

**PROPOSAL PROYEK AKHIR (PA)
EC 5010 KEAMANAN SISTEM INFORMASI
DOSEN: BUDI RAHARDJO**

**NAMA: IVAN CHRISTIAN
NIM : 13200160**

**JUDUL YANG DIAJUKAN :
SISTEM OTENTIFIKASI KERBEROS PADA JARINGAN KOMPUTER ITB**

Abstrak

Sebuah sistem jaringan terbuka tidak memiliki tingkat keamanan yang sama dengan sistem jaringan tertutup. Sistem otentikasi konvensional (*password-based*) rentan terhadap serangan seperti *eavesdropping*, *tampering*, dan *impersonation*. Untuk itu dibutuhkan sistem otentikasi yang lebih aman dan *scalable*.

Kerberos adalah protokol otentikasi jaringan yang dikembangkan oleh MIT. Protokol ini menggunakan kriptografi untuk otentikasi baik *client* maupun *server*, sehingga diharapkan protokol ini mampu mengatasi kelemahan dari sistem otentikasi *password-based*.

Makalah ini akan membahas apa itu Kerberos, bagaimana cara protokol ini melakukan otentikasi pada jaringan, keunggulan dan keterbatasan dari protokol ini, dan struktur Kerberos pada jaringan yang besar. Dengan merujuk pada beberapa universitas yang telah mengimplementasikan Kerberos (seperti MIT dan Stanford), saya akan mencoba mendesain struktur sistem otentifikasi Kerberos pada jaringan ITB.

Referensi:

1. Jeniffer G. Steiner, Clifford Neumann, and Jeffrey I. Schiller, *Kerberos: An Authentication Service of Open Network System*, MIT Project Athena, Cambridge, Massachusetts (12 January 1988)
2. Steven M. Bellovin and Michael Merritt, *Limitation of The Kerberos Authentication System*. AT&T Bell Laboratories, (Winter 1991)
3. <http://www.isi.edu/gost/brian/security/kerberos.html>, *The Moron's Guide To Kerberos, Version 1.2.2*
4. <http://web.mit.edu/kerberos/www/dialogue.html>, *Designing an Authentication System: A Dialogue in Four Scenes*
5. <http://www.stanford.edu/services/kerberos/>, *Kerberos at Stanford*
6. http://www.computerworld.com/computerworld/records/images/pdf/kerberos_chart.pdf, *Sharing a Secret: How Kerberos Works*
7. Red Hat Enterprise Linux 3: Reference Guide, *Chapter 18. Kerberos*