METODOLOGIA PARA A GESTÃO SEGURA NO USO DE UMA REDE DE IOT

Monteiro, T.G.[(1)], Mota, L.T.M.[(2)],

(1) PPG em Engenharia Elétrica, PUC-Campinas, Brasil. E-mail: tiago.monteiro@gmail.com
(2) PPG em Engenharia Elétrica, PUC-Campinas, Brasil. E-mail: lia.mota@puc-campinas.edu.br

Introdução: O aumento do uso de dispositivos conectados à Internet e também o surgimento da Internet das Coisas (IoT – Internet of Things) levaram a uma explosão na quantidade de dados que trafegam pelas redes mundiais. Nesse tráfego, é necessário garantir a privacidade dos dados, e consequentemente, de seus usuários e beneficiários.

Objetivos: Este trabalho tem por objetivo apresentar uma metodologia de gestão segura no uso de dados em uma rede IoT, visando garantir que somente os agentes autorizados tenham acesso a esses dados.

Metodologia: Através da análise de artigos científicos foi possível a identificação de diversos aspectos das redes IoT que carecem de uma análise mais detalhada. Um destes aspectos é a segurança dos dados que trafegam por essas redes. Os ataques realizados por *hackers* na tentativa de conseguir esses dados são cada vez mais robustos e variados.

As questões de segurança primordiais em redes IoT são: uso de redes não confiáveis, maior parte dos acessos é por meio remoto, falta de interfaces de atualização confiáveis e a criptografia de dados não é suportada por dispositivos IoT.

Foram analisadas as metodologias de gerenciamento de Tecnologia da Informação (TI) como o ITIL (*Information Technology Infrastructure Library* ou Biblioteca de Infraestrutura de Tecnologia da Informação) e o COBIT (*Control Objectives for Information and related Technology* ou Objetivos de Controle de Informação e Tecnologia Relacionada) mas estas metodologias estão focadas em garantir a uniformidade da infraestrutura das redes de TI e padronização dos softwares utilizados nessas redes.

Em virtude destes aspectos este trabalho propõe uma metodologia onde a inclusão de certificados digitais garanta um único e exclusivo acesso à rede IoT, através da chave criptografada assimétrica presente nesse tipo de certificado. A propriedade do certificado é do administrador da rede e a sua segurança é garantida por uma empresa certificadora ou por um serviço na rede, como por exemplo os disponíveis na Amazon Web Service IoT (AWS-IoT) e na Microsoft AZURE – IoT Edge.

A inclusão de certificados digitais no início das configurações das redes IoT tem sido uma alternativa já usada em ambientes virtuais e que tem apresentado resultados satisfatórios. É claro que o ambiente virtual desses serviços já dispõe de uma segurança adicional presente em todos os serviços oferecidos pela internet através do controle de acesso aos sites.

Resultados: Através de uma análise dos tipos de certificados disponíveis levando em conta que o uso de certificados pagos tem um preço extremamente alto, o que inviabiliza seu uso em redes IoT residenciais e de empresas de pequeno porte, demonstra-se que o mais indicado é o uso de certificados fornecidos em serviços virtuais, como AWS-IoT e Microsoft AZURE IoT Edge.

Conclusões: Mesmo com a solução dada por grandes empresas de rede virtuais de IoT, o uso dos certificados ainda necessita de um alto investimento para que o administrador (proprietário) da rede IoT possa configurar os parâmetros de segurança necessários para sua rede.

Palavras-chave: Internet das Coisas, Segurança, Certificados Digitais

Tema Preferencial: Área 5: Internet das Coisas (IoT – Internet of Things)