Correlação de Alertas Utilizando CBR em um *Internet Early Warning System*

Tarcisio Ceolin Junior, Osmar Marchi dos Santos, Giani Petri, Raul Ceretta Nunes, Luís Alvaro de Lima Silva
Programa de Pós-Graduação em Informática – PPGI
Universidade Federal de Santa Maria – UFSM
{ceolin,osmar,gpetri,ceretta,luisalvaro}@inf.ufsm.br

***Resumo*—Sistemas de Detecção de Instrução *(Intrusion Detection Systems – IDS)* são projetados para monitorar possíveis ataques à infraestruturas da rede através da geração de alertas. Com a crescente quantidade de componentes conectados, os IDS tradicionais não estão sendo suficientes para a efetiva detecção de ataques maliciosos, tanto pelo volume de dados como pela crescente complexidade de novos ataques. Nesse sentido, a construção de uma arquitetura *Internet Early Warning Systems* (IEWS) possibilita detectar precocemente as ameaças, antes de causar qualquer perigo para os recursos da rede. O IEWS funciona como um coletor de diferentes geradores de alertas (possivelmente IDS), centralizando e correlacionado informações afim de gerar uma visão holística da rede. Nesse contexto, o presente trabalho tem como objetivo descrever uma arquitetura para a correlação de alertas gerados por *IDS* dispersos geograficamente através da utilização da técnica de Raciocínio Baseado em Casos *(Case-Based Reasoning – CBR)*. Além da arquitetura, são apresentados resultados sobre um estudo de caso em um ambiente real.**

I. Introdução

A Internet é amplamente utilizada pela sociedade, indo da concretização de negócios até a realização de tarefas pessoais. Junto com a crescente dependência da nossa sociedade sobre recursos de Tecnologia da Informação (TI), as preocupações em relação a segurança estão cada vez mais urgentes, pois todos os dias são descobertas novas vulnerabilidades em sistemas que oferecem algum tipo de serviço na internet.

Segundo [1], é notório um acréscimo substancial no número de ataques cibernéticos ano após ano. Diante deste cenário [2], Sistemas de Detecção de Intrusão (*Intrusion Detection System* – IDS) tradicionais, por trabalhar de forma isolada, estão tornando-se obsoletos. Com a crescente quantidade de dispositivos conectados à rede, e consequentemente, o acréscimo de informações transferidas, os IDS tradicionais não estão sendo suficientes para efetiva detecção de ataques maliciosos.

Para suprir a necessidade de monitorar a Internet perante este novo cenário, uma nova abordagem, a construção de uma arquitetura *Internet Early Warning Systems* (IEWS) é apresentada por diversos pesquisadores [2], [3] e [4]. O objetivo deste sistema proteger as funcionalidades da Internet, detectando precocemente as ameaças, antes de causar qualquer perigo para os recursos da rede.

Em trabalhos anteriores [5] e [6], foi proposta uma modelagem de dados de uma base de conhecimento para IEWS (Knowledge Base Attacks Monitoring – KBAM). O modelo representa os dados de diferentes aspectos da rede com foco em eventos relacionados a detecção de intrusão, tais como: dados de alertas gerados por sistemas de detecção de intrusão, informações sobre medidas de respostas, estatísticas do tráfego e assinaturas de ataques já conhecidos. O presente trabalho tem como objetivo trabalhar sobre essa base de conhecimento, provendo uma forma de correlação entre alertas através do uso da técnica de Raciocínio Baseado em Casos *(Case-Based Reasoning – CBR)*.

Através da técnica de CBR, possibilita-se a criação de um ciclo que analisa informações de casos de alertas passados, automaticamente criando novos casos a partir de informações atuais. Esse trabalho descreve o desenvolvimento dessa arquitetura focando na correlação de alertas encontrados na base. Por ser um estudo preliminar, este trabalho contempla a etapa de recuperação do ciclo CBR inserida no contexto de detecção de intrusão.

O presente artigo é estruturado da seguinte forma. A próxima seção descreve conceitos fundamentais para o desenvolvimento do trabalho. Na seção III é apresentada uma arquitetura para a correlação de alertas utilizando a técnica CBR. Resultados do uso da arquitetura em um ambiente real são apresentados na Seção IV. A Seção V apresenta considerações finais e trabalhos futuros.

II. Conceitos Fundamentais

Essa seção descreve uma revisão sobre *Internet Early Warning Systems*, a base de conhecimento KBAM e a técnica de Raciocínio Baseado em Casos.

A. Internet Early Warning Systems – IEWS

O cenário atual da Internet juntamente com o acréscimo gradativo no número de informações compartilhadas pelas redes de computadores têm motivado a construção de *Internet Early Warning Systems*. Um IEWS trabalha no monitoramento da Internet e tem como objetivo principal a detecção precoce de eventos que ameaçam as funcionalidades da Internet [3]. Além disso, um IEWS visa construir uma consciência situacional e gerar contramedidas para ameaças atuais com base nas informações adquiridas do ambiente monitorado [6].

Segundo [3], um IEWS é composto por diversos componentes técnicos, dentre eles: sensores, componente de detecção, base de conhecimento, componente de reação e gerenciamento de incidentes, componente de perpetuação de evidências e componente de distribuição das informações.

Sensores são utilizados para a geração da visão da atual situação do ambiente monitorado, criando a consciência situacional. Além disso, são responsáveis pela detecção dos eventos

de segurança e identificação de novas ameaças. O componente de detecção é dividido em duas camadas: a camada de sinal, onde os dados da rede ou os logs são analisados por métodos de detecção por anomalia ou assinaturas, e a camada de eventos, na qual ocorre o relacionamento dos eventos da camada de sinal com eventos reportados por órgãos externos [7].

A base de conhecimento é um dos principais componentes de um IEWS, pois armazena informações de diferentes aspectos da rede. As assinaturas de ameaças, o comportamento da rede, as informações sobre os incidentes e suas medidas de respostas estão armazenadas na base de conhecimento e dão suporte a construção da consciência situacional do ambiente monitorado.

B. Knowledge Base Attacks Monitoring – KBAM

De modo a trabalhar como um componente técnico em arquiteturas de IEWS, a Base de Conhecimento KBAM [8], [9], [5] representa os dados de eventos de detecção de intrusão explorando o formato Intrusion *Detection Message Exchange Format* (IDMEF) para mensagens de detecção de intrusão e o formato *Intrusion Detection Response Exchange Format* (IDREF) para mensagens de respostas.

Os dados contidos na KBAM consideram os seguintes aspectos: dados de alertas gerados por sistemas de detecção de intrusão, informações sobre as medidas aplicadas em resposta a um alerta e a quantificação do tráfego da rede [8]. Ao modelar os dados com base nos formatos padrões IDREF e IDMEF, a KBAM pode ser inserida em infraestruturas de rede que possuem IDSs que utilizam esses padrões. Neste caso, a KBAM pode ser utilizada como um componente que armazena dados de diferentes aspectos da rede, que são essenciais para o monitoramento de ataques.

Em trabalhos anteriores foi proposto a integração de diferentes IDS utilizando-se um sistema gerenciador de eventos de segurança denominado Prelude [10]. Este sistema gerenciador de eventos é compatível com o formato IDMEF, permitindo que diferentes tipos de sensores criem alertas utilizando um único padrão de comunicação.

C. Raciocínio Baseado em Casos – CBR

CBR é uma técnica que busca soluções para problemas atuais em soluções encontradas no passado, baseando-se em uma das principais características do ser humano, a memória. Segundo [11], Sistemas de Raciocínio Baseado em Casos (*Case-Based Reasoning* – CBR) tem como objetivo resolver novos problemas utilizando e adaptando experiências anteriores contidas em um repositório de experiências concretas de soluções de problemas, denominada base de casos. Na forma mais simplificada, um caso é composto por três elementos: uma descrição do problema, uma solução e uma avaliação da solução. Em geral, o ciclo de CBR consiste em quatro etapas: recuperar (*retrieve*), reutilizar (*reuse*), revisar (*revise*) e reter (*retain*).

O ciclo CBR descrito em [12], considerado um formato completo que permite modelar os principais passos de um sistema CBR, é representado por um ciclo de raciocínio que pode ser contínuo. Este ciclo é composto pelas tarefas de recuperar, reutilizar, revisar e reter um caso. De acordo com o problema informado, ou novo caso usado como consulta no sistema CBR, a base de casos é pesquisada para buscar problemas anteriormente resolvidos. Este processo de busca é realizado de acordo com o nível de similaridade entre atributos do novo problema e da base de casos [11]. Em resumo, a partir da necessidade de resolver determinado problema, esta etapa de recuperação realiza uma busca na base de casos. Como resultado, a etapa de recuperação seleciona quais casos podem conter soluções relevantes (ou reusáveis) para a solução do novo problema, tomando como referência o nível de similaridade entre o problema atual e os casos da base de casos.

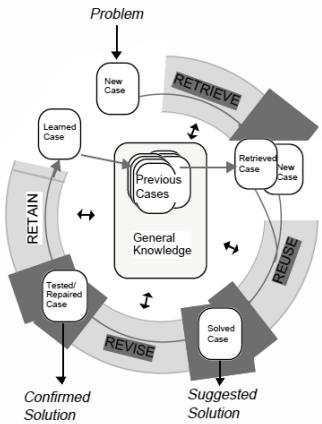

Figura 1. Ciclo CBR [12].

No processo de recuperação de casos, uma métrica de similaridade é uma função que permite avaliar analiticamente os graus de similaridade entre dois casos. Usualmente, são atribuídos pesos diferentes a cada uma das características de um caso. No intuito de combinar as similaridades medidas entre cada um dos atributos representados nos casos, ou similaridades locais, e métodos de agregação como a média ponderada aplicada a valores de similaridades locais são utilizados para gerar um valor global de similaridade entre dois casos. Neste processo, o valor de cada peso é diretamente proporcional à importância de cada atributo definido na estrutura de um caso. A determinação numérica de pesos é geralmente definida como resultado de um processo gradual de ajuste de pesos e consequente avaliação da performance do sistema. Em geral, este processo é caracterizado como um processo de tentativa e erro orientado por resultados de "precision and recall". Este trabalho foca na etapa de recuperação visto que esta etapa é fundamental para a performance de um sistema CBR.

III. Uma Arquitetura de Correlações de Alertas Utilizando CBR

Uma das principais características de um sistema IEWS é a capacidade de correlacionar eventos de segurança de forma

que uma atividade maliciosa seja detectada antecipadamente. Nesse sentido, o objetivo deste trabalho é a criação de uma consciência situacional a partir de uma ou diversas redes de computadores, através de agentes distribuídos geograficamente, correlacionando os alertas gerados por estes agentes em um sistema *Internet Early Warning Systems*.

Um sistema de Raciocínio Baseado em Casos tem como objetivo recuperar de sua base os casos mais similares ao problema apresentado. Os casos, que são alertas gerados por IDS distribuídos, não precisam ser necessariamente idênticos a situação atual. Porém, geralmente, quanto maior o nível de similaridade, melhor será a solução encontrada [12]. Um caso recuperado pode ser útil para a solução de determinado problema quando a similaridade entre o problema informado e o caso recuperado da base de casos é alta. Um ou vários casos podem ser recuperados, cabendo ao algoritmo determinar a melhor solução.

Para detectarmos a correlação entre um novo alerta e a extensão da base KBAM, utilizou-se métricas de similaridade local e global entre cada atributo do alerta informado. Similaridade local é utilizada para medir a similaridade entre cada atributo do novo alerta com cada atributo de todos alertas na base de casos (atacantes maliciosos). A partir do resultado do cálculo anterior, realiza-se uma média entre a soma dos resultados obtidos pela quantidade de atributos do alerta, tendo-se assim o cálculo de similaridade global entre dois casos selecionados.

A. *Correlação de Alertas*

A geração de alertas é feita através múltiplas instâncias do IDS Snort [13]. Estes sensores estão distribuídos em pontos distintos dentro da infraestrutura da UFSM e tem seus alertas centralizados diretamente na KBAM.

Inicialmente, para alimentarmos a base de conhecimento KBAM a ser utilizado como parâmetro de comparação, utilizamos todos os alertas gerados por IDS com o tipo de assinatura compatível com varredura de portas (port-scan). Um port-scan tem como objetivo testar as portas lógicas de determinado servidor remoto. Neste teste ele verifica o status das portas, se estão fechadas, escutando ou abertas. Técnicas de port-scan são utilizadas por pessoas mal intencionadas para identificar portas abertas em um computador remoto. Port-scan são facilmente detectados por IDS tradicionais.

Entre todos atributos do formato IDMEF, foram considerados como relevantes na estrutura de um caso, os quais são empregados no cálculo de similaridade: *Analyser ID* (identificador único do sensor), *DetectTime* (Instante de criação do alerta), *Classification* (Classificação do alerta), *Source IP* (Identificação do atacante), *Target IP* (Identificação do alvo), *Source Port* (Porta de origen) e *Target Port* (Porta de destino).

Quando um novo alerta é gerado, o mesmo é correlacionado medindo-se a similaridade entre os atributos do novo alerta e os atributos de cada alerta de toda a base de casos. Assim, ordena-se o resultado encontrado por ordem decrescente por similaridade.

Através de um conjunto de testes randômicos, foram utilizadas diferentes métricas para cálculo de distância ou de similaridade entre os diferentes atributos selecionados. Foram obtidos melhores resultados utilizando-se o cálculo de distância Euclidiana. Após isso, definiu-se pesos, novamente através de testes, para cada atributo de acordo com a sua relevância para a solução do problema. Por exemplo: o endereço IP do atacante é considerado um atributo de grande importância para a correlação de alertas. Logo, o mesmo recebe um peso 2 pela sua importância. O mesmo critério serve para quantificar o peso do atributo Sensor ID.

Para realizar o cálculo de distância entre atributos que referenciam uma unidade de tempo foi utilizada a seguinte abordagem. Converte-se do formato *timestamp* para *unixtime* e então calcula-se a distância euclidiana entre os valores. A seguir, segundo os testes realizados, percebeu-se que quanto menor a distância entre os atributos, maior era a precisão de acertos nos resultados obtidos. Quanto a classificação do alerta, foi construída uma taxonomia dos diferentes tipos de classificação de ataques e, partir disto, realizado o cálculo de distância entre este atributo.

Com base em testes realizados, obteve-se melhores resultados (possibilidade de um novo alerta malicioso) quando a similaridade foi superior a 90% (valor de threshold que possibilita obter melhores resultados na performance do sistema), sendo assim, utilizou-se essa métrica em todos experimentos.

IV. Estudo de Caso

O ambiente de testes foi utilizado para verificar os resultados da abordagem proposta anteriormente. Conforme descrito na Tabela I, observa-se que a partir da grande quantidade de alertas gerados, foram extraídos cerca de 3000 alertas, estes classificados como *port-scan* e inseridos na base inicial de casos da aplicação CBR. Nesta abordagem, consideramos que todo atacante malicioso, inicialmente, realiza um ataque *port-scan.*

Tabela I. CONTAGEM DE ALERTAS E PORT-SCAN EM DISTINTOS IDS

servidor	alertas	port-scan
coral.ufsm.br	72209	1936
sucuri.cpd.ufsm.br	108152	354
coralx.ufsm.br	348263	513
husm.ufsm.br	28500	84
coperves.ufsm.br	72486	71

Um caso pode conter um ou mais atributos, conforme as características do cenário de intrusão ou da atividade suspeita sendo descrita. Um exemplo de port-scan já inserido como caso é apresentado na Tabela II. O caso descreve cada atributo utilizado para calcular a similaridade entre novos casos.

Tabela II. MODELO DE REPRESENTAÇÃO DE UM CASO

Atributo	Caso A
Alert ID	970690
Sensor ID	snort-coralx (1)
Detection time	2013-07-12 11:58:47
Source IP Address	113.107.205.57
Source Port	25:80
Target IP Address	200.18.33.52
Target Port	25:80
Service Protocol	TCP
Alert Type	(portscan) TCP Portscan
Classification Type	13

Na Tabela III é descrito o cálculo de similaridade entre um alerta da base de casos e dois novos alertas gerados por

Tabela III. MODELO SIMPLES PARA REPRESENTAÇÃO DO CÁLCULO DE SIMILARIDADE

Atributo	Caso A	Alerta 1	S1	Alerta 2	S2
Sensor ID	snort-coralx (1)	snort-sucuri (2)	0	snort-coralx (1)	1
Detection Unixtime	1373630327	1378617841	0,2	1373958426	0,6
Source IP	113.107.205.57	218.108.170.169	0	113.107.205.57	1
Source Port	25:80	8080	0	80	1
Target IP	200.18.33.52	200.18.33.57	0	200.18.33.52	1
Target Port	25:80	8080	0	80	1
Service Protocol	TCP	TCP	1	TCP	1
Classification Type	13	9	0	13	1
Alert Type	(portscan) TCP Portscan	WEB-CGI /cgi-bin/ access	*	Cross-Site scripting attempt	*

dois IDS, devidamente identificados no atributo *Sensor ID*. O atributo Alert ID refere-se ao identificador único de cada alerta na base de casos.

No exemplo, observa-se que o mesmo atacante em um primeiro momento, realizou um *port-scan* e foi inserido na base de casos. Em seguida pode-se observar que o mesmo atacante disparou dois novos alertas em servidores distintos. Analisando o Alerta 1, não foi observado praticamente nenhum grau de similaridade (S1) entre os atributos analisados. Já analisando o grau de similaridade (S2) entre os atributos do Alerta 2 e o Caso A, percebe-se que só não ocorreu uma alta similaridade no atributo *Detection Unixtime.*

Com base nessa análise, pode-se observar que o Alerta 1 é um falso-positivo. Já para o Alerta 2, uma resposta no padrão IDREF pode ser gerada e enviada para todos servidores monitorados da rede, com o objetivo de bloquear qualquer tráfego originado do endereço IP deste atacante em questão.

V. CONCLUSÃO

O conceito de *Internet Early Warning Systems* (IEWS) tem como objetivo possibilitar a detecção precoce de eventos maliciosos sobre a Internet. O presente trabalho apresentou uma forma de correlacionar eventos maliciosos sobre uma base de conhecimento (KBAM), que representa informações de um IEWS, desenvolvida anteriormente em nossos projetos de pesquisa [5], [6], [9]. Nesse trabalho, a correlação de eventos maliciosos foi realizada através da técnica de Raciocínio Baseado em Casos *(Case-Based Reasoning – CBR)*, focando-se na fase de recuperação de casos. Uma das grandes dificuldades no desenvolvimento deste trabalho foi o dimensionamento dos pesos dos atributos utilizados nas correlações. Resultados apresentados sobre um estudo de caso real, demonstram a viabilidade da técnica.

Como primeiro trabalho futuro, pretende-se analisar mudanças na arquitetura da base KBAM. Atualmente, um conjunto muito grande de informações é gerado na base. Utilizando a própria solução desenvolvida nesse artigo, a base de conhecimento poderia ser reduzida, eliminando uma grande quantidade de falsos-positivos do sistema.

Outro trabalho futuro importante é o uso de arquiteturas de baixo custo, como Raspberry Pi [14] ou BeagleBoard [15], para o desenvolvimento embarcado de sensores dinâmicos de alertas (*probes*), que serviriam de fonte a base de conhecimento KBAM. Pelo baixo custo destes equipamentos embarcados, seria possível colocar em funcionamento centenas de sensores em uma mesma organização (ou até país), obtendo um ótimo índice de monitoramento da rede. Esse trabalho já está em fase de testes, onde foram desenvolvidos softwares de captura e envio de alertas diretamente para a KBAM a partir de *probes* de baixo custo.

REFERÊNCIAS

[1] CERT.BR, "Centro de Estudos, Resposta e Tratamento de Incidentes no Brasil." 2013. [Online]. Available: http://www.cert.br/

[2] M. Golling and B. Stelte, "Requirements for a future EWS-Cyber Defence in the internet of the future," *2011 3rd International Conference on Cyber Conflict (ICCC)*, pp. 1–16, 2011. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5954706

[3] S. Bastke and S. Schmidt, "Internet Early Warning Systems - Overview and Architecture Objectives of an Internet Early Warning Sys- tem A definition for early warning in the area of natural catastrophe is following :," pp. 1–19, 2009.

[4] M. Apel, J. Biskup, U. Flegel, and M. Meier, "Towards Early Warning Systems – Challenges, Technologies and Architecture," *Critical Information Infrastructures . . .*, pp. 151–164, 2010. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-14379-3_13

[5] G. Petri, T. Ceolin Junior, R. C. Nunes, and O. M. Santos, "Modelagem de uma Base de Conhecimento para o Monitoramento de Ataques," *Escola Regional de Redes de Computadores*, 2012.

[6] G. Petri, R. C. Nunes, V. L. O. Lopez, T. Ceolin Junior, and O. M. Santos, "Building Situation Awareness to Monitor Critical Infrastructures," *Latin-American Symposium on Dependable Computing (LADC)*, 2013. [Online]. Available: http://www.lbd.dcc.ufmg.br/colecoes/ladc/2013/0019.pdf

[7] G. Fan, Y. JiHua, and Y. Min, "Design and implementation of a distributed IDS alert aggregation model," *4th International Conference on Computer Science \& Education, 2009. ICCSE '09.*, pp. 975–980, 2009. [Online]. Available: http://ieeexplore.ieee.orghttp://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5228172

[8] G. Petri, "Modelo de Dados de uma Base de Conhecimento para Internet Early Warning Systems," Master's thesis, Universidade Federal de Santa Maria, 2013.

[9] G. Petri, R. C. Nunes, V. L. O. Lopez, T. Ceolin Junior, and O. M. Santos, "KBAM: Data Model of a Knowledge Base for Monitoring Attacks," *Latin-American Symposium on Dependable Computing (LADC)*, 2013. [Online]. Available: http://www.lbd.dcc.ufmg.br/colecoes/ladc/2013/0021.pdf

[10] Prelude, "Prelude SIEM." [Online]. Available: http://www.prelude-ids.com/index.php/uk/

[11] A. von Wangenheim and C. G. von Wangenheim, *Raciocínio Baseado em Casos*, 2003.

[12] A. Aamodt and E. Plaza, "Case-based reasoning: Foundational issues, methodological variations, and system approaches," *AI communications*, vol. 7, pp. 39 —- 59, 1994. [Online]. Available: http://iospress.metapress.com/index/316258107242JP65.pdf

[13] Snort, "Snort." [Online]. Available: http://www.snort.org/

[14] R. Pi, "Raspberry Pi." [Online]. Available: http://www.raspberrypi.org/

[15] BeagleBoard, "BeagleBoard.org." [Online]. Available: http://beagleboard.org/Products/BeagleBone