Composed SoD - Uma Proposta para Auxiliar Modelos de Controle de Acesso

Eduardo Sakaue, Felipe A. Almeida

[1]Instituto Tecnológico de Aeronáutica (ITA)
São José dos Campos – SP

e.sakaue@uol.com.br,felal@uol.com.br

Abstract. *One of the main sources of attack to the internal system of companies, their own employees. The current models of access control do not cover organized groups of badly intentioned employees. This article considers a way to identify groups of users and to verify its executed tasks. And thus, to prevent further damages the company.*

Resumo. *Uma das principais fontes de ataque ao sistema interno de empresas, ainda são os próprios funcionários. Os modelos de controle de acesso atuais não cobrem grupos organizados de funcionários mal intencionados. Este artigo propõe uma maneira de identificar estes grupos de usuários e verificar suas tarefas executadas e, desta forma, impedir maiores danos a empresa.*

1. Introdução

Existem várias necessidades que justificam o avanço dos modelos de controle de acesso. O *Role Based Access Control* (RBAC) é um deles e foi motivado em razão da dificuldade de gerenciar muitas pessoas em grandes organizações. Baseado nesta mesma dificuldade, pequenas vulnerabilidades acabam se tornando grandes problemas para as instituições. Segundo [Sandhu et al. 1997, Sandhu et al. 1996], o RBAC é neutro a políticas e flexível. O modelo suporta diretamente três princípios básicos de segurança: Privilégio Mínimo, Separação de Deveres e Abstração de Dados. Mas nem sempre as políticas cobrem todas as brechas, principalmente em relação aos funcionários.
Um grupo de funcionários pode facilmente dentro de suas funções diárias conspirar contra a empresa, podendo também ficar incógnito por um período indesejável.
O presente esforço de pesquisa visa desenvolver um método para auxiliar a busca por vulnerabilidades exploradas por mais de um funcionário.

2. *Role Based Access Control*

Desde que foi concebido em 1992 [Ferraiolo and Kuhn 1992], o RBAC se mostrou o modelo dominante na década de 90 [Sandhu 1996] , e esta mesma tendência segue até os dias de hoje.
O conceito é simples, estabelecer permissões baseada em funções e cargos de empresas, e associa apropriadamente usuários a cargos, ou conjunto de cargos [Sandhu et al. 2000]. RBAC traz um poderoso mecanismo para reduzir a complexidade, custo e potenciais erros de associação, como apresentado a seguir na Figura 1. O RBAC reforça variedade

de políticas.
Não existe associação direta entre usuários e permissões. Os papéis podem ser o "cargo"que a pessoa ocupa dentro da organização, ou um conjunto de funções que um certo objeto recebe para executar.
Por não se basear no usuário, o RBAC simplifica o controle em grandes organizações, onde pode haver centenas ou milhares de funcionários.
Uma característica importante no RBAC é ser neutro em relação as políticas de segurança. A partir do momento em que o RBAC é implantado na empresa, deve-se então configura-lo e adapta-lo através de regras para as políticas da própria empresa.

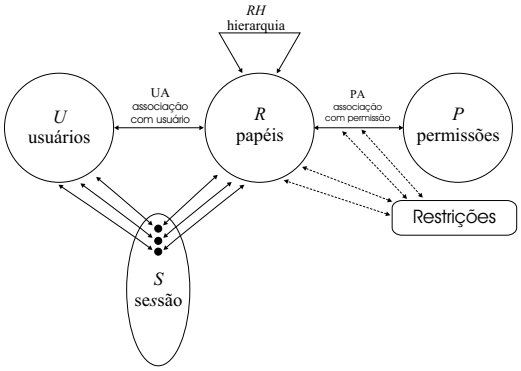

Figura 1. Modelo RBAC

3. Grupos

Embora o RBAC facilite o gerenciamento de controle de acesso, certas vulnerabilidades ainda podem passar por políticas de segurança e pelas *constraints* acrescentadas ao modelo.
Várias extensões já foram propostas para enriquecer o modelo [Joshi et al. 2005], [Sandhu et al. 1997], entre outros. Porém certos pontos de segurança ainda permanecem descobertos.
O problema origina-se quando o resultado de uma tarefa é manipulado por dois ou mais usuários. Neste caso existiria um agrupamento de usuários que podem unir-se no manejo deste objeto.
Uma dessas vulnerabilidades é o ataque em grupo. Por exemplo, se uma empresa paga gratificação proporcional aos funcionários, estes podem "dar um jeito"de trabalhar mais. Digamos que certo vendedor de iates consegue preferências sobre a fábrica. Isso porque seu contato na fábrica passa seus pedidos na frente dos demais. E o supervisor que deveria monitorar os atos, deixa isso acontecer propositalmente. Ao final do ano, os 3 dividem a gratificação.
Este artigo propõe um RBAC auxiliado a eventos visando coibir ataques de grupos de funcionários, ou a utilização indevida do sistema interno da empresa. A cada vez que um Usuário acessar um Role, a cada vez que um Role precisar de uma Permissão, ou a cada vez que uma Sessão é criada, um novo evento é computado. Assim é gerado uma sequência de eventos, que podem ser monitorados com mais facilidade. Dessa forma torna-se necessário uma ferramenta para analisar tais eventos.
Normalmente o RBAC observa a empresa de forma horizontal, separando os usuários em

Roles e adicionando hierarquia sobre eles. Porém, para estes casos a empresa precisa ser vista através de grupos relacionados por funções, conforme mostrado na Figura 2. Estes grupos nem sempre são notados dentro do controle de segurança. Uma vez que *Separation of Duties* (SoD) prevê ataques de apenas um usuário, e não de grupos de usuários.

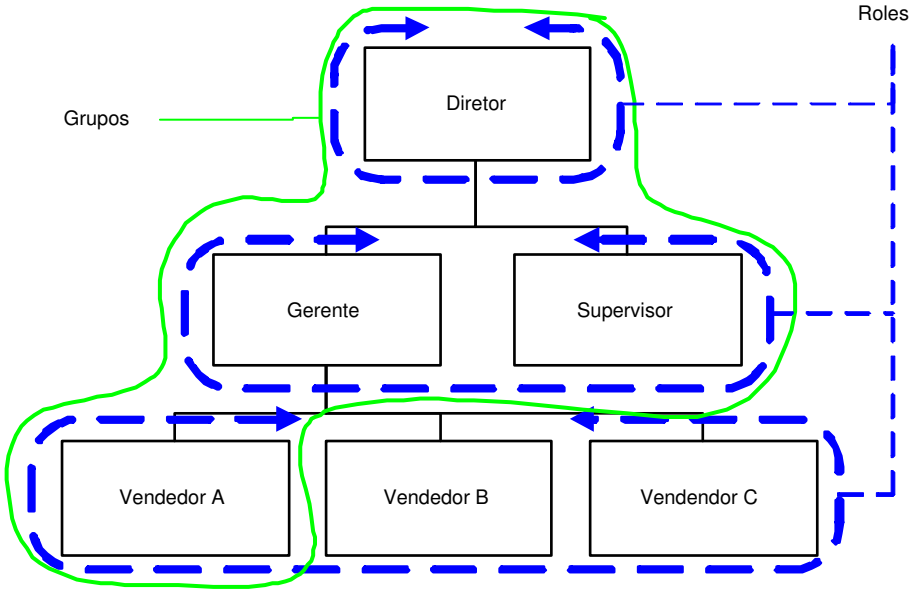

Figura 2. RBAC sobre o organograma

A forma mais simples para se detectar um grupo de funcionários relacionados é observar suas funções dentro do sistema. Se as funções estiverem relacionadas de alguma forma, por um produto ou algum documento, então podemos rastrear todo o grupo. Neste artigo denominamos esta extensão a modelos de *Composed SoD*.
Para identificar e bloquear um grupo é necessário dois procedimentos: Eventos, registrando os acessos as funções de cada usuário. E um Analisador de eventos, percorrendo todos os registros em busca de funcionalidades em comum, para então julgá-las de acordo com regras.

3.1. Eventos

A abordagem adotada visa registrar cada função executada por cada usuário do sistema, possibilitando comparar com as ações de outros funcionários. Dessa forma é possível relacionar tais ações e rastrear todos os passos de cada processo existente no sistema.

3.2. Analisador

O objetivo do analisador é percorrer todo o registro de eventos em busca de processos. Ao identificar um processo, o analisador irá verificar se o mesmo está de acordo com as regras pré-inseridas, que fazem parte da política da empresa. As regras podem ser tanto estatísticas, quanto em cima de *workflow*, *data mining* ou redes neurais.

4. conclusão

Através de uma análise dos eventos feitos por cada funcionário podemos encontrar diversos meios de bloquear ataques ao sistema. Uma limitação está em encontrar as possibilidades ainda não previstas pelos analisadores ou analistas. Para um trabalho futuro, pode-se colocar um analisador que utilize técnicas de redes neurais para aprender novas regras e encontrar mais possibilidades antes mesmo que estas aconteçam.
Os modelos de controle de acesso, normalmente observam cada funcionário, e depois grupos horizontais de funcionários. Foi apresentado aqui uma nova visão, baseada em eventos individuais e globais da empresa.

Referências

Ferraiolo, D. and Kuhn, R. (1992). Role-based access control. In *15th NIST-NCSC National Computer Security Conference*, pages 554–563, Gaithersburg, Maryland, United States. National Institute of Standards and Technology.

Joshi, J., Bertino, E., Latif, U., and Ghafoor, A. (2005). A generalized temporal role-based access control model. In *Knowledge and Data Engineering, IEEE Transactions on*, page 19, Los Alamitos, CA. IEEE Computer Society Press.

Sandhu, R., Bhamidipati, V., Coyne, E., Ganta, S., and Youman, C. (1997). The ARBAC97 model for role-based administration of roles: Preliminary description and outline. In *RBAC '97: Proceedings of the second ACM workshop on Role-based access control*, pages 41–50, New York, NY, USA. ACM Workshop on Role Based Access Control, ACM Press.

Sandhu, R., Ferraiolo, D., and Kuhn, R. (2000). The nist model for role-based access control: towards a unified standard. In *RBAC '00: Proceedings of the fifth ACM workshop on Role-based access control*, pages 47–63, New York, NY, USA. ACM workshop on Role-based access control, ACM Press.

Sandhu, R. S. (1996). Rationale for the RBAC96 family of access control models. In *RBAC '95: Proceedings of the first ACM Workshop on Role-based access control*, page 9, New York, NY, USA. ACM Workshop on Role-based access control, ACM Press.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., , and Youman, C. E. (1996). Role based access control models. *Computer IEEE*, 29(2):38–47.