# Composição de IDSs Usando *Web Services*

**José Eduardo M. S. Brandão[1,2], Joni da Silva Fraga[1], Paulo Manoel Mafra[1]**

[1]Dep. de Automação e Sistemas (DAS) – Univ. Federal de Santa Catarina (UFSC) UFSC
Caixa Postal 476, CEP 88040-900, Florianópolis – SC

[2]Instituto de Pesquisa Econômica Aplicada (IPEA) – SBS Q.1 Ed. BNDES, Brasília – DF

{jemsb, fraga, mafra}@das.ufsc.br

***Abstract.*** *This paper presents a model for manual and dynamic composition of intrusion detection systems. Such systems can work either in medium and large sized companies environments. It can also work in open environment, which uses Internet. The construction of such systems is possible through the application of introduced standards (or in definition process) and still, for the extensive use of XML language and the Web Services technology.*

***Resumo.*** *Este artigo apresenta um modelo para a composição, mesmo dinâmica, de sistemas de detecção de intrusão que funcionem tanto em ambientes fechados de médias e grandes empresas, quanto em ambientes abertos, que fazem uso da Internet. A construção de tais sistemas é possível através da aplicação de padrões introduzidos (ou em processo de definição) e ainda, pelo emprego extensivo da linguagem XML e da tecnologia de Web Services.*

## 1. Introdução

Nesse artigo descrevemos um modelo que propomos para composição, mesmo dinâmica, de sistemas de detecção de intrusão. O modelo proposto é concretizado a partir de uma infra-estrutura de serviços que permite a composição de sistemas de detecção de intrusão e pela aplicação de padrões para a interoperabilidade e comunicação entre IDSs, principalmente aqueles desenvolvidos pelo grupo IDWG da IETF (*The Internet Engineering Task Force*) (Debar et al., 2005)(Wood e Erlinger, 2002). Esta infra-estrutura segue uma arquitetura orientada a serviços (SOA: *Service Oriented Architecture*) suprida, principalmente, pela tecnologia de *Web Services* (W3C, 2004). O modelo faz ainda uso extensivo da linguagem XML (*Extensible Markup Language*) e suas extensões para segurança (BRAY et al., 2004).

## 2. Trabalhos Relacionados

As novas propostas de construção de IDSs distribuídos, em geral, continuam usando formatos e protocolos não padronizados para a comunicação entre seus componentes. As propostas de (Bass, 2004) exemplifica esta situação. O *DOMINO* (Yegneswaran et al, 2004) e o *STAT* (Vigna et al., 2003) são algumas das poucas experiências que fazem do padrão IDMEF (Debar et al., 2005). Contudo, em ambos os casos, o uso dos padrões é restrito à comunicação interna dos IDSs e as adaptações realizadas para o uso dos padrões não são completamente compatíveis com a especificação original destes padrões. Um dos IDSs de rede mais populares, o *SNORT*, apesar de não ter sido projetado para o uso de padrões, possui um *plug-in* que permite o envio de notificações no formato IDMEF. O

IDS que mais parece se adequar à nossa proposta é o *Prelude-ids* (Prelude, 2005), que se encaixa em nosso modelo tanto como um sensor, quanto um analisador que integra diversos componentes. Infelizmente, o controle e a configuração destes componentes é manual e diferenciado para cada um deles. O *Prelude-ids*, como os outros IDSs utilizam protocolos de transporte diversos, o que dificulta o controle e a passagem dos dados pelos sistemas de *firewall*. O emprego de *Web Services*, como proposto pelo nosso modelo, permite padronizar o transporte, facilitando a comunicação e o controle da rede.

## 3. Requisitos do Modelo de Composição de IDSs

O modelo proposto é baseado em cinco objetivos principais: a detecção de intrusão distribuída; o uso de elementos heterogêneos na detecção de intrusão; a composição dinâmica de sistemas de detecção de intrusão; o uso de padrões de interoperabilidade e a segurança nas interações e manipulações do próprio sistema de detecção distribuída. Estes objetivos são evidenciados na seqüência.

- Detecção de Intrusão distribuída - prioriza a distribuição de elementos envolvidos na detecção de intrusos, que devem trocar informações entre si sem a necessidade de elementos centrais, evitando os gargalos ou pontos únicos de falha que se formam com a centralização de funções ou componentes de um IDS.

- Elementos Heterogêneos - nem sempre um IDS é capaz de coletar, analisar e gerenciar informações provenientes de diversos níveis e de diferentes ambientes. O modelo proposto deve permitir a integração de qualquer tipo de ferramentas previamente existentes, mesmo que de diferentes fabricantes. O modelo é fundamentado em um suporte integrador que é usado tanto para a integração de IDSs completos e independentes, quanto para componentes de um IDS. Componentes de um IDS poderão ser, por exemplo, ferramentas para segurança de perímetro, IDSs comerciais (monolíticos ou distribuídos), baseados em agentes (móveis ou fixos), etc.

- Composição Dinâmica de IDSs - a composição de IDSs e a integração de componentes pode formar uma base computacional significativa, permitindo uma maior eficiência e uma possibilidade de adaptação em funções de detecção de anomalias e do estabelecimento de correlações entre as mesmas. A composição de sistemas de detecção de intrusão pode ser feita de forma dinâmica, envolvendo mesmo o compartilhamento, entre IDSs, de componentes que poderão ser entidades autônomas. Uma composição pode ser permanente ou temporária, definida com a finalidade, por exemplo, de coletar dados de determinados sensores, pesquisar diversas bases de dados de eventos ou para compartilhar informações sobre um ataque em andamento. O modelo que propomos é o veículo para estas composições flexíveis e para o próprio controle das configurações destes IDSs. Adotamos como componentes básicos de um IDS, aqueles definidos por (Wood e Erlinger, 2002): sensores, analisadores e gerentes.

- Padrões de Interoperabilidade - a composição de sistemas de detecção de intrusão a partir do nosso modelo deve atender as necessidades de ambientes fechados de médias e grandes empresas, mas principalmente as de ambientes abertos que fazem uso da Internet. A interoperabilidade é importante, visto que assumimos nas composições de sistemas de detecção, componentes ou IDSs monolíticos fornecidos por diferentes fabricantes. É necessário nestas composições que seus elementos “falem a mesma

língua", ou seja, possuam formas padronizadas de comunicação e de integração. Para viabilizar tais sistemas, propomos a integração de padrões que permitam a interoperabilidade nestas composições distribuídas. Nos concentramos neste trabalho nos esforços de padronização da IETF e no uso extensivo da linguagem XML e da tecnologia *Web Services* de programação distribuída orientada a serviços.

- Segurança - a segurança dos próprios IDSs é obviamente crítica para qualquer sistema sendo monitorado. Para tal, é necessário o uso de mecanismos que possam garantir as propriedades de segurança das próprias informações trocadas ou manipuladas nestas composições distribuídas de IDSs.

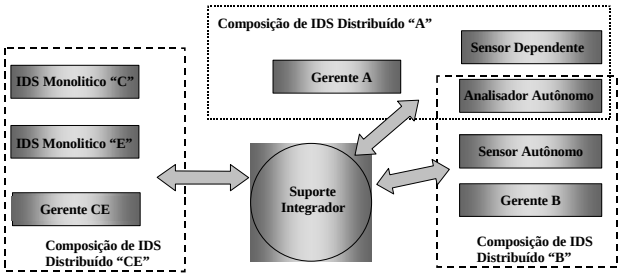


**Figura 1 – Composições de Sistemas de Detecção de Intrusão**

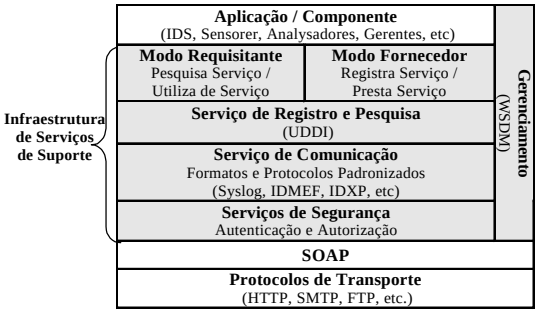


**Figura 2 – Suporte de Serviços para Composição de IDSs**

## 4. Composição de IDSs em uma Arquitetura Orientada a Serviços

Um IDS pode ser composto, por exemplo, por sensores autônomos que fornecem serviços de geração de eventos e elementos que executam análise, redução ou correlação destes eventos. A Figura 1 ilustra algumas possibilidades de configuração supridas pelo nosso modelo a partir de uma *infra-estrutura* de serviços (suporte integrador na Figura 1 e Figura 2). A composição de IDS "B" mostrado na Figura 1 é um exemplo desta possibilidade. Sensores e analisadores, portanto, podem ser dependentes ou autônomos, assumindo papéis de requisitantes e fornecedores de serviços, conforme o tipo de interação que estejam participando. Outro aspecto que estamos explorando é a possibilidade do compartilhamento destes componentes elementares entre IDSs; na Figura 1, as composições "A" e "B" compartilham um analisador autônomo. A composição "CE" reúne IDSs monolíticos provavelmente complementares, fornecendo um serviço mais confiável de detecção. Gerentes usam serviços de sensores e analisadores, podendo também interagir com outros gerentes no nosso modelo.

As associações podem se estender por diferentes organizações, permitindo, por exemplo, o compartilhamento de alertas de segurança. Esta troca de informações pode estar sujeita a políticas que limitam o fluxo que sai de cada organização no sentido das comunicações entre organizações. Para isso, tanto os componentes de uma composição de IDSs, quanto os serviços associados ao suporte integrador (uma infra-estrutura de serviços) são apresentados como *Web Services*.

Um componente pode funcionar no modo requisitante, no modo fornecedor ou em ambos os modos. A Figura 2 apresenta a estratificação de serviços necessária para composições de IDSs. Na programação orientada a serviços, cada elemento de uma composição de IDSs é visto como um serviço. Suas interfaces são descritas em um formato processável por computador fornecido pela linguagem WSDL (*Web Services*

*Description Language*) (W3C, 2005). As informações referentes a estes serviços, necessárias nas interações com os mesmos, são disponibilizadas através de um Serviço de Registro e Pesquisa na nossa infra-estrutura de suporte. Tal serviço está fundamentado no UDDI (*Universal Description, Discovery and Integration specification*) (OASIS, 2004). Os serviços de uma composição trocam informações entre si através de mensagens. Tais mensagens seguem formatos padronizados e são transportadas por protocolos padrões, mantendo propriedades de segurança. Os vários componentes de um IDS, na forma de serviço, fazem uso de padrões como o IDMEF (*Intrusion Detection Message Exchange Format*) (Debar et al., 2005) e *Syslog* (Lonvick, 2001), codificados nas trocas de requisições e respostas SOAP (W3C, 2003). As extensões de segurança do XML são usadas para garantir aspectos de integridade e confidencialidade nestas comunicações. O gerenciamento das composições de IDSs se dá através de serviços do *Web Services Distributed Management* (WSDM) (OASIS, 2005). O uso deste suporte permite que qualquer serviço seja gerenciado através de padrões de gerenciamento específicos para *Web Services*.

O amplo emprego de formatos, protocolos e arquiteturas padrões para a construção do *framework* e, em especial, do serviço de registro e pesquisa, torna o modelo interoperável em qualquer ambiente. O uso do Serviço de Registro e Pesquisa em conjunto com uma taxonomia para a classificação de componentes de monitoramento torna a localização de serviços especializados mais fácil e precisa.

## Referências


BASS, T.; 2004. Service-Oriented Horizontal Fusion in Distributed Coordination-Based Systems. IEEE MILCOM 2004 (Nov. 2004: Monterey, CA).

BRAY, T. et al.; 2004. *Extensible Markup Language (XML) 1.0 (Third Edition)*. W3C.

DEBAR H., CURRY D. and FEINSTEIN B.; 2005. *The Intrusion Detection Message Exchange Format*. IETF Internet-Draft draft-ietf-idwg-idmef-xml-14.

LONVICK, C.; 2001. The BSD syslog Protocol. RFC 3164. IETF Network Working Group.

OASIS; 2004. *UDDI Version 3.0.2*. OASIS UDDI Spec TC.

OASIS; 2005. *Web Services Distributed Management: Management Using Web Services (MUWS 1.0) Part 2 - Web Services Distributed Management: Management of Web Services (WSDM-MOWS) 1.0*. OASIS *Web Services* Distributed Management (WSDM) TC.

PRELUDE; 2005. Prelude: an Open Source, Hybrid Intrusion Detection System. (current: http://www.prelude-ids.org/, Jun. 2005).

VIGNA, G. VALEUR, F., and KEMMERER R.A.; 2003. Designing and implementing a family of intrusion detection systems. In: 9th European software engineering conference held jointly with 11th ACM SIGSOFT international symposium on Foundations of software engineering. *Proceedings*. Vol.28 n.5. p. 88-97.

W3C; 2003. *SOAP Version 1.2 Part 0: Primer*. World Wide Web Consortium.

W3C; 2004. *Services Architecture*. W3C Working Group Note 11 February 2004.

W3C; 2005. *Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language*. World Wide Web Consortium.

WOOD, M., and ERLINGER, M.; 2002. *Intrusion Detection Message Exchange Requirements*. IETF Internet-Draft draft-ietf-idwg-requirements-10.

YEGNESWARAN, V., BARFORD, P., JHA, S.; 2004. Global Intrusion Detection in the DOMINO Overlay System. In: of Network and Distributed System Security Symposium (NDSS) (Feb. 2004: San Diego, Ca). *Proceedings*.