



# Computer Science and Communications Research Unit

**CSC Projects List, 2010**



# CSC Projects and Grants Overview

---

The CSC research unit is part of the UL with the primary mission to conduct fundamental and applied research in the area of computer, communication and information sciences.

CSC focus on different research priorities (Advanced Software Systems, Communicative Systems, Intelligent and Adaptive Systems, Information Security) and is in charge of developing P1 - the strategic priority on security and reliability of the University of Luxembourg. Currently, the CSC research unit includes 24 professors, 7 research assistants, 46 junior researchers, 18 collaborators on projects, 8 scientific support staff members, 4 technical support staff members and 7 technical aid staff members. Their research fields range from the investigation of the theoretical foundations to the development of interdisciplinary applications.

This chapter proposes a brief overview of the projects conducted in the Computer Science and Communications Research Unit in 2009 and 2010.

Projects are listed in the following order:

1. European project (FP7, ERCIM etc.)
2. FNR CORE projects
3. UL projects
4. AFR projects
5. University of Luxembourg projects

6. Other projects (Partnerships, FNR AM2a, FNR Accompanying Measures)

In each section projects are listed by CSC research laboratories:

- ComSys
- ILIAS
- LACS
- LASSY

Details of each projects are provided in chapter [2](#).

## European projects

Lab	Acronym	Title	PI	Funding	Duration
COMSYS	EFIPSANS Ref: p.14	Exposing the Features in IP version Six protocols that can be exploited/extended for the purposes of designing/building Autonomous Networks and Services	Prof. Dr. Thomas Engel	FP7 European Commission (565 K€). UL budget: 917.600 €.	01/01/2008 – 31/05/2010
	IRMA Ref: p.15	IRMA	Prof. Dr. Thomas Engel	Total EU funding 2.481.395€. UL budget: 523.651€.	01/06/2008 – 31/05/2011 (official dates)
	NARTUS Ref: p.16	European Platform Roadmap for Future Public Safety Communication	Prof. Dr. Thomas Engel	FP6 European Commission (760.000€). UL budget: 156.934€	01/06/2006 – 31/05/2009
	SECRICOM Ref: p.17	Seamless Communication for Crisis Management	Prof. Dr. Thomas Engel	FP7 European Commission (300 K€). UL budget: 304.625€.	01/09/2008 – 31/05/2012
	U2010 Ref: p.18	Ubiquitous IP-centric Government and enterprise next Generation Networks Vision 2010	Prof. Dr. Thomas Engel	FP6 European Commission (800 K€). UL budget: 821.000€.	01/05/2006 – 30/04/2009
LASSY	DIAMONDS Ref: p.20	Development and Industrial Application of Multi-Domain Security Testing Technologies	Prof. Dr. Nicolas Guelfi	ITEA2 European Project (not funded)	01/07/2010 – 31/12/2012
ILIAS	WiSafeCar Ref: p.19	Wireless traffic Safety network between Cars	Pekka Eloranta (MobiSoft, Finland)	EUREKA-CELTIC, 300000€	01/07/2009 – 31/12/2011

## FNR projects

Lab	Acronym	Title	PI	Funding	Duration
LACS	ATREES Ref: p.21	Attack Trees	Prof. Dr. Sjouke Mauw	FNR-CORE, 299000€	01/04/2009 – 31/03/2012
	CRYPTO-SEC Ref: p.22	Cryptography and Information Security in the Real World	Dr. Jean-Sébastien Coron	FNR-CORE, 272000€	01/03/2010 – 28/02/2013
	SeRTVS Ref: p.23	Secure, Reliable and Trustworthy Voting Systems	Prof. Dr. Peter Ryan	FNR-Core, 333000€ FNR-AFR, 216216€ IMT Luca, 130000€ University of Melbourne, 60000€ UL, 268596€	01/02/2010 – 01/02/2013
	CRKI Ref: p.70	Science Festival 2009 - "Cryptography for Kids"	Prof. Dr. Alex Biryukov	FNR-Science Festival, 1800€	12/11/2009 – 15/11/2009
LASSY	COMPLEX Ref: p.30	Model Composition for Executable Modeling	Prof. Dr. Pierre Kelsen	UL: 171K€	01/08/2010 – 31/07/2010
	SETER Ref: p.24	Security Testing of Resilient Systems	Prof. Dr. Nicolas Guelfi	FNR-CORE, 268000€	01/05/2009 – 30/04/2012
	MOVERE Ref: p.29	Model-Driven Validation and Verification of Resilient Software Systems	Prof. Dr. Nicolas Guelfi	FNR-CORE, 265K€	01/05/2010 – 31/04/2013
ILIAS	DYNARG Ref: p.24	The Dynamics of Argumentation	Prof. Dr. Leon van der Torre	FNR	01/10/2009 – 31/09/2012
	S-GAMES Ref: p.25	Security Games	Prof. Dr. Leon van der Torre	FNR-CORE, 314000€	01/04/2009 – 31/03/2012
	GreenIT Ref: p.27	EnerGy-efficient REsourcE Allocation in AutonomIc Cloud ComputIng	Prof. Dr. Pascal Bouvry	FNR-CORE, 450K€	1/01/2010 – 31/12/2012
	TITAN Ref: p.27	Trust-assurance for critical infrastructures in multi-agents environments	Dr. Benjamin Gateau	FNR-CORE, 108000€	1/01/2009 – 31/12/2010

## AFR projects

Lab	Acronym	Title	PI	Funding	Duration
COMSYS	MSN Ref: p.68	Multimedia Sensor Networks (PhD thesis)	Prof. Dr. Thomas Engel	FNR and EPT (108K€)	2010 – 2013
	WinSEOM Ref: p.69	Energy Optimization and Monitoring in Wireless Mesh Sensor Networks(PhD thesis)	Prof. Dr. Thomas Engel	FNR and Ville de Luxembourg (108K€)	2010 – 2013
	WOA Ref: p.69	Wireless outdoor access. Managed and Community Networks (PhD thesis)	Prof. Dr. Thomas Engel	FNR and Telindus (116K€)	2010 – 2013
LACS	EPRIV-MAA Ref: p.51	A Formal Approach to Enforced Privacy: Modelling, Analysis and Applications	Prof. Dr. Sjouke Mauw	FNR–AFR, 105222€	01/12/2009 – 30/11/2012
	GMASec Ref: p.52	Games for Modelling and Analysis of Security	Prof. Dr. Sjouke Mauw	FNR–AFR, 105223.44€	01/11/2009– 31/10/2012
	CRHF Ref: p.56	Cryptanalysis of Hash Functions	Prof. Dr. Alex Biryukov	FNR-AFR, 36,379€ per year	01/05/2007 – 28/02/2011
	PRIV-VOTE Ref: p.53	A Formal Approach to Privacy in Voting	Prof. Dr. Sjouke Mauw	BFR, FNR-AFR, 16098.30€	01/05/2007 – 31/05/2009
	SADT Ref: p.54	Security Analysis Through Attack-Defense Trees	Prof. Dr. Sjouke Mauw	FNR-AFR, 106476€	01/01/2010 – 31/12/2012
	SPIM Ref: p.55	Security Protocols in Identity Management	Prof. Dr. Sjouke Mauw	BFR, FNR-AFR, 88984€	01/10/2007- 30/11/2010
LASSY	SPEM Ref: p.56	Selected Problems in Executable Modeling	Prof. Dr. Pierre KELSEN	AFR PHD-09-084	15/11/2009 – 15/11/2012
	ENFRDEM Ref: p.57	Expressing Non-Functional Requirements in Declarative Executable Models	Prof. Dr. Pierre Kelsen	FNR - AFR PostDoc	01/01/2008 – 31/05/2010

## AFR projects (cont.)

Lab	Acronym	Title	PI	Funding	Duration
ILIAS	CUBA Ref: p.62	Conviviality and User Behavior Analysis: Inventing profile discovery for e-conviviality	Prof. Dr. Christoph SCHOMMER	FNR - AFR PhD (30K€)	01/07/2007 – 30/06/2010
	ULFAUC Ref: p.59	Towards a unified logical framework for action, uncertainty and causality	Prof. Dr. Leon van der Torre	FNR-AFR-Postdoc	01/09/2008 – 31/08/2010
	FSL Ref: p.60	Modeling and Developing a Novel Distributed Authorization Logic	Prof. Leon van der Torre	FNR-AFR	01/09/2009 – 31/08/2012
	GMASec Ref: p.61	Games for Modelling and Analysis of Security	Prof. Dr. Sjouke Mauw	FNR-AFR	01/11/2009 – 31/10/2012
	LCNMAS Ref: p.62	Logic and Communication in Normative Multi-Agent Systems	Prof. Dr. Leon van der Torre	FNR-AFR-Postdoc	01/03/2009 – 28/02/2011
	UNISON Ref: p.58	Universality and Self-Organization in Next-Generation Distributed Environments	Prof. Dr. Stefan Rothkugel	AFR, 106476€	01/01/2009 – 31/12/2011
	RRMTNOT Ref: p.63	Reliable and robust management for telecommunication network with optimization techniques	Prof. Dr. Pascal Bouvry	FNR - AFR Ph.D.	01/12/2008 – 30/11/2010
	TMAHN Ref: p.63	Trust Management for Ad-Hoc Networks	Prof. Dr. Pascal Bouvry	FNR - AFR PhD	01/02/2007 – 31/01/2011
	GPSTCFPM Ref: p.64	Grid-based Parallel Software(GPS) for predicting thermal conversion and fuel particles motion in combustion chamber	Prof. Dr. Pascal Bouvry	FNR - AFR PostDoc	01/03/2009 – 28/02/2010
	COPSCG Ref: p.65	Combinatorial optimization on P2P systems and computational grids	Prof. Dr. Pascal Bouvry	FNR - AFR PhD	01/09/2007 – 31/10/2010
	RSDG Ref: p.66	Robust Scheduling on Desktop Grids	Prof. Dr. Pascal Bouvry	FNR - AFR PostDoc	01/09/2009 – 31/08/2011
	WiCaN Ref: p.67	Efficient data transfer in vehicle2vehicle wireless communication networks, using distributed algorithms based on collective intelligence such as ant colonies.	Prof. Dr. Pascal Bouvry	FNR - AFR PostDoc	15/10/2009 – 14/10/2011
TIGRIS Ref: p.67	Risk Prediction Framework for Interdependent Systems using Graph Theory	Prof. Dr. Pascal Bouvry	FNR - AFR PhD	15/10/2009 – 15/10/2012	

## University of Luxembourg Internal project

Lab	Acronym	Title	PI	Funding	Duration
LACS	RKCTM Ref: p.31	Refining Key Components in Trust Models	Prof. Dr. Sjouke Mauw	FNR-AFR, 50,360€ per year	01/01/2009–31/07/2010
	EPRIV Ref: p.32	A Formal Approach to Enforced Privacy in e-Services	Prof. dr. Sjouke Mauw	UL, 254955€	01/05/2009–30/04/2012
	ESS Ref: p.33	Embedded Systems Security	Prof. Dr. Alex Biryukov, Prof. Dr. Jean-Sebastien Coron, Prof. Dr. Sjouke Mauw	UL, 331106.73€	01/10/2008 - 31/01/2012
	SECRYPT Ref: p.34	Security and Cryptography in the Real World	Prof. Dr. Jean-Sébastien Coron	UL, 950000 €	01/01/2007 - 31/08/2010
LASSY	DT4BP Ref: p.35	Modelling Dependable Collaborative Time-Constrained Business Processes	Prof. Dr. Nicolas Guelfi	UL (Assistant contract)	01/01/2007 – 15/12/2010
	PRISMA Ref: p.35	PRISMA : a Process for Requirements Identification, Specification and Machine-supported Analysis, targeting Transactional Models seen under a Product Line perspective	Prof. Dr. Nicolas Guelfi	UL (Assistant contract)	16/03/2006 – 15/03/2010
	RADTN Ref: p.36	Resource Allocation in Delay and Disruption Tolerant Networks	Prof. Dr. Simin Nadjm-Tehrani	UL (part time Assistant contract)	01/09/2007 – 01/09/2011
	AEKF Ref: p.37	Adaptive High-gain Extended Kalman Filter and Applications	Prof. Dr. Juergen Sachau	UL (Project RAIP) - Junior Researcher contract	2006 – 2010
	VERITY Ref: p.38	VERification of fault-tolerant advanced Transactional distributed sYstems	Prof. Dr. Nicolas Guelfi	University of Luxembourg, 364257€	01/01/2008 – 31/12/2010
	MaRCo Ref: p.39	Managing Regulatory Compliance: a Business-Centred Approach	Prof. Dr. Pierre Kelsen	FNR: 749K €	01/05/2010 – 30/04/2013
	Medal Ref: p.39	Model-Driven Engineering using a Declarative Behavioural Description Language	Prof. Pierre Kelsen	University of Luxembourg	01/10/2008 – 30/09/2011

## University of Luxembourg Internal project (cont.)

Lab	Acronym	Title	PI	Funding	Duration
ILIAS	D2 Ref: p.40	DECISION DECK – University of Luxembourg	Prof. Dr. Raymond Bisdorff	UL, 140000€	01/04/2007 – 31/12/2009
	RMSD Ref: p.41	Recherches Mathématiques en Sciences de Décision	Prof. Dr. Raymond Bisdorff	UL, 93300€	01/01/2008 – 31/12/2010
	AASTM Ref: p.42	Advanced Argumentation Techniques for Trust Management	Prof. Dr. Leon van der Torre	UL	01/08/2007 – 30/04/2010
	DYTRIL Ref: p.43	Dynamics of trust in logic-based multi-agent systems	Prof. Dr. Leon van der Torre	UL-PHD	01/01/2007 – 31/12/2010
	ICR Ref: p.42	Individual and Collective Reasoning	Prof. Dr. Leon van der Torre	UL, Projet de démarrage	01/10/2006 – 30/09/2011
	EVOSEC Ref: p.43	Evolutionary Computing & Security	Prof. Dr. Pascal Bouvry	UL, 250000€	2008 – 2010

## Other misc projects

Lab	Acronym	Title	PI	Funding	Duration
COMSYS	MBITSRC Ref: p.46	Modelling of Business and IT Landscapes addressing Security, Risk and Compliance in a Real-World banking environment (PhD thesis)	Prof. Dr. Thomas Engel	Funding by Credit Suisse and FNR (128.50K€)	2005-2010
	EWSSAOP Ref: p.46	End-to-end Web Service Security in Aspect Oriented Programming	Prof. Dr. Thomas Engel	Funding by EPT (75K€)	2008 – 2011
	SCS Ref: p.48	Satellite Communication Security (PhD thesis)	Prof. Dr. Thomas Engel	Funding by ESA and FNR (90K€)	2005 – 2009
	SUTMDNiBE Ref: p.49	Secure Usage and Trust of Mobile Devices in Networks for international banking environments (PhD thesis)	Prof. Dr. Thomas Engel	Funding by Dresdner Bank and FNR (45K€)	2005-2010
	SOSSHIN Ref: p.50	Self Organizing Security Sensors in highly-distributed IP networks (PhD thesis)	Prof. Dr. Thomas Engel	Funding by SES-ASTRA and FNR (45K€)	2007 – 2011
	SESMP Ref: p.45	Study of certain evolution systems in mathematical physics: magnetohydrodynamics of partially ionized plasmas, time irreversibility and decoherence in quantum systems	Prof. Dr. Manuel Nunez Jimenez	University of Valladolid - 9700€	01/01/2008 – 31/12/2010
LACS	LEWIS Ref: p.51	Lux. Early-Warning Analysis and Information Sharing System	Prof. Dr. Peter Ryan	Ministère de l'Economie, 70000€ UL, 29120€	2009 – 2010 (6 months)
LASSY	Business-learning Ref: p.44	Développement d'outils d'apprentissage en ligne pour les techniques de comptabilité, d'analyse financière et de gestion d'entreprise	Prof. Dr. ZAM-PUNIERIS Denis	External funding (IUIL)	01/01/2008 – 31/12/2009

## Accompanying measures (AM)

Lab	Acronym	Title	PI	Funding	Duration
LACS	FATES and FAST Ref: p.71	Formal Methods Week	Baptiste Alcalde	FNR-AM2a, 2000€	02/11/2009–06/11/2009
	CSF and FCC Ref: p.72	Computer Security Foundations Symposium and Workshop on Formal and Computational Cryptography	Sasa Radomirovic	FNR-AM2a, 697,77€	08/07/2009–12/07/2009
	ICFEM Ref: p.72	International Conference on Formal Engineering Methods	Ton van Deursen	FNR-AM2a, 930,72€	08/12/2009–11/12/2009
	FOSAD Ref: p.72	9th International School on Foundations of Security Analysis and Design	Barbara Kordy	FNR-AM2a, 1638,36€	30/08/2009–04/09/2009
	ESC 2010 Ref: p.70	ESC 2010 - Echternach Symmetric Cryptography Workshop	Prof. Dr. Alex Biryukov	FNR-AM, 8000€	11/01/2010 - 15/01/2010
	VOTE-ID 2009 Ref: p.71	Second International Conference on e-Voting and Identity	Prof. Dr. Peter Ryan	FNR-AM, 5240€	07/09/2009 – 08/09/2009
ILIAS	LSACP Ref: p.72	Logical Systems for Access Control Policies	Prof. Leon van der Torre	FNR AM2C	01/01/2009 – 28/02/2010

# CSC Projects and Grants Details

---

This chapter details the projects listed in the previous chapter, structured as follows:

1. European funding project (FP7, ERCIM etc.): see §2.1.1
2. FNR CORE projects: see §2.1.2
3. UL projects: see §2.1.3
4. Other miscellaneous projects (French ANR, Grant agreement for research, development, and innovation etc.): see §2.1.4
5. Grants obtained (AFR, FNR AM3 etc.): see §2.2.

## 2.1 Research projects

### 2.1.1 European funding projects

Exposing the Features in IP version Six protocols that can be exploited/extended for the purposes of designing/building Autonomous Networks and Services	
<b>Acronym</b>	EFIPSANS
<b>Reference</b>	F1R-CSC-PEU-0801EF
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	FP7 European Commission (565 K€). UL budget: 917.600 €.
<b>Running Time</b>	01/01/2008 – 31/05/2010

#### Members:

Thomas Engel, Thorsten Ries, Sheila Becker, Cynthia Wagner

#### Domain(s):

autonomic networks, network security

#### Partner(s):

Ericsson AB, Sweden Fraunhofer Gesellschaft, Germany Telcordia Technologies, Poland The Telecommunications Software & Systems Group, Ireland Institute of Communication and Computer Systems, Greece Telefónica Móviles España, Spain Beijing University of Posts and Telecommunications, China Greek Research & Technology Network S.A., Greece Warsaw University of Technology, Poland Velti S.A., Greece Technical University Berlin, Germany Fujitsu Laboratories Europe, UK

#### Description:

The EFIPSANS project aims at exposing the features in IP version six protocols that can be exploited or extended for the purposes of designing or building autonomic networks and services. What this means is, a study of the emerging research areas that target desirable user behaviours, terminal behaviours, service mobility, e-mobility, context-aware communications, self-aware, autonomic communication/computing/networking will be carried out, and out of these areas desirable autonomic(self-\*) behaviours in diverse environments e.g. end systems, access networks, wireless versus fixed network environments will be captured and specified. Appropriate IPv6 protocol or architectural extensions that enable the implementation of the captured desirable autonomic behaviours will be sought and specified.

A selected set of the specified autonomic behaviours will be implemented and demonstrated. Also, technical reports on the concrete IPv6 feature combination scenarios including any new extensions used to implement the selected set of autonomic behaviours will be presented. The vision is that, the specified autonomic behaviour specifications, the identified exploitable IPv6 features and new protocol and architectural extensions will one day be standardized in the long run (after the first 3 years of EFIPSANS) i.e. maturing from being drafts to standards.

More information: <http://www.efipsans.org>

IRMA	
<b>Acronym</b>	IRMA
<b>Reference</b>	F1R-CSC-PEU-0802IR
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	Total EU funding 2.481.395€. UL budget: 523.651€.
<b>Running Time</b>	01/06/2008 – 31/05/2011 (official dates)

**Domain(s):**

IPv6, networks

**Partner(s):**

Université du Luxembourg, Luxembourg Centre de Communications du Gouvernement, Luxembourg Technologies sans Frontieres, Luxembourg SPA-CEBEL, Belgium Thales-Alenia Space, France SES-ASTRA TECHCOM SA, Luxembourg Cisco, Belgium RENATER, France Universiteit van Tilburg, The Netherlands Council for Scientific and Industrial Research, South Africa Centre de Suivi Ecologique, Senegal Centre Royal de Télédetection Spatiale, Morocco Agence Nationale de Réglementation des Télécommunications, Morocco Ecole Nationale Supérieure Polytechnique de l'Université de Yaoundé, Cameroon Unidade Técnica de Implementação da Política de Informatica (ICT Policy Implementation Technical Unit), Mozambique

**Description:**

Disaster risk reduction policies and institutional mechanism exist at various degrees of completeness in the African countries part of the consortium. Their effectiveness is however limited when having to deal with major disasters and complex emergencies. Risk management is often limited to specific hazard monitoring with limited or no consideration of the vulnerability of the area at risk neither to the systemic nature and possible domino effect between risks of different nature. It is the vulnerability of the population

and of the infrastructure at risk that may transform a hazard into a major disaster. The purpose of the project is to build a reference platform suitable for the management of natural and environmental risks in Africa. The platform must allow the stakeholders in risks management to develop and use tailored risk management models; therefore, the platform will provide similar facilities as WIN, ORCHESTRA, SSE, SANY and u-2010 solutions and should make it easy to build a multi-risks management, i.e. the platform will exploit the commonalities of the information sources and take into account the interdependencies between different hazards. The platform will feature two major technical components: An environment for providing services of all kinds related to the acquisition, processing, dissemination of information and an efficient storage of all relevant information so that the stakeholders can analyse afterwards the sequence of events and adapt operational procedures consequently, and a multi-purpose solution for the communications (sensor networks, remote sensed data transfer, service access, alert, emergency communications) based on IPv6 either to federate legacy communications or to provide native IPv6 solutions. The project intends to deliver a pre-operational open platform, assessed by end-users through operational scenarios serving as reference for future larger scale deployment and providing the facilities for prototyping risk management systems and for supporting a rapid development of applications services. This platform will be populated with specific applications (Bushfire, Flood, Desertification and urban risks).

European Platform Roadmap for Future Public Safety Communication	
<b>Acronym</b>	NARTUS
<b>Reference</b>	F1R-CSC-PEU-07NART
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	FP6 European Commission (760.000€).
<b>Running Time</b>	UL budget: 156.934€ 01/06/2006 – 31/05/2009

**Domain(s):**

Autonomic networks, network security

**Partner(s):**

Teknillinen Korkeakoulu (Helsinki University of Technology), Finland British Association of Public Safety Communication Officers, United Kingdom THALES COMMUNICATIONS SA, France EADS SECURE NETWORKS, France TIEMS, Belgium Squaris Consultants, Belgium National Technical University of Athens, Greece Martel GmbH, Switzerland University of Luxem-

bourg, Luxembourg Centre de Communications du Gouvernement, Luxembourg

### Description:

The SSA NARTUS project has established a European platform and roadmap for future public safety communication, in order to facilitate European integration in the area of Public Safety with particular focus on public safety communications and information systems. Recent events in Europe and other parts of the world have again demonstrated that effective response to emergencies, crises and disasters depends on timely available, reliable and intelligible information. Advanced information and communications technologies (ICT's) offer an increasing number of valuable, however divergent, tools for emergency response, crisis management, and disaster preparedness and response. The speed with which ICT's emerge, leads to different levels of implementation. Successful application of ICT's by the increasing number of national and international stakeholders confronted with cross-border incidents, depends on better integration of frameworks for action. A European Public Safety Communication Forum (PSCE Forum) has been created : the goal is to establish a European platform and roadmap for future public safety communication and to help facilitating European integration in the area of Public Safety with particular focus on public safety communications and information systems. More information: <http://www.nartus.org>

Seamless Communication for Crisis Management	
<b>Acronym</b>	SECRICOM
<b>Reference</b>	F1R-CSC-PEU-08SECR
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	FP7 European Commission (300 K€). UL budget: 304.625€.
<b>Running Time</b>	01/09/2008 – 31/05/2012

### Members:

Thomas Engel, Latif Ladid, Aurel Machalek

### Domain(s):

Emergency services, critical infrastructure

### Partner(s):

QinetiQ Ltd., United Kingdom Ardaco, a.s., Slovakia Bumar Ltd, Poland NEXTEL S.A., Spain Infineon Technologies AG, Germany Université du Luxembourg, Luxembourg Institute of Informatics, Slovak Academy of Sciences, Slovakia Graz University of Technology, Austria Smartrends, s.r.o.,

Slovakia ITTI Sp. z o.o., Poland British Association of Public Safety Communication Officers, United Kingdom CEA LETI, France Hitachi Europe SAS, France

**Description:**

SECRICOM is proposed as a collaborative research project aiming at development of a reference security platform for EU crisis management operations with two essential ambitions: (A) Solve or mitigate problems of contemporary crisis communication infrastructures (Tetra, GSM, Citizen Band, IP) such as poor interoperability of specialized communication means, vulnerability against tapping and misuse, lack of possibilities to recover from failures, inability to use alternative data carrier and high deployment and operational costs. (B) Add new smart functions to existing services which will make the communication more effective and helpful for users. Smart functions will be provided by distributed IT systems based on an agents' infrastructure. Achieving these two project ambitions will allow creating a pervasive and trusted communication infrastructure fulfilling requirements of crisis management users and ready for immediate application.

More information: <http://www.secricom.eu>

Ubiquitous IP-centric Government and enterprise next Generation Networks Vision 2010	
<b>Acronym</b>	U2010
<b>Reference</b>	F1R-CSC-PEU-06UWP1
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	FP6 European Commission (800 K€). UL budget: 821.000€.
<b>Running Time</b>	01/05/2006 – 30/04/2009

**Members:**

Thomas Engel, Thomas Scherer, Aurel Machalek

**Domain(s):**

Emergency services, critical infrastructure

**Partner(s):**

University of Luxembourg, Luxembourg Centre de Communications du Gouvernement, Luxembourg HITEC Luxembourg SA, Luxembourg Telindus SA, Luxembourg University College of London, United Kingdom Cisco Systems International BV France Telecom, France Industrieanlagen-Betriebsgesellschaft mbh, Germany SES-ASTRA TECHCOM SA, Luxembourg M-

Plify SA, Luxembourg Entreprise des Postes et Télécommunications, Luxembourg KORAK SLOVAKIA sro, Slovakia Nokia-Siemens Networks, Luxembourg Lancaster University, United Kingdom Teknillinen Korkeakoulu (Helsinki University of Technology), Finland Ministrstvo za obrambo, Uprava Republike Slovenije za zascito in resevanje, Slovenia

#### Description:

Modern society has reached a high dependability on ubiquitous services and networks. Especially in crisis or emergency situations the availability of these services is crucial. Today, governmental and rescue entity communication services are characterized by a strong technical compartmentalization; the interworking and availability of crisis communication resources is not assured. This project highlights and deploys concepts to enhance the availability of these services and the existing networks by leveraging redundant communication channels wherever possible and using automatic redirection in the case of network failures. In crisis situations, rescue teams have to be assembled fast and flexibly; mobile and ad-hoc networks are one possible solution. Additional research on these networks will be conducted in this project to fulfil the requirements of crisis intervention teams. The problem of identification will be resolved using new research results in wireless and ad-hoc networks, where especially the integration of distributed knowledge of the current network environment (location information, RFID messages, recommended trust relations, etc.) into the protocols is a key issue for context adaptable recognition. The project will take advantage of IPv6 features for many of the ICT aspects related to crisis scenarios. With Luxembourg as the first test bed and the Luxembourg Government as a partner in the project, there is an ideal possibility to show the feasibility and usability of the results in a real environment and provide the basis for all European countries.

Wireless traffic Safety network between Cars	
<b>Acronym</b>	WiSafeCar
<b>Head of Project</b>	Pekka Eloranta (Mobisoft, Finland)
<b>Funding</b>	EUREKA-CELTIC, 300000€
<b>Running Time</b>	01/07/2009 – 31/12/2011

#### Members:

Pascal Bouvry, Grégoire Danoy, Yoann Pigné, Guillaume-Jean Herbiet, Patricia Ruiz.

**Domain(s):**

Vehicular Ad Hoc Networks, Secure Communications, Traffic Management, Accident Warning.

**Partner(s):**

Mobisoft, Finland (Pekka Eloranta, Coordinator),  
 Finnish Meteorological Institute, Finland (Dr. Timo Sukuvaara),  
 VTT, Finland (Tapio Frantti),  
 Taipale Telematics, Finland (Juha Laitsaari),  
 Sunit, Finland (Esa Suutari),  
 Ubridge, South Korea (Johnatan Jin),  
 University of Luxembourg (Prof. Pascal Bouvry),  
 CRP Henri Tudor (Dr. Djamel Khadraoui),  
 Ubistream, Luxembourg (Michel Krim).

**Description:**

WiSafeCar aims to develop an effective service platform and advanced intelligent wireless traffic safety network between cars and infrastructure, with possibility to exploit vehicle based sensor and observation data in order to generate secure and reliable intelligent real-time services and service platform for vehicles. More information: <http://www.wisafecar.com>

Development and Industrial Application of Multi-Domain Security Testing Technologies	
<b>Acronym</b>	DIAMONDS
<b>Reference</b>	N/A
<b>Head of Project</b>	Prof. Dr. Nicolas Guelfi
<b>Funding</b>	ITEA2 European Project (not funded)
<b>Running Time</b>	01/07/2010 – 31/12/2012

**Members:** Dr. Benoit Ries

**Domain(s):** Methodology, Security, Test, Model-driven Engineering, Banking Domain

**Partner(s):** Carlo Harpes,itrust (Luxembourg), Ina Schieferdecker, Fraunhofer FOKUS (Germany)

**Description:** DIAMONDS will leverage systematic, model-based testing and monitoring approaches for security testing to enable highly secure systems by early testing and test automation. Advanced model-based security

testing methods will allow the early identification of design vulnerabilities and efficient system/test design targeting security aspects. The DIAMONDS security test methodology will be adaptable to different multi-domain security standards, and enable a risk analysis-oriented test generation and risk assessments by evaluation of the test results. DIAMONDS will develop a well-visible European security test methodology of industrial scale, which demonstrates to be successful for security-critical systems in different application domains. The project is based on the complementary, interdisciplinary expertise and technologies of the partners from Austria, Finland, France, Germany, Luxembourg, Norway, and Spain, who have built competence through partnerships with industry and research in the various dimensions implied to address this issue: domain expertise, networked systems and services, security engineering, testing infrastructure, and model-based testing.

### 2.1.2 FNR CORE Projects

Attack Trees	
Acronym	ATREES
Reference	C08/IS/26
Head of Project	Prof. Dr. Sjouke Mauw
Funding	FNR-CORE, 299000€
Running Time	01/04/2009 – 31/03/2012

#### Members:

Sjouke Mauw, Barbara Kordy, Patrick Schweitzer, Saša Radomirović

#### Domain(s):

Security, formal methods, attack trees, security assessment

#### Partner(s):

Interdisciplinary Centre for Security, Reliability and Trust Telindus Luxembourg (Andre Adelsbach, Olivier Medoc and Joany Boutet)

#### Description:

Security assessment of systems is a standard but suboptimal procedure due to its informal nature. While a formal approach would be desirable, but out of reach, a systematic approach would be beneficial and feasible.

Attack trees are a well-known methodology to describe the possible security weaknesses of a system. An attack tree basically consists of a description

of an attacker's goals and their refinement into sub-goals. We believe that attack trees provide an ideal systematic approach for security assessment.

The purpose of this project is to extend, formalize, and develop the attack tree methodology as to make it a systematic, fully-fledged, and practical security assessment tool.

Due to their intuitive nature, attack trees are already one of several tools in security assessment. However, significant development of the methodology is needed before all potential benefits can be taken advantage of. Specifically, we have identified the following areas to be in need of work

- full formal semantics,
- parameterization, refinement, patterns, and libraries for applicability to large systems,
- integration of defense trees into attack trees,
- tool support.

The project benefits from our contacts with Telindus Luxembourg, a consultancy company offering security-related services such as security assessment. We work on case studies with the help of Telindus. Additionally, Telindus provides us its know-how in contemporary security assessment methodologies.

Cryptography and Information Security in the Real World	
<b>Acronym</b>	CRYPTOSEC
<b>Reference</b>	F1R-CSC-PFN-09IS04
<b>Head of Project</b>	Dr. Jean-Sébastien Coron
<b>Funding</b>	FNR-CORE, 272000€
<b>Running Time</b>	01/03/2010 - 28/02/2013

#### Domain(s):

Cryptography, Information Security, Side-Channel Attacks

#### Description:

Cryptography is only one component of information security, but it is a crucial component. Without cryptography, it would be impossible to establish secure communications between users over insecure networks like the internet. In particular, public-key cryptography (invented by Diffie and Hellmann in 1974) enables to establish secure communications between users who have never met physically before. One can argue that companies like E-Bay or

Amazon could not exist without public-key cryptography. Since 30 years the theory of cryptography has developed considerably. However, cryptography is not only a theoretical science; namely at some point the cryptographic algorithms must be implemented on physical devices, like PCs, smart-cards or RFIDs. Then problems arise: in general smart-cards and RFIDs have limited computing power and leak information through power consumption and electro-magnetic radiations. A cryptographic algorithm which is perfectly secure in theory can be completely insecure in practice if improperly implemented. Therefore, the aim of this proposal is to take into account every aspect of the implementation of secure systems in the real world, from the mathematical algorithms to the cryptographic protocols, and from the cryptographic protocols to their implementation in the real world. This allows creating a bridge between theoretical research in cryptography on the one side and its applications and the end users of the new technology on the other side. When dealing with cryptographic protocols, we will work in the framework of provable security: every security goal will be clearly defined, and every new cryptographic scheme or protocol should have a proof that the corresponding security goal is achieved, based on some well defined computational hardness assumption. When dealing with cryptographic implementations, we will try to cover all known side-channel attacks: timing attacks, power attacks, cache attack, etc.

Secure, Reliable and Trustworthy Voting Systems	
<b>Acronym</b>	SeRTVS
<b>Reference</b>	I2R-DIR-PFN-09IS06
<b>Head of Project</b>	Prof. Dr. Peter Ryan
<b>Funding</b>	FNR-Core, 333000€ FNR-AFR, 216216€ IMT Luca, 130000€ University of Melbourne, 60000€ UL, 268596€
<b>Running Time</b>	01/02/2010 - 01/02/2013

**Domain(s):**

e-Voting

**Partner(s):**

University of Surrey (UK), University of Birmingham (UK), Institute for Advanced Studies (I), University of Melbourne (Australia)

**Description:**

To be added.

Security Testing of Resilient Systems	
<b>Acronym</b>	SETER
<b>Reference</b>	F1R-CSC-PFN-08IS01
<b>Head of Project</b>	Prof. Dr. Nicolas Guelfi
<b>Funding</b>	FNR-CORE, 268000€
<b>Running Time</b>	01/05/2009 – 30/04/2012

**Members:**

Prof. Dr. Yves Le Traon Dr. Gilles Perrouin Dr. Benoit Ries

**Domain(s):**

Model-Driven Engineering and Testing, Fault Tolerance, Security, Resilient and Dynamically Adaptive Systems.

**Description:**

Resilient systems can be viewed as open distributed systems that have capabilities to dynamically adapt, in a predictable way, to unexpected and harmful events, including faults and errors. Engineering such systems is a challenging issue which implies reasoning explicitly and in a consistent way about functional and non-functional characteristics of systems. The difficulty to build resilient systems and the economic pressure to produce software with constraints on costs, quality, security, reliability, etc... enforce the use of practical solutions founded on scientific knowledge. One of these solutions is to propose an innovative testing process. Testing is an activity that aims at both demonstrating discrepancies between a systems actual and intended behaviours and increasing the confidence that there is no such discrepancy. One of the main features of a system to test is the security of the system, especially for those which are safety or business critical. The security of a system classically relates to the confidentiality and integrity of data as well as the availability of systems. Testing security properties is a real challenge, especially for resilient systems which have the capability to dynamically evolve to improve the security attributes. The objective of the SETER project fits with these ideas by proposing new security testing approaches for resilient systems the earlier possible during the software development lifecycle to propose more secure and more reliable system.

The Dynamics of Argumentation	
<b>Acronym</b>	DYNARG
<b>Reference</b>	F1R-CSC-PFN-09DYNAR
<b>Head of Project</b>	Prof. Dr. Leon van der Torre
<b>Funding</b>	FNR
<b>Running Time</b>	01/10/2009 – 31/09/2012

**Members:**

Richard Booth, Martin Caminada, Gabriella Pigozzi, Marija Slavkovic, Emil Weydert, Yining Wu

**Domain(s):**

argumentation theory, belief dynamics, multi-agent systems

**Partner(s):**

Universite d'Artois, Lens, France (Dr Souhila Kaci)

**Description:**

Artificial Intelligence is a science that aims to implement human intelligence. For this purpose it studies the behaviour of rational agents. Pertinent information may however be insufficient or there may be too much relevant but partially incoherent information. Different theories have been proposed for decision-making dealing with such information. However the growing development of multi-agent systems needs to handle collective decision and information coming from different sources. Moreover in multi-agent systems, agents need to interact in order to inform, convince, and negotiate with other agents. Argumentation theory is a suitable theory to support such interactions. In this project we will develop an abstract theory of dynamic argumentation in which arguments/conflict relations can be added/removed. We will also provide a framework for aggregation of argumentation frameworks for interaction among arguing agents. To this end we will develop new notions of distance between argument graph labellings, in order to define when an agent's position can be said to be "close to" or "far" from that of another. Finally we plan to apply the dynamic argumentation theory to dialogue between agents.

Security Games	
<b>Acronym</b>	S-GAMES
<b>Reference</b>	F1R-CSC-PFN-08IS03
<b>Head of Project</b>	Prof. Dr. Leon van der Torre
<b>Funding</b>	FNR-CORE, 314000€
<b>Running Time</b>	01/04/2009 – 31/03/2012

**Members:**

Leon van der Torre, Sjouke Mauw, Wojtek Jamroga, Matthijs Melissen

**Domain(s):**

Game theory, security protocols, non-zero sum games, imperfect information games, attack-defense analysis, verification, model-checking.

**Partner(s):**

GAMES Network

**Description:**

Information security is not a static black-and-white system feature. Rather, it is a dynamic balance between a service provider trying to keep his system secure and an adversary trying to penetrate or abuse the service. Such interplay can be considered as a game between the adversary and the service provider and the field of game theory provides methods and tools to analyze such interactions.

Games for verification and design have been studied in computer science for the last ten years. This fundamental research into extending and complementing traditional verification approaches from formal methods with game theoretic reasoning is paving the way for more effective verification tools. These developments are of particular interest to the field of security, in which formal verification has always played an important role. The purpose of the project is to study how these new developments can be used to strengthen current analysis and verification techniques in information security.

The project has two main lines of research: 1) A study of the use of game-theoretic methods in the field of security, resulting in requirements on game-theoretic methods for security. 2) The development of novel verification methods based on the combined use of formal verification techniques and a game theoretic approach, and its application to the field of security.

For the first line, two areas in security are selected for which the application of these techniques seems particularly promising: fair exchange protocols and attack/defense analysis. The second line focuses on the interplay of finite and infinite games, mathematical logic and automata theory, in particular on analysis techniques for infinite-state systems, linear-time model checking, and game models for protocols.

The S-GAMES project is a joint project of the SaToSS group and the ICR group.

Trust-assurance for critical infrastructures in multi-agents environments	
<b>Acronym</b>	TITAN
<b>Reference</b>	F1R-CSC-PFN-08IS21
<b>Head of Project</b>	Dr. Benjamin Gateau
<b>Funding</b>	FNR-CORE, 108000€
<b>Running Time</b>	1/01/2009 – 31/12/2010

**Members:**

Pascal Bouvry, Grégoire Danoy, Marcin Seredynski, Thomas Schaberreiter.

**Domain(s):**

Trust, Security, Critical Infrastructures, Metrics, Policy Engineering, Governance, Responsibility, Distributed and Multi-agents Systems, Aggregation techniques, Constraints in Policies, Organisational Models.

**Partner(s):**

North Dakota University (Asst. Prof. Samee U. Khan),  
VTT Technical Research Centre of Finland (Prof. Eila Niemela),  
Ecole Nationale Supérieure des Mines de St-Etienne (Prof. Olivier Boissier).

**Description:**

The University of Luxembourg work-packages aim at providing innovative methodologies to efficiently and effectively retrieve and manage trust metrics, such as access rights, trust measures, and reputation in critical infrastructures. More information: <http://titan.gforge.uni.lu>

EnerGy-efficient REsourceE AllocationN in AutonomIc Cloud CompuTing	
<b>Acronym</b>	GreenIT
<b>Reference</b>	F1R-CSC-PFN-08IS21
<b>Head of Project</b>	Prof. Dr. Pascal Bouvry
<b>Funding</b>	FNR-CORE, 450K€
<b>Running Time</b>	1/01/2010 – 31/12/2012

**Members:**

Pascal Bouvry, Grégoire Danoy, Marcin Seredynski, Bernabe Dorronsoro, Sebastien Varrette, Johnatan Pecero, Zdislaw Suchanecki, Dzmitry Kliazovich, Thanga Raj.

**Domain(s):**

Energy-efficiency; resource management; heterogeneous computing; multi-objective optimization; multi-agent systems; parallel and distributed computing; telecommunication networks; cloud computing.

**Partner(s):**

North Dakota University (Asst. Prof. Samee U. Khan),  
LuxConnect (Prof. Dr. Thomas Engel),  
GoodYear S.A. Luxembourg  
University of Sydney, Australia (Prof. Dr. Albert Zomaya),  
University of Toulouse, France (Prof. Dr. J-M Pierson),  
INRIA Lille, France (Prof. Dr. El-Ghazali Talbi)

**Description:**

The project GreenIT aims to provide a holistic autonomic energy-efficient solution to manage, provision, and administer the various resources of Cloud-Computing (CC) data/HPC centers.

The main research challenges that will be tackled to achieve the holistic approach are:

- Development of a multi-objective mathematical meta-model: CC is a complex system of numerous pervasive devices that request services over heterogeneous network infrastructures from a data center that is energy gobbler. Because each computing entity's performance is defined uniquely, we must develop a multi-objective meta-model that can adequately define a unified and performance metric of the whole system. The multiple constraints and objectives dealing with the quality of service (QoS), cost and environment impact must be formulated and their relationship analyzed.
- Develop resource management and optimization methodologies: With several possible objectives and constraints, the meta-models must result in multi-objective multi-constraint optimization problems (MOP). Green-ICT will develop, refine, and evolve solutions for MOP that will primarily be based on metaheuristics (e.g. multi-objective evolutionary algorithms, multi-objective local search, hybrid metaheuristics).

- Develop autonomic resource management: The anytime anywhere slogan only will be effective when an autonomic management of resources can be achieved. The resource allocation methodologies developed must go further refinement such that the system at hand is self-healing, repairing, and optimizing. In particular, it is our intention to utilize multi-agent systems (MAS) that can learn to adapt (machine learning methodologies) and gracefully evolve to adapt (evolutionary game theoretical methodologies).

Model-Driven Validation and Verification of Resilient Software Systems	
<b>Acronym</b>	MOVE
<b>Reference</b>	F1R-CSC-PFN-09IS02
<b>Head of Project</b>	Prof. Dr. Nicolas Guelfi
<b>Funding</b>	FNR-CORE, 265K€
<b>Running Time</b>	01/05/2010 – 31/04/2013

**Members:** Levi Lucio, Yasir Khan, Qin Zhang

**Domain(s):** Software Engineering, Security, Dependability, Model Checking, DSL, Model Driven Engineering, Testing

**Partner(s):** University of Geneva

**Description:** Verification and Validation of software have nowadays clear meanings in the context of Model-Driven Development. With test based verification we worry about producing a set of test cases that will, on the one hand find faults in an implementation - also called in the test literature System Under Test (SUT) - and on the other hand increase trust in the final product. With validation we worry about understanding if the model we are using as reference for implementation and for extracting test cases from is sound. Formal validation is often achieved by mechanically proving properties the model should satisfy. For example, dynamic properties could be expressed in a temporal logic and static properties on the system state could be expressed using logical invariants and then verified on the system's model. In this project we will focus our attention on the application of validation and verification techniques to the Model Driven Engineering of systems where resilience mechanisms are explicitly modelled and implemented according to that model. Resilience corresponds to the fact that a system has the capability to adapt to harmful events and recover to a stable state or at least continue operation in a degraded mode without failing completely. These harmful events might cause the fundamental security properties (confidentiality, integrity and availability) to be violated. With this project we aim at improving the state of the art of the construction of reliable resilient systems

by using verification and validation techniques within the context of Model Driven Development (MDD). The current trend of Software Engineering is to increasingly reason about the system being built at the model level by using appropriate Domain Specific Languages (DSL) for each conceptual domain. In this project we will concentrate on resilience and materialize it as a DSL. Model composition techniques can then be used in order to compose resilience features expressed in the resilience DSL with other domains equally defined as DSLs. When the composed model is validated, verification techniques can then be used to insure the resilience properties are well implemented. We will tackle this problem both at a theoretical and a practical level.

<b>Model Composition for Executable Modeling</b>	
<b>Acronym</b>	COMPEX
<b>Reference</b>	F1R-CSC-PUL-10MCEM
<b>Head of Project</b>	Prof. Dr. Pierre Kelsen
<b>Funding</b>	UL: 171K€
<b>Running Time</b>	01/08/2010 – 31/07/2010

#### **Members:**

Pierre Kelsen, NN

#### **Domain(s):**

model-driven software development, model composition, executable modeling

#### **Description:**

In model-driven software development models are the primary artifacts for constructing software. Model composition or the process of composing simpler models into more complex models helps in mastering the complexity of model-driven development. Most of the current model composition techniques can be viewed naturally as model transformations taking two input models and producing one output model. In our work we have introduced a new composition technique for building executable models. It has several properties that traditional composition techniques do not have: it is additive rather than transformational; it can be applied to any meta-model; and it has a formal semantics.

The present project will investigate the power of our composition technique with respect to existing composition techniques. In particular we will compare our technique with approaches from aspect-oriented modeling that are typically used to express crosscutting concerns. The project will investigate whether our approach can be extended to match the power of these techniques; and/or how it can complement the existing approaches in mod-

eling systems in a more straightforward, elegant, and light-weight manner. The main goal is to enhance our current modeling framework and tool for executable modeling with new model composition techniques so that they can handle not only the academic examples studied so far but can be used effectively on larger systems.

### 2.1.3 UL Projects

Refining Key Components in Trust Models	
Acronym	RKCTM
Head of Project	Prof. Dr. Sjouke Mauw
Funding	FNR-AFR, 50,360€ per year
Running Time	01/01/2009–31/07/2010

#### Members:

Sjouke Mauw, Baptiste Alcalde

#### Domain(s):

Trust, Recommender Systems, Formal Methods

#### Partner(s):

N.A.

#### Description:

Trust is a prediction of reliance on an action, based on what one party knows about another party. The fundamental problem in trust management concerns the establishment of a trust relation in a virtual environment. A trust model attempts to quantify trust by combining relevant information from various sources.

The main aim of the present project is to investigate two research areas, namely delegation and competence, in the scope of a recently developed trust model. A wide variety of practical applications can be foreseen in domains such as e-banking services, spam filters, personal health records, and online communities. We also intend to establish a new area of research in solving decision problems based on risk and trust.

The insights gained in the course of this research will be put to test by developing case scenarios, in particular a case study on e-banking services. We will investigate the scalability and practical effectiveness of our approach and use our insights to refine the model and its components. The case study is adapted to Luxembourg's needs in order to maintain its leading role as a

financial place.

A Formal Approach to Enforced Privacy in e-Services	
<b>Acronym</b>	EPRIV
<b>Reference</b>	PUL-09EPRI
<b>Head of Project</b>	Prof. dr. Sjouke Mauw
<b>Funding</b>	UL, 254955€
<b>Running Time</b>	01/05/2009–30/04/2012

**Members:**

Sjouke mauw, Jun Pang, Hugo Jonker, Naipeng Dong

**Domain(s):**

Enforced privacy, verification, formal modelling, e-services

**Partner(s):**

ENS CACHAN (Steve Kremer)

**Description:**

Privacy has been a fundamental property for distributed systems which provide e-services to users. In these systems, users become more and more concerned about their anonymity and how their personal information has been used. For example, in voting systems a voter wants to keep her vote secret. Recently, strong privacy properties in voting such as receipt-freeness and coercion-resistance were proposed and have received considerable attention. These notions seek to prevent vote buying (where a voter chooses to renounce her vote). These strong notions of privacy, which we will call enforced privacy, actually capture the essential idea that privacy must be enforced by a system upon its users, instead of users desiring privacy.

The first aim of this project is to extend enforced privacy from voting to other domains, such as online auctions, anonymous communications, healthcare, and digital rights management, where enforced privacy is a paramount requirement. For example, in healthcare, a patient's health record is private information. However, a patient contracting a serious disease is at risk of discrimination by parties aware of her illness. The inability to unveil (specific parts of) the health record of a patient is a minimal requirement for her privacy.

The second aim of the project is to develop a domain-independent formal framework in which enforced privacy properties in different domains can be captured in a natural, uniform and precise way. Typically, enforced privacy properties will be formalized as equivalence relations on traces, which

take into account both the knowledge of the intruder and the users. Within the framework, algorithms can be designed to support analysis of e-service systems which claim to have enforced privacy properties. In the end, the formalization and techniques will be applied to verify existing real-life systems and to help the design of new systems with enforced privacy properties.

Embedded Systems Security	
<b>Acronym</b>	ESS
<b>Reference</b>	F1R-CSC-PUL-08ESSE
<b>Head of Project</b>	Prof. Dr. Alex Biryukov, Prof. Dr. Jean-Sebastien Coron, Prof. Dr. Sjouke Mauw
<b>Funding</b>	UL, 331106.73€
<b>Running Time</b>	01/10/2008 - 31/01/2012

**Members:**

Alex Biryukov, Jean-Sebastien Coron, Sjouke Mauw, Ralf-Philipp Weimann, Chenyi Zhang

**Domain(s):**

Verification, Security Protocol, Model Checking

**Partner(s):**

None

**Description:**

The goal of this project is to study cryptosystems and secure protocols for embedded systems (mobile phones, PDAs, smartcards, RFID tags). This is currently an important area of research due to proliferation of portable information processing devices and their penetration in our everyday life. This process is driven by public demand and by the industry. By working together with the industry, the academic research can provide necessary tools in order to procure information security and privacy which becomes more and more important (and often is lacking) in the digital world. The project currently is structured as follows: cryptography for embedded systems (secret key and public key), secure protocols for embedded systems, implementation aspects, biometrics and privacy issues, wireless security. This is a joint project of the SaToSS group with LACS professors Alex Biryukov and Jean-Sebastien Coron.

Security and Cryptography in the Real World	
<b>Acronym</b>	SECRYPT
<b>Reference</b>	F1R-CSC-PUL-07SECR
<b>Head of Project</b>	Prof. Dr. Jean-Sébastien Coron
<b>Funding</b>	UL, 950000 €
<b>Running Time</b>	01/01/2007 - 31/08/2010

**Members:**

Jean-Sébastien Coron, Alex Biryukov, Volker Müller, David Galindo, Ilya Kizhvatov, Avradip Mandal, Jean-François Gallais, Bin Zhang

**Domain(s):**

Cryptography, Information Security, Security Proofs

**Description:**

Today, information technology has expanded to encompass most facets of our daily lives - at work, at school, at home for leisure or learning, and on the move - and it is reaching ever-widening segments of our society. The Internet, e-mails, mobile phones, etc. are already standard channels for the information society to communicate, gain access to new multimedia services, do business or learn new skills. The recent "digital revolution" and widespread access to telecommunication networks have enabled the emergence of e-commerce, which will most likely deeply alter the very concept of business in the near future. This proliferation of digital communications has raised new concerns in terms of security: for example, copyright protection, access rights management and privacy protection. Security is an interdisciplinary subject, drawing from several fields: cryptography, network security, algorithmic number theory, software and hardware engineering, formal verification, AI, signal processing, legal issues, data and text mining, anomaly and fraud detection, any many more. In this context, we find it very appropriate to outline in this document a "Security and Cryptography in the Real World" research program proposal. This research program builds on an existing expertise in the relevant fields among the University's faculty members, and its goal is to bring together specialists of the different fields mentioned above to address the problems of security in a global and really efficient way. This research program would therefore prove to be a very innovative and profitable step towards the advancement of the state of the art in a field that is sure to be of paramount importance in tomorrow's society.

<b>Modelling Dependable Collaborative Time-Constrained Business Processes</b>	
<b>Acronym</b>	DT4BP
<b>Head of Project</b>	Prof. Dr. Nicolas Guelfi
<b>Funding</b>	UL (Assistant contract)
<b>Running Time</b>	01/01/2007 – 15/12/2010

**Members:**

Alfredo Capozucca

**Domain(s):**

Dependable Distributed Software Systems, Transaction Processing, Real-Time Computing, Model-Driven Engineering, Metamodelling, Business Processes, Workflows.

**Description:**

A dependable collaborative time-constrained business process (DCTC-BP) is one whose participants interact closely to reach a goal that is of common interest; time-related information is used to constrain its behaviour, and failures (i.e. missing the goal) are not unacceptably frequent or severe. Since DCTC-BPs descriptions are not just written, but also read and rewritten many times, business analysts in charge of eliciting them must rely on a suitable and expressive modelling notation that allows such business process to be written in an elegant and readable way. A modelling notation that embeds concepts related to collaboration, time and dependability as first-class citizens along with tools that support its use are fundamental to succeed in providing not only "elegant" and "readable" business processes, but also correct ones.

<b>PRISMA : a Process for Requirements Identification, Specification and Machine-supported Analysis, targeting Transactional Models seen under a Product Line perspective</b>	
<b>Acronym</b>	PRISMA
<b>Head of Project</b>	Prof. Dr. Nicolas Guelfi
<b>Funding</b>	UL (Assistant contract)
<b>Running Time</b>	16/03/2006 – 15/03/2010

**Members:**

Barbara Gallina

**Domain(s):**

Transaction Processing, Requirements Engineering, Software Product Lines Engineering, Formal Methods

**Partner(s):**

University of Newcastle upon Tyne, UK (Prof. Alexander ROMANOVSKY)

**Description:**

Engineering the requirements of the right Transactional Model (right with respect to the business goals of the application to be supported) is a hard task since it involves the critical choice of the right degree of ACIDity, that is the right selection of requirements in terms of Atomicity, Consistency, Isolation and Durability, which altogether are fundamental to ensure dependability and, more specifically, reliability. Up to now, this task is definitively not supported by a process. The PRISMA project is aimed at providing a novel process, called PRISMA. PRISMA is a Process for Requirements Identification, Specification and Machine-supported Analysis which targets Transactional Models. PRISMA aims at being helpful as a prism in the identification of fundamental constituting properties of Transactional Models to achieve, as a result of the PRISMA process, a correct and valid requirements specification. The main idea behind PRISMA is that Transactional Models may be considered as a Product Line (PL) and that variabilities and commonalities may be identified to distinguish similarities and differences among "products". Specifically, PRISMA is conceived for engineering the specification of a Transactional Model by placing the effort in revealing its Atomicity, Consistency, Isolation and Durability requirements, which represent the variabilities of the PL.

**Resource Allocation in Delay and Disruption Tolerant Networks**

<b>Acronym</b>	RADTN
<b>Reference</b>	F1R-CSC-COM-0800
<b>Head of Project</b>	Prof. Dr. Simin Nadjm-Tehrani
<b>Funding</b>	UL (part time Assistant contract)
<b>Running Time</b>	01/09/2007 – 01/09/2011

**Members:**

Prof. Dr. Simin Nadjm-Tehrani, Gabriel Sandulescu

**Domain(s):**

delay-tolerant communications, opportunistic network, erasure coding, communication theory, performance evaluation

**Partner(s):**

University of Linköping, Sweden (Prof. Simin Nadjm-Tehrani)

**Description:**

This PhD research project aims at proposing new architectures, algorithms and communication protocols in intermittently connected ad hoc networks, also referred to as delay-tolerant networks. One potential interest is to minimise the impact of connectivity interruption when commuting or travelling, while also keeping the usage of network resources under control. The solutions proposed need to rely on a sound theoretical background and should be usable by network engineers. When a purely analytical framework proves to be insufficient, a simulation environment or practical implementation can be used in order to validate research results.

Adaptive High-gain Extended Kalman Filter and Applications	
<b>Acronym</b>	AEKF
<b>Head of Project</b>	Prof. Dr. ing. Juergen Sachau
<b>Funding</b>	UL (Project RAIP) - Junior Researcher contract
<b>Running Time</b>	2006 – 2010

**Members:**

Nicolas Boizot

**Domain(s):**

Process control, Observers for nonlinear Systems, Applied mathematics, High-gain Extended Kalman Filter.

**Partner(s):**

University of Burgundy (Prof. Eric Busvelle, co-directeur de thèse).

**Description:**

The work concerns the "observability problem" – the reconstruction of a dynamic process's full state from a partially measured state for nonlinear dynamic systems. The Extended Kalman Filter (EKF) is a widely-used observer for such nonlinear systems. However it suffers from a lack of theoretical justifications and displays poor performance when the estimated state is far from the real state, e.g. due to large perturbations, a poor initial state estimate, etc.

We propose a solution to these problems, the Adaptive High-Gain (EKF).

Observability theory reveals the existence of special representations characterizing nonlinear systems having the observability property. Such representations are called observability normal forms. A variant of the EKF based

on the usage of a single scalar parameter, combined with an observability normal form, leads to an observer, the High-Gain EKF, with improved performance when the estimated state is far from the actual state. Its convergence for any initial estimated state is proven. Unfortunately, and contrary to the EKF, this latter observer is very sensitive to measurement noise.

Our observer combines the behaviors of the EKF and of the high-gain EKF. Our aim is to take advantage of both efficiency with respect to noise smoothing and reactivity to large estimation errors. In order to achieve this, the observer automatically switches between two modes, based on a parameter value that is the heart of the high-gain technique. *Voila*, the Adaptive High-Gain EKF.

A measure of the quality of the estimation is needed in order to drive the adaptation. We propose such an index and prove the relevance of its usage. We provide a proof of convergence for the resulting observer, and the final algorithm is demonstrated via both simulations and a real-time implementation. Finally, extensions to multiple output and to continuous-discrete systems are given.

VERIFICATION of fault-tolerant advanced Transactional distributed sYstems	
<b>Acronym</b>	VERITY
<b>Reference</b>	F1R-CSC-PUL-08VERI
<b>Head of Project</b>	Prof. Dr. Nicolas Guelfi
<b>Funding</b>	University of Luxembourg, 364257€
<b>Running Time</b>	01/01/2008 – 31/12/2010

#### Members:

MSc Federico Wiecko

#### Domain(s):

Software Engineering, Dependability, Model Driven Engineering, Model Transformation, Simulation, Domain Specific Languages (DSL)

#### Description:

The VERITY project is a 3 year long research project that aims at developing tool support for (semi) formal languages to allow software engineers to model and verify secure and dependable advanced transactional distributed systems.

Model-Driven Engineering using a Declarative Behavioural Description Language	
<b>Acronym</b>	Medal
<b>Reference</b>	F1R-CSC-PUL-08MEDA
<b>Head of Project</b>	Prof. Pierre Kelsen
<b>Funding</b>	University of Luxembourg
<b>Running Time</b>	01/10/2008 – 30/09/2011

**Members:** Nuno Amálio, Christian Glodt

**Domain(s):** Visual Languages, modelling languages, software modelling

**Description:** Provide here a short abstract describing the project

Managing Regulatory Compliance: a Business-Centred Approach	
<b>Acronym</b>	MaRCo
<b>Reference</b>	I2R-DIR-PFN-09IS01
<b>Head of Project</b>	Prof. Dr. Pierre Kelsen
<b>Funding</b>	FNR: 749K €
<b>Running Time</b>	01/05/2010 – 30/04/2013

**Members:**

Pierre Kelsen, Leon van der Torre (University of Luxembourg)

**Domain(s):**

compliance, business process modeling, normative requirements

**Partner(s):**

Guido Governatori, NICTA Queensland Research Laboratory Elke Pulvermueller, University of Osnabrueck

**Description:**

The processes that underpin the businesses of our everyday lives are governed by regulations of ever growing complexity. In this context, it is important (a) to be able to describe these complex regulations rigorously, precisely and unambiguously, (b) that business practitioners are actually able to specify both regulations and business processes, and (c) to be able to check in an automated way that business processes comply with their underlying regulations. This project proposes to tackle these three issues. On one hand we want to improve existing approaches to formally describe (or model) norms. On the other hand we would like to make this practical and usable by prac-

tioners in such a way that the mathematical based formalisms involved in norm specification do not constitute a barrier to practitioners that know the business domain, but not the underlying mathematical formalism being used and so we propose a visual-based approach to norm specification. Finally, we intend to check the compliance of business processes against the norms that govern them in order to be able to detect in an automated way business processes that violate their underlying regulations.

The proposed research project aims at creating added value for service-related industries (e.g. in the banking sector) by making the specification of business processes and norms rigorous and precise yet accessible to domain experts, and enabling an automated approach to compliance checking. This should provide means to ensure that services are aligned with their underlying local and international regulations. With the growing need for regulatory compliance this will strengthen the expertise in service science in Luxembourg.

DECISION DECK – University of Luxembourg	
<b>Acronym</b>	D2
<b>Reference</b>	F1R-CSC-PUL-07D2D2
<b>Head of Project</b>	Prof. Dr. Raymond Bisdorff
<b>Funding</b>	UL, 140000€
<b>Running Time</b>	01/04/2007 – 31/12/2009

#### Members:

Thomas Veneziano (assistant/PhD student), Alexandru Olteanu (assistant/PhD student)

#### Domain(s):

Decision Aid, Operational Research

#### Partner(s):

Ecole Centrale de Paris (Pr. Vincent Mousseau)  
UMons, Faculté Polytechnique (Pr. Marc Pirlot)  
Karmic Software Research, Université Paris-Dauphine (Dr. Michel Zam)

#### Description:

The international DECISION DECK project aims at collaboratively developing Open Source software tools implementing Multiple Criteria Decision Aid (MCDA). These software components implement the common functionalities of a large range of MCDA methods. The UL specific contribution in this international project was initially focused on designing and implement-

ing web services around the RUBIS decision aid methodology<sup>1</sup>. The 2009 specific contribution, more ambitiously, concentrates at present on the design and implementation of **d4**: an on-line generic **D**eclarative **D**esigner for **D**ECISION **D**ECK multiple criteria decision aid web applications.

Recherches Mathématiques en Sciences de Décision	
Acronym	RMSD
Reference	F1R-CSC-PUL-08RMSD
Head of Project	Prof. Dr. Raymond Bisdorff
Funding	UL, 93300€
Running Time	01/01/2008 – 31/12/2010

#### Members:

Erkko Lehtonen (ass. researcher, postdoc, CSC)

#### Domain(s):

Discrete Mathematics, Theory of clones

#### Partner(s):

Miguel Couceiro (Mathematics RU, UL), Stephan Foldes (Tampere University of Technology, Finland), Léonard Kwuida (Zurich University of Applied Sciences, Switzerland), Jean-Luc Marichal (Mathematics RU, UL), Jaroslav Nešetřil (Charles University, Prague, Czech Republic), Ágnes Szendrei (University of Colorado at Boulder, USA and Bolyai Institute, Szeged, Hungary)

#### Description:

The RMSD project contributes to the areas of universal algebra, multiple-valued logic, combinatorics, and discrete mathematics in general, more precisely to the theory of clones, ordered sets, lattices, graphs, Boolean functions, and finite functions. Erkko Lehtonen's research topics include the study of substitution instances of functions when the inner functions are taken from a given set of functions. Every clone  $C$  on a fixed domain  $A$  induces a preorder and an equivalence relation on the set of all operations on  $A$ . Namely, let  $f$  and  $g$  be operations on  $A$ . We say that  $f$  is a  $C$ -minor of  $g$  if  $f = g(h_1, \dots, h_m)$  for some  $h_1, \dots, h_m$  in  $C$ . We say that  $f$  and  $g$  are  $C$ -equivalent if  $f$  and  $g$  are  $C$ -minors of each other. These notions unify and generalize various ideas that have been used by several authors in the theory of finite functions, and the  $C$ -equivalence can be seen as a relativized analogue of GREEN's  $R$ -relation, which is a fundamental notion in semigroup theory.

<sup>1</sup>see Bisdorff (2008), UL-ARTICLE-2009-854 [BMR08].

Advanced Argumentation Techniques for Trust Management	
<b>Acronym</b>	AASTM
<b>Reference</b>	F1R-CSC-PUL-07AAST
<b>Head of Project</b>	Prof. Dr. Leon van der Torre
<b>Funding</b>	UL
<b>Running Time</b>	01/08/2007 – 30/04/2010

**Members:**

Leon van der Torre, Martin Caminada, Yining Wu

**Domain(s):**

Computational argumentation, trust

**Partner(s):**

University of Luxembourg

**Description:**

The overall aim of AASTM is to enhance today's generation of argumentation formalisms and implementations in order to become suitable for a wider variety of real-life applications, such as reasoning about trust. This requires a unified theory that integrates the various forms of argumentation related functionality, as well as efficient proof procedures and sound and scalable software components.

Individual and Collective Reasoning	
<b>Acronym</b>	ICR
<b>Reference</b>	F1R-CSC-LAB-05ILIA
<b>Head of Project</b>	Prof. Dr. Leon van der Torre
<b>Funding</b>	UL, Projet de demarrage
<b>Running Time</b>	01/10/2006 – 30/09/2011

**Members:**

Gabriella Pigozzi, Marija Slavkovic, Leon van der Torre

**Domain(s):**

judgment aggregation, group-decision making, social choice theory, normative systems

**Description:**

Aim of the project is to investigate aspects of individual and collective ra-

tionality and to develop formal approaches for their representation. In particular, we are interested both in the generalization of existing frameworks for individual agent reasoning to its collective counterpart, and in the study and representation of the interactions between agents in a group.

Dynamics of trust in logic-based multi-agent systems	
<b>Acronym</b>	DYTRIL
<b>Reference</b>	F1R-CSC-F1-070058
<b>Head of Project</b>	Prof. Dr. Leon van der Torre
<b>Funding</b>	UL-PHD
<b>Running Time</b>	01/01/2007 – 31/12/2010

**Members:**

Mathijs de Boer

**Domain(s):**

Belief revision, trust, socio-epistemology, multi-agent systems,

**Partner(s):**

University of Luxembourg

**Description:**

The subject of the thesis is the investigation of the "Dynamics of trust in logic-based multi-agent systems". Trust is a concept which is of central importance for the security and reliability of systems communicating in open networks, e.g. in the context of e-commerce, cyberdefense, or e-science. However, existing frameworks to deal with trust are characterized by a static perspective, a low expressivity, and/or the absence of suitable mathematical foundations. The present project tries to tackle these issues in the context of logic-based multi-agent systems, which are a promising technology for the planned so-called semantic web. The main focus of the project has become the investigation of iterated revision formalisms exploiting trust information and modeling doxastic change as a social process.

Evolutionary Computing & Security	
<b>Acronym</b>	EVOSEC
<b>Reference</b>	F1R-CC-PUL-08VOS
<b>Head of Project</b>	Prof. Dr. Pascal Bouvry
<b>Funding</b>	UL, 250000€
<b>Running Time</b>	2008 – 2010

**Members:**

Grégoire Danoy, Marcin Seredynski, Marek Ostazewski, Julien Schleich, Apivadee Piyaturmong, Malika Mehdi.

**Domain(s):**

Evolutionary Algorithms, Intrusion Detection, MANETs

**Partner(s):**

Polish Academy of Sciences (Prof. Seredynski),  
University of Lille/INRIA (Prof. Talbi),  
University of Metz (Prof. Le Thi Hoai),  
University of Malaga (Prof. Alba).

**Description:**

EVOSEC aims to reinforce the knowledge of applying evolutionary techniques for security, including the use of cellular automata for random number generation, immune-system based intrusion detection, robust protocols for ad hoc networks, etc. More information: <http://evosec.gforge.uni.lu>

**2.1.4 Other miscellaneous projects**

Développement d'outils d'apprentissage en ligne pour les techniques de comptabilité, d'analyse financière et de gestion d'entreprise	
<b>Acronym</b>	Business-learning
<b>Reference</b>	F1R-CSC-PAU-07ELEA
<b>Head of Project</b>	Prof. Dr. ZAMPUNIERIS Denis
<b>Funding</b>	External funding (IUIL)
<b>Running Time</b>	01/01/2008 – 31/12/2009

**Members:**

PECORARO Gaëtan, DIAS Sergio

**Domain(s):**

e-Learning, accounting, entrepreneurship,

**Partner(s):**

IUIL (Mr. Wagner)

**Description:**

L'objectif du projet est de développer un outil e-learning en comptabilité, analyse financière et gestion d'entreprise et de l'implémenter au niveau de la formation initiale (enseignement secondaire, enseignement secondaire technique et enseignement supérieur) et au niveau de la formation continue (formations, cours et séminaires de l'Institut de Formation de la Chambre de Commerce, IFCC, du Luxembourg Lifelong Learning Center, LLLC, etc.). Cet outil sera prioritairement destiné au "blended learning", c'est-à-dire en tant que complément à un cours en présentiel.

Study of certain evolution systems in mathematical physics: magnetohydrodynamics of partially ionized plasmas, time irreversibility and decoherence in quantum systems	
<b>Acronym</b>	SESMP
<b>Reference</b>	VA108A08
<b>Head of Project</b>	Prof. Dr. Manuel Nunez Jimenez
<b>Funding</b>	University of Valladolid - 9700€
<b>Running Time</b>	01/01/2008 – 31/12/2010

**Members:**

Manuel Nunez Jimenez, Fernando María Gomez Cubillo, Zdzislaw Suchanecki

**Domain(s):**

Mathematics, Physics

**Partner(s):**

Dirección General de Universidades e Investigación Conserjería de Educación  
Junta de Castilla y León Spain

University of Valladolid (Manuel Nunez Jimenez, Fernando María Gomez Cubillo)

University of Luxembourg (Zdzislaw Suchanecki)

**Description:**

We intend to analyse certain important problems in Mathematical Physics by means of Functional Analytic techniques. Specifically, we will study the behaviour of plasmas formed by several fluid species. A second topic is the study of resonances and temporal irreversibility in classical quantum systems as well as the relations of these subjects with decoherence in open systems

and applications to the quantum information and computation theories. The main research tool will be the spectral analysis of wavelets. This requires, however, a development of new methods of constructing wavelets followed by the development of suitable computational algorithms.

**Modelling of Business and IT Landscapes addressing Security, Risk and Compliance in a Real-World banking environment (PhD thesis)**

<b>Acronym</b>	MBITSRC
<b>Reference</b>	F1R-CSC-PAU-06CRE
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	Funding by Credit Suisse and FNR (128.50K€)
<b>Running Time</b>	2005-2010

**Domain(s):**

IP and software modelling

**Partner(s):**

Credit Suisse

**Description:**

The overall focus is on reusing existing models first, adapting existing models second, and finally create new ones if needed. Further on the focus is on usability and automation of the modelling and checking process. The notion of clickable mathematics came up in this context.

**End-to-end Web Service Security in Aspect Oriented Programming**

<b>Acronym</b>	EWSSAOP
<b>Reference</b>	F1R-CSC-PAU-07LIA
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	Funding by EPT (75K€)
<b>Running Time</b>	2008 – 2011

**Members:**

Thomas Engel, Shaonan Wang,

**Domain(s):**

Network Security

**Partner(s):**

EPT

**Description:**

The monitoring of large network traffic volumes is limited by the existing technological solutions. Monitoring high speed 40 Gbps links is challenged by the already existing work charge on the routing data plane. One of the few activities that can be done is limited to recording and analyzing flow records. IP flow records are simple information records capturing the source, destination, the associated ports, the traffic volume and additional time stamps and flow related status. The natural question is how should these pieces of information be processed. On one side, the number of flow records is huge even for small sized edge routers, and on the other side it's not obvious what information should be analyzed. We have considered this research question in this paper. The main contribution of our paper is twofold: we propose a simple dependency model for IP flow records and show how link based analysis can reveal interesting flow events. We will use in this paper the words IP flow records and NetFlow records interchangeably. We have validated our approach using the proprietary NetFlow data format, but our method is general and can be applied to any flow record format. We aimed in this paper at identifying relevant flow records, where by relevant we understand the records that have generated ulterior network activity. We don't consider that a flow matching a specific signature (application level or based on the involved IP addresses) is relevant per se, but we do consider that flows, having triggered an important follow-up network activity, are relevant. The notion of triggering is linked to a potential dependency relationship among flow records. The best illustration for this is the case of an attacker breaking in over an SSH account. While the SSH related flow traffic is in general not relevant, in this case this could be the case if follow-up activities of the compromised host will be observed: large scale network scanning, rootkit downloading, massive SMTP traffic or botnet membership. For scoring such relevant IP flow records and understanding the most active activities on the network, our approach consists of two major steps. Firstly, with a simple yet efficient dependency model, we discover the causality dependency between NetFlow records. Then, to facilitate analyzing the overwhelming scale of NetFlow dependency graph, we automatically select the most relevant NetFlow records using the link analysis algorithm HIT. To the best of our knowledge, this is the first attempt to apply HITS algorithm from the web search and bibliometrics domain, in the field of network monitoring.

Satellite Communication Security (PhD thesis)	
Acronym	SCS
Reference	F1R-CSC-PAU-05ESA
Head of Project	Prof. Dr. Thomas Engel
Funding	Funding by ESA and FNR (90K€)
Running Time	2005 – 2009

**Members:**

Thomas Engel, Daniel Fischer

**Domain(s):**

Satellite Security

**Partner(s):**

European Space Agency

**Description:**

Space-link communication is using specialized protocols that differ very much from the network protocols that are used in terrestrial networks. Therefore, adaptation of existing information security features for these protocols is not straight forward. Development and validation of such information security solutions is required for space-link communication systems. Further, next-generation space missions will make use of a networked infrastructure in space. Such a spacecraft network is subject to environmental influences of space and therefore a topology has to be developed. Also, existing routing protocols perform badly in spacecraft networks and new (and also secure) solutions are anticipated here.

Until now, none of the existing spacecraft missions for the European Space Agency (ESA) uses information security features to protect spacecraft commanding and telemetry. However, data security starts to play a very important role in order to counteract the more and more numerous security threads. Some of the upcoming ESA missions already have security requirements defined and proprietary security systems are being developed for these missions. However, this is not a solution for the long term. More and more missions will require the implementation of security features and even purely scientific missions should be equipped with a minimum of protection. Therefore, it is crucial that a generic approach for space link security. We propose an approach for the integration of information security, especially confidentiality and authentication, into the existing CCSDS standards. This includes defining security layer locations in the space link communication protocol stacks and from this point identification of the ground segment infrastructure components that are needed to support them.

Next generation space missions will have a more complex infrastructure and will be supported by a spacecraft network. These networks will be strongly affected by a number of special properties of the space environment, in particular predictability of spacecraft movement, presence of ground stations and large propagation delays. While appropriate topology models and routing protocols exist to comply with large delays and intermittent connectivity, the important property of predictability has not been investigated to a greater extent. Further, since space missions are more and more considered to be vital infrastructure, information security solutions must be developed for these networks.

Secure Usage and Trust of Mobile Devices in Networks for international banking environments (PhD thesis)	
<b>Acronym</b>	SUTMDNiBE
<b>Reference</b>	F1R-PHY-PUL-06DRE
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	Funding by Dresdner Bank and FNR (45K€)
<b>Running Time</b>	2005-2010

#### Members:

Thomas Engel, Michael Stieghahn

#### Domain(s):

Access Control

#### Partner(s):

Dresdner Bank

#### Description:

Cross-border access to a variety of data such as market information, strategic information, or customer-related information defines the daily business of many global companies, including financial institutions. These companies are obliged by law to keep any data processing legal. Today's solutions for remote access are not able to dynamically adapt their access decisions to the current context. Therefore, they may decide either over-restrictive or under-restrictive, because the basis of a decision is the underlying static access control system.

We focus on the incorporation of legal constraints as a context information into a decision making process for international banking environments. Such constraints account for the identity of the user, who accesses the data, the identity of the customer, whose information is stored as data, and the loca-

tions, where the data is hosted and accessed. The locations serve the second purpose to determine which sets of legislation need to be observed [SE09g]. We are implementing our approach in the eXtensible Access Control Markup Language that promotes interoperability between different systems and is widely used as policy definition language [SE09f].

Work of the next period will be the completion and evaluation of the prototype of the law-aware access control. The refinement of the protocol that used for the communication between client and server is also an active task.

Self Organizing Security Sensors in highly-distributed IP networks (PhD thesis)	
<b>Acronym</b>	SOSSHIN
<b>Reference</b>	F1R-EDR-LIA-000005
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	Funding by SES-ASTRA and FNR (45K€)
<b>Running Time</b>	2007 – 2011

#### Members:

Thomas Engel, Gerard Wagner

#### Domain(s):

Adaptative Honeypots

#### Partner(s):

SES

#### Description:

The recent research activities have addressed the conceptual design and practical assessment of an adaptive honeypot based on game theory. We have addressed these topics, by proposing a game model for a system level honeypots. The best configuration profile has been determined based on the Nash equilibrium, where the best actions for the honeypot (and for an attacker) have been resulted. This work has been awarded the best paper award at the The 11th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2009) . A lateral research result, regarding the modeling and detection of malicious software has addressed the use of support vector machines and process level intrinsec monitoring. The results have been published [WWSE09] as a paper in the proceedings of the Malware 2009 Conference, in Montreal, Canada. We have also addressed a game theoretical model for the Tor anonymisation network, where attacker's and defendant's strategies can be modeled. This work is under

current submission. The current work is addressing more complex game models, based on repeated games- this work will identify the pertinent conceptual approaches, the definition of strategies and the identification of the associated equilibriums. The application domain will be twofold: netflow based monitoring (in collaboration with Alexandre Dulanoy) and system/host level monitoring.

Lux. Early-Warning Analysis and Information Sharing System	
<b>Acronym</b>	LEWIS
<b>Reference</b>	I2R-DIR-PAU-09LEWI
<b>Head of Project</b>	Prof. Dr. Peter Ryan
<b>Funding</b>	Ministère de l'Economie, 70000€ UL, 29120€
<b>Running Time</b>	2009 – 2010 (6 months)

#### Description:

To be added.

## 2.2 Grants

### 2.2.1 AFR

A Formal Approach to Enforced Privacy: Modelling, Analysis and Applications	
<b>Acronym</b>	EPRIV-MAA
<b>Reference</b>	PHD-09-027
<b>Head of Project</b>	Prof. Dr. Sjouke Mauw
<b>Funding</b>	FNR–AFR, 105222€
<b>Running Time</b>	01/12/2009 – 30/11/2012

#### Members:

Sjouke Mauw, Naipeng Dong, Jun Pang, Hugo Jonker

#### Domain(s):

Formal methods, verification, model checking, security, privacy, e-services

#### Partner(s):

ENS Cachan (Dr. Steve Kremer) University of Luxembourg (Prof. Dr. Peter Ryan)

**Description:**

The project is part of a peer-reviewed research project EPRIV - ‘A Formal Approach to Enforced Privacy in e-Services’, accepted for funding at the University of Luxembourg. The overall goal of this project is to develop a domain-independent formal framework to express the proposed concept of enforced privacy. We extend the notion of enforced privacy outside the domain of voting. Our formalization will take into account coalition-forming and defensive options. Moreover, within this framework, algorithms to verify these requirements will be developed to facilitate verification with tool support. This generic goal is comprised of the following sub-goals:

- Lifting the notion of enforced privacy to other e-service domains such as online auctions, anonymous communications, and healthcare; and formalizing the resulting notions;
- Establishing per-domain formal notions to verify enforced privacy;
- Capturing these notions in a domain-independent formal framework;
- Investigating enhancements to the formal framework to verify privacy.

Games for Modelling and Analysis of Security	
<b>Acronym</b>	GMASec
<b>Reference</b>	FNR–AFR PHD-09-082
<b>Head of Project</b>	Prof. Dr. Sjouke Mauw
<b>Funding</b>	FNR–AFR, 105223.44€
<b>Running Time</b>	01/11/2009–31/10/2012

**Members:**

Matthijs Melissen, Sjouke Mauw, Leon van der Torre, Wojtek Jamroga

**Domain(s):**

Formal methods, game theory, security, imperfect information games, verification, model checking

**Partner(s):**

Universite Libre de Bruxelles (Prof. Dr. Jean-Francois Raskin) Colorado State University (Prof. Dr. Ricky Yu-Kwong Kwok) GAMES Network

**Description:**

Agents participating in a security protocol try to achieve a common goal in a hostile environment. For some classes of security protocols, such as non-repudiation protocols or fair-exchange protocols, the participating agents

themselves cannot be trusted. We study the definition of the related security properties and the analysis of such protocols, and combine techniques from game theory and formal methods. Building on the results, we develop methods for the formal specification and verification of security protocols. The methods are implemented as an extension of a state-of-the-art security protocol verification tool. Case studies are performed by verifying existing protocols and developing new protocols.

The second thread in the project is related to the notion of attack trees that provide an informal, but very practical way to analyze the security of a complex system. When extending these with defenses, as to obtain attack–defense trees, it becomes possible to search for optimal defense strategies through the application of game theoretical concepts. In this project, we develop a methodology for analyzing attack–defense trees, and then to perform case studies to validate the methodology.

The project is executed in the context of the S-GAMES project. Here, we focus more on the practical issues in security analysis, modeling, and verification.

The GMASec project is a joint project of the SaToSS group and the ICR group.

<b>A Formal Approach to Privacy in Voting</b>	
<b>Acronym</b>	PRIV-VOTE
<b>Reference</b>	TR-PHD BFR07-030
<b>Head of Project</b>	Prof. Dr. Sjouke Mauw
<b>Funding</b>	BFR, FNR-AFR, 16098.30€
<b>Running Time</b>	01/05/2007 – 31/05/2009

#### **Members:**

Sjouke Mauw, Hugo Jonker

#### **Domain(s):**

Receipt-freeness, electronic voting, privacy, anonymity, protocol analysis, formal methods.

#### **Partner(s):**

Eindhoven University of Technology (Prof. Dr. J.C.M. Baeten)

#### **Description:**

This project investigated privacy notions in the context of electronic voting. The focus was on examining voting protocols that use untrustworthy

(Dolev-Yao like) networks as a communication channel, that promise to offer privacy. The research resulted in a formal, process-algebraic framework in which privacy notions and voting protocols can be expressed. Privacy notions such as receipt-freeness and anonymity are formalized in this framework. Additionally, various voting protocols from literature were modeled in a process-algebraic manner. These models are then evaluated within the framework with respect to the established requirements. Where the framework indicated privacy issues, these issues were translated back into problems in the original voting scheme, and discussions for improvements were made. The project was successfully concluded in May 2009, resulting in a successful defense in August 2009.

Security Analysis Through Attack-Defense Trees	
<b>Acronym</b>	SADT
<b>Reference</b>	PHD-09-167
<b>Head of Project</b>	Prof. Dr. Sjouke Mauw
<b>Funding</b>	FNR-AFR, 106476€
<b>Running Time</b>	01/01/2010 – 31/12/2012

#### Members:

Patrick Schweitzer, Sjouke Mauw, Barbara Kordy, Sasa Radomirovic

#### Domain(s):

Security, formal methods, attack trees, defense trees, attack-defense trees, security assessment.

#### Partner(s):

Interdisciplinary Centre for Security, Reliability and Trust Telindus Luxembourg (Andre Adelsbach, Olivier Medoc and Joany Boutet)

#### Description:

The project SADT project – security analysis through Attack–Defense Trees – is part of the ATREES peer reviewed CORE project. It aims to generalize attack trees, first introduced by Bruce Schneier in 1999. By combining attack trees with defense trees into one coherent framework of Attack–Defense Trees (ADTs), counteractions can be included into the security analysis.

The SADT project is a joint project of the Interdisciplinary Centre for Security Reliability and Trust (SnT) and SaToSS. It is funded by SnT and the FNR.

The aim of the project is to define a unified language for ADTs, to introduce several semantics arising from different mathematical disciplines, and to

create a software tool that helps to support the work of security analysts. With the help of case studies provided by the industry partner Telindus, different use cases will be examined in order to tailor and refine the semantics and improve the usability of the software tool.

Security Protocols in Identity Management	
<b>Acronym</b>	SPIM
<b>Reference</b>	BFR07-103, TR-PHD BFR07-103
<b>Head of Project</b>	Prof. Dr. Sjouke Mauw
<b>Funding</b>	BFR, FNR-AFR, 88984€
<b>Running Time</b>	01/10/2007-30/11/2010

#### Members:

Sjouke Mauw, Ton van Deursen, Sasa Radomirovic

#### Domain(s):

Security protocols, RFID, formal verification, security properties.

#### Description:

Nowadays, our identity is represented by an ever growing pile of paper and plastic documents such as passports, social security cards, bank cards, store loyalty cards, and company employee badges. Each of these items is backed by an entry in an electronic database. With increasing frequency we are also being represented by so-called virtual identities, for instance when purchasing items in online stores, visiting social networking websites, or simply accepting a website's "cookies". We can create and abandon these virtual identities at will and even share them with others.

Identity management is the assignment, verification, and revocation of the privileges, rights, and duties of electronic and virtual identities. The increase in electronic and virtual identities over the years has been dramatic. As a consequence, today, identity management is recognized as an important and expensive business problem. The number of electronic and virtual identities per individual, however, will grow even larger, due to the continuing effort to connect and network every aspect of our lives.

The advancement of a technology promotes new possibilities, new applications, but also new threats. For example, the imminent pervasiveness of Radio-frequency identification (RFID) systems will make it possible to cheaply collect and cross-reference a vast amount of data in order to infer sensitive personal information. It is clear that the communication between RFID tags and RFID readers needs to be secure.

The primary objective of the proposed work is the design and verification of secure communication protocols related to identity management and with a view towards emerging technologies such as RFID. We intend to achieve this objective by developing advanced formal verification methods and implementing an automatic tool. This development requires a fundamental study of non-standard security properties, such as non-traceability and no-theft-of-service, and an extension of a formal model for modeling of physical tokens.

Cryptanalysis of Hash Functions	
<b>Acronym</b>	CRHF
<b>Reference</b>	TR-PHD-BFR07-031
<b>Head of Project</b>	Prof. Dr. Alex Biryukov
<b>Funding</b>	FNR-AFR, 36,379€ per year
<b>Running Time</b>	01/05/2007 – 28/02/2011

**Members:** Ivica Nikolic

**Domain(s):** Cryptography

**Partner(s):**

none

**Description:**

The goal of this project is to study design and cryptanalysis of cryptographic hash functions. Cryptographic hash functions are central primitives used as building blocks in most of security protocols. They provide data integrity (both in storage and in transit), are used in digital signatures, user identification (e.g. remote access), and are closely related to MACs (message authentication codes).

Selected Problems in Executable Modeling	
<b>Acronym</b>	SPEM
<b>Head of Project</b>	Prof. Dr. Pierre KELSEN
<b>Funding</b>	AFR PHD-09-084
<b>Running Time</b>	15/11/2009 – 15/11/2012

**Members:**

Moussa AMRANI

**Domain(s):**

Model-Driven Engineering, Domain-Specific Modeling Languages, Structural Specification, Behavioural Specification, Semantics, Executability

### Description:

Model-Driven Engineering shifted the way software were developed from code-centric view to model-centric view: the system is generated from the model specification without roundtrips to keep code and models synchronized. Because real systems are large and complicated, several domain-specific modeling languages are required: accurately specific, they describe adequately the relevant concepts of a given domain; but in order to be integrated to form the final system, they must conform to an underlying common formalism that adequately represent the behaviour of the overall system that must be generated.

EP [KM08] systems allow a modeler to define both structural and behavioural specification of a system. In the current approach<sup>2</sup>, domain hierarchy is the structuring notion of systems: each domain of a system is defined in a self-contained manner, and because domains are not sufficient to describe a full system, bridges are used to propagate the behaviour of each domain through other domains in a consistent way. For example, consider an application that describes a Document Management system: domains specify libraries and management (basically, a GUI) but in order to be executable, events described by the GUI and triggered by the user of the system must affect the library (e.g, by effectively adding a new document).

The goal of the PhD is to define how domain-specific modeling capabilities can be integrated in the EP framework by providing an user-friendly mechanism to define and exploit domain-specific domains and bridges.

Expressing Non-Functional Requirements in Declarative Executable Models	
<b>Acronym</b>	ENFRDEM
<b>Reference</b>	AFR
<b>Head of Project</b>	Prof. Dr. Pierre Kelsen
<b>Funding</b>	FNR - AFR PostDoc
<b>Running Time</b>	01/01/2008 – 31/05/2010

### Members:

Qin Ma, Pierre Kelsen

### Domain(s):

<sup>2</sup>See [http://democles.lassy.uni.lu/documentation/TR\\_LASSY\\_08\\_05.pdf](http://democles.lassy.uni.lu/documentation/TR_LASSY_08_05.pdf)

Model-driven software engineering, formal semantics, executable modeling, domain integration, modular model composition.

**Description:**

The context of this project is the model-centric approach within model-driven software development that aims at providing a model-based description of a system that is precise enough for generating the full implementation. In particular the case where the behavior of the system is expressed using a declarative language will be considered. The goal of the project is to develop approaches for representing non-functional requirements in systems that have been specified in this way. Current work in aspect-oriented programming and aspect-oriented modeling will be analyzed for its applicability to this problem. The analysis will be based on a formal semantics of the behavioral description language that will be developed in a preparatory phase, based on existing approaches for defining the semantics of programming languages and of software models.

The project is closely related to the MEDAL project (see page 39) that is carried out at the Laboratory for Advanced Software Systems of the University of Luxembourg and fits within the high priority area P1 "Security and Reliability" of the University.

Universality and Self-Organization in Next-Generation Distributed Environments	
<b>Acronym</b>	UNISON
<b>Reference</b>	AFR PHD-08-016
<b>Head of Project</b>	Prof. Dr. Steffen Rothkugel
<b>Funding</b>	AFR, 106476€
<b>Running Time</b>	01/01/2009 – 31/12/2011

**Members:**

Jean Botev

**Domain(s):**

Self-Organization, Complex Networks, Social Networks, Topology Control, Distributed Virtual Environments, Peer-to-Peer

**Description:**

The increasing awareness of complex networks has led in recent years to a number of interesting findings in various scientific areas. These display underlying principles that, by virtue of their universal character, can be employed for the design of self-organizing systems. This research project aims

at investigating how such principles can be utilized to enable the efficient provision of massively distributed, scalable and interactive applications. Due to the immense number of potential users, the expedient conceptual design of network topologies for such future global-scale application domains is a central problem in the area of distributed systems. Recently established applications such as social-based virtual environments, pose severe challenges to existing networks like the Internet. These cannot be met by today's prevalingly deterministic architectures which expose bad scalability and fault-tolerance behavior. In the last few years, a paradigm shift occurred, pointing towards more stochastic-oriented approaches to complex networks. Originating from statistical mechanics, such an approach allows quantitative and qualitative statements to be made using just an essential set of global parameters, known as universality. The research project is intended to contribute to the understanding of how universality can be utilized to improve next-generation networks. Self-organization and dynamic adaption shall be substantiated as appropriate modeling mechanisms for efficient topologies. A set of algorithms and methodologies tailored to virtual environments shall be developed by identifying critical parameters and exploiting inherent characteristics of the underlying complex networks.

Towards a unified logical framework for action, uncertainty and causality	
<b>Acronym</b>	ULFAUC
<b>Reference</b>	TR-PDR BFR08-056
<b>Head of Project</b>	Prof. Dr. Leon van der Torre
<b>Funding</b>	FNR-AFR-Postdoc
<b>Running Time</b>	01/09/2008 – 31/08/2010

#### Members:

Guillaume Aucher

#### Domain(s):

Knowledge representation, logic, causality

#### Description:

Reasoning adequately about actions and causality under uncertainty is an important issue that is relevant to many fields such as artificial intelligence, social sciences, economics, cognitive psychology, and engineering. This problem has only been partly tackled by declarative logic-oriented approaches, which usually have focused (mainly) on one of the relevant themes: action, causality, uncertainty. Popular accounts include the situation calculus, dynamic epistemic logic, Pearl's causal networks, and conditional logics.

However, because these issues are closely related, they should preferably be addressed together. It is the goal of this project to contribute to the creation of such an integrated logical framework. Furthermore, we try to apply the techniques developed in this context also to open questions in normative reasoning.

Modeling and Developing a Novel Distributed Authorization Logic	
<b>Acronym</b>	FSL
<b>Reference</b>	PHD-09-026
<b>Head of Project</b>	Prof. Leon van der Torre
<b>Funding</b>	FNR-AFR
<b>Running Time</b>	01/09/2009 – 31/08/2012

**Members:**

Valerio Genovese, Guido Boella, Leon van der Torre, Dov Gabbay

**Domain(s):**

access control, authentication, security and privacy policies, language-based security, logic, artificial intelligence

**Partner(s):**

University of Torino (Prof. Guido Boella)

**Description:** Access Control, Authorization and Authentication are main-stream topics in computer science security that can be grouped under the notion of "trust management". In an increasingly interconnected world security policies are evolving from a static disconnected environment to a highly dynamic and distributed one (e.g. Internet, Social Networks).

The main aim of this project, is to create a formal and expressive logic through which computers can reason to grant access to external entities and users can model and specify, in a clear and explicit way, what are the policies which govern their systems. The new logic we plan to develop deeply extends and enrich existing approaches from the literature. We also plan to create a calculus for this logic in order to define an efficient algorithm to automatize the reasoning process for large scale applications. From the modelling point of view, we aim to define a model checking methodology to assist ICT security officers in crafting secure and stable systems.

Games for Modelling and Analysis of Security	
<b>Acronym</b>	GMASec
<b>Reference</b>	FNR–AFR PHD-09-082
<b>Head of Project</b>	Prof. Dr. Sjouke Mauw
<b>Funding</b>	FNR-AFR
<b>Running Time</b>	01/11/2009 – 31/10/2012

**Members:**

Matthijs Melissen, Sjouke Mauw, Leon van der Torre, Wojtek Jamroga

**Domain(s):**

formal methods, game theory, security protocols, non-zero sum games, imperfect information games, attack-defense analysis

**Partner(s):**

Universite Libre de Bruxelles (Prof. Dr. Jean-Francois Raskin) - Colorado State University (Prof. Dr. Ricky Yu-Kwong Kwok) - GAMES Network

**Description:**

Agents participating in a security protocol try to achieve a common goal in a hostile environment. For some classes of security protocols, such as non-repudiation protocols or fair-exchange protocols, the participating agents themselves cannot be trusted. We study the definition of the related security properties and the analysis of such protocols, and combine techniques from game theory and formal methods. Building on the results, we develop methods for the formal specification and verification of security protocols. The methods are implemented as an extension of a state-of-the-art security protocol verification tool. Case studies are performed by verifying existing protocols and developing new protocols.

The second thread in the project is related to the notion of attack trees that provide an informal, but very practical way to analyze the security of a complex system. When extending these with defenses, as to obtain attack–defense trees, it becomes possible to search for optimal defense strategies through the application of game theoretical concepts. In this project, we develop a methodology for analyzing attack–defense trees, and then to perform case studies to validate the methodology.

The project is executed in the context of the S-GAMES project. Here, we focus more on the practical issues in security analysis, modeling, and verification.

The GMASec project is a joint project of the SaToSS group and the ICR group.

Logic and Communication in Normative Multi-Agent Systems	
<b>Acronym</b>	LCNMAS
<b>Reference</b>	PDR-08-013
<b>Head of Project</b>	Prof. Dr. Leon van der Torre
<b>Funding</b>	FNR-AFR-Postdoc
<b>Running Time</b>	01/03/2009 – 28/02/2011

**Members:**

Xavier Parent

**Domain(s):**

Agent communication languages, normative multi-agent systems, deontic logic

**Description:**

The project's aim is to explore the use of deontic logic in the context of communication protocols in multi-agent systems, with a view to demonstrating the fruitfulness of the Normative Multi-Agent System (NorMAS) approach to Agent Communication Language (ACL). The project is constructed along two axes: whether the notion of commitment can be analyzed in terms of obligation; whether conversation rules or protocols can be described as soft rather than hard constraints.

Conviviality and User Behavior Analysis: Inventing profile discovery for e-conviviality	
<b>Acronym</b>	CUBA
<b>Reference</b>	TR-PHD-BFR07-036
<b>Head of Project</b>	Prof. Dr. Christoph SCHOMMER
<b>Funding</b>	FNR - AFR PhD (30K€)
<b>Running Time</b>	01/07/2007 – 30/06/2010

**Members:** Sascha KAUFMANN

**Domain(s):** Conviviality, User Behaviour Analysis, Profiling, Web Intelligence

**Description:**

Inventing profile discovery for e-conviviality: We want to motivate the idea of conviviality in web portals and argue that a convivial social being deeply depends on the implicit and explicit co-operation and collaboration of natural users inside a community. Our belief is that an individual conviviality can

benefit from the wisdom of the crowd, meaning that a continuously and dynamic understanding of the user's behaviour can heavily influences the individual well-being.

For this, we develop the system CUBA, which stands for "Conviviality and User Behaviour Analysis". The purpose of CUBA is to find novel ways to support users during their visits while discovering their interests. In this respect, CUBA comes up with certain recommendations and suggestions, which are partially based on a common behaviour of participants in general. To this end, concepts like time, space, and diverse user-based actions are taken into account.

Reliable and robust management for telecommunication network with optimization techniques	
<b>Acronym</b>	RRMTNOT
<b>Reference</b>	TR-PHD BFR07-105
<b>Head of Project</b>	Prof. Dr. Pascal Bouvry
<b>Funding</b>	FNR - AFR Ph.D.
<b>Running Time</b>	01/12/2008 – 30/11/2010

#### Members:

Julien Schleich

#### Domain(s):

mobile ad hoc network, virtual backbone, decentralized algorithm, global optimization

#### Partner(s):

University of Metz (Prof. Le Thi Hoai An)

#### Description:

Reliable and robust management for telecommunication network with optimization techniques

Trust Management for Ad-Hoc Networks	
<b>Acronym</b>	TMAHN
<b>Reference</b>	TR-PHD BFR05-037
<b>Head of Project</b>	Prof. Dr. Pascal Bouvry
<b>Funding</b>	FNR - AFR PhD
<b>Running Time</b>	01/02/2007 – 31/01/2011

**Members:**

Apivadee Piyatumrong

**Domain(s):**

Mobile Ad Hoc Networks, Virtual Backbone, Trust, Spanning Tree, Multi-Objective Optimization

**Partner(s):**

University of Le Havre (Prof. Dr. Frederic Guinand)  
King Mongkut's University of Technology Thonburi (Assoc. Prof. Kittichai Lavangnananda)

**Description:**

Within the framework of confident management (trust), the emerging characteristics of one of the new types of networks, Mobile Ad Hoc Network (a network which has high dynamic movement of participants and needs decentralized management system) will be studied. Indeed, the traditional management sciences of identification and of reputation do not adapt to a new generation of this self-organized networks. MANETs (mobile Ad Hoc Networks) nowadays benefit of a quite large literature. However, they are often restricted to a fully connected to a fully connected network operating on TCP-IP. We wished to have the opportunity to also address Delay Tolerant Networks (DTNs) that may be partitioned from time to time. Existing studies consider such partitions as a low layer concern similar to latency or as a high level concern by considering that a DTN consists of a set of separated structures that may latter on split or merge depending on the mobility and environment of the devices. Furthermore, the system should be emerged in distributed and mobile environments. Classial security mechanisms do not apply for such networks that need fully decentralized management schemes. This thesis proposes to explore new opportunities through the concept of reputation in dynamic environment.

<b>Grid-based Parallel Software(GPS) for predicting thermal conversion and fuel particles motion in combustion chamber</b>	
<b>Acronym</b>	GPSTCFPM
<b>Reference</b>	BFR07-141, TR-PDR BFR07-141
<b>Head of Project</b>	Prof. Dr. Pascal Bouvry
<b>Funding</b>	FNR - AFR PostDoc
<b>Running Time</b>	01/03/2009 – 28/02/2010

**Members:**

Dr. Grima Berhe, Prof. Dr. Pascal Bouvry, Prof. Dr. Ing Bernhard Peters

**Domain(s):**

Grid Computing, Parallel Algorithms, Dynamic Resource Allocation, Thermal Conversion, Solid-Waste Combustion, Thermo- and Fluid Dynamics

**Description:**

The increasing municipal population growth and living standard improvements in urban areas have brought a substantial increment of sold wastes year after year. For example, in the European cities, the household waste, which constitutes two-third of the municipal solid waste (MSW), is expected to increase by 22% over the period 1995-2010. This has a great impact on the ambient environment, people's health, and quality of life. Consequently, the disposal of the municipal solid wastes has become a serious problem with which urban cities are currently confronted. There are two principal methods of municipal solid waste disposal used in the world today: incineration/combustion and sanitary landfill. In this project the focus is on the incineration/combustion method.

This project aims to study the behavior of the combustion process by employing computational tools in order to study better way of designing the combustion chambers and to propose efficient and effective way of chamber operation. The objective of this project is to propose a grid-based parallel software to predict both thermal conversion and motion of a large number of fuel particles in a combustion chamber. This will lead to a significant reduction in CPU-time, because several processors will share the task of computation.

<b>Combinatorial optimization on P2P systems and computational grids</b>	
<b>Acronym</b>	COPSCG
<b>Reference</b>	TR-PHD BFR07-079
<b>Head of Project</b>	Prof. Dr. Pascal Bouvry
<b>Funding</b>	FNR - AFR PhD
<b>Running Time</b>	01/09/2007 – 31/10/2010

**Members:**

Malika Mehdi

**Domain(s):**

Combinatorial Optimization, Grid Computing

**Partner(s):**

University of Lille (Prof. El-Ghazali Talbi, Prof. Nouredine Melab)  
 University of Luxembourg (Prfo. Raymond Bisdorff)

#### Description:

The objectives of this PhD are the design of efficient hybridization schemes combining different kinds of optimization methods (exact methods and heuristics) and the design of a framework for large scale parallel optimization on computational grids to solve large benchmarks of permutation problems.

Robust Scheduling on Desktop Grids	
Acronym	RSDG
Reference	PDR-08-010
Head of Project	Prof. Dr. Pascal Bouvry
Funding	FNR - AFR PostDoc
Running Time	01/09/2009 – 31/08/2011

#### Members:

Dr. Johnatan E. Pecero Sanchez

#### Domain(s):

Computer Science, Information Science, Grid Computing, Scheduling, Optimization

#### Description:

"Desktop Grids" are distributed platforms, based on volunteer computing, that interconnects unused resources for computing purpose. In such platforms new nodes may go up and down that new generation of schedulers should bring the required level of reliability and robustness. One important point for a more effective use of such systems is the management and optimization of resources, particularly scheduling. It consists of allocating the tasks of a parallel program to processors on the platform and to determine at what time the tasks will start their execution. Desktop Grids are characterized by many new features that should be taken into account for optimizing the performance. The handled data are subject to uncertainties and/or disturbances, and thus, it is mostly impossible to have a precise prediction of the input parameters of the scheduling problem.

Efficient data transfer in vehicle2vehicle wireless communication networks, using distributed algorithms based on collective intelligence such as ant colonies.	
<b>Acronym</b>	WiCaN
<b>Reference</b>	PDR-09-042
<b>Head of Project</b>	Prof. Dr. Pascal Bouvry
<b>Funding</b>	FNR - AFR PostDoc
<b>Running Time</b>	15/10/2009 – 14/10/2011

**Members:**

Dr. Yoann Pigné

**Domain(s):**

VANET, Distributed Computing, Routing Algorithms, Collective Intelligence, Ant-Based Algorithms, Multiobjective Optimization

**Description:**

Nowadays, safety efforts are more and more put into communications to prevent accidents rather than into safety devices and equipments (airbags, seat belts) to reduce the seriousness of accidents. New technology trends give us wireless possibilities for mobile networking. These technologies can help in designing communication and warning systems needed with the help of vehicle-to-vehicle (V2V) communication. If we consider the communication network as a dynamic graph, routing in such a network can be reduced to finding and maintaining shortest paths in this graph, using only local information. We already successfully proposed a multiobjective algorithm based on ant colonies to find and maintain routes in a MANET. The proposal here is to apply this previous work to the special constraints of V2V networks and propose efficient data transmission algorithms with the help of artificial ants. Those methods will be tested and validated in realistic simulations, against other state of the art methods.

Risk Prediction Framework for Interdependent Systems using Graph Theory	
<b>Acronym</b>	TIGRIS
<b>Reference</b>	PHD-09-103
<b>Head of Project</b>	Prof. Dr. Pascal Bouvry
<b>Funding</b>	FNR - AFR PhD
<b>Running Time</b>	15/10/2009 – 15/10/2012

**Members:**

Thomas Schaberreiter

**Domain(s):**

critical infrastructures, security modelling, graph modelling

**Partner(s):**

CRP Henri Tudor (Dr. Djamel Khadraoui)  
University of Oulu (Prof. Juha Rönning)

**Description:**

Critical infrastructure protection is an up-to-date topic. Critical infrastructure is usually composed of interdependent systems that rely on each other in order to function correctly or provide adequate security. The interdependencies of the systems are usually quite complex to understand and therefore modelling of the infrastructure and its interdependencies can be helpful in determining the security requirements.

During this work a model of interdependent systems based on graph theory will be proposed that aims to model the security attributes of interdependent systems. Adequate ways to model the security properties of infrastructure as well as of the interdependencies will have to be found in order to achieve a close-to-reality model. Furthermore, machine learning tools will have to be developed in order to process the graph and allow real-time simulations.

Multimedia Sensor Networks (PhD thesis)	
<b>Acronym</b>	MSN
<b>Reference</b>	N/A
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	FNR and EPT (108K€)
<b>Running Time</b>	2010 – 2013

**Members:**

Thomas Engel, Stefan Hommes

**Domain(s):**

Wireless Sensor Networks

**Partner(s):**

EPT Luxembourg

**Description:**

N/A

Energy Optimization and Monitoring in Wireless Mesh Sensor Networks(PhD thesis)	
<b>Acronym</b>	WinSEOM
<b>Reference</b>	N/A
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	FNR and Ville de Luxembourg (108K€)
<b>Running Time</b>	2010 – 2013

**Members:**

Thomas Engel, David Fotue

**Domain(s):**

Wireless Communications

**Partner(s):**

Ville de Luxembourg

**Description:**

N/A

Wireless outdoor access. Managed and Community Networks (PhD thesis)	
<b>Acronym</b>	WOA
<b>Reference</b>	N/A
<b>Head of Project</b>	Prof. Dr. Thomas Engel
<b>Funding</b>	FNR and Telindus (116K€)
<b>Running Time</b>	2010 – 2013

**Members:**

Thomas Engel, Yves Neisius

**Domain(s):**

Wireless Communications

**Partner(s):**

Telindus

**Description:**

N/A

### 2.2.2 Workshop & Conferences (FNR Accompanying Measures)

Science Festival 2009 - "Cryptography for Kids"	
<b>Acronym</b>	CRKI
<b>Reference</b>	F1C-CSC-PFN-09CRKI
<b>Head of Project</b>	Prof. Dr. Alex Biryukov
<b>Funding</b>	FNR-Science Festival, 1800€
<b>Running Time</b>	12/11/2009 – 15/11/2009

#### Members:

Jean-Claude Asselborn, David Galindo, Jean-François Gallais Johann Großschädl, Dmitry Khovratovich, Ilya Kizhvatov, André Stemper, Ralf-Philipp Weinmann

#### Domain(s):

Cryptography for Kids, Science Festival

#### Description:

This was a four day activity for middle and high school children and their parents. The goal was to introduce children to cryptography and information security in attractive and fun way.

ESC 2010 - Echternach Symmetric Cryptography Workshop	
<b>Acronym</b>	ESC 2010
<b>Reference</b>	F1C-CSC-PMA-090314
<b>Head of Project</b>	Prof. Dr. Alex Biryukov
<b>Funding</b>	FNR-AM, 8000€
<b>Running Time</b>	11/01/2010 - 15/01/2010

#### Members:

Ralf-Philipp Weinmann

#### Domain(s):

Symmetric Cryptography

**Description:**

This was a five-day Dagstuhl-like seminar that took place in January 2010. All the organization was done in 2009.

Second International Conference on e-Voting and Identity	
<b>Acronym</b>	VOTE-ID 2009
<b>Reference</b>	F1C-CSC-PMA-090303
<b>Head of Project</b>	Prof. Dr. Peter Ryan
<b>Funding</b>	FNR-AM, 5240€
<b>Running Time</b>	07/09/2009 – 08/09/2009

**Members:**

Hugo Jonker, Baptiste Alcalde

**Domain(s):**

Electronic Voting

**Description:**

Electronic voting is a very active research area covering a broad range of issues, from computer security and cryptographic issues to human psychology and legal issues. The aim of VoteID 2009 was to bring together researchers and practitioners from academia, industry and governmental institutions, working on all aspects of e-voting systems, ranging from security, cryptography, usability, availability, software engineering issues to legal and socio-logical issues.

Formal Methods Week	
<b>Acronym</b>	FATES and FAST
<b>Reference</b>	FNR/09/AM2a/144
<b>Head of Project</b>	Baptiste Alcalde
<b>Funding</b>	FNR-AM2a, 2000€
<b>Running Time</b>	02/11/2009–06/11/2009

**Description:**

Participation in conference, Eindhoven, The Netherlands

Computer Security Foundations Symposium and Workshop on Formal and Computational Cryptography	
<b>Acronym</b>	CSF and FCC
<b>Reference</b>	FNR/09/AM2a/80
<b>Head of Project</b>	Sasa Radomirovic
<b>Funding</b>	FNR-AM2a, 697,77€
<b>Running Time</b>	08/07/2009–12/07/2009

**Description:**

Participation in symposium and workshop, Port Jefferson, NY, USA

International Conference on Formal Engineering Methods	
<b>Acronym</b>	ICFEM
<b>Reference</b>	FNR/09/AM2a/182
<b>Head of Project</b>	Ton van Deursen
<b>Funding</b>	FNR-AM2a, 930,72€
<b>Running Time</b>	08/12/2009–11/12/2009

**Description:**

Participation in conference, Rio de Janeiro, Brazil

9th International School on Foundations of Security Analysis and Design	
<b>Acronym</b>	FOSAD
<b>Reference</b>	FNR/09/AM2b/35
<b>Head of Project</b>	Barbara Kordy
<b>Funding</b>	FNR-AM2a, 1638,36€
<b>Running Time</b>	30/08/2009–04/09/2009

**Description:**

Participation in summer school, University Residential Center of Bertinoro, Italy

Logical Systems for Access Control Policies	
<b>Acronym</b>	LSACP
<b>Reference</b>	FNR/08/AM2c/38
<b>Head of Project</b>	Prof. Leon van der Torre
<b>Funding</b>	FNR AM2C
<b>Running Time</b>	01/01/2009 – 28/02/2010

**Members:** Guido Boella

**Domain(s):** access control policies, security, modal logic, epistemic logic, privacy, norms

**Partner(s):** Dipartimento di Informatica – Università di Torino

**Description:** This project concerns the 2 months visiting professorship of Prof. Guido Boella on the topic of building logical system to formalize access control policies.



## References

---

- [KM08] Pierre Kelsen and Qin Ma. A lightweight approach for defining the formal semantics of a modeling language. In *ACM/IEEE 11th International Conference on Model Driven Engineering Languages and Systems (MODELS 2008)*, volume 5301. 5301 of *Lecture Notes in Computer Science*, pages 5301 – 690. Springer Berlin / Heidelberg, 2008.
- [BMR08] Raymond Bisdorff, Patrick Meyer, and Marc Roubens. Rubis: a bipolar-valued outranking method for the choice problem. *4OR, A Quarterly Journal of Operations Research*, 6(2):143–165, 2008.
- [SE09f] Michael Stieghahn and Thomas Engel. Law-aware access control for international financial environments. In *MobiDE '09: Proceedings of the Eighth ACM International Workshop on Data Engineering for Wireless and Mobile Access*, pages 33–40. ACM New York, NY, USA, 2009.
- [SE09g] Michael Stieghahn and Thomas Engel. Using xacml for law-aware access control. In *3rd. International Workshop on Juris-informatics (JURISIN 2009)*, 2009.
- [WWSE09] Cynthia Wagner, Gerard Wagener, Radu State, and Thomas Engel. Malware analysis with graph kernels and support vector machines. In *4th International Conference on Malicious*

*and Unwanted Software (Malware 2009)*, pages 63–68. IEEE, 2009.