# IRTF Open Meeting

Lars Eggert

IRTF Chair

IETF-89, London, UK

# IRTF IPR Policy

**The IRTF follows the IETF Intellectual Property Rights (IPR) disclosure rules.** This is a summary of these rules as they relate to IRTF research group discussions, mailing lists and Internet Drafts:

- If you include your own or your employer's IPR in a contribution to an IRTF research group, then you must file an IPR disclosure with the IETF.

- If you recognize your own or your employer's IPR in someone else's contribution and you are participating in the discussions in the research group relating to that contribution, then you must file an IPR disclosure with the IETF. Even if you are not participating in the discussion, the IRTF still requests that you file an IPR disclosure with the IETF.

- Finally, the IRTF requests that you file an IPR disclosure with the IETF if you recognize IPR owned by others in any IRTF contribution.

**The IRTF expects that you file IPR disclosures in a timely manner, i.e., in a period measured in days or weeks, not months. The IRTF prefers that the most liberal licensing terms possible are available for IRTF Stream documents, see RFC 5743.** You may file an IPR disclosure here: http://www.ietf.org/ipr/file-disclosure

See RFC 3979 (BCP 79) for definitions of "IPR" and "contribution" and for the detailed rules (substituting "IRTF" for "IETF").

# Administrativa

- **Today's slides**
  - https://datatracker.ietf.org/meeting/89/materials.html#session.group-irtfopen
- **Remote participation**
  - https://www.ietf.org/meeting/89/remote-participation.html
- **Mailing lists**
  - http://irtf.org/mailman/listinfo/irtf-announce
  - http://irtf.org/mailman/listinfo/irtf-discuss

# IRTF Open Meeting Agenda
## Wednesday, 9:00

**9:00**   **State of the IRTF**                                      Lars Eggert
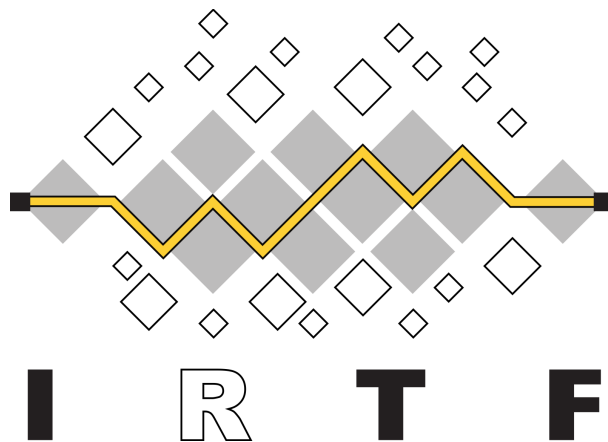
**Applied Networking Prize 2013 (ANRP) Awards**

**9:10**   **Lucky 13, BEAST, CRIME,… - Is TLS dead, or just resting?**        Kenny Paterson

**10:10**  **Stochastic Forecasts Achieve High Throughput and Low Delay over Cellular Networks**        Keith Winstein

# State of the IRTF

# IRTF Meetings This Week

**Seven RGs are meeting this week, one proposed RG is meeting**

- Information-Centric Networking (**ICNRG**)
- Crypto Forum (**CFRG**)
- Internet Congestion Control (**ICCRG**)
- Network Complexity (**NCRG**)
- Software-Defined Networking (**SDNRG**)
- Network Management (**NMRG**)
- Network Coding (**NWCRG**)
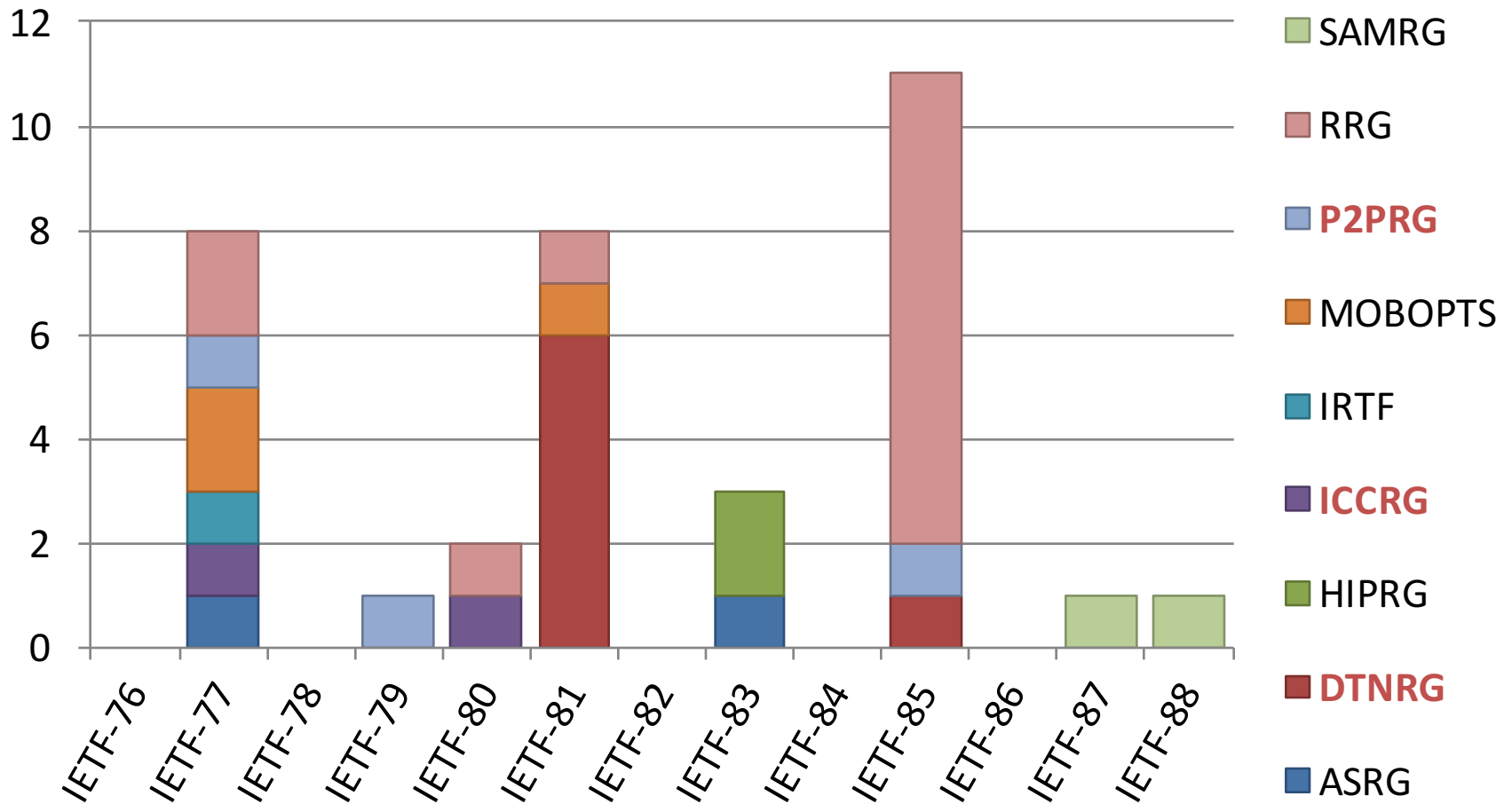- Global Access to the Internet for All (**GAIA**); Proposed RG

**Other IRTF-related meetings**

- **IRTF Open Meeting** Wednesday, 9:00
- Reviewing the **ICCRG** with the IAB on Tuesday

# Research Group Status

- **Active**
  - <u>CFRG</u>, DTNRG, SDNRG, NWCRG (new!)
- **Little activity**
  - ICCRG, ICNRG,NCRG, NMRG
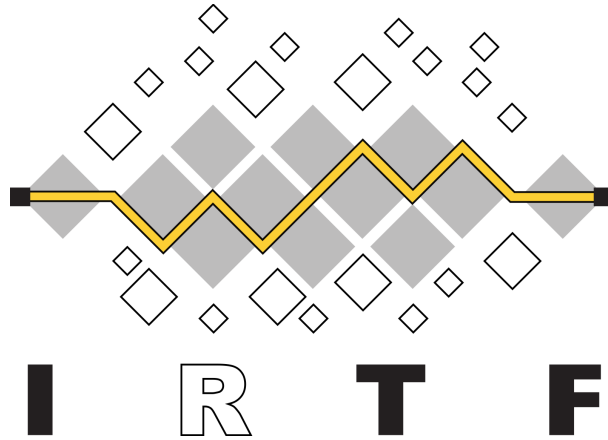- **Closing**
  - RRG (?)
- **Closed**
  - SAMRG

# IRTF Stream RFC Publications

# IRTF RFC Publications since IETF-87

- **SAMRG**

  - **RFC 7046** on A Common API for Transparent Hybrid Multicast

# CFRG Chairing Discussion & Appeal

# Timeline

**Dec 20, 2013**    Trevor Perrin emails IRTF Chair, IAB and CFRG requesting that Kevin Igoe be removed as a co-chair of the RG.

**Jan 7, 2014**    Lars Eggert responds to Trevor Perrin, rejecting the request.

**Jan 7, 2014**    Trevor Perrin appeals this decision to the IAB.

**Jan 24, 2014**    The IAB responds to Trevor Perrin, taking no action.

# Argumentation

## Trevor Perrin

1. Kevin Igoe provided the only positive feedback on the "Dragonfly" key exchange protocol.
2. Kevin Igoe made technical suggestions that would have weakened the cryptographic properties of "Dragonfly".
3. Kevin Igoe misrepresented the CFRG opinion on "Dragonfly" to the IETF's TLS working group.
4. Kevin Igoe is employed by the NSA.

## Lars Eggert

- RG process was followed imperfectly (#1-3), but not severe enough to warrant an immediate dismissal of Kevin Igoe.
- IETF and IRTF participation is by individuals.
- Chairs have little more power than other participants.
- Our best defense against subversion is an open, transparent process.
- Eliminating groups of participants solely based on their affiliations is unlikely to help.
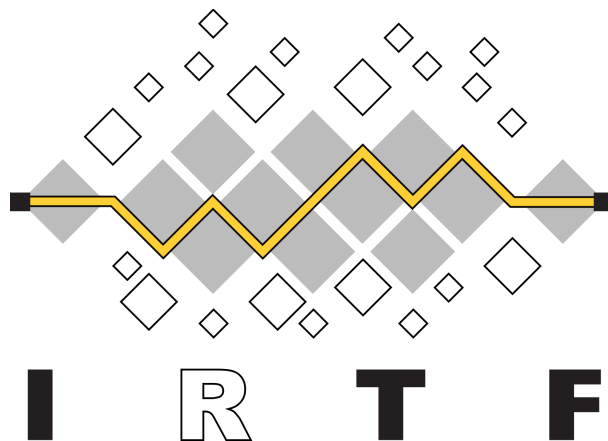
# Applied Networking Research Prize Awards & Presentations

# Applied Networking Research Prize

- Jointly with ISOC
- 46 nominations for 2014 (record!)
- Selection committee of IETF, IRTF, past winners
- Six prize winners for 2014
  - **Kenny Paterson**
  - **Keith Winstein**
  - (plus four more)
- Talks at the IRTF Open Meeting

*"…awarded for recent results in applied networking research that are relevant for transitioning into shipping Internet products and related standardization efforts…"*

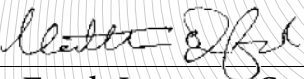Nomination period for 2015 starts in the fall!

# Applied Networking Research Prize

## Presented to

# Kenny Paterson

N. J. Al Fardan and K. G. Paterson. **Lucky Thirteen: Breaking the TLS and DTLS Record Protocols.** Proc. *IEEE Symposium on Security and Privacy*, pp. 526-540, San Francisco, CA, USA, May 2013.
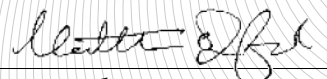
Mat Ford, Internet Society

Lars Eggert, IRTF Chair

# Applied Networking Research Prize

## Presented to

# Keith Winstein

Keith Winstein, Anirudh Sivaraman, and Hari Balakrishnan. **Stochastic Forecasts Achieve High Throughput and Low Delay over Cellular Networks.** Proc. *10th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, Lombard, IL, USA, April 2013.

_____
Mat Ford, Internet Society

_____
Lars Eggert, IRTF Chair