

Análise do Protocolo Kerberos: Autenticação e Segurança em Sistemas Distribuídos

**Luiz Antônio Lima de Freitas Leite¹, Max José Lobato Pantoja Junior¹,
Wesley Pontes Barbosa¹, Luiz Sérgio Samico Maciel¹**

¹Instituto 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 é um dos desafios fundamentais no projeto de Sistemas Distribuídos. Diferente de sistemas centralizados, onde o sistema operacional tem controle total sobre o acesso à memória e recursos, sistemas distribuídos dependem de redes de comunicação que podem ser acessíveis a terceiros mal-intencionados...

2. Conceitos de Segurança em Sistemas Distribuídos

2.1. Canais Seguros e Criptografia

Para garantir a confidencialidade e integridade dos dados trafegados...

2.2. Autenticação e Terceira Parte Confiável (TTP)

A autenticação em larga escala torna-se inviável se cada servidor precisar armazenar as senhas de todos os usuários. Surge então a necessidade de uma autoridade central confiável...

3. O Protocolo Kerberos

3.1. Arquitetura e Componentes

O Kerberos, desenvolvido pelo MIT, baseia-se no modelo de chave simétrica de Needham-Schroeder. Sua arquitetura é composta por três entidades principais...

3.2. Funcionamento e Troca de Mensagens

Uma característica fundamental do Kerberos é o uso de "Tickets". O usuário não se autentica em cada serviço; ele se autentica uma vez no AS e recebe um bilhete mestre (TGT)...

3.3. Mitigação de Ataques

Para evitar que um atacante copie um ticket válido e o reutilize posteriormente (ataque de repetição), o Kerberos utiliza rigorosos carimbos de tempo...

4. Estudo de Caso: Microsoft Active Directory

Embora o Kerberos tenha nascido no mundo Unix/Linux (projeto Athena do MIT), sua adoção massiva ocorreu através do Microsoft Active Directory (AD). Em um ambiente corporativo Windows...

4.1. Single Sign-On (SSO)

A aplicação prática mais visível do Kerberos é a capacidade de *Single Sign-On*. O usuário insere suas credenciais apenas na estação de trabalho...

5. Conclusão

O estudo do protocolo Kerberos demonstra a importância de mecanismos centralizados de confiança em ambientes distribuídos. Apesar de sua robustez, a centralização no KDC exige estratégias de replicação para evitar indisponibilidade...

Referências

- Coulouris, G., Dollimore, J., Kindberg, T., and Blair, G. (2013). *Distributed Systems: Concepts and Design*. Pearson, 5th edition.
- Tanenbaum, A. S. and van Steen, M. (2017). *Distributed Systems: Principles and Paradigms*. Pearson Education, 3rd edition.
- Neuman, B. C. and Ts'o, T. (1994). Kerberos: An authentication service for computer networks. *IEEE Communications Magazine*, 32(9):33–38.