

**MS Theses by Dr. M. Ufuk Çağlayan**  
**29 May 2011**

**1. Extracting Trust Information from Security Policies**

Trust based systems are complementary solutions to existing traditional security systems in computer science. Therefore, trust is a significant topic of the security research. It has been recognized that the computation of trust of security systems in dynamic environments is a complex task. The computation of trust necessitates trust models that reflect all properties of systems precisely. Moreover, trust computations related to the security systems of services necessitate information that meets needs of each entity. Obtaining such information is a challenging issue for entities. Specifically, extracting trust information from security policies based on needs of a specific person, entity, in an automated way is an important problem. Security policies of interacting peers, such as entity-service and entity-entity interactions, have to be modeled according to needs of a specific interacting entity. Then, trust information has to be extracted by considering this model. An MS student may propose and apply such kind of model for specific security policies in a particular context. For instance, security policies related to access control may be used to extract trust information. More specifically, the security policies may be on firewalls of two communicating personal computers or mobile devices. Further analyses may be done on security policies of companies. References will later be provided to the student.

**Thesis co-supervisor: Şerif Bahtiyar**

**2. An Efficient Enforcement Architecture for Location and Mobility Related Security Policies**

The student will design and implement an efficient enforcement architecture for location and mobility related security policies. Multi-domain issues will also be covered by the security policy. The work will be based on the recently proposed FPM-RBAC model (Formal Policy Model for Mobility with Role Based Access Control). FPM-RBAC supports the specification of mobility and location constraints, role hierarchy mapping, inter-domain services, inter-domain access rights and separation of duty. The enforcement architecture will include a prototype Policy Decision Point (PDP) and Policy Enforcement Point (PEP) for FPM-RBAC policies. The student will be provided with XML schemas related to the FPM-RBAC security policy model. The software will be implemented in Java and fully documented with UML v2. All data structures will be designed using XML and XML schemas will be presented. References will later be provided to the student.

**Thesis Co-supervisor: Devrim Ünal**

**3. Software Design Verification using UML and OCL**

Software design, development and maintenance cost is always one of the top concerns of the software industry. Software companies are continuously looking for new areas where they can improve on the costs. One simple way to have a significant reduction on the cost is to better analyse and design the system such that number of errors and flaws will be less after the software is on the shelf. Nowadays, UML and OCL are the defacto standards for the software industry. Therefore, industry will directly benefit from any improvement on analysis and design using UML and OCL. In this theses, student will be responsible to define a methodology to model check software design models created using UML and OCL. This methodology has to contain a proper way to convert the software design (both UML+OCL) into PROMELA and execute model checking using SPIN Model Checker.

**Thesis Co-supervisor: Engin Deveci**

**4. Performance Evaluation of the SPIN Model Checker**

The SPIN Model Checker is an award-winner verification tool to analyze functional properties of communication protocols, concurrent systems and systems alike. Model Checkers basically analyze

the state space of a model to see whether the model satisfies certain properties or not. This process is completely automated but quite resource-hungry. Analysis of a complex model can easily lead to a state space explosion, which is a common problem for those using automated tools such as model checkers. Therefore, a modeler, who is actually a human-being using the model checker, should consider the complexity of his/her model during the modeling phase. In this thesis, we would like to see the verification performance of the SPIN Model Checker under different system and workload conditions. SPIN supports multi-core as well as multi-computer processing. The cluster environment in our department can be used to run the multi-computer experiments. See [5] and [6] for the performance analysis of SPIN during the development of its multi-computer support.

**Keywords:** Model Checking, the SPIN Model Checker, Verification Performance, Performance Analysis, Distributed-memory Model Checking, Parallel Processing, Parallel Verification.

**References:**

- [1] G. Holzmann, the SPIN Model Checker: Primer and Reference Manual, Addison Wesley, 2003.
- [2] M. Ben-Ari, Principles of the SPIN Model Checker, Springer, 2008.
- [3] SPIN site, <http://spinroot.com>, SPIN.
- [4] Swarm Verification Script Generator for SPIN, <http://spinroot.com/swarm/>.
- [5] Gerard Holzmann, Rajeev Joshi, and Alex Groce. "Tackling Large Verification Problems with the Swarm Tool." In *SPIN Workshop on Model Checking of Software (SPIN)*, pages 134--143, Los Angeles, California, August 2008
- [6] Gerard Holzmann, Rajeev Joshi, and Alex Groce. "Swarm Verification Techniques" *IEEE Transactions on Software Engineering*, PP Issue:99, December 2010.

**Thesis Co-supervisor: A. Burak Gürdağ**

## 5. Designing a Secure and Peer-to-Peer version of Session Initiation Protocol (SIP)

SIP is a signalling protocol mainly developed to standardize the session establishment procedure in voice over IP (VoIP) application. It is by design a server-centric protocol in which end points use certain network entities to join the VOIP network and to make calls to each other. However, it is also possible to take the servers out of the picture and make the endpoints connect to each other in a peer-to-peer (p2p) manner. For example, Skype is a good example of a p2p VoIP system although it is not entirely p2p and not a SIP-based system. In this thesis, we would like to explore the security aspects of P2P SIP as defined in [5] and to design a (more) secure version of this protocol. Note that P2P SIP is not a standardized protocol and this will be quite a challenging and also a pioneering work.

**Keywords:** P2P, SIP, VOIP, ad hoc operation, Security.

**References:**

- [1] RFC 3261, Session Initiation Protocol. <http://www.faqs.org/rfcs/rfc3261.html>
- [2] Tech Invite, a SIP Information Portal, <http://www.tech-invite.com>
- [3] Peer-to-Peer SIP, Wikipedia Page, [http://en.wikipedia.org/wiki/Peer-to-peer\\_SIP](http://en.wikipedia.org/wiki/Peer-to-peer_SIP)
- [4] IETF P2PSIP Workgroup Page, <http://tools.ietf.org/wg/p2psip/>
- [5] RELOAD, IETF Draft, <http://tools.ietf.org/wg/p2psip/draft-ietf-p2psip-base/>
- [6] SIP Security, <http://www.voip-info.org/wiki/view/SIP+security>

**Thesis Co-supervisor: A. Burak Gürdağ**