INTERSECTION
Project

EC Grant Agreement n. 216585
Salvatore D’Antonio
CINI
saldanto@unina.it

ICT Fair for Trust and Security Research – Olomouc, 19 May 2009
Project overview

- **IN-TE-R-SE-C-T-I-O-N**: Infrastructure for heterogeneous, Resilient, Secure, Complex, Tightly Inter-Operating Networks

- **Work programme topic addressed**
  - Challenge 1: Pervasive and Trusted Network and Service Infrastructures
  - Objective ICT-2007.1.4: Secure, dependable and trusted infrastructures

- Start date: January 1st, 2008
- Duration: 24 months
The Consortium

ACADEMY
- Consorzio Interuniversitario Nazionale per l’Informatica [Italy]
- Lancaster University [UK]
- Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung [Germany]
- Eidgenoessische Technische Hochschule Zuerich [Switzerland]

INDUSTRY
- Elsag Datamat (Coordinator) [Italy]
- Thales Research and Technology [UK]
- ITTI (SME) [Poland]

END USERS
- Telefonica ID Investigación y Desarrollo [Spain]
- Telespazio [Italy]
- Polska Telefonia Cyfrowa [Poland]
Project Motivation

MORE PROTECTION IS NEEDED

MORE PROTECTION IS NEEDED

HETEROGENEOUS COMMUNICATION INFRASTRUCTURES

MORE PROTECTION IS NEEDED

increasing complexity and heterogeneity of the communication networks

progressive disuse of dedicated communication infrastructures and proprietary networked components, together with the growing adoption of IP-based solutions

HUGE CRITICAL INFRASTRUCTURES

threats coming from cyberspace

failures in the information exchange

cascade effects caused by relationships among infrastructures

acts of terrorism and other extreme events
Heterogeneous networks

• Networks based on different low-level protocols (physical, data link)
• A data network composed of devices from different manufacturers and/or different types of LANs
• A heterogeneous network is a network connecting computers and other devices with different operating systems and/or protocols, services and applications
• Interconnection of different type of networks relying on different communication technologies
• Interconnection of networks managed by different telecom operators adopting diverse security policies
Main objectives and principles

Identify and classify the vulnerabilities of heterogeneous and interconnected network infrastructures (wired, wireless, satellite, mobile networks)

Create and maintain a network vulnerability database

Design and implement an integrated network security framework including different components and tools:
- detecting anomalous events
- reacting to well-known, as well as new kinds of anomalies
- deploying truly distributed countermeasures against ongoing attacks
- providing systems with mechanisms for intrusion tolerance, i.e. preventing intrusions from generating a system failure
Expected Project results and innovation

Contribution to **STANDARDS** (IETF, ETSI)

**ROADMAP** to guide telecom operators in the adoption of security-enhancing strategies

Security and resiliency **METRICS**

Integrated **NETWORKSECURITY FRAMEWORK**:
- specification
- prototype

**VULNERABILITY DATABASE AND ONTOLOGY**
Impact

A STRONG AND COMPETITIVE ICT INDUSTRY IN EUROPE

December 31st 2009

VULNERABILITY ANALYSIS
ARCHITECTURAL DESIGN
NOVEL SECURITY AND RESILIENCY TECHNIQUES
DEMONSTRATION, VALIDATION, BENCHMARKING

GROUP OF EXPERTS

European Telecommunications Standards Institute, Federuntility, ACEA, IRIDE, SAG Group, INTRAS, Hitachi Europe, ACOFI, Vodafone Group, PWR, Acque Torino, British Telecom Group, Societa Metropolitana

http://www.intersection-project.eu
info@intersection-project.eu

January 1st 2008

EC Grant Agreement n. 216585
Project status

- State of the art and requirements analysis: completed
  - State of the art
  - Vulnerabilities of heterogeneous networks
  - Requirements specification

- Specification of the framework: completed
  - Framework architecture
  - Vulnerability database and ontology

- Design and development: in progress
  - Innovative techniques for intrusion detection
  - Data visualization techniques
  - Topology discovery tools
The real-time intrusion detection and tolerance system
The INTERSECTION Intrusion Detection System
Network-based Intrusion Detection

EC Grant Agreement n. 216585
Building the demo network

- Built over GEANT and national NRENs
- GRE tunnels are used to provide an Internet-like VPN for INTERSECTION demonstration, integration, and testing activities
- All available INTERSECTION labs (TID, PTC, Telespazio and Elsag Datamat) and integration testbed are fully interconnected, and SW developers have indirect access for integration and testing activities
Contacts

- Website: http://www.intersection-project.eu
- Information: info@intersection-project.eu
- Technical Coordinator: saldanto@unina.it
- Project Coordinator: Stefano.Vertechi@ElsagDatamat.com
- Dissemination: Marcello.Antonucci@ElsagDatamat.com