Trusted Computing Engineering for Resource Constrained Embedded Systems Applications

Deliverable D1.4

Project Presentation

Project:	TERESA
Project Number:	IST-248410
Deliverable:	section for D1.4
Title:	Project Presentation
Version:	v1.0
Confidentiality:	Public
Author:	Barbara Raither (Trialog)
Date:	10 February 2010

Part of the Seventh Framework Programme
Funded by the EC - DG INFSO

Table of Contents

1 Document History

Version	Status	Date
V0.1	draft	15/01/2010
V0.2	final	10/02/2010

Approval		
	Name	**Date**
Prepared	Antonio Kung	12/02/2010
Reviewed	All Project Partners	15/02/2010
Authorised	Antonio Kung	15/02/2010
Circulation		
Recipient	Date of submission	
Project partners	10 June 2010	
European Commission	15 June 2010	

2 List of Participants

No.	Consortium Partners
1	**TRIALOG** Project Co-ordinator TRIALOG 25 rue du Général Foy 75008 Paris, France
2	**escrypt** escrypt GmbH - Embedded Security Lise-Meitner-Allee 4 D-44801 Bochum Germany
3	**Fraunhofer SIT** Fraunhofer Institut SIT Rheinstr 75 64295 Darmstadt German
4	**Ikerlan IK-4** Ikerlan Pº J.M. arizmendiarrieta 20500 Mondragon Spain
5	**IRIT** Université de Toulouse 2 - Le Mirail Département de Mathématiques-Informatique 5 allées Antonio Machado 31058 Toulouse France
6	**University of Siegen** Universität Siegen Hoelderlinstrasse 3 57076 Siegen Germany

3 Co-ordinator Contact Details

Partner	TRIALOG
Contact person	Antonio Kung
Address	25 rue du Général Foy 75008 Paris, France
Telephone	+33 1 44 70 61 03
Fax	+33 1 44 70 05 91
e-mail	antonio.kung@trialog.com

4 Project Data

Contract Number	INFSO-ICT-248410
Project Acronym	TERESA
Project Name	**T**rusted Computing **E**ngineering for **R**esource Constrained **E**mbedded **S**ystems **A**pplications
Duration	36 months
Execution	1 November 2009 - 31 October 2012
Contract Type	Collaborative project (generic)

5 Cost and Funding

Funded Under	7th FWP (Seventh Framework Programme)
Total Cost	3.79 million euro
EU Contribution	2.9 million euro

6 Project Image

Project Website	http://www.teresa-project.org
Project Factsheet	Available on the TERESA web site [1] Also included in Publication: ICT-2009.3.4 Portfolio of embedded system projects
Project Flyer	Preliminary version included in D8.1 Dissemination Material
Project Logo	

7 Project Presentation

7.1 Key Words

- Trust
- Security
- Dependability
- Patterns
- Resource Constrained Embedded Systems
- Model Driven Engineering

7.2 Goal

The goal of TERESA [1] (**T**rusted Computing **E**ngineering for **R**esource Constrained **E**mbedded **S**ystems **A**pplications) is to define, demonstrate and validate an engineering discipline for trust that is adapted to resource constrained embedded systems. We define trust as the degree with which Security and Dependability (S&D) requirements are met.

7.3 Objectives

Resource Constrained Embedded Systems (RCES) have the following characteristics:

- They belong to different application sectors.
- They have statically determined computing resources which are usually allocated through a process consisting of a configuration phase and a building phase.
- They are generally high integrity systems with strong assurance requirements. They therefore use advanced engineering disciplines.
- Many different application sectors can benefit from their use.

TERESA has the following objectives:

- Provide guidelines for the specification of sector-specific RCES trusted computing engineering. Software process engineers in a given sector use the guidelines to define a trusted computing engineering process that is integrated with the software engineering process used in the RCES sector.
- Define a trusted computing engineering approach that is suited to the following sectors:
  - Automotive
  - Home control
  - Industrial control
  - Metering.

7.4 Approach

The proposed approach is to use a model-based repository of security and dependability patterns:

- Application sector trust models are defined as profiles (e.g. UML, SysML profiles), based on a common trust meta-model.
- Security and dependability platform independent patterns are identified and defined for each application sector (while some patterns could be used by several application sectors).
- Formal properties on security and dependability are defined and validated for patterns belonging to application sectors requiring a specific level of assurance.
- Platform dependent implementation of the patterns is guided by very precise requirements.

The engineering process for resource constrained embedded systems will be validated in the four application sectors listed above.

Defining an engineering discipline for trust that is adapted to resource constrained embedded systems must take into account the described trend, since not all RCES have the same needs. The TERESA approach is to use a **model-based approach coupled with a repository of security and dependability patterns.**

Patterns are widely used today to specify architecture and design aspects. They refer to templates describing a solution to solve a commonly occurring problem. Most importantly, they can be provided by security and dependability experts who might not be always available in companies involved in the development of RCES.

Models are abstractions which are closer to particular domain concepts and are decoupled from implementation concepts. Model-Driven Engineering (MDE) is widely used in embedded systems where assurance requirements are important. This allows implementation independent validation of models, for instance, generally considered as an important assurance step. The TERESA vision is that security and dependability patterns that are derived from / associated with domain specific models will help application developers to integrate application building blocks with security and dependability building blocks. This is the reason why we are advocating the use of a **pattern repository, where patterns can be integrated in application models.**

- A common trust meta-model will serve as the foundation of the whole repository. Trust meta-models have been studied in the ITEA TECOM project [2]
- Domain specific trust models based on the common trust meta-model will be defined, i.e. they will cope with specific needs of a given application sector. Well known trust models are Examples of well known trust models are Bell-la Padula [7] and role-based access. Trust models will generally focus on the specification of policies to protect access to assets (e.g. who has the right to download software in au automotive control electronic). Domain specific trust models to protect vehicle intrusion are being studied in the ITS EVITA project [3] which will be input to TERESA. The resulting application sector trust models should be defined as profiles of well known modelling languages (e.g. UML, SysML).
- Security and dependability patterns, are not only defined from a platform independence viewpoint (i.e. they are independent from the implementation), but they are also expressed in a consistent way with domain specific trust models. Consequently, they will be much easier to understand and validate by application designers in a specific area.

Depending on the assurance requirements for a pattern, **formal verification or security and dependability patterns** could also be needed. This work has been carried out within the Serenity project for the evaluation and validation of TPM based solutions. In TERESA formal properties on security and dependability will be defined and validated for each pattern belonging to a domain area where this is required.

7.5 Trust Engineering

Once the repository is available, it must serve an underlying **trust engineering process** that must also be domain specific. To this end, TERESA will also define a trust engineering meta-model from which **domain specific trust engineering** models can be defined. The association of a trust engineering meta-model with guidelines to define a domain specific trust model can be considered as the overarching contribution of TERESA. The resulting engineering approach for resource constrained embedded systems will be validated in four application sectors: automotive systems, home control systems, industry control, and metering. In other words, the trust engineering meta-model will be associated with four validated trust engineering models.

For each individual domain application we will have:

- A trust model based on a common trust meta-model, associated with a number of security and dependability patterns. If required by the domain application, the pattern will be formally verified and validated.
- A trust engineering model based on a common trust engineering meta-model. Trust engineering models and trust models are associated as part of the same domain specific ontology.
- A resulting **documented and tool supported domain specific trust engineering process** supported by the repository as well as a number of guidelines will facilitate 1) the populating of the repository with

further security and dependability or S&D patterns, and 2) the transformation of the S&D patterns into platform dependent specifications. When a pattern has been formally validated, implementations with automatic **derived guidelines for platform dependent implementation of the patterns** will be available.

The common trust engineering meta-model will have to recognize the need to separate expertise on applications (represented by an application designer), expertise on security and dependability (represented by an S&D engineer), and expertise on repository development (represented by a model-driven and pattern engineer). As a result, individual application domains could have different trust engineering processes, for example, a domain where application engineers do not use model-driven engineering should have a more decoupled interaction with the pattern repository.

7.6 Expected Impact

TERESA contributes to the security and reliability of Information and Communication Technology (ICT) through the increased productivity of embedded system development. The engineering process promotes the separation of engineering concerns. It provides application designers with the following benefits:

- The reuse of state-of-the-art S&D solutions.
- The advantage of MDE and pattern based approaches. The MDE approach allows the reuse of S&D artefacts at an earlier stage of design.
- The repository access tool allows application designers to have the advantage of MDE even though they do not use MDE for application design and are not experts in modelling.

TERESA's engineering process takes into account domain specific processes. This allows for the support of specific standards, as well as the assurance of the approach.

TERESA's open repository facilitates the emergence of new tools for repository access. This will in turn encourage the emergence and growth of new companies.

TERESA contributes to European leadership in embedded system design and competitiveness in the area of trusted computing engineering of resource constrained embedded systems.

In the future, new systems used for the Internet, for alternative paths to ICT components and systems, and for ICT sustainable development will be resource constrained embedded systems. By focusing on the trusted computing engineering aspects of such systems, TERESA will contribute to the advent of such breakthroughs.

7.7 Exploitation Plan

The following exploitation items have been identified:

- Engineering process meta-models and domain specific models
- Trust meta-models and domain specific models
- Initial wealth of patterns for the four application domain (automotive, home control, industry control, metering)
- Guidelines for engineering
- Repository structure.
- Repository prototype
- Repository access tools.

All specification documents will be public. All digital representations of models and patterns will also be public. The repository structure specification will be available for further development. The repository, while being a prototype, will be freely available, and when possible it will be based on tools that are publicly available. Access tools will also be available freely for research and development.

The target market and market potential is the following:

- Resource constrained embedded systems (RCES) can be found everywhere, in different application sectors (e.g. automotive, aerospace, home control), in different form factors (e.g. stand-alone systems, peripheral subsystems to main computing systems), and in many different devices (sensors, automotive

electronic control units, intelligent switches, home appliances such as washing machine drum control, and meters).

- Computing resources such as memory, tasks, and buffers are statically determined. For instance, the entities managed by the underlying operating systems are typically predetermined. This involves complex development environments dealing with many software components (e.g. the Autosar standard [4]).
- Most RCES are high integrity systems, or systems which must meet assurance requirements. Depending on application requirements, different levels of assurance can be involved from the most stringent involving certification (e.g. DO178 [5], IEC-61508 [6] for safety-relevant embedded systems development), to lighter levels of assurance (e.g. industry practices). In fact, many RCES involve very significant software development cost and therefore use advanced engineering disciplines (automatic code generation, model-driven developments).

The TERESA target market is the following:

- Expertise and engineering activities for RCES systems
  - RCES core software engineering activities: TERESA will offer a process allowing reuse of S&D expertise using patterns and models.
  - S&D pattern engineering: S&D experts can use the TERESA approach to provide patterns for multiple sectors.
  - MDE engineering: MDE experts can use the TERESA approach to store models and patterns in the TERESA repository.
  - Security formal validation: Security properties of a given S&D pattern can be formally defined and verified.
- S&D components for RCES components.
- MDE based tools for the engineering of RCES applications.

TERESA market potential is viewed as follows:

- All of the four addressed application domains are high-volume markets. The metering, home control, and industry control sectors are fragmented and very little has been achieved in terms of S&D. The automotive sector is more mature with strong standardization initiatives (e.g. Autosar) but it has not yet taken full advantage of MDE and pattern approaches. We believe that the availability of TERESA proof of concepts in the 4 addressed domains could trigger significant market opportunities for expertise and tools.
- TERESA results could also be exploited in other application areas.

8 Glossary

Term	Definition
EVITA	E-safety Vehicle Intrusion proTected Applications
ICT	Information and Communication Technology
MDE	Model-Driven Engineering
RCES	Resource Constrained Embedded Systems
S&D	Security and Dependability
SysML	Systems Modeling Language
TECOM	Trusted Embedded Computing
UML	Unified Modeling Language

9 References

[1] Project TERESA: http://www.teresa-project.org

[2] Project ITEA TECOM: http://www.tecom-itea.org

[3] Project EVITA: http://www.evita-project.org

[4] Autosar standard: http://www.autosar.org

[5] DO-178, Software Considerations in Airborne Systems and Equipment Certification: http://www.rtca.org/downloads/ListofAvailable%20Docs-March2010.htm

[6] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems: http://www.iec.ch/zone/fsafety/

[7] D. Bell and L. LaPadula, “Secure computer system unified exposition and multics interpretation,” MITRE Corp., Bedford, MA, Tech. Rep. MTR-2997, July 1975.