Universidade de Aveiro

Identificação, Autenticação e Autorização

Risk Aware SSO with SAML

Ricardo Ferreira 98411

Índice

Conteúdo

Introdução

O projeto desenvolvido tem como objetivo desenvolver um IdP capaz de suportar múltiplos serviços com MFA dependendo do serviço. É baseado num flow de SAML. O tipo de autenticação tem de ser baseado num risk score, sendo que à medida que aumenta o risco, aumenta também o número de métodos de autenticação necessários.

O código está também presente num repositório do git, pelo seguinte link: https://github.com/RicardoSerranoFerreira/IdP_SAML_98411/tree/main

Componentes Criados

IdP (Identity Provider)

O Provedor de Identidade (IdP) implementado é responsável por gerir a autenticação dos users a pedido do Service Provider (SP).

O IdP foi criado para suportar múltiplos métodos de autenticação, implementando assim MFA (hotp, hotp e hardware), sendo que o hardware não foi completamente implementado e apenas devolve “True”, ou seja, que passou a autenticação sempre que é pedida.

O risk score presente aqui é um risk score calculado com base em valores de teste, mas simulado o que seria pretendido. Neste caso, um cálculo de risk score teria que ter em conta valores tais como número de tentativas de login, localização da tentativa de login, tipo de user a dar login, atividade recente , tipo de dispositivo a ser usado para dar login, o serviço ao qual dá login, entre outros.

Isto para conseguir calcular um bom valor de risco associado à autenticação da pessoa em questão no serviço pretendido.

SAML

O SAML (Security Assertion Markup Language) é um protocolo utilizado para troca de informações de autenticação e autorização entre o IdP e os serviços. O IdP gera asserções SAML que são usadas pelos serviços para autenticar usuários.

Aqui neste projeto, foi configurado uma versão base de SAML entre ambos o IdP e o SP que dá uso aos certificados gerados pela biblioteca openssl para realizar a autenticação do user de forma eficaz.

SP (Service Provider)

O Serviço Web (Service Provider) é uma aplicação que utiliza o IdP para autenticação de seus usuários. O serviço é configurado para se integrar com o IdP e utilizar asserções SAML para autenticar usuários e ter um controlo sobre a sessão.

Quando o utilizador é autenticado, o SP mostra uma página nova que contém informação à qual o user tentava aceder, que neste caso é um documento com apenas texto.

Certificados, Dados & Templates

Certificados gerados

Aqui apresento os comandos utilizados para gerar as chaves e certificados necessários para o funcionamento do IdP e do serviço criado. De salientar que a passphrase usada para a geração foi "1234".

Geração para o IdP

openssl genrsa -out idp_key.pem 2048

openssl req -new -key idp_key.pem -out idp_csr.pem

openssl x509 -req -days 365 -in idp_csr.pem -signkey idp_key.pem -out idp_cert.pem

Geração para o Service

openssl genrsa -out sp_key.pem 2048

openssl req -new -key sp_key.pem -out sp_csr.pem

openssl x509 -req -days 365 -in sp_csr.pem -signkey sp_key.pem -out sp_cert.pem

Dados

Os dados presentes são guardados numa base de dados Flask, sendo que do lado do IdP temos duas tabelas: *User* & *Serviço* e do lado do Serviço existem também duas: *User* & *Documento,* com os atributos necessários.

Templates

Para além dos certificados gerados e forma de organizar os dados com uso a base de dados, foram criadas templates simples para as páginas web necessárias, tais como templates para as formas diferentes de autenticação, um template inicial do serviço e um template para quando o user fica logged-in.