
Progress since the last meeting



- Kerberos cells have been set up at ORNL, ARL, ANL, and FNC
 - ORNL's KDC is on an HP CMW workstation
 - ORNL and ANL have successfully done cross-realm authentication, even through a third (trusted) party
 - "How to Kerberize your site" web page completed <http://www.epm.ornl.gov/~jar/HowToKerb.htm>
 - Kerberos 5 V1.0 released and installed.
 - Doug Engert (ANL) wkrlogin tested on W95 and NT
 - Jim Dray - NIST generic authentication module
-
-
-

Kerberos Task Force

James A. Rome, ORNL
February 13, 1997



Why isn't Kerberos more widely adopted?



- It is a non-trivial task to "make" Kerberos
 - Compiles best with GNU C compiler which itself is hard to make
 - Takes lots of disk space during the make process
 - Different configure switches may be needed for each platform
 - Not all components really work (IBM rlogin)
 - Most clients not there yet in PC world
 - Only *wkrlogin* and *telnet* on Windows now. FTP missing.
 - Users don't want "security"
-
-
-

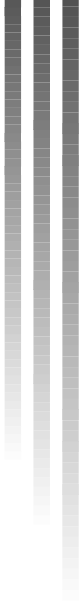
Other problems

- Significant resource commitment
 - secure kdc and slaves, and host machines
 - administration of user accounts and services
 - Size of realm
 - If too small it will not cross authenticate well (i.e., everyone is a domain)
 - Can you trust the security of a small realm
 - Need "lab" wide, but hard to sell to "lab"
-
-
-



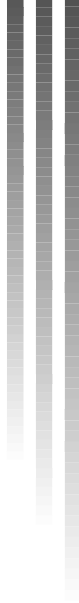
On the plus side ...

- Kerberos is free from MIT
- It provides once-a-day logins for users
- K5 interoperates with DCE
- It has proven itself to be quite resistant to attack
- Commercial options are available



The DCE option

- DCE 1.2.2 - K5 rlogin, rlogind, k5lib
- Several commercial vendors support DCE



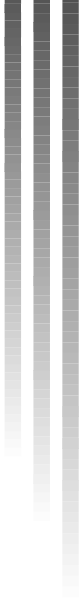
Commercial options

Problems with commercial vendors

- They prefer to offer enterprise solutions
- It is hard to extract any price guidelines (phone tag)
- There are often key components missing (e.g., ftp)
- They claim to "have fixed the MIT version"

But they provide some real advantages

- They guarantee the components work
- They offer frequent bug fixes
- They support hardware authentication tokens
- May have clients for other platforms, e.g., CyberSafe Mac



Cross-realm authentication

Solves the problem of only having one ticket principal at a time since this ticket can be used to obtain tickets for other realms. Thus, cross-site distributed computing becomes possible.

- It is enabled via some compile-time switches and configuration file entries.
- Doug Engert will give a demo of cross-realm authentication.

