Kerberos Preauth Framework

Sam Hartman
Larry Zhu
IETF68

Introduction

- A brief history of the preauth-framework

What is Kerb Fast

- Protected Channel for pre-authentication
- Simplify pre-authentication design

Client Name Hiding

- Fast option to hide client identity to attackers

Referrals

- Fast option for the KDC to chase down referrals

More Preauth Required Error

- KDC_ERR_MORE_PREAUTH_DATA_NEEDED
- It is a new error code

Pre-authentication Set

- Decomposition of containers in the set
- Checksum of container
- Set not changed as authentication progresses

Pa-hint and Initial Challenges

- What if you have a padata type as the first member of a set that requires a challenge
- the pa-hints need to be sufficient that you can determine what information you will require from a user ahead of time we can simplify the UI for login

KDC State Management

- Stateless cookie
- replays

Key-based Armors

- Are shared long-term keys appropriate for associations between a client implementation and the KDC to protect pre-auth?

Error Msg and Krb Fast

- The current text causes errors unrelated to pre-auth to suddenly be expected to have typed data simply because FAST was used in one direction