Kitten: Common Authentication Technologies Next Generation

IETF 60

Introduction

Introduction

- Four years since CAT closed
- Wide deployment have revealed RFCs 2743 (GSSAPI v2) and 2744 (C Bindings) to be less well-defined then they could be and are missing necessary functionality:
  - Credentials Management
  - Thread safety
  - Channel Bindings usability
  - ABI stability
  - Mechanism specific extensibility
  - Support for mechanisms without a single canonical name

Introduction (2)

- GSS SPNEGO (RFC 2748) is flawed. It is not possible to create interoperable implementations
- Channel Bindings must be defined to support cryptographic channels such as TLS, IPSec, SSH
- A new GSS mechanism to negotiate channel bindings must be defined
- Language Bindings for C# are desired

Agenda

Agenda

- Introduction and Welcome [5 minutes]
- Global Grid Forum GSS requirements [15 minutes] - Doug Engert
- Channel bindings portability issues [2 minutes] - Sam Hartman
- GSSAPI naming [10 minutes] - Sam Hartman
- Need for cryptographic channel bindings and CCM [20 minutes] - Nicolas Williams
- Stackable Psuedo Mechanisms [15 minutes] - Nicolas Williams
- GSSAPI SPNEGO issues [10 minutes] - Wyllys Ingersol
- C# Bindings for GSSAPI [10 minutes] – J.K.
- Kitten Working Group Charter discussion

Charter Discussion

Proposed Charter (1)

- The Generic Security Services API [RFC 2743, RFC 2744] provides an API for applications to set up security contexts and to use these contexts for per-message protection services. The Common Authentication Technology Next Generation Working Group (Kitten) will work on standardizing extensions and improvements to the core GSSAPI specification and language bindings that the IETF believes are necessary based on experience using GSSAPI over the last 10 years. Extensions may be published as separate drafts or included in a GSSAPI version 3. While version 2 of the GSSAPI may be clarified, no backward incompatible changes will be made to this version of the API.

Proposed Charter (2)

- This working group is chartered to revise the GSSAPI v2 RFCs for the purpose of clarifying areas of ambiguity:
  - Use of channel bindings
  - Thread safety restrictions
  - C Language utilization
    - use of const
    - utilization of gss types by the application
    - gss name space
    - Improve recommendations for implementation specific types (e.g., use pointers to incomplete structs)
  - Guidelines for GSS-API mechanism designers
  - Guidelines for GSS-API application protocol designers

Proposed Charter (3a)

- This working group is chartered to specify a non-backward compatible GSSAPI v3 to support the following extensions:
  - Clarify the portable use of channel bindings and better specify channel bindings in a language-independent manner.
  - Specify thread safety extensions to allow multi-threaded applications to use GSSAPI
  - Definitions of channel bindings for TLS, IPSec, SSH and other cryptographic channels based on work started in the NFSV4 working group.

Proposed Charter (3b)

- Defined a GSSAPI extension to allow applications to store credentials.
- Extensions to solve problems posed by the Global Grid Forum's GSSAPI extensions document.
- Extensions to deal with mechanism-specific extensibility in a multi-mechanism environment.
- Extend GSSAPI to support mechanisms that do not have a single canonical name for each authentication identity.
- Extensions to support stackable GSSAPI mechanisms.

Proposed Charter (4)

- This working group is chartered to perform the following GSSAPI mechanism specification work:
  - Specify a GSSAPI v2/v3 Channel Conjunction Mechanism
  - Revise RFC 2748 (SPNEGO) to correct problems that make the specification unimplementable and to document the problems found in widely-deployed attempts to implement this spec.

Proposed Charter (5)

- This working group is chartered to perform the following new GSSAPI Language Binding specification work:
  - Specify a language binding for C#

Milestones (1)

Either:

- Clarifications to GSSAPIv2 (six months to IESG)

  Informational

  [editor: TBD]

Or:

- Generic Security Service Application Program Interface Version 2, Update 2 (six months to IESG)

  Proposed Standard

  [editor: TBD]
- Generic Security Service API Version 2 : C-bindings (six months to IESG)

  Proposed Standard

  [editor: TBD]

Milestones (2)

- The Channel Conjunction Mechanism (CCM) for the GSSAPI (six months to IESG)

  Proposed Standard

  [editors: Nicolas Williams/Mike Eisler]
- On the Use of Channel Bindings to Secure Channels (six months to IESG)

  Proposed Standard

  [editor: Nicolas Williams]

  draft-ietf-nfsv4-channel-bindings-01.txt
- GSSAPIv3 (18 months to IESG)

  Proposed Standard

  [editor: to be determined]

Milestones (3)

- Stackable Generic Security Service Pseudo-mechanisms
  Proposed Standard or to be folded into GSSAPIv3
  [editor: Nicolas Williams]
  draft-williams-gssapi-stackable-pseudo-mechs-00.txt
- GSS-APIv2 Extension for Storing Delegated Credentials
  Proposed Standard or to be folded into GSSAPIv3
  [editor: Nicolas Williams]
  draft-williams-gssapi-store-deleg-creds-00.txt
- GSSAPI Mechanisms without a Single Canonical Name (12 months to IESG)
  to be folded into GSSAPIv3
  [editor: Sam Hartman]
  draft-hartman-gss-naming-00.txt

Milestones (4)

- SPNEGO (RFC 2478) Revisions (18 months to IESG)

  Proposed Standard

  [editor: TBD]
- C# Bindings for GSSAPI (12 months to IESG)

  Proposed Standard

  [editor: Larry Zhu]

Mailing List

The current mailing list for discussions is

ietf-cat-wg@lists.stanford.edu.
Ietf-cat-wg-request@lists.stanford.edu

Due to the facts that no one at Stanford is actively involved in the discussions and the mailing list software is quite old, the working group when formed will switch to a new mailing list hosted by ietf.org

Discussion

Thank you for attending