Towards Colored Petri Net Modeling of Expanded C-TMAC

Apostolos K. Provatidis, Christos K. Georgiadis, and Ioannis K. Mavridis

University of Macedonia, Department of Applied Informatics,
Egnatia 156, 540 06 Thessaloniki, Greece
{Provatidis,geor,mavridis}@uom.gr

Abstract. Today advancements in information technology have led to multi-user information systems of high complexity, where users can group, collaborate and share resources. The variety of such systems include a wide range of applications such as collaborative document sharing and editing, social networks, work flow management systems, mobile location based applications etc. As those systems continue to evolve, additional requirements arise which need to be met, such as context inclusion in access control decision making and security policies that support grouping, collaboration and sharing. To address this need, we are working on expanding C-TMAC, a security model that intrinsically supports grouping, collaboration and context awareness. In this perspective, we utilize the mathematical modeling language of Colored Petri Nets, along with the CPNtools, in order to represent and analyze the basic components of C-TMAC model.

Keywords: Security, Access Control, C-TMAC, RBAC, Colored Petri Nets, CPNtools, Formal Modeling and Analysis.

1 Introduction

A multi-user, information and resource sharing environment is bound to the conflict of the competing goals of collaboration and security, as ease of access is not easily paired to the availability, confidentiality, and integrity requirements of a solid security policy. In addition, the inclusion of context in these systems means that information of high sensitivity is processed which needs to be very carefully controlled. The particular need of controlling the information flow between individuals in such systems, demands for a security model that can effectively address these combined requirements.

Besides the classical access control approaches, like Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role based Access Control (RBAC), the Context-Based Team Access Control (C-TMAC) model was first introduced in [1]. C-TMAC is an extension of the highly established RBAC [2]. The purpose of this paper is to formally represent and analyze the basic components of the C-TMAC model, in order to identify its strengths and shortcomings. Working on this direction, we aim at expanding C-TMAC by enriching its intrinsic support of

H. Jahankhani et al. (Eds.): ICGS3/e-Democracy 2011, LNICST 99, pp. 88–95, 2012.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012

grouping collaboration and context awareness. In order to represent and analyze the C-TMAC model we utilize the strong mathematical modeling language of Colored Petri Nets (CPNs) that permit future analysis and verification processes.

The rest of the paper is organized as follows: the fundamental notions and notations used throughout the paper are presented in Section 2, which includes a brief presentation of the C-TMAC model. Moreover, the mathematical language chosen for modeling C-TMAC and the specific tool suite CPNtools for editing, simulating, and analyzing Colored Petri nets are briefly discussed. Section 3 contains related research that has been developed in two directions: exploiting of the context concept in RBAC-based access control approaches and utilizing formal analysis and verification methods for access control requirements addressing purposes. The developed Colored Petri Net of the expanded C-TMAC, is presented in Section 4. Section 5 concludes this paper and outlines future research directions.

2 Background

2.1 C-TMAC

The need for Users being able to collaborate in Teams and the notion of access rights associated to Teams was recognized early in the development of access control models. In RBAC [2] [3] models, Users belonging to the same Role can be defined as a group, but there are limitations in collaboration of users assigned to different Roles. Thomas in [4] proposed the Team Based Access Control (TMAC) model in which he explores the team-based nature of access and work in collaborative settings by defining two aspects of the collaboration context, user context and object context and the ability to apply this context to decisions concerning permission activation.

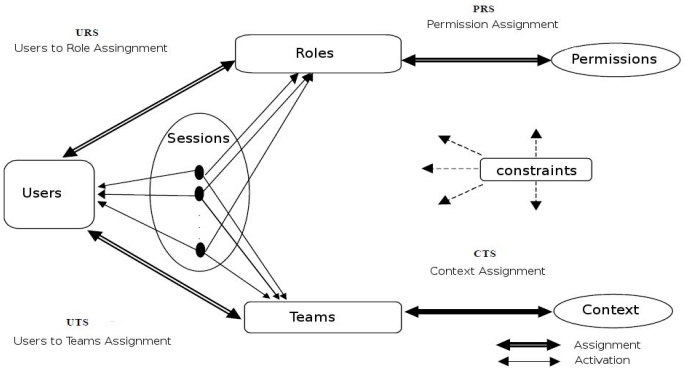

Fig. 1. The C-TMAC model

With the introduction of the C-TMAC model [1], the original TMAC was extended in two key directions: a framework to integrate TMAC concepts with RBAC and the use of other contextual information besides what is currently used in the user context

and object context in TMAC such as time, place, etc. Context is integrated as an entity in the model schema (Fig 1). A further expansion of C-TMAC is discussed in Section 4.

2.2 Colored Petri Nets and CPNtools

A Petri Net or Place – Transition Net, is a graphical tool used for the description and analysis of concurrent processes which arise in systems with many components, first proposed by Carl Adam Petri in 1962. The classical Petri net is a directed bipartite graph with two node types: rectangular shapes which denote Places (or Conditions or States) and round shapes which denote Transitions. They are interconnected by directed arcs. Only connections between different types of nodes are allowed. At any given time a place can contain zero or more Tokens, drawn as black dots. Tokens indicate the present state-of affairs and can be moved by the occurrence of transitions.

An extension of Petri Nets was introduced by Jensen [5], named Colored Petri Nets (CPNs), allowing tokens to be associated with colors. CPNs are an extension of Petri Nets with more expressive power. In a standard Petri net, tokens are indistinguishable. In a CPN, every token has a value (color).

In order to be able to practically make use of CPN graphical tool we need the aid of computer tools supporting the creation and manipulation of models. CPNtools is a tool suite for editing, simulation, and state space or performance analysis of CPN models. CPNtools suite provides a graphical representation of the CPN model, which is easy to edit, and capable of running extensive simulations.

3 Related Work

Several research efforts have addressed the issue of context inclusion in RBAC based models such as the TRBAC model [6] that allows temporal constraints on role enabling and disabling. The GTRBAC model [7] is a more generalized version of the Temporal RBAC model that supports various temporal constraints on User-Role assignment, Role activation, Role-Permission assignment, Role hierarchy and Separation of Duty. Covington et al. [8] define context information as environmental Roles, which are used to perform context-dependent tasks, and are activated based on environment conditions at the time of request. In a different approach [9], context based constraints are associated with activation of Role permissions. In [10] a programming framework for building context aware applications is presented, providing mechanisms for specifying and enforcing context-based access control requirements.

Also in a more collaborative approach, Liscano and Wang [11] extends the dRBAC model [12], by applying context information conditions into delegations and propose a temporary Session Role, which Users can use to delegate a set of their permissions, in order to enable access to each other's resources. Collaborations in Teams, was also explored in [13]. In addition, Tolone et al. in [14] provide an examination of access control models as applied to collaboration, pointing out the benefits and the weaknesses of these models. In their work the C-TMAC model

promisingly addresses the criteria the models are examined against, but as they state: "is not yet been fully developed, and it is not clear how to incorporate the team concept into a general RBAC framework".

As context inclusion and collaboration support in the security model of multi-user environments is an ongoing research area, we contribute to the need for the C-TMAC model to be further investigated and explored. In order to accomplish that, a formal verification method is required: our decision to relay on CPNs is consistent with several other researchers' efforts that explored RBAC based models using the same method.

Specifically Shafiq et al. in [15] proposed a Petri-Net based framework for the verification of correctness of event-driven RBAC policies. Rakkay and Boucheneb in [16] use CPNs and CPNtools to provide a general CPN model that shape most access control aspects with respect to RBAC policy requirements, also using CPN reachability analysis to check whether the access control requirements have been sufficiently addressed. Timed CPNs are used in [17] to model temporal constraints and analyze the TRBAC model [6]. Furthermore, Generalized Temporal RBAC (GTRBAC) model [7] is analyzed in [18] with the aid of timed automata.

To the best of our knowledge, no attempt has been made yet to represent and analyze TMAC or C-TMAC using CPNs or any other formal verification method.

4 Modeling C-TMAC

Over the last decade there were many important advancements concerning RBAC based models, as illustrated in the previous sections. In order to expand the C-TMAC model, we adopt the event based realization of RBAC specified in GTRBAC [7]. GTRBAC distinguishes between different states of a Role, namely *assigned*, *enabled* and *active*.

If a User is authorized to use a Role then this Role is *assigned* to the User. The *enabled* state indicates that Users who are authorized to use a Role at the time of the request may activate the Role and subsequently the *disabled* state indicates that the Role cannot be used in any User Session (due to constraints). A role in the *active* state implies that there is at least one User who has activated the Role.

According to previous CPNs of RBAC based models [15, 16], the constraints related to state transitions of Roles that are taken into account are:

- Cardinality constraints
- Role hierarchy constraints
- Separation of Duty constraints

In the C-TMAC model, both Roles and Teams are assigned to Users (see figure 1). The use of Teams as an intermediary to enable Users obtain context is similar to the use of Roles as an intermediary to enable Users obtain Permissions. Context entity includes information regarding the required data objects for a specific activity, as well as contextual information such as locations or time intervals, and can be expressed in terms of ranges of values.

For the detailed representation of the C-TMAC, we isolate in this work two important aspects of the model: the User-Role-Session aspect and the User-Team-Session aspect.

In the User-Role-Session aspect of C-TMAC the User obtains the sum of Permissions of the Roles he activates within a Session (we call them Session-Roles Permissions). The event based RBAC CPN model presented in [16] can be sufficiently used for the User-Role-Session aspect of the C-TMAC.

In the User-Team-Session aspect of C-TMAC, the User obtains the sum of Context of all Teams he participates in a Session (we call it Session-Team Context). Besides context, the User also obtains a combination of permissions of the Roles participating in those Teams (combination responds to Aggregation, Maximum/Minimum or Current Team Structure, see [1]), which we call Team-Roles Permissions. Following the event based approach, we define states for the Teams as well, which in accordance to these of Roles are: *assigned*, *enabled* and *active*. The CPN representation of the User-Team-Session aspect of the event based C-TMAC model is shown in figure 2.

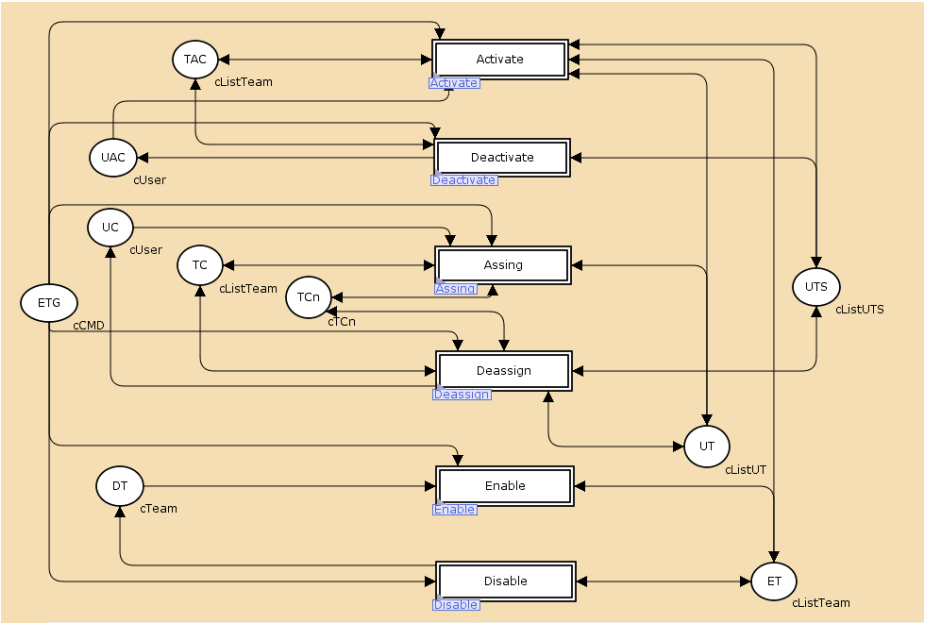

Fig. 2. CPN representation of the User-Team-Session aspect of the event based C-TMAC model

The specification of this CPN is similar to the previously mentioned User-Role-Session CPN. Due to space limitations we state some key elements and differences:

- Color declarations are changed to include Teams instead of Roles (figure 3).
- Role Cardinality (RC), Role Activation Cardinality (RAC), Enabled Roles (ER), Disabled Roles (DR), User Role Assignment/Authorization (UR) and

User Role Session Activation (URS) places are replaced with Team Cardinality (TC), Team Activation Cardinality (TAC), Enabled Teams (ET), Disabled Teams (DT), User Team Assignment/Authorization (UR) and User Team Session Activation (UTS) places respectively.

- There are no hierarchy constraints. Instead we have Teams that are in conflict with each other and cannot be assigned to the same User, thus Role hierarchy (RH) place is replaced with Team Conflict (TCn) place.
- Guard functions and tokens are changed accordingly.

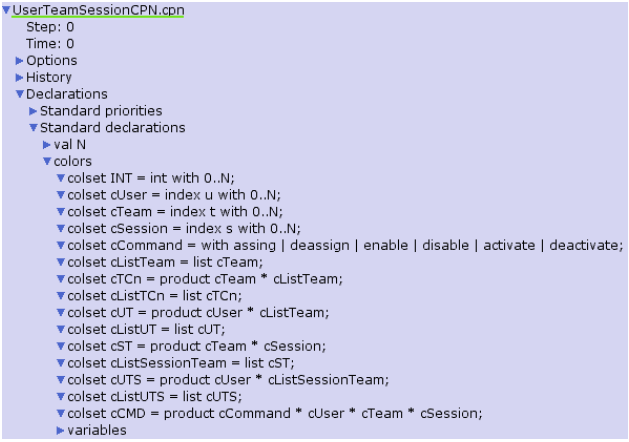

Fig. 3. Color declarations of User-Team-Session CPN

The constraints related to state transitions of Teams, which are defined and taken into account in this CPN, are:

- Cardinality Constraints
  - Team Cardinality (TC): The number of authorized Users for any Team does not exceed the authorization cardinality of that Team.
  - User Cardinality (UC): The number of Teams authorized for any User does not exceed the maximum number of Teams the User is entitled to acquire.
  - User Activation Cardinality (UAC): The number of Teams activated by any User does not exceed the maximum number of Teams the User is entitled to activate at any time
  - Team Activation Cardinality (TAC): The number of Users who have activated a Team in their Sessions does not exceed the Team activation cardinality.
- Separation of duty Constraints
  - Any two Teams assigned to the same User are not in conflict with each other

The two aspects of the C-TMAC jointly provide the final Permission set of the User: the Context-based Permissions, which are produced by the combination of Session-Roles Permissions and Team-Roles Permissions, filtered by Session-Team Context.

This CPN can be used for security policy verification regarding the participation of Users to Teams within Sessions. In combination with the corresponding CPN of the User-Role-Session aspect, they form a framework for security policy verification of C-TMAC systems.

5 Conclusions

In this paper an expanded C-TMAC model is presented, which combines notions of GTRBAC with grouping and context awareness. Using CPNs to represent the expanded C-TMAC aids to the clarification of the model, and makes the incorporation of the Team concept into a general RBAC framework clearer. Several Team related constraints could now be defined and illustrated along with the process of User participation to Teams within a Session in the corresponding CPN. For the CPN produced, an effort has been made to be as much identical to the one illustrating Roles constraints and User activation of Roles within a Session, as possible. This significantly reduces the complexity of the C-TMAC formal verification using CPNs.

Furthermore, adopting the event based approach of GTRBAC and integrating it to Teams as well as Roles results into an expanded version of C-TMAC and aids to the definition of Team Constraints. Temporal constrains in a context aware model are certainly a direction worth of closer examination in future research. An extensive version of this paper can include the full specification, simulations and reachability analysis of the CPNs for security policies verification of C-TMAC systems. Also, more Team related constrains can be defined, tailored to specific case studies.

Among the various applications of C-TMAC, defining a fine grained framework of Teams (groups) formation and user-permission assignment on them based on context, can aid to today's struggle of fine-tuning user permissions on the emerging social networks and the privacy concerns that they have surfaced.

C-TMAC can be particularly effective on emergency information systems, where the group of people corresponding to the emergency must obtain elevated permissions in accordance to the context of the emergency event.

References

1. Georgiadis, C.K., Mavridis, I., Pangalos, G., Thomas, R.K.: Flexible Team-Based Access Control Using Contexts. In: Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies, Chantilly, Virginia, USA (2001)
2. Sandhu, R.S., Coyne, E.J., Feinstein, H.L., Youman, C.E.: Role-based access control models. Computer 29(2), 38–47 (1996)
3. Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R.: Proposed NIST standard for role-based access control. ACM Trans. Inf. Syst. Secur. 4(3), 224–274 (2001)
4. Thomas, R.K.: Team-Based Access Control (TMAC): A Primitive for Applying Role-Based Access Controls in Collaborative Environments. In: Proceedings of the Second ACM Workshop on Role-based Access Control, Fairfax, VAUSA, pp. 13–19 (1997)
5. Jensen, K.: Coloured Petri Nets. Basic Concepts, Analysis Methods and Practical Use. Three Volumes (1997)

6. Bertino, E., Bonatti, P.A., Ferrari, E.: TRBAC: A temporal role based access control model. ACM Transactions on Information and System Security 4(3), 191–223 (2001)
7. Joshi, J.B.D., Bertino, E., Latif, U., Ghafoor, A.: A generalized temporal role based access control model. IEEE Transactions on Knowledge and Data Engineering 17(1), 4–23 (2005)
8. Covington, M.J., Long, W., Srinivasan, S., Dey, A.K., Ahamad, M., Abowd, G.D.: Securing Context-Aware Applications Using Environment Roles. In: SACMAT 2001: Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies, pp. 10–20 (2001)
9. Neumann, G., Strembeck, M.: An Approach to Engineer and Enforce Context Constraints in an RBAC Environment. In: SACMAT 2003: Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies, pp. 65–79 (2003)
10. Kulkarni, D., Tripathi, A.: Context-aware role-based access control in pervasive computing systems. In: SACMAT, pp. 113–122 (2008)
11. Liscano, R., Wang, K.: A SIP-based Architecture model for Contextual Coalition Access Control for Ubiquitous Computing. In: Proceedings of the Second Annual Conference on Mobile and Ubiquitous Systems (MobiQuitous 2005). IEEE Computer Society Press (2005)
12. Freudenthal, E., Pesin, T., Port, L., Keenan, E.: dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments. In: 22nd International Conference on Distributed Computing Systems (ICDCS 2002), pp. 411–420. IEEE ((2002)
13. Alotaiby, F.T., Chen, J.X.: A Model for Team-based Access Control (TMAC 2004). In: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC 2004), vol. 2, p. 450. IEEE Computer Society, Washington, DC (2004)
14. Tolone, W., Ahn, G., Pai, T., Hong, S.: Access control in collaborative systems. ACM Comput. Surv. 37(1), 29–41 (2005)
15. Shafiq, B., Masood, A., Joshi, J., Ghafoor, A.: A role-based access control policy verification framework for real-time systems. In: WORDS 2005: Proceedings of the 10th IEEE International Workshop on Object-Oriented Real-Time Dependable Systems, pp. 13–20. IEEE Computer Society, Washington (2005)
16. Rakkay, H., Boucheneb, H.: Security Analysis of Role Based Access Control Models Using Colored Petri Nets and CPNtools. In: Gavrilova, M.L., Tan, C.J.K., Moreno, E.D. (eds.) Transactions on Computational Science IV. LNCS, vol. 5430, pp. 149–176. Springer, Heidelberg (2009)
17. Kadloul, L., Djouani, K., Tfaili, W.: Using Timed Colored Petri Nets and CPN-tool to Model and Verify TRBAC Security Policies. In: Fourth International Workshop on Verification and Evaluation of Computer and Communication Systems, VECoS 2010 (2010)
18. Mondal, S., Sural, S., Atluri, V.: Towards formal security analysis of GTRBAC using timed automata. In: Proceedings of the 14th ACM Symposium on Access Control Models and Technologies (SACMAT 2009), pp. 33–42. ACM, NY (2009)