

A l'occasion de la tenue des

Assises Nationales de la Recherche – Novembre 2007

L'Association Tunisienne de la Sécurité Numérique

Organise

Un workshop International

sur le thème

Méthodes Formelles pour la Sécurité des Systèmes et Réseaux

Mercredi 24 Octobre 2007 à 14 h 30

Amphithéâtre de l'ISET'Com

Cité Technologique des Communications



Ce workshop est également sponsorisé par le projet DGRSRT/INRIA 06/104

Programme

14h30-15h00 : Ouverture officielle

- Allocution de Bienvenue par **M. Adel BOUHOULA**, Président de l'Association Tunisienne de la Sécurité Numérique.
- Allocution d'ouverture par **M. Jmaiel BEN BRAHIM**, Président de l'Université du 7 Novembre à Carthage.

Président de séance : M. Naceur AMMAR, Directeur de l'Ecole Supérieure des Communications de Tunis.

15h00-15h40 : « Verifying Regular Trace Properties of Security Protocols with Explicit Destructors and Implicit Induction ».

Par **M. Florent JACQUEMARD**, Chargé de Recherche à l'INRIA Futurs.

15h40-16h20 : « Méthodes Formelles et Certifications Sécuritaires dans le Contexte de la Carte à Puce ».

Par **M. Olivier LY**, Maître de Conférences à l'Université Bordeaux 1.

16h20-17h00 : « Algorithmique des systèmes distribués ».

Par **M. Mohamed MOSBAH**, Professeur à l'Université Bordeaux 1.

17h00-17h40 : « Quantum and Parallel Computing via Fuzzy Logic ».

Par **M. Skander HANNACHI**, Research Associate at Tokyo Institute of Technology.

17h40-18h30 : Cocktail.

Association Tunisienne de la Sécurité Numérique

L'Association Tunisienne de la Sécurité Numérique, de création récente, s'est fixée un programme ambitieux devant permettre de réunir le plus grand nombre de compétences tunisiennes dans ce domaine de technologie de pointe, facilitant ainsi l'instauration d'une synergie fructueuse entre les différents facteurs d'incitation à l'innovation technologique.

Nos principaux objectifs sont :

- Contribution au développement de la recherche et de l'innovation scientifique et technologique dans le domaine de la sécurité numérique.
- Promotion des réalisations nationales et internationales dans le domaine de la sécurité numérique.
- Contribution à la diffusion de la culture numérique, essentiellement auprès des jeunes, et à la sensibilisation de l'importance de la sécurité numérique et ceci, à travers l'organisation de séminaires et d'expositions sur ce thème.

منتزه السعادة بالمرسي - 2070 المرسي صفصاف - تونس

☎: +216 98 437 437 - ☎: +216 71 856 829

Email: atsn@planet.tn

☎ 17001000000077696024

« Verifying Regular Trace Properties of Security Protocols with Explicit Destructors and Implicit Induction »

We present a procedure for the verification of cryptographic protocols based on a new method for automatic implicit induction theorem proving for specifications made of conditional and constrained rewrite rules.

The method handles axioms between constructor terms which are used to introduce explicit destructor symbols for the specification of cryptographic operators. Moreover, it can deal with non-confluent rewrite systems. This is required in the context of the verification of security protocols because of the non-deterministic behavior of attackers.

Our induction method makes an intensive use of constrained tree grammars, which are used in proofs both as induction schemes and as oracles for checking validity and redundancy criteria by reduction to an emptiness problem.

The grammars make possible the development of a generic framework for the specification and verification of protocols, where the specifications can be parametrized with (possibly infinite) regular sets of user names or attacker's initial knowledge and complex security properties can be expressed, referring to some fixed regular sets of bad traces representing potential vulnerabilities.

We present some case studies giving very promising results, for the detection of attacks (our procedure is complete for refutation), and also for the validation of protocols.

« Méthodes Formelles et Certifications Sécritaires Dans le Contexte de la Carte à Puce »

Les travaux présentés concernent la mise en œuvre de techniques formelles dans le contexte de la certification de produits liés à la sécurité, en particulier des cartes à microprocesseurs.

J'évoquerai la méthodologie préconisée par les normes de certification, en particulier les critères communs, et son articulation avec les méthodes formelles. Je décrirai l'exemple de la propriété de confidentialité et de son traitement dans l'architecture JavaCard. Enfin, j'aborderai des directions prospectives concernant les attaques par canaux cachés.

« Algorithmique des systèmes distribués »

L'informatique a été marquée ces dernières années par le développement d'une information de plus en plus complexe et massivement distribuée sur les réseaux (comme Internet). Les progrès technologiques des postes de travail et des réseaux, notamment à haut débit, et les efforts de standardisation des services d'interopérabilité (comme CORBA) ont permis d'envisager de réelles applications distribuées. Ceci continue de stimuler une intense activité de recherche autour des systèmes et des applications distribués, et de leur fondement que constitue l'algorithmique distribuée. Cet exposé présente un modèle formel fondé sur les réécritures de graphes pour modéliser les calculs distribués d'un système, ainsi que les preuves de ces calculs (sûreté, vivacité, etc). Un environnement logiciel de visualisation et d'animation de calcul distribué sera également présenté.

« Quantum and Parallel Computing via Fuzzy Logic »

The possibility of using fuzzy logic for emulating quantum and parallel computing is examined. Mathematical frameworks for computing with fuzzy quantum bits and fuzzy bits are presented, as well as basic logic gates and operations, and hardware implementation is briefly discussed. Some basic algorithms are formulated, and advantages over conventional quantum computing and other parallel quantum computing methods are discussed. First, the possibility of emulating QC with fuzzy logic is examined. Theoretical quantum logic based automata and quantum logic pushdown automata are presented using the fuzzy set formulation of quantum logic. Using geometrical analogies and a suitable transformation, qubits are modeled as pairs of fuzzy membership functions evolving on the unit square and basic one qubit gates are modeled as transformations on this unit square. These gates can be easily implemented using dedicated fuzzy analogue hardware. A fuzzy implementation of the one bit and two bit Deutsch-Jozsa algorithm is proposed. Next, the possibility of using fuzzy logic for performing parallel computation (independent of quantum computing) is introduced. An analogy is drawn between non-deterministic models of computing and fuzzy computing, and practical implementation of fuzzy computing by encoding fuzzy sets into strings of fuzzy bits is proposed. The possibility of speeding up computations using oracle machines based on fuzzy logic is examined, and a fuzzy search algorithm is proposed which, under certain conditions is exponentially faster than both classical and quantum algorithms. Also the rapid solution to Deutsch's problem using Lukasiewicz fuzzy logic is presented. Finally, the proposed two dimensional model of fuzzy qubits is used for the implementation of quantum associative memory (QAM). The equivalent of the Feynman gate for fuzzy qubits is proposed, the fuzzy C-not, which leads to the possibility of emulating previously proposed quantum learning and retrieval algorithms for quantum associative memory.