Kerberos Working Group

A Framework for Preauthentication

Sam Hartman

Problems of Current Preauth

- Behavior of multiple mechanisms unspecified
- Many mechanisms reinvent encrypted timestamp
- Need for multiple mechanisms at once

Needs for Multiple Mechanisms

- SAM could benefit from anonymous DH
- Anonymous DH needs to authenticate the client
- Extra TGT should avoid encrypted timestamp

Goals of Preauth Framework

- Describe how mechanisms interact with each other.
- Reuse components.
- Avoid additional dependence on encrypted timestamp.
- Simplify Security Analysis.

Making Framework Implementable

- Work with existing preauth mechanisms.
- Work with base Kerberos protocol.
- Provide useful utilities for future mechanisms.

How Framework Works

- Breaks preauth into phases.
- Feeds state of each preauth mechanism int next.
- Defines requirements for common facilities.

Facilities a Preauth May Provide

- Client Authentication
- Key replacement/strengthening
- Verification of responses

Questions for WG

- Should we continue to develop the framework?
- Should this be a working group item?