

# SPNEGO ISSUES

- ◆ RFC 2478 – Simple and Protected GSS-API Negotiation Mechanism
  - ▶ Baize, Pinkas, Bull – December 1998
- ◆ OID 1.3.6.5.5.2
- ◆ Negotiates “real” GSS-API security mechanisms
- ◆ Implemented as a standard GSS-API “pseudo-mechanism”
  - ▶ Callers need not be aware that SPNEGO is being used.
  - ▶ Applications code to GSS-API, not SPNEGO

# SPNEGO SPEC. ISSUES

- ◆ Encoding is not specified (DER? BER?)
- ◆ Tagging – Explicit or Implicit?
- ◆ MechListMIC
  - ▶ Only covers mechlist, does not include any other fields – should it?
- ◆ Extensibility concerns
- ◆ Incomplete ASN.1 section

# Implementation Issues

- ◆ MS Implementation is broken and cannot be fixed in a backwards compatible manner
  - ▶ MechListMIC field is not a MIC. It is a copy of the responseToken field.
  - ▶ Incorrect Kerberos Mechanism OID used
    - ◆ 1.2.840.48018.1.2.2
    - ◆ (possibly fixed by recent Service Packs)
- ◆ client apps ignore the MechListMIC field in NegTokenTarg
  - ▶ sequence numbering to become out of sync
  - ▶ server called `get_mic`, thus incrementing seq #, client ignores it, making seq #s become out of sync

# Workarounds

- ◆ Don't create or send MechListMIC fields when talking to SSPI Negotiate apps.
  - ▶ Not secure – Becomes SNEGO
- ◆ Servers (GSS/SPNEGO Acceptor) must know apriori that it is talking to a non-compliant client in order to succeed.
- ◆ Impossible to interoperate with both broken and correct implementations at the same time.

# How to Fix It?

- ◆ “Flag Day” for everyone ?
- ◆ Define a new OID for “CORRECT” SPNEGO implementors to use.
  - ▶ Broken implementations must continue to use current OID
  - ▶ Acceptors can make decisions on how to interpret the tokens dynamically based on OIDs.