

INTERSECTION – Resiliency and Security for Heterogeneous Communication Infrastructures

Stefano Romani



A common feature of the critical infrastructures – the electricity grid, oil and natural gas production, transportation and distribution and water supply networks – is emerging; each relies increasingly on the widespread use of networked systems and components to provide more efficient and innovative services and to meet novel user requirements and expectations.

In the past, critical infrastructures were physically and logically separate systems with little interdependence. As digital information gained more and more importance in the operation of such infrastructures, what we might call a ‘cyber component’ of each critical system grew. These cyber components are currently connected through heterogeneous networks and represent the information infrastructure on which critical systems depend.

Unfortunately the growing complexity and heterogeneity of the communication networks used to interconnect such cyber components also increased their level of vulnerability. Furthermore, the progressive disuse of dedicated communication infrastructures and proprietary networked components, together with the growing adoption of IP-based solutions, exposes critical information infrastructures to cyber-attacks from the Internet.

These infrastructures are thus characterised by a vulnerability level similar to other systems connected to the Internet, but the socio-economic impact of their failure can be huge.

It is therefore extremely important to protect network infrastructures from attacks and failures in order to ensure the secure end-to-end transmission of control information generated by critical systems.

A further element complicates the situation: traffic flows generated by the geographically distributed systems devoted to controlling critical information infrastructures usually cross multiple network domains. Thus, issues linked to the transport of information in an inter-domain environment must be addressed in order to effectively manage and control the elements of the infrastructure. In addition, computer security incidents usually occur across administrative domains, spanning different organisations and national borders. In the case of distributed attacks, it is likely that different aspects of a single incident will be visible to different systems. For these reasons, it is clear that it would be advantageous for different organisations and network operators to be able to share data on attacks in progress. The exchange of incident information and statistics among involved parties is crucial for both the detection of ongoing attacks and the proactive identification of trends that could lead to incident prevention.

Organisations and network operators have always been reticent about disclosing information about attacks on their systems or through their networks. However, this tendency seems now to be outweighed by a new awareness that it is only through co-operation that networking infrastructures can be made robust to attacks and failures.

In the light of this, it is clear that there is a need to deploy a common framework that allows different systems and technologies to interoperate in the field of security through the development and adoption of standard solutions, interfaces and protocols.

INTERSECTION – **I**nfrastructure for **HeT**erogeneous, **R**esilient, **SE**cure, **C**omplex, **T**ightly **I**nter-**O**perating **N**etworks – is a research project co-funded by the European Commission under the FP7 ICT Work Programme 2007-08 (ftp://ftp.cordis.lu/pub/fp7/ict/docs/ict-wp-2007-08_en.pdf – Objective 1.4: Secure, dependable and trusted infrastructures) which is operating in this context. Its aim is the design and implementation of an integrated framework made up of different subsystems and components which

provide network and infrastructure security. A working prototype will be implemented to be used as a final demonstrator of specific scenarios.

In order to achieve its objectives, INTERSECTION has identified the following technical areas of work:

- Analysis and classification of the vulnerabilities in heterogeneous networks
- Requirements analysis and the design of an integrated framework comprising different security tools
- Development of techniques and tools for increasing the security and resilience of networked systems
- Integration of the developed tools and their validation.

The keywords of the INTERSECTION project are *networked co-operation*. The project aims to propose a novel security strategy on four planes, whereby network entities share information needed in order to:

- Try to prevent attacks (**Co-operative Prevention**)
- Detect the attack, in case it bypasses prevention barriers (**Co-operative Detection**)
- React effectively to the attack (**Co-operative Reaction**)
- Tolerate intrusions (**Co-operative Tolerance**).

The Consortium represents a good balance of representatives of academia, industry and end-users: ElSag Datamat (Project Co-ordinator), Consorzio Interuniversitario Nazionale per l'Informatica, Thales Research & Technology, Lancaster University, Telefonica Investigacion y Desarrollo, Fraunhofer Gesellschaft zur Förderung der angewandten Forschung, Coronis Systems, ITTI, Eidgenössische Technische Hochschule Zürich, Telespazio and Polska Telefonia Cyfrowa.

The project began operation in January 2008, and will run for 24 months.

For further information, please contact the Consortium at info@intersection-project.eu or visit the Project website at www.intersection-project.eu.

Stefano Romani (stefano.romani@elsagdatamat.com) is with ElSag Datamat spa and is the Project Manager of the INTERSECTION FP7 project.