HIP-RG meeting
IETF 79

November 9, 2010

Andrei Gurtov and Tom Henderson
{gurtov@hiit.fi, thomas.r.henderson@boeing.com}

What is HIP?

- A proposal to use public keys as names for Internet stacks, and to use these names within the TCP/IP architecture
  - Please see RFC 4423 for an overview of the HIP architecture
  - Please see RFC 5201-5206 for specifications
  - WG is rechartered to produce standard-track HIP specifications

- What is the difference between the HIP WG and the HIP RG?

HIP RG administrative overview

- Mailing list:
  - http://www.irtf.org/mailman/listinfo/hiprg
- Supplemental web page (wiki):
  - http://trac.tools.ietf.org/group/irtf/trac/wiki/hiprg
- HIPRG charter
  - Evaluate benefit/impact of deploying HIP
  - Experiment with HIP software
  - Analyze HIP in context of real networks
  - Prepare report to IESG
  - Work on 4 other RG items

Snapshot of IRTF-based wiki

Software sites

- Three public implementations of HIP available:
  - HIPL (HIP for Linux) (Helsinki HIIT)
    - http://infrahip.hiit.fi
  - HIP4BSD (Ericsson NomadicLab)
    - http://hip4inter.net
  - OpenHIP
    - http://www.openhip.org
- Three test servers:
  - http://hipserver.mct.phantomworks.org
  - http://woodstock{4|6}.hip4inter.net
  - http://crossroads.infrahip.net

HIP research group

Agenda

1. Andrei Gurtov. Status of HIPRG work items and their further progress [15 min]
2. Gyu Myoung Lee. Update on HIP RFID. [30 min]

3. Dacheng Zhang. Updates on key revocation [30 min]
   Proxies
   Hierarchical HITs

4. Tobias Heer. A Certificate-based Namespace for HIP [30 min]
   Update on HIPL implementation
   Status of HIP WLAN deployment project

5. Jani Pellikka. Certificate request mechanism [15 min]

6. Jani Pellikka. Comparison and Analysis of Secure Mobile Architecture and Evolved Packet System [20 min]

7. General discussion [10 min]

Research Group drafts

- RFC 5743 published in December 2009

```
Internet Research Task Force (IRTF)                          A. Falk
Request for Comments: 5743                                      IRTF
Category: Informational                               December 2009
ISSN: 2070-1721


       Definition of an Internet Research Task Force (IRTF) Document Stream

Abstract

   This memo defines the publication stream for RFCs from the Internet
   Research Task Force.  Most documents undergoing this process will
   come from IRTF Research Groups, and it is expected that they will be
   published as Informational or Experimental RFCs by the RFC Editor.

Status of this Memo

   This document is not an Internet Standards Track specification; it is
   published for informational purposes.
```

- Details on the document process are available at:

  http://trac.tools.ietf.org/group/irtf/trac/wiki/IRTF-RFCs

RG draft status

- **draft-irtf-hip-experiment-09.txt**
  - New version taking Dacheng and Miika's feedback
  - Tom plans to update soon
- **draft-irtf-hiprg-dht-02.txt**
  - Reviewed, updated, requesting publication
- **draft-irtf-hiprg-proxies-01.txt**
  - Reviewed by Tom
- **draft-irtf-hiprg-revocation-01.txt**
  - Reviewed by Hamid, Tom
- **draft-irtf-hiprg-rfid-01.txt**
  - Will be posted soon
  - -00 has been reviewed by T. Heer et al

HIP research group

Meeting goals

- Survey the progress on RG items
  - What is blocking each draft from publication?

- Final comments on mature drafts
  - DHT
  - Experiment report

- Introduce new drafts
  - Certificate request

RG draft status

New drafts since last meeting:

- **draft-pellikka-hiprg-certreq-00 (TBD)**

Updated drafts since last meeting:

- **draft-irtf-hip-experiment-09.txt**
- **draft-irtf-hiprg-dht-02.txt**
- **draft-irtf-hiprg-proxies-01.txt**
- **draft-irtf-hiprg-revocation-01.txt**
- **draft-irtf-hiprg-rfid-01.txt (TBD)**
- **draft-xu-hip-hierarchical-01.txt**

HIP in UFA

- New and supposedly interesting HIP related articles in the area of distributed mobility management and flat network architectures:

- Evaluation and Comparison of Signaling Protocol Alternatives for the Ultra Flat Architecture http://www.mcl.hu/~goodzi/Evaluation_and_Comparison_of_Signaling_Protocol_Alternatives_for_the_Ultra_Flat_Architecture_ICSNC2010.pdf

- A Delegation-based HIP Signaling Scheme for the Ultra Flat Architecture http://www.mcl.hu/~goodzi/A_Delegation-based_HIP_Signaling_Scheme_for_the_Ultra_Flat_Architecture_IWSCN2010.pdf

802.15 HIP Interest Group (IG)

- Started in July by Robert Moskowitz

- Working on HIP as a key management system for 802.15

- For further information, one can subscribe here: http://grouper.ieee.org/groups/802/15/pub/Subscribe.html

Relevant BOFs

- Name-based sockets BOF
  - Took place on Monday morning
  - Potential upgrades with HIP to provide security?

- Internet-of-things barBOF
  - Scheduled for Wed evening?
  - Potential links to RFID and Diet-HIP