IdP4IoT: Autenticação de Dispositivos da IoT em Provedores de Identidades SAML

Michelle Silva Wangham[1,3], **Allex Magno**[2,3], **Felipe Cardoso**[2,3]

[1]Laboratório de Sistemas Embarcados e Distribuídos (LEDS)
Universidade do Vale do Itajaí (UNIVALI) – Itajaí, SC – Brasil

[2]Instituto Federal de Santa Catarina (IFSC) – São José, SC – Brasil

[3]Rede Nacional de Ensino e Pesquisa (RNP)

wangham@univali.br, allex.m@aluno.ifsc.edu.br

felipepassoscardoso@gmail.com

Abstract. *Internet of Things (IoT) covers hardware, software, and services infrastructure able to connect things to the Internet. Things need authentication for secure communication. Support for different authentication mechanisms for devices in the same infrastructure is an open problem in the context of IoT. This lightning talk describes a SAML Identity Provider able to authenticate IoT devices that is available for researchers at GIdLab from RNP. After authentication, IdP issues short-lived tokens in a portable and interoperable manner (SAML tokens).*

1. Introdução

A Internet das Coisas (IoT) apresenta características como restrições de recursos computacionais e de energia. Neste cenário, as questões de segurança requerem abordagens diferenciadas das adotadas nos ambientes computacionais tradicionais [Atzori et al. 2010]. Na IoT, dispositivos heterogêneos precisam provar a sua autenticidade para as entidades com as quais se comunicam. Um problema neste cenário é garantir a autenticidade de dispositivos que se comunicam entre si e que podem estar localizados em domínios administrativos de segurança diferentes [Wangham et al. 2013].

A especificação SAML 2.0 define um padrão de representação e troca de informações de segurança entre componentes de um sistema distribuído. Por ser um padrão, o uso do SAML favorece a interoperabilidade entre sistemas. O SAML provê ainda suporte nativo a mecanismos para autenticação de dispositivos e de usuários, além de pontos de extensão que permitem a inclusão de outros mecanismos de autenticação, sem perda de interoperabilidade. Mensagens SAML podem ser transportadas utilizando mensagens HTTP padrão, o que viabiliza o uso da especificação tanto para autenticação de usuários quanto de dispositivos da IoT. O padrão SAML é a solução mais adotada em sistemas de gestão de identidades que seguem o modelo federado e proveem autenticação única (*Single Sign On*) federada de usuários. Entretanto, a gestão de identidade federada de dispositivos ainda é um desafio de pesquisa [Oliveira et al. 2017] e requer soluções (projetos e experimentações) que visam lidar com os desafios da IoT.

Esta palestra curta visa apresentar o **IdP4IoT**, um Provedor de Identidades (*Identity Provider* - IdP), baseado na especificação SAML (*Security Assertion Markup Language*), capaz de autenticar dispositivos IoT, por meio de diferentes mecanismos. Após

a autenticação, o IdP gera *tokens* de vida curta, os quais são aceitos por entidades que confiam no IdP e das quais o dispositivo deseja consumir um recurso. O IdP4IoT é uma atualização e extensão do trabalho desenvolvido em [Domenech et al. 2016] que, atualmente, está disponível no serviço para experimentação GIdLab[1] da RNP, possibilitando que pesquisadores possam conduzir experimentos utilizando diferentes métodos de autenticação. Nesta nova versão, o IdP, que utiliza o *framework* SimpleSAMLPHP, suporta além do perfil SAML Web browser SSO, o perfil ECP (*Enhanced Client and Proxy*)[2], que define a troca de informações de segurança envolvendo clientes ativos que não usam um navegador web. Entretanto, a implementação do perfil ECP no IdP SimpleSAMLPHP possibilita apenas autenticação via *HTTP Basic authentication*. O IdP4IoT suporta os seguintes métodos de autenticação: senha/pin, certificado digital e o acordo não-interativo de chaves de sessão Sakai-Ohgishi-Kasahara - SOK [Sakai et al. 2000], que é um criptosistema baseado em identidades. O IdP4IoT está sendo desenvolvido para que novos mecanismos de autenticação possam ser implementados e adicionados. Pesquisadores que desenvolvem soluções de autenticação de dispositivos podem receber o auxílio da equipe do GIdLab para integrar seu método de autenticação ao IdP4IoT.

Conforme definido em [Domenech et al. 2016], os atributos dos dispositivos são o número de série (identificador único), nome de exibição, contato do administrador ou dono, organização, unidade organizacional, descrição, tipo de dispositivo, referência de localização física (latitude, longitude, altitude), disposição (fixo ou móvel), exposição (*indoor* ou *outdoor*) e status (*online* ou *offline*). Uma aplicação web de registro foi desenvolvida para ser utilizada pelo administrador do IdP para cadastrar, recuperar, atualizar e excluir registros de dispositivos (seus atributos). Por fim, vale destacar ainda que clientes ativos de exemplos (para serem embarcados em dispositivos de IoT) estão sendo desenvolvidos em Java, possibilitando que pesquisadores e interessados testem o IdP4IoT.

Referências

Atzori, L., Iera, A., e Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15):2787–2805.

Domenech, M. C., Boukerche, A., e Wangham, M. S. (2016). An authentication and authorization infrastructure for the web of things. In *Proceedings of the 12th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Q2SWinet '16, pages 39–46, New York, NY, USA. ACM.

Oliveira, L. B., Pereira, F. M. Q., Misoczki, R., Aranha, D. F., Borges, F., Nogueira, M., e Wangham, M. (2017). O computador para o século 21: Desafios de segurança e privacidade após 25 anos. In *Minicursos do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg 2017*.

Sakai, R., Ohgishi, K., e Kasahara, M. (2000). Cryptosystems based on pairing. In *The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan*, pages 135–148.

Wangham, M. S., Domenech, M. C., e de Mello, E. R. (2013). Infraestruturas de autenticação e de autorização para internet das coisas. In *Minicursos do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais - SBSeg 2013*.

[1] https://gidlab.rnp.br

[2] `https://bit.ly/30mFihK`