Artigo final de sistemas distribuídos - Análise do Protocolo Kerberos: Autenticação e Segurança em Sistemas Distribuídos

Luiz Antônio Lima de Freitas Leite[1], **Max José Lobato Pantoja Junior**[1], **Wesley Pontes Barbosa**[1], **Luiz Sérgio Samico Maciel**[1]

[1]Instituto de Ciências Exatas e Naturais (ICEN) – Universidade Federal Pará
Belém, PA – Brasil

{luiz.freitas.leite,max.junior,wesley.pontes.barbosa,luiz.filho}@icen.ufpa.br

Abstract. *This article presents a study on digital security techniques in distributed systems, focusing on the Kerberos protocol. It explores the concepts of authentication, trusted third parties, and symmetric cryptography. Furthermore, a case study on its implementation in directory services (Active Directory) is presented, demonstrating its effectiveness in mitigating network threats.*

Resumo. *Este artigo apresenta um estudo sobre técnicas de segurança digital em sistemas distribuídos, com foco no protocolo Kerberos. São explorados os conceitos de autenticação, terceira parte confiável e criptografia simétrica. Além disso, é apresentado um estudo de caso sobre sua implementação em serviços de diretório (Active Directory), demonstrando sua eficácia na mitigação de ameaças em rede.*

1. Introdução

A segurança da informação compõe um dos pilares fundamentais no projeto e implementação de Sistemas Distribuídos. Segundo Tanenbaum e Van Steen [Tanenbaum and Van Steen 2017], a abertura e a conectividade inerentes a esses sistemas, embora permitam o compartilhamento eficiente de recursos, introduzem vulnerabilidades críticas inexistentes em sistemas centralizados. Enquanto um sistema operacional local detém controle total sobre o acesso à memória e aos periféricos, os sistemas distribuídos dependem de redes de comunicação para a troca de mensagens. Frequentemente, essas redes comportam-se como canais inseguros, suscetíveis à interceptação passiva (*sniffing*) e à modificação ativa ou mascaramento (*spoofing*) de dados por agentes mal-intencionados.

O cerne dessa problemática reside na **autenticação**: a necessidade de um cliente provar sua identidade a um servidor remoto sem a exposição de sua senha em texto claro pela rede. O tráfego de credenciais por meios inseguros, ainda que ocorra de forma esporádica, vulnerabiliza o sistema a ataques de captura de tráfego. Adicionalmente, em cenários compostos por múltiplos serviços, como sistemas de arquivos e bancos de dados, a exigência de repetidas inserções de senhas degrada a usabilidade e induz o usuário a adotar práticas de segurança frágeis.

Neste cenário, o protocolo **Kerberos** consolida-se como uma solução padrão para autenticação em redes inseguras. Desenvolvido originalmente no Projeto Athena do MIT [Neuman and Ts'o 1994], o protocolo fundamenta-se no uso de criptografia simétrica e na existência de uma Terceira Parte Confiável (Trusted Third Party - TTP) para mediar

a confiança entre clientes e servidores. O Kerberos permite que entidades comprovem sua identidade mutuamente, garantindo a integridade e a confidencialidade das sessões estabelecidas.

Este artigo tem como objetivo analisar a arquitetura de segurança do protocolo Kerberos. Serão detalhados os conceitos fundamentais de criptografia e canais seguros, o fluxo de troca de mensagens para obtenção de tickets e a mitigação de ataques de repetição. Por fim, apresenta-se um estudo de caso sobre sua implementação no Microsoft Active Directory, demonstrando sua aplicabilidade em infraestruturas modernas.

2. Conceitos de Segurança em Sistemas Distribuídoss

Para compreender o funcionamento e as decisões de projeto do Kerberos, é imperativo estabelecer os fundamentos sobre canais seguros e os modelos de confiança em redes distribuídas. A segurança nestes sistemas depende da capacidade de transformar um canal de comunicação inseguro em um canal seguro através de mecanismos criptográficos.

2.1. Canais Seguros e Criptografia

Um canal seguro é um meio de comunicação que garante propriedades essenciais de segurança, nomeadamente: a **confidencialidade**, assegurando que apenas as partes autorizadas tenham acesso à informação; a **integridade**, garantindo que a mensagem não foi alterada em trânsito; e a **autenticação**, que confirma a identidade das partes envolvidas [Coulouris et al. 2013].

Para implementar tais canais, utilizam-se algoritmos criptográficos divididos em duas categorias principais:

- Criptografia assimétrica (Chave Pública): utiliza um par de chaves (pública e privada). Embora resolva problemas de distribuição de chaves e assinatura digital, possui alto custo computacional, sendo centenas de vezes mais lenta que a criptografia simétrica.
- Criptografia simétrica (Chave Secreta): utiliza uma única chave compartilhada entre as partes para cifrar e decifrar as mensagens (ex: AES, DES). Devido ao seu alto desempenho, é a escolha ideal para cifrar o fluxo de dados em sessões de comunicação longas.

O protocolo Kerberos baseia-se primordialmente na criptografia simétrica para garantir velocidade no processamento de milhares de autenticações simultâneas. No entanto, o uso exclusivo de chaves simétricas introduz um desafio logístico crítico: a distribuição segura dessas chaves.

2.2. Autenticação e Terceira Parte Confiável (TTP)

Em um sistema distribuído de larga escala com N entidades (usuários e servidores), se cada par de entidades precisasse se comunicar diretamente com segurança, seriam necessárias $N(N-1)/2$ chaves secretas distintas. O gerenciamento descentralizado dessas chaves torna-se inviável à medida que o sistema cresce.

Para mitigar esse problema de complexidade quadrática, adota-se o modelo de Terceira Parte Confiável (*Trusted Third Party* – TTP). Neste modelo, introduz-se uma autoridade central na qual todos os participantes confiam, denominada Centro de Distribuição de Chaves (*Key Distribution Center* – KDC).

Em vez de o cliente provar sua identidade diretamente para cada servidor de arquivos ou impressão, ele prova sua identidade uma única vez para o KDC. A autoridade central, então, emite credenciais temporárias (tickets) cifradas, que o cliente apresenta aos servidores de destino. Essa arquitetura centraliza a administração de segurança, minimiza a exposição de segredos de longa duração (senhas) e permite a escalabilidade do sistema, visto que cada nova entidade precisa estabelecer uma chave secreta apenas com o KDC, e não com todos os outros participantes da rede.

3. O Protocolo Kerberos

[LA]

Desenvolvido pelo MIT no projeto Athena, o Kerberos é um protocolo de autenticação de rede projetado para fornecer autenticação forte para aplicações cliente/servidor.

3.1. Arquitetura e Componentes

O ecossistema Kerberos é composto por três entidades lógicas principais:

- **Cliente:** A entidade (usuário ou software) que deseja acessar um recurso.
- **Servidor de Aplicação (SS - Service Server):** O recurso que o cliente deseja acessar (ex: servidor de arquivos).
- **KDC (Key Distribution Center):** A terceira parte confiável. O KDC mantém um banco de dados com as chaves secretas de todos os usuários e serviços. Logicamente, ele é dividido em dois subcomponentes:
  - *Authentication Server (AS):* Responsável pelo login inicial e emissão do TGT.
  - *Ticket Granting Server (TGS):* Responsável por emitir tickets para serviços específicos com base em um TGT válido.

3.2. Funcionamento e Troca de Mensagens

O fluxo de autenticação no Kerberos ocorre em etapas distintas, desenhadas para garantir que a senha do usuário nunca trafegue pela rede:

1. **Solicitação de Autenticação (AS_REQ):** O cliente envia uma solicitação ao AS informando sua identidade (em texto claro).
2. **Emissão do TGT (AS_REP):** O AS verifica se o usuário existe. Se sim, gera uma chave de sessão e um Ticket de Concessão de Tickets (TGT). O TGT é criptografado com a chave do TGS, e a resposta para o cliente é criptografada com a chave derivada da senha do usuário. O cliente decifra essa resposta, obtendo a chave de sessão e o TGT, sem que a senha tenha saído de sua máquina.
3. **Solicitação de Serviço (TGS_REQ):** Quando o cliente precisa acessar um recurso (ex: impressora), ele envia ao TGS o seu TGT e um "Autenticador".
4. **Emissão do Ticket de Serviço (TGS_REP):** O TGS valida o TGT. Se válido, gera um Ticket de Serviço (criptografado com a chave do servidor de destino) e o envia ao cliente.
5. **Acesso ao Recurso (AP_REQ):** O cliente apresenta o Ticket de Serviço ao servidor da aplicação, que o decifra e valida a identidade do cliente, permitindo o acesso.

3.3. Mitigação de Ataques

[SAMICO]

Uma das principais ameaças em autenticação distribuída é o "Ataque de Repetição"(*Replay Attack*), onde um atacante intercepta um ticket válido e o reenvia para o servidor para ganhar acesso não autorizado.

O Kerberos mitiga isso através do uso de *Timestamps* (carimbos de tempo). Cada ticket e autenticador possui a hora de criação e um tempo de vida (TTL) curto (geralmente 8 a 10 horas para TGTs e minutos para autenticadores). Se um servidor receber um pacote com um horário muito diferente do seu relógio local (fora de uma janela de tolerância, comumente 5 minutos), a solicitação é rejeitada. Isso implica que a sincronização de relógios (via NTP) é um requisito obrigatório para o funcionamento de redes Kerberos.

4. Estudo de Caso: Microsoft Active Directory

[WESLEY]

Embora o Kerberos seja um padrão aberto, sua implementação mais difundida ocorre no Microsoft Active Directory (AD), utilizado globalmente para gerenciamento de identidades em redes corporativas. Desde o Windows 2000, o Kerberos é o protocolo de autenticação padrão, substituindo o antigo NTLM.

No AD, os Controladores de Domínio (Domain Controllers) atuam como o KDC. Ao ingressar em um domínio, computadores e usuários recebem chaves secretas que são gerenciadas centralmente pelo AD.

4.1. Single Sign-On (SSO)

A principal aplicação prática perceptível ao usuário final é o recurso de *Single Sign-On* (SSO). Em um ambiente distribuído sem Kerberos, o usuário teria que digitar sua senha cada vez que acessasse uma pasta compartilhada em um servidor diferente ou acessasse a intranet.

Com a implementação do Kerberos no AD, o processo ocorre em segundo plano:

1. O usuário faz login na estação de trabalho (autenticação junto ao AS).
2. O sistema operacional armazena o TGT na memória segura (LSASS).
3. Quando o usuário clica em uma pasta de rede, o sistema operacional detecta a necessidade de autenticação, envia o TGT ao Controlador de Domínio (TGS), obtém o ticket de serviço e autentica-se no servidor de arquivos.

Tudo isso ocorre de forma transparente, proporcionando segurança robusta sem sacrificar a usabilidade.

5. Conclusão

O protocolo Kerberos representa um marco na segurança de Sistemas Distribuídos, resolvendo o complexo problema de autenticação em redes inseguras através de criptografia simétrica e de uma arquitetura de confiança centralizada. Sua capacidade de separar as credenciais de longa duração (senhas) das credenciais de sessão (tickets) reduz drasticamente a superfície de ataque.

Contudo, o modelo apresenta desafios. O KDC torna-se um ponto único de falha e um potencial gargalo de desempenho; se o KDC estiver indisponível, ninguém consegue acessar recursos na rede. Por isso, implementações reais, como o Active Directory, exigem replicação de servidores KDC. Além disso, a dependência estrita de sincronização de relógios impõe requisitos de infraestrutura adicionais. Apesar dessas limitações, o Kerberos permanece como o padrão da indústria para autenticação segura em intranets e sistemas corporativos.

Referências

Coulouris, G., Dollimore, J., Kindberg, T., and Blair, G. (2013). *Sistemas Distribuídos: Conceitos e Projeto*. Bookman Editora, 5 edition.

Neuman, B. C. and Ts'o, T. (1994). Kerberos: An authentication service for computer networks. *IEEE Communications Magazine*, 32(9):33–38.

Tanenbaum, A. S. and Van Steen, M. (2017). *Sistemas Distribuídos: Princípios e Paradigmas*. Pearson Education do Brasil, 3 edition.