Módulo de Autenticação via Eduroam para o Pluggable Authentication Modules

Marcos Laerte G. de Lima[1], **Pedro Henrique Lara Campos**[1], **Paulo Matias**[1]

[1]Departamento de Computação
Universidade Federal de São Carlos (UFSCar)
São Carlos, SP – Brasil

{marcoslaerte, pedrohlc, matias}@ufscar.br

Abstract. *Universities and research institutions often want to offer services to external collaborators and visitors. Federations are one of the most traditional ways of achieving that aim. Eduroam is a federated network which facilitates roaming internet access amongst participant institutions. However, internet access usually occurs through a personal device owned by the user and, until now, there was no simple method for setting up a public terminal or classroom computer to use Eduroam credentials as login information. This work presents a novel, yet production-proven, solution for accepting Eduroam credentials in systems compatible with Pluggable Authentication Modules (PAM).*

Resumo. *Universidades e instituições de pesquisa frequentemente desejam oferecer serviços para colaboradores externos e visitantes. Federações são uma das formas mais consagradas de atingir esse objetivo. Eduroam é uma rede federada que facilita a itinerância no acesso à internet entre instituições participantes. No entanto, o acesso geralmente se dá por meio de dispositivo pessoal do usuário sendo que, até então, não existia método simples para configurar um terminal público ou computador de sala de aula para ser acessado com as credenciais da própria rede Eduroam. Este trabalho apresenta uma solução inovadora e comprovada em produção para aceitar as credenciais do Eduroam em sistemas compatíveis com o Pluggable Authentication Modules (PAM).*

1. Motivação

Universidades e instituições de pesquisa costumam receber alunos, pesquisadores e professores de vários lugares por uma série de motivos, tais como participar de palestras, eventos e cursos. Federações possibilitam aos usuários utilizar serviços de outras instituições identificando-se com as credenciais de sua instituição de origem, desde que ambas tenham aderido à federação. Em particular, a rede federada Eduroam permite que o usuário mantenha-se conectado à internet quando estiver visitando qualquer instituição associada, sem precisar alterar configurações de seu computador ou dispositivo móvel.

No entanto, quando o usuário deseja acessar a rede Eduroam a partir de um equipamento público pertencente à instituição visitada em vez de utilizar um dispositivo pessoal, surgem problemas que não são tratados pelas ferramentas atualmente disponíveis. Em primeiro lugar, para oferecer uma área pessoal (*home*) separada para cada usuário, é necessário que o usuário efetue *login* no sistema operacional antes de conectar-se a rede, exigindo uma infraestrutura separada para a validação desse *login*. A preocupação de

oferecer uma área separada é importante pois, se fosse disponibilizada uma área comum a todos os usuários, seria trivial para um adversário prejudicar a privacidade de outros usuários. Além disso, se a tarefa de configurar a conexão à rede fosse delegada ao próprio usuário, vazamentos de credenciais poderiam ocorrer devido à dificuldade de se configurar corretamente uma conexão com autenticação 802.1X [Reynolds 2010].

O problema de configurar automaticamente uma conexão já foi tratado por uma ferramenta anteriormente publicada [Bello 2014], no entanto essa ferramenta é incapaz de funcionar de forma federada, além de não isolar a área pessoal de cada usuário nem verificar se a autenticação ocorreu com sucesso.

A ferramenta apresentada neste trabalho proporciona uma solução mais completa, acoplando a autenticação de usuários do sistema operacional à autenticação na rede 802.1X. Desta forma, credenciais corretas de acesso à rede são tratadas como credenciais válidas para acesso ao sistema operacional. Além de colaborar para a privacidade dos usuários, esse modelo permite que a instituição condicione o acesso a outros serviços, tais como o acesso a programas instalados na máquina, a usuários de instituições federadas.

2. Principais funcionalidades

A ferramenta apresentada integra-se à infraestrutura de gerenciamento de usuários e de redes adotada pela maioria dos sistemas operacionais para estações de trabalho (*desktops*) baseados em Linux. A solução foi testada com as versões 16.04 e 18.04 da distribuição Ubuntu, ambas de longo prazo de suporte (LTS).

Cada usuário recebe seu próprio identificador de usuário (*uid*) e sua própria área pessoal (*home*) no sistema, proporcionando isolamento entre os diversos usuários. Além disso, a conexão com a rede é configurada seguindo as especificações de autenticação de cada instituição federada e com os certificados raiz de ICP (Infraestrutura de Chaves Públicas) adequados.

3. Arquitetura da solução

Para realizar a autenticação do usuário no sistema operacional, dando acesso aos outros programas e à rede, foi necessário interagir com três componentes do sistema: o PAM, que gerencia a autenticação de usuários, o D-BUS, um barramento de mensagens que media a comunicação entre aplicativos e, por fim, o NetworkManager, responsável pelo gerenciamento das conexões de rede.

3.1. PAM

Pluggable Authentication Modules (PAM) é um *framework* para a autenticação de usuários [Geisshirt 2007]. Seu mecanismo de autenticação permite que desenvolvedores e administradores de sistema criem seus próprios módulos de autenticação. O PAM é compatível com uma ampla gama de sistemas operacionais, desde os baseados em Unix até o Windows [Itoi and Honeyman 1998]. Na solução proposta, um módulo chamado `pam_eduroam` foi criado e acoplado ao PAM.

3.2. D-BUS

D-BUS é um barramento de mensagens para comunicação entre processos que pode ser utilizado de forma mais simples que as primitivas baseadas em compartilhamento de memória geralmente disponibilizadas pelo sistema operacional [Pennington et al. 2016].

Como o D-BUS já está consolidado em sistemas baseados em Unix, diversos aplicativos têm criado interfaces de comunicação que suportam D-BUS. Assim, cada aplicativo pode configurar uma interface de comunicação exibindo os métodos e os atributos que podem ser solicitados. Os métodos são ações que um aplicativo requisitante pode solicitar que outro aplicativo execute. Os atributos são informações que um aplicativo pode requisitar de outro, por exemplo para consultar o estado de um recurso.

Para implementar o processo de autenticação, foi criada uma conexão intermediada pelo D-BUS entre o módulo PAM e o NetworkManager.

3.3. NetworkManager

NetworkManager é um serviço controlador de rede dinâmico que gerencia as conexões de rede, procurando manter as interfaces e as conexões ativas sempre que possível. O NetworkManager inicializa junto com o sistema operacional e executa como um *daemon*. Na solução proposta, o sistema inicia sem conexão ativa ou com conexão a uma rede limitada (para permitir que o computador seja acessado remotamente pelo administrador), e permanece assim até que o usuário forneça suas credenciais.

Quando o usuário fornece os dados para autenticação, o NetworkManager é acionado para criar uma nova conexão. Essa conexão é estabelecida com base no padrão de autenticação 802.1X e utiliza os protocolos *Extensible Authentication Protocol* e *Tunneled Transport Layer Security* (EAP-TTLS) para que os dados não sejam transmitidos em texto claro [Congdon et al. 2003]. Uma vez estabelecida a nova conexão, o NetworkManager a define como primária, permitindo o acesso à internet.

3.4. Visão geral

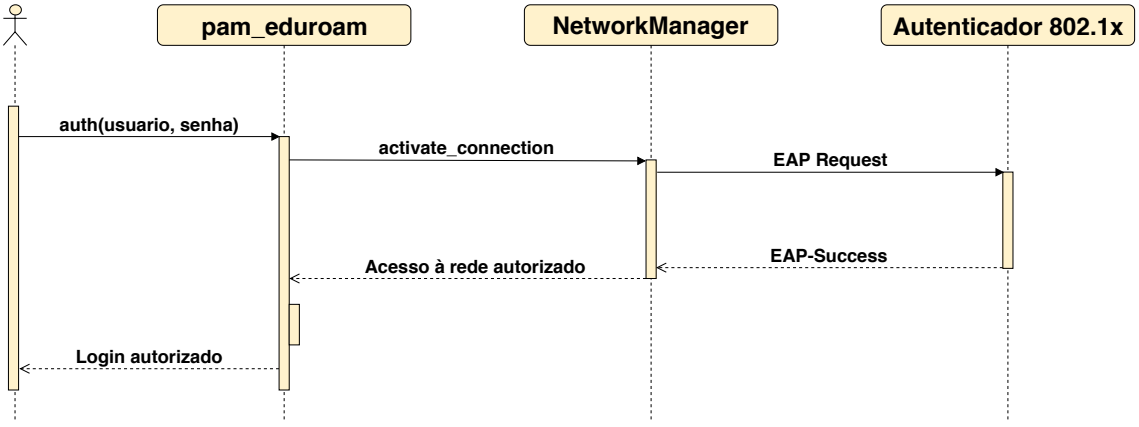

Figura 1. Diagrama de sequência para autenticação efetuada com sucesso.

Na Figura 1 é possível observar o fluxo de acionamento dos módulos para que a autenticação de um usuário seja efetuada.

Primeiramente, o usuário fornece nome de usuário e senha na tela de *login* do sistema. O módulo `pam_eduroam` recebe esses dados e configura uma rede 802.1X com os protocolos EAP-TTLS, permitindo que as credenciais sejam comunicadas ao autenticador. Caso as credenciais sejam aceitas, o NetworkManager habilita o acesso à internet e o `pam_eduroam` libera a sessão para o usuário. Caso contrário, o NetworkManager permanece sem conexão ou conectado a uma rede limitada e a sessão não é liberada.

Quando o usuário encerra a sessão, o módulo `pam_eduroam` envia uma mensagem solicitando ao NetworkManager que apague a configuração da rede. Dessa forma, mantém-se a privacidade das credenciais e evita-se que um usuário utilize uma conexão alheia.

4. Maturidade

A solução descrita neste trabalho está em produção desde maio de 2017 na sala 24 horas da Universidade Federal de São Carlos (UFSCar), que inicialmente era localizada no saguão da Secretaria Geral de Informática (SIn) e, mais recentemente, foi migrada para a Biblioteca Comunitária (BCo).

5. Disponibilidade

A solução proposta está disponível como software livre sob a licença MIT em `https://gitlab.com/asgardlab/pam_eduroam`. A documentação está disponível em `https://gitlab.com/asgardlab/pam_eduroam/wikis/home`.

6. Limitações

As especificações de autenticação e os certificados raiz de ICP de cada instituição federada cujos usuários possam vir a acessar a máquina precisam ser previamente instalados e mantidos atualizados. No futuro, pretende-se obter essas informações automaticamente da base de dados do Eduroam CAT (*Configuration Assistant Tool*) para distribui-las aos terminais que utilizem a solução.

7. Demonstração planejada para o WGID

Durante o IX Workshop de Gestão de Identidades Digitais (WGID), será disponibilizado um notebook ou computador com a solução já implantada para ser testada pela comunidade. Em sua sessão, o usuário poderá usufruir dos programas instalados e terá acesso à internet normalmente. Ao encerrar a sessão, a conexão de rede será excluída e os próximos usuários não poderão utilizar a sua configuração, nem acessar os arquivos de outros usuários.

Referências

Bello, E. H. (2014). Pluggable authentication module for 802.1x authentication protocol. `https://github.com/ehbello/pam-8021x`.

Congdon, P., Aboba, B., Smith, A., Zorn, G., and Roese, J. (2003). IEEE 802.1X remote authentication dial in user service (RADIUS) usage guidelines. RFC 3580, RFC Editor.

Geisshirt, K. (2007). *Pluggable Authentication Modules - The Definitive Guide to PAM for Linux SysAdmins and C Developers*. Packt Publishing Ltd.

Itoi, N. and Honeyman, P. (1998). Pluggable authentication module for Windows NT. In *Proceedings of 2nd USENIX Windows NT Symposium*, Seattle.

Pennington, H., Carlsson, A., Larsson, A., Herzberg, S., McVittie, S., and Zeuthen, D. (2016). *D-Bus Specification*. `https://dbus.freedesktop.org/doc/dbus-specification.html`.

Reynolds, J. (2010). When 802.1x/PEAP/EAP-TTLS is worse than no wireless security. `https://depthsecurity.com/blog/when-802-1x-peap-eap-ttls-is-worse-than-no-wireless-security`.