n. 225553

- To analyze vulnerabilities which affect SCADA systems
- To analyze dependencies between CIs and the underlying communication networks
- To design a self-reconfigurable architecture, suited for SCADA systems
- To develop diagnosis and recovery techniques, suited for SCADA systems
- To provide SCADA traffic with Quality of Service (QoS) guarantees



Objectives – 2/2



I N S P I R E

EC Grant Agreement n. 225553

- To implement Peer-to-Peer (P2P) overlay routing mechanisms for improving the resilience of the network infrastructure
- To disseminate research results, to define best practices, and to contribute to standards for CIP
- To define a roadmap for improving the protection of CIs
- To link European CIP research to major US initiatives



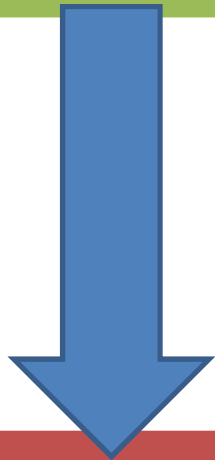
A Bird's Eye view of INSPIRE



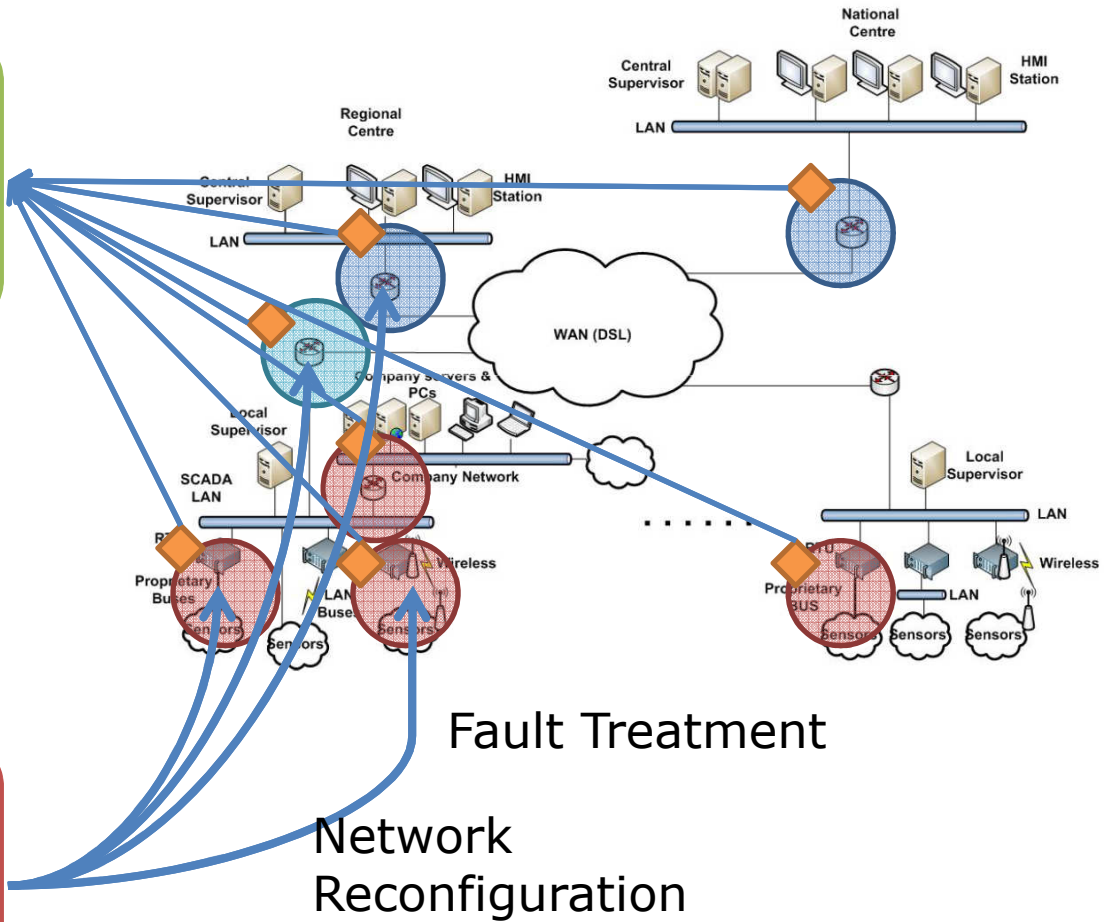
INSPIRE

EC Grant Agreement n. 225553

Diagnoser



Reconfigurator





Connections to US initiatives



INSPIRE

EC Grant Agreement n. 225553

- David (Dave) Bakken - Washington State University - and Mohsen Jafari - Rutgers University - are members of the INSPIRE Group of Experts
- Both of them participate in a number of NSF projects on Critical Infrastructure Protection (CIP)
- Dave Bakken:
 - is the coordinator of the GridStat project on power grids protection
 - is very involved with the TCIP (Trustworthy Cyber Infrastructure for Power) center
- **A joint project proposal between INSPIRE and GridStat has been submitted to Call 4 ICT, Objective 9.2 “Supplements to Support International Cooperation between Ongoing Projects”**



More info



EC Grant Agreement n. 225553

INSPIRE

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

Coordinator:

Salvatore D'Antonio

salvatore.dantonio@uniparthenope.it

Technical Lead:

Luigi Romano

luigi.romano@uniparthenope.it