Kerberos and KINK

Kerberos-clarifications
and RFC 3961

Changes from RFC 1510

- Crypto split out, treated as black box
- Fixed some bugs, refined ASN.1
  - Compatible with existing implementations
- Some updates like TCP and DNS SRV support

Changes from RFC 1510

- Added extensibility hooks more than extensions
  - no PFS (yet)
- NOT kerberos-revisions
  - no KRB-ERROR checksum (yet)
- draft-yu-krb-wg-kerberos-extensions-02.txt

Kerberos crypto (RFC 3961)

- Black box
- Simple(?) operations and attributes
- Don't make extra assumptions

Encryption systems

- Key generation for Kerberos
- Mandatory checksum type
  - Must be available if this encryption type is used, not required to be the only one used
- PRF(key, octet-string) -> octet-string
  - Arbitrary input string
  - Specific size output
  - If not big enough, make multiple calls

Encryption systems

- Encrypt with integrity protection
  - “authenticated encryption”
  - treated as inseparable
  - not deterministic or fixed-length
- Decrypt with verification
  - may leave trailing padding bytes, I mean octets

“Checksum” systems

- MAC, not simple hash function
- Generate and Verify operations
- Need not be deterministic
- Need not be fixed-length (but < 64K)