z/OS V1R13

Network Authentication Services: Kerberos RFC 4537

Session objectives

- Describe new function and value of new support
- Overview of how function is implemented and how it can be exploited
- List considerations when implementing support

Overview

- **Application client and server encryption type negotiation for more secure communication.**
- Problem Statement / Need Addressed
  - KDC selects encryption type for application client and server based on encryption types set in the configuration file and settings of individual principals
  - Client and/or Server will use a weak encryption type selected by the KDC when they support a stronger encryption type
- Solution
  - Allow application client and server to negotiate an encryption type independent of KDC and configuration file and principal settings
- Benefit / Value
  - Higher level of security in communication between application client and server

Usage and invocation

- All existing applications making calls to gss_accept_sec_context and krb5_mk_req with **mutual authentication** will drive the new function
- There are no required changes to function calls or the krb5.conf file.

Interactions and dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - Any application that uses mutual authentication within Kerberos (including Kerberos Mechanism of GSSAPI)

Migration and coexistence considerations

- None

Installation

- None

Session summary

- Describe new function and value of new support
- Overview of how function is implemented and how it can be exploited
- List considerations when implementing support

Appendix - References

- Network Authentication Service Administration (SC24-5926)
- Network Authentication Service Programming (SC24-5927)
- RFC4120 – The Kerberos Network Authentication Service (V5)
- RFC4537 – Kerberos Cryptosystem Negotiation Extension