Provendo uma Rede Sem Fio de Grande Escala para Visitantes com Auditoria e com Identidade Verificável

Diogo Menezes Ferrazani Mattos[1] **e Luiz Claudio Schara Magalhães**[1]

[1]Laboratório MídiaCom – Universidade Federal Fluminense
Niterói - RJ - Brasil

Resumo. *A rede sem fio institucional da Universidade Federal Fluminense (UFF) é federada à rede educacional internacional Eduroam. No entanto, diariamente, por volta de 200 usuários não cadastrados visitam a rede. Atender a esses usuários e prover auditoria sobre o uso da rede é um desafio. Esta palestra apresenta a proposta de gestão da identidade de visitantes na rede sem fio da UFF. A ideia central é vincular a identidade de cada usuário a um número de telefone celular verificável e registrado perante a operadora.*

1. Introdução

O Eduroam[1] (*education roaming*) é um serviço de rede sem fio federado, desenvolvido pela comunidade acadêmica internacional. O objetivo do Eduroam é prover acesso à Internet a membros de instituições participantes quando estão em deslocamento em outras instituições. Embora a autenticação federada esteja presente em aproximadamente 120 países[2], no Brasil ainda há diversas instituições que não estão federadas. Nesse sentido, um desafio para a gestão de identidades em redes federadas ao Eduroam é o provimento de identificação temporária, local, verificável e auditável para usuários que não tenham credenciais na rede Eduroam, mas estejam visitando instituições federadas.

Esta palestra apresenta a proposta de rede para visitantes implantada na rede sem fio institucional da Universidade Federal Fluminense (UFF) [Mattos et al., 2019, Magalhães e Mattos, 2018]. A ideia central é criar um provedor de identidade específico para visitantes que vincula a credencial de acesso de um visitante a um telefone celular válido e registrado. Ao vincular ao telefone celular, gera-se uma cadeia de confiança na operadora de telefonia, pois assume-se que o número de celular está registrado sob uma identificação real verificada.

2. A Rede Sem Fio da Universidade Federal Fluminense

Os pontos de acesso na rede sem fio da UFF são equipamentos de baixo custo e empregam uma versão personalizada de *firmware*, desenvolvida na própria UFF, com apoio do programa de grupos de trabalho da RNP (Rede Nacional de Ensino e Pesquisa) - o GT SCIFI (Sistema de Controle Inteligente para redes sem fio). A rede implementa ainda um controlador de *software* próprio que realiza o controle de potência e de canais nos pontos de acesso para reduzir a interferência na malha densa de pontos de acesso. A estrutura da rede atual é composta de seis redes sobrecamada (*overlay*) sobre a rede

Este trabalho foi realizado com recursos da CNPq, CAPES, RNP e FAPERJ.

[1]É um serviço de acesso a redes sem fio com conexão à Internet, desenvolvido para a comunidade internacional de educação e pesquisa, que se vale da federação de identidade para prover uma forma simples, rápida e segura de acesso à Internet. A autenticação dos usuários ocorre na instituição de origem.

[2]Disponível em https://www.eduroam.org/where/?location=br.

cabeada da UFF. A rede sem fio usa sete VLANs, três que abrangem todo o *campus*. Quatro VLANs cobrem grandes áreas da UFF. A UFF é distribuída em mais de 90 prédios em Niterói, em mais de 16 *campi* distintos. Cada VLAN tem seu próprio servidor DNS e realiza o seu próprio NAT para o acesso à Internet. Nas três VLANs que cobrem todos os *campi* trafegam os dados de controle, da rede cadastro e da rede de visitantes. A rede de controle serve para a comunicação entre os pontos de acesso (APs) e o controlador.As VLANs de cadastro e visitantes compõem a proposta de rede para visitantes.

3. A Proposta de Rede para Visitantes

A rede de cadastro é uma rede *sand-boxed*, que não dá acesso à Internet, mas permite aos usuários acessar os manuais de como usar a rede Eduroam, o aplicativo de configuração automática, para Android, e para os que não possuem credenciais na UFF, ou federada na rede Eduroam, é apresentada uma página de cadastro. Esta, ao ser preenchida, gera uma conta na rede visitantes. A rede cadastro é aberta. O usuário que se cadastra deve informar o número de um documento de identificação e um número de telefone celular válido. Ao final do cadastro, uma senha aleatória é gerada e enviada ao número de celular através de uma mensagem de texto curta (SMS)[3]. O documento informado e a senha são as credenciais de acesso à rede visitante, com proteção WPA2 Enterprise. As credenciais de acesso são armazenadas em um banco de dados *MySQL*. O banco de dados segue um esquema semelhante ao padrão do provido pelo *Freeradius*[4] para autenticação. Contudo, o padrão foi alterado para comportar a informação do número de celular associado a cada usuário cadastrado. A autenticação na rede visitante é confiada a um servidor RADIUS dedicado que realiza *proxy* para autenticação de usuários federados Eduroam. o RADIUS dedicado à rede visitante realizada a auditoria na base de dados MySQL, permitindo a realização de consultas SQL para identificar usuários conectados em um dado instante e a auditoria de uso da rede. Cada usuário é desabilitado após trinta dias do cadastro. Contudo, os dados não são apagados do banco de dados, pois é necessário manter o dado caso haja uma auditoria futura. Como a rede visitante tem uma VLAN diferente das demais, o seu tráfego é isolado do restante do tráfego wi-fi da UFF. O monitoramento da rede é realizado pelo SNMP (*Simple Network Management Protocol*). O tráfego na rede é monitorado usando o *NetFlow*que realiza a coleta e a agregação de informações sobre o tráfego de rede que entra ou sai dos *gateways* da VLAN visitante.

4. Conclusão

Essa palestra apresentou as principais decisões de projeto para o desenvolvimento de uma abordagem local, de baixo custo, auditável e com identidade verificável de usuários em uma rede de visitantes federada à rede educacional internacional Eduroam. A proposta mantém os visitantes como usuários locais e garante que usuários Eduroam acessem também a rede visitante.

Referências

Magalhães, L. C. S. e Mattos, D. M. F. (2018). Caracterização do uso de uma rede sem fio de grande porte distribuída por uma ampla Área. *XVII Workshop em Desempenho de Sistemas Computacionais e de Comunicação (WPerformance - CSBC 2018)*, 17(1/2018).

Mattos, D. M. F., Medeiros, D. S. V., Fernandes, N. C. e Magalhaes, L. C. S. (2019). Uma abordagem não supervisionada para inferir qualidade de experiência em redes sem fio de grande escala. Em *Anais XXIV Workshop de Gerência e Operação de Redes e Serviços - WGRS'2019 (SBRC'2019)*, Gramado, RS.

[3]Caso o celular informado for inválido, o usuário não recebe a senha gerada, logo, não acessa a rede.

[4]Disponível em https://freeradius.org/.