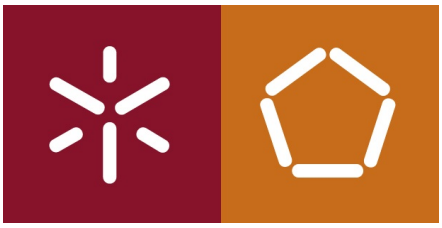

Engenharia de Segurança
Grupo 7
Aula 4

Bruno Machado - A74941
Diogo Gomes - A73825
Francisco Mendes - A75097

Fevereiro 2018

1 TOR (The Onion Router)

1.1

Devido ao âmbito do `TOR` e ao anonimato que este garante, é impossível prever-se qual será o próximo "salto". Isto é, após se efetuar o comando `sudo anonsurf change` nada garante qual será a localização do *OR* de saída.

Contudo, é possível escolher-se a localização de um *OR* caso este exista. Para tal, basta acrescentar no ficheiro `/etc/tor/torrc` a linha `ExitNodes {us} StrictNodes 1` fazendo com que na proxima vez que se efetuar o comando `sudo anonsurf change` seja garantido que o *OR* esteja localizado nos EUA.
Fonte: `https://www.torproject.org/docs/faq.html.en#ChooseEntryExit`

1.2

Para esta questão foi escolhido o primeiro link, onde conhecemos 3 *routers*, e desconhecemos outros 3 que aparecem como *relay*.

Estes ultimos aparecem assim, por causa dos pontos de *Rendezvous*. Estes pontos disponibilizam um serviço anónimo. Para tal ser possível, o cliente informa o *Diretory Server* que pretende aceder a um domínio *onion*, escolhendo de uma lista de *introduction points* quais pretende se conectar, e qual é o seu ponto de *rendezvous*.

O seu ponto de *rendezvous* consiste em 3 *OR*, em que o último é o *rendezvous point(RP)*. Do lado do servidor acontece a mesma situação, onde este utiliza 3 *OR* para se conectar ao *RP* do cliente.

É de referir que nem o servidor sabe quais são os *OR's* que o cliente usa, nem o cliente sabe quais são utilizados pelo servidor.

2 Projeto de desenvolvimento de software

O Grupo 7 decidiu escolher como projeto o Gestor de passwords com base em QRCodes. De seguida serão explicadas as etapas que esta aplicação terá de conter para que seja viável.

1ª etapa: Geração por parte do site do QRCode

O site onde o utilizador se pretende autenticar terá que gerar um QRCode distinto, para cada utilizador que se pretenda autenticar com as seguintes informações:

1. Localização para a qual a aplicação terá de enviar os dados de autenticação como o username e a password;
2. Certificado do site para garantir a sua identidade;
3. Possivelmente poderá ter a informação sobre o algoritmo de cifra simétrico a utilizar assim como a chave de sessão a utilizar na conexão;
4. Opcionalmente o site pode pedir o envio de um certificado por parte do cliente.

Este QRCode deverá ter um tempo de vida curto no qual será válido, de maneira a aumentar a segurança do protocolo.

2ª etapa: Leitura do QRCode por parte da aplicação do cliente

Depois da leitura do QRCode do site a aplicação de gestão de password terá de ser capaz de verificar a autenticidade do certificado do site de forma a poder continuar com o processo de autenticação caso este seja válido ou terminar o processo caso este seja inválido. De seguida

a aplicação de gestão de passwords verifica na sua base de dados as credenciais para o site específico, enviando-as para a localização especificada cifradas com o a chave e algoritmo presente no QRCode.

3ª etapa: Verificação por parte do site das credenciais do utilizador

Finalmente depois da aplicação ter enviado as suas credenciais para o site este deve decifrar a informação com a chave de sessão e verificar se existe um utilizador com a mesma password e username, na sua base de dados de maneira a garantir ou restringir acesso ao site.