Computer Networks 57 (2013) 330–350

Contents lists available at SciVerse ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

A formal role-based access control model for security policies in multi-domain mobile networks

D. Unal [a,*], M.U. Caglayan [b,1]

[a] TUBITAK BILGEM (Center of Research for Advanced Technologies of Informatics and Information Security), TUBITAK Gebze Yerleskesi, P.O Box 74, 41470 Gebze, Kocaeli, Turkey
[b] Bogazici University, TAM Research Center, Kandilli, Istanbul, Turkey

ARTICLE INFO

Article history:
Received 25 February 2011
Received in revised form 16 November 2011
Accepted 24 September 2012
Available online 5 October 2012

Keywords:
Mobile network
Multi-domain
Security policy
Access control
Model checking

ABSTRACT

Mobile users present challenges for security in multi-domain mobile networks. The actions of mobile users moving across security domains need to be specified and checked against domain and inter-domain policies. We propose a new formal security policy model for multi-domain mobile networks, called FPM-RBAC, 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. Associated with FPM-RBAC, we also present a formal security policy constraint specification language for domain and inter-domain security policies. Formal policy constraint specifications are based on ambient logic and predicate logic. We also use ambient calculus to specify the current state of a mobile network and actions within security policies for evaluation of access requests according to security policies. A novel aspect of the proposed policy model is the support for formal and automated analysis of security policies related to mobility within multiple security domains.

1. Introduction

The provision of services in networks with multiple administrative domains requires support for cross-domain security policy enforcement, management and verification. The multi-domain mobile network environment consists of multiple interconnected domains and mobile users, hosts and objects as sketched in Fig. 1. Inter-domain policies in such an environment need to support concepts such as mobility, inter-domain access rights, role mapping and separation of duty between domains.

An inter-domain security policy is based on a set of security agreements by participating organizations. The provision of inter-domain information sharing with mobile users call for an inter-domain policy model for mobile networks, which supports the concepts of inter-domain access rights, role mapping, locations and mobility, as explained below:

1. *Inter-domain access rights* are access rights for roles of a foreign domain in a local domain and access rights for local roles when accessing from a foreign domain. These rights relate to inter-domain operations.
2. *Role mapping* maps user roles in one domain to another. e.g. a lecturer in one university may become a researcher in another.
3. *Locations and mobility* in multiple domains relate to object, host and user mobility across domains. A mobile user needs to be given access due to location and mobility constraints.

Current state-of-the-art in the area of multi-domain security policy management are mostly related to federated systems. The federated system approach [1,2] requires a centralized knowledge of all system resources

* Corresponding author. Tel.: +90 2626481352; fax: +90 2626481100.
E-mail addresses: devrim.unal@tubitak.gov.tr (D. Unal), caglayan@boun.edu.tr (M.U. Caglayan).
[1] Principal corresponding author.

1389-1286/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.comnet.2012.09.018

and multi-domain users, which are assumed to be static in the network. This approach is not suitable for multi-domain mobile networks where administration is distributed and also users and resources are mobile. Other studies such as [3–9] in the area of role based access control policies with location information is mostly based on location of users, not providing a general model for security policies in a multi-domain mobile network.

In this paper, we propose a new formal security policy model for multi-domain mobile networks, called FPM-RBAC, Formal Policy Model for Mobility with Role Based Access Control, for specification of domain and inter-domain security policies. The FPM-RBAC model is based on the well-known RBAC [10,11] model. We use the RBAC model since roles provide flexibility in assignment and administration of permissions. In the context of multi-domain networks, roles are means of mapping permissions of a user in one domain to another domain. In the context of mobile networks, roles provide a user with the capability to carry all permissions associated with a role from one location to another. We augment the RBAC model by introducing services, inter-domain access rights, role hierarchy mapping, mobility and location constraints and separation of duty based on role mapping, locations and mobility.

Within the FPM-RBAC policy model, ambient logic [12,13] is used to specify dynamic mobility and location constraints in security policy rules. Logical constructs based on predicate logic are used for specification of static constraints such as separation of duty. We use the ambient calculus [14] to specify the current state of a mobile network and actions within security policies for evaluation of access requests according to security policies. The matching of mobility and location constraints in policy rules is accomplished by checking the validity of ambient logic formulas against ambient calculus specifications based on the model checking algorithms presented in our previous work [15].

Our first contribution is the introduction of a formal inter-domain policy model for mobile networks. Second contribution is a process calculus based formal mobility model within security policies, capable of representing mobile network state as well as complex location and mobility constraints. The administration model is distributed, where policy rules for inter-domain access are defined by role hierarchy mapping between home, inter-domain and foreign roles. Therefore our model does not require the global knowledge of users and objects and does not introduce conflicts caused by inter-domain hierarchy mapping.

In this study, we present an example scenario where we demonstrate the concepts introduced above. In this scenario, we consider a university involved in a joint research project in the e-health area, with a hospital and an industrial partner. The project members have a need to access and share information both locally and remotely from different locations, possibly using mobile communication and computing devices. Roles in each individual domain may be mapped to another one through role mapping relations during the project. Policy rules for inter-domain access rights should be in place for accessing joint project information. Location and mobility of users and information also need to be restricted. An inter-domain security policy rule may state that database records from the hospital domain related to patients may not be accessible from the university or industrial partner domain and may not be written to the university domain.

Section 2 summarizes the related work. In Section 3, we present the formal role-based security policy model called FPM-RBAC. In Section 4, we present the verification of FPM-RBAC security policies by model checking. In Section 5, we present an algorithm for giving the permission

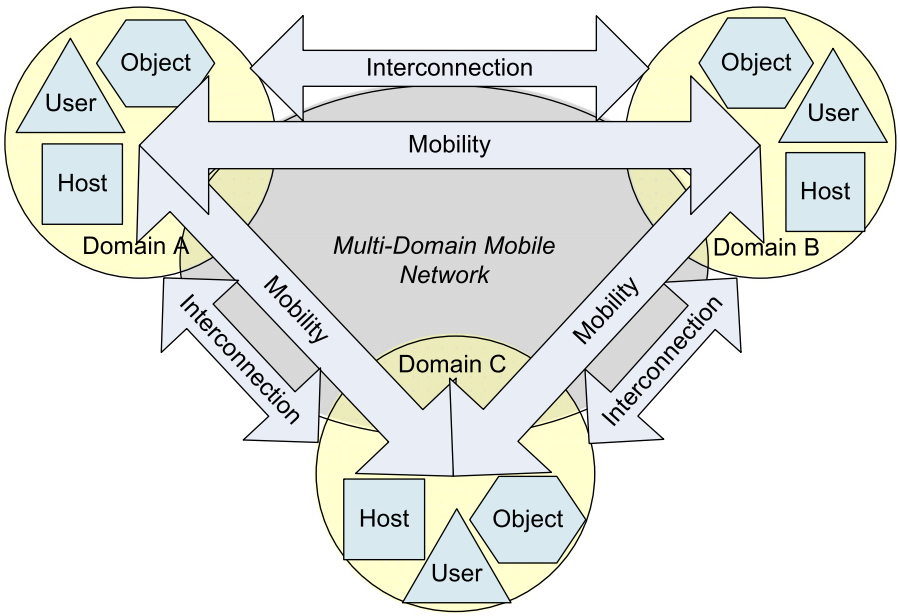

Fig. 1. Example multi-domain mobile network environment.