Detecção de Intrusões com Auxílio de Agentes Móveis

FRANCISCO GOMES MILAGRES

ORIENTADOR:
PROF. DR. EDSON DOS SANTOS MOREIRA

USP – Universidade de São Paulo
ICMC – Instituto de Ciências Matemáticas e de Computação
SCE – Departamento de Computação e Estatística
Laboratório Intermídia
Cx. Postal 668 – CEP 13560-970 – São Carlos, SP
francisco@milagres.com
edson@icmc.sc.usp.br

Resumo: Este artigo traça um novo perfil de segurança, visando a segurança ativa e de proteção contra invasores de origem tanto externa quanto interna a sistemas protegidos e mostra uma visão geral e integrada de projetos em desenvolvimento por pesquisadores no Laboratório Intermídia do ICMC, USP de São Carlos, com apoio da FAPESP. Este perfil é a integração de sistemas de detecção de intrusão adaptativos com uso de agentes de software móveis integrados com tecnologias de firewall e detecção de intrusão.

Palavras Chave: segurança, detecção, intrusão, agentes, móveis.

1 Introdução

Aliada à necessidade de segurança em todas as divisões de uma corporação e à constante evolução das técnicas de auditoria, proteção e autenticação, os responsáveis por invasões às redes e modificações em web sites — os *crackers* — também se atualizam, quase sempre através dos mesmos meios usados pelos especialistas em proteção.

As pesquisas mais recentes divulgadas pelo *Computer Security Institute* [CSI, 2001] em conjunto com o FBI e a mais recente Pesquisa Nacional de Segurança da Informação [Módulo, 2000] divulgada pela *Módulo Security Solutions* mostram os destaques na mudança do cenário da segurança computacional e as preocupações que devem ser tomadas com os progressos dos intrusos lado a lado com a tecnologia de proteção.

O primeiro dos destaques de ambas as pesquisas é a crescente preocupação com os agentes criados pelos invasores para ocasionarem desde destruição de dados em computadores domésticos até permitirem acesso a registros de dados sigilosos para espionagem industrial, os vírus, que são a maior preocupação de 75% das empresas participantes da pesquisa nacional realizada pela Módulo.

Com o passar dos anos e a crescente conectividade, a via principal de contaminação por vírus também se alterou, saindo dos discos flexíveis e passando para as mensagens e arquivos trocados pela Internet. Apesar de quase a totalidade dos participantes desta pesquisa afirmarem que utilizam ferramentas de verificação antivírus, quase a metade delas já sofreu contaminação, sendo que aproximadamente 10% afirmaram nunca ter sofrido alguma contaminação.

A divulgação de senhas e a invasão por quebra de autenticação por meio de senhas são a segunda maior ameaça à segurança das empresas brasileiras que responderam à pesquisa da Módulo, com 57% do total. No entanto, as ameaças que se seguem são as que mais intrigam por, apesar de serem de origens diferentes, serem de valores bastante próximos.

Os *crackers* — geralmente chamados também de *hackers* — são responsáveis por 44% dentre as maiores preocupações das corporações para a segurança. Os funcionários insatisfeitos, responsáveis geralmente por invasões internas e facilitações de invasões externas, são os seguintes nesta lista de preocupações, com total de 42%.

Na pesquisa realizada pelo Computer Security Institute, com empresas norte-americanas, aproximadamente 40% das entrevistadas destacaram a Internet como principal canal utilizado para invasões, enquanto 34% apontaram os sistemas internos à própria corporação como ponto de entrada para os *crackers*.

Com este crescente aumento no número de ataques internos e a necessidade de proteção tanto externa como interna da corporação, a utilização de mecanismos como o *firewall* deve ser ampliada. Visto que este tipo de ataque, ocasionado pelos próprios usuários do sistema, não permite a localização imediata, torna-se necessário o uso integrado de diversas tecnologias para aumentar a capacidade de defesa, seja de uma corporação ou de um usuário doméstico.

Entre estas tecnologias, torna-se cada vez mais necessária a presença de mecanismos que acrescentem características de mobilidade no processo de monitoria do sistema. Desta forma, a introdução de agentes móveis em apoio à segurança computacional apresenta-se como uma solução natural, uma vez que permitirá a distribuição de tarefas de monitoria do sistema e a agilização no processo de tomada de decisão no caso de ausência do administrador [Milagres, 2001].

2 Agentes Móveis e Autônomos

O grau de proteção contra cada ação maliciosa está diretamente relacionado ao tempo e esforços gastos construindo e gerenciando os sistemas de segurança. Utilizando-se complexas ferramentas que continuamente monitoram e notificam atividades suspeitas, é possível identificar um ataque no momento em que está em curso. Entretanto, isso envolve um alto custo em termos de tempo e dinheiro na construção e gerenciamento de sistemas de monitoria. Esses sistemas também impõem penalidades de performance no ambiente que está sendo protegido, o que pode ocasionar a sua rejeição pelos usuários.

A arquitetura monolítica de Sistemas de Detecção de Intrusão (SDI), comumente utilizada em sistemas comerciais ou de pesquisa, apresenta um número de problemas que limitam sua capacidade de configuração, escalabilidade ou eficiência [Crosbie, 1995a] [Crosbie, 1995b].

A seguir será apresenta a modelagem apresentada por Mauro César Bernardes para o desenvolvimento de um Sistema de Detecção de Intrusão não-monolítico baseado em agentes móveis [Bernardes, 2000], bem como seu relacionamento com o projeto de pesquisa em desenvolvimento no instituto.

3 As Vantagens de um Sistema de Detecção de Intrusão Não-Monolítico

A abordagem monolítica apresenta alguns problemas práticos. Se uma nova forma de intrusão não prevista no sistema é descoberta - fato que ocorrem cada dia com maior freqüência - o SDI deve ser completamente reconstruído para conseguir tratá-la e isso, com certeza, não é uma ação trivial.

Outra preocupação diz respeito à tolerância à falhas, uma vez que um sistema monolítico apresenta-se como um único ponto de falha e ataques. Conseqüentemente, metodologias de ataques bem conhecidas (como por exemplo, ataques de *Denial of Service*), quando lançadas contra a máquina que hospeda o SDI, podem comprometer a integridade do sistema.

A utilização de agentes autônomos tem sido proposta por alguns autores como uma forma de se construir sistemas de detecção de intrusão não-monolíticos, entre eles, do grupo AAFID (*Autonomous Agents for Intrusion Detection*) do Cerias/Purdue University [Cerias, 2001], entre outros. A capacidade dos agentes autônomos de manterem informações específicas do seu domínio de aplicação, nesse caso, aplicação de segurança, dá a estes agentes, e conseqüentemente a todo o sistema, grande flexibilidade e facilidade de administração.

Em vez de um grande módulo monolítico, a proposta apresentada é de uma abordagem modular baseada em agentes autônomos e móveis para o desenvolvimento de um SDI. Este sistema consiste em um conjunto de pequenos processos (agentes) que podem agir independentemente no ambiente em construção. Eles são desenvolvidos para se moverem pelo ambiente no qual está inserido, observarem os comportamentos do sistema, cooperarem uns com os outros via passagem de mensagens, notificarem quando uma ação for considerada suspeita e, ainda, proverem ações reativas (contra-ataque).

Cada agente observa somente um pequeno aspecto de todo o sistema. Um simples agente, sozinho, não pode formar um sistema de detecção de intrusão, uma vez que sua visão é limitada a pequena "fatia" do sistema. Entretanto, se muitos agentes operam em um sistema e cooperam entre si, então um poderoso SDI pode ser desenvolvido. Uma vez que os agentes são independentes, eles podem ser adicionados e removidos do sistema

dinamicamente, de forma que não é necessário reconstruir todo o SDI ou, ainda, interromper suas atividades. Assim, a qualquer sinal de identificação de uma nova forma de ataque, novos agentes especializados podem ser desenvolvidos, adicionados ao sistema e configurados para atender a uma política de segurança ou ação específica.

Outra vantagem da abordagem descrita é a facilidade de configuração apresentada pelo sistema em atendimento às necessidades políticas do ambiente ao qual está inserido. Isso se torna uma característica importante uma vez que, conforme as diferentes políticas de segurança nas corporações e suas interpretações, o que é considerado uma quebra de segurança para um ambiente pode não ser em outro, em função do tipo de informação que se quer proteger e em função da empresa e setor onde a segurança está sendo feita.

Uma vez que a mudança é subjacente a todo trabalho de software e que esta é inevitável quando se constrói sistemas baseados em computador, outra vantagem deste sistema é a sua alta manutenibilidade. Definida qualitativamente na normatização de engenharia de software como sendo a facilidade com que um software pode ser compreendido e mantido, esta se torna a meta primordial que orienta os passos de um processo de engenharia de um software.

Sendo dividido em módulos contendo um conjunto de pequenos agentes especializados em uma única função e que conseqüentemente apresentam uma menor complexidade lógica, o sistema procura minimizar o esforço gasto com a manutenibilidade. Isso se deve ao fato de que, desta forma, cada agente apresenta uma estrutura bem compreensível, facilitando o seu entendimento e conseqüentes necessidades de manutenção. Isso é refletido diretamente em termos de:

- Tempo de reconhecimento do problema;
- Tempo de análise do problema;
- Tempo de especificação das mudanças;
- Tempo de correção (ou modificação) ativa;
- Tempo de testes locais;
- Tempo de testes globais;
- Tempo de revisão de manutenção;
- Tempo de recuperação total.

Cada uma das métricas anteriores pode, de fato, ser registrada sem grandes dificuldades. Além dessas medidas orientadas para o tempo, a manutenibilidade pode ser medida indiretamente ao considerarmos as medidas da estrutura do projeto e as métricas da complexidade do sistema as quais indicarão também um ganho significativo no momento da inserção de novas funções e conseqüentemente de novos agentes.

Além dessas vantagens, os pesquisadores do AAFID especificam um sistema baseado em agentes autônomos no qual as capacidades dos agentes são modificadas por meio do uso de algoritmos genéticos. Os autores reconhecem, entre outras, as seguintes vantagens de sistemas baseados em agentes autônomos sobre sistemas monolíticos:

- Fácil configuração: uma vez que é possível ter uma série de pequenos agentes especializados em tarefas específicas de detecção, o sistema de detecção pode ser configurado da forma mais adequada para cada caso; a adição e remoção de agentes do sistema são facilitadas;
- Eficiência: agentes podem ser treinados previamente e otimizados para que realizem suas tarefas de maneira a gerar a menor sobrecarga possível no sistema;
- Distribuição da vigilância: um sistema de agentes pode ser facilmente modificado para operar em rede e permitir migração para rastrear comportamentos anômalos através da rede, ou mover para máquinas onde eles possam ser mais úteis. A monitoria interna do sistema também pode ser destacada, já que estatisticamente, a segurança externa é mais reforçada e o maior número de ataques possuem origem interna;
- Resistência à subversão: caso um sistema de defesa seja subvertido, ele poderá dar a falsa sensação de segurança. Entretanto, isto se torna mais difícil, pois os conhecimentos adquiridos de um agente não fornecem o conhecimento das operações de outros, visto que eles desempenham funções diferentes;
- Escalabilidade: para atuar em sistemas maiores, basta adicionar mais agentes e aumentar sua diversidade.

4 SDI Baseado em Agentes Autônomos e Móveis

O principal conceito que envolve o SDI baseado em agentes autônomos e móveis é a simplicidade. Cada agente é uma entidade simples que irá desempenhar uma atividade específica e cooperar com outros agentes, da forma mais eficiente possível. Quando uma atividade for considerada suspeita por um agente, ele irá comunicar aos demais agentes do sistema sua suspeita de possível intrusão. Neste momento, será acionado um agente (ou um conjunto deles) com maior grau de especialização naquele tipo de suspeita. Naturalmente um agente poderá cometer erro que será identificado por um agente com nível de especialização superior. Uma vez que um número maior de agentes suspeita de uma possível intrusão, uma mensagem pode ser enviada pedindo a intervenção de um operador humano (via alguns processos de monitoramento) e agentes de reação poderão ser acionados [Barrus, 1998] [Zamboni, 1995].

Isso demonstra que uma decisão deverá ser tomada em conjunto, já que nenhum agente possui a autoridade de identificar uma intrusão por conta própria. Essa decisão será tomada com base no consenso de vários agentes no sistema. Se somente um agente suspeita de uma intrusão, ele poderá ser ignorado após uma votação dos agentes envolvidos naquela suspeita. Entretanto, se mais de um agente suspeitam de um comportamento anômalo, então há uma maior probabilidade de ser uma intrusão potencial e, neste caso, poderá ser tomada a decisão de comunicar um operador humano ou acionar agentes especializados em contra ataque. Fica claro que certos eventos podem ser mais "importantes" neste esquema do que outros. Por exemplo, 50 falhas em tentativas de *login* como *root* receberá um grau de suspeita maior que uma conexão de *FTP* externa ao domínio monitorado.

Uma arquitetura para a introdução de agentes móveis em Sistemas Detecção de Intrusão foi introduzida por Bernardes e é apresentada na Figura 1. As camadas são numeradas a partir da camada de Vigilância (camada 1), e cada uma delas representa um grupo de tarefas específicas desempenhadas por agentes especializados nas funções desta camada. Por meio do mecanismo de troca de mensagens, um agente em uma camada aciona um ou mais agentes em uma camada superior. Em outras palavras, a camada N utiliza os serviços da camada N-1, desempenha suas funções e fornece serviços para a camada N+1.

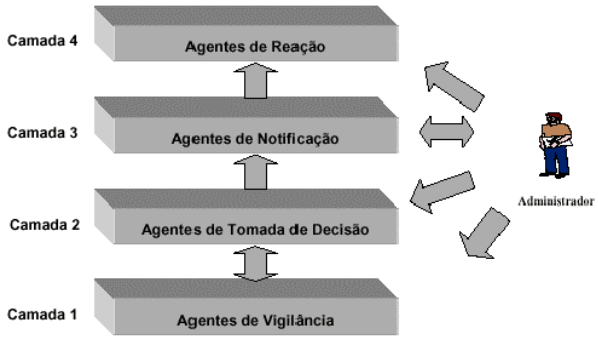

Figura 1: Arquitetura em camadas do SDI.

Com base em informações coletadas pelos *Agentes de Vigilânci*a, os *Agentes de Tomada de Decisão* entrarão em ação, analisando e identificando possíveis intrusões. Caso uma ação seja considerada suspeita por estes agentes, os *Agentes de Notificação* serão acionados e cuidarão de notificar o administrador da rede (via *e-mail*, *page*r, ligação telefônica, alarme, etc.) ou acionar os agentes de nível superior. Em último nível, encontram-se os *Agentes de Reaçã*o. Estes agentes cuidarão de contra-atacar automaticamente as possíveis intrusões com base nas informações dos agentes de notificação — como, por exemplo, aumentando o nível de segurança de um *firewall* e ativando *sniffers* — ou, ainda, serem acionados por meio de uma intervenção do administrador da rede.

Apesar do exemplo anterior destacar uma comunicação *bottom-up* através das camadas da arquitetura proposta, há a possibilidade de uma comunicação *top-down* entre a camada de tomada de decisão e a camada de vigilância. Temos, por exemplo, um cenário em que um *Agente de Tomada de Decisão*, após receber uma mensagem ou um conjunto de dados dos *Agentes de Vigilância*, poderá no momento em que desempenhar uma análise, necessitar de mais informações. Neste ponto, novos *Agentes de Vigilância* deverão ser acionados e mais informações deverão ser coletadas, na tentativa de se conseguir uma decisão com maior grau de certeza.

A ampliação do SDI para atender uma nova configuração de ataque pode envolver o desenvolvimento e conseqüente adição de novos agentes em uma única camada ou, ainda, a criação de um novo cenário que envolverá a adição de agentes em todas as camadas.

5 Pesquisas na Área

Entre os trabalhos em desenvolvimento no Laboratório Intermídia, encontram-se a modelagem do sistema de detecção de intrusão utilizando agentes móveis, a análise de ambientes servidores de agentes, a integração de sistemas de segurança com agentes e SMNP, a criação de novos cenários de execução do ambiente e pesquisas em novas formas de captura de dados.

Recentemente, o Cerias *(Center for Education and Research in Information Assurance and Security, Computer Science Department at Purdue Universit*y) [Cerias, 2001] disponibilizou uma implementação de um ambiente que segue as idéias do sistema proposto por Crosbie e Spafford [Crosbie, 1995a] [Crosbie, 1995b]. Este ambiente denominado *Autonomous Agents for Intrusion Detection* (AAFID) foi implementado utilizando-se a linguagem de *script*s Perl e diversos recursos de administração de sistemas e segurança comuns em ambiente UNIX.

O ambiente AAFID possui duas entidades distintas que suportam a execução dos agentes do sistema: *Transceivers* e *Monitor*s, sendo estes últimos entidades de nível mais alto que podem detectar possíveis eventos intrusivos não notados por entidades mais simples como *Transceiver*s. As informações preliminares sobre o sistema AAFID podem ser encontradas nas referências a seguir.

Outro trabalho na área de aplicação de agentes autônomos em sistemas de detecção de intrusão é apresentado por Barrus & Rowe [Barrus, 1998]. A idéia dos autores é utilizar agentes autônomos estáticos que se comunicam por meio de um sistema de mensagens de alerta em de uma arquitetura distribuída. Algumas abordagens interessantes sugeridas são: a utilização de agentes especializados na detecção baseada em anomalia, detecção baseada em uso indevido e a criação de objetos específicos para tratar os diversos tipos de ataque.

6 Referências

[Barrus, 1998] Barrus, J. & Rowe, N.C. "*A Distributed Automous-Agent Network-Intrusion Detection and Response System.*" Proceedings of the 1998 Command and Control Research and Technology. Monterrey CA, Jun-Jul 1998.

[Bernardes, 2000] Bernardes, M. C. "*Avaliação do Uso de Agentes Móveis em Segurança Computacional*". Dissertação de Mestrado, apresentada e defendida no ICMC/USP, 2000.

[Cerias, 2001] Cerias/Department of Computer Sciences, Purdue University. "*Autonomous Agents For Intrusion Detection Research Group.* " 2001 `http://www.cerias.purdue.edu/homes/aafid/`

[Crosbie, 1995a] Crosbie, M. & Spafford, E.H. *"Active Defense of a Computer System Using Autonomous Agents*". Department of Computer Sciences, Purdue University, 1995.

[Crosbie, 1995b] Crosbie, M. & Spafford, E.H. *"Defending a Computer System Using Autonomous Agents*". Department of Computer Sciences, Purdue University, 1995.

[CSI, 2001] CSI & FBI, "*Computer Crime and Security Survey 2001*." `http://www.gocsi.com`

[Milagres, 2001] Milagres, F. G. "*Mobilidade na Segurança Corporativa*". Developer's Magazine CEO. Fev-2001.

[Módulo, 2000] Módulo S. S., "*6ª Pesquisa Nacional Sobre Segurança da Informação, 2000*." `http://www.modulo.com.br`

[Zamboni, 1995] Zamboni, D. & Spafford, E. H. *"Autonomous Agents For Intrusion Detection*". Department of Computer Sciences, Purdue University, 1995.