Sistema de autenticação – Uma visão geral do funcionamento do protocolo Kerberos

Autor: Luciano Renovato de Albuquerque

1-Introdução

Muitas corporações, hoje em dia, permitem a seus funcionários, clientes e parceiros, acessar diversos serviços de forma remota. Podendo um desses serviços ser acessado, por exemplo, através da Internet, que é uma rede pública.

O parágrafo acima deixa claro que a rede privada de uma empresa ou de um laboratório, por exemplo, pode ser acessada por qualquer pessoa através de uma rede pública. Justamente nesse contexto entra a questão da autenticação.

A autenticação tem como objetivo garantir o acesso à uma rede, e seus serviços, por usuários legítimos, ou seja, quando nos referimos a uma empresa X, somente funcionários, clientes e parceiros autorizados pela empresa X devem ter acesso aos serviços disponíveis em sua rede privada. Impedindo qualquer acesso não autorizado.

2-Sistemas de Autenticação

Quando um usuário tenta acessar uma rede protegida por um sistema de autenticação, antes de permitir o acesso desse usuário, o sistema valida sua identidade.

Verificando que se trata de uma identidade com acesso permitido, o sistema gera uma autorização para o usuário. A partir desse instante, o usuário terá acesso garantido durante um determinado período de tempo estabelecido pelo sistema de autenticação. Sendo assim, quando a validade de sua autorização esgotar-se, um novo processo de autenticação será necessário.

Essa visão genérica, nos permite ter uma idéia de como ocorre o processo de autenticação num sistema dessa natureza. Porém, existem diferentes sistemas de autenticação, e a forma como implementam esse processo, para garantir a segurança de uma rede privada, pode variar.

3-Protocolo Kerberos

Após essa breve introdução, veremos como funciona um protocolo de autenticação muito conhecido na área de segurança, o Kerberos.

Esse protocolo foi desenvolvido no MIT (*Massachusetts Institute of Technology*), com o objetivo de prover autenticação forte entre aplicações cliente/servidor, utilizando-se criptografia com chave secreta. O algoritmo de criptografia utilizado pelo Kerberos é o Data Encryption Standard (DES), criado a partir do algoritmo Lucifer na década de 70.

Como mencionado anteriormente, um sistema de autenticação verifica a identidade de um usuário, permitindo ou não que o mesmo tenha acesso a serviços de uma rede privada. O Kerberos realiza esse processo utilizando três servidores, com os quais os clientes precisam se comunicar quando desejam autenticar-se. Pelo fato desses servidores trabalharem de forma independente, o Kerberos pode ser classificado como um sistema de autenticação distribuído.

É importante frisar, que ao final do processo de autenticação de um usuário, a autorização concedida para o mesmo se refere a apenas um serviço, ou seja, para cada serviço que o usuário deseje utilizar, ele deverá autenticar-se exclusivamente para o mesmo. O protocolo Kerberos utiliza um Servidor de Autenticação (SA), onde o usuário prova sua identidade, um Servidor de Concessão de Tickets (TGS) e um Servidor de Administração (KADM).

Cada um desses servidores têm a função de:

- Servidor de Autenticação (SA)

Recebe o pedido de autenticação do usuário e verifica a autenticidade de sua identidade. Tratando-se de um usuário válido, o SA fornece um ticket que o permite entrar em contato com o TGS, solicitando um ticket para um serviço específico, dando continuidade ao processo de autenticação.

- Servidor de Concessão de Tickets (TGS)

Fornece tickets para cada serviço disponível. Após o usuário ter autenticado-se no SA, entra em contato com o TGS afim de conseguir um ticket para um serviço específico. O TGS valida as informações apresentadas pelo usuário, considerando-as válidas, concede um novo ticket para ele.

- Servidor de Administração (KADM)

Realiza o controle das chaves secretas. O passo inicial antes do usuário ser capaz de autenticar-se no sistema, é cadastrar seus dados através do KADM.

4-Funcionamento

4.1-Passo Inicial

O passo inicial necessário para que o sistema de autenticação funcione, é o cadastramento tanto dos clientes como dos serviços que estarão disponíveis.

O Kerberos possuirá uma chave secreta associada a cada cliente e cada serviço, sendo conhecidas como chave de cliente e chave de serviço respectivamente. Essa chave é obtida a partir da senha fornecida pelo cliente/serviço no momento de seu cadastramento. Sendo assim, apenas o próprio cliente/serviço conhece sua chave secreta, além do Kerberos.

** os passos a seguir podem ser acompanhados através da figura no final do artigo.*

4.2-Passo 1

Quando um cliente deseja acessar um serviço qualquer protegido pelo Kerberos, antes de conseguir acessá-lo, ele deverá autenticar-se.

Nesse momento, o cliente envia uma requisição de autenticação para o SA. O SA verifica os dados fornecidos pelo cliente(identificação do cliente e uma identificação do tipo da mensagem), busca em sua base de dados as chaves secretas correspondentes ao cliente(origem da requisição) e ao TGS(onde o cliente deseja autenticar-se), e cria uma chave de sessão que será utilizada por ambos, cliente e TGS.

O SA responde ao pedido de autenticação do cliente, quando a validação de seus dados é positiva, enviando-lhe um ticket que permite acessar o TGS. Esse ticket é composto da seguinte forma: nome do cliente, nome do TGS, tempo corrente, tempo de vida do ticket, IP do cliente e a chave de sessão.

Antes de ser enviado, o ticket é criptografado utilizando-se a chave de serviço que apenas o próprio serviço e o Kerberos conhecem. Além disso, tanto o ticket, já criptografado, quanto a chave de sessão, são criptografados utilizando-se a chave de cliente.

4.3-Passo 2

Ao receber a resposta do SA, o cliente deve descriptografar a mensagem utilizando sua chave secreta. No entanto, para que isso seja possível, a senha de acesso será solicitada ao cliente. Somente a senha correta será capaz de gerar a chave secreta válida para que o processo de descriptografia tenha êxito.

Uma vez que a senha correta tenha sido informada, o cliente terá acesso ao ticket e a chave de sessão, enviados pelo SA. O ticket permitirá ao cliente comunicar-se com o TGS, e assim finalmente, obter um novo ticket para o serviço que deseja acessar.

É importante ressaltar, que a senha do cliente só foi solicitada durante o processo de autenticação uma única vez. Sendo que mesmo nesse momento, não foi necessário enviá-la através da rede, onde ela poderia ser capturada alguém sem autorização. A chave secreta do cliente, obtida através da senha, é apagada da memória após ter sido utilizada. Não é possível obter a chave secreta sem o conhecimento da senha do cliente.

4.4-Passo 3

Nesse passo, o cliente deve enviar a requisição ao TGS. Na requisição deverão constar: um autenticador, o ticket enviado pelo SA, devidamente criptografado com a chave secreta do serviço, e a identificação do serviço requisitado.

O autenticador é uma mensagem onde constam, uma identificação do cliente(nome + IP) e uma identificação do tipo de mensagem, semelhante a utilizada na requisição feita no passo 1. O autenticador é criptografado utilizando-se a chave de sessão fornecida pelo SA.

4.5-Passo 4

Ao receber a requisição, o TGS utiliza sua chave secreta para descriptografar o ticket, e utiliza a chave de sessão que acabou de receber, na própria requisição, para descriptografar o autenticador.

No final desse processo, o TGS utiliza os dados que obteve para validar a requisição do cliente. Os nomes do cliente, os IPs obtidos e o tempo corrente, tanto do ticket quanto do autenticador, são comparados. Sendo todos os dados comparados, válidos, uma nova chave de sessão é criada pelo TGS.

Um novo ticket é criado, dessa vez contendo as informações referentes ao cliente e serviço. A chave de serviço é utilizada para criptografar o ticket. Em seguida, a chave de sessão e o ticket, já criptografado, são criptografados juntos utilizando-se a chave de sessão enviada pelo próprio cliente. Finalmente, a mensagem de resposta é enviada para o cliente.

4.6-Passo 5

A partir de agora, o cliente será capaz de utilizar o serviço que deseja. Porém, antes disso, é preciso descriptografar a mensagem utilizando a chave de sessão.

Terminado esse processo, o cliente tem em "mãos" o ticket que lhe permitirá acessar o serviço, e também, a nova chave de sessão que será utilizada para estabelecer a comunicação entre os dois.

Para finalizar o processo de autenticação, o cliente deve criar um autenticador, contendo seu nome, IP e tempo corrente. Criptografar esse autenticador com a chave de sessão, e junto com

ticket fornecido pelo TGS, formar uma requisição que será enviada diretamente para o serviço que deseja-se acessar.

Só resta agora que o serviço verifique a requisição recebida. Com sua chave secreta o serviço consegue descriptografar o ticket recebido. Dentre outras informações, consta no ticket a chave de sessão criada pelo TGS, que o permitirá descriptografar o autenticador enviado pelo criente.

Os nomes do cliente, os IPs obtidos e o tempo corrente, tanto do ticket quanto do autenticador, são comparados. Considerando os dados válidos, o serviço tem certeza quanto a veracidade da identidade do cliente e a autenticação é finalizada.

A comunicação entre o cliente e o serviço poderá ser feita de três formas diferentes:

- Normal

Apenas a autenticação inicial é exigida. A partir daí, não é feita mais nenhuma autenticação e as mensagens também não são criptografadas.

- Safe Messages

Todas as mensagens são autenticadas, porém não são criptografadas.

- Private Message

É a forma mais segura e também a mais custosa. Todas as mensagens são criptografadas e autenticadas.

5-Problemas

O Kerberos também possui suas fraquezas, veremos a seguir um ponto negativo inerente a sua arquitetura.

Costumamos nos referir ao Protocolo Kerberos, como sendo a implementação de um sistema distribuído. Isso porque possui características, que pudemos conhecer nesse artigo, como a existência de 3 servidores que funcionam independentemente uns dos outros. O que teoricamente, o tornaria mais robusto.

A princípio, quando pensamos num sistema distribuído, imaginamos que diante de uma situação caótica, onde problemas ocorreriam afetando parte do sistema, o mesmo não poderiam ser afetado em sua totalidade. Com isso, seria possível manter o serviço ao qual o sistema se predispõem a realizar, mesmo que, devido ao cenário levado em consideração, funcionando de forma menos eficiente.

Considerando o Kerberos em uma situação como a citada no parágrafo anterior, imaginando que a base de dados do Protocolo fosse violada, e seus dados fossem acessados, todo o sistema estaria comprometido. No que se refere a funcionalidade, os serviços do Protocolo Kerberos, não funcionam independentemente, se lembrarmos por exemplo, que antes de solicitar um ticket referente a um determinado serviço, o cliente deve realizar um pedido de autenticação ao SA.

Além dessa fraqueza, o Kerberos possui falhas que permitem um atacante se passar por um cliente autenticado, "roubando" sua identidade, ou até mesmo paralisar parte do sistema realizando um overflow, Para uma visão detalhada dessas falhas, além de suas soluções, como a aplicação de patches, aconselho ao leitor as referências [6] e [7].

6-Conclusão

Esse artigo nos permite ter uma visão geral do funcionamento do protocolo Kerberos, observando seu funcionamento distribuído, além de nos permitir perceber porque esse protocolo é também conhecido como um protocolo de autenticação third-party, onde uma terceira entidade, o Kerberos, existe entre o cliente e o serviço, com o objetivo de garantir a segurança na comunicação entre os dois.

7-Figura

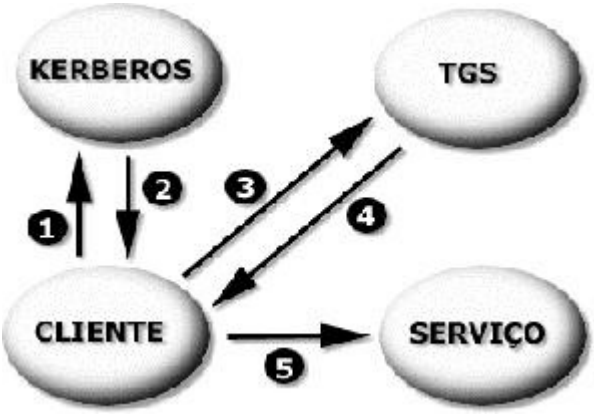

Figura 1 - Protocolo Kerberos