ERCIM “Alain Bensoussan” Fellowship Scientific Report

Fellow: **Sendroiu Elena**
Visited Location : NTNU
Duration of Visit: 02/03/09 -- 01/03/10

I - Scientific activity

I have been working in team doing research in the area of software security and safety of critical software. In particular I am focusing on software verification and validation, test methods, and testing tools for safety and security critical systems. Based on my previous special studies (i.e. faculty + master + PhD) in denotational semantics, I am working with program verification based on denotational semantics. Based on new semantics approach theory, my goal is to improve current methods and tools for verification and validation.
Since a categorical semantics of mathematical ontologies is useful in the problem of ontology composition, I employed category theory to formalize scientific ontologies to modeling huge scientific metadata. And, I built special tools for optimal computation of scientific metadata and automatic verification tools. In particular, I provided procedures for constructing ontology limits and colimits. I presented some correspondences between categorical concepts that can be used in automatic verification. Moreover, I formalized secure ontology structures by adding a security component that includes access control information.
It is well known that improving the security of computer systems, networks, and applications has become an important and difficult problem. Attack detection is complex and time-consuming for system administrators. Sheaf theory can be a solution to improve the security of computer systems. So, I proposed a way to use sheaf theory in security of systems. Since it requires an efficient way of constructing sheaves, I focused on an algorithmic procedure to achieve this. More precisely, for my computational approach I introduced various finiteness and/or minimality conditions on a site and its sieves. And in that special case, I gave an alternative description of the associated sheaf functor, more adapted for implementation on a computer system. My proofs are more adapted in automatic verification, construction and implementation of algorithms that efficiently generate and handle sheaves on well structured sites. My sheaf construction consists then in first choosing an arbitrary finite diagram in the site and defining a presheaf via the colimit of the corresponding diagram of representable functors. And I did show that by applying my sheaf construction to that presheaf yields a sheaf as expected.
Moreover, I have written a new secret sharing scheme by using sheaves. Here are my new results:
– My secret sharing scheme gives us the possibility to give shares to possible adversaries but restrictions in reconstructing of the secret. In fact, I am using the expression ”possible adversaries” since a possible adversary may be an unknown new player. This is a kind of quarantine. And my secret sharing scheme has tools to check/verify the honesty of a player.
– We may verify the integrity of any share. And this is a kind of intrusion detection. The ”integrity of the share” means checking if the share of a player (or a share communicated by a player) is indeed the share distributed by dealer.
– A player can re-share his share as a dealer and the new players are integrated in the main sharing system as all players. So the scheme can modified by individuals without reconstructing the secret and then sharing the secret again. In the re-sharing process the dealer may be substituted as player in order to verify the honesty of the new distributor of shares. The ”verifiable secret sharing” means checking if the distributor gives a correct share.

II- Publication(s) during your fellowship

E. Sendroiu. *Sheaf Construction*, to appear in AIP Conference Proceedings of ICCMSE 2009, Rhodes, Greece

Abstract. In this paper we consider the most general notion of a sheaf, as a functor on a site, which is a category equipped with a Grothendieck topology. In [4], we have introduced a notion in sheaf theory, family for matching, to construct an optimal validation algorithm of sheaves. By using this notion, in this paper, we give a new associated sheaf functor for a certain class of sites called well structured sites. We show that there are many interesting examples, both finite and infinite, of such sites. Using this, we can construct verification tools and an algorithm that efficiently generates sheaves on well structured sites.

E. Sendroiu, *Categorical Ontology Structures Equipped with Security Tools*, Research Report of my visit to the lab. RAL, STFC, UK, may, 2009

Abstract. We formalize scientific metadata in category theory that is a well founded mathematics framework. So, we define the category of ontologies and in particular the category of studies by using scientific metadata developed by the STFC. By introducing and formalizing a security substructure, we define then the category of secure ontologies. We are applying category theory since the categorical framework gives us the possibility to construct computation tools for huge scientific metadata. So, we can build special tools for optimal computation of scientific metadata and automatic verification tools. In particular, we provide procedures for constructing ontology limits and colimits. We present some correspondences between categorical concepts that can be used in automatic verification.

Drafts that will be submitted:

E. Sendroiu, *Sheaf Construction (full paper)*

Abstract. In this paper we consider the most general notion of a sheaf, as a functor on a site, which is a category equipped with a Grothendieck topology. In [5], we have introduced a notion in sheaf theory, family for matching, in order to simplify the sheaf definition in well structured sites. This has given us the possibility to construct an optimal validation algorithm of sheaves. By using this notion, in this paper, we give a new associated sheaf functor for a certain class of sites called well structured sites. We show that there are many interesting examples, both finite and infinite, of such sites. Using this, we construct verification tools and an algorithm that efficiently generates sheaves on well structured sites. Finally, from the proof of lemma 10 we describe a computation algorithm of almagamations for the sheaf authentication method for system security.

E. Sendroiu, *Computing on Categorical Ontology Structures*

Abstract. We formalize ontologies in category theory that is a well founded mathematics framework. By introducing and formalizing a security substructure, we define then the category of secure ontologies. In fact, the categorical framework gives us the possibility to construct computation tools for huge scientific metadata. So, we can build special tools for optimal computation of scientific metadata and automatic verification tools. In particular, we provide procedures for constructing ontology limits and colimits. We present some correspondences between categorical concepts that can be used in automatic verification.

E. Sendroiu, *Sheaf Secret Sharing Scheme*

Abstract. In this paper we provide a new secret sharing scheme by using sheaves. This secret sharing scheme gives us the possibility to give shares to possible adversaries but restrictions in reconstructing of the secret. A player can re-share his share as a dealer and the new players are integrated in the main sharing system as all players. In the re-sharing process the dealer may be substituted as player in order to verify the honesty of the new distributor of shares.

*Moreover, I am reviewing articles for the journal **Applied Mathematics and Computation**.*

III -Attended Seminars, Workshops, and Conferences

I have participated at:

- NTNU Information Security Research Meeting - a monthly (first Wednesday of the month) colloquium of people doing information security research PhD-students, postdocs and visitors affiliated with Dep. Telematics including those at Q2S centre, and at cooperating Departments where Telematics professors are co-supervisors.
- May 12, 2009, A. Arenas, *An Overview of XtreemOS: A Grid-based Operating System*, RAL, STFC, Didcot, Oxfordshire, UK
- June 16-18, 2009, visit at NTNU of Prof Jean-Charles Faugère, Research Director at INRIA
    1. Lecture 1 (Topic - Efficient Computation of Gröbner bases -- (I))
    2. Lecture 2 (Topic - Application of Gröbner bases in Multivariate Cryptology

  Discussion on future cooperation (work on Public Keyalgorithms, hash functions, hardware accelerators for Groebner bases).
    3. Lecture 3 (Topic - Efficient Computation of Gröbner bases -- (II))
    4. Lecture 4 (Topic - Algebraic Cryptanlysis), Meeting at Q2S, Description of a technical characteristics of a cluster where Magma and Groebner bases are used,
    5. Lecture 5 (Topic - Overview of Quasi-Groups in Cryptology), Technical Discussions
- Oct. 27, 2009, NTNU Itovation, http://itovation.wordpress.com/
- Nov. 5, 2009, NTNU *Free industrial Seminar on Open Source*
- Nov. 18, 2009, NSEP Seminar, *Location Trajectory System*
- Dec. 3, 2009, NOKIA QT SEMINAR
- Jan. 15, 2010, Category Seminar, University of Paris 7
- Feb. 17, 2010, NSEP Seminar, Sampling clinical reality
- Feb. 19, 2010, SIG CRYPTOLOGY E-voting workshop

I have presented at:

- May 11 - *22, 2009, RAL, STFC, Didcot, Oxfordshire, UK, Ontology Structure* and *Category theory* (an intuitive introduction)
- June 3, 2009, NTNU Information Security Research Meeting, talk, *Categorical Ontology Structures Equipped with Security Tools* and *Category theory* (an intuitive introduction)
- Oct. 4, 2009, *Sheaf Construction*, Seventh International Conference of Computational Methods in Sciences and Engineering **(**ICCMSE 2009), Rhodes, Greece, http://www.iccmse.org/docs/Program ICCMSE 2009.pdf , page 54
- Nov. 4, 2009, NTNU Information Security Research Meeting, talk, *Sheaf Construction*

I was chair of SESSION: *Computational Methods VIII*, ICCMSE 2009,
Rhodes, Greece, http://www.iccmse.org/docs/Program ICCMSE 2009.pdf , page 54

IV – Research Exchange Programme (12 month scheme)

Scientific contact: ***Alvaro Arenas***, email: "Arenas, AE (Alvaro)" alvaro.arenas@stfc.ac.uk
May 10 - 26, *RAL, STFC, Didcot, Oxfordshire, UK*
I analyzed 3 versions of scientific metadata described by STFC and I formalized it. I defined these ontologies in a well founded mathematics framework. I applied category theory in order to construct computation tools for huge scientific metadata. So, I built special tools for optimal computation of scientific metadata and automatic verification tools. Finally, I finished formalizing the security substructure. STFC asked me to write a research report.

Scientific contact: ***Anne Canteaut***, email: "Anne Canteaut" Anne.Canteaut@inria.fr
January 14 - 31, SECRET - Security, Cryptology and Transmissions team, INRIA Paris-Rocquencourt, France
I have studied the paper: *Merkle-Damgard Revisited: how to Construct a Hash Function* by Jean-Sebastien Coron, Yevgeniy Dodis, Cecile Malinaud, and Prashant Puniya.
In addition, I have corrected several minor typos. Now, I am writing a paper that summarizes my suggestions to improve this topic.