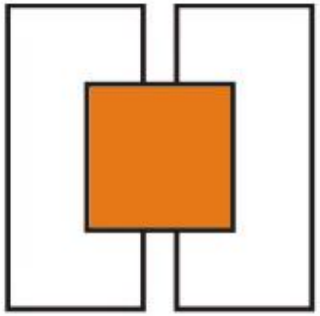


inter SECTION

The INTERSECTION Research Project

EC Grant Agreement n. 216585

Stefano Vertechi
INTERSECTION Project Coordinator
stefano.vertechi@elsagdatamat.com

SEVENTH FRAMEWORK PROGRAMME

ELSAG DATAMAT
A Finmeccanica Company

cini
Consorzio Interuniversitario Nazionale per l'Informatica

LANCASTER UNIVERSITY

THALES

FOKUS

Fraunhofer
Institute for Open Communication Systems

Telefónica

iTTi
e-technologies & business

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

TELESPAZIO
A Finmeccanica / Thales Company

era
MOŻESZ WIECEJ

EC Grant Agreement n. 216585

Outline

- Security and Resilience: current scenario and open issues
- Proposals for research work on resilience
- A bird eye view of the INTERSECTION research project
- Additional info on INTERSECTION

inter SECTION

EC Grant Agreement n. 216585

Security and Resilience: Current Scenario and Open Issues

SEVENTH FRAMEWORK PROGRAMME

Life in an interconnected world
The PERFECT WORLD version

EC Grant Agreement n. 216585

- Hardware is becoming more and more powerful (as well as cheaper and cheaper), while still exhibiting an easy-to-predict, highly deterministic behaviour
- A variety of network technologies makes seamless integration of individual systems possible, allowing to build highly-dependable Systems of Systems (SoS)
- The resulting SoS, although extremely complex, are easy to use and manage
- A plethora of applications - ranging from e-government to entertainment - is deployed at no risk (since failures do not exist and bad guys are locked out at all times)

Life in an interconnected world
The REAL WORLD version

EC Grant Agreement n. 216585

- Hardware cost is indeed dropping, and computing power is increasing dramatically. Embedded systems have become pervasive (there will be more than 3 embedded systems per person by 2010!) but they have also become more complex than a Main Frame of some ten years ago
- Many different network technologies – optic, WiMax, Ethernet (in a variety of flavours), WiFi, Bluetooth, NFC – are being interconnected, but this leads to a number of interoperability and security problems
- Properly configuring and managing the resulting SoS has become a security and availability nightmare
- Despite such problems, complex distributed SoS are being extensively used for deployment of critical services, with challenging requirements in terms of resilience

Current Protection Approach
Basic Network Elements

EC Grant Agreement n. 216585

- **Network endpoints** (computers) *should* have local security agents (antivirus software, password policies, good system administration)
- **Network elements** (routers and probes) can provide IP metrics, detect patterns and apply filtering rules
- **Network security** is based on Intrusion Detection Systems (IDSs) that interact with network elements

Current Protection Approach
Intrusion Detection Systems

EC Grant Agreement n. 216585

- **IDSs are centralized and located off-network, at Security Operation Centres**
  - ⇨ They typically work in isolation and are thus unable to provide any support in terms of active resilience
- **IDSs do not support real time analysis**
  - ⇨ They're slow! In many cases a late detection of an attack cannot prevent or mitigate damages
- **IDSs do not cooperate among them**
  - ⇨ Every network carrier has its own IDS that does not share critical attack information with contiguous IDSs operated by commercial competitors
  - ⇨ In case of distributed attacks, two contiguous IDSs might discover only part of the evidence required to trigger a fruitful reaction

EC Grant Agreement n. 216585

Proposals for Research Work on Resilience

SEVENTH FRAMEWORK PROGRAMME

Suggested Main Research Themes

EC Grant Agreement n. 216585

- **Real-time processing of security-related data**
  - How to filter, process, and correlate information coming from a variety of sources (e.g. network infrastructure, application logs, operating system data structures, and more) in order to raise alarms in a dependable (i.e. reliable and timely) fashion
- **Intrusion Tolerance**
  - How to build systems that deliver a dependable service even when intruders break in
- **Effective diagnosis for complex networked systems**
  - How to filter, process, and correlate information, so as to:
    - assess the extent of the damage in individual system components
    - trigger recovery actions

IDS Technology Challenges

EC Grant Agreement n. 216585

- **IDSs should react automatically and in real-time**
  - they have to react soon, before damage is made
  - reactions must intelligently take into account their own side-effects, e.g. the impact of reaction on SLA on provided network services
- **IDSs should be located in-network**
- **IDSs should be distributed and redundant to improve resilience**
- **IDSs should cooperate horizontally with peers**
  - information exchange can allow a deeper and more effective analysis
- **IDSs should be modular**
  - several detection technologies can be deployed as additive, cooperative and pluggable modules thus making IDSs more flexible

EC Grant Agreement n. 216585

A bird eye view of The INTERSECTION research project

The INTERSECTION Project

EC Grant Agreement n. 216585

- **In**frastructure for he**te**rogeneous, **r**esilient, **se**cure, **c**omplex, **t**ightly **i**nter-**o**perating **n**etworks
  - FP7, Area 5 sub-programme: “Security, Privacy and Trust in the Future Internet”
    - Creation of a trustworthy and resilient Future Internet as a conglomerate of networks and systems, with built-in security, dependability, privacy and trust
    - Enabling users to understand security, privacy and trust in the Future Internet
  - Start date: January 1st, 2008
  - Duration: 24 months
- **Part of the Future Internet programme**

The INTERSECTION Consortium

EC Grant Agreement n. 216585

ACADEMIA

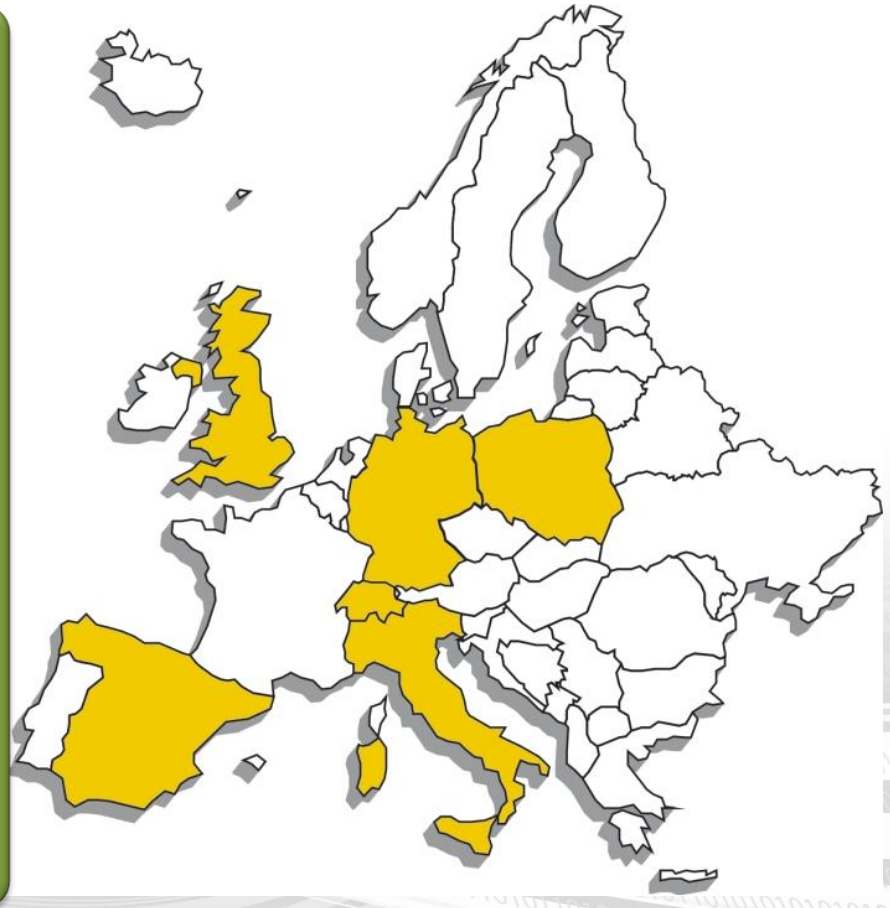
- Consorzio Interuniversitario Nazionale per l'Informatica
- Lancaster University
- Fraunhofer Gesellschaft Zur Foerderung Der Angewandten Forschung
- Eidgenoessische Technische Hochschule Zuerich

INDUSTRY

- Elsag Datamat (Coordinator)
- Thales Research and Technology
- ITTI (SME)

END USERS

- Telefonica Investigación y Desarollo
- Telespazio
- Polska Telefonia Cyfrowa



Project Focus

EC Grant Agreement n. 216585

Main Project Objectives

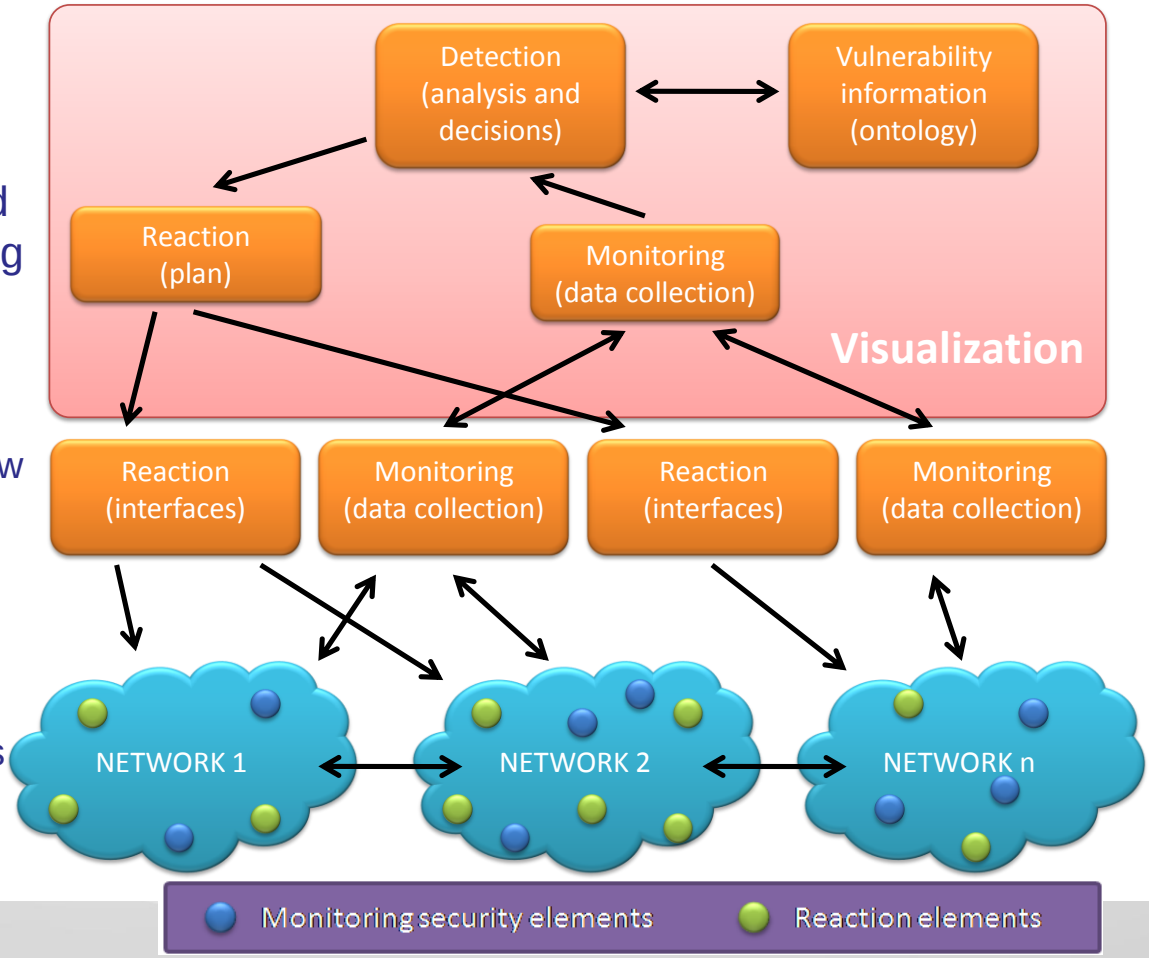
EC Grant Agreement n. 216585

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

Create a European vulnerability database

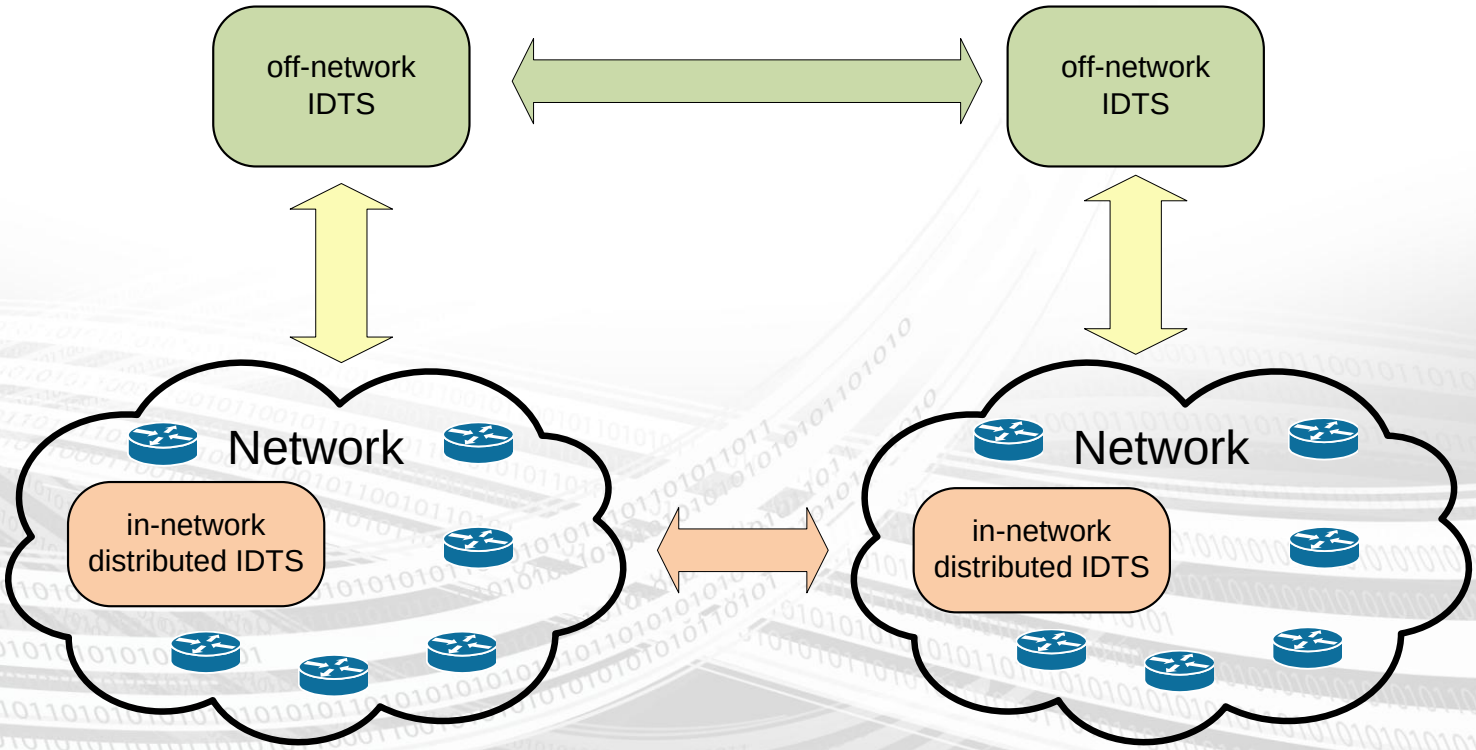
Design and implement an integrated network security framework including different components and tools able to:

- detect anomalous events
- react to well-known, as well as to new forms of anomalies
- deploy distributed countermeasures against evolving threats
- provide mechanisms for intrusion tolerance to reduce the likelihood of intrusions generating system failures



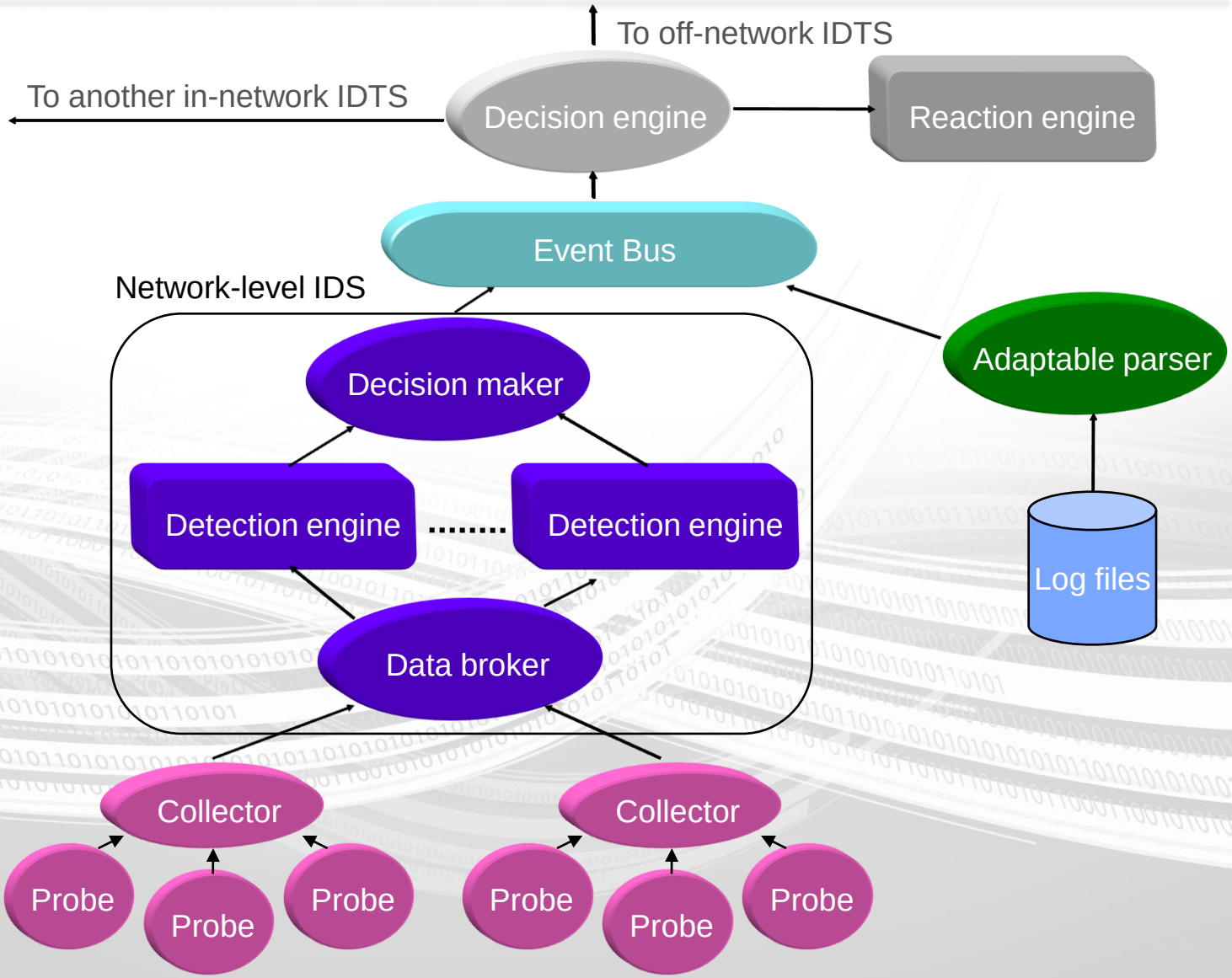
Intersection Top-level Architecture

EC Grant Agreement n. 216585



Intersection Framework Architecture
In-Network Elements

EC Grant Agreement n. 216585



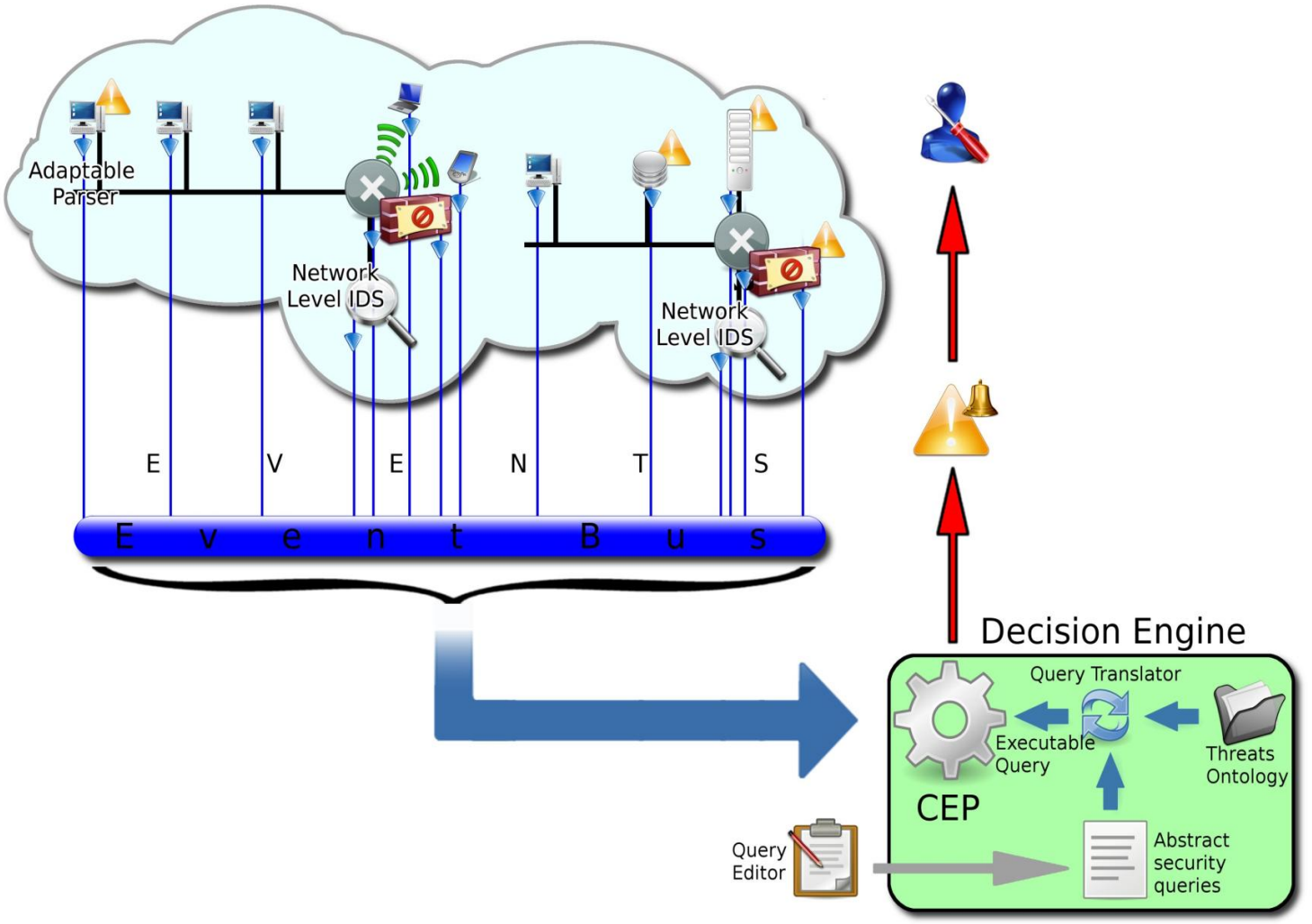
EC Grant Agreement n. 216585

Main IDS Research Related Issues

- A key activity in Intrusion Detection is dependable (i.e. accurate and timely) information extraction from multiple data feeds
- Ability to process data streams in real-time is crucial
- Correlation analysis is needed for improving detection while reducing false positives
- Data feeds can be highly heterogeneous (ranging from Web server logs to firewall traces), but the definition of a unified format for all data feeds is not a viable solution, especially when dealing with COTS and/or a (typically large) installed base of proprietary technologies

Architecture of the INTERSECTION IDS

EC Grant Agreement n. 216585



References

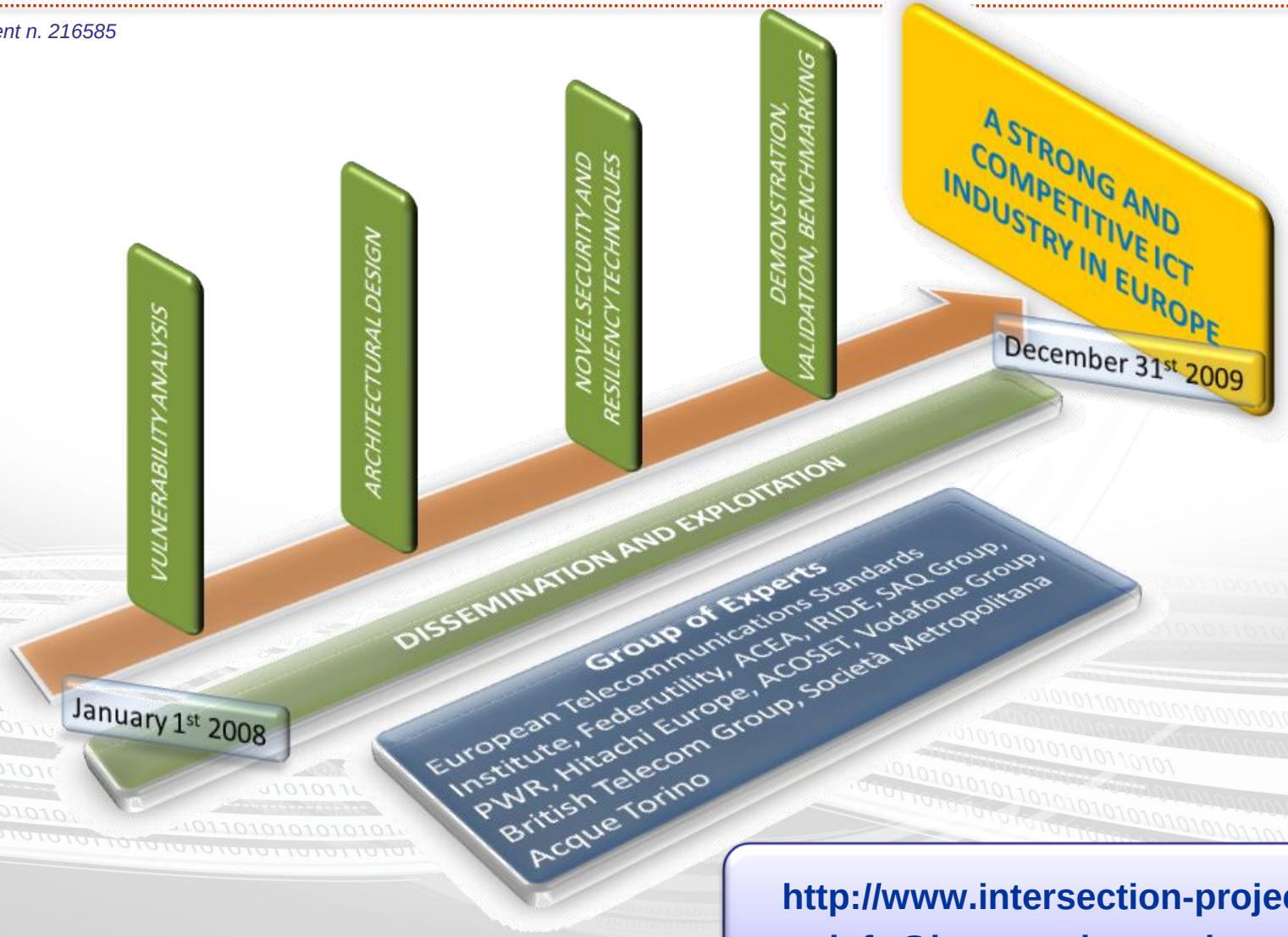
- Dingbang Xu and Peng Ning, “Correlation Analysis of Intrusion Alerts”, Advances in Information Security, Intrusion Detection Systems, Springer US, Volume 38, pagg. 65-92, 2008
- Kruegel, C. 2004 "Intrusion Detection and Correlation: Challenges and Solutions". Springer-Verlag TELOS
- “The ESRAB report”, September 2006
- “The Essential Guide to Semiconductors” - James L. Turley

EC Grant Agreement n. 216585

Additional info on INTERSECTION

Project Plan

EC Grant Agreement n. 216585



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

Expected Project results and innovation

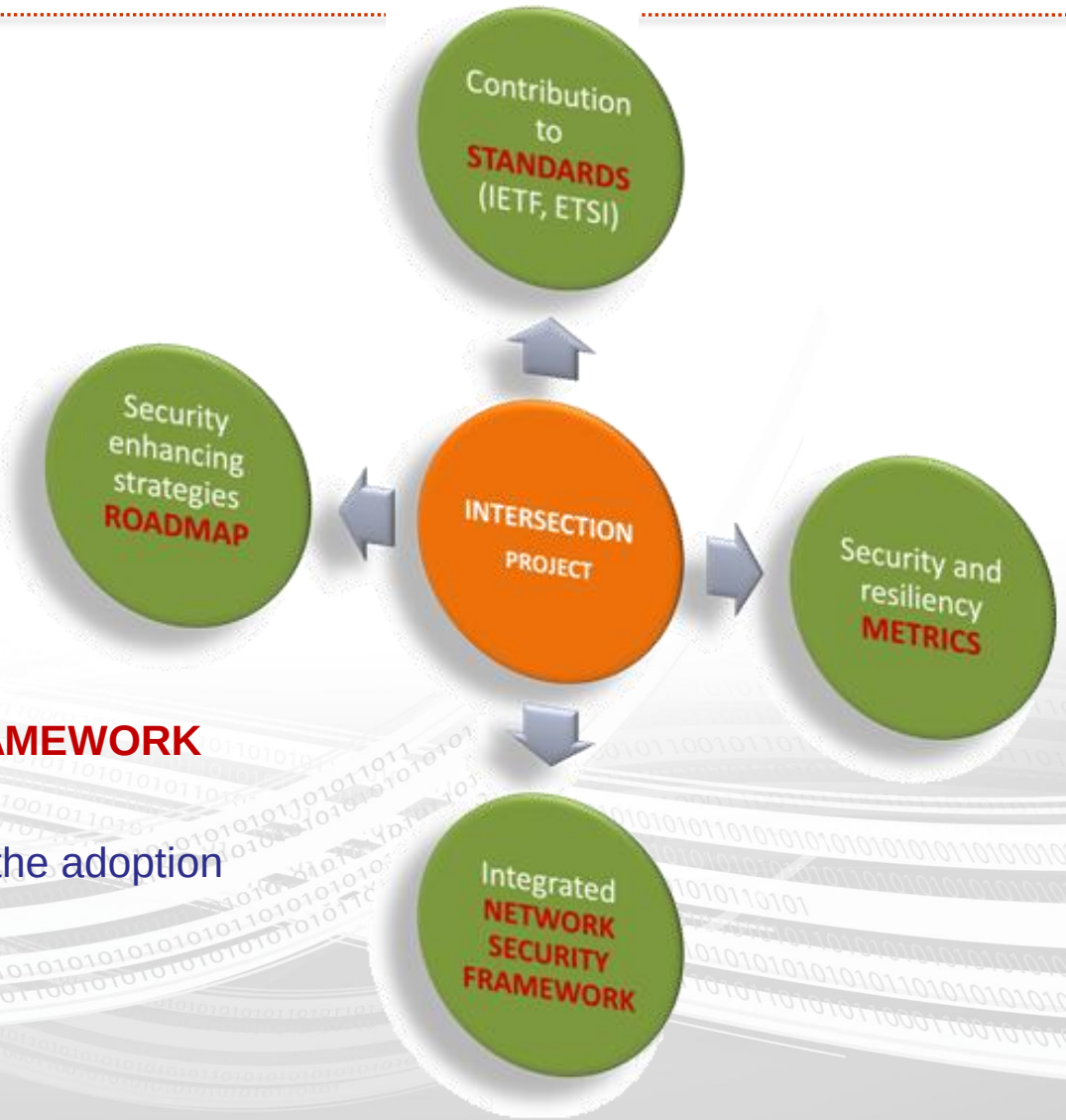
EC Grant Agreement n. 216585

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

Security and resiliency **METRICS**

Integrated **NETWORK SECURITY FRAMEWORK**

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



Intersection Framework Architecture
Off-Network Elements

EC Grant Agreement n. 216585