Web/GSSAPI Integration

Doug Rosenthal

EINet Corporation

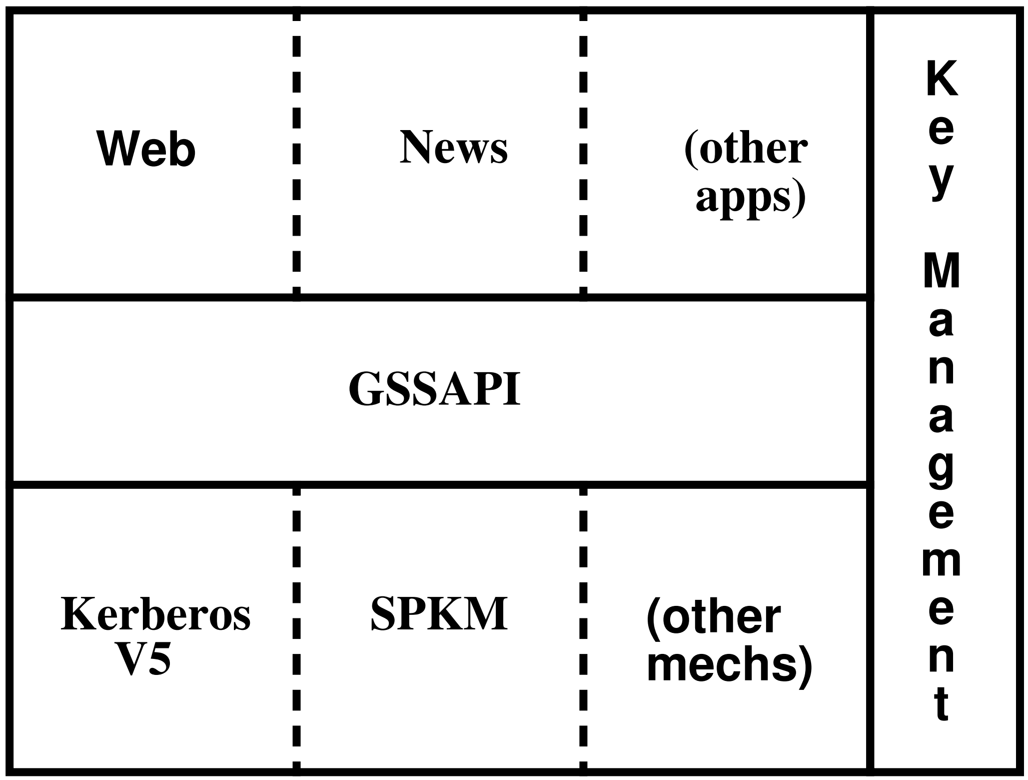
(rosenthal@einet.net)

GSSAPI Overview

- IETF standard activity since 1991
- Application-independent
- Security mechanism-independent (public key, Kerberos)
- Supported security services:
  - User/service authentication
  - Various strengths of data confidentiality and integrity
  - Digital signatures (public key implementations)

GSSAPI Overview

- Proposed support for run-time mechanism negotiation
- Proposed support for off-line message/file security (IDUP-GSSAPI)
  - Consistent security APIs for session-oriented and store-and-forward applications
  - Enables single credentials to be used for both types of applications


Web
News
(other apps)
GSSAPI
Kerberos V5
SPKM
(other mechs)
Key Management

Web Integration

- Proposed new URL type: gss-http
  - GSS mechanism negotiation, authentication, and key establishment performed at connect-time
- Use URL to identify target service for authentication
  - URL->DN, or URL->Kerberos principal
- Protect entire transaction
  - Client requests and server responses, including form submission

Status

- Integrating GSSAPI with winWeb and macWeb browsers, and NCSA httpd server
- Using GSSAPI/SPKM toolkit from Northern Telecom (Entrust)
- Will pilot with EINet CA services (also based on Entrust)
- Augmenting with access control based on authenticated user IDs
- Preparing Internet-Draft specification