Listas de conteúdo disponíveis no SciVerse ScienceDirect

Journal of Network and Computer Applications

Página inicial da revista: www.elsevier.com/locate/jnca

Revisão

Sistema de detecção de intrusão: Uma revisão abrangente

Hung-Jen Liao[a], Chun-Hung Richard Lin[a,n], Ying-Chih Lin[a,b], Kuang-Yuan Tung[a]

[a] *Departamento de Ciência da Computação e Engenharia, Universidade Nacional Sun Yat-Sen, No. 70, Lien-hai Rd., 80424 Kaohsiung, Taiwan, ROC*

[b] *Departamento de Ciência da Computação e Engenharia da Informação, Cheng Shiu University, No. 840, Cheng-cing Rd., 83347 Kaohsiung, Taiwan, ROC*

ARTICLEINFO

Histórico do artigo:
Recebido em 25 de abril
de 2012 Recebido em
formato revisado em 27
de agosto de 2012
Aceito em 11 de setembro de 2012
Disponível on-line em 23 de setembro de 2012

Palavras-chave:
Detecção de
intrusão Anomalia
Uso indevido

ABSTRACT

Com o aumento da taxa de transferência da rede e das ameaças à segurança, o estudo dos sistemas de detecção de intrusão (IDSs) tem recebido muita atenção no campo da ciência da computação. Os IDSs atuais apresentam desafios não apenas em relação às categorias de intrusão caprichosas, mas também ao enorme poder computacional. Embora existam várias literaturas sobre questões de IDS, tentamos fornecer uma imagem mais elaborada para uma análise abrangente. Por meio de uma pesquisa abrangente e de uma organização sofisticada, propomos a taxonomia para delinear os IDSs modernos. Além disso, as tabelas e as figuras que resumimos no conteúdo contribuem para a fácil compreensão do quadro geral dos IDSs.

Conteúdo

1. Introdução

3W?>Nas últimas décadas, a Internet e os sistemas de computador levantaram vários problemas de segurança devido ao uso explosivo das redes. As estatísticas do CERT (CERT) relatam que a quantidade de invasões tem aumentado excessivamente a cada ano. Qualquer invasão ou ataque mal-intencionado às vulnerabilidades da rede, aos computadores ou aos sistemas de informações pode causar sérios desastres e violar as políticas de segurança do computador, ou seja, *Confidencialidade, Integridade e Disponibilidade* (CIA). Até o momento, as ameaças à segurança da rede e das informações ainda são questões de pesquisa importantes. Embora haja uma série de literaturas existentes para pesquisar o IDS e seus

[n] Autor correspondente. Tel: +886 7 5252000x4339; fax: + 886 7 5254301.
Endereços de e-mail: hjliao@cse.nsysu.edu.tw (H.-J. Liao), lin@cse.nsysu.edu.tw (C.-H. Richard Lin), yclin@cse.nsysu.edu.tw (Y.-C. Lin), beck@cse.nsysu.edu.tw (K.-Y. Tung).

taxonomia (Denning, 1987; Lunt, 1993; Mukherjee et al., 1994; Debar et al., 1999; Axelsson, 2000; Mishra et al., 2004; Krugel e Toth, 2000; Jones e Sielken, 2000; Debar et al., 2000; Mukkamala e Sung, 2003; Estevez-Tapiador et al., 2004; Delgado et al, 2004; Kabiri e Ghorbani, 2005; Anantvalee e Wu, 2007; Patcha e Park, 2007; Tucker et al., 2007; Mandala et al., 2008; Garcia-Teodoro et al., 2009; Amer e Hamilton, 2010; Xie et al., 2011), tentamos dar uma imagem mais sistemática, arquitetônica e contemporânea para uma revisão abrangente.

Em primeiro lugar, fazemos uma distinção clara entre intrusão, detecção de intrusão, sistema de detecção de intrusão (IDS) e sistema de prevenção de intrusão (IPS). O NIST (Bace e Mell, 2001) descreve a intrusão como uma tentativa de comprometer a CIA ou de contornar os mecanismos de segurança de um computador ou rede; a detecção de intrusão é o processo de monitoramento dos eventos que ocorrem em um sistema ou rede de computadores e sua análise em busca de sinais de intrusão. As redes sem fio, em especial, ganharam recentemente uma implantação generalizada e são muito

1084-8045/$ - see front matter & 2012 Elsevier Ltd. Todos os direitos reservados.
http://dx.doi.org/10.1016/j.jnca.2012.09.004

mais fácil de atacar do que qualquer rede com fio. Em estudos recentes (Pelechrinis et al., 2011; Tan et al., 2011), muitos tipos de ataques de negação de serviço sem fio (WDoS) foram analisados. Portanto, categorizamos os IDS em tipos baseados em tecnologia sem fio e outros tipos de tecnologia. O sistema de detecção de intrusão é o sistema de software ou hardware para automatizar o processo de detecção de intrusão (Bace e Mell, 2001; Stavroulakis e Stamp, 2010). Além disso, o sistema de prevenção de intrusão (IPS) é o sistema que tem todos os recursos de IDS e pode tentar impedir possíveis incidentes (Stavroulakis e Stamp, 2010). Em alguns artigos, os termos sistema de detecção e prevenção de intrusões (IDPS) e IPS são sinônimos, sendo que o termo IDPS é raramente usado na comunidade de segurança. Neste documento, concentramo-nos na pesquisa e na classificação das técnicas relacionadas ao IDS e apresentamos uma breve comparação entre elas.

Por outro lado, a computação em nuvem aproveita as tecnologias existentes, como virtualização e computação distribuída, e surgiu recentemente como um novo paradigma para hospedagem e fornecimento de serviços pela Internet. A virtualização é uma tecnologia que abstrai os detalhes do hardware físico e oferece a capacidade de agrupar recursos de computação de clusters de servidores, armazenamentos e redes para aplicativos de alto nível. As plataformas de nuvem utilizam a tecnologia de virtualização para atingir o objetivo de fornecer recursos de computação como um utilitário. Portanto, também estudamos questões de segurança em *máquinas virtuais* (VMs).

O lembrete deste artigo está organizado da seguinte forma. Descrevemos as metodologias de IDS na Seção 2 e a classificação das abordagens de IDS na Seção 3. A Seção 4 apresenta quatro classes de tecnologias de IDS. Estudamos os problemas de IDS em VMs na Seção 5. Posteriormente, duas soluções orientadas por software, Snort e ClamAV, são estudadas na Seção 6, pois são as ferramentas de código aberto mais usadas. A Seção 7 traz nossa conclusão e apresenta desafios futuros.

2. Metodologias de detecção

As metodologias de detecção de intrusão são classificadas em três categorias principais: *Detecção baseada em assinatura* (SD), *Detecção baseada em anomalia* (AD) e *Análise de protocolo com estado* (SPA). A Tabela 1 mostra os prós e contras das três metodologias de detecção (Axelsson, 2000; Jones e Sielken, 2000; Debar et al., 2000; Stavroulakis e Stamp, 2010; Lazarevic et al., 2005; Xenakis et al., 2011). Suas descrições conceituais são as seguintes

A seguir: detecção baseada em assinatura (SD) - Uma assinatura é um padrão ou
string que corresponde a um ataque ou ameaça conhecida. SD é o processo
para comparar padrões com eventos capturados para reconhecer possíveis intrusões. Por usar o conhecimento acumulado por ataques específicos e vulnerabilidades do sistema, o SD também é conhecido como *Knowledge-*

Detecção baseada em anomalias ou *Detecção de uso indevido*.
Detecção baseada em anomalias (AD)
Uma anomalia é um desvio de um comportamento conhecido, e os perfis
representam os comportamentos normais ou esperados derivados de
monitoramento de atividades regulares, conexões de rede, hosts ou usuários durante um período de tempo. Os perfis podem ser estáticos ou dinâmicos e desenvolvidos para muitos atributos, por exemplo, tentativas de login com falha, uso do processador, contagem de e-mails enviados etc. Em seguida, o AD compara perfis normais com eventos observados para reconhecer ataques significativos. O AD também é chamado de *Detecção baseada em comportamento* em alguns artigos. Alguns exemplos de AD, por exemplo, tentativa de invasão, mascaramento, penetração por um usuário legítimo, *negação de serviço* (DOS), cavalo de Troia etc., são

Além disso, a análise de protocolo com estado (SPA) - O stateful no SPA indica que o IDS pode conhecer e rastrear os estados do protocolo (por exemplo,
emparelhamento de solicitações com respostas). Embora o processo SPA se pareça com o AD, eles são essencialmente diferentes. O AD adota perfis específicos de rede ou host pré-carregados, enquanto o SPA depende de perfis genéricos desenvolvidos pelo fornecedor para protocolos específicos. Em geral, os modelos de protocolo de rede no SPA são baseados originalmente em padrões de protocolo de organizações de padrões internacionais, por exemplo, IETF. A SPA também é conhecida como *Detecção baseada em especificação.* Híbrido - *A maioria dos* IDSs usa várias metodologias para oferecer uma detecção mais abrangente e precisa. Por exemplo, SD e AD são métodos complementares, porque o primeiro se refere a determinados ataques/ameaças e o segundo se concentra em ataques desconhecidos.

3. Abordagens de detecção

Tradicionalmente, as pessoas estudam as abordagens de detecção de intrusão a partir de dois pontos de vista principais, detecção de anomalias e detecção de uso indevido, mas não há diferença considerável em suas características. Stavroulakis e Stamp (2010) propuseram uma classificação para subdividir essas abordagens em três subcategorias, incluindo abordagem dependente de computação, inteligência artificial e conceitos biológicos. No entanto, essa classificação é muito difícil de visualizar todas as propriedades das abordagens de detecção. Considerando que há falta de uma visão mais detalhada das abordagens de detecção, apresentamos uma classificação de cinco subclasses com uma perspectiva aprofundada de suas características: Baseada em *estatísticas*, baseada *em padrões*, baseada em *regras*, *baseada em estados* e *baseada em heurística*. Com base nesse ponto de vista, apresentamos cuidadosamente as abordagens atuais de detecção de intrusão na Tabela 2.

O campo Série temporal na Tabela 2 indica se a abordagem mencionada considera ou não o comportamento da série temporal. O tipo de ataque que pode ser identificado por uma abordagem específica é apresentado no campo de detecção de ataques. O campo Desempenho indica a eficiência com que o IDS processa os eventos de auditoria, o que já foi discutido (Debar et al., 2000; Lazarevic et al., 2005). Além disso, o tipo de fonte contém dados de auditoria, perfil de usuário, políticas de segurança e conhecimento extraído de ataques anteriores. Esses dados disponíveis podem ser usados para discriminar comportamentos de intrusão de atividades suspeitas. Características mais especializadas para cada

Tabela 1
Prós e contras das metodologias de detecção de intrusão.

Baseado em assinatura (baseado em conhecimento)	Baseado em anomalias (baseado em comportamento)	Análise de protocolo com estado (baseado em especificações)
Prós		
• Método mais simples e eficaz para detectar ataques conhecidos.	• Análise contextual detalhada.	• Eficaz para detectar vulnerabilidades novas e imprevistas.

- Menos dependente do sistema operacional.
- Facilitar a detecção de abuso de privilégios.

- Conhecer e rastrear os estados do protocolo.
- Distinguir sequências inesperadas de comandos.

Contras

- Ineficaz para detectar ataques desconhecidos, ataques de evasão e variantes de ataques conhecidos.
- Pouca compreensão dos estados e protocolos.
- É difícil manter as assinaturas/padrões atualizados.
- Consome tempo para manter o conhecimento

- Precisão fraca dos perfis devido ao fato de os eventos observados serem constantemente alterados.
- Indisponível durante a reconstrução de perfis de comportamento.
- É difícil acionar alertas no momento certo.

- Consumo de recursos para rastreamento e exame do estado do protocolo.
- Não é possível inspecionar ataques com aparência de comportamentos de protocolo benignos.
- Pode ser incompatível com sistemas operacionais ou APs dedicados.

Tabela 2
Classificações e comparações de várias abordagens de detecção de intrusão.

	Abordagem de detecção	Detecção metodologia[a]			Tempo série	Tecnologia tipo[b]	Detecção de ataques[c]	Desempenho[d]	Tipo de fonte	Outros características
		AD	SD	SP						
Estatísticas com base	Estatísticas (Axelsson, 2000; Debar et al., 2000; Patcha e Park, 2007; Garcia-Teodoro et al., 2009; Xie et al., 2011; Murali e Rao, 2005; Sabahi e Movaghar, 2008; Lazarevic et al., 2005; Fragkiadakis et al., 2012; Mar et al., 2012)	○	○	-	✓	H/N	B	M	Dados de auditoria, usuário perfis, uso de disco e memória	Simples, mas menos precisão
	Baseado em distância (Patcha e Park, 2007; Murali e Rao, 2005; Sabahi e Movaghar, 2008; Lazarevic et al., 2005)	○	-	-	✓	N	U	M	Dados de auditoria, pacotes de rede	Em tempo real e ativo medição
	Baseado em Bayesian (Kabiri e Ghorbani, 2005; Patcha e Park, 2007; Garcia-Teodoro et al., 2009; Stavroulakis e Stamp, 2010; Lazarevic et al, 2005)	○	○	-	✓	N	B	H	Dados de auditoria, Prévia eventos, rede tráfego, usuário perfis	Ótimo estatística (probabilística) modelo
	Teoria dos jogos (Li et al., 2012; Paramasivan e Pitchai, 2011; Kantzavelou e Katsikas, 2010; Shena et al., 2011)	○	-	-	✓	H/N	U	L	Eventos do sistema ou incidentes, Registro eventos, bytes enviados	Estudo autônomo, o controle é fraco
Padrão com base	Correspondência de padrões (Debar et al., 1999; Axelsson, 2000; Krugel e Toth, 2000; Debar et al., 2000; Murali e Rao, 2005; Sabahi e Movaghar, 2008; Lazarevic et al., 2005; Kartit et al., 2012)	-	○	-	×	N	K	H	Registros de auditoria, assinaturas de ataques conhecidos	Simples, mas menos flexível
	Perti Net (Debar et al., 1999; Axelsson, 2000; Dexbar et al., 2000; Murali e Rao, 2005; Lazarevic et al., 2005)	-	○	-	✓	H	K	M	Registros de auditoria, definido pelo usuário intrusão conhecida assinaturas	Conceito simples e gráfico representação
	Monitoramento de pressionamento de teclas (Krugel-e Toth, 2000; Murali e Rao, 2005; Lazarevic et al., 2005)		○	-	✓	H	K	H	Registros de auditoria, perfis de usuário, registros de pressionamento de teclas	Usando o padrão de digitação
	Verificação do sistema de arquivos (Murali e Rao, 2005; Lazarevic et al., 2005)	○	○	-	×	H	B	H	Sistema// configuração/ Arquivos de usuário, registro arquivos,	Integridade do arquivo verificação
Regra com base	Baseado em regras (Axelsson, 2000; Krugel e Toth, 2000); Jones e Sielken, 2000; Xie et al., 2011; Stavroulakis e Stamp, 2010; Sabahi e Movaghar, 2008; Lazarevic et al., 2005; Farooqi et al., 2012; Modi et al., 2012; Wang et al., 2011)	○	○	-	×	H/N	B	H	aplicativos Registros de auditoria, padrões de regras dos perfis de usuário e política	Não é fácil criado e atualizado
	Mineração de dados (Kabiri e Ghorbani, 2005; Patcha e Park, 2007; Xie et al., 2011; Murali e Rao, 2005; Lazarevic et al., 2005)	○	○	-	×	N	B	M	Dados de auditoria, Base de conhecimento para associação descoberta de regras	Automaticamente gerada modelos Variado
	Baseado em modelo/perfil (Krugel e Toth, 2000; Murali e Rao, 2005; Sabahi e Movaghar, 2008; Lazarevic et al., 2005; Kartit et al., 2012)	○	-	-	×	H/N	U	M	Registros de auditoria, Perfis de usuário, Pacotes de rede, Perfis de AP	modelagem / criação de perfis métodos
	Máquina de vetor de suporte (SVM) (Modi et al., 2012; Kolias et al., 2011; Li et al., 2012; Horng et al, 2011)	○	○	-	✓	N	B	H	Amostra limitada dados, dados binários	Inferior falso taxa positiva, alta precisão
Estado-com base	Análise de transição de estado (Debar et al., 1999; Axelsson, 2000; Krugel e Toth, 2000; Jones e Sielken, 2000; Debar et al., 2000; Stavroulakis e Stamp, 2010; Murali e Rao, 2005; Sabahi e	-	○	-	✓	H/N	K	H	Registros de auditoria, Transição de estado diagrama de ataques conhecidos	Flexibilidade, Detectar através de sessões de usuário

	Movaghar, 2008; Lazarevic et al., 2005)									
	Identificação da intenção do usuário (Debar et al., 1999); Debar et al., 2000; Murali e Rao, 2005; Lazarevic et al., 2005)	○	-	-	✓	H	U	H	Registros de auditoria, perfis de usuário	Tarefa de alto nível padrão
	Modelo de processo de Markov (Patcha e Park, 2007; Garcia-Teodoro et al., 2009; Murali e Rao, 2005; Lazarevic et al., 2005; Couture, 2012; Li et al., 2012)	○	-	-	✓	H/N	U	M	Data da auditoria, Sequência de chamadas de sistema ou comandos.	Probabilístico, Auto-treinamento
	Análise de protocolo (Stavroulakis e Stamp, 2010; Murali e Rao, 2005; Sabahi e Movaghar, 2008; Lazarevic et al., 2005)	○	○	○	✓	P	T	L	Registros de auditoria, Log arquivo, Uso normal (Modelo) de um protocolo	Baixo falso taxa positiva, Menos eficaz
Heurística com base	Redes neurais (Axelsson, 2000; Patcha e Park, 2007; Stavroulakis e Stamp, 2010; Murali e Rao, 2005; Lazarevic et al., 2005; Mar et al., 2012; Modi et al., 2012; Wang et al., 2011)	○	○	-	✓	N	B	M	Dados de auditoria, Sequência de comandos, Prever eventos	Autoaprendizagem, Tolerância a falhas
	Lógica Fuzzy (Kabiri e Ghorbani, 2005; Patcha e Park, 2007; Garcia-Teodoro et al., 2009; Stavroulakis e Stamp, 2010; Mar et al., 2012; Modi et al., 2012)	○	-	-	×	H/N	U	H	Registros de auditoria, tráfego de rede (TCP/UDP/ICMP)	Configurável, escalável, flexível
	Algoritmo genético (Patcha e Park, 2007; Garcia-Teodoro et al., 2009; Murali e Rao, 2005;	-	○	-	✓	N	K	L	Dados de auditoria, ataques conhecidos	

Tabela 2 (*continuação*)

Abordagem de detecção	Detecção metodologia[a]			Tempo tipo de série[b]	Tecnologia	Detecção de ataques[c]	Desempenho[d]	Tipo de fonte	Outros características
	AD	SD	SP						
Lazarevic et al., 2005; Modi et al., 2012; Li et al, 2012; Sen e Clark, 2011)								expresso como padrões binários	Heurística e evolutivo aprendizado
Sistema imunológico (Debar et al., 1999; Debar et al, 2000; Stavroulakis e Stamp, 2010; Murali e Rao, 2005; Lazarevic et al., 2005)	○	○	-	J	H	B	M	Dados de auditoria, sequência de chamadas de sistema	Distribuído, alto nível geral segurança
Enxame inteligente (SI) (Kolias et al., 2011; Chung e Wahid, 2012; Alomari e Othman, 2012)	○	-	-	J	N	U	H	Rede dados de conexão, dados do arquivo de registro	Bio-inspirado computação inteligência

[a] Metodologia de detecção: detecção baseada em anomalia (AD), detecção baseada em assinatura (SD), análise de protocolo com estado (SP).
[b] Tipo de tecnologia: baseada em host (H), baseada em rede (N), baseada em protocolo (P).
[c] Detecção de ataques: ataques conhecidos (K), ataques desconhecidos (U), ataques conhecidos e desconhecidos (B), tripartite de AD, SD e SP (T).
[d] Desempenho: alto (H), moderado (M), baixo (L).

Tabela 3
Comparações de tipos de tecnologia de IDS.

Item	Tecnologia			
	HIDS	NIDS	WIDS	NBA
Componentes[a]	Agente: software (em linha) MS: 1 ~ *n* DS: 1 ~ *n* (opcional)	Sensor: *n* (em linha/passivo) MS: 1~ *n* DS: 1 ~ *n* (opcional)	Sensor: *n* (passivo) MS: 1 ~ *n* DS: 1 ~ *n* (opcional)	Sensor: *n* (mais passivo) MS: 1 ~ *n* (opcional) DS: opcional
Escopo da detecção do sensor/agente	Host único	Sub-rede de rede: *n* Host: *n*	WLAN: *n* Cliente WLAN: *n*	Sub-rede de rede: *n* Host: *n*
Arquitetura[b]	MN ou SN	MN	MN ou SN	MN ou SN
Pontos fortes	Somente os HIDS podem analisar os dados de ponta a ponta. acabar com as comunicações criptografadas atividade.	Capaz de analisar os mais amplos escopos dos protocolos AP	O WIDS é mais preciso devido à sua foco restrito. Somente o WIDS pode supervisionar o protocolo sem fio atividade.	Poderes de detecção superiores em varredura de reconhecimento, reconstruir o malware infecções e ataques de DoS
Limitações tecnológicas[c]	• Mais desafiador em precisão de detecção devido à falta de conhecimento do contexto • Atrasos na geração de alertas e relatórios centralizados • Consumir recursos do host • Conflito com os existentes controles de segurança	• Não é possível monitorar a rede sem fio protocolos • Altas taxas de falsos positivos e falsos negativos • Não é possível detectar ataques no tráfego criptografado • Não há suporte para análise completa sob altas cargas.	• Não é possível monitorar AL, TL e Atividades do protocolo NL. • Não é possível evitar técnicas de evasão. • Os sensores são suscetíveis a ataques de interferência física. • Não é possível compensar protocolos sem fio inseguros	• A principal limitação é a atraso na detecção de ataques, causado pela transferência de dados de fluxo para o NBA em lotes, mas não em tempo real.
Recursos de segurança				
Coleta de informações dispositivos (por exemplo, APs,	Tráfego de rede, chamadas de sistema, arquivos Hosts, SOs, APs, tráfego de rede. WLAN, atividade do sistema.		clientes).	Hosts, sistema operacional, serviços (IP, TCP, UDP, etc.).
Registro em log	Referência (Stavroulakis e Stamp, 2010)	Referência (Stavroulakis e Stamp, 2010)	Referência (Stavroulakis e Stamp, 2010)	Referência (Stavroulakis e Stamp, 2010)
Metodologia de detecção[d]	SD e AD (combinados)	SD (principal), AD e SPA	AD (maior), SD e SPA	AD (maior), SPA
Tipo de eventos suspeitos detectados	Tráfego de rede AL, TL e NL, registros de eventos (por exemplo, atividades de aplicativos, atividades do sistema de arquivos), Registros do sistema (por exemplo, configurações, violações, atividade do sistema operacional)	AL, TL, NL e HW reconhecimento e ataques, serviços de AP inesperados, política	Atividade de protocolo sem fio, WLAN e dispositivos inseguros, ataques DoS, varredura de rede, violações de políticas	AL, TL, NL fluxos de tráfego anômalos (ataques DoS, malware) serviços de AP inesperados, varredura de rede, violações de políticas

[a] Componentes: servidor de gerenciamento (MS), servidor de banco de dados (DS).
[b] Arquitetura de rede: redes gerenciadas (MN), redes padrão (SN).
[c] Limitações tecnológicas: aplicativo (AP), camada de aplicativo (AL), camada de transporte (TL), camada de rede (NL), hardware (HW), sistema operacional (OS).
[d] Metodologia de detecção: baseada em assinatura (SD), baseada em anomalia (AD), análise de protocolo com estado (SPA).

As técnicas mencionadas são enumeradas em outras características. A seguir, apresentamos uma breve visão geral das abordagens de detecção. As abordagens baseadas em estatísticas são feitas principalmente por meio de limites predefinidos, média e desvio padrão e probabilidades para identificar intrusões. A detecção baseada em padrões concentra-se em ataques conhecidos por meio da correspondência de strings . Além disso, as regras If-Then ou If-Then-Else são aplicadas em técnicas baseadas em regras para construir o

modelo e o perfil de intrusões conhecidas. Especialmente, os métodos baseados em estado exploram a máquina de estado finito derivada dos comportamentos da rede para identificar ataques. A última é a abordagem baseada em heurística, que é inspirada em conceitos biológicos e inteligência artificial. Trabalhos mais recentes (Fragkiadakis et al, 2012; Mar et al., 2012; Kartit et al., 2012; Farooqi et al.,2012; Modi et al., 2012; Wang et al., 2011; Couture, 2012; Li et al., 2012) integram várias abordagens de detecção de cinco subclasses em uma abordagem sofisticada para proporcionar melhor eficiência e menor taxa de alarme falso em relação às abordagens individuais.

4. Tipos de tecnologia

Atualmente, existem muitos tipos de tecnologias de IDS. Classificamos as tecnologias em quatro classes, de acordo com a

são implantados para inspecionar atividades suspeitas e que tipos de eventos podem reconhecer (Mukherjee et al., 1994; Stavroulakis e Stamp, 2010; Sabahi e Movaghar, 2008; Modi et al., 2012). As quatro classes da Tabela 3 são as seguintes: *IDS baseado em host* (HIDS), *IDS baseado em rede* (NIDS), *IDS baseado em rede sem fio* (WIDS), *análise de comportamento de rede* (NBA) e *IDS misto* (MIDS). Um HIDS monitora e coleta as características de hosts que contêm informações confidenciais, servidores que executam serviços públicos e atividades suspeitas. Um NIDS captura o tráfego de rede em segmentos de rede específicos por meio de sensores e, posteriormente, analisa as atividades de aplicativos e protocolos para reconhecer incidentes suspeitos. O WIDS é semelhante ao NIDS, mas captura o tráfego de rede sem fio, como redes ad hoc, redes de sensores sem fio e redes mesh sem fio. Além disso, um sistema NBA inspeciona o tráfego de rede para reconhecer ataques com fluxos de tráfego inesperados. A adoção de várias tecnologias como MIDS pode cumprir a meta de uma detecção mais completa e precisa.

Aqui estão descritas mais informações adicionais na Tabela 3. Os componentes do IDS incluem o sensor e o agente, sendo que o primeiro é normalmente usado pelos sistemas NIDS, WIDS e NBA para monitorar as redes, e o HIDS usa o segundo para monitorar e analisar as atividades. Tanto o sensor quanto o agente podem fornecer dados ao *Management Server (*MS) e ao *Database Server* (DS), sendo que o MS é um dispositivo centralizado para processar incidentes capturados e o DS é apenas um repositório que armazena informações de eventos. Além disso, há dois tipos de arquiteturas de rede. Uma é a *Managed Network* (MN), uma rede isolada implantada para o gerenciamento do software de segurança para ocultar as informações do IDS dos invasores. A MN aumenta os custos extras de hardware e traz alguns inconvenientes para os administradores. Outra é a *Rede Padrão* (SN), que é uma rede pública sem proteção. A maneira de melhorar a segurança da SN é criar uma rede virtual isolada configurando uma rede local virtual. Por outro lado, a maioria das tecnologias de IDS oferece quatro recursos comuns para manter a segurança, incluindo coleta de informações, registro, detecção e prevenção. A coleta de informações reúne informações sobre hosts/redes a partir de atividades observadas. O registro, os dados de registro relacionados aos eventos detectados, pode ser usado para validar os alertas e os incidentes investigados. As metodologias de detecção na maioria dos IDSs geralmente precisam de um ajuste sofisticado para obter maior precisão. Quanto à questão da prevenção, sugerimos que o leitor consulte o artigo da pesquisa (Stavroulakis e Stamp, 2010) para obter mais exposições excelentes. Uma desvantagem comum das tecnologias de IDS é que elas não podem fornecer uma detecção absolutamente precisa. *Falso positivo* (FP) e *falso negativo* (FN) são dois indicadores para avaliar o grau de precisão. O primeiro ocorre quando o IDS identifica incorretamente a atividade benigna como sendo mal-intencionada, enquanto o segundo ocorre quando o IDS não consegue identificar a atividade mal-intencionada (Stavroulakis e Stamp, 2010; Elshousha e Osmanb, 2011; Shanbhag e Wolf, 2009; Ho et al., 2012). Em circunstâncias em que não é possível obter o melhor dos dois mundos, muitos administradores de segurança preferem diminuir os FNs a aumentar os FPs devido à alta consideração de segurança. Em outras palavras, podemos levantar mais incidentes suspeitos e, em seguida, distinguir laboriosamente os FPs de incidentes suspeitos reais. Mais recentemente, Ho et al. (2012) coletaram casos de FP e FN do tráfego do mundo real, analisaram estatisticamente esses casos e propuseram três conclusões. Primeiro, a grande maioria dos casos falsos são FNs, porque a maioria dos comportamentos de aplicativos e seu formato de conteúdo são autodefinidos e não estão em conformidade com as especificações RFC. Em segundo lugar, a maioria dos alertas de FP não está relacionada a problemas de segurança, mas à política de gerenciamento. Por fim, há uma porcentagem incrivelmente alta de FNs para os ataques antigos, incluindo estouro de buffer, ataques ao servidor SQL e ataques de worm slammer.

Além disso, resumimos e refinamos muitas das pesquisas anteriores (Debar et al., 1999, , 2000; Axelsson, 2000; Estevez-Tapiador et al., 2004; Amer e Hamilton, 2010; Bace e Mell, 2001; Sabahi e Movaghar, 2008; Lazarevic et al., 2005; Xenakis et al., 2011) para oferecer uma nova perspectiva de taxonomia para IDSs. A Figura 1 apresenta quatro aspectos para classificar os IDSs, e a seguir apresentamos uma breve descrição em

sequência. No ramo de *implantação de sistemas*, a *arquitetura de rede* será "centralizada", que coleta e analisa as informações de um único sistema monitorado, "distribuída", que coleta dados de vários sistemas monitorados para detectar ataques inteiros, distribuídos e cooperativos, ou "híbrida" de ambos. Com o estado da arte, a configuração distribuída deve ser paralelizada, baseada em grade ou em nuvem. O *tipo de rede* aponta a interconexão dos IDSs com o sistema, que é monitorado por meio de uma forma "com fio", "sem fio" ou "mista". Especialmente, os IDSs sem fio adquirem requisitos explosivos, que são configurados em ambiente autônomo, cooperativo ou hierárquico. O item mais significativo é o *Tipo de tecnologia*, que foi demonstrado na última seção. Em segundo lugar, a faceta da *fonte de dados* que discrimina os IDSs com base no sistema é monitorada e consiste no *componente de coleta*, ou seja, "agente" ou "sensor". *Coleta de dados* por meio de coleta "centralizada" ou "distribuída". Além disso, *o Tipo de Dados* pode ser (i) trilhas de auditoria (por exemplo, registros do sistema, comandos do sistema, etc.) em um host, (ii) pacotes ou conexões de rede, (iii) tráfego de rede sem fio e (iv) registros de aplicativos. Em terceiro lugar, o *Timeliness* aponta que o *Tempo de Detecção* é a detecção em "tempo real/on-line" ou em "tempo não real/off-line" para um IDS. Além disso, o processamento "contínuo", "periódico" ou "em lote" de sinais de ataques é a *granularidade do tempo*. Além disso, *a Resposta de Detecção* a uma intrusão tem dois tipos: "passiva", se um IDS não tiver contramedidas e apenas gerar alarmes; "ativa", se um IDS tomar a ação corretiva ou preventiva. Por fim, o ponto de vista da *Estratégia de Detecção* indica que a *Disciplina de Detecção* seria "baseada no estado" (seguro ou inseguro) ou "baseada na transição" (de seguro para inseguro e vice-versa), e ambas podem ser avaliações estimulantes ou não obstrutivas. Além disso, *a estratégia de processamento* é intuitivamente "centralizada" ou "distribuída". Quanto à *metodologia de detecção*, uma das seguintes: "baseada em anomalia", "baseada em assinatura" e "baseada em especificação" foi adotada e ilustrada na seção anterior.

5. Máquinas virtuais

Uma máquina virtual (VM) (Krutz e Vines, 2010) é uma implementação de software que emula a funcionalidade de uma máquina real. A Figura 2 é uma visão geral da arquitetura da VM. Quando a virtualização da rede isola as redes virtuais usadas pelas VMs, ela também isola as falhas e os impactos de ataques em uma rede. As ameaças, as intrusões e os ataques existentes às redes físicas e virtuais são, portanto, ameaças menores às VMs (Mosharaf e Boutaba, 2010). Entretanto, a virtualização da rede pode expor novas vulnerabilidades de segurança. Por exemplo, os ataques DoS contra a rede física em um ambiente virtualizado também afetarão todas as VMs comunicadas na rede virtual. Estima-se que 60% das VMs em produção sejam menos seguras do que suas contrapartes físicas e que 30% das implantações tenham um incidente de segurança relacionado à VM (Nikitasha et al., 2011).

Como uma VM pode ser usada sob demanda, ela deve estar em uso o tempo todo; no entanto, a natureza dinâmica das VMs, conhecida como expansão de VMs (Embotics, 2010), dificulta a manutenção da consistência da segurança. A clonagem e a migração de VMs entre servidores físicos podem disseminar vulnerabilidades de segurança e negligência humana de forma rápida e ignorante. Isso será um desastre contra um pool de servidores virtualizados para uso em produção, porque geralmente não há firewalls físicos separando as VMs em um ambiente virtual.

Felizmente, a maioria das questões de segurança foi resolvida, de modo que podemos evitar a maioria das intrusões aplicando defesas de segurança tradicionais a cada VM (Zhao et al., 2009). Um método nativo é designar uma VM dedicada para monitorar outras VMs que compartilham um hypervi- sor idêntico. O monitor pode ser usado não apenas em IDS, mas também em verificação de integridade, sistemas de honeypot e análise forense, etc. (Payne et al., 2007). Intuitivamente, esse método introduz mais ou menos uma sobrecarga de desempenho (Xiang et al., 2010). Para a detecção de intrusão dentro de VMs, o *Virtual Memory Introspection* (VMI) (Garfinkel e Rosenblum, 2003)

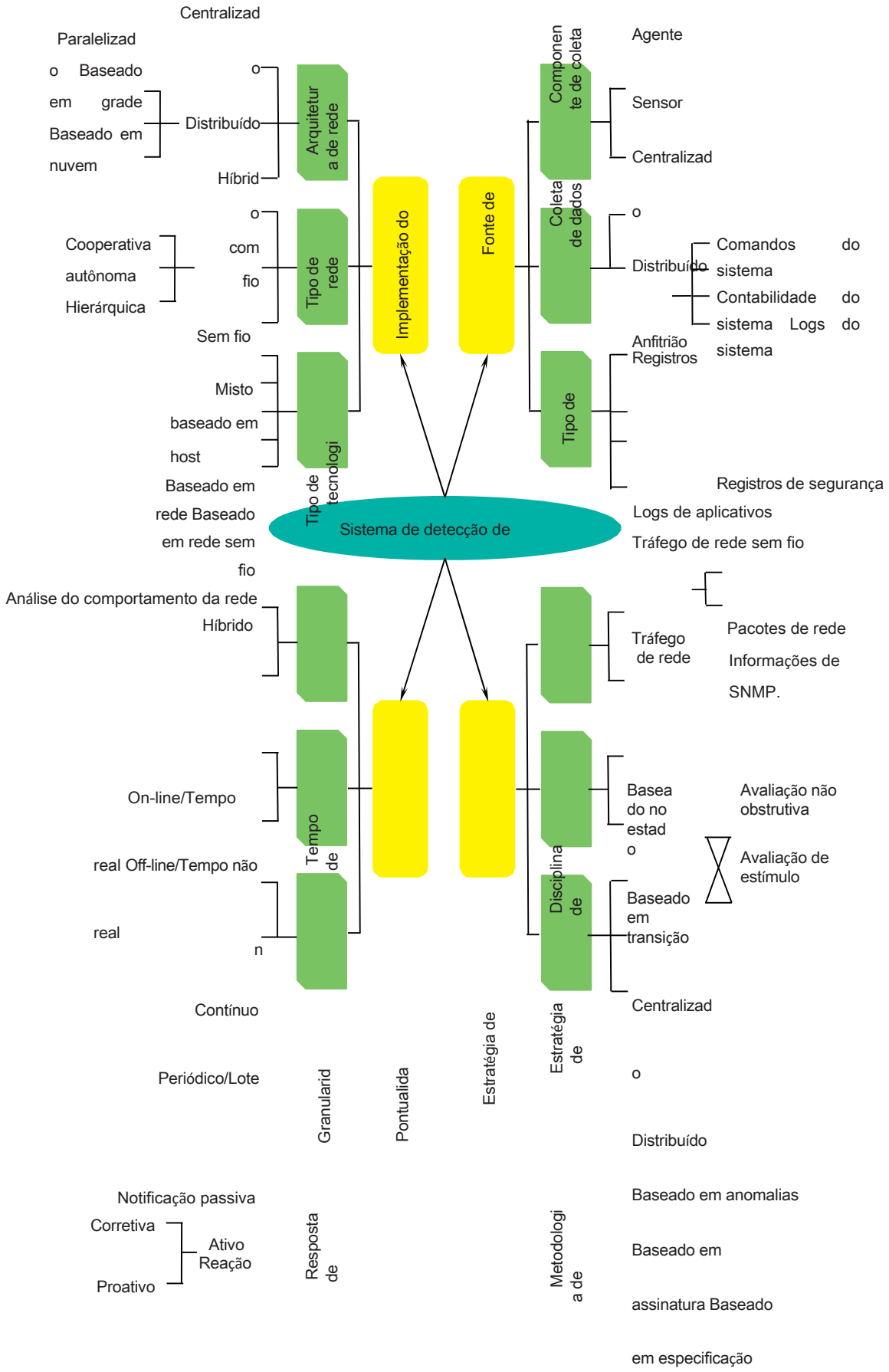
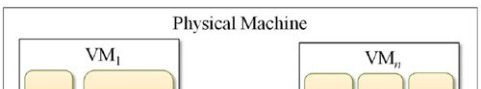


Fig. 1. Uma visão geral da taxonomia do IDS.



A entrada do fluxo de rede (por exemplo, balanceador de carga)

Fig. 2. Visão geral da máquina virtual.

é introduzido para aproveitar a tecnologia virtual no hipervisor, enquanto o HyperSpector (Kourai e Chiba, 2005) fornece um ambiente de monitoramento virtual distribuído. Além disso, a implementação de IDS nos ambientes críticos também é uma solução viável (Reese, 2009).

O hipervisor é uma junção de hardware de abstração e permite o compartilhamento de recursos do host entre o host e as VMs. Ele é um programa executado no host e, portanto, suscetível a riscos quando o volume e a complexidade do código do aplicativo aumentam (Krutz e Vines, 2010). Um ataque de modificação externa do hypervisor é conhecido como malware/rootkit baseado em VM (VMBR) (Carbone et al., 2008; Le e Wang, 2011), que tenta executar código malicioso em vez de chamada de sistema do hypervisor para o sistema operacional do host. Um *Trusted Platform Module* (TPM) no host ajuda a criar uma relação de confiança com o hypervisor (Krutz e Vines, 2010).

6. Snort e ClamAV

As redes de alta velocidade e as ameaças de rápida propagação representam desafios para os IDSs atuais, que detectam tentativas de invasão monitorando cuidadosamente cada pacote no tráfego intenso da rede. A maioria dos modernos

Os IDSs possuem suas próprias regras, por meio das quais podem examinar detalhadamente cada byte dos pacotes. Gostaríamos de apresentar aqui duas ferramentas populares e de código aberto implementadas pela abordagem baseada em regras (Snort; ClamAV). Em geral, uma regra consiste nos seguintes elementos: Uma especificação de filtro para qual ameaça de um determinado fluxo a regra funciona, uma cadeia de caracteres para ser a assinatura de cargas úteis suspeitas, uma posição para a ocorrência dessa cadeia de caracteres e uma ação correspondente quando todas as condições são atendidas.

De acordo com a lei de Amdal, a correspondência de strings seria a primeira consideração a ser feita para melhorar drasticamente o desempenho, pois representa cerca de 75% da carga da CPU dos IDSs (Cabrera et al., 2004). O enorme custo vem da verificação do pacote para ver se ele atende ou não a uma regra. Embora existam muitos algoritmos de correspondência de vários padrões propostos, não podemos nos dar ao luxo de examinar esse volume de tráfego em relação a um grande conjunto de cadeias de caracteres. Além disso, determinadas assinaturas são representadas na expressão regular para economizar espaço de armazenamento, o que pode exigir técnicas de pré-processamento para obter melhorias significativas.

Muitos trabalhos dedicam atenção às técnicas paralelas com tecnologias de hardware especializadas para melhorar a taxa de transferência do processamento de pacotes, como ASIC, processador de rede, FPGA, TCAM, etc. (Goyal et al., 2008). Essas implementações geralmente apresentam desempenho satisfatório, p o r exemplo, Jiang et al., 2010 afirma que seu protótipo de implementação em FPGA sustenta mais de 10 Gbps rendimento. No entanto, as abordagens de hardware geralmente são de alta custo, difíceis de modificar e vinculados a uma implementação específica, o que limita suas aplicações.

Devido às desvantagens do método de hardware, alguns estudos buscam soluções orientadas por software, sendo que o Snort e o ClamAV são as duas ferramentas de código aberto mais usadas. A primeira se concentra na detecção de intrusão de rede, enquanto a segunda é um mecanismo antivírus. Ambos têm seus próprios conjuntos de assinaturas, mas com uma grande diversidade. A Figura 3 mostra a distribuição do comprimento de suas assinaturas. Observe que o ClamAV-RE na Figura 3 representa as assinaturas com forma de expressão regular no ClamAV, e não expandimos a expressão para simplificar. Em contraste com o conjunto de assinaturas do Snort, o ClamAV tem mais strings e mais longas. Atualmente, o número de assinaturas no ClamAV é superior a 800.000, e o Snort tem pouco mais de 4.000 regras. Mesmo assim, as detecções do Snort podem ser demoradas porque ele examina vários critérios em uma regra.

O Snort explora o algoritmo Aho-Cora (Aho e Corasick, 1975) para a detecção de assinaturas de correspondência exata; o ClamAV usa uma variante do mesmo algoritmo para processar as assinaturas com expressão regular e, no entanto, o algoritmo Boyer-Moore (Boyer e Moore, 1977) para detectar as outras assinaturas. Há um aumento considerável na implementação e no aprimoramento de ambas as ferramentas. Por exemplo, o Snort e o NTOP, uma ferramenta para monitorar a rede, são combinados para formar um NIDS em (Peng, 2012). Existem

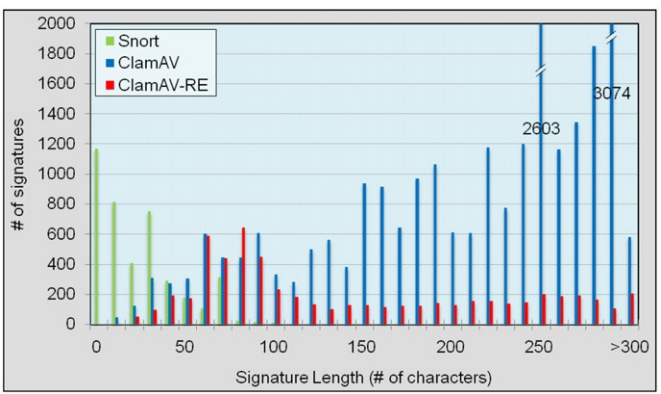


Fig. 3. Distribuições de comprimentos de assinatura no Snort e no ClamAV.

trabalhos contribuíram para avaliar o desempenho do Snort nos sistemas operacionais Linux e Windows (Salah e Kahtani, 2009, 2010; Salah et al., 2011). Além disso, o Gnort (Vasiliadis et al., 2008), baseado no Snort, é um IDS popular que usa GPU e atinge uma taxa de transferência máxima de processamento de tráfego de 2,3 Gbps. Até mesmo o Gravity (Vasiliadis e Ioannidis, 2010) pode chegar a 20 Gbps, muito melhor do que o desempenho do ClamAV somente com CPU. Para o conjunto de padrões do ClamAV, foi proposto um método de economia de memória para fazer a pesquisa de strings para aplicativos antivírus (Wang et al., 2011).

7. Conclusões

7.1. Lições aprendidas

Apresentamos uma visão geral das metodologias, abordagens e tecnologias de detecção para IDSs. Cada técnica tem sua superioridade e suas limitações, portanto, devemos ser cautelosos ao selecionar as abordagens. Tomemos como exemplo o IDS baseado em padrões, embora seja simples de implementar e muito eficaz para inspecionar ataques conhecidos, a abordagem dificilmente poderia identificar ataques desconhecidos, ataques ocultos por técnicas de evasão e muitas variantes de ataques conhecidos. Além disso, foram propostas várias abordagens baseadas em regras para detectar ataques desconhecidos. Entretanto, essas técnicas podem resultar no problema da dificuldade de criar e atualizar o conhecimento para determinados ataques. Além disso, as abordagens baseadas em heurística têm o mérito de não exigir conhecimento prévio dos ataques, mas não funcionam bem em aplicativos em tempo real devido à alta complexidade computacional. Portanto, é indispensável ter uma visão abrangente dos IDSs e dos requisitos dos aplicativos antes de usá-los na prática. Além disso, propomos uma revisão mais elaborada sobre IDSs. As tabelas e as figuras que resumimos contribuem para a fácil compreensão do quadro geral. Além disso, apresentamos brevemente duas ferramentas famosas e de código aberto para o estudo de IDSs.

Por outro lado, a tecnologia de virtualização é cada vez mais importante, pois é amplamente usada em plataformas de nuvem. A VM é o primeiro componente virtual que entra em contato direto com os usuários e, por isso, também estudamos vários problemas de IDS em VMs.

7.2. Desafios futuros

Neste artigo, incluímos uma pesquisa abrangente e uma avaliação dos IDSs atuais. No entanto, ainda há muitas questões em aberto e desafios futuros. Por exemplo, a tecnologia *sem* fio - *devido* a algumas particularidades
recursos (por exemplo, mobilidade, ausência de pontos centrais, largura de banda limitada de
links sem fio e recursos limitados), os IDSs sem fio levantam problemas de segurança, comunicação e gerenciamento. Além disso, a maioria dos IDSs sem fio precisa ser testada em vários cenários de mobilidade e topologia para garantir a capacidade de proteção. *Objetivo*
de IDSs neurais, difusos e heurísticos baseados em imunidade
O sistema de IDS em tempo real foi proposto, mas é preciso regular a sensibilidade do alerta de ataques maliciosos para diminuir a taxa de alarmes falsos. O *paralelismo* - a computação de alto desempenho torna os IDSs em tempo real de baixo custo mais fáceis de usar.
No entanto, ainda há muitos desafios, como dividir os trabalhos de detecção de intrusão em paralelo, a coordenação e o gerenciamento de vários nós, etc. Além disso, os sistemas transparentes, como os recursos de filtragem de rede, devem se concentrar no tempo de processamento de baixo atraso, e não no desempenho de alta taxa de transferência. Além disso, o IDS para VMs com uma degradação de desempenho mais leve é um tópico urgente para serviços em computação em nuvem.

Referências

Aho AV, Corasick MJ. Efficient string matching: an aid to bibliographic search. Communications of the ACM 1975;18:333-40.

Alomari O, Othman ZA. Algoritmo Bees para seleção de recursos na detecção de anomalias de rede. Journal of Applied Sciences Research 2012;8:1748-56.

Amer SH, Hamilton JA. Taxonomia dos sistemas de detecção de intrusão (IDS) - uma breve
revisão. Journal of Software Technology 2010;13.

Anantvalee T, Wu J. Uma pesquisa sobre detecção de intrusão em redes ad hoc móveis. Em: Xiao Y, Shen X, Du D-Z, editores. Wireless/mobile network security. Springer- Verlag; 2007. p. 170-96.

Axelsson S, Intrusion detection systems: a survey and taxonomy (Sistemas de detecção de intrusão: uma pesquisa e taxonomia), Chalmers University of Technology, Suécia, Technical Report 99-15 (2000), pp. 1-27.

R Bace, P Mell, Intrusion detection systems (Sistemas de detecção de intrusão), National Institute of Standards and Technology (NIST), Technical Report 800-31, 2001.

Boyer RS, Moore JS. Um algoritmo de busca rápida de strings. Communications of the ACM 1977;20:762-72.

CERT, ⁄http://www.cert.org/statsS.

Cabrera JBD, Gosar J, Lee W, Mehra RK, Sobre a distribuição estatística do processamento vezes na detecção de intrusão de rede. Em: 43ª Conferência do IEEE sobre decisão e controle, Paradise Island, Bahamas, 2004, pp. 75-80.

Carbone M, Lee W, Zamboni D. Domando a virtualização. IEEE Security and Privacy 2008;6:65-7.

Chung YY, Wahid N. Um sistema híbrido de detecção de intrusão de rede usando swarm optimization (SSO) simplificado. Applied Soft Computing 2012;12:3014-22.

ClamAV, ⁄http://www.clamav.netS.

Couture M. Real time intrusion prediction based on optimized alerts with hidden Markov model (Previsão de intrusão em tempo real baseada em alertas otimizados com modelo oculto de Markov). Journal of Networks 2012;7:311-21.

Debar H, Dacier M, Wespi A. Towards a taxonomy of intrusion detection systems (Rumo a uma taxonomia de sistemas de detecção de intrusão).
Redes de computadores 1999;31:805-22.

Debar H, Dacier M, Wespi A. Uma taxonomia revisada para o sistema de detecção de intrusão.
Annals of Telecommunications 2000;55:361-78.

Delgado N, Gates Q, Roach S. Uma taxonomia e um catálogo de ferramentas de monitoramento de falhas de software em tempo de execução. IEEE Transactions on Software Engineering 2004;30:859-72. Denning DE. Um modelo de detecção de intrusão. IEEE Transactions on Software Engi-
neering 1987;SE-13:222-32.

Elshousha HT, Osmanb IM. Alert correlation in collaborative intelligent intrusion detection systems - a survey (Correlação de alertas em sistemas colaborativos inteligentes de detecção de intrusão - uma pesquisa). Applied Soft Computing 2011;11:4349-65.

Embotics, Controlando a expansão da VM: práticas recomendadas para obter e manter
controle de infraestruturas virtualizadas, White Paper, 2010.

Estevez-Tapiador JM, Garcia-Teodoro P, Diaz-Verdejo JE. Detecção de anomalias métodos em redes com fio: uma pesquisa e uma taxonomia. Computer Communica- tions 2004;27:1569-84.

AH Farooqi, FA Khan, J Wang, S Lee, Uma nova estrutura de detecção de intrusão para redes de sensores sem fio , Personal and Ubiquitous Computing. Disponível on-line em 2012.

Fragkiadakis AG, Tragos EZ, Tryfonas T, Askoxylakis IG. Projeto e desempenho avaliação de um protótipo de detecção de intrusão de alerta antecipado sem fio leve. EURASIP Journal on Wireless Communications and Networking 2012;73: 1-18.

Garcia-Teodoro P, Diaz-Verdejo J, Macia-Fernandez G, Vazquez E. Anomaly-based network intrusion detection: techniques, systems and challenges (Detecção de intrusão de rede baseada em anomalias: técnicas, sistemas e desafios). Computadores & Security 2009;28:18-28.

Garfinkel T, Rosenblum M, A virtual machine introspection based architecture for intrusion detection. Em: Simpósio de segurança de redes e sistemas distribuídos, San Diego, Califórnia, EUA, 2003.

Goyal N, Ormont J, Smith R, Sankaralingam K, Estan C, Signature matching in network processing using SIMD/GPU architectures, University of Wisconsin-Madison, Technical Report 1628, 2008.

Ho C-Y, Lai Y-C, Chen I-W, Wang F-Y, Tai W-H. Análise estatística de falsos positivos e falsos negativos do tráfego real com sistemas de detecção/prevenção de intrusão. IEEE Communications Magazine 2012;50:146-54.

Horng SJ, Su MY, Chen YH, Kao TW, Chen RJ, Lai JL, Perkasa CD. Um novo sistema de detecção de intrusão baseado em agrupamento hierárquico e máquinas de vetor de suporte. Expert Systems with Applications 2011;38:306-13.

W Jiang, Y-HE Yang, VK Prasanna, Arquitetura escalável de várias linhas de pipeline para correspondência de strings multipadrão de alto desempenho. Em: 24º Simpósio Internacional de Processamento Paralelo e Distribuído do IEEE, Atlanta, Geórgia, EUA, 2010, pp. 1-12.

Jones AK, Sielken RS, Computer system intrusion detection: a survey, University of Virginia, Technical Report (2000).

Kabiri P, Ghorbani AA. Pesquisa sobre detecção e resposta a intrusões: um levantamento.
International Journal of Network Security 2005;1:84-102.

Kantzavelou I, Katsikas S. Um mecanismo de detecção de intrusão baseado em jogos para confrontar atacantes internos. Computers & Security 2010;29:859-74.

Kartit A, Saidi A, Bezzazi F, Marraki ME, Radi A. Uma nova abordagem para o sistema de detecção de intrusão. Journal of theoretical and applied information technology 2012;36:284-9.

Kolias C, Kambourakis G, Maragoudakis M. Swarm intelligence in intrusion detection: a survey. Computers & Security 2011;30:625-42.

Kourai K, Chiba S, HyperSpector: ambientes virtuais de monitoramento distribuído para detecção segura de intrusões. Em: Primeira conferência internacional da ACM/USENIX sobre ambientes de execução virtual, Chicago, IL, EUA, 2005, pp. 197-207.

Krugel C, Toth T, A survey on intrusion detection systems (Uma pesquisa sobre sistemas de detecção de intrusão), Universidade Técnica de Viena, Áustria, Relatório Técnico TUV-1841-00-11 (2000), pp. 22-33.

Krutz RL, Vines RD. Cloud security: a comprehensive guide to secure cloud computing.Indianapolis: Wiley; 2010.

Lazarevic A, Kumar V, Srivastava J. Managing cyber threats: issues, approaches, and challenges.New York: Springer-Verlag; 2005.

Le D, Wang H. Uma otimização eficaz da memória para sistemas baseados em máquinas virtuais.
IEEE Transactions on Parallel and Distributed Systems 2011;22:1705-13.

L Li, Zhang G, Nie J, Niu Y, Yao A, O aplicativo de algoritmo genético para detecção de intrusão na rede MP2P. Em: Terceira conferência internacional sobre avanços em inteligência de enxame, Shenzhen, China, 2012, pp. 390-397.

Li Y, Xia J, Zhang S, Yan J, Ai X, Dai K. Um sistema eficiente de detecção de intrusão baseado em máquinas de vetores de suporte e método de remoção gradual de recursos. Expert Systems with Applications 2012;39:424-30.

Lunt TF. Uma pesquisa sobre técnicas de detecção de intrusão. Computers & Security 1993;12:405-18.

Mandala S, Ngadi MA, Abdullah AH. Uma pesquisa sobre detecção de intrusão em MANET.
International Journal of Computer Science and Security 2008;2:1-11.

Mar J, Hsiao IF, Yeh YC, Kuo CC, Wu SR. Detecção inteligente de intrusão e defesa nula robusta para redes sem fio. International Journal of Innovative Com- puting Information and Control 2012;8:3341-59.

Mishra A, Nadkarni K, Patcha A, Tech V. Intrusion detection in wireless ad-hoc networks (Detecção de intrusão em redes ad-hoc sem fio). IEEE Wireless Communications 2004;11:48-60.

C Modi, D Patel, B Borisaniya, H Patel, A Patel, M Rajarajan, Uma pesquisa sobre técnicas de detecção de intrusão na nuvem. Journal of Network and Computer Applications. Disponível on-line em 2012.

Mosharaf NMMK, Boutaba R. Uma pesquisa sobre virtualização de redes. Redes de computadores 2010;54:862-76.

Mukherjee B, Heberlein LT, Levitt KN. Detecção de intrusão de rede. IEEE Network 1994;8:26-41.

Mukkamala S, Sung AH, A comparative study of techniques for intrusion detection, In: 15th IEEE international conference on tools with artificial intelligence, Sacramento, California, USA, 2003, pp. 570-577.

Murali A, Rao M, A survey on intrusion detection approaches (Uma pesquisa sobre abordagens de detecção de intrusão), In: First international conference information and communication technologies, Karachi, Paquistão, 2005, pp. 233-240.

Nikitasha P, Jyotiprakash S, Subasish M, Prasanna PS. Uma estrutura de segurança para ambiente de computação baseado em virtualização. International Journal of Engi- neering Science and Technology 2011;3:6423-9.

Paramasivan B, Pitchai KM. Pesquisa abrangente sobre o sistema de detecção de invasão baseado na teoria dos jogos para redes adhoc móveis. Revista Internacional de Aplicativos de Computação 2011;5:23-9.

Patcha A, Park JM. Uma visão geral das técnicas de detecção de anomalias: soluções existentes e últimas tendências tecnológicas. Computer Networks 2007;51: 3448-70.

Payne BD, Carbone M, Lee W, Secure and flexible monitoring of virtual machines, In: 23rd annual computer security applications conference, Miami Beach, FL, 2007, pp. 385-397.

Pelechrinis K, Iliofotou M, Krishnamurthy SV. Ataques de negação de serviço em redes sem fio: o caso dos jammers. IEEE Communications Surveys and Tutorials 2011;13:245-57.

Peng YH, Pesquisa do sistema de detecção de intrusão de rede baseado em snort e NTOP, In: Nona conferência internacional sobre sistemas fuzzy e descoberta de conhecimento, Chongqing, China, 2012, pp. 2764-2768.

Reese G. Cloud application architectures: building applications and infrastructure in the cloud (Arquiteturas de aplicativos na nuvem: criação de aplicativos e infraestrutura na nuvem). O'Reilly Media; 2009.

Sabahi F, Movaghar A, Intrusion detection: a survey (Detecção de intrusão: uma pesquisa), In: Terceira conferência internacional sobre sistema e comunicação de rede, Sliema, Malta, 2008,
pp. 23-26.

Salah K, Kahtani A. Melhorando o desempenho do Snort no Linux. IET Communica- tions 2009;3:1883-95.

Salah K, Kahtani A. Comparação da avaliação de desempenho do Snort NIDS no Linux e no Windows Server. Journal of Network and Computer Applications 2010;33:6-15.

Salah K, Al-Khiaty M-A-R, Ahmed R, Mahdi A. Avaliação de desempenho do Snort no Windows 7 e no Windows Server 2008. Journal of Universal Computer Science 2011;17:1605-22.

Sen S, Clark JA. Evolutionary computation techniques for intrusion detection in mobile ad hoc networks (Técnicas de computação evolutiva para detecção de intrusão em redes ad hoc móveis). Computer Networks 2011;55:3441-57.

Shanbhag S, Wolf T. Accurate anomaly detection through parallelism (Detecção precisa de anomalias por meio do paralelismo). IEEE Network 2009;23:22-8.

Shena S, Li Y, Xua H, Caoa Q. Estratégia baseada em jogo de sinalização para detecção de intrusão em redes de sensores sem fio. Computers & Mathematics with Applications 2011;62:2404-16.

Snort, ⁄http://www.snort.orgS.

Stavroulakis P, Stamp M. Handbook of information and communication security - Nova York: Springer-Verlag; 2010.

Tan Y, Sengupta S, Subbalakshmi KP. Análise de ataques coordenados de negação de serviço em redes IEEE 802.22. IEEE Journal on Selected Areas in Commu- nications 2011;29:890-902.

Tucker CJ, Furnell SM, Ghita BV, Brooke PJ. A new taxonomy for comparing intrusion detection systems (Uma nova taxonomia para comparar sistemas de detecção de intrusão). Internet Research 2007;17:88-98.

Vasiliadis G, Ioannidis S, GrAVity: um mecanismo antivírus massivamente paralelo, In: Third international conference on recent advances in intrusion detection, Ottawa, Ontário, Canadá, 2010, pp. 79-96.

Vasiliadis G, Antonatos S, Polychronakis M, Markatos EP, Ioannidis S, Gnort: high performance network intrusion detection using graphics processors, In: 11th international symposium on recent advances in intrusion detection, Boston, MA, USA, 2008, pp. 116-134.

Wang SS, Yan KQ, Wang SC, Liu CW. Um sistema integrado de detecção de intrusão para redes de sensores sem fio baseadas em cluster. Expert Systems with Applications 2011;38:15234-43.

Wang X, Wang X, Cao C, Zhu Y. Mecanismo de pesquisa de strings para verificação de vírus. IEEE Transactions on Computers 2011;60:1596-609.

Xenakis C, Panos C, Stavrakakis I. Uma avaliação comparativa das arquiteturas de detecção de intrusão para redes ad hoc móveis. Computers & Security 2011;30:63-80.

Xiang G, Jin H, Zou D, Zhang X, Wen S, Zhao F, VMDriver: um mecanismo de monitoramento baseado em driver para virtualização, In: 29th IEEE symposium on reliable distributed systems, New Delhi, 2010, pp. 72-81.

Xie M, Han S, Tian B, Parvin S. Anomaly detection in wireless sensor networks: a survey (Detecção de anomalias em redes de sensores sem fio: uma pesquisa). Journal of Network and Computer Applications 2011;34:1302-25.

Zhao S, Chen K, Zheng W, A aplicação de máquinas virtuais na segurança do sistema. Em: Quarta conferência anual da ChinaGrid, Yantai, Shandong, 2009, pp. 222-229.