

Artigo final de sistemas distribuídos - 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

2. Conceitos de Segurança em Sistemas Distribuídos

2.1. Canais Seguros e Criptografia

2.2. Autenticação e Terceira Parte Confiável (TTP)

3. O Protocolo Kerberos

3.1. Arquitetura e Componentes

3.2. Funcionamento e Troca de Mensagens

3.3. Mitigação de Ataques

4. Estudo de Caso: Microsoft Active Directory

4.1. Single Sign-On (SSO)

5. Conclusão

Referências