Pesquisas Exploratórias no Testbed Eduroam do GidLab*

Allex Magno Andrade[1], Jucélio Jair Silva[2], Edelberto F. Silva[3], Luciano F. da Rocha[4], Michelle Wangham[2]

[1]Instituto Federal de Santa Catarina – IFSC

[2]Universidade do Vale do Itajaí – UNIVALI

[3]Universidade Federal de Juiz de Fora – UFJF/DCC

[4]Rede Nacional de Pesquisas – RNP

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

Abstract. *The challenge to allocate resources and to provide a test environment can cause delays that jeopardize the main focus of an explanatory research, which is experimentation. Testbeds are a solution for this demand and can also offer a controlled environment with realistic elements in order to perform these experiments. RNP (Brazilian National Education and Research Network) has created the Eduroam Tested for Brazilian and Latin-American researchers. This testbed is a complete infrastructure that enables technology studies and developments and is supported by an infrastructure based on the RADIUS and 802.1X protocols that are aligned with the Eduroam. This paper aims to present explanatory research suggestions that can be performed in this testbed.*

Resumo. *A dificuldade de alocar recursos e disponibilizar um ambiente de testes pode ocasionar atrasos que prejudicam o real foco de uma pesquisa exploratória que é a experimentação. Uma solução que visa contornar esta demanda e ainda oferecer um ambiente controlado e próximo das características reais e necessárias é o uso de* testbeds*. A Rede Nacional de Ensino e Pesquisa (RNP) disponibiliza aos pesquisadores brasileiros e latino americanos o* testbed eduroam*, uma infraestrutura completa que viabiliza estudos e desenvolvimento de tecnologias, tendo como base uma infraestrutura baseada no RADIUS e no protocolo 802.1X, alinhada ao eduroam. Este artigo visa apresentar sugestões de pesquisas exploratórias que podem ser conduzidas neste* testbed*.*

1. Introdução

Os serviços de Gestão de Identidades[1] (GId) que a Rede Nacional de Ensino e Pesquisa (RNP) oferece às suas instituições usuárias não permitem, em suas políticas de uso, que pesquisadores os utilizem para realizar experimentos práticos. Desenvolver pesquisas aplicadas na área de GId exige que os experimentos sejam conduzidos em um ambiente distribuído. A complexidade para montar tal ambiente depende das soluções tecnológicas escolhidas e de uma infraestrutura confiável. Configurar este ambiente pode ser uma tarefa mais árdua e demorada que a própria pesquisa [Wangham et al. 2013].

*Projeto financiado pela Rede Nacional de Ensino e Pesquisa (RNP)

[1]A Infraestrutura de Chaves Públicas para ensino e pesquisa (*ICPedu*), a Comunidade Acadêmica Federada (*CAFe*) e o serviço de autenticação em redes sem fio (*eduroam*).

O serviço para experimentação em Gestão de Identidade (GIdLab) [Wangham et al. 2013], mantido pela RNP desde 2013, disponibiliza aos pesquisadores um ambiente virtual distribuído (*testbed*) para que estes possam conduzir experimentos com diferentes Infraestruturas de Autenticação e de Autorização (IAA) e com Infraestruturas de Chaves Públicas (ICPs).

Em Novembro de 2017, foi apresentado o ***testbed eduroam*** [Silva et al. 2017], que descreve a primeira iniciativa mundial de oferta de uma infraestrutura de autenticação e de autorização para experimentação baseada no RADIUS (*Remote Authentication Dial-In User Service*)[2], no protocolo IEEE 802.1X[3] e no serviço *eduroam* (*education roaming*)[4]. A partir de maio de 2018, este ambiente foi integrado ao GIdLab, permitindo assim que pesquisadores e profissionais interessados nestas redes sem fio executem seus experimentos com o apoio de assistentes técnicos e com outras facilidades oferecidas aos usuários do GIdLab. Este artigo tem por objetivo sugerir pesquisas exploratórias no *testbed eduroam*.

2. Serviço para Experimentação GIdLab

A motivação para criação de um *testbed* é o emprego de tecnologias para obter resultados próximos ao que se consegue em um ambiente real e o melhor aproveitamento da infraestrutura usada. De acordo com [Anderson et al. 2005], o fácil acesso a *testbeds* virtuais pode promover um renascimento da pesquisa aplicada (*live experimentation*) que pode se estender além das pesquisas baseadas em simuladores e emuladores. Um *testbed* deve ajudar o pesquisador a entender o que funciona e o que não funciona em um experimento, para que seja possível corrigir o que está sendo experimentado e com isso desenvolver soluções mais rapidamente. Por não prejudicar sistemas e usuários em produção, testes podem ser revisados, interrompidos e reexecutados sempre que necessário.

A RNP visa, através dos seus serviços para experimentação (*testbeds*[5]), promover pesquisas experimentais e o desenvolvimento de novas tecnologias e serviços. O GIdLab[6] é um *testbed* configurável que possui uma infraestrutura composta por servidores e serviços de gestão de identidades distribuídos nos Pontos de Presença (PoPs) da RNP.

Dentre os serviços oferecidos pelo GidLab, destacam-se: (1) uma federação *Shibboleth* (CAFe Expresso); (2) uma federação[7] que faz uso do *framework SimpleSAMLphp*; (3) um ambiente *OpenID Connect*, que faz uso do *MITREId Connect*; e (4) o *testbed eduroam*. O GIdLab oferece ainda aos pesquisadores roteiros de degustação e webinares para uso dos serviços oferecidos no GIdLab, um serviço de monitoramento dos servidores do ambiente, *docker containers* preparados para facilitar a instalação e configuração e, por fim, atendimento via *service desk* da RNP e com os assistentes técnicos do *testbed*.

2.1. Testbed Eduroam

O eduroam é o serviço de acesso sem fio (*roaming*) seguro, desenvolvido para a comunidade internacional de educação e pesquisa. O serviço oferece benefícios para indivíduos, instituições e redes nacionais de ensino e pesquisa (*National Research Network - NRENs*).

[2]https://tools.ietf.org/html/rfc2865

[3]https://tools.ietf.org/html/rfc3580

[4]https://www.eduroam.org

[5]Outros *testbeds* financiados em projetos da RNP são: FIBRE, FIWARE-Lab, LOFT e CloudLAB.

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

[7]Adequada para experimentos que envolvam autenticação de dispositivos da Internet das Coisas (IoT).

Para estudantes, pesquisadores e funcionários das instituições, este oferece conectividade à Internet, através de conexão sem fio (Wi-Fi), no Campus e ao visitar instituições parceiras, simplesmente ao abrir seus dispositivos (*laptops*, *smartphones*, *tablets*, etc). Para as instituições, elimina-se a necessidade de fornecer nomes de usuários e senhas temporárias ou compartilhadas de maneira insegura. O acesso pode ser controlado com muito mais facilidade e a carga de trabalho para registro e revogação de identidades é removida. Por meio do *eduroam*, as NRENs oferecem um serviço altamente visível e altamente valorizado que auxilia diretamente suas instituições clientes e seus usuários[8].

O serviço *eduroam* utiliza hierarquia de servidores RADIUS e pontos de acesso sem fio IEEE802.11, que estão distribuídos pelas instituições de ensino participantes. Quando o usuário requisita o acesso, a autenticação é tratada em sua instituição de origem. Para que o acesso ocorra de maneira segura, padrões IEEE802.1X e IEEE802.11i são utilizados. Desta forma, este serviço facilita a movimentação de seus usuários em qualquer lugar onde o serviço está presente no mundo. Em setembro de 2018, no Brasil, há 2.365 pontos de acessos, sendo 122 provedores de identidades, que oferecem este serviço e mais de 24.000 pontos espalhados pelo mundo [9].

O *Remote Authentication Dial In User - RADIUS*, padrão IETF, oferece serviço AAA e é conhecido no mercado como uma solução robusta. Este serviço, em conjunto com a infraestrutura IEEE 802.11i, oferece um dos métodos mais seguros para controlar o acesso às redes sem fio [Saade et al. 2013].

A infraestrutura do *testbed eduroam* está distribuída não apenas nos PoPs da RNP, mas também no México e no Peru para disponibilizar o acesso a nível de confederação. A configuração do *testbed eduroam* possui três níveis de servidores RADIUS: local, nacional (federação) e *top-level* da confederação. No nível local, tem-se 2 servidores no Brasil, 1 no Peru e 1 no México. No nível da federação, tem-se 3 servidores *proxy*, representando exatamente os 3 países. No nível da confederação, 2 servidores *top-level* representam a ligação entre os países, sendo 1 no Brasil e outro no Peru. Cada servidor RADIUS local está conectado diretamente a seu servidor federado, utilizando um canal de comunicação TCP/TLS (utilizando o RadSec). Já os servidores do nível da federação se conectam aos dois servidores confederados por meio de UDP RADIUS[10] [Silva et al. 2017].

3. Sugestões de Pesquisas Exploratórias

O *testbed eduroam* oferece benefícios para pesquisadores conduzirem experimentos de larga escala tanto para desenvolverem novas soluções que visam aprimorar o serviço *eduroam* como soluções que o utilizam. A seguir, um conjunto de sugestões de pesquisas indicam o quão abrangente o ambiente pode ser:

- Uso do *eduroam* para prover uma infraestrutura de AAA[11] para *Software-Defined Networking*. Estas novas infraestruturas podem oferecer diferentes métodos de autenticação e soluções de controle de acesso tendo como base os atributos dos usuários de uma federação, atributos de geolocalização e do próprio dispositivo usado pelo usuário.

[8] https://www.eduroam.org

[9] Estes dados foram extraídos em https://monitor.eduroam.org/

[10] Os softwares e versões utilizados são: FreeRadius 3.0.15 e radsecproxy 1.6.9.

[11] *Authentication, authorization, and accounting*.

- Com o aumento do número de dispositivos IoT (*smart devices*) conectados nas redes dos Campus Inteligentes, o aprimoramento do *eduroam* para prover uma AAA alinhada aos requisitos destes dispositivos é um desafio.
- Diante dos crescentes e complexos ataques cibernéticos, investigações para aprimorar a segurança do *eduroam* são necessários, em especial, para garantir a disponibilidade do serviço e a privacidade de seus usuários.
- Pesquisas experimentais de avaliação de desempenho, de escalabilidade e de usabilidade para aprimorar a qualidade do serviço (QoS) e de experiência do usuário (QoE).
- Transposição de autenticação entre *eduroam* e federação SAML. Após uma autenticação bem sucedida no *eduroam*, a autenticação na Federação pode ser implícita.
- Exploração múltiplas formas de autenticação (MFA) de usuários para aprimorar a robustez do processo de autenticação sem comprometer a usabilidade. Fluxos de autenticação que se adaptam à rede acessada e ao dispositivo usado. Uso de certificados digitais[12], fatores biométricos e outros fatores de autenticação adequados a dispositivos de IoT com restrição.
- Avaliação qualitativa e quantitativa de outras soluções que implementam o padrão RADIUS e que suportam *Network Function Virtualization*.

4. Conclusão

O desenvolvimento de pesquisas exploratórias possui um caminho árduo e a falta de recursos tecnológicos, muitas vezes, pode dificultar ou inviabilizar este caminho. Iniciativas de criação de *testbeds* são as soluções mais adequadas para quem necessita de tempo e infraestrutura de larga escala. Este artigo apresentou algumas sugestões de pesquisas exploratórias que podem ser conduzidas no *testbed eduroam* em conjunto com outros serviços oferecidos pelo GIdLab, como a federação CAFe Expresso. Por fim, vale destacar que o *testbed eduroam* estendeu o serviço GIdLab para **toda a comunidade latino americana**.

Referências

Anderson, T., Peterson, L., Shenker, S., and Turner, J. (2005). Overcoming the internet impasse through virtualization. *Computer*, 38(4):34–41.

Saade, D. C. M., Carrano, R. C., and Silva, E. F. (2013). *Acesso sem fio seguro para Comunidade Acadêmica Federadas*. Escola Superior de redes.

Silva, E. F., da Rocha, L. F., Ancieta, J. R. Q., Forigato, A., Almeida, A., and Welley, J. (2017). Eduroam testbed: Um ambiente real para experimentação em aaa. In *Anais do XVII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg2013) - Workshop de Gestão de Identidade (WGID)*, pages 632–635. Sociedade Brasileira de Computação.

Wangham, M. S., Mello, E. R., Souza, M. C., and Coelho, H. (2013). Gidlab: Laboratório de experimentação em gestão de identidade. In *Anais do XIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg2013) Workshop de Gestão de Identidade (WGID)*, pages 481–486. Sociedade Brasileira de Computação.

[12]Por exemplo, o uso de certificado P1 da ICPedu.