SEGURANÇA EM INTERNET DAS COISAS

por Daniel Batista, Carlos Alberto Kaminski
e Otto Carlos Muniz Bandeira Duarte

O AUMENTO SIGNIFICATIVO DA QUANTIDADE DE DISPOSITIVOS CONECTADOS À INTERNET, NA CHAMADA INTERNET DAS COISAS, TRAZ NOVOS DESAFIOS À SEGURANÇA DA INFORMAÇÃO. COMO PROTEGER ESSE NOVO AMBIENTE DE FORMA EFICIENTE E ESCALÁVEL?

A aglomeração de pessoas ocasiona diversos problemas intrínsecos às cidades, e são necessárias novas soluções para esses problemas emergenciais de natureza pública. O conceito de cidades inteligentes prevê ambientes nos quais a tecnologia da informação seja uma ferramenta para resolver alguns desses problemas. Para isso, é necessário uma rede interconectada de dispositivos que monitoram a cidade, conhecida como rede de sensoriamento urbano[1].

Os novos dispositivos conectados na internet, incluindo aqueles que fornecem dados que ajudam indiretamente nas tomadas de decisão dos gestores das cidades, como telefones celulares, relógios inteligentes e carros autônomos, compõem a chamada Internet das Coisas (*Internet of Things* – IoT).

O fluxo de informação em uma cidade inteligente com dispositivos pertencentes à IoT consiste na coleta de dados pelos sensores, processamento desses dados em ambientes distribuídos e envio de decisões para atuadores. A expectativa por uma grande quantidade de sensores em uma cidade inteligente traz como consequência um alto volume de dados trafegado na rede. Ataques de segurança em um ambiente como esse podem trazer sérios problemas para a população, já que agora o ambiente computacional não se restringe a uma empresa de TI ou ao computador pessoal de um usuário, mas, sim, à cidade como um todo. A detecção desses ataques deve ser feita o mais rápido possível, de preferência antecipadamente, o que justifica a implantação de mecanismos de monitoramento em diversos pontos da infraestrutura de TI da cidade. Entretanto, as ferramentas atuais de monitoramento de rede não atendem às necessidades de velocidade e gerenciamento de grandes domínios de rede como o de uma cidade inteligente. Além disso, muitas dessas ferramentas geram uma enorme quantidade de dados que requerem processamento de outro tipo de ferramentas para extrair conhecimento dos dados coletados.

O fluxo de informação em uma cidade inteligente consiste na coleta de dados pelos sensores, processamento desses dados em ambientes distribuídos e envio de decisões para atuadores.

Muitas das soluções que vêm sendo desenvolvidas para melhorar o desempenho dos atuais sistemas de segurança para cenários como a IoT baseiam-se em sistemas de processamento por fluxos para grandes massas de dados como o Apache Spark[2 3]. Nessas soluções, também é comum a utilização de ferramentas para filtragem de dados, como

o Logstash, para agregação dos dados, como o Kafka, e para visualização de dados, como o Kibana. É importante observar que a simples instalação das ferramentas não é suficiente para resolver os problemas. É necessária a implementação de algoritmos principalmente para realizar a classificação do tráfego[4].

Além do monitoramento de dados das camadas de rede e de transporte na IoT, existem propostas que buscam antecipar ataques por meio de dados não estruturados como aqueles divulgados por seres humanos em redes sociais online[5]. Nesse caso, o monitoramento é feito diretamente na camada de aplicação. A justificativa para utilizar redes sociais online em sistemas de segurança vem principalmente do fato de que, nesses ambientes, usuários tendem a propagar mensagens consideradas relevantes, além de serem influenciados por outros usuários com muitos seguidores[6].

Apesar do avanço que vem sendo realizado em segurança da informação para IoT, diversos desafios de pesquisa ainda precisam ser resolvidos, como a redução de falsos positivos gerados pelos sistemas de alerta, a busca pelos melhores algoritmos de aprendizado de máquina para detecção de novos ataques e o desenvolvimento de técnicas mais eficientes para a correlação de dados heterogêneos. ●

Referências

1 ZYRIANOFF, I.; BORELLI, F.; KAMIENSKI, C. A. SenSE - Sensor Simulation Environment: Uma ferramenta para geração de tráfego IoT em larga escala. In: Anais do Salão de Ferramentas do SBRC 2017, pg. 1134-1141.

2 https://www.gta.ufrj.br/catraca

3 http://gtbis.ime.usp.br

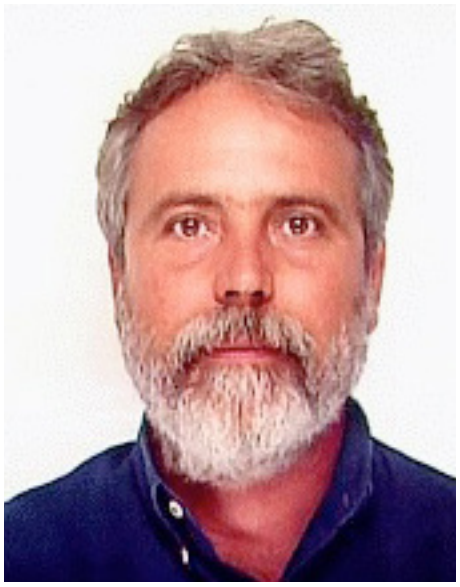
4 SANTOS, L. A. F. ; CAMPIOLO, R. ; MONTEVERDE, W. A. ; BATISTA, D. M. . Abordagem autonômica para mitigar ciberataques em LANs. In: Anais do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC 2016), pg. 600-613.

5 http://gtews.ime.usp.br

6 ZANOTTO, D.; KAMIENSKI, C. A. Compreendendo Mecanismos de Influência no Twitter através do Comportamento dos Usuários. In: Anais do Workshop de Redes P2P, Dinâmicas, Sociais e Orientadas a Conteúdo (Wp2p+ 2016), pg. 3-16.

DANIEL MACÊDO BATISTA | É professor associado no DCC da USP, onde trabalha desde 2011. De 2014 a 2017 coordenou o projeto "GT-EWS: Mecanismos para um Sistema de Alerta Antecipado", e desde abril de 2017, coordena o projeto "GT-BIS: Mecanismos para Análise de Big Data em Segurança da Informação". Os dois projetos foram financiados pela RNP e estão relacionados com segurança da informação.

CARLOS ALBERTO KAMIENSKI | É professor titular no CMCC da UFABC, onde trabalha desde 2006. Seus interesses atuais de pesquisa incluem computação em nuvem, redes definidas por software, análise de redes sociais online, cidades inteligentes e Internet do Futuro. Coordenou e participou de vários projetos financiados por agências de fomento, órgãos públicos e empresas privadas.



OTTO CARLOS MUNIZ BANDEIRA DUARTE | É professor titular na COPPE da UFRJ, onde trabalha desde 1978. Desde 2017 coordena o projeto "SUNI: Infraestrutura de Rede Unificada e Segura", financiado pelo CNPq, e desde 2015 coordena o projeto "VISEMFUN: VIrtualização, SEgurança, grande Massa de dados, internet do FUturo e Nuvem", financiado pela FAPERJ. Ambos têm relação com segurança da informação.