Sistemas de detecção de intrusão em ambientes de nuvem

João Fiuza de Alencastro
Departamento de Engenharia Elétrica
Universidade de Brasília

***Abstract*—Pela sua natureza distribuída, ambientes são alvos fáceis de serem explorados. Atacantes disfarçados de usuários legítimos podem se aproveitar dos abundantes recursos que a nuvem pode oferecer. Neste artigo é discutido como um sistema de detecção de intrusão distribuído em nuvem funciona, suas vantagens e desvantagens.**

***Index Terms*—Cloud computing, Intrusion Detection, security.**

I. Introdução

AO analisar ambientes em nuvem, deve-se ter sempre uma visão distribuída dos componentes da topologia. Assim como aplicações comuns da internet, esses ambientes também são alvos de ataques mal intencionados.

Os nós fazem parte dessa composição, esses quais devem ser monitorados individualmente, e quando um ataque ocorre, todos os outros nós que compõem a rede devem ser notificados do padrão de ataque que pode ser eminente.

O monitoramento pode ser realizado por sistemas de detecção de intrusão, porém toda a comunicação requer compatibilidade entre os diferentes hospedeiros, mecanismos de comunicação, e permissões de controle sobre manutenções e atualizações dos sistemas. Middlewares em nuvem normalmente provêm tais funcionalidades, portanto uma opção interessante seria um serviço de IDS oferecido na camada de middleware (em oposição às camadas de infraestrutura e de software) [1].

II. Computação em Nuvem

A computação em nuvem é um modelo computacional no qual os recursos são providos como um serviço através da internet. Movida conforme a demanda, ela trabalha desafogando do usuário a responsabilidade de comprar e gerenciar equipamentos complexos e dedicados de infraestrutura.

O aluguel de recursos computacionais sob-demanda desloca a responsabilidade de gerência e administração para uma equipe de especialistas, reduzindo os riscos de segurança tipicamente oriundos de má configuração de sistema, falta de atualizações, ou comportamento indevido do usuário. Apesar disso, o ambiente em nuvem introduz um risco considerável ao fazer com que os usuários compartilhem recursos físicos.

Cada um desses riscos de segurança deve ser tratado de forma cautelosa e de forma específica, seja o ataque conhecido ou não, deve ser detectado e devidamente analisado. Esta é outra razão pela qual uma solução integrada, levando em conta diferentes aspectos relacionados à segurança, é necessária para proteger dados de usuários e prevenir ações maliciosas contra ambientes em nuvem[2].

III. Intrusões em 'Grid'

A. Acesso não-autorizado

É uma intrusão feita por alguém que não deveria ter acesso por meio de uma máscara ou um disfarce de usuário legítimo. Pode ser feito conseguindo a senha do usuário, seja por roubo, força bruta, palpitação, ou até mesmo por descuido do mesmo. Ataques ao serviço de autenticação é outra possibilidade, porém pode deixar rastros.

B. Uso indevido

Pode ser uma consequência de (A), configurado como abuso de privilégios de um usuário legítimo e geralmente resulta em um comportamento anômalo. Depende de quais políticas foram definidas pelo prestador do serviço.

C. Ataque em 'Grid'

Ataques realizados com a utilização de ferramentas ou scripts de *'exploits'* que almejam vulnerabilidades de protocolos,serviços e aplicações em 'grid'. Esses podem aparecer em forma de negação de serviço, sondas, e vermes, e pdem deixar rastros de sua existência em vários pontos a infraestrutura.

D. Instrusões específicas de hospedeiro/rede

Enquanto que (A), (B) e (C) são ataques específicos em 'grid', estes são quaisquer outros ataques aos hospedeiros ou à rede[3].

IV. Detecção de Intrusão

Um ataque a um sistema de computação em nuvem pode ser silencioso "aos olhos" de um IDS baseado em rede, ou um NIDS, já que a comunicação entre nós, ou a comunicação a nível de aplicação é, normalmente, criptografada. E também, na visão do IDS baseado em detecção interna do hospedeiro, ou HIDS, pode ser despercebido, já que nem sempre ataques específicos de nuvem deixam rastros nos sistemas operacionais que compõem os nós. Dessa maneira, IDS's tradicionais não são o suficiente para identificar os ataques a ambientes em nuvem.

Em [1] é proposto o 'Grid and Cloud Computing Intrusion Detection System' (GCCIDS), um tipo de IDS específico

para nuvem, no qual tem um sistema de auditoria embutido, integra conhecimento e análise comportamental para detectar intrusões.

Na solução apresentada, cada nó identifica eventos locais que possam representar ameaças e violações e alerta os outros nós. Cada IDS individual coopera na detecção de intrusão.

Os nós contêm os recursos, enquanto que o middleware define as políticas de acesso e controle e suporta um ambiente orientado a serviço.

O componente auditor de eventos citado no sistema proposto captura dados de várias fontes, como logs de sistemas, serviço, e mensagens entre nós. Dessa maneira, o serviço de IDS analisa esses dados e aplica as devidas técnicas de detecção. Caso seja encontrado algo incomum ou inválido, o middleware é responsável por comunicar os nós e sincronizar suas tabelas de ”vacinas”. É importante mencionar que todos os nós devem ter acesso aos mesmos dados, para que o middleware possa criar uma virtualização do ambiente homogêneo[1].

V. Tratamento de erros

A partir do momento que o auditor de eventos armazena a atividade maliciosa, dependendo o ’timing’ do IDS, ele pode tratá-los em tempo real ou esperar certo período de tempo. Cada aplicação trata esse serviço de forma que a convir.

A informação auditorada é processada pelo núcleo do IDS, que analisa seu comportamento utilizando inteligência artificial para detectar suas divergências. O analisador de regras recebe pacotes auditorados e determina se alguma regra está sendo quebrada, depois retorna o resultado ao núcleo de serviço do IDS. Em posse desses resultados, o IDS calcula a probabilidade de a ação representar ou não um ataque, caso seja uma ameaça grande o bastante, gera um alerta aos outros nós.

VI. Proposta para IoT

Analogamente, se um serviço que oferece uma aplicação em nuvem, trata-se a detecção de invasão dessa forma, aplicaremos esta abordagem em um ambiente de Internet das Coisas (IoT).

Utilizando a definição de IoT em [4] como referência, onde há uma comunicação direta e indireta entre sensores/dispositivos e o middleware, utilizando comunicação ’Machine-to-Machine’ (M2M), normalmente via serviço web REST. Este middleware proposto apresenta grande similaridade com a arquitetura orientada a serviço (SOA).

Partindo desse ponto, sabe-se de certa forma como é o tráfego da comunicação estabelecida, mesmo que em vários pontos, é tangível fazer uma estimativa real levando em consideração os objetos na rede IoT.

Seguindo um viés de segurança cibernética, deve ser considerado ataques nessas instâncias da rede IoT, e como foi visto em III, intrusões em ’Grid’ são comuns em sistemas finais, como especificados a cima. Logo, o tráfego proveniente dos objetos, na visão do middleware, deve ser analisado. É proposto, então, a utilização de um sistema de detecção de instrusão de rede (NIDS) no middleware em questão.

No sistema proposto, todo o tráfego da instância será auditorado e analisado baseado no que é considerado comum, caso o sistema encontre possíveis intrusões, o middleware tomará as devidas ações relacionadas a essa atividade.

VII. Conclusão

Serviços de nuvem são, em sua grande maioria, utilizados por usuários desinformados na área de segurança da informação. Sobem aplicações sem a menor noção de vulnerabilidades expostas, deixam portas abertas, entrada de dados de usuário sem tratamento, entre outros erros comuns. Por esses e outros motivos, compartilhamento de recursos em ambientes em nuvem podem se tornar extremamente inseguros, logo a segurança deve ser provida pelo contratado. Isso facilita todo o processo de segurança, já que ele tem a visão maior da infraestrutura do ambiente. Apresentados neste artigo, os métodos de detecção de intrusão são independentes das aplicações que são executadas nas camadas superiores.

O middleware citado acima facilita o processo de intagração dos diferentes componentes utilizados em uma rede em nuvem, serve como controlador dos dados e os centraliza, lembrando bastante uma rede definida por software (SDN), tema bastante debatido na atualidade.

Apesar de não ter sido muito abordado, a inteligência artificial que se baseia em redes neurais para a análise dos dados autidorados é muito bem vista da área de detecção de anomalias. Porém, é algo que deve ser utilizado com muito conhecimento e deve passar por muitos testes antes de ser considerada válida, pois redes neurais artificiais não são determinísticas e geram falso positivos e negativos em uma progressão não-linear.s

References

[1] Intrusion Detection for Grid and Cloud Computing - CyberSecurity, Kleber Vieira, Alexandre Schulter, Carlos Becker Westphall, and Carla Merkle Westphall, Federal University of Santa Catarina, Brazil.

[2] Integrating a Network IDS into an Open Source Cloud Computing Environment, 2010 Sixth International Conference on Information Assurance and Security - Claudio Mazzariello, Roberto Bifulco and Roberto Canonico.

[3] Intrusion Detection For Computational Grids, Alexandre Schulter, Kleber Vieira, Carols Westphal, Carla Westphal,Sekkaki Abderrahim.

[4] Increasing the Dependability of IoT Middleware with Cloud Computing and Microservices - UCIoT 2017 Workshop Presentation UCC Companion’17 - Rafael T. de Sousa Júnior, Lucas M. C. e Martins, Francisco L. de Caldas Filho, William F. Giozza, João Paulo C. L. da Costa.