Kerberos Working Group

Reorganizing Kerberos Extensions

Sam Hartman
Tom Yu

Alternative for Kerberos Extensions Document

- Tom Yu produced draft-yu-krb-wg-kerberos-extensions-00
  .
- Alternate document structure to consider for Extensions
- Ideally his draft describes the same wire protocol.

Motivation for New Structure

- Clarifications is both too verbose and too hard to understand.
- Content is duplicated between section 3 and section 5.

Goals of Document Structure

- Give document good hierarchical reorganization.
- Put semantics in one place.
- Integrate semantics and message definitions.
- Remove implementation-specific detail.

Accomplishing these Goals

- Move all the overview material to the beginning
- before message descriptions.

- Treat the TGS and AS request as specializations
- of the more general KDC request.

- Describe Kerberos in terms of the ASN.1 types.

New Layout

- Overview
- Basic Concepts
- Individual sections for Three Protocols of Kerberos

Description of Overview

- Trusted Third Party Authentication
- Identify parties in Kerberos exchanges
- Briefly describe three protocols of Kerberos

Basic Concepts of Kerberos

- ASN.1 Usage
- Principals
- Encrypted Data
- Tickets

Three Protocols of Kerberos

- Credentials Acquisition
- Application Authentication
- Session Key Usage

Credentials Acquisition

- Describe common elements of KDC request handling.
- Better discussion of keys used in the request
- Clear up time handling.

Missing from Document

- Most discussion of naming issues
- Discussion of transport
- Instances of the typed holes
- Empty sections

Questions for Working Group

- Is this structure easier to understand than clarifications?
- How should we choose which structure to adopt?