SPOLM 2007

ISSN 2175-6295 Rio de Janeiro- Brasil, 08 e 09 novembro de 2007.

# USO DE TRILHAS DE AUDITORIA, CRIADAS POR SIMULAÇÃO, PARA AVALIAÇÃO DE TÉCNICAS DE DETECÇÃO DE INTRUSÃO

**Júlio Luiz Nunes Carvalho**
Centro de Análises de Sistemas Navais (CASNAV), Marinha do Brasil
Pça. Br. de Ladário, s/nº, Ilha das Cobras, Ed. 8, do AMRJ, 3º andar, Centro, Rio de Janeiro, 20.090-030
nunes@casnav.mar.mil.br
Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia (COPPE)
Universidade Federal do Rio de Janeiro (UFRJ)
juliolncarvalho@netbotanic.com.br

**Sergio Laranjeira da Cunha Lage**
Centro de Análises de Sistemas Navais, Marinha do Brasil
Pça. Br. de Ladário, s/nº, Ilha das Cobras, Ed. 8, do AMRJ, 3º andar, Centro, Rio de Janeiro, 20.090-030
sergio@casnav.mar.mil.br

## Resumo

Vigilância por detecção de intrusão pode ser um controle utilizado para o gerenciamento da segurança da informação nas organizações.

Apresentamos um estudo de técnicas de detecção, que podem ser usadas em sistemas reais de Módulos Criptográficos.

Este artigo descreve resultados obtidos de nosso módulo de detecção de intrusão baseado em variações do método proposto por [Forrest *et. al*. (1996)], onde trilhas de auditoria são criadas por simulação.

*Palavras-chave: Segurança da informação, detecção de intrusão, risco de ataque, simulação.*

## Abstract

Surveillance by intrusion detection can be a control used for information security management in the organizations.

We present a study of detection techniques, which can be used in real systems of Cryptographic Modules.

This paper describes results of our detection intrusion module based on variations of method proposed by [Forrest *et. al*. (1996)], where audit trails are created by simulation.

*Keywords: Information security, surveillance and intrusion detection, attack risk, simulation.*

## 1 - INTRODUÇÃO

Problemas de Proteção Digital e Vigilância de ambiente operacional de Módulos Criptográficos (**PDV-MC**) são problemas de interesse na Divisão de Gestão e Segurança da Informação do Centro de Análises de Sistemas Navais (CASNAV). Estes problemas são problemas de segurança de sistemas computacionais, cujas soluções devem proteger e vigiar o acesso a dados, informações e parâmetros de seguranças sensíveis, do ambiente operacional do Módulo Criptográfico em desenvolvimento. Uma boa prática é utilizar diferentes camadas de proteção e vigilância, por meio de procedimentos, métodos, modelos e mecanismos de segurança.

[Schneier (2000)] destaca que problemas de segurança de sistemas computacionais, como o PDV-MC, devem ser "solucionados" com um conjunto de processos de segurança, envolvendo aspectos organizacionais, tecnológicos e humanos, de modo que a falha de um processo não implique na perda total de segurança.

[Carvalho *et al.* (2005)] afirmam que sistemas computacionais de Módulos Criptográficos de infra-estruturas críticas, como os existentes na Infra-estrutura de Chaves Públicas Brasileiras (ICP-Brasil), devem ser plenamente auditáveis, de modo a verificar, por exemplo, por meio de testes de software (caixa-preta e caixa branca) o atendimento dos requisitos de segurança estabelecidos para o ambiente operacional do sistema.

De forma análoga, sistemas criptográficos em uso na Marinha devem ser considerados sistemas críticos. Por esta razão é interessante que sejam incorporados em tais sistemas, mecanismos, que possibilitem não somente uma auditabilidade das suas funcionalidades, como também do uso dos sistemas pelos seus diferentes usuários.

Neste trabalho foram definidas três (3) fronteiras para o estabelecimento de mecanismos de segurança do nosso **Pseudo Ambiente de Módulo Criptográfico (PA-MC)** em estudo, que para uma melhor compreensão são representadas esquematicamente na Figura 1 a seguir.

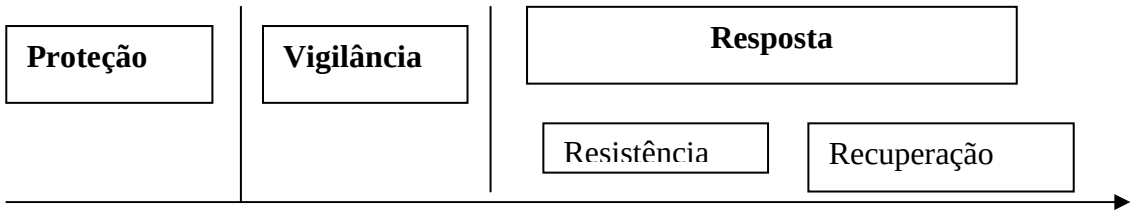


**Fig 1 - Exemplos de fronteiras de mecanismos de segurança do PA-MC**

Nas fronteiras de **proteção** do PA-MC são utilizados, por exemplo, mecanismos que limitem os privilégios dos usuários no PA-MC. Nas fronteiras de **vigilância** do PA-MC, por exemplo, são utilizados mecanismos que reconheçam sinais e atividades que representem riscos para o PA-MC. Nas fronteiras de **resposta** são executados procedimentos automatizados ou não, para neutralizar ataques identificados, ou se não for possível reduzir seu impacto.

O escopo principal deste estudo é propor um modelo de vigilância para o PA-MC, que possa ser aplicado em sistemas reais. Este modelo deve utilizar um conjunto de filtros para o reconhecimento de padrões de ataques existentes em trilhas de auditoria do PA-MC.

No nosso trabalho os padrões de ataques estão relacionados a violações de política de segurança que, por hipótese, são estabelecidas pelo "Engenheiro de Segurança" do PA-MC, por meio de um Banco de Assinaturas de ataque para o PA-MC.

Cenários de ataques fictícios são criados por simulação e experimentos computacionais mostram que a arquitetura de vigilância proposta é adequada para o processo de vigilância e para a resolução de parte do PDV-MC.

## 2 – CENÁRIO ATUAL

O problema da segurança da informação digital é um problema de grande relevância nas sociedades atuais, devido ao crescente uso da Tecnologia da Informação (TI), pois cada vez mais a informação digital é um "patrimônio" para as organizações.

De um lado, constata-se que a TI vem auxiliando a realização automatizada das diversas atividades associadas aos negócios ou campos de atuação das organizações. Por outro lado, estas crescentes automatizações (dos processos organizacionais) podem permitir a ocorrência de riscos de ataques ao ambiente computacional das organizações, permitindo, por exemplo, a revelação e/ou modificação não autorizada de informações digitais, bem como possibilitando algum tipo de fraude. Por esta razão, é imperioso o uso de controles, ou seja, medidas de segurança da informação de caráter técnico, organizacional ou humano para diminuir tais problemas, principalmente em sistemas críticos como os existentes em sistemas criptográficos.

De acordo com pesquisa de segurança da informação, realizada nos Estados Unidos, ameaças como vírus, acesso não autorizado, furto de *notebook* e roubo de informação proprietária das organizações são responsáveis por mais de 70 % das perdas financeiras das empresas [Gordon *et al.* (2006)].

No Brasil, pesquisas de empresas de segurança nacionais têm mostrado que, em regra, as empresas brasileiras têm tido dificuldades na identificação dos responsáveis por problemas nos seus ambientes computacionais. Surpreendentemente, quando as empresas conseguem identificar as fontes dos problemas, elas constatam que as falhas de segurança são causadas, principalmente, pelos próprios funcionários da empresa, seguida de atacantes externos e de vírus [Modulo- 10 PNSI (2006)].

Tais aspectos são uma motivação para a realização de pesquisas e estudos na área de segurança computacional, de modo a buscar soluções práticas para diagnosticar, por exemplo, procedimentos de mau-uso e/ou fraudulentos que possam ser realizados por usuários internos.

## 3 – O PROBLEMA DE DETECÇÃO DE INTRUSÃO

### 3.1 – Tecnologias Atuais de Detecção de Intrusão

[Denning (1987)], num dos trabalhos pioneiros na área de detecção de intrusão, considera importante o uso de sistemas de detecção de intrusão devido a quatro fatores principais:

Primeiro, a maioria dos sistemas computacionais possui vulnerabilidades, que podem possibilitar a ocorrência de intrusões e outras formas de abusos; segundo, em muitos casos os sistemas computacionais desenvolvidos, mesmo com falhas conhecidas, não são substituídos por sistemas mais seguros devido a razões econômicas da empresa responsável pelo desenvolvimento do sistema, pois a operação e o uso do sistema são mais importantes que a segurança em si; terceiro, o desenvolvimento de sistemas absolutamente seguros é muito difícil, o que, em regra, deve ser considerado impossível de ser atingido; e quarto, até mesmo os sistemas mais seguros são vulneráveis a abuso de usuário da organização, que utiliza os sistemas.

[Lee *et. al.* (2000)] define intrusão como "um conjunto de ações que tentam comprometer a integridade, confidencialidade e disponibilidade de um recurso computacional" e a segurança de um ambiente computacional é comprometida, quando uma intrusão acontece.

Para [Kent e Mell (2006)] a detecção de intrusão pode ser entendida como procedimentos de monitoramento que capturam e analisam eventos de um sistema computacional ou numa rede de computadores, de modo a verificar sinais de possíveis ataques. Estes sinais podem representar violações ou ameaças de violações: nas políticas de segurança do(s) sistema(s) computacional(ais) e/ou ambiente de rede; nas políticas de uso aceitável do(s) sistema(s) e/ou rede; e nos procedimentos de segurança estabelecidos para o(s)

sistema(s) e/ou rede.

Os citados autores consideram a prevenção de intrusão como procedimentos relacionados à detecção de intrusão e à tentativa de parar um ataque potencial detectado.

[Kent e Mell (2006)] afirmam ainda que as técnicas para favorecer a detecção e prevenção de intrusão podem armazenar informações relacionadas a eventos observados de um ou mais sistemas computacionais, bem como executar procedimentos para notificar os administradores de segurança.

As diversas técnicas que favorecem a detecção estão relacionadas a soluções de diversos problemas, tais como: problemas de identificação, onde o objetivo é classificar se o evento do sistema em estudo é intrusivo ou não; problemas de documentação de ameaças, onde táticas de ataques, que podem ser usadas para explorar o sistema em estudo, devem ser identificadas em um banco de dados de ataque conhecidos; e problemas de detecção de fraquezas do sistema, onde vulnerabilidades de configuração do sistema em estudo devem ser identificadas.

No estudo de [Kent e Mell, (2006)] são identificadas quatro tecnologias principais de Sistemas de Detecção e Prevenção de Intrusão, a saber: tecnologia baseada em rede – estes sistemas monitoram o tráfego de segmentos da rede corporativa, de modo a analisar as atividades dos protocolos de comunicações e identificar possíveis ataques; tecnologia baseada em rede sem fio (em inglês *wireless*) – estes sistemas monitoram o tráfego de redes sem fio, com a finalidade de analisar e identificar atividades suspeitas relacionadas aos protocolos de comunicações da rede sem fio; tecnologia baseada em rede com detecção anômala – estes sistemas examinam o tráfego de rede para identificar ameaças que geram fluxos de tráfego fora da normalidade, ou seja, anômalos, tais como aqueles produzidos por programas maliciosos de varredura, negação de serviço, dentre outros; e tecnologia baseada na máquina-hospedeira (*host*) **–** estes sistemas monitoram e analisam as características do ambiente de um único sistema e eventos, que ocorrem dentro dele, de modo a identificar atividades suspeitas e ataques.

[Kent e Mell (2006)] afirmam também que as tecnologias atuais de detecção e prevenção de intrusão diferem da forma de coletar, registrar e analisar as informações. Por esta razão algumas tecnologias podem identificar determinados eventos, que outras não podem, bem como detectar eventos com uma precisão melhor do que outras. Para os autores é interessante que as soluções desenvolvidas de detecção de intrusão combinem as diferentes tecnologias, bem como usem programas que integrem as informações de diferentes fontes de monitoramento, permitindo com isto uma análise mais eficaz.

Neste trabalho o interesse principal é estudar e/ou propor métodos e técnicas que possam ser utilizados em tecnologia baseada na máquina-hospedeira (*host*).

## 3.2 – Métodos e Técnicas de Detecção de Intrusão

Os métodos e técnicas de detecção são classificados, na literatura de detecção, em duas categorias principais definidas como detecção de mau-uso (em inglês *misuse detection*) e detecção de anomalia (em inglês *anomaly detection*) [Lee *et. al*. (2000)].

Na detecção de mau-uso (baseada na detecção de assinaturas) são usados métodos, técnicas e procedimentos de análise de dados, com o propósito de reconhecer em um determinado conjunto, dados de um ambiente computacional em estudo, a existência ou não de assinaturas de ataques no referido ambiente.

[Lee *et al.* (2000)] afirmam que alguns sistemas de detecção de intrusos, como IDIOT e STAT, usam padrões de ataques bem conhecidos para identificar as intrusões. Por exemplo, o ataque de adivinhar a senha poderia ser definido como um evento de quatro tentativas de acesso (login) sem sucesso num período de dois (2) minutos. Segundo os autores, a principal vantagem das técnicas de detecção de mau-uso é a precisão e eficácia em detectar ataques conhecidos. Entretanto, sua principal desvantagem é a dificuldade de detectar novos tipos de ataques.

**Na detecção anômala (baseada na detecção de anomalias)** são utilizados métodos, técnicas e procedimentos de análise de dados, com o propósito de identificar algum comportamento não comum ao sistema computacional. Estas técnicas trabalham com hipóteses e pressuposições, que o comportamento de um atacante difere do comportamento do usuário normal. A chave da detecção é, por exemplo, o estabelecimento de uma linha base de comportamento normal, através de observações do comportamento dos usuários e então, por meio de um indicador (ou seja, de uma métrica) poder reconhecer se o evento capturado possui valores ou atributos que desviam de um determinado valor ou faixa de valores. Este tipo de abordagem permite detectar táticas de ataques desconhecidas.

Segundo [Lee *et. al.* (2000)], sistemas de detecção de intrusos como IDES identificam as atividades observadas do usuário ou do sistema, que desviam das características (em inglês *profiles*) estabelecidas como "normais".

[Lee *et. al.* (2000)] afirmam ainda que, para os pesquisadores de técnicas de detecção de intrusão os maiores desafios são, sem sombra de dúvida, a detecção de novos ataques.

### 3.3 – Trabalhos Relacionados sobre Detecção de Intrusão

A abordagem deste estudo é baseada nos trabalhos de [Forrest *et al.* (1996)] e [Hofmeyer *et al.* (1998)].

[Forrest *et al.* (1996)] abordam o problema de detecção de intrusão em ambientes computacionais de forma análoga aos problemas enfrentados pelos sistemas imunológicos dos seres humanos, definido como problema de distinção das moléculas do tipo *self* (moléculas que não representam ameaças ao corpo humano) das moléculas do tipo *non-self* (moléculas que representam perigos e outros materiais não reconhecidos como pertencente ao corpo humano). O reconhecimento de uma molécula, como sendo do tipo *self* ou *non-self,* é feito pela verificação de seqüências de fragmentos de proteína, que são componentes de toda matéria viva. [Forrest *et al.* (1996)] escolheram seqüências curtas para serem observadas e utilizaram uma técnica definida como "olhar-para-frente no valor de 6" para a observação de anomalias no ambiente do sistema UNIX.

[Hofmeyer *et al.* (1998)], posteriormente, propuseram um método de detecção de anomalia a nível do processo do sistema UNIX com base nos estudos de [Forrest *e. al.* (1996)]. [Hofmeyer *et al.* (1998)] utilizaram para detecção de anomalia a técnica de "olhar-para-frente no valor de 10" associada a um discriminador de anomalia com base na "distância de Hamming". Os autores, embora considerem que nem todas as chamadas são representadas como eventos de auditoria, demonstraram que a coleta das seqüências de chamadas dos usuários por trilhas de auditoria é menos intrusiva do que a inclusão de um processo adicional de gravação das chamadas do sistema.

## 4 – VIGILÂNCIA POR FILTROS ANALISADORES

### 4.1 – Arquitetura Inicial

A arquitetura proposta para o PA-MC é baseada em três subprocessos principais: o primeiro trata da definição dos eventos de segurança do sistema; o segundo aborda o estabelecimento da Política de Segurança (PS), que é feito por meio de regras de segurança a serem cumpridas no PA-MC; e o terceiro trata dos mecanismos de reconhecimento quanto à "existência" ou "não" de padrão de assinaturas de ataque (ou seja, mau uso do sistema) nas trilhas de auditoria geradas pelos indivíduos que utilizam o PA-MC.

A arquitetura de vigilância proposta neste trabalho é uma arquitetura que deve permitir a incorporação de novos mecanismos de reconhecimento, não somente para assinaturas de ataques baseadas em regras (ou seja, violação de PS), como também tentar detectar "modificações dos padrões de ataques".

A idéia principal da arquitetura é integrar mecanismos, baseados em filtros de busca (reconhecimento) de um ou mais padrões de ataque (vide Figura 2), que detectem eventos a

serem “vigiados” e “analisados“ com maior cuidado, por parte do indivíduo que atua no papel de auditor do PA-MC.

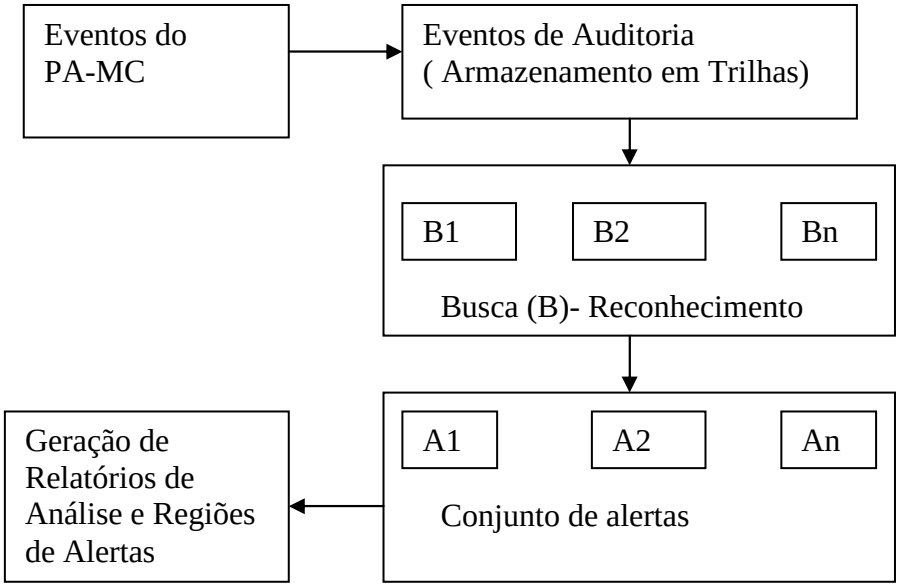


**Fig 2 - Exemplos de fronteiras de mecanismos de segurança do PA-MC**

## 4.2 – Metodologia de Trabalho

**Experimento 1**

No experimento 1 buscou-se criar cenários de ataques, por simulação, de modo a realizar técnicas de busca, com o propósito de identificar no pseudo ambiente teste, ou seja PA-MC Nr 1, não somente “seqüências iguais” aos padrões de assinatura de ataque definidos, como também “seqüências próximas”, que por hipótese deste trabalho, podem representar uma “evolução do ataque”, ou tentativa de ataque pelo possível atacante.

Para isto estendeu-se a análise inicialmente efetuada por [Hofmeyer *et al.* (1998)], que utiliza uma técnica de anomalia definida como “olhar-para-frente no valor de 10”, associada a um discriminador de anomalia com base na “distância de Hamming”, para uma técnica “olhar-para-frente no valor de k, onde k é o comprimento da assinatura de ataque. Os alertas são classificados k classes, que estão relacionadas respectivamente aos números de coincidências obtidos.

Uma regra heurística é estabelecida para definir um “Valor Recomendado para o número de coincidências, que, por hipótese, deve ser adequado para uma análise “manual” dos indivíduos no papel de auditor do PA-MC.

No experimento 1 as trilhas de auditoria têm 100.000 eventos, onde os eventos de auditoria são representados por caracteres alfabéticos. Os eventos não constantes dos caracteres das assinaturas de ataque são considerados eventos “neutros” e, em princípio, não devem representar riscos de ataques ao PA-MC.

O conjunto de assinaturas de ataques é formado por onze (11) tipos de assinaturas no tamanho de *k* caracteres seqüenciais, que são geradas de forma aleatória.

Convencionou-se que as assinaturas têm um tamanho de *k* caracteres seqüenciais, considerando que *k* assume valores de 5 a 11. Assim, a *assinatura nº 1* possui 5 caracteres; .a *assinatura n º 2* tem 6 caracteres; *a assinatura nº 3* , por sua vez, possui 7 caracteres; e assim sucessivamente, até a *assinatura nº 11*, que possui 15 caracteres.

**Experimento 2**

No experimento 2, criou-se cenários de ataques, por simulação, de modo a realizar técnicas de busca identificadas na literatura científica e estendê-las com a proposição de heurísticas, que possibilitem auxiliar o procedimento de análise do indivíduo no papel de auditor, por meio de quatro (4) buscas, a saber:

**Busca padrão**- implementa técnica "olhar-para-frente no valor de k", proposta inicialmente por [Forrest et al. (1996)], onde k é o comprimento da assinatura de ataque. Esta busca tem o objetivo de identificar a posição exata dos ataques verdadeiramente-positivos (ou seja, ataques que contêm todos os eventos de segurança na seqüência definida no Banco de Dados de assinatura de ataques). Esta busca é importante, pois possibilita verificar se os alertas das outras buscas estão próximos ou distantes dos ataques verdadeiramente-positivos;

**Busca 1** - técnica "olhar-para-frente no valor de k". Os alertas são classificados em k classes, que estão relacionadas respectivamente aos números de coincidências obtidos. O objetivo não é identificar os ataques verdadeiramente-positivos, mas definir alertas de interesse de análise de acordo com regra heurística para seleção do "valor recomendado" pelo indivíduo no papel de auditor do PA-MC;

**Busca 2** – Estendeu-se a técnica de segmentação de padrão proposta por [Forrest *et al.* (1996)], para elevar alertas relacionados, por hipótese, com três (3) eventos consecutivos relacionados às subseqüências das assinaturas de ataques. A análise das subseqüências mais freqüentes pode auxiliar o indivíduo, no papel de auditor do PA-MC, a fazer reflexões sobre a importância dos segmentos da assinatura de ataque e possíveis aspectos de vulnerabilidades do PA-MC que possam estar associados; e

**Busca 3** – Estendeu-se a técnica de segmentação de padrão proposta por [Forrest et al. (1996)], para elevar alertas relacionados, por hipótese, com uma heurística de decisão, que combina um (1) ou mais segmentos de assinaturas com três (3) eventos consecutivos. Esta abordagem permite detectar os alertas relacionados aos ataques verdadeiramente-positivos, como também outros alertas, que tenham um menor grau de coincidências.

Cabe aqui ressaltar que, neste trabalho, evento "verdadeiramente-positivo" é entendido como "ataque verdadeiro", classificado como "ataque" pelo módulo de detecção. Evento "falso-positivo" é entendido como um comportamento "normal do usuário", que é classificado como "ataque" pelo módulo de detecção. E, evento "falso-negativo" trata-se de um "ataque verdadeiro", no qual o módulo de detecção não classificou como "ataque".

A tabela 1 abaixo exemplifica uma matriz de cinco (5) assinaturas de ataque, definida manualmente para o experimento 2, onde os eventos de auditoria são representados por caracteres alfabéticos e uma assinatura de ataque por uma seqüência de eventos, tais como a seqüência "ABBBF", que representa a assinatura de ataque n º 1.

Tabela 1 - **Exemplo de Matriz de Assinaturas de Ataques**

| Evento de Segurança | Assinaturas de Ataques | | | | |
|---|---|---|---|---|---|
| | N º 1 | N º 2 | N º 3 | N º 4 | N º 5 |
| A | 1 | 1 | 3 | 3 | 3 |
| B | 3 | 3 | 1 | 0 | 0 |
| C | 0 | 0 | 0 | 0 | 0 |
| D | 0 | 1 | 0 | 1 | 0 |
| E | 0 | 0 | 1 | 1 | 0 |
| F | 1 | 1 | 0 | 1 | 3 |
| G | 0 | 1 | 1 | 1 | 1 |
| H | 0 | 0 | 0 | 1 | 0 |
| I | 0 | 1 | 1 | 1 | 0 |
| Comprimento da Assinatura | 5 | 8 | 7 | 9 | 7 |

## 5 – RESULTADOS

### 5.1 – Experimento 1

Nesta parte do trabalho são apresentados os resultados preliminares obtidos nas 500 corridas experimentais de cada uma das onze assinaturas de ataque.

Nosso objetivo foi o de analisar e verificar quais as "boas faixas" de valores de coincidência que devem ser usados para o levantamento de alarmes, em relação às diferentes assinaturas de ataque, de modo a não somente identificar os eventos "verdadeiramente-positivos" (100 % de coincidência), como também eventos "semelhantes".

Neste estudo, foi considerado, por hipótese, que o valor recomendado é o menor valor de coincidências, que resulta numa faixa de menor número de levantamento de alertas de detecção, onde o número médio de levantamento de alarmes deve ser superior a um determinado valor (no nosso experimento este número, por hipótese, terá que ser superior a cinco).

Tabela 2 - **Médias de Alarmes Levantados por Valor (es) de Coincidência e Valor Recomendado**

| **Valor Recomendado (VR)** | **Experimentos** |
|---|---|
| **VR = 3** | **T : 05** -> 17.408,39 (1) 1.449,89 (2) **60,27 (3)** 1,27 (4) 5,00 (5)<br>Valor Ideal (5) ...Valor Recomendado (3) ... Valores ruins (1, 2 e 4) |
| | **T : 06** -> 20.051,51 (1) 2.089,98 (2) **116,00 (3)** 3,61 (4) 0,06 (5) 5,00 (6)<br>Valor Ideal (6) ...Valor Recomendado (3) ... Valores ruins (1, 2, 4 e 5) |
| **VR = 4** | **T : 07** -> 22.458,55 (1) 2.808,79 (2) 194,74 (3) **7,98 (4)** 0,18 (5) 0,00 (6) 5,00 (7)<br>Valor Ideal (6) ..Valor Recomendado (4) ... Valores ruins (1, 2, 4 e 5) |
| | **T : 08** -> 24.640,22 (1) 3.594,32 (2) 299,42 (3) **15,47 (4)** 0,52 (5) 0,01(6) 0,00 (7) 5,00 (8)<br>Valor Ideal (8) ...Valor Recomendado (4) ... Valores ruins (1, 2, 5, 6 e 7) |
| | **T : 09** -> 26.612,29 (1) 4.436,01(2) 431,03 (3) **26,81 (4)** 1,17 (5) 0,03 (6) 0,00 (7) 0,00 (8) 5,00 (9)<br>Valor Ideal (9) ...Valor Recomendado (4) ... Valores ruins (1, 2, 5, 6, 7 e 8) |
| | **T : 10** -> 28.391,21 (1) 5.322,88 (2) 591,56 (3) **42,96 (4)** 2,28 (5) 0,07 (6) 0,00 (7) 0,00 (8) 0,00 (9) 5,00 (10)<br>Valor Ideal (10) ...Valor Recomendado (4) ... Valores ruins (1, 2, 5, 6, 7, 8 e 9) |
| | **T : 11** -> 29.980,05 (1) 6.245,22 (2) 781,55 (3) **65,00 (4)** 3,87(5) 0,17 (6) 0,00 (7) 0,00 (8) 0,00 (9) 0,00 (10) 5,00 (11)<br>Valor Ideal (11) ...Valor Recomendado (4) ... Valores ruins (1, 2, 5, 6, 7, 8, 9 e 10) |
| **VR = 5** | **T : 12** -> 31.400,37 (1) 7.189,80 (2) 1.000,44 (3) 93,32 (4) **6,31 (5**) 0,34 (6) 0,00 (7) 0,00 (8) 0,00 (9) 0,00 (10) 0,00 (11) 5,00 (12)<br>Valor Ideal (12) ...Valor Recomendado (5) ... Valores ruins (1, 2, 3, 5, 4, 6, 7, 8, 9, 10 e 11) |
| | **T : 13** -> 32.658,04 (1) 8.158,17 (2) 1.247,62 (3) 129,73 (4) **9,70 (5)** 0,59 (6) 0,02 (7) 0,00 (8) 0,00 (19) 0,00 (10) 0,00 (11) 0,00 (12) 5,00 (13)<br>Valor Ideal (13) ...Valor Recomendado (5) ... Valores ruins (1, 2, 3, 4, 6, 7, 8, 9, 10, 11 e 12) |

| | |
|---|---|
| | **T : 14** -> 33.768,24 (1) 9.135,77 (2) 1524,40 (3) 174,78 (4) **14,46 (5)** 0,97 (6) 0,03 (7) 0,00 (8) 0,00 (9) 0,00 (10) 0,00 (11) 0,00 (12) 0,00 (13) 5,00 (14)<br>Valor Ideal (14) .Valor Recomendado (5) ... Valores ruins (1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12 e 13) |
| | **T : 15** -> 34.729,23 (1) 10.120,17 (2) 1.827,33 (3) 229,29 (4) **20,92 (5)** 1,57 (6) 0,07 (7) 0,00 (8) 0,00 (9) 0,00 (10) 0,00 (11) 0,00 (12) 0,00 (13) 0,00 (14) 5,00 (15)<br>Valor Ideal (15) .Valor Recomendado (5) ... Valores ruins (1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 12, 14 e 15 |

## 5.2 – Experimento 2

Nesta parte do trabalho são apresentados os resultados do experimento número 2, obtidos em uma corrida experimental, com 110.000 eventos de auditoria, contendo 5 ocorrências da Assinatura Nº 1; 2 ocorrências da Assinatura Nº 2 ; 3 ocorrências Assinatura Nº 3 , 06 ocorrências da Assinatura Nº 4, e 1 ocorrência da Assinatura Nº 5.

Tabela 3 - **Resultados da Busca Padrão – Assinatura 1**

| Assinatura <ABBBF> | |
|---|---|
| # 1 -> 9065<br># 2 -> 12605<br># 3 -> 28696<br># 4 -> 51615<br># 5 -> 95456 | Foram levantados 5 alertas – correspondentes aos 5 ataques existentes na trilha de auditoria. |

Tabela 4 - **Resultados da Busca 1 – Assinatura 1**

| Assinatura <ABBBF> | |
|---|---|
| 1 coincidência (20 %) -> 17463 alertas<br>2 coincidências (40 %)-> 1511 alertas<br>**3 coincidências (60 %) -> 049 alertas**<br>4 coincidências (80 %) -> 003 alertas<br>5 coincidência – (100 ) > 005 alertas | Segundo a heurística estabelecida, existe interesse em analisar com mais detalhe 49 alertas, considerados tentativas de ataques ou ataques evolutivos. |

Tabela 5 - **Resultados da Busca 2 – Assinatura 1**

| Assinatura <ABBBF> | |
|---|---|
| **ABB -> 013**<br>BBB -> 012<br>BBF -> 011 | Foram localizados 36 segmentos de 3 eventos seguidos da assinatura 1. |

Tabela 6 - **Resultados da Busca 3 – Assinatura 1**

| Assinatura <ABBBF> | |
|---|---|
| # **1 -> 00009.065** - ABB<br># **2 -> 00012.605** - ABB<br>**# 3 -> 00028.696** - ABB<br># 4 -> 00041.909 - BBB<br>**# 5 -> 00051.615** - ABB<br># 6 -> 00054.438 - ABB | Foram levantados 9 alertas e detectados todos os cinco ataques verdadeiramente positivos<br>( # 1 -> 9065; # 2 -> 12605;<br># 3 -> 28696; # 4 -> 51615; e<br># 5 -> 95456) |

| | |
|---|---|
| **# 7 -> 00095.456** - ABB<br># 8 -> 00096.963 - ABB<br># 9 -> 00099.495 - ABB | |

Tabela 7 - **Resultados da Busca Padrão – Assinatura 2**

| Assinatura <ABBBDFGI> | |
|---|---|
| # 1 -> 54.438<br># 2 -> 99.495 | Foram levantados 2 alertas – correspondentes aos 2 ataques existentes na trilha de auditoria.. |

Tabela 8 - **Resultados da Busca 1 – Assinatura 2**

| Assinatura < ABBBDFGI > | |
|---|---|
| 1 coincidência (12,5 %) -> 24.628 alertas<br>2 coincidências ( 25 %) -> 3.622 alertas<br>3 coincidências (37,5 %) -> 302 alertas<br>**4 coincidências (50 %) -> 021 alertas**<br>5 coincidências (62 %) -> 002 alertas<br>6 coincidências (75 %) -> 000<br>7 coincidências (87 %) -> 000<br>8 coincidências (100 %) -> 002 alertas | Segundo a heurística estabelecida, existe interesse em analisar com mais detalhe 21 alertas, considerados tentativas de ataques ou ataques evolutivos. |

Tabela 9 - **Resultados da Busca 2 – Assinatura 2**

| Assinatura < ABBBDFGI > | |
|---|---|
| ABB -> 013<br>BBB -> 012<br>BBD -> 009<br>BDF -> 012<br>**DFG -> 016**<br>FGI -> 009 | Foram localizados 71 segmentos de 3 eventos seguidos da assinatura 2. |

Tabela 10 - **Resultados da Busca 3 – Assinatura 2**

| Assinatura < ABBBDFGI > | |
|---|---|
| # 1 -> 00009.065 - ABB<br># 2 -> 00012.605 - ABB<br># 3 -> 00020.619 - BDF<br># 4 -> 00028.696 - ABB<br># 5 -> 00041.909 - BBB<br># 6 -> 00051.615 - ABB<br>**# 7 -> 00054.438 - ABB**<br># 8 -> 00059.484 - DFG<br># 9 -> 00095.456 - ABB<br>**# 10 -> 00099.495 - ABB** | Foram levantados 10 alertas e detectados os dois ataques verdadeiramente positivos ( # 1 -> 54.438, # 2 -> 99.495) |

Tabela 11 - **Resultados da Busca Padrão – Assinatura 3**

| Assinatura < AAABEGI > | |
|---|---|
| # 1 -> 9.569<br># 2 -> 31.590<br># 3 -> 77.868 | Foram levantados 3 alertas – correspondentes aos 3 ataques existentes na trilha de auditoria. |

Tabela 12 - **Resultados da Busca 1 – Assinatura 3**

| Assinatura <AAABEGI> | |
|---|---|
| 1 coincidência (14,2 %) -> 22.284 alertas<br>2 coincidências (28,5 %) -> 2.942 alertas<br>3 coincidências (42,8 %) -> 206 alertas<br>**4 coincidências (57,1 %) -> 012 alertas**<br>5 coincidências (71,4 %)-> 000<br>6 coincidências (85,7 %) -> 000<br>7 coincidências (100 %) -> 003 alertas | Segundo a heurística estabelecida, existe interesse em analisar com mais detalhe 12 alertas, considerados tentativas de ataques ou ataques evolutivos. |

Tabela 13 - **Resultados da Busca 2 – Assinatura 3**

| Assinatura <AAABEGI> | |
|---|---|
| **AAA -> 022**<br>AAB -> 011<br>ABE -> 008<br>BEG -> 007<br>EGI -> 011 | Foram localizados 59 segmentos de 3 eventos seguidos da assinatura 3. |

Tabela 14 - **Resultados da Alertas Busca 3 – Assinatura 3**

| Assinatura <AAABEGI> | |
|---|---|
| **# 1 -> 00009569 - AAA**<br>**# 2 -> 00031590 - AAA**<br># 3 -> 00031.626 - AAA<br># 4 -> 00051.591 - ABE<br>**# 5-> 00077.868 - AAA** | Foram levantados 5 alertas e detectados os 3 ataques verdadeiramente positivos<br>( # 1 -> 9.569; # 2 -> 31.590;<br># 3 -> 77.868) |

Tabela 15 - **Resultados da Busca Padrão – Assinatura 4**

| Assinatura < AAADEFGHI> | |
|---|---|
| # 1 -> 27607<br># 2 -> 31627<br># 3 -> 41178<br># 4 -> 43205<br># 5 -> 94631<br># 6 -> 99545 | Foram levantados 6 alertas – correspondentes aos 6 ataques existentes na trilha de auditoria. |

Tabela 16 - **Resultados da Alertas Busca 1 – Assinatura 4**

| Assinatura < AAADEFGHI> | |
|---|---|
| 1 coincidência (11,1 %) -> 26340 alertas<br>2 coincidências (22,2 %) -> 4515 alertas | Segundo a heurística estabelecida, existe interesse em analisar com mais detalhe 24 |

| | |
|---|---|
| 3 coincidências (33,3 %) -> 470 alertas<br>**4 coincidências (44,4 %) -> 024 alertas**<br>5 coincidências (55,5 %) -> 001 alerta<br>6 coincidências (66,6 %) -> 000<br>7 coincidências (77,7 %)-> 000<br>8 coincidências (88,8 %)-> 000<br>9 coincidências (100,0 %) -> 006 alertas | alertas, considerados tentativas de ataques ou ataques evolutivos. |

Tabela 17 - **Resultados da Busca 2 – Assinatura 4**

| Assinatura < AAADEFGHI> | |
|---|---|
| **AAA -> 022**<br>AAD -> 009<br>ADE -> 010<br>DEF -> 013<br>EFG -> 013<br>FGH -> 011<br>GHI -> 008 | Foram localizados 86 segmentos de 3 eventos seguidos da assinatura 3. |

Tabela 18 - **Resultados da Alertas Busca 3 – Assinatura 4**

| Assinatura < AAADEFGHI> | |
|---|---|
| **# 1 -> 00027.607 - AAA**<br>**# 2 -> 00031.626 - AAA**<br>**# 3 -> 00041.178 - AAA**<br>**# 4 -> 00043.205 - AAA**<br># 5 -> 00044968 - EFG<br>**# 6 -> 00094.631 - AAA**<br>**# 7 -> 00099.545 - AAA** | Foram levantados 7 alertas e detectados os 5 ataques verdadeiramente positivos<br>(# 1 -> 27.607; # 2 -> 31.627, # 3 -> 41.178; # 4 -> 43.205; # 5 -> 94.631; # 6 -> 99.545) |

Tabela 19 - **Resultados da Busca Padrão – Assinatura 5**

| Assinatura < AAAFFFG> | |
|---|---|
| # 1 -> 71.998 | Foi levantado 6 alerta – correspondentes ao ataque existentes na trilha de auditoria. |

Tabela 20 - **Resultados da Busca 1 – Assinatura 5**

| Assinatura <AAAFFFG> | |
|---|---|
| 1 coincidência (14,2 %) -> 22.282 alertas<br>2 coincidências (28,5 %) -> 2.834 alertas<br>3 coincidências (42,8 %) -> 217 alertas<br>4 coincidências (57,1 %) -> 009 alertas<br>**5 coincidências (71,4 %)-> 006**<br>6 coincidências (85,7 %) -> 000<br>7 coincidências (100 %) -> 001 alerta | Segundo a heurística estabelecida, existe interesse em analisar com mais detalhe 6 alertas, considerados tentativas de ataques ou ataques evolutivos. |

Tabela 21 - **Resultados da Busca 2 – Assinatura 5**

| Assinatura <AAAFFFG> | |
|---|---|
| **AAA -> 022**<br>AAF -> 011<br>AFF -> 005<br>FFF -> 001<br>FFG -> 008 | Foram localizados 47 segmentos de 3 eventos seguidos da assinatura 3. |

Tabela 22 - **Resultados da Busca 3 – Assinatura 5**

| Assinatura <AAAFFFG> | |
|---|---|
| # 1 -> 00031.626 - AAA<br># 2 -> 00039.929 - AFF<br># 3 -> 00069.872 - AAA<br>**# 4 -> 00071.998 - AAA** | Foram levantados 4 alertas e detectado ataque verdadeiramente positivo;<br>(# 1 -> 71.998) |

## 6- CONCLUSÕES E TRABALHOS FUTUROS

### Considerações Iniciais

Este trabalho cria, por simulação, um ambiente de testes para avaliar um módulo de detecção de intrusão com base em assinaturas de ataques de tamanhos variados.

O método de detecção usado no nosso módulo é uma variante do método proposto [Forrest *et al.* (1996)] ("olhe-para-adiante tamanho 6"), onde são executados procedimentos de varredura de tamanho variável e são feitas comparações com um banco de dados de assinatura de ataque, ao invés de um banco de dados de assinaturas de comportamento normal dos usuários.

### Experimento 1

Como principal reflexão, constatou-se, no experimento 1, que o valor recomendado (VR) para a detecção de eventos "sensíveis", varia na faixa de 3 a 5 caracteres (vide tabela 2) para as assinaturas estudadas.

Ressalta-se que a nossa preocupação inicial do experimento 1 não foi a de identificar exatamente os eventos "verdadeiramente-positivos" e sim investigar, a partir do estabelecimento de um critério, eventos que pudessem ser classificados como "sensíveis", ou seja, eventos semelhantes às assinaturas de ataque estabelecidas.

Esta abordagem visa preencher lacunas da técnica de detecção por assinatura (100 % de coincidência), de modo a levantar alarmes para tentativas de ataques ou, por hipótese, para ataques evolutivos, que ainda não foram previstos pelo "Engenheiro de Segurança" do PA-MC.

### Experimento 2

Foram utilizadas quatro (4) buscas para o reconhecimento de padrões relacionados às cinco (5) assinaturas de ataques: a **busca padrão**: apresenta a característica de detectar exatamente se existe ou não este padrão de ataque na trilha analisada; a **busca 1**: apresenta a característica de detectar alertas de interesse de análise de acordo com regra heurística para seleção do "valor recomendado", por hipótese, maior que 5 (cinco); a **busca 2:** eleva alertas relacionados a três (3) eventos consecutivos das assinaturas de ataques, de forma a identificar a importância do segmento e possíveis vulnerabilidades; e a **busca 3**: eleva alertas associados a presença de segmentos consecutivos da assinatura de ataques, permitindo detectar os eventos "verdadeiramente-positivos" do PA-MC, bem como eventos relacionados a tentativas

de ataques, que mereçam a observação mais cuidadosa do indivíduo no papel de auditor do PA-MC.

**Uso da Simulação de Cenários de Ataques**

O uso de trilhas de auditoria criadas por simulação é interessante para desenvolver novas técnicas e/ou abordagens a serem aplicadas no nosso módulo de detecção, tendo como vantagens:

- Evitar o uso de dados sigilosos de sistemas reais;
- Usar modelagens de dados mais simples, pois os formatos internos das trilhas de auditoria podem ser feitos com uso de caracteres. Esta abordagem permite um melhor entendimento da "inteligência", ou seja, "chave para detecção" associada às técnicas de detecção utilizadas e/ou propostas para o nosso módulo de detecção.

**Consideração Final**

A arquitetura de vigilância proposta é adequada para resolver parte do problema (**PDV-MC**).

**Trabalhos Futuros**

Como trabalhos futuros, nós planejamos:

- Melhorar a qualidade de apresentação do protótipo desenvolvido;

Ampliar as funcionalidades do protótipo, de modo a possibilitar guardar diversos nomes de arquivos, tais como: trilha 1, trilha 2, ..., trilha <n>, bem como selecionar a busca ( padrão, 1, 2 e 3 para um destes arquivos);

- Estabelecer regras práticas para selecionar os "segmentos da assinatura de ataque mais freqüentes ou comuns", de modo a priorizar o reconhecimento de tais regiões da trilha de auditoria. Por exemplo, segmentos comuns a duas assinaturas de ataques; e
- Acrescentar à busca 3, uma nova busca com segmentos diferentes de 3 eventos consecutivos, por exemplo, segmentos com 2 ou 4 eventos consecutivos, de modo a verificar a melhoria ou degradação do procedimento de reconhecimento de violações das políticas de segurança.

## 6- BIBLIOGRAFIA

**[Carvalho *et al.* (2005)]** – CARVALHO, Júlio Luiz Nunes, SAISSE, Nilmar de Carvalho, MOREIRA, Jefferson Brandão. *O Papel do Sofware Livre para o Desenvolvimento do Módulo de Segurança Criptográfica (HSM- Hardware Security Module) para a AC-Raiz da ICP-Brasil*. Painel apresentado na Conferência de Segurança para Governo – SECGov BRASIL, 2005.

**[Denning, 1987]** - DENNING, Dorothy. "An Intrusion-Detection Model". IEEE Transactions on Software Engineering, Vol. SE-13, No. 2, 1987.

**[Forrest *et. al.* (1996]** – FORREST, S., HOFMEYER, S.A., SOMAYAJI, A. "A sense of self for unix processes". In Proceedings of the 1996 IEEE Symposium on Research in Security and Privacy, 1996.

**[Gordon *et al*. (2006)].** GORDON, Lawrence A., LOEB, Martin P., LUCYSHYN, William e RICHARDSON, Robert. *2006 CSI/FBI Computer Crime and Security Survey*, 2006.

**[Hofmeyer *et al*. (1998)]** – HOFMEYER, Steven A., FORREST, Stephanie, SOMAYAJI, Anil. " Intrusion Detection using Sequences of System Calls", Journal of Computer Security, 6 (3): 151-180, 1998.

**[Kent e Mell (2006)]** – KENT, Karen. MELL, Peter. National Institute of Standards and Technology (NIST). *Guide to Intrusion Detection and Prevention (IDP) System (Draft) - Recommendations of National Institute of Standards and Technology (NIST),* 2006.

**[Lee *et al*. (2000)]** – LEE, Wenke; NIMBALKAR, Rahul A.; YEE, Kam; PATIL, Sunil B.; DESAI, Pragneshkumar H.; TRAN, Thuan T.; e STOLFO, Salvatore. "A Data Mining and CIDF Based Approach for Detecting Novel and Distributed Intrusions". Recent advances in intrusion detection: third international workshop; proceedings / RAID 2000, Hervé Debar (ed.) – London: Springer, 2000.

**[Modulo- 10 PNSI (2006)] -** Módulo Technology for Risk Management – *10ª Pesquisa Nacional de Segurança da Informação*, 2006.
Disponível em: < http://www.modulo.com.br>

**[Schneier (2000)]** – SCHNEIER, Bruce. *The Process of Security*, Information Security Magazine, 2000.