PRESENTATIONS ABSTRACTS

DESEREC

Dependability and Security by Enhanced Reconfigurability

DESEREC 3rd Training Workshop

Murcia, Spain
16-17 October, 2008

on

The Results and Applications of DESEREC

organized by

University of Murcia

DESEREC Project

Objective

The results of research will be presented by the authors in a form suitable for potential users from outside the consortium. This training material will be enhanced by results of demonstration implementations.

Venue

Faculty of Informatics
Campus of Espinardo
30100 Murcia, Spain

Registration and Participation

The training as well as lunch and dinner are **free of charge** for all participants, but registration is mandatory since the number of participants is limited. Participants will only have to face their own travel and accommodation expenses.

The registration form, as well as additional information about how to reach the meeting place, is available at http://deserec.inf.um.es/training

Thursday, 16th October

[09:00-09:30] **Registration**

Session 1: DESEREC objectives and requirements

Chair: **Maurice Israel (Thales Communications)**

[09:30-10:00]

Overview and objectives of DESEREC

Speaker: **Maurice Israel**

Company: **Thales Communications** (France)

DESEREC aims at providing a management architecture to enhance the dependability and reliability of large mission Critical Information Systems. Such systems are supporting critical business services that require performance, security, availability and sustainability. As a result any failure, evolution or policy change may impact those non-functional properties and finally the IS capacity experimented by end-users.

The DESEREC consortium addresses those problems by means of an innovative but pragmatic approach, that aims at simplifying the IS monitoring and configuration. This paradigm called the *molecular decomposition* allow to describe large IS in a manageable way. This level of abstraction bring to each person running a Business Service the capability to optimize the cost of the level of dependability committed while supporting the Security and Infrastructure administrators duties. The coordination of those management roles under the priority given to the Business-level agreements achieves a maximum of resilience for a minimum of redundant resources.

A detailed presentation of the implemented concepts will be exposed during this workshop using concrete and real end-users example as a main thread. Starting from this example, all the successive stages of the DESEREC workflow will be detailed, from the modelling and simulation tasks to the run-time environment. To conclude end-users will give us their feedback and some tracks to improve the framework.

[10:00-10:30]

User requirements and example scenario

Speaker: **Peggy Stergiou**

Company: **OTE** (Greece)

OTE (Hellenic Telecom Organization S.A.) role is to provide a wide range of telecom services in Greece and in the Balkan area. Since OTE is a full service telecom operator and the former incumbent operator of Greece, it operates a variety of telecom networks, which are also offered on a wholesale basis to alternative operators.

Since 2006 many available IPTV solutions have been evaluated and tested, and a Pilot Field Trial of the IPTV Service has been launched. The Pilot Field Trial uses open-source solutions, in order to test the network infrastructure under real content distribution conditions and to obtain useful knowledge prior to the full deployment.

Since IPTV is a very critical service with stringent requirements (in terms of security, dependability and resilience) OTE is using the pilot IPTV network within DESEREC's framework in order to investigate and minimize the risks that will face during the national deployment.

More specifically the IPTV service should be able to provide very high (99.99%) availability (therefore network and service resources should under all possible circumstances be available – see scenario 3 below) and also be able to protect itself from both external and internal threats (pls. refer to scenarios 1 & 2 below).

OTE expectations are that the DESEREC project results will provide a valuable insight of the complexities and vulnerability risks that OTE might face during the next phase of its IPTV project. Due to the above the selected testcase scenarios that have been proposed for the final demo, which involve three different aspects of the service namely 1) vulnerabilities from a public network (Internet) 2) vulnerabilities on the trusted network (IPTV intranet) and 3) network element failures. More specifically the three scenarios under investigation are:

- Attack to a public WEB server
- Attack to the IPTV WEB/EPG server
- VoD server failure

[10:30-11:00]

DESEREC architecture for the dependability and security management

Speaker: **Maximilian List**

Company: **IABG mbH** (Germany)

This presentation gives an overview of the defined and implemented DESEREC system architecture which aims for increasing the dependability of large CIS from a business point of view. It explains how the three-tiered approach has been realized. This approach allows for an easy distribution of management functions which perform an automated and/or semi-automated reconfiguration.

The three conceptual levels of DESEREC are explained as well as the realization of the concept through distributed global and local agents. These agents are responsible for monitoring of the critical infrastructure, detection of relevant incidents, decision/reaction processing and the deployment of new configurations. Even though the principal architecture of local and global agents is based on the same base structure this separation allows DESEREC to react on a large amount of different incidents. Hence the response time can reach from seconds/minutes (local) to hours (global). In order to guarantee such time constraints and to support the decision process at global level the concept of "molecules" has been introduced. Molecules are clusters of technical services which create "virtual" entities that can easily be handled. This concept also supports the reallocation process of business services because services can now be transferred between molecules instead of dedicated server machines. Hence, it also reduces the number of required physical redundancies in the CIS.

The whole system can be adjusted to the current needs (policy dependant) which allows for an optimal use of resources. Finally, an example gives an explanative summary of how the DESEREC approach will be used in a real scenario and explains the workflow of the above mentioned concepts.

Coffee break

Session 2: Modelling and simulation of complex information systems

Chair: **Antonio Lioy (Politecnico di Torino)**

[11:30-12:00]

Introduction to modelling and operational planning in complex information systems

Speakers: **Marco Aime** / **Antonio F. Gómez Skarmeta**
Companies: **Politecnico di Torino** (Italy) / **University of Murcia** (Spain)

This presentation introduces the models selected by DESEREC to describe heterogeneous ICT systems for security and dependability analysis and management. These models describe provisioned services and their dependability requirements, available system resources and their security capabilities, the incidents that may affect the system.

These models are used to semi-automatically configure the system and to evaluate the resulting security and dependability level.

The concept of *operational plan* will be also introduced in this presentation as the needed information by the system to allocate the technical services into servers and configure them to run properly. Several configurations are generated to set up each technical service in different servers in order to increase the dependability of existing and new Information and Communications Technology (ICT) systems.

An operation plan also defines how to react when incidents appear, so that the impact of such incidents on the provided services is as small as possible, by switching from current configuration to a different one that fixes the incident detected.

[12:00-12:30]

Analysis of wide information systems

Speaker: **Dariusz Caban**
Company: **Wroclaw University of Technology** (Poland)

Sophisticated and business critical services are provided by heterogeneous wide computer networks. The pervasive use and diffusion of these networks and services provided by them, ranging from on-line ticketing to traffic control, makes it crucial to analyze the potential consequences of accidental faults, user misbehavior and even deliberate, orchestrated cyber attacks. The aim is to design and manage these networks to be immune to all predictable inauspicious events and to be as resilient and self-healing as possible when unexpected negative situations occur.

The solution proposed by the DESEREC Project relies on two complementary techniques of system analysis: formal verification and service/network simulation. The presentation will discuss the theoretical choices made in developing these techniques, particularly on the values added by combining these approaches.

The formal analyzer and the simulator share the same description of the network ranging from the low-level network and computing resources, up to the highest level business services, relying on properly configured software servers. Users, permissions, access control lists and software modules and their versions are considered. Finally, models of security and dependability policies, threats, vulnerabilities, faults and resource consumption are needed in order to provide the "realistic context" to the analysis.

Starting from such a complex description, the system is analyzed at two different levels, which are complementary to some extent. The formal analyzer carries out an exhaustive analysis to produce an attack model (potential orchestrated malicious attacks based on exploiting vulnerabilities, affecting the high level business services) and a fault propagation model (describing how faults occurring in physical system components can affect the high level business services). The simulator analyzes specific behaviors of the system, in order to provide performance measures, both in standard operational conditions and when a fault occurs, acting as a magnifying glass to the weaknesses identified by formal analysis.

The presentation will give a formal background to the practical demonstrations of the DESEREC analysis tools, presented later at the end of this same session.

[12:30-11:00]

Panel discussion (moderated)

Lunch

Modelling and operational planning

[14:30-15:00]

Business services modelling

Speaker: **Marco Aime**

Company: **Politecnico di Torino** (Italy)

This presentation introduces the models selected by DESEREC for describing the business services to be provisioned in a target ICT system and the ICT system itself. This presentation also shows how these models can be used to automatically generate alternative system configurations with different dependability characteristics.

System modelling and the automatic generation (and evaluation) of system configurations are core problems in policy-based management of large distributed systems whose complexity overcome traditional ICT control infrastructure.

[15:00-15:30]

Services configurations generation

Speaker: **Daniel Martínez**

Company: **University of Murcia** (Spain)

Administrators of dependable systems are expected to define operational plans as a set of high-level objectives that later need to be translated to formal representations, and finally to configurations that can be enforced in final devices. However, this is usually a manual process that would benefit from any kind of automation. Following this idea, this presentation provides a set of guidelines and requirements to help automating the translation process. The use of CIM (Common Information Model) is also presented and justified, as a target standard model allowing to specify system-level rules which can then be enforced to the specific devices being managed.

The concepts introduced are have been implemented for the DESEREC framework as the Service Configurations Generator, which is a submodule of the Configuration Generator (COG).

Coffee break

Dependability and security analysis of complex information systems

[16:00-16:30]

Formal verification and vulnerability modelling

Speaker: **Luca Durante**

Company: **IEIIT/CNR** (Italy)

Dealing with hardware and software faults, as well as vulnerabilities, is a difficult task especially on large networks, in which many hardware and software components are interconnected and exhibit significant dependencies and interrelationships.

In particular, given the ever increasing number of software vulnerabilities being discovered, it is practically impossible for administrators to keep the software running on their systems completely free of vulnerabilities. Hence, being able to assess the actual impact which a set of vulnerabilities could have in the context of their own system is especially important.

As the complexity of the network grows, the problem rapidly becomes hard to tackle by hand, due to the subtle and unforeseen interactions that may occur among apparently unrelated vulnerabilities, thus bearing the focus on the full automation of the analysis. Going into this direction, a software tool is presented that, given an accurate and machine-readable description of vulnerabilities, detects whether they are of concern or not, and evaluates their consequences in the context of large networks providing business services.

[16:30-17:00]

Simulation

Speaker: **Tomasz Walkowiak**

Company: **Wroclaw University of Technology** (Poland)

The presentation will give the practical demonstration of one of the DESEREC analysis tools - the simulator. The demo mainly deals with a tool able to check the dependability requirements of a network starting from a conceptual model. It can be used both during the very early stages of the design and during the network operation, provided that a model of the network is available.

The system analysis is based on integrating different information models from the DESEREC modeling tools into one coherent model suitable for simulation: the networked systems and applications model (System Description Language, SDL), communication between services in the analyzed system (Web Services Choreography Description Language, WS-CDL), services allocation. The integration of system and services models is done in an automatic way and additional information not present in the mentioned models (i.e. consumption model) are incorporated. The integrated model is transformed into an input file for the modified SSFNet simulator. The system is simulated - additional information on the input models is read from fault and input models or the user can play with all the parameters. Based on the

simulation results dependability metrics are calculated: availability, response time and service performance. The output produced helps the system designer and/or manager to modify the system in order to make it more resilient with respect to critical situations highlighted by the analysis tools.

The same tool can be run again on the updated system (description), in order to check the effectiveness of introduced modifications.

[17:00-17:30]

SIMICS - Information systems simulation

Speaker: **Philipp Hofmann**

Company: **IABG mbH** (Germany)

The development of tools for the planning and analysis of communication and information systems (CIS) including their optimal configuration is one of the DESEREC goals. The planning tools allow the description of a CIS comprising the network topology with single entities, provided business services, their configuration and policies as well as possible faults and vulnerabilities. The analysis tools are then used to assess the planned CIS and different alternative configurations with respect to performance, security and dependability – enabling the identification of optimal configuration(s).

One of the employed analysis tools is the full system simulator SIMICS. Full system simulator means that SIMICS allows modelling and simulating the entities of a CIS down to the processor type and its registers, I/O chips, bus system and so on. This low level of simulation even allows using real software (operating systems, drivers, applications, DESEREC agents and so on) in SIMICS like on real hardware.

Hence, SIMICS is used in DESEREC to perform low-level system performance analyses of the different alternative configurations generated by the planning tools. We describe the functionality of SIMICS and how it is integrated in the DESEREC planning and analysis framework. We furthermore show how the low-level simulator SIMICS can be used to complement and verify the results obtained by high-level simulations.

Finally, we present example-based results of a CIS configuration analysis through SIMICS.

[17:30-18:00]

Panel discussion (moderated)

[20:30]

Gala dinner

Friday, 17th October

Session 3: Incident detection and system reconfiguration

Chair: **Patrick Radja (EADS Defence and Security Systems)**

[09:00-09:30]

Dependability and security metrics

Speaker: **Imre Kocsis**

Company: **Budapest University of Technology and Economics** (Hungary)

In our presentation, we treat system and service resilience as a control problem and briefly describe how classes of the widely used, but vague notion of 'IT metrics' map to the concepts of generic control with a special emphasis on the control aspects of structural reconfiguration as a generic resilience mechanism.

Large, distributed IT infrastructures providing business-critical services have to protect themselves against internal and external threats and adapt to changing environmental parameters, as workload. Most widely applied, structural resilience mechanisms use some form of local static redundancy deployed to each critical resource for failover. However, recently both large-scale interconnected distributed systems and virtualization enable on-line structural reconfiguration exploiting a globally managed spare capacity as on-demand failover resource.

The core step in control is impact analysis estimating the influence of low level candidate repair actions onto the overall user observable service quality. Impact analysis is used in the practice both explicitly and implicitly (implemented as a control heuristics) for the dependability/security assessment of the compliance of the current system state (or the predicted future one) with the extra-functional objectives and assessment of the severity of the deviation from the goals. Subsequently the selection of an action (or action series) is performed according to a (sub)optimal state change.

We briefly review the common high-level, phenomenological metrics that remain valid choices as control objective variables with the transition to structural reconfiguration based resilience. However, the typical aggregation logic patterns as well as the generic set of monitored and influenced variables have to be adapted.

Most importantly, metrics are needed to be able to quantify the ability of the system to deal with faults and attacks with the given constrained set of resources using the predefined reconfiguration logic. Hence, we introduce a family of Quality of Management metrics. On the one hand, we define process oriented metrics that measure the quality of the reconfiguration processes. On the other hand, we introduce reconfigurability metrics that are defined on the configuration state space of the system and quantify the self-management capability in design time as well as runtime (remaining reconfigurability).

Lastly, we present analysis methods of uninterpreted models of reconfiguration.

[09:30-10:00]

Global decision and system views for decision support

Speaker: **Vincent Loriot**

Company: **EADS Defence and Security Systems** (France)

DESEREC reconfiguration framework aims to increase information system dependability by maintaining critical services, even by bringing the system to a degraded performance state to ensure operation of the most critical system functionalities.

Reconfiguration decision relies on proactive detection of incidents and potential faults on the system. For that, the DESEREC framework aims to provide to the system operator a computer aided reconfiguration process which relies on:

- Providing a consolidated high level view of the system health status computed from detected incidents and dependability metrics.
- Reconfiguration proposals based on operational plans previously validated with modelling and simulation tools.

Based on this information, the DESEREC system operator will be able to easily make the appropriate choice regarding the configuration to enforce.

[10:00-10:30]

Deployment and reconfiguration framework to enhance dependability and security

Speaker: **Manuel Gil**

Company: **University of Murcia** (Spain)

The main goal of a deployment and reconfiguration framework is to decrease the management cost of the Communication and Information Systems (CIS) whilst increasing its resilience and dependability. For this, and after detecting abnormal events on a system, mechanisms to ensure the deployment of an operational plan come into play to fix the problems caused by those abnormal events.

This framework allows translating an operational plan into device specific configuration rules and its deployment to the target system as a result of a decision. This deployment is an automatic process which is carried out according to the output of the translation module and/or the decision one. This will reconfigure all or part of the system in order to continue providing the same services that were provided before detecting the abnormal events.

Several approaches have been studied and developed such as the use of a policy-based management paradigm.

Coffee break

[10:45-11:15]

Data mining with RARES tool

Speaker: **Simon Caban**

Company: **Thales Communications** (France)

RaresData is a data mining software tool made up of 2 sub-modules: a Clustering module (used during the Design Phase) and a Categorisation module (used during the Runtime Phase). The Clustering module detects clusters of similar data (events collected on the network and IS) in unsupervised way (Knowledge Discovery). Relational metrics are used to evaluate the quality of the obtained results, like the clusters homogeneity, their quality, and other quality indexes. Once the clustering has been performed at least once (i.e. if clusters already exist), the Categorisation module affects each new event (retrieved at runtime from the network and IS) to existing clusters.

The aim is to identify the following kinds of behaviour (Clusters): known normal behaviour, known abnormal behaviour, unknown behaviour. Thus, as reactions are associated to these Clusters, the Categorisation module enables to take the appropriate (reconfiguration) actions.

[11:15-11:45]

Integration of ExaProtect SMS and SPS in the whole DESEREC loop

Speaker: **Luc Paffumi**

Company: **EPT** (France)

DESEREC aims at providing a complete framework to increase the overall dependability of large scale Communication and Information Systems (CIS). DESEREC should deal with the entire loop from the detection of failures and attacks to the reconfiguration of any kind of device spread out over the IS.

On the one hand, thanks to its aggregation and correlation capabilities and its ability to handle heterogeneous components, Exaprotect SMS can easily detect attacks and failures occurring on the IS - based on the Detection Scenarios produced by the modelling part of the DESEREC model – and generate incidents that will be handled by the DESEREC decision engine and the DESEREC administrator to select the most suitable reaction.

On the other hand, due to the variety of network components and technologies, administrators need tools to design and deploy easily security configurations and policies in the IS. Exaprotect SPS provides an easy-to-use graphical user interface to define high-level security policies that are then converted into device specific rules. Thanks to the generated Operational configuration designed in the modelling part of the DESEREC framework, SPS generates device specific configurations and deploys them throughout the IS.

The presentation will present the overall integration of the Exaprotect SMS detection and SPS reconfiguration in the DESEREC framework through a demonstration of a DESEREC use case.

Panel Session: User experiments

[11:45-12:05]

OTE services

Speaker: **Peggy Stergiou**

Company: **OTE** (Greece)

OTE provides a wide range of telecom services in Greece in which currently is the major telecom operator. OTE is also practically the dominating player in the Broadband Access (ADSL, ADSL2+, WIMAX, etc) in Greece since LLU is currently bellow European average. In this scope, OTE plans to offer Value Added Services over its broadband networks, specifically Triple Play services. IPTV being is the most demanding of them in terms of security, dependability and resilience. The services offered by OTE pilot IPTV testbed are the following:

- Fast Internet
- IPTV
- VoD

At a later stage time-shifted TV and PVR services will be added.

The end-user access to these services is encompassed via a network infrastructure that is composed of access and metro network elements. This equipment provides the required connectivity between the CPE (user terminal devices) and the set of devices that implement the services offered to the subscribers. The IPTV servers should be secured against unauthorized access both for the services they provide as well as for the content (the most valuable asset) they store and process.

OTE is interested in the exploitation of DESEREC results to simplify, improve security in our the network infrastructure while at the same time reducing security costs and minimize the risks before the deployment of Triple-Play services in the commercial network.

[12:05-12:25]

eGov service

Speaker: **Julien Borgel**

Company: **Thales Services SAS** (France)

Thales Services / D3S is a division of Thales which delivers advanced security solutions for mission critical information systems, infrastructure and applications.

The offer is focused on market with strong requirement of security and criticality in the domain of Defense/Aerospace, Civil Administration, Industry and Finance (transport, energy, high tech, Consulting and System Integration).

The development strategy relies on four major markets which are:

- Ground transportation,
- Critical infrastructures,
- Government,
- Industry & Finance.

In that context, Thales Services contributes to a global trend which aims to enhance the public services provided by administrations. The so called e-government projects refer to the use of internet technology for providing services and transactions with users. These users or clients could be citizens or government officers. The final goal is to improve the service delivered to the users, and to increase the administration efficiency.

This kind of project has stringent requirements for availability, security, scalability, reliability and performance, with different service levels to manage. So the management of such Information System, especially regarding faults, hardware failures, response time, and attacks is a complex challenge in such environment.

The overall interest of Thales Services in DESEREC is mainly to improve the management of this kind of complex and large systems, while decreasing exploitation costs. In that context, Thales Services intends to expose their feedback and experiments of DESEREC technologies.

[12:25-12:45]

Land border control

Speaker: **Bernard de Francqueville**

Company: **EADS Defence and Security Systems** (France)

EADS' Global Security provides fully-integrated modular solutions and services in order to minimise risk exposure through protecting people and territories.

Solutions for the protection of population, critical infrastructure and border control typically require a System of Systems approach entailing a variety of mission critical subsystems. Each of these subsystems is specialised in a particular domain but must interact with other subsystems. This is so as to ensure that all security stakeholders possess up to date and relevant information in order to respond in the most effective and coordinated manner. Some examples of these Subsystems are:

- Command & Control (C2)
- Portal with collaboration tools (mail, chat, video conferencing, etc.)
- Identity and access control including use of biometrics
- Computer aided Dispatch (CAD)
- Common Operating Picture (COP)
- Automatic Vehicle and Person Location (AVL)
- Sensor Management subsystems (for video, radar, sonar, intrusion detectors)
- Data mining
- Mobile Data terminals

The proposed platform shows the integration of two systems: a web portal application and a Command & Control application (C2) in the context of land border control.

Goal of the EADS GLS Testbed is to prove DESEREC capabilities on a "real" platform which requires, by its nature, to be extremely robust and secured. This will be demonstrated through presentation of a scenario showing detection and reaction to an incident caused by an insider.

[12:45-13:00]

Conclusions