THIAGO ROSCIA CERDEIRO DE LIMA

SISTEMAS DE DETECÇÃO DE INTRUSÃO EM REDE BASEADOS EM ANOMALIAS

CURITIBA

2015

THIAGO ROSCIA CERDEIRO DE LIMA

SISTEMAS DE DETECÇÃO DE INTRUSÃO EM REDE BASEADOS EM ANOMALIAS

Monografia apresentada para obtenção do Grau de Bacharel em Ciência da Computação pela Universidade Federal do Paraná.
Orientador: Prof. Dr. Luis Allan Kunzle

CURITIBA

2015

CONTENTS

RESUMO **iii**

1 INTRODUÇÃO **1**

2 SIGNATURE-BASED IDS **3**

3 ANOMALY-BASED IDS (A-NIDS) **4**

3.1 Técinas Estatísticas 4

3.2 Técnicas Baseadas em Conhecimento 5

3.3 Técnicas de Machine Learning 5

3.4 Combinação de Classificadores 6

3.4.1 Classificadores Híbridos 6

3.4.2 Classificadores em Cascata 6

3.4.3 Composição de Classificadores 7

4 SISTEMAS A-NIDS FUNCIONAIS **8**

4.1 Arquitetura 8

4.2 Comercialmente 9

5 DADOS **10**

5.1 Origem dos Dados 10

5.1.1 Cabeçalho de pacote 11

5.1.2 Corpo de pacote 11

5.2 Pré-processamento 12

5.2.1 Derivação 12

5.3 Conjuntos de Características 13

5.3.1 Conexões múltiplas 13

5.3.2 Única conexão 13

5.3.3 KDD Cup 99 14

6 CONCLUSÃO **15**

BIBLIOGRAFIA **15**

RESUMO

O aumento da resolução espacial de imagens é de grande interesse para várias aplicações. Dentro da biometria isto pode implicar no aumento da performance dos algoritmos e do relaxamento do grau de cooperação necessário dos indivíduos a serem identificados. A super-resolução surge como meio de realização desta tarefa, alternativa à acquisição de novos sensores de custo mais elevado. O método consiste em combinar os dados contidos em diversas vistas de uma mesma cena, sejam elas capturadas por um único ou múltiplos sensores, a fim de gerar um quadro de maior resolução como saída. Sistemas que utilizam informação 3D também podem ser beneficiados, pois quando aplicado a imagens de profundidade, a super-resolução cria nuvens de pontos de maior densidade. Neste trabalho foi avaliada a possibilidade da aplicação de técnicas de super-resolução em sistemas biométricos 2D e 3D, com ênfase em sistemas de reconhecimento facial. No caso 2D, um algoritmo capaz de obter resultados melhores que a interpolação bicúbica foi implementado. Para 3D, uma análise visual nos resultados do nosso algoritmo aplicado em objetos rígidos mostrou potencial para aplicações práticas.

Palavras-chave: Super-Resolução, Imagens de Profundidade, Biometria, Reconhecimento Facial

CHAPTER 1

INTRODUÇÃO

A Internet representa, atualmente, não apenas mais uma ferramenta de uso diário, mas um completo ambiente utilizado por cidadãos para armazenamento de arquivos pessoais, por bancos para efetuar transações bancárias e por governos para trocas de informações preciosas. Assim como é possível se conectar de uma máquina pessoal a um servidor web, é possível fazer o contrário. Qualquer máquina conectada a uma rede está teoricamente sujeita ao acesso de fora. Roteadores e sistemas operacionais atuais estão equipados com ferramentas básicas para previnir acesso não autorizado ao computador. Ainda assim, há pessoas dedicadas a burlar tais proteções. Alguns desses invasores conseguem copiar arquivos, instalar malware e até ganhar controle sobre o sistema sem serem notados pelo dono.

A fim de cobrir esse ponto cego, foram criados sistemas de detecção de intrusão, ou IDS (intrusiondetection systems). Seu objetivo é reconhecer comportamentos incomuns dentro de uma rede. No meio acadêmico, muitos artigos foram publicados explorando algoritmos de Machine Learning nesta aplicação.

Existem diversos tipos de ataques e diferentes protocolos de comunicação, mas o problema de se detectar uma intrusão pode ser simplificado em um problema de classificação binária do comportoamento do sistema, onde os dois possíveis resultados seriam "normal" ou "intrusivo". Existem duas "escolas de pensamento" bem definidas no meio acadêmico acerca do assunto:

1. Signature-based, ou baseado em assinatura. Esse é o método padrão e atualmente o único utilizado comercialmente. Ele possui baixa adaptabilidade a novas ameaças.

2. Anomaly-based, ou baseado em anomalia. Ainda uma área de estudo, possui alta taxa de Falso-Positivo, mas boa adaptabilidade.

Este artigo dará, posteriormente, foco aos conceitos e desenvolvimento de algoritmos de

Machine Learning e Sistemas de Detecção de Intrusão em Rede baseados em Anomalia (A-NIDS).

CHAPTER 2

SIGNATURE-BASED IDS

Apesar de não ser o foco deste artigo, vamos descrever brevemente os sistemas baseados em assinatura, a fim de comparação com os métodos nos quais vamos nos aprofundar.

Sistemas baseados em assinatura têm sido os mais bem sucedidos para detecção de intrusão até hoje. A ideia é comparar o tráfego da rede com padrões de comportamento conhecidos durante certos ataques. O maior problema é a ineficiência em detectar ataques novos.

Os primeiros sistemas utilizavam apenas o método de reconhecimento de padrão. Essa técnica possui um banco de dados preenchido com assinaturas de cada ameaça conhecida. Um evento malicioso é detectado se o atual estado da rede se iguala a uma assinatura. Como ele tenta comparar todas as assinaturas e a quantidade de dados transmitidos simultaneamente cresce a cada ano, o custo computacional tronou-se muito alto.

Uma segunda técnica é o método de *implication rules*, ou regras de inferência. Ela fornece um conjunto de regras que descrevem eventos conhecidos que podem inferir o acontecimento de um a intrusão. De qualquer modo, IDS de assinatura geralmente necessita de um humano capacitado, que cria um novo conjunto de regras toda vez que um novo tipo de ataque surge, para adquirir modelos de tráfego.

Daí surge a motivação para se utilizar técnicas de *data mining* em sistemas de assinatura. Elas provém um modo de aumentar a automação na hora de construir e ajustar o modelo. Eles podem adaptar os modelos à medida que acessam tráfego de rede contendo novas ameaças ou detectando diferentes versões de um ataque conhecido. Ainda assim, é impossível identificar comportamentos maliciosos completamente desconhecidos.

CHAPTER 3

ANOMALY-BASED IDS (A-NIDS)

A técnica de detecção de anomalia analisa o atual comportamento da rede para checar se corresponde ou não a um comportamento normal. O maior benefício desse método é a habilidade de identificar novos ataques com sucesso. A desvantagem é a alta taxa de Falso Positivo. Ao invés de requerer um novo modelo a ser adaptado, sistemas baseados em anomalia necessitam de dados de tráfego de rede sem livres de ataques. *Data mining* também tem sido utilizado em sistemas baseados em anomalia, junto a outros métodos estatísticos e de *Machine Learning* (aprendizado de máquina).

As diferentes técnicas podem ser agrupadas em três categorias, de acordo com o processamento envolvido: estatístico, knowledge-based (baseado em conhecimento) ou algoritmos de aprendizado de máquina.

3.1 Técinas Estatísticas

Um modelo de probabilidade de um determinado comportamento é criado a partir da atividade capturada do tráfego de rede, tal como taxa de tráfego, número de pacotes e quantidade de endereços de IP distintos.

Ele não requer conehcimento prévio pois está capacitado a aprender o comportamento normal a partir de observações sem ataques. Outro benefício das técnicas estatísticas é a possibilidade de identificar, com precisão, atividades maliciosas que ocorrem ao longo de períodos de tempo mais extensos. Por outro lado, nem todos os possíveis comportamentos conseguem ser modelados e o equilíbrio entre taxas de Falso Positivo e Falso Negativo dependem fortemente na configuração correta dos parâmetros.

3.2 Técnicas Baseadas em Conhecimento

Também chamados de expert systems, sistemas baseados em conhecimento são implementados criando-se um conjunto de regras de classificação para categorizar os dados. O modelo é geralmente criado por um humano experiente no campo da aplicação. Esse tipo de sistema não aponta novas atividades inofensivas como sendo maliciosas, garantindo, assim, um número reduzido de Falso Positivo. Por essa razão, o conjunto de regras precisa ser específico o suficiente e, apesar de ser possível atingir um certo nível de automatização usando uma máquina de estados finitos, requer grande conhecimento sobre o comportamento da rede e tempo significativo para ser desenvolvido.

3.3 Técnicas de Machine Learning

Métodos de aprendizado de máquina exigem um conjunto de dados categorizados para treinar o comportamento esperado do modelo. A característica principal dessa técnica é a habilidade de adaptar suas regras de classificação à medida que novos dados são recebidos. Isso garante pouca necessidade por intervenção humana, uma vez funcionando. O lado ruim do aprendizado de máquina é o alto custo computacional. Os algoritmos mais populares usados em A-NIDS são:

- Rede Bayesiana – cria uma rede de relações de probabilidade entre características
- Modelos de Markov – comapra a probabilidade dos dados observados com um threshold definido
- Redeus neurais – cria um rede de perceptrons com habilidade de se adaptar
- Lógica Fuzzy – enxerga características como variáveis fuzzy e classifica com base em valores contínuos
- Algoritmos Genéticos – deriva regras de classificação e seleciona as características mais discriminantes

- Support Vector Machines – encontra um hiperplano que eficientemente separa ambas as opções de classificação
- Árvores de Decisão – cria uma árvore onde cada folha representa uma classe e arestas correspondem a diferentes valores de atributos
- Clustering – algoritmo não-supervisionado que agrupa dados com base em suas similaridades.

3.4 Combinação de Classificadores

Como cada método possui seus pontos fortes e pontos fracos. Uma ideia bastante estudada no meio acadêmico é a combinação de classificadores. Tais combinações podem se dar de diversas maneiras, como por exemplo: Classificadores Híbridos, Composição de Classificadores [1] e Classificadores em Cascata.

3.4.1 Classificadores Híbridos

Um classificador híbrido consiste de dois componentes. O primeiro pré-processa o dado de entrada e envia ao segundo classificador, que chega ao resultado final. O primeiro componente de classificadores híbridos pode ser usado tanto como uma técnica de clustering para achar as classes que o segundo componente utilizará para categorizar os dados; quanto como um otimizadoe de performance para o segundo modelo, que corresponde ao método integrado.

3.4.2 Classificadores em Cascata

Pode ser considerado uma extensão dos classificadores híbridos, podendo consistir de inúmeros classificadores, onde o n-ésimo classificador utiliza como entrada os dados rejeitados pelo classificador anterior, ou seja, que não atingiram um grau de certeza satisfatório. Esse método foi analsiado mais a fundo e testado a fim de comparar a agilidade e precisão em uma base de dados própria.

[1] Tradução livre do termo em inglês Ensemble Classifiers.

3.4.3 Composição de Classificadores

Uma composição de classificadores pode ser obtida usando-se técnicas fracas de aprendizado (geralmente mais rápidas). Cada classificador é treinado usando um subconjunto distinto dos dados. A base de testes é, então, processada por todos eles e, finalmente, categorizados pela maioria.

CHAPTER 4

SISTEMAS A-NIDS FUNCIONAIS

O estudo feito em [**?**] apresenta sistemas A-NIDS divididos em duas categorias: comerciais e de pesquisa. Sistemas comerciais geralmente trabalham com um núcleo baseado em assinatura, enquanto sistemas de pesquisa protótipos e metodologias inovadoras.

4.1 Arquitetura

Enquanto alguns detalhes de implementação podem variar, a base da esquematização de um A-NIDS é como apresentado em [**?**]:

- Aquisição de dados de tráfego – coleta informação sobre os quadros da rede para processamento futuro.
- Gerador de características do tráfego – extrai características do tráfego capturado. Tais características podem ser classificadas como "baixo nível" (obtidas diretamente do dado bruto), "alto nível" (deduzidas de um processamento subsequente), "pacote" (coletadas de cabeçalhos de pacotes), "fluxo" (contendo informação das conexões) e "payload" (obtidos da carga do pacote).
- Detector de incidente – identifica atividades intrusivas. Pode ser tanto baseado em assinatura quanto em anomalia.
- Gerador de modelo de tráfego – contei informação base usada para guiar o detector de incidente.
- Gerenciamento de resposta – inicia manobras para superar uma intrusão em potencial. É inicializado pelo detector de incidente.

4.2 Comercialmente

Um dos primeiros projetos de detecção de anomalia a ser amplamente conhecido foi o SPADE, um plugin para o Snort que anhalisava transferência de pacotes procurando comportamentos fora do comum. Alternativamente, Stealthwatch utilizava detecção de anomalia baseada em fluxo.

Sistemas recentes usam um arquitetura distribuída utilizando sensores e um console central para gerenciar o processo de detecção. Esse é o caso do DeepSight, que usa um método estatístico. A maioria dos sistemas comerciais utilizam um módulo de detecção baseado em assnatura aliado com um núcleo baseado em anomalia. Todos esses sistemas se enquadram na categoria de classificadores híbridos.

CHAPTER 5

DADOS

Os passos mais relevantes para o modelamento de dados de um NIDS são os seguintes:

1. Criação da base – identifica dados categorizados (normal ou anômalo) representativos para treino e teste. Categorização de tráfego de rede pode ser uma tarefa difícil e longa, que geralmente envolve um especialista.

2. Construção de características – cria características com maior discriminabilidade. Tais características podem ser construídas por um humano ou por algoritmos de aprendizado de máquina.

3. Redução – também chamado de "seleção de caterísticas", diminui a dimensionalidade da base de dados descartando características irrelevantes ou redundantes. Usado para atenuar a "Maldição da Dimensionalidade" [1].

5.1 Origem dos Dados

A escolha de informações da rede é amplamente afetada pelos requisitos de detecção ao se projetar o sistema. É possível ter sistemas de detecção específicos, utilizando um conjunto de características limitado. Para um sistema mais genérico, o ideal seria utilizar detectores separados utilizando conjuntos de características distintos, um para cada especificidade. Dependendo da origem desses dados, têm-se algumas vantagens e desvantagens. Técnicas para análise de conteúdo ainda não estão tão concretizadas quanto as que extraem características de cabeçalhos. Assim comoanalisar conteúdo do lado do cliente ainda é um campo não tão estudado quanto o lado do servidor numa perspectiva de A-NIDS. Técnicas do lado do cliente almejam detectar ameaças em aplicações web, como *drive-by downloads*, *cross-site scripting* e trechos maliciosos de JavaScript.

[1] *Curse of Dimensionality*: Ao se usar muitas características, supostamente se obtém baixa precisão.

5.1.1 Cabeçalho de pacote

Características obtidas através de cabeçalhos de pacotes têm a qualidade de serem rápidos, sem exigir muito processamento ou memória, e evitarem preocupações legais acerca de análise de dados da rede. O conjunto de característica mais simples contém características básicas extraídas dos cabeçalhos. Essas características podem ser usadas para apontar pacotes individuais que são anômalos quando comaprados ao modelo de treino; ou como um processo de filtragem para que apenas pacotes incomuns sejam usados por algoritmos de detecção posteriores. Entretanto, pacotes individuais não podem ser usados para identificar padrões incomuns durante um grande período. Existem ataques que contém cabeçalhos normais quando analisados individualmente, enquanto sua repetição durante um certo tempo pode ser considerada anômala. Um exemplo seria o ataque de negação de serviço, popularmente conhecido como *DoS*.

5.1.2 Corpo de pacote

Quando ataques são destinados a aplicações, os bytes maliciosos estão dentro do corpo do pacote e, portanto, as técnicas baseadas em cabeçalho não podem ser usadas. Isso representa um defeito considerável, principalmente porque diversos ataques da atualidade não são direcionados à rede em si, mas a aplicações conectadas a ela.

NIDS devem utilizar características baseadas em conteúdo, extraídas do corpo dos pacotes, para detectar tais tipos de ataques, uma vez que cabeçalhos podem aparentar completamente normais. Análise de conteúdo é computacionalmente mais cara do que análsie de cabeçalho porque requer uma inspeção mais profunda do pacote. Ela lida com uma variedade de tipo de conteúdo (pdf, jpg, HTML), compressão, e métodos que encobrem dados. Entretanto, o benefício da análise do corpo é ter acesso a todos os bytes transferidos entre os aparelhos na rede, permitindo a cosntrução de um rico conjunto de características baseadas em conteúdo para detecção de anomalia.

Como análise de conteúdo possui uma alta complexidade, diversos métodos focam em pequenos subconjuntos de conteúdo, como requisições HTTP ou apenas o JavaScript de um conteúdo baixado. Métodos baseados em anomalia não tentam comparar assinatoras

de malware conhecido, mas podem aplicar heurísticas, como Casamento de Padrões para detectar a presença de código shell.

5.2 Pré-processamento

Como anteriormente apontado, sistemas baseados em anomalia estão sujeitos a uma alta taxa de Falso Positivo. Apenas 1% sequer de Falso Positivo resulta em um número absurdo de falsos alertas. Deve-se ter em mente que servidores lidam com centenas de conexões simultâneas e inúmeros pacotes a cada centésimo de segundo.

O pré-processamento de dados é, então, exigido para atingir uma melhor performance na detecção de intrusão. O pré-processamento converte tráfego de rede em uma série de ocorrências, onde cada uma é representada por um vetor de características. As informações seguintes acerca dos dados e características foram baseadas nos estudos presentes em [**?**].

5.2.1 Derivação

Dfierentes tipos de características que podem ser usados em NIDS baseados em anomalia foram cobertos em [**?**]. Cada tipo de característica é derivada de vários métodos de pré-processamento, incluindo organizar pacotes em fluxos, analizar conteúdo de aplicações em busca de campos de interesse ou percorrer cabeçalhos de cada pacote. A derivação do potencial conjunto de características é um passo essencial para o NIDS baseado em anomalia. Analogamente, pré-processamentos subsequentes podem ajudar ainda mais a aumentar a eficiência do NIDS.

Métodos de pré-processamento de mineiração de dados podem ser usados, incluindo tranformação, redução e discretização de dados, como os apresentados em [**?**]. Uma técnica de redução geralmente utilziada é a *Principal Component Analysis*. PCA tem se msotrado útil para redução da dimensionaldiade dos dados, consequentemente redizindo o custo computacional do sistema de detecção

Para eliminar caracterśiticas redundantes, diversos algoritmos automatizados para

seleção de características também existem, resultando em redução de dados similar. Tais métodos de redução de dados fornecem um meio preciso para a conversão de um conjunto candidato para o conjunto final de características. É possível que métodos automáticos de redução possam melhorar ainda mais o NIDS, apesar de que alguns sistemas são construídos apenas se baseando no conhecimento de um especialista para construir conjuntos de características significativos.

5.3 Conjuntos de Características

5.3.1 Conexões múltiplas

Grande parte dos NIDS analisados em [**?**] usam dados de rede referentes a fluxo ou sessão. Características são construídas a partir do fluxo. O método mais popular é o de cabeçalho de pacotes utilizando características derivadas de múltiplas conexões (MCD). Essas características são geralmente divididas usando média, desvio padrão, e procentagem de fluxos, cobrindo múltiplas sessões. NIDS baseados em anomalia que utilizam essas caracterśiticas são capazes de discernir entre atividade normal da rede e tráfego incomum como *DoS* e *scanning*.

características MCD são geralmente extraídas a partir de conexões dentro de um intervalo de tempo. A maioria das características de MCD são baseadas em volume, como o a quantidade de conexões a um endereço de IP e porta em um espaço de tempo. Portanto, características derivadas de múltiplas conexões podem ser facilmente usados para detectar volumes excessivos de tráfego relacionados a *DoS* e *probing*. Como pacotes anômalos individuais não suprem o valor baseado em volume, eles podem ser ignorados.

5.3.2 Única conexão

Características derivadas de conexões individuais (SCD) são utilziadas para detectar comportamento anômalo dentro de uma úncia sessão. Elas podem apontar um protocolo inesperado, tamanhos incomuns de dados, timestamp não condizente, ou sequências incomuns de *flags* de TCP. Portanto, características SCD permitem detecção de uso anômalo da

rede por *backdoors*, túnel HTTP e afins.

As características SCD fornecem contexto que pode ser usado para encotnrar anomalias não contextuais. Por exemplo, se a temporização de pacotes dentro de uma porta monitorada não se encaixa com um perfil esperado, um alerta pode ser disparado, uma vez que pode se tratar de um protocolo de tunelamento.

5.3.3 KDD Cup 99

O KDD Cup 99 se trata de uma base dados para uso livre. Ela contém tanto características SCD quando MCD, incluindo 13 características baseadas em conteúdo que podem ser usadas para detectar ataques *R2L* e *U2R*. Tais características foram construídas por um especialista e involvem informações de mais alto nível, como o número de tentativas de login sem sucesso, se acesso root ao terminal foi conseguido, e o número de operações de criação de arquivo.

Consdierando que o KDD Cup 99 já tem mais de 15 anos, é provável que sessas características não sejam mais úteis para detectar os tipos de ataques recentes na realidade do fluxo de dados na rede atualmente. Para se detectar ameaças atuais, é necessário construir características baseadas em conteúdo novas, uma vez que o conteúdo em si mudou.

CHAPTER 6

CONCLUSÃO

Neste trabalho foram realizados estudos sobre o tema super-resolução de forma a avaliar sua aplicabilidade em dois cenários. O primeiro em imagens RGB de sequência de vídeo contendo uma pessoa, de forma a fornecer quadros de maior resolução a sistemas biométricos. Segundo em imagens de profundidade com objetos rígidos, a fim de verificar o potencial da aplicação futura com biometria.

Através da codificação de dois algoritmos, um para cada modalidade, mostrou-se que o método, mesmo baseado em um modelo simplificado de observação, permite a obtenção de resultados melhores no aumento da resolução espacial de imagens quando comparado a soluções tradicionais, como a interpolação bicúbica.

A confirmação da eficácia da super-resolução em sequências de vídeo contendo faces indica o potencial de sua aplicação em sistemas biométricos. Podendo tanto diminuir o custo, quanto permitir maior performance.

Em trabalhos futuros espera-se considerar outros tipos de movimento além da translação; tratar oclusões; experimentar e comparar outros métodos de estimação de movimento na etapa de alinhamento; avaliar os resultados obtidos com diferentes métodos de reconstrução; incluir estimação de ruído e desfoque; e quantificar a influência da super-resolução no aumento da performance de sistemas biométricos, como por exemplo, de reconhecimento facial.

BIBLIOGRAFIA