Análise de segurança da autenticação baseada em OpenID Connect com IdP externos para OpenStack

Glauber Cassiano Batista[1], **Charles Christian Miers**[1]

[1] Departamento de Ciência da Computação - CCT
Universidade do Estado de Santa Catarina - UDESC
Joinville, SC – Brasil

{glauber,charles}@colmeia.udesc.br

Resumo. *Diversos serviços na Internet requerem diferentes pares de usuário e senha para autenticar seus usuários. O processo de gerenciamento de senhas é custoso e suscetível a problemas de segurança, e as soluções de nuvens computacionais já enfrentam problemas relacionados. Nesse sentido, o objetivo deste artigo é analisar aspectos de segurança na utilização do OpenID Connect, um mecanismo de autenticação única, em nuvens computacionais baseadas no OpenStack.*

1. Introdução

Uma nuvem computacional é um modelo que permite acesso ubíquo, conveniente e sob demanda a um conjunto de recursos configuráveis que podem ser rapidamente provisionados e liberados com o mínimo de esforço [Mell and Grance 2011]. O OpenStack[1] é uma solução aberta, de grande destaque, para nuvens computacionais do tipo *Infrastructure-as-a-Service* (IaaS) e tem apoio de grandes organizações [Bonner et al. 2013].

Assim como grande parte dos serviços na Internet, as nuvens computacionais se deparam com problemas de gerenciamento de identidades e algumas já empregam mecanismos *Single Sign-On* (SSO) para autenticar seus usuários [Chadwick et al. 2013, Sette and Ferraz 2014]. A principal característica de um mecanismo SSO é prover um identificador único ao usuário para que este possa se autenticar em qualquer serviço que o suporte. O uso de tecnologias de autenticação/autorização centradas no usuário (*e.g.,* OpenID e OAuth) proporcionam uma possibilidade mais dinâmica e acessível para a autenticação única, especialmente quando utilizadas com um Provedor de Identidades (IdP) externo. Este trabalho tem como objetivo analisar a segurança do uso de tecnologias de autenticação e autorização centradas no usuário (*i.e.,* OpenID Connect) para disponibilização em serviços de nuvens baseadas no OpenStack.

2. OpenStack

O OpenStack é uma solução de nuvem que controla diversos conjuntos de recursos de processamento, armazenamento e rede de um *data center* [Khan et al. 2011]. O OpenStack é composto pelos serviços principais (*Core Services*) Neutron, Horizon, Nova, Cinder, Glance, Swift e Keystone, responsáveis pela rede, painel de instrumentos, computação, armazenamento de blocos, imagens, armazenamento de objetos e gerenciamento de identidades, respectivamente. Há também os serviços opcionais (*Optional Services*) que são instalados segundo a demanda de cada provedor de nuvem.

[1] http://www.openstack.org

O serviço de identidade do OpenStack, Keystone, é responsável pelo gerenciamento e autenticação dos usuários. Além da autenticação, o Keystone faz uma autorização de alto nível, transformando os atributos de autenticação em papéis, *Role-Based Access Control* (RBAC). Porém, a autorização ocorre de forma descentralizada em cada módulo do OpenStack, com base nos papéis e projetos do usuário [Sette and Ferraz 2014]. O Keystone possui a extensão OS-FEDERATION que gerencia a autenticação única através do uso de *plugins* do Apache. Dessa forma, é possível utilizar o *plugin* `mod_auth_openidc` para autenticar os usuários através de um IdP com o OpenID Connect. Os usuários autenticados com o OpenID Connect são mapeados para seus respectivos projetos com base nos atributos recebidos do IdP [Martinelli et al. 2015]. Um mapeamento especifica quais usuários podem acessar o serviço e em qual grupo e projeto estes devem ser alocados.

3. OpenID Connect

O OpenID Connect opera com o protocolo de autorização OAuth 2.0[2] e fluxo de mensagens diretas REST/JSON, utilizando também *Secure Sockets Layer* (SSL) para a cifragem e aspectos de comunicação segura [Lynch 2011]. O OpenID Connect permite que os desenvolvedores autentiquem os seus usuários em múltiplas aplicações sem ter que gerenciar suas senhas, fazendo uso apenas de requisições e respostas HTTP/HTTPS.

A autenticação com o OpenID Connect segue o seguinte fluxo: *(1)* O usuário acessa a aplicação desejada, denominada Provedor de Serviço (SP), através do *User-Agent* (UA), e escolhe/informa um IdP no qual possua uma conta. O IdP, neste momento, executa o processo de descoberta. *(2)* Em seguida, o SP, através de uma requisição redirecionada, envia o usuário ao IdP. *(3)* Neste momento o usuário utiliza suas credenciais (*e.g.,* par de usuário e senha) para se autenticar no IdP. *(4)* Uma vez autenticado, o IdP redireciona o usuário para o SP, que concederá o acesso aos recursos desejados.

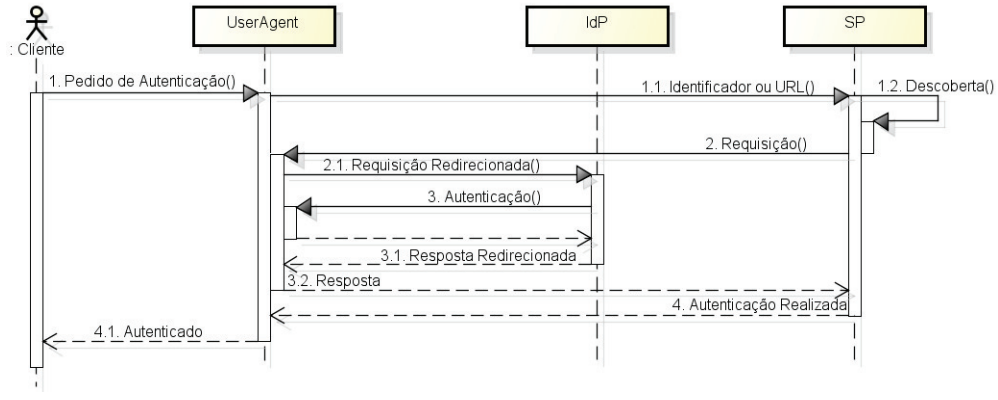

Figura 1. Autenticação SSO com o OpenID Connect.

4. Trabalhos Relacionados

Nos últimos anos os mecanismos SSO tem sido muito debatidos e diversas soluções surgiram. Dessa forma, trabalhos sobre a segurança e implementação são comumente encontrados na literatura [Delft and Oostdijk 2010, Yang and Manoharan 2013, Li and Mitchell 2015]. Delft and Oostdijk 2010 realizaram uma análise de segurança do protocolo

[2] `http://oauth.net/2/`

OpenID 2.0. Foram identificados problemas de registro das atividades do usuário no IdP, ataques *Cross-Site Scripting* (XSS) e *Man-in-the-Middle* e reciclagem de identificadores OpenID. Yang and Manoharan 2013 realizaram uma análise de segurança do protocolo OAuth 2. Foi constatado que os canais de comunicação não eram devidamente protegidos com SSL/TLS e que os códigos de segurança eram reutilizados. Por fim, Li and Mitchell 2015 analisaram a segurança da implementação do OpenID Connect do Google. Foi constatado que grande parte das vulnerabilidades são oriundas da não entendimento dos desenvolvedores. Também foram identificados ataques *Cross-Site Request Forgery* (CSRF).

Ainda que as análises citadas ofereçam informações importantes a serem consideradas na escolha de um sistema SSO, não foram encontradas análises de segurança da utilização do OpenID Connect em nuvens computacionais, principalmente àquelas baseadas em OpenStack.

5. Ambiente de Testes

O ambiente utilizado para os experimentos é formado por três servidores: um nó controlador, um nó de rede e um nó de computação, executando RDO OpenStack Liberty sobre GNU/Linux CentOS 7. Os usuários se autenticam através do protocolo OpenID Connect, com IdP do Google. O Keystone é instalado no nó controlador e todos os serviços se autenticam pela porta TCP/5000. Para habilitar o uso do OpenID Connect no OpenStack é necessário instalar e configurar seu módulo, também são necessárias as credenciais do Google Developers para autenticar o usuário.

Para análise do tráfego, foi utilizada a ferramenta `tcpdump` com escuta na interface externa do controlador. As coletas foram realizadas dez vezes a fim de assegurar que o fluxo de requisições segue um mesmo padrão, tanto quanto a natureza dos dados como das partes envolvidas.

6. Análise de Segurança

Para a análise de segurança, foram levados em conta os seguintes critérios, definidos com base nos trabalhos da Seção 4: Cifragem dos dados; Utilização de um IdP Externo; e Acesso administrativo não autorizado ou a outros projetos no Openstack.

Para o critério Cifragem dos Dados, foi realizada uma escuta entre todos os canais de comunicação: OpenStack (SP) e IdP; SP e UA; e entre UA e IdP. Foi possível observar que o OpenStack já utiliza soluções contra algumas vulnerabilidades, como o CSRF, porém não utiliza TLS para proteger o canal SP – UA. Por não utilizar TLS nesse canal, os dados do usuário podem ser interceptados. Também foi possível observar que não existe tráfego direto entre o SP e o IdP, pois este tráfego é redirecionado pelo UA. Já o canal UA – IdP é protegido com TLS e não apresentou potenciais problemas. Também foi encontrada uma falha no SP, com análise do código, e permite que um atacante use o `id_token` de outro usuário, uma vez que não o valida na autenticação.

A utilização de um IdP externo tem impacto maior na privacidade, uma vez que os IdPs podem rastrear a atividade do usuário, como é o caso do Google. Portanto, é necessário avaliar a política de privacidade e verificar se esta não fere a política interna da organização. O acesso administrativo não autorizado, ou a outros projetos, pode ser resolvido através do mapeamento do usuário, através de outras informações (*e.g.,* e-mail),

além do identificador, no OpenStack. Mesmo que o Google não recicle os identificadores OpenID, é possível que outro IdP o faça, portanto é necessário mapear corretamente os usuários.

7. Considerações e Trabalhos Futuros

A análise realizada através dos critérios estabelecidos reforça as afirmações que as nuvens computacionais, quanto a segurança, herdam os aspectos das tecnologias que empregam e somam-se novos aspectos oriundos da sua integração com outros *softwares*. Neste sentido, percebe-se que a tecnologias como TLS trazem toda uma herança de questões de segurança e atenção quanto a vulnerabilidades. Ainda, o uso de IdPs externos, ao mesmo tempo que terceiriza a segurança de parte do processo de autenticação, também inclui novos aspectos. É de conhecimento dos autores que existem versões mais novas do OpenStack. Contudo, a versão Mitaka apresentou problemas com a API de autenticação única e não permitiu a realização dos testes. A versão Newton será testada futuramente para verificar se as vulnerabilidades encontradas ainda persistem.

Referências

Bonner, S., Pulley, C., Kureshi, I., Holmes, V., Brennan, J., and James, Y. (2013). Using OpenStack to improve student experience in an h.e. environment. In *Science and Information Conference (SAI), 2013*, pages 888–893.

Chadwick, D. W., Siu, K., Lee, C., Fouillat, Y., and Germonville, D. (2013). Adding federated identity management to OpenStack. *Journal of Grid Computing*, 12(1):3–27.

Delft, B. v. and Oostdijk, M. (2010). A Security Analysis of OpenID. In Leeuw, E. d., Fischer-Hübner, S., and Fritsch, L., editors, *Policies and Research in Identity Management*, number 343 in IFIP Advances in Information and Communication Technology, pages 73–84. Springer Berlin Heidelberg. DOI: 10.1007/978-3-642-17303-5_6.

Khan, R., Ylitalo, J., and Ahmed, A. (2011). OpenID authentication as a service in OpenStack. In *2011 7th International Conference on Information Assurance and Security (IAS)*, pages 372–377.

Li, W. and Mitchell, C. J. (2015). Analysing the security of google's implementation of openid connect. *arXiv preprint arXiv:1508.01707*.

Lynch, L. (2011). Inside the Identity Management Game. *IEEE Internet Computing*, 15(5):78–82.

Martinelli, S., Nash, H., and Topol, B. (2015). *Identity, Authentication, and Access Management in OpenStack: Implementing and Deploying Keystone*. O'Reilly Media.

Mell, P. and Grance, T. (2011). The NIST definition of cloud computing.

Sette, I. and Ferraz, C. (2014). Integrating cloud platforms to identity federations. In *2014 Brazilian Symposium on Computer Networks and Distributed Systems (SBRC)*, pages 310–318.

Yang, F. and Manoharan, S. (2013). A security analysis of the OAuth protocol. In *2013 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*, pages 271–276.