EURO-MILS: Secure virtualisation for trustworthy applications in critical domains

Security-related Definitions and Semantics

MILS: Multiple Independent Levels of Security is a high-assurance security architecture based on the concepts of separation and controlled information flow.

Embedded system Safety and Security: Embedded systems must be safe and secure, that is the environment is unable to affect the system in an undesirable way as well as the system unable to affect its environment in an undesirable way.

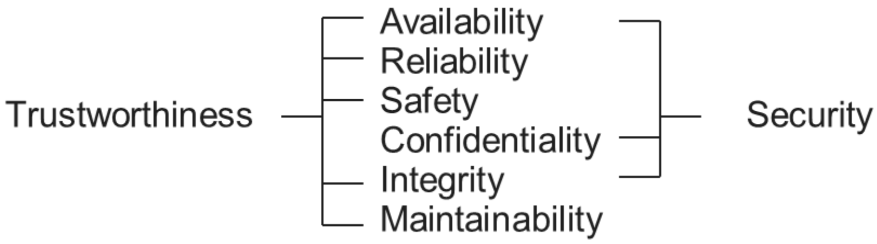
Trustworthiness (a.k.a Dependability): Trustworthiness is the ability for a system to deliver service that can justifiably be trusted:

Information security can also require :

- *Accountability:* Availability and integrity of the person who performed the operation.
- *Authenticity:* Integrity of a message content and origin, and possibly of some other information, such as time of emission.
- *Non-repudiability***:** availability and integrity of the identity of the sender or receiver of a message.

Assurance: The level of guarantee that a secure system will behave as expected.

Risk: A possible event which could cause a loss.



- *Availability:* readiness for correct service.
- *Reliability:* continuity of correct service.
- *Safety:* absence of catastrophic consequences on the user(s) and the environment.
- *Integrity:* absence of improper system alterations.
- *Maintainability:* ability to undergo modifications and repairs.

Information Security: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

- *Confidentiality*: A requirement that private or confidential information not be disclosed to unauthorized individuals.
- *Integrity*: Information has integrity when it is timely, accurate, complete, and consistent.
- *Availability*: A requirement intended to assure that systems work promptly and service is not denied to authorized users.

- *External risk***:** When someone outside the organization “breaks into” the organization information network to try to secure items of value.
- *Internal risk:* When an organization´s employees or authorized users access the information network to secure personal information for their own benefit.
- *Human error risk:* An information security network may be improperly designed leaving some employees at risk for error and causing harm to the organization.

Vulnerability: A weakness in a target that can potentially be exploited by a security threat.

Threat: A method of triggering a risk event that is dangerous.

Exploit: A vulnerability that has been triggered by a threat.

Countermeasure: A way to stop a threat from triggering a risk event.

EURO-MILS at a glance

Project number:
318353

EURO-MILS mission:
The mission of the EURO-MILS project is to develop a solution for virtualisation of heterogeneous resources and provide strong guarantees for isolation of resources by means of Common Criteria certification with usage of formal methods.

Project start:
01.10.2012

Project end:
30.09.2015

Total costs:
EUR 8.447.558

EC contribution:
EUR 6.000.000

Consortium:
14 partners from 5 different countries.

Project Coordinator:
Dr. Klaus-Michael Koch
coordination@euromils.eu

Technical Leader:
Dr. Sergey Tverdyshev
sergey.tverdyshev@sysgo.com

Project website:
www.euromils.eu

Acknowledgements
The EURO-MILS project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-318353.

SEVENTH FRAMEWORK PROGRAMME

Many of the definitions are derived from A. Avizienis, J.C. Laprie, B. Randell, C.Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Transactions on Dependable and Secure Computing*, Vol.1, No.1, Jan-March 2004