

# Kerberos V4

Raj Jain

Washington University in Saint Louis

Saint Louis, MO 63130

Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

<http://www.cse.wustl.edu/~jain/cse571-07/>



- ❑ What is Kerberos?
- ❑ Kerberos V4 Concepts and Design Principles
- ❑ Replicated KDCs
- ❑ Multiple Realms
- ❑ Other details

# Overview of Kerberos



- ❑ Allows two users (or client and server) to authenticate each other over an insecure network
- ❑ Named after the Greek mythological character *Kerberos* (or *Cerberus*), known in Greek mythology as being the *monstrous three-headed guard dog of Hades*
- ❑ Designed originally for Project Athena at M.I.T.
- ❑ Implementation freely available from M.I.T.
- ❑ V5 is proposed as an Internet Standard (RFC 4120)
- ❑ Windows 2000/XP/Server 2003/Vista use Kerberos as their default authentication mechanism
- ❑ Apple's Mac OS X clients and servers also use Kerberos
- ❑ Apache HTTP Server, Eudora, NFS, OpenSSH, rcp (remote copy), rsh, X window system allow using Kerberos for authentication.