HIP-RG meeting
IETF 82

November 17, 2011

Andrei Gurtov and Tom Henderson
{gurtov@ee.oulu.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
  - Also RFCs 5338,6079,6253,6078,5770,6317,6261, 6028
  - 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 topics not yet ready for standardization

Snapshot of IRTF-based wiki

IETF TOOLS

IETF Home
About Tools
Tools:
diffs spell
xml2rfc idnits
tracker src
News
Get Passwd
IETF-82:
Rooms
Agenda
Calendar
Documents
RFCs
Doc fetch:

Wikis:
IESG IRTF
IAOC RSOC
Chairs Edu
Tools BOFs
Development
NomCom
Areas
WGs:
concluded...
6lowpan
6man*
6renum
Abfab
Adslmib
Alto*
Ancp
Appsawg
Armd
Atoca
Autoconf
Awtcore*
Awtext

IRTF

Search

Login | Help/Guide | About Trac | Preferences

Wiki | Timeline | Roadmap | Browse Source | View Tickets | Search

wiki: hiprg

Start Page | Index | History

Host Identity Protocol Research Group (HIPRG)

⇨HIPRG homepage & charter

⇨Mailing list

Next Meeting

- planning for IETF 82, Taipei. Please contact Andrei Gurtov for any agenda requests.

Last Meeting

⇨IETF 81, Thursday July 29, 0900-1130, Room 202

- ⇨Meeting materials

Active Documents

The following are being worked on as ⇨IRTF stream documents.

Draft name	Draft title	Status
⇨draft-irtf-hiprg-dht-04.txt	HIP DHT Interface	⇨Awaiting IRSG review
⇨draft-irtf-hip-experiment-13.txt	HIP Experiment Report	⇨Awaiting IRSG review
⇨draft-irtf-hiprg-revocation-03.txt	Host Identifier Revocation in HIP	Updated July 2011
⇨draft-irtf-hiprg-proxies-03.txt	Investigation in HIP Proxies	Updated July 2011
⇨draft-irtf-hiprg-rfid-03.txt	HIP support for RFID	Updated July 2011

Other documents for discussion at IETF 80:

Draft name	Draft title
⇨draft-moskowitz-hip-rg-dex-05.txt	HIP Diet EXchange (DEX)
⇨draft-cao-hiprg-flow-mobility-00.txt	HIP Flow Mobility
⇨draft-cao-hiprg-legacy-host-00.txt	Communication between a HIP-enabled Host and a Legacy Host
⇨draft-kuptsov-hhit-02.txt	Hierarchical Host Identity Tags
⇨draft-pellikka-hiprg-certreq.txt	HIP Certificate Requests

Software sites

- Three public implementations of HIP available:
  - HIPL (HIP for Linux) (Helsinki HIIT/RWTH Aachen)
    - http://infrahip.hiit.fi (Version 1.0.6 released!)
  - HIP4BSD (Ericsson NomadicLab)
    - http://hip4inter.net
  - OpenHIP (Boeing)
    - http://www.openhip.org (Version 0.8 released!)
- Three test servers:
  - http://hipserver.mct.phantomworks.org
  - http://woodstock{4|6}.hip4inter.net
  - http://crossroads.infrahip.net

Agenda

THURSDAY, November 17, 2011

0900-1130 Morning Session I

Andrei Gurtov/CWC. Sign Sheets. HIPRG Status update (10 m)

Bob Moskowitz/Verizon. IEEE 802.15.HIP update (30 m)

Laszlo BOKOR/BME-HIT. Proactive mobility management for distributed/flat architectures using HIP and IEEE 802.21 protocols (30 m)

Rene Hummen/RWTH. WLAN roaming project update and draft-heer-hip-middle-auth (25 m)

Xiaohu Xu/Huawei. Hierarchical HIP and proxies updates (20 m)

Ari Keranen/Ericsson. HIP deployment study results (20 m)

Gyu Lee/Telecom SudParis. HIP support for RFIDs. draft-irtf-hiprg-rfid-04 (15 m)

Open Mic, future discussions

Andrei Gurtov/CWC mHIP vs MPTCP (if time permits)

Research Group draft guidelines

- RFC 5743 published in December 2009

Internet Research Task Force (IRTF)
Request for Comments: 5743
Category: Informational
ISSN: 2070-1721

A. Falk
IRTF

December 2009

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-14.txt**
  - Passed IESG review
  - Final revision before publication
- **draft-irtf-hiprg-dht-04.txt**
  - Passed IESG review
- **draft-irtf-hiprg-proxies-04.txt**
  - Tom helps to edit
- **draft-irtf-hiprg-revocation-04.txt**
  - More reviews needed
- **draft-irtf-hiprg-rfid-04.txt**
  - Reviewed by Andrei on mailing list

Meeting goals

- Survey the progress on RG items
  - What is blocking each draft from publication?
- Updates on use cases and software releases
  - 3GPP architecture
  - IEEE
  - WLAN roaming
  - IoT
  - Multipath
- Discuss future of HIPRG
  - What should we focus on in future?

HIP DEX: **draft-moskowitz-hip-rg-dex-05**

- Perceived by some as most interesting activity in RG
  - Consider moving to WG for publication?
- Java DEX implementation from Aalto University
  - P. Nie, J. Vaha-Herttua, T. Aura and A. Gurtov, Performance Analysis of HIP Diet Exchange for WSN Security Establishment, in Proc. of 7th ACM Annual International Symposium on QoS and Security for Wireless and Mobile Networks, November 2011.
- C implementation from CWC
  - Jani Pellikka et al, paper under submission
- Fast Initial Authentication for WLAN master thesis
  - Konstantinos Georgantas. Fast Initial Authentication: a New Mechanism to Enable Fast WLAN Mobility. KTH/HIIT. 2011

RG draft status

New drafts since last meeting:

- draft-yuan-hiprg-failure-detection-recovery-02.txt
- draft-cao-hiprg-flow-mobility-01

Updated drafts since last meeting:

- **draft-irtf-hip-experiment-14.txt**
- **draft-irtf-hiprg-dht-04.txt**
- **draft-irtf-hiprg-proxies-04.txt**
- **draft-irtf-hiprg-revocation-04.txt**
- **draft-irtf-hiprg-rfid-04.txt**
- **draft-xu-hip-hierarchical-02.txt**
- **draft-pellikka-hiprg-certreq-01**
- **draft-heer-hip-middle-auth-04**

802.15 HIP Interest Group (IG)

- Started in July 2010 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
- 802.15.9 Task Group was just approved at IEEE
  - Focuses on Key Management for 802.15.4 and .7
- HIP DEX will be one candidate for KMP
  - Need to progress DEX specs
  - At IETF or at IEEE?

Testing Tofino EndBox (based on HIP)

- Pre-product release from Byres Security (Canadian Company)
- Transparent secure interconnection of legacy network devices
- Used by Boeing to protect factory SCADA systems
- Under testing in HIIT
  - Generally works well
  - Hard to configure (manual XML editing)
  - Has issues with some devices (ARP details)
- New commercial release planned soon with user-friendly GUI

Future of HIPRG

- Some pressure from IRTF chair to close RGs with insufficient activity, also HIPRG
- We have too little traffic on the mailing list
  - Please be more active in reviewing each other drafts
- What should be our future research focus?
  - Identifying topics that people from different institutions will collaborate on
- Informal discussion took place over dinner on Wed
  - Announced on the list
- Meeting in Paris IETF?
  - Or another venue meeting?