

Kerberos Testing (2)

MIT and Windows2000 Interoperability

Test 1 Purpose:

Test current MIT infrastructure with Microsoft solution, in part to determine dependence on CyberSafe technologies. Test trust relationship behavior between MIT KDC and Win2000 KDC. Run tests on various scenarios and record results. This is a test of the limitations of interoperability and not necessarily a practical test of a proposed implementation.

Components:

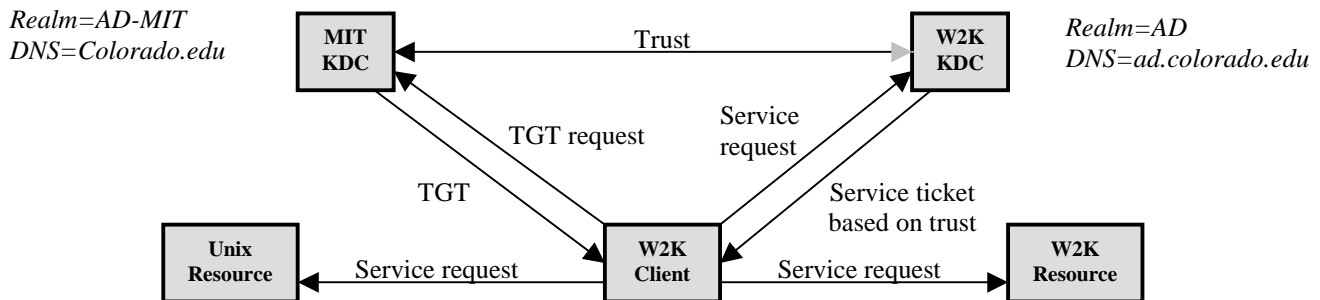
MIT KDC, with test realm: AD-MIT

W2K KDC, with test realm: ad.Colorado.edu

-Same set of principals on each KDC

Win2000 desktop machine as test client

Kerb principals: test principals on MIT KDC. User objects with same id as MIT-side test principals on MS KDC but with different passwords; kerberos mapping to principals on MIT KDC.



Testing:

The test should involve the following interoperability scenarios with a) one-way, then b) two-way trusts:

| | <u>Client (init)</u> | <u>KDC</u> | <u>Resource</u> | <u>Mode/Trust</u> | <u>Result</u> |
|----|----------------------|------------|-----------------|-------------------|----------------------------------|
| a. | Win2000 | MIT | Win2000 | one-way | login OK, credentials challenged |
| | Win2000 | MIT | non-W2K | one-way | login OK, ktelnet tool n/a |

Set one-way, non-transitive trust relationship to MIT Kerberos realm (AD-MIT). On MIT KDC (olaf), Emeson adds: krbtgt/AD.COLORADO.EDU@AD-MIT.COLORADO.EDU. Created account mapping from W2K account to MIT account.

| | | | | | |
|----|---------|-----|---------|---------|----------------------------------|
| b. | Win2000 | MIT | Win2000 | two-way | login OK, credentials challenged |
| | Win2000 | MIT | non-W2K | two-way | login OK, ktelnet tool n/a |

Set two-way, non-transitive trust between AD.Colorado.edu and AD-MIT.Colorado.edu.

General Results: One-way, non-transitive trust

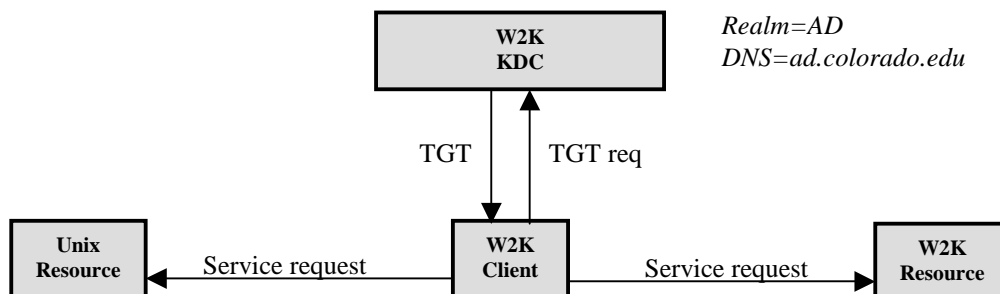
- Attempt to log in to AD-MIT.COLORADO.EDU realm from W2K client GINA: Login is successful, captured contents of kerb cache. Attempt to browse a share on W2K server in ad.Colorado.edu yields a credential challenge. Supplying valid ad.Colorado.edu credentials allows access to the share on adtestdc.
- Both logins to AD and to AD-MIT were successful; however, a TGT from the AD-MIT realm did not allow us to access windows resources in the native W2K realm(a credentials challenge was issued exactly like the one way trust scenario). We are currently trying to obtain information and a hot-fix from Microsoft which could address this problem. Our hope is that the hot-fix will allow us to use the TGT obtained in the foreign MIT realm to access resources in the native W2k realm. As in the one-way trust scenario, a Ktelnet for Windows2000 tool was not available to test.

Test 2 Purpose:

Test utility of Microsoft KDC as sole authentication authority. Run tests on various scenarios and record results. This is a test of the limitations of interoperability and not necessarily a practical test of a proposed implementation.

Components:

W2K KDC, with test realm: ad.Colorado.edu
Win2000 desktop machine as test client
Resource in MIT (AD-MIT) realm to access



Testing 2a:

The test should involve the following interoperability scenarios:

| <u>Client (init)</u> | <u>KDC</u> | <u>Resource</u> | <u>Mode/Trust</u> | <u>Result</u> |
|----------------------|------------|-----------------|-------------------|----------------------------|
| Win2000 | MS | Win2000 | native | successful, as expected |
| Win2000 | MS | non-W2K | one-way | login OK, ktelnet tool n/a |

General Results:

Attempt to log in to ad.Colorado.edu realm from W2K client GINA: Login is successful, captured contents of kerb cache. Attempt to browse a share on W2K server in ad.Colorado.edu is successful.

Ktelnet tool for Windows2000 not available to test access to non-W2K resource.

Testing 2b:

Repeat client (kinit, ktelnet, etc.) test matrix against MS KDC. This should specifically include running the current lab kinit (spinning key) against an MS KDC:

General Results:

The current public lab kinit/spinning key was successfully tested against the W2K KDC on both Win9.x and Mac OS. Users were able to successfully login against the Windows2000 KDC and obtain a TGT. However, without a valid method for sharing a keytab or encryption key with a UNIX based service provider, we have no way to validate a service ticket or request based on the TGT. We are researching possibilities for sharing a keytab or encryption key with a UNIX based service provider.

Next Steps:

Rerun tests with hot-fixes acquired from Microsoft. Server-side fix allows for non-hierarchical referrals from one realm to another. This apparently fixes problems with authenticating to both an MIT and W2K realm. Client-side fix may allow W2K client to use TGT from the non-W2K (MIT) KDC.