O Sistema de Detecção de Intrusão Asgaard

Rafael Saldanha Campello, Raul Fernando Weber,
Vinicius da Silveira Serafim, Vinicius Gadis Ribeiro

Instituto de Informática, PPGC, Universidade Federal do Rio Grande do Sul
Av. Bento Gonçalves, 9500, Porto Alegre, RS
{campello,weber,serafim,vribeiro}@inf.ufrgs.br

Abstract: This paper describes a study being developed at the Security Group (GSeg-UFRGS), of the Federal University of Rio Grande do Sul, aimed to the creation of a modular and decentralized intrusion detection system, called Asgaard, trying to fill the main gaps left for the current IDS. Its main characteristics and features are described, as well as its architecture and main modules.

Palavras-Chaves: segurança, detecção de intrusão, confiabilidade

1 Introdução

A detecção de intrusão é uma das áreas de maior expansão, pesquisa e investimento na segurança em redes de computadores. Com o grande crescimento da interconexão de computadores em todo o mundo, materializado pela Internet, é verificado um conseqüente aumento nos tipos e no número de ataques a esses sistemas, gerando uma complexidade muito elevada para a capacidade dos tradicionais mecanismos de prevenção. Para a maioria das aplicação atuais, desde redes corporativas simples até sistemas de e-comerce ou aplicações bancárias, é praticamente inviável a simples utilização de mecanismos que diminuam a probabilidade de eventuais ataques. Um ataque força, em casos extremos, a interrupções totais dos serviços para que um lento e oneroso processo de auditoria e de posterior restauração manual seja efetuado. Isso justifica todo investimento feito visando a criação de mecanismos que ultrapassem a barreira da simples prevenção, garantindo aos sistemas um funcionamento contínuo e correto mesmo na presença de falhas de segurança, principal objetivo dos chamados Sistemas de Detecção de Intrusão (IDS).

Constantes avanços na arquitetura dessas ferramentas vêm sendo observados, resultando em soluções fortemente centralizadas e robustas [1], em idéias completamente distribuídas [2], que segmentam o problema em vários níveis diferentes, ou em arquiteturas híbridas [3]. Da mesma forma, estudam-se novos métodos usados na busca por evidências de um ataque, aumentando a eficiência e também adequando os IDSs à realidade das redes atuais (altas velocidades, por exemplo). Alguns desses métodos visam analisar o comportamento do sistema e identificar possíveis desvios, comparando o estado observado a um padrão de comportamento considerado normal [4][5]. Outras técnicas buscam seqüências de ações nitidamente caracterizadas como inválidas, registradas em uma base de dados que contém assinaturas dos ataques conhecidos [6][7]. Além desses, outros métodos são alvos de estudo e vêm sendo gradativamente empregados em IDSs, envolvendo áreas como sistemas especialistas [5], redes neurais [8] e data mining [9], ou, inclusive, conceitos como o sistema imunológico humano [10], solidificando soluções úteis na manutenção da segurança dos sistemas.

Mesmo com todo o esforço de pesquisa feito até então, verifica-se uma certa imaturidade nos atuais IDSs, principalmente decorrente de detalhes ainda pouco explorados e de fundamental importância para soluções realmente adequadas. A dificuldade de interação entre as diversas ferramentas já desenvolvidas, decorrente da falta de um padrão de interconexão entre esses mecanismos, a adoção ainda pequena de soluções híbridas e de fácil crescimento modular, a falta de habilidade para reagir a possíveis ataques e a pouca preocupação com a confiabilidade dos próprios IDSs são alguns dos exemplos que demonstram tal imaturidade.

Com o objetivo de abordar alguns desses problemas, este artigo apresenta um estudo em andamento no Grupo de Segurança da Universidade Federal do Rio Grande do Sul (GSeg-UFRGS), que tem como meta principal a concretização de um sistema de detecção de intrusão, chamado Asgaard e voltado ao emprego de técnicas que cubram as principais lacunas deixadas pelos IDS atuais.

2 Sistemas de Detecção de Intrusão

Como já foi enfatizado, a área de detecção de intrusão ainda está longe de atingir uma maturidade tecnológica adequada, apesar de todos os avanços verificados nas últimas duas décadas. Mesmo as ferramentas mais atuais

ainda não atentam para alguns problemas reais que acabam colocando os IDSs em um lugar de pouco destaque dentre os mecanismos de segurança utilizados. Quanto a esses problemas, pode-se citar como exemplos expressivos:

- *Nível dos ataques*: com uma taxa de crescimento semelhante à verificada nos mecanismos de segurança, as ferramentas voltadas para explorar as vulnerabilidades dos sistemas vêm aumentando em complexidade e eficiência, facilitando cada vez mais a tarefa dos atacantes. Além disso, técnicas projetadas para aumentar a segurança, como a criptografia, por exemplo, vêm sendo usadas para burlar os sistemas de detecção de intrusão, criando dificuldades ainda não tratadas.
- *Dimensão e complexidade das redes*: o desempenho dos IDS é um dos fatores afetados pelo crescimento das redes de computadores, seja na dimensão ou na crescente complexidade dessas estruturas. Isso significa maior dificuldade em tratar quantidades tão expressivas de informação em tempo hábil, problemas com a diversidade de plataformas encontradas (hardware e sistemas operacionais), dificuldade de monitoramento do tráfego em redes segmentadas (uso de *switch*), manutenção, dentre outros. Encontrar soluções eficientes que minimizem tais problemas tem impulsionado muitos estudos na área.
- *Tolerância a falhas*: um dos principais responsáveis pela segurança de uma organização, o sistema de detecção de intrusão vem se tornando alvo freqüente dos atacantes mais experientes, comprometido por técnicas de negação de serviço (denial-of-service), spoofing, dentre outras. Assim, o emprego de técnicas de tolerância a falhas para garantir a confiabilidade e disponibilidade dos IDS é outro desafio ainda pouco explorado.
- *Autenticação e privacidade*: pelos mesmos motivos mencionados acima, é fundamental garantir a privacidade das informações trocadas entre os módulos do sistema e, principalmente, a autenticidade dessas informações. Contrastando com a preocupação em melhorar o desempenho dos IDS, a obtenção da autenticidade e da privacidade nos sistemas atuais é de fundamental importância, principalmente devido à descentralização verificada.
- *Interoperabilidade e padronização*: talvez um dos assuntos mais pesquisados atualmente em detecção de intrusão, a busca por um padrão de interação entre diferentes ferramentas facilitaria a integração de tecnologias complementares e, com isso, aumentaria as chances de uma detecção bem sucedida. Vários padrões estão sendo propostos mas muito caminho ainda será percorrido até que a padronização da troca de informação seja uma realidade.
- *Arquiteturas distribuídas*: estruturas centralizadas compartilham vantagens inegáveis em vários aspectos, seja pela facilidade de manutenção, simplicidade - e conseqüente desempenho dos protocolos empregados - ou pela facilidade de desenvolvimento. Por outro lado, a complexidade dos sistemas atuais aliada à diversidade e dimensões da maioria das instalações computacionais, praticamente inviabiliza qualquer solução completamente centralizada. Mecanismos de segurança devem, obrigatoriamente, cooperar na busca por um sistema mais confiável, seja do ponto de vista funcional (maior segurança) como da tolerância a falhas nos próprios mecanismos. Isso remete a uma arquitetura distribuída, com módulos independentes cooperando através da troca de mensagens, podendo ser extrapolada para uma solução híbrida, onde mecanismos centralizados interagem com módulos distribuídos. Vários problemas surgem nesse ponto, já que a redundância inerente aos sistemas distribuídos (e conseqüente facilidade de aplicação de tolerância a falhas) contrasta com a necessidade de mecanismos mais robustos para a manutenção dessa cooperação. Do mesmo modo, a adoção de arquiteturas que obedeçam a uma estrutura hierárquica compromete a disponibilidade do sistema, principalmente pela criação de pontos únicos de falha.

Muitos outros problemas poderiam ser citados, como a popularização da computação móvel, questões legais envolvendo o monitoramento e a privacidade dos usuários, a tentativa de ações pró-ativas, ou seja, a detecção antecipada de ameaças de intrusão, dentre outros, evidenciando um vasto campo para novas pesquisas. Mesmo assim, algumas direções já podem ser apontadas, não como soluções definitivas mas como caminhos viáveis para a criação de um sistema de detecção de intrusão mais completo e robusto. Já citados por alguns trabalhos [2][3][6], muitas dessas idéias permanecem no papel:

- *Arquitetura híbrida*: vários trabalhos já colocam em prática a idéia de implementar uma estrutura híbrida, onde a mescla de detectores centralizados baseados em host e de outros distribuídos baseados em rede é incentivada. Por outro lado, na maioria dos casos, uma arquitetura hierárquica é adotada, criando novos problemas, principalmente no tocante à tolerância a falhas (único ponto de falhas). Fica evidente, com isso, a importância de uma estrutura completamente distribuída, restando solucionar os problemas característicos de todo sistema distribuído.

- *Crescimento modular*: praticamente conseqüência de uma arquitetura híbrida, o crescimento modular é uma característica de grande impacto na adequação de um IDS às novas ameaças, surgidas a cada dia. Sobre uma estrutura modular, um IDS tem a possibilidade de gerar soluções perfeitamente adaptáveis a qualquer tipo e dimensão de organização, facilitando o desenvolvimento incremental de novos conceitos e técnicas.
- *Portabilidade*: a diversidade de plataformas utilizadas, como já citado, é uma realidade na maioria das empresas. Visando solucionar os problemas relativos a isso, é de suma importância a adoção de mecanismos que permitam a fácil portabilidade das técnicas implementadas.
- *Integração com ferramentas já existentes*: enquanto um padrão de interconexão não é adotado por todos os IDS existentes, desenvolver módulos que interajam com ferramentas já consagradas, servindo como *proxies* entre o IDS e tais ferramentas, é outro aspecto que pode gerar uma proteção mais abrangente.
- *Confiabilidade*: é evidente, principalmente em ambientes distribuídos, a preocupação em manter a confiabilidade de todos os módulos existentes no sistema, garantindo, no mínimo, um comportamento livre de falhas (fail-safe). Isso significa que, na falha de algum componente do sistema, todos os outros módulos fiquem cientes dessa condição e que alguma ação seja tomada no sentido de conduzir o sistema a um estado seguro, seja pela reativação do módulo perdido ou por um alerta relatado ao administrador, citando dois exemplos. Fica claro que, para a implementação de um IDS suficientemente robusto, o importante é manter um consenso sobre quais módulos estão ativos em determinado momento, assunto bastante debatido na área de tolerância a falhas (membership, comunicação de grupo, etc). O problema que persiste na adoção dessa tecnologia é o custo atrelado à maioria dos algoritmos desenvolvidos com esse fim, ponto de futuras discussões.

3 O Sistema Asgaard

Tomando por base os problemas e propostas citados na seção anterior, foi idealizado o Projeto Asgaard, voltado a criar uma solução própria para IDS e capaz de servir como base para o desenvolvimento de novos conceitos na área. Isso significou ir além dos conceitos de um IDS convencional, criando não uma ferramenta mas uma plataforma que possibilite, com o passar do tempo, agregar e testar novos módulos e técnicas. Em nenhum momento, no entanto, a solução proposta abdicou de características projetadas para sua utilização efetiva em situações reais, incluindo preocupações como desempenho e facilidade de administração, por exemplo.

Optou-se, então, por um sistema completamente distribuído, com características de tolerância a falhas, modular, de fácil portabilidade e com uma estrutura que permitisse a criação e teste de novas técnicas de detecção e de confinamento e avaliação, além da possível integração com ferramentas já existentes. Assim, muitos estudos poderiam ser realizados, integrando à segurança áreas como, por exemplo, tolerância a falhas (confiabilidade e distribuição dos módulos), redes (manutenção e desempenho), sistemas operacionais (otimização de rotinas de baixo nível) e inteligência artificial (métodos de detecção de intrusão).

A arquitetura do sistema Asgaard é baseada no conceito de módulos. Distribuídos por vários hosts de uma rede, esses módulos desempenham diferentes funções dentro do Asgaard, desde tarefas como coletar e analisar dados, consideradas atividades fim, até autenticar, controlar e efetivar a entrada e a saída de novos módulos, atividades meio. Para tanto, cada módulo Asgaard possui uma *infra-estrutura de comunicação*, que fornece primitivas de interação, confiabilidade e autenticação. Aliado a isso, todo módulo possui uma funcionalidade específica que define seu papel no sistema, situada imediatamente acima da *infra-estrutura de comunicação*. A existência dessas camadas básicas possibilita a integração entre os diferentes módulos criados, característica fundamental no sistema Asgaard e um dos avanços em relação a outros IDSs. A figura 1 mostra a arquitetura adotada.

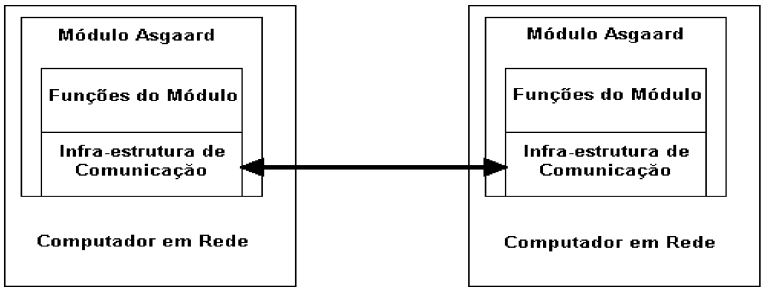

Fig.1. Representação gráfica da arquitetura do sistema Asgaard

Outra vantagem dessa estrutura é o fácil desenvolvimento de novos módulos, abstraindo funções básicas de comunicação e liberando o desenvolvedor para preocupar-se com detalhes específicos da funcionalidade do módulo. Além disso, portar módulos como analisadores e coletores para outros sistemas operacionais representa, simplesmente, adequar algumas funções da infra-estrutura de comunicação, com alterações mínimas na funcionalidade do módulo.

Dessa forma, com módulos distribuídos por vários pontos da rede e nos hosts mais importantes, fica facilitada a tarefa de detectar, investigar e reagir a possíveis ataques, aumentando a segurança do sistema. A medida que novos métodos de detecção e/ou mecanismos de segurança forem desenvolvidos, é possível a criação de módulos, com funcionalidades diferentes mas com a possibilidade de interação total com o restante da arquitetura, refletindo os novos avanços tecnológicos sem a necessidade de mudanças substanciais no IDS.

Embora dentro de uma rede exista a possibilidade de comunicação entre os diferentes módulos, componentes dispostos em redes distintas, com relações de confiança restritas, não podem trocar dados livremente. Essa é uma preocupação evidente com a segurança do sistema, evitando que redes mal administradas interfiram no bom funcionamento de outras. Por outro lado, é importante a existência de algum tipo de interação entre diferentes sistemas Asgaard, principalmente entre redes que mantenham certas relações de confiança. Isso permitiria a troca de informações importantes, como bases de assinaturas, ataques em andamento, dentre outros, facilitando a administração e possibilitando ações em conjunto no rastreamento ou análise de ataques. Essa funcionalidade foi incorporada ao sistema com o conceito de *domínios Asgaard*.

Um domínio Asgaard é a reunião de todos os módulos de uma dada rede, sem restrições de interação entre esses módulos. Em um mesmo domínio, todos os módulos comunicam-se diretamente entre si, sem nenhum tipo de hierarquia de comunicação. Além disso, todo módulo de um domínio passa, necessariamente, por um processo de autenticação antes de entrar em operação, evitando que módulos maliciosos sejam inseridos na arquitetura e interfiram em seu funcionamento. Essa tarefa de autenticação e de disparo de novos módulos é desempenhada por um componente especial, também no formato de módulo, chamado *Heimdal.* Cada máquina pertencente ao sistema, ou seja, que mantenha ao menos um módulo Asgaard, deve possuir um Heimdal em operação. Assim, todos as componente da arquitetura Asgaard são disparados pelo Heimdal responsável pela máquina, cuja responsabilidade de autenticação o torna o equivalente a uma CA (Certification Authority). A autenticação, por sua vez, é obtida através de funções criptográficas de hash, como SHA e MD5, bem como por algoritmos de assinatura digital, como DSS ou RSA [11].

Outra característica importante de um domínio é a existência de um outro módulo especial, chamado *Odin*. Único módulo autenticado manualmente, Odin é a CA principal de um domínio, responsável por autenticar todos os demais Heimdal desse domínio. Dessa forma, deve existir em cada domínio Asgaard no mínimo um Odin, responsável pelo bootstrap do processo de autenticação dos módulos.

Como citado acima, existe a possibilidade de interação entre diferentes domínios Asgaard, permitindo a troca de várias informações úteis. Essa interação, entretanto, não é feita diretamente entre os módulos de ambos os domínios, sendo necessário a figura de um módulo especialmente projetado para tal fim, chamado *Bifrost.* Responsável pela ligação entre diferentes domínios Asgaard, Bifrost realiza a autenticação de domínios confiáveis e o tratamento das informações trocadas, evitando que dados importantes sejam enviados a algum domínio malicioso ou mesmo interceptados.

Além desses, outros módulos especiais estão presentes na arquitetura Asgaard. Tarefas como a interface com o administrador, a interação com outros mecanismos de segurança (firewalls, por exemplo) e o repasse de dados de uma sub-rede para outra, no caso de redes separadas por algum dispositivo de filtragem ou por algum proxy, são exemplos de outros módulos especiais. A exemplo dos módulos convencionais, todos esses componentes especiais da arquitetura possuem a mesma infra-estrutura de comunicação, ilustrada na figura 2. Suas funções específicas encontram-se situadas sobre várias camadas, responsáveis por características como detecção de falhas, autenticação, etc. Todas essas camadas, por sua vez, baseiam-se em chamadas de sistema abstratas, ou seja, independentes de plataforma, facilitando a portabilidade de todo o sistema. Cada camada fornece serviços específicos às camadas adjacentes, isolando detalhes de implementação.

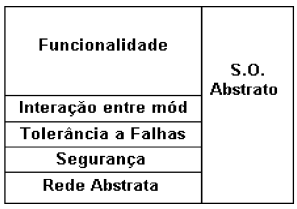

Fig. 2. Estrutura em camadas de um módulo Asgaard

A primeira camada descrita, chamada de *rede abstrata*, incorpora primitivas de comunicação simples, como send, receive, listen e broadcast. A exemplo da camada vertical de S.O. abstrato, esse nível foi projetado para isolar os detalhes de implementação e as peculiaridades de cada rede das camadas superiores, permitindo a mudança de tecnologias de rede empregadas como meio de comunicação sem interferir nas implementações já realizadas. Como especificação para o primeiro protótipo, essa camada simplesmente disponibiliza primitivas para o trabalho com sockets TCP/IP, eliminando toda a preocupação com criação ou destruição de sockets.

O nível de *S.O. abstrato*, por sua vez, isolará todas as camadas do sistema dos detalhes dependentes de sistema operacional. Com isso, migrar todo o sistema para uma nova plataforma significará praticamente substituir essa camada, sendo que todas as chamadas de sistema necessárias continuarão com a mesma interface para as demais camadas. O primeiro protótipo utiliza a plataforma Unix, mais precisamente o S.O. Linux.

A segunda camada horizontal, *segurança*, responde pelo sigilo e autenticidade das informações enviadas. Todas as mensagens trocadas pelos módulos Asgaard são cifradas de modo a evitar que algum agente (atacante ou modulo) malicioso interfira nas comunicações. Outra preocupação é com a autenticidade dessas mensagens. Como já citado, um protocolo de autenticação foi criado no Asgaard para garantir que os módulos ligados ao sistema são de procedência conhecida. Com isso, um atacante não poderá inserir módulos adulterados que interfiram no bom funcionamento do sistema sem que seja detectado. Essa camada disponibiliza algoritmos de criptografia, tanto de chave simétrica como assimétrica, algoritmos para geração de chaves de sessão, e a implementação do protocolo de autenticação.

A camada seguinte trata da *tolerância a falhas* dos módulos. Garantir que um modulo falho seja detectado em tempo hábil e de forma distribuída, evitando qualquer ataque que vise interromper ou degradar o funcionamento do IDS, é outra função primordial no Asgaard. Para tanto, técnicas de tolerância a falhas em sistemas distribuídos, como detetores de defeitos ou comunicação de grupo, devem estar inseridas neste nível.

Outra característica dessa camada é a manutenção de uma visão geral dos módulos existentes no sistema. Construir novas visões e atender as solicitações de novos módulos interessados em participar do IDS, são tarefas que complementam a funcionalidade da camada, podendo ser desempenhado em conjunto com as técnicas de detecção.

Por fim, a última camada da infra-estrutura de comunicação, chamada de *interação entre módulos*, é responsável pela interação entre os diferentes módulos funcionais, representados por diferentes sensores, analisadores, módulos de reação, etc. Esse problema vem sendo trabalhado, atualmente, por vários grupos de pesquisa, que tentam criar um padrão internacional para a troca de informações entre diferentes IDSs. Para permitir e facilitar uma futura adesão a esses padrões, esse nível fornecerá aos módulos do sistema uma interface padrão para comunicar possíveis alertas, eventos ou ações a serem desencadeadas.

A *funcionalidade* do módulo (camada superior da figura) define as tarefas específicas do mesmo. Essa é a camada de maior importância em toda estrutura, a atividade fim de cada módulo. Assim, uma grande diversidade de funções podem ser implementadas, como coletores, analisadores, módulos de reação, proxies, etc.

4 Considerações Finais

Campo de pesquisa recente, a detecção de intrusão ainda não atingiu a maturidade desejada em um mecanismo de segurança. Mesmo adotado em um número crescente de instituições, os sistemas de detecção de intrusão atuais não apresentam soluções para problemas como a sua própria resiliência, a privacidade das informações trocadas entre diferentes módulos do sistema e nem para a autenticidade dos mesmos. Além disso, problemas mais clássicos como o desempenho em altas taxas de transferência, a análise dos dados coletados (e a conseqüente diminuição de falsos positivos/negativos), a manutenção de grandes bases de assinatura ou de estatísticas apuradas de utilização, a resposta automática a determinados ataques, dentre outros, comprometem alguns sistemas. Muitos desses aspectos são alvos freqüentes de estudos, deixando inúmeras portas abertas para futuros trabalhos.

O sistema Asgaard tem como objetivo alavancar o desenvolvimento de conceitos ainda pouco discutidos na literatura atual, além de permitir a integração de diversas soluções para os problemas ainda em estudo. Com essa característica, desenvolver, testar e comparar, por exemplo, formas distintas de analisar um mesmo conjunto de dados coletados, reforça a importância de um sistema multiplataforma, modular e aberto no avanço dessa área.

Por outro lado, essa mesma modularidade e distribuição aliada a conceitos como autenticação, "survivability" e privacidade, capacitam o sistema Asgaard a ser empregado na mais variada gama de instituições, aliando esforços com outros mecanismo de segurança já empregados. Distribuir módulos coletores pela rede interna, posicionar analisadores e reatores em pontos-chave da estrutura, concentrar monitores e

gerenciadores e, até mesmo, interligar diferentes domínios Asgaard exemplifica a flexibilidade de uma ferramenta dessa natureza.

Vale a pena ressaltar, ainda, que mesmo com uma estrutura totalmente distribuída e com técnicas de tolerância a falhas embutidas, alguns problemas podem ser verificados. O particionamento da rede é um desses problemas. Um roteador que interliga diversas sub-redes pode apresentar um defeito em uma de suas portas, por exemplo, deixando isolada justamente aquela sub-rede que mantinha máquinas especializadas em coletar dados dos outros segmentos e gerar informações sobre a ocorrência ou não de um ataque (analisadores). Até que os outros módulos do sistema detectem essa falha e que esses analisadores sejam disparados em outra sub-rede, toda a rede estará a mercê de um atacante oportunista. Uma solução possível para esse problema seria a replicação de módulos importantes em todas os segmentos de uma rede, aumentando o nível de segurança de toda a instituição, reforçando a importância de um estudo cauteloso na distribuição e configuração do sistema.

Outro problema diretamente ligado à disposição e configuração dos diferentes módulos é o desempenho e a sobrecarga gerada pelo IDS. Analisadores e coletores distribuídos em máquinas separadas ou dispostos em redes diferentes certamente gerarão um número elevado de mensagens trocadas entre esses segmentos, podendo acarretar sérias conseqüências aos usuários normais. Avaliar as vantagens e desvantagens de uma total distribuição dos elementos da arquitetura Asgaard é uma tarefa importante a ser tomada em cada instalação, dependendo de características como largura de banda, dimensão, confiabilidade e, principalmente, nível de segurança exigido.

A estrutura atual das redes e seus serviços é extremamente vulnerável a ataques e falhas. Enquanto é impossível desenvolver uma ferramenta que resolva todas esses problemas eficientemente, as características do sistema Asgaard permitem que ele seja facilmente adaptado ou expandido para combater novas ameaças.

Referências

1. Roesch, M.: Snort: Lightweight Intrusion Detection for Networks. In: LISA, 13., november 1999. Proceedings... Seattle, 1999.
2. Asaka, M., Okazawa, S., Taguchi, A., Goto, S.: A Method of Tracing Intruders by Use of Mobile Agents. In: INET'99, June 1999. Proceedings... [S.l:s.n], 1999. (Disponível em http://www.ipa.go.jp:80/STC/IDA/paper/inet99.ps.gz)
3. Porras, P.A., Newmann, P.G.: EMERALD: Event monitoring enabling response to anomalous live disturbances. In: National Information Systems Security Conference (NISSC), 20., 1997, Baltimore. Proceedings... [Sl:s.n], 1997. (Disponível em http://www2.csl.sri.com/emerald/presentations/NISSC97/sld001.htm)
4. Lunt, T. F. et al.: A Real-Time Intrusion Detection Expert System (IDES). Menlo Park: Computer Science Laboratory, SRI International, 1992. (Disponível em http://www2.csl.sri.com/nides.index5.html)
5. Anderson, D., Frivold, T., Valdes, A.: Next-Generation Intrusion Detection Expert System (NIDES): A Summary. Menlo Park: Computer Science Laboratory, SRI International, 1995. (Disponível em http://www.sdl.sri.com/nides.index5.html)
6. Zamboni, D. et al.: An Architecture for Intrusion Detection Using Autonomous Agents. Technical Report 98/05. West Lafayette: COAST Laboratory, 1998. (Disponível em http://www.cs.purdue.edu/coast/projects/autonomous-agents.html)
7. Network Flight Recorder, Inc.: Step-by-Step Network Monitoring Using NFR [online]. NFR, 1998. (Disponível em http://www.nswc.navy.mil/ISSEC/CID/nfr.htm).
8. Cansian, A.: Desenvolvimento de um sistema adaptativo de detecção de intrusos em redes de computadores. São Carlos: USP, 1997.
9. Lee, W., Stolfo, S., Mok, K.: A data mining framework for building intrusion detection models. In: IEEE Symposium on Security and Privacy, 1997. Proceedings... [Sl:s.n], 1999.
10. Forrest, S., Hofmeyr, S.A., Somayaji, A.: Computer Immunology. Communications of the ACM, v. 40, n. 10, p. 80-96, October 1997. (Disponível em http://www.cs.unm.edu/~forrest/papers.html)
11. Schneier, B.: Applied Cryptography. 2 ed. John Willey & Sons, 1996.