

## Kerberos Proposal

### Existing MIT Realm and Windows2000 Support

#### Goals:

- Preserve existing MIT-based Kerberos 5 infrastructure so that no current functionality is lost.
- Continue to support free desktop tools that are in wide use on campus.
- Extend present architecture to include support for Windows 2000 clients and services.
- Promote further expansion of Kerberos to faculty/staff desktops, PLUS, application authentication, etc.
- Maintain one authoritative realm (MIT) for the campus. Leverage the account management, authentication mechanisms and authorizations.
- Do not compromise the security or integrity of the primary Key Distribution Centers or any device participating in a trust relationship.
- Single sign-on: Allow an authenticated entity to gain access to all authorized resources in either realm without additional authentication. Seamlessly integrated from user's perspective.
- Minimize dependence on additional third party products or services

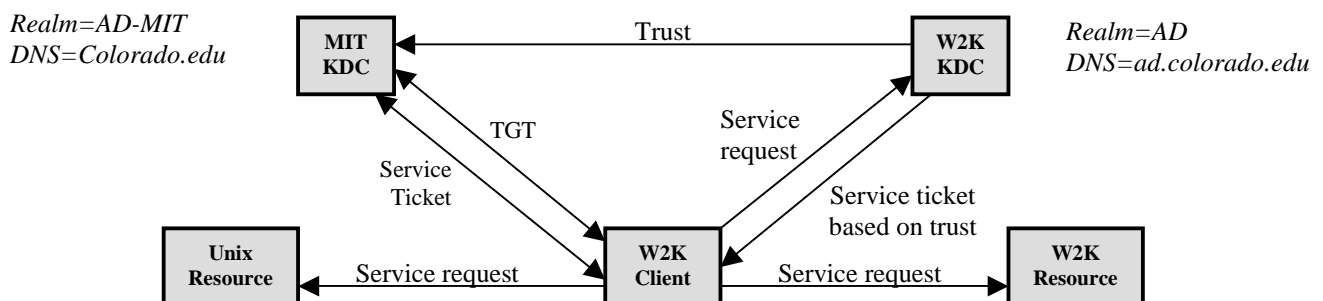
#### Givens:

- UCB has a well-established Kerberos 5 realm with ~35,000 principals and good account management.
- Windows 2000 requires the existence of its own KDC in the Windows 2000 domain.
- One-way trust relationship, with the Windows2000 realm (domain) trusting the MIT K5 realm, functions properly as verified through testing.
- Most popular desktop tools in use on campus are distributed free of charge and are standards-based.
- Majority of users are unaware of the mechanics and benefits of Kerberos authentication.
- Kerberos authentication "authorizes" use of dial-in modems and desktop systems in student labs.

#### Proposal:

- Create a two realm Kerberos environment: existing MIT realm and new Windows2000 realm (domain). Continue to use the existing MIT-based KDC as the primary authentication authority for campus.
- Populate the Windows2000 KDC with account principal information from the MIT KDC. Passwords will not (cannot) be synchronized between the two realms, so passwords will be randomly generated for Windows2000 accounts and remain unknown to the account owners and administrators.
- Access to resources in the Windows2000 realm will be accomplished through a one-way, non-transitive trust relationship.
- The Windows2000 realm will defer to the MIT realm for authentications and honor credentials acquired for gaining access to services.
- Authorizations established in the Windows2000 domain will determine access privileges for users and resources that reside in that domain.

#### Logical Diagram:



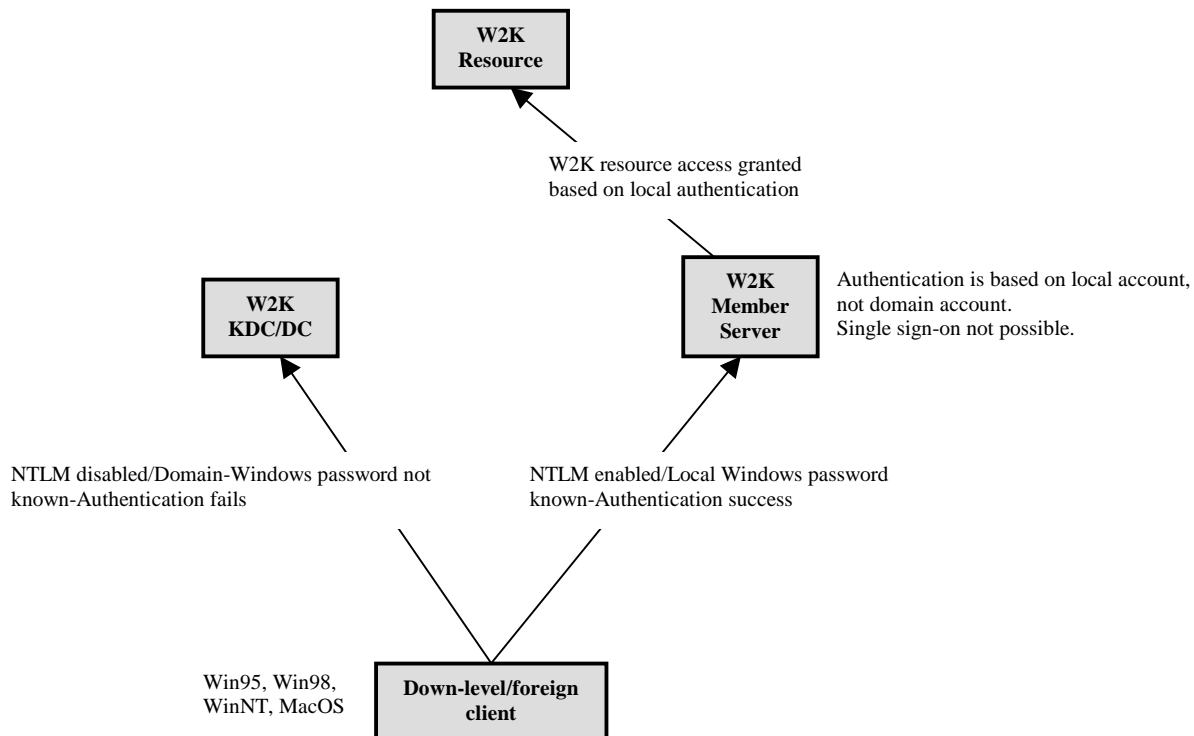
**Limitations and Risks:**

- The required Windows2000 KDC represents an additional instance of the Kerberos database. The vulnerability of the Windows2000 KDC is not well understood yet.
- Method of populating Windows KDC with account information from existing MIT system has not been defined.
- There is no known method of synching passwords for account principals that exist in both realms. Passwords will need to be managed in one realm only (MIT). Since passwords are unknown to users in the Windows2000 domain, they cannot provide credentials directly to gain access to a W2K resource.
- Access to resources that is based on Kerberos authentication occurs via established trust relationships.
- The future of Kerberos development is unclear. Changes in "ownership" or focus may require us to rework parts of our infrastructure and client tools.
- The proposed implementation does not allow for down-level/foreign (Win9x, WinNT, MacOS) client authentication to the Active Directory. NTLM will be disabled at the DC's, but not for the entire domain. NTLM is still required for down-level client access to Windows2000 member servers within individual OU's.

**Support for Down-level Clients:**

Problem: Since NTLM is disabled at the DC's, support for down-level/foreign client access to resources in the Windows2000 realm doesn't exist. Furthermore, the password assigned to an account in the Windows2000 domain is unknown to the user, so they cannot provide it on demand.

Solution: NTLM security can be enabled locally (at the OU level). Local administrators can choose to use NTLM authentication for the resources they manage and create local accounts for their users. Users would then have access to resources from their down-level/foreign clients, but these privileges would be available locally only, with no value or impact elsewhere in the domain. They would also not have the benefit of single sign-on access to these resources.



### Required Interoperability:

Authentication Authority: MIT Kerberos 5 Key Distribution Center  
Mode/Trust: One-way, non-transitive trust wherein MS KDC trusts MIT KDC

### Existing Clients:

<u>Client OS</u>	<u>Client</u>	<u>Resource</u>	<u>Comments</u>
Unix	kinit		
Unix	rlogin	non-W2K	
Unix	ktelnet	non-W2K	
Mac OS	IDKey v3.0	local desktop	ITS labs
Mac OS	ktelnet	non-W2K	
Mac OS	Chooser	Win2000 share	not kerberized
Win95/98	IDKey v3.0	local desktop	ITS labs
Win95/98	ktelnet	non-W2K	
Win95/98	Explorer	Win2000 share	not kerberized
WinNT 4	IDKey v3.0	local desktop	ITS labs
WinNT 4	ktelnet	non-W2K	
WinNT 4	Explorer	Win2000 share	not kerberized

### New Clients/Services:

<u>Client OS</u>	<u>Client</u>	<u>Resource</u>	<u>Comments</u>
Win2000	login GINA	Win2000	Successful login
Win2000	Explorer	Win2000 share	Successfully browse share
Win2000	ktelnet	non-W2K	

### Next Steps:

Continue testing Hummingbird and Kermit95 Ktelnet/Kftp clients. We have been unable to successfully configure these clients for a valid test.

Begin design/work on methods to populate Windows2000 from MIT KDC and current LDAP directory.

Renew effort to clean-up account management with regard to Identikey.

Continue effort to place "master" MIT KDC in Telecom switch room.

Redesign LDAP loads for frequency, and privacy enacted student records.