Uma Infraestrutura de Autenticação e de Autorização para Internet das Coisas baseada no SAML e XACML

Marlon C. Domenech, Michelle S. Wangham

Programa de Mestrado em Computação Aplicada – Universidade do Vale do Itajaí (UNIVALI) – Itajaí - SC - Brasil

marloncdomenech@gmail.com, wangham@univali.br

Abstract. *The adoption of an Authentication and Authorization Infrastructure (IAA) is an important factor to the effective use of the Internet of Things (IoT). This work aims to provide authentication and authorization of users and smart devices that are in different administrative security domains and that use different communication technology. For this, an IAA based in the federated identity model and that adopts SAML and XACML standards is being developed. For the impacts evaluation of the IAA, an IoT application of remote control and monitoring of industrial machines is being developed.*

Resumo. *A adoção de uma Infraestrutura de Autenticação e de Autorização (IAA) é um fator importante para o efetivo uso da Internet das Coisas (IoT). Esse trabalho visa prover autenticação e autorização de usuários e dispositivos inteligentes que estejam em domínios administrativos de segurança diferentes e usam tecnologias de comunicação distintas. Para isto, uma IAA que segue o modelo de identidades federadas e que adota os padrões SAML e XACML está sendo desenvolvida. Para avaliar os impactos decorrentes do uso da IAA, uma aplicação de IoT de controle e monitoramento de máquinas industriais está sendo desenvolvida.*

1. Introdução

A Internet das Coisas (*Internet of Things* – IoT) consiste na presença de uma diversidade de dispositivos que interagem e cooperam entre si a fim de atingir um objetivo comum, como por exemplo, o compartilhamento de informações, utilizando métodos de endereçamento único e protocolos de comunicação padronizados [Atzori et al. 2010].

Alguns fatores dificultam o efetivo uso da Internet das Coisas, como a heterogeneidade dos dispositivos, as restrições de conectividade e, principalmente, a segurança. Alguns dispositivos não suportam diretamente a conectividade com a Internet através do protocolo IP. Desta forma, torna-se necessária a utilização de um dispositivo intermediário entre os serviços finais da Internet e o dispositivo, chamado de *Smart Gateway* [Mahalle et al. 2010].

Um conceito importante para o desenvolvimento de aplicações para IoT é o de Web das Coisas (*Web of Things* – WoT). A principal característica na WoT é a adoção de protocolos usados amplamente em aplicações web, como por exemplo, o HTTP, cujo principal ganho está na facilidade de integração entre os serviços da WoT e outros serviços e sistemas disponíveis na Internet. Na WoT, a integração dos dispositivos ocorre no nível de aplicação, acima da conectividade de rede. Neste contexto, uma metodologia para a

criação de aplicações em linguagem comum para os dispositivos é o REST (*Representational State Transfer*) [Guinard e Trifa 2009].

A IoT apresenta requisitos singulares que demandam abordagens diferenciadas acerca da segurança. Segundo [Babar et al. 2011], acrescentar mecanismos de segurança em dispositivos embarcados com restrições computacionais pode ser um desafio. Diante da heterogeneidade dos dispositivos, desenvolver mecanismos de segurança que possam ser executados em diferentes plataformas é também um requisito importante para IoT.

Dentre o conjunto de requisitos de segurança para IoT cabe destacar a gestão de identidades (IdM) de usuários e de dispositivos e mecanismos de autorização para garantir acesso somente a dispositivos autorizados [Babar et al. 2011]. Pode-se atender a estes requisitos de segurança por meio de uma infraestrutura de autenticação e de autorização (IAA). Com esta infraestrutura, é possível implantar a IdM de forma a impedir que usuários ou dispositivos não autorizados tenham acesso aos recursos, impedir que usuários ou dispositivos legítimos acessem recursos para os quais não estejam autorizados e permitir que usuários ou dispositivos legítimos não tenham acesso negado aos recursos a estes autorizados [Liu et al. 2012].

A IdM pode ser entendida como o conjunto de processos e tecnologias usados para garantir a identidade de uma entidade ou de um objeto, garantir a qualidade das informações de uma identidade (identificadores, credenciais e atributos) e para prover procedimentos de autenticação, autorização, contabilização e auditoria [ITU-T 2009].

No contexto de IdM, destaca-se o conjunto de especificações SAML (*Security Assertion Markup Language*), que é um padrão baseado em XML (*eXtensible Markup Language*) para a descrição e troca de asserções de segurança entre parceiros de negócio na Internet. O SAML permite, dentre outras coisas, a autenticação *Single Sign On* (SSO) entre múltiplos domínios administrativos, provendo suporte a diversos mecanismos para gestão de identidades federadas, sendo uma das principais tecnologias para abordar o problema [OASIS 2008]. No que tange a autorização, um padrão reconhecido é o XACML (*eXtensible Access Control Markup Language*), o qual é uma linguagem também baseada em XML para a descrição de políticas de autorização e para requisição/resposta de decisões de controle de acesso [OASIS 2003].

Este trabalho tem como objetivo prover autenticação e autorização de usuários e de dispositivos em domínios de segurança diferentes, que utilizam tecnologias de comunicação e de autenticação diferentes, por meio do desenvolvimento de uma infraestrutura de autenticação e de autorização (IAA), alinhada aos requisitos singulares da IoT, que faz uso dos padrões SAML e XACML.

2. Infraestrutura de Autenticação e de Autorização Proposta

A IAA proposta segue o modelo de gestão de identidades federadas, sendo que será usado para a troca de dados de autenticação de usuários e de dispositivos o padrão SAML. Cada domínio administrativo da Federação possui uma IAA que pode ser utilizada para prover a autenticação e contribuir com o controle de acesso de serviços/recursos disponíveis nos dispositivos da WoT. A IAA adota o padrão XACML para expressar políticas de controle de acesso e como protocolo para troca de dados de autorização, visando o suporte a mecanismos de autorização flexíveis. O modelo de controle de políticas escolhido foi o de *outsourcing* [IETF 2001]. Neste modelo, toda solicitação de acesso recebida pelo guardião do serviço, chamado PEP (*Policy Enforcement Point*), é encaminhada ao PDP (*Policy*

Decision Point), responsável por tomar a decisão de autorização tendo como base a asserção SAML resultante do processo de autenticação e a política de controle de acesso do dispositivo. O PEP é responsável por receber e honrar a decisão retornada pelo PDP, liberando ou bloqueando o acesso ao serviço protegido.

A IAA proposta será disponibilizada como um serviço (*web service RESTful*). Em cada domínio, serão usados princípios REST para disponibilizar os recursos fornecidos pelos dispositivos, sem a exigência de uso de um navegador web, em especial, para a interação entre dispositivos (*machine to machine* – M2M).

A Figura 1 apresenta a visão geral do uso da infraestrutura de autenticação e autorização na WoT. A IAA é composta de duas partes: uma disponibilizada como um serviço (contempla o IdP e o PDP de um dado domínio) e outra que deve ser embarcada em cada dispositivo ou *smart gateway* para que estes possam fazer uso das funcionalidades de autenticação e de autorização da IAA ou para prover a implementação do PEP (monitor de referência).

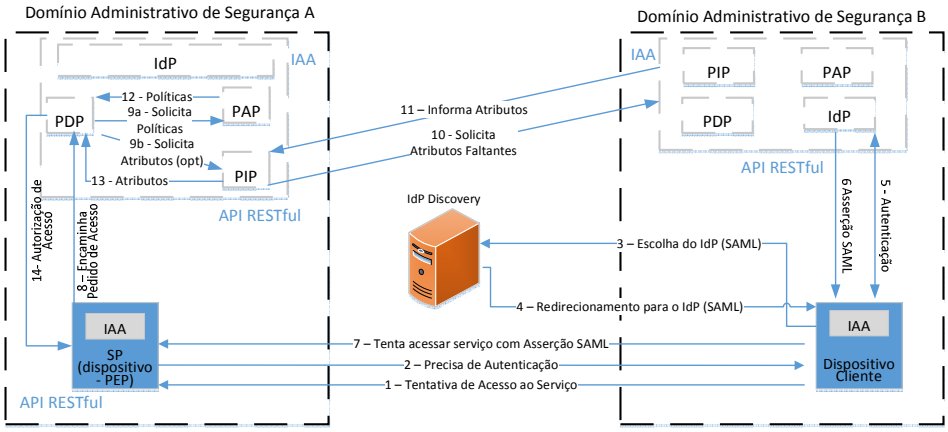

Figura 1. Arquitetura para Autenticação e Autorização Proposta

No passo 1, um dispositivo (cliente ativo) tenta acessar um serviço ou recurso de outro dispositivo no provedor de serviços (SP) A. Por ser um serviço/recurso protegido, o SP A informa, por meio de uma política de segurança (conforme o padrão *WS-SecurityPolicy*), que a autenticação e autorização são necessárias (passo 2). O cliente ativo de um dispositivo, por meio da IAA, acessa via protocolo SAML um serviço de descoberta de IdP, para auxiliar a identificação do IdP do domínio do SP (passo 3). O serviço de descoberta redireciona o cliente ativo ao IdP, para que o dispositivo se autentique através do método de sua escolha (passo 5). Em seguida, o IdP gera uma asserção SAML para o cliente (passo 6), a qual é utilizada no passo 7 para acesso ao serviço/recurso no SP A. Ao receber a asserção SAML, o SP a encaminha para a IAA, para o *Policy Decision Point* (PDP), o qual irá tomar a decisão de autorização em nome do dispositivo. O PDP, no passo 9, solicita as políticas de autorização para o *Policy Admin Point* (PAP) e, caso necessário, mais atributos do usuário para o *Policy Information Point* (PIP), que recupera essas informações nos passos 10 e 11. As políticas e os atributos adicionais são retornados nos passos 12 e 13, para que o PDP tome sua decisão de acesso. Essa decisão é encaminhada para o *Policy Enforcement Point* (PEP) do SP para que este a aplique.

Na federação, as relações de confiança entre as IAAs de cada domínio e as IAAs embarcadas nos dispositivos precisam ser estabelecidas. A comunicação entre estas faz uso do protocolo HTTPS para prover um canal seguro.

3. Considerações Finais

No contexto deste trabalho, está sendo desenvolvida uma aplicação para IoT que irá prover controle e monitoramento remoto de máquinas industriais que fará uso da IAA proposta. A implementação dos padrões SAML e XACML em dispositivos com as limitações de recursos características do cenário de IoT, assim como a implementação dos mecanismos que garantem a autenticidade e integridade das mensagens, poderão levar a custos computacionais que limitem o uso da IAA. Esses custos serão avaliados durante o uso desta por uma aplicação de IoT, em termos de desempenho da rede e uso de recursos computacionais dos dispositivos, permitindo que conclusões sejam obtidas sobre os impactos do uso de uma IAA que utilize esses padrões no cenário da IoT.

Como resultado, espera-se conceber uma IAA para WoT que seja capaz de prover a autenticação SSO de usuários e dispositivos, a gestão de identidades federadas e mecanismos de autorização flexíveis.

4. Agradecimentos

Os autores agradecem o apoio financeiro da CAPES.

Referências

Atzori, L., Iera, A. e Morabito, G. (2010), “The Internet of Things: A survey”, In: *Computer Networks*, n. 54, pages 2787-2805.

Babar, S., Stango, A., Prasad, N., Sen, J. e Prasad, R. (2011). Proposed embedded security framework for internet of things (iot). In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*, pages 1–5.

Guinard, D. e Trifa, V. (2009), “Towards the Web of Things: Web Mashups for Embedded Devices”, In: *International World Wide Web conferences, Proceedings of Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web*, pages 196-199, IEEE Press.

IETF. (2001), “Policy Core Information Model”. www.ietf.org/rfc/rfc3060.txt, Set 2013.

ITU-T (2009), “NGN identity management framework. Recommendation Y.2720”, http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2720-200901-I!!PDF-E&type=items, Maio 2013.

Liu, J., Xiao, Y., e Chen, C. P. (2012), “Authentication And Access Control in the Internet of Things”, In: *32nd International Conference, Distributed Computing Systems Workshops*, pages 588-592, IEEE Computer Society.

Mahalle, P., Babar, S., Prasad, N. R., & Prasad, R. (2010), “Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges”, In: Recent Trends in Network Security and Applications, v. 89, pages 430 – 439.

OASIS (2003), “A Brief Introduction to XACML”, https://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html, 2013.

OASIS (2008), “Security Assertion Markup Language (SAML) V2.0 Technical Overview”, https://www.oasis-open.org/committees/download.php/27819/sstc-saml-tech-overview-2.0-cd-02.pdf, Junho 2013.

