Preauth Framework

Sam Hartman
Painless security
IETF75
Minor LC issues on Pre-auth Framework

• Unspecified error for unknown armor (Sam)
• Minor editorial issues (Greg, Larry)
• Explain origin of Encrypted Challenge name (Greg)
• Appendix A: DES random to key (Tom)
Complicated Pre-auth Framework Issues

- Client Verification of KDC reply (Love)
- Ap-req armor and TGS (Sam)
Client verification of KDC reply

• Issue: Wording surrounding "Whether the contents of the KDC reply can be verified by the client principal"

• Resolution: Remove principal, clarify in text
Explicit Ap-Req Armor for TGS

• Issue: Implementation experience suggested explicit TGS armor is hard to use. Security problems were found because the inner request is not bound to the outer request.

• Resolution:
  – Remove explicit tgs-req armor
  – Note that tgs-req armor MUST authenticate the client to the KDC
  – Require strengthenReply key