Devrim Ünal

Thesis Supervisor: Prof. Dr. Mehmet Ufuk Çağlayan

FPFM: A Formal Specification and Verification Framework for Security Policies in Multi-Domain Mobile Networks

In his Ph.D. thesis, Dr. Ünal has proposed a security policy specification and verification framework named FPFM (Formal Policy Framework for Mobility). This framework targets multi-domain mobile networks. The proposed framework presents novel findings in the areas of location and mobility based security, multi-domain security and formal verification of security models and security policies, including information flow analysis, model checking of security policies based on process calculus and inductive theorem proving of security policies. A formal role-based access control model named FPM-RBAC has been proposed for the specification of security policies. The security policy model represents novelty regarding location and mobility constraints, mapping of role hierarchies, specification of multi-domain security policies and separation of duty constraints. In order to utilize FPM-RBAC security policy model within a network by applications and software services, an XML-based security policy langugage named XFPM-RBAC has also been proposed. Multi-domain security policies including location and mobility constraints may be specified using this language. Formal specifications corresponding to XML-based security policy specifications are generated automatically. In this way, system administrators and software developers are abstracted away from complexities of process calculus and logic statements while benefiting from the advantages of using a formal security model, such as formal verification.

Formal verification of security policies are supported through model checking and theorem proving. A model checking algorithm based on Ambient Logic has been proposed, for the formal verification of Ambient Calculus based specifications for mobile systems. The proposed model checking algorithm has lower complexity compared to similar algorithms in the literature and has the additional advantage that an implementation is provided. The proposed algorithm is capable of spatio-temporal model checking of mobile network configurations with respect to location and mobility constraints. Information flow analysis, based on allowed flows by a security policy, is also possible by using the same approach. The NuSMV model checker has been utilized for temporal model checking whereas spatial model checking is achieved through the Ambient Calculus Model checker, proposed and implemented within the thesis. With regards to theorem proving, the approach is based on the Calculus of Inductive Constructions (CIC), which is implemented by the Coq proof assistant. Conflicts within multiple security policies are detected and resolved through the theorem prover. Formal specifications have been developed for the purpose of verification of role based access control policies. The proposed approach for theorem proving presents novelty in the area of verification of multiple role-based access control policies.

PUBLICATIONS

Journal Publications

1. Ünal, D., Çaglayan, M. U., Spatio-Temporal Model Checking of Location and Mobility Related Security Policy Specifications, Turk. J. Electrical Engineering and Computer Sciences, 2011, In Press.

2. Ünal, D., Çaglayan, M. U., XFPM-RBAC: XML Based Specification Language for Security Policies in Multi-Domain Mobile Networks, Wiley Security and Communication Networks, 2011, In Press.
3. Ünal, D., Çaglayan, M. U., FPM-RBAC: A Formal Role-Based Access Control Model for Security Policies in Multi-Domain Mobile Networks, Elsevier Computer Networks, 2011, Under Review.

Conference and Symposium Papers

1. Ünal, D., Akar, O. and Çağlayan, M. U., *Model Checking of Location and Mobility Related Security Policy Specifications in Ambient Calculus*, in: Kotenko, I. & Skormin, V. (Eds.) Computer Network Security, MMM-ACNS International Conference, St.Petersburg, Russia, *2010*, LNCS 6258, 155-168
2. Ünal, D., Çağlayan, M. U., *Formal Specification of Security Policies in Multi-Domain Mobile Networks, Akademik Bilişim, Urfa, 2009*
3. Ünal, D., Çağlayan, M. U., *Çok Etki Alanlı Ağlar için Formel Güvenlik Politikası Betimleme, Akademik Bilişim, Çanakkale, 2008*
4. Ünal, D., Çağlayan, M. U., Theorem proving for Modeling and Conflict Checking of Authorization Policies, Proc. International Symposium on Computer Networks, 2006

Defense Jury Members

Prof. Mehmet Ufuk Çağlayan	Bogazici University
Assoc. Prof. Tuna Tuğcu	Bogazici University
Assoc. Prof. Albert Levi	Sabancı University
Prof. Oğuz Dikenelli	Ege University
Assoc. Prof. Fatih Alagöz	Bogazici University

Defense Date: 03.10.2011