74th IETF

Kerberos Working Group

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- the IETF plenary session,
- any IETF working group or portion thereof,
- the IESG or any member thereof on behalf of the IESG,
- the IAB or any member thereof on behalf of the IAB,
- any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices,
- the RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 3978 (updated by RFC 4748) and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 3978 (and RFC 4748) for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Kerberos Working Group Introduction

- Web Page: http://tools.ietf.org/wg/krb-wg/

- Mailing List: ietf-krb-wg@anl.gov
  - Archives: ftp://ftp.ietf.org/ietf-mail-archive/krb-wg/
  - To Subscribe: https://lists.anl.gov/mailman/listinfo/ietf-krb-wg

Kerberos Working Group
Meeting Participation

□ Audio:	http://tinyurl.com/ietf74-krb-audio
□ Jabber:	krb-wg@jabber.ietf.org
□ Materials:	http://tinyurl.com/ietf74-krb-slides

Please Use The Mic!

Kerberos Working Group
Agenda

□ Preliminaries (5 min)
□ Document Status (5 min)
□ Last Call (5 min)
□ Proposed work (10 min)
□ Technical Discussion (75 min)
□ Open Mic (whatever is left)

Kerberos Working Group
Document Status

- STARTTLS
  - draft-josefsson-kerberos5-starttls-06.txt
  - draft-josefsson-krb5starttls-bootstrap-02.txt
  - Discussion in progress on mailing list

Kerberos Working Group
Last Call

- Data Model
  - draft-ietf-krb-wg-kdc-model-03.txt
  - Last call to start today
- IAKERB
  - draft-ietf-krb-wg-iakerb-01.txt
  - Last call Nov-Dec 2008
  - One LC comment

Kerberos Working Group
Proposed Work

- Ticket Extensions
  - draft-lha-krb-wg-ticket-extensions-03.txt
- DHCP Option
  - draft-sakane-dhc-dhcpv6-kdc-option-04.txt

Kerberos Working Group Technical Discussion

- RFC3961 PRF problems
- Preauth Framework
  - draft-ietf-krb-wg-preauth-framework-10

Kerberos Working Group
PRF Problems - Background

- Simplified Profile Parameters (RFC3961 §5.2):
  - H: Unkeyed hash algorithm
  - E: Encryption function
  - m: message block size (smallest message size E can handle)

- AES128-CTS-HMAC-SHA1-96 (RFC3962 §6):
  - H = SHA-1
  - E = AES in CBC-CTS mode
  - m = 1 octet

Kerberos Working Group
PRF Problems - RFC3961 PRF

- PRF from RFC3961 §5.3:

```
tmp1 = H(octet-string)
tmp2 = truncate tmp1 to multiple of m
PRF = E(DK(protocol-key, prfconstant),
        tmp2, initial-cipher-state)
DK is defined in RFC3961 §5.1
```

Kerberos Working Group
PRF Problems - MIT_AES_PRF

- Proposed new PRF:

```
tmp1 = H(octet-string)
tmp2 = truncate tmp1 to cipher block size
PRF = E(DK(protocol-key, prfconstant),
        tmp2, initial-cipher-state)
DK is defined in RFC3961 §5.1
```

- New Profile Parameter:
  - b: Preferred cipher block size

Kerberos Working Group
Technical Discussion

- RFC3961 PRF problems
- Preauth Framework
  - draft-ietf-krb-wg-preauth-framework-10

Kerberos Working Group

Open Mic