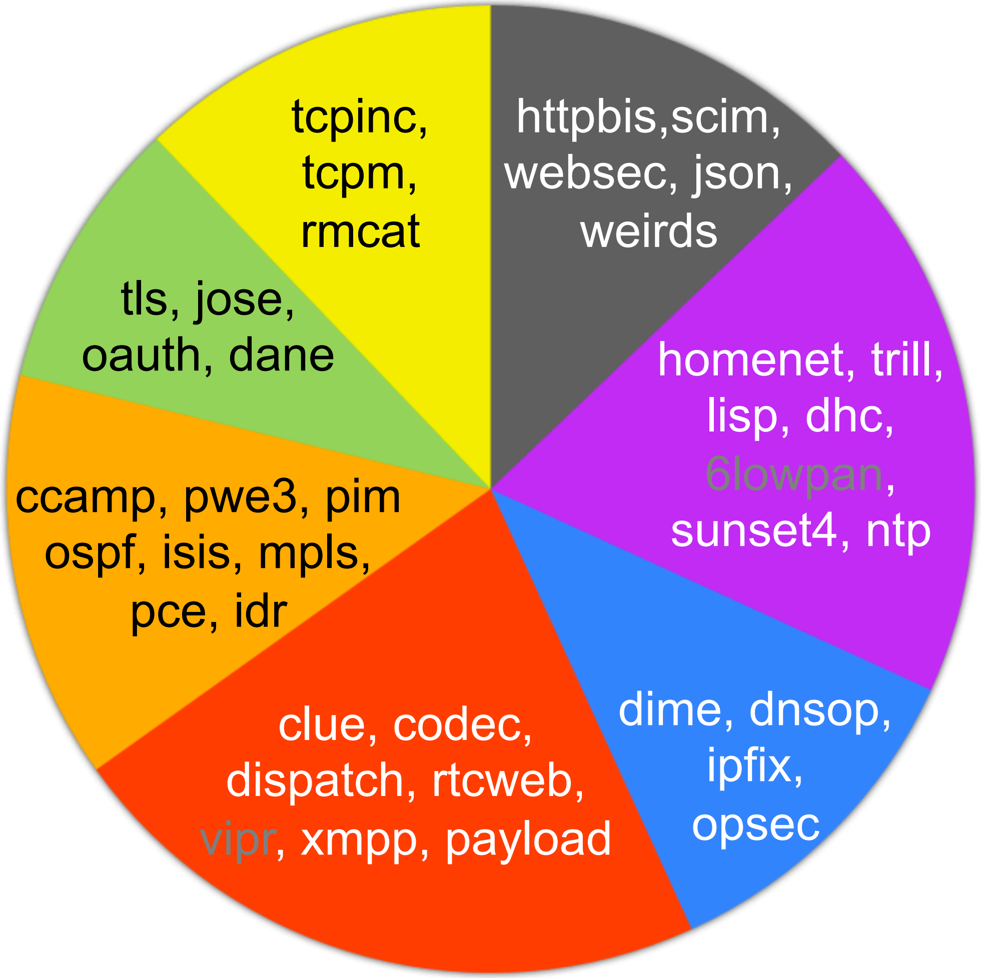
IETF Working Groups

https://datatracker.ietf.org/wg/

127 Working Groups in:

- ● Applications
- ● Transport
- ● Internet
- ● Operations and Management
- ● Real-time Applications and Infrastructure
- ● Routing
- ● Security



Mission of the IETF

Make the Internet work better by producing **high quality, relevant technical documents** that influence the way people **design, use, and manage the Internet**.

RFC3935

Ethos of the IETF

- Open standards process
  - Everyone is invited to participate at all levels
  - Our primary venue is email
  - All working and published documents are freely available online
- One Internet
  - Open standards for a global Internet
  - Maximum interoperability and scalability
  - Avoid specialized protocols in different places
- Contributions are judged on technical merits: **rough consensus and running code, RFC7282**

IETF Security Active/Recent Working Groups

Crypto

- TLS – Transport Layer Security
- IPsec – IP Security
- PKIX – Public Key Infrastructure (X.509)
- JOSE – JavaScript Object Signing and Encryption
- DANE – DNS-based Authentication of Named Entities
- UTA – Using TLS in Applications

Authentication and Authorization

- Oauth – Open Authentication
- AbFab – Application Bridging for Federated Access Beyond Web
- Kitten – Common Authentication Technology Next Generation
- HTTPAuth – HTTP Authentication
- ACE – Authentication and Authorization for Constrained Environments
- SCIM – System for Cross-Domain Identity Management (one of many security related WGs in other IETF areas)

IETF Security Active/Recent Working Groups

Security Automation and Incident Response

- SACM – Security Automation and Continuous Monitoring
- MILE – Managed Incident Lightweight Exchange
- NEA – Network Endpoint Assessment

Routing and Application

- SIDR – Secure Inter-Domain Routing
- KARP – Keying and Authentication for Routing Protocols
- WebSec – Web Security

IETF Security Internet of Things

- ACE – Authentication and Authorization for Constrained Environments
  - https://datatracker.ietf.org/wg/ace/charter/
- DICE – DTLS In Constrained Environments
  - https://datatracker.ietf.org/wg/dice/charter/
- CORE – Constrained RESTful Environments
  - https://datatracker.ietf.org/wg/core/charter/
- LWIG – Light-Weight Implementation Guidance
  - https://datatracker.ietf.org/wg/lwig/charter/

New IETF Work Related to Pervasive Monitoring (PM)

- **“Pervasive Monitoring Is an Attack”**
  - RFC7258/BCP188 published after major IETF LC debate – sets the basis for further actions
  - https://www.rfc-editor.org/rfc/rfc7258.txt
  - BCP says to consider PM in IETF work
  - Existing-RFC privacy/PM review team formed
- **Opportunistic security (OS)**
  - Provides a way to get much easier deployment for some intermediate level of security
  - Fallback to unauthenticated encrypted sessions instead of plaintext
  - https://datatracker.ietf.org/doc/draft-dukhovni-opportunistic-security/

IETF Work related to PM and Opportunistic Security

- Using TLS is Applications (UTA WG)
  - Update existing RFCs on how to use TLS in applications and mandate implementation of non-PFS ciphersuites
  - Generic BCP for TLS ciphersuites
- TLS 1.3 (TLS WG)
  - TLS 1.3 being developed aiming for better handshake performance and encryption properties
  - And learning from our history of previous TLS problems
- HTTP/2.0 (HTTPBIS WG)
  - Major deployment model: HTTP over TLS
  - Significant debate: concept of http: URIs being accessed via TLS (alt-svc), with no browser indication that crypto is happening
  - Debate on requiring server auth
- TCP Increased Security (TCPInc)
  - Provide TLS functionality within TCP
  - Support Opportunistic security with a way to hook in authentication
- DNS Privacy
  - Reducing exposure of sensitive names found in DNS
  - https://datatracker.ietf.org/doc/draft-bortzmeyer-dnsop-dns-privacy/

Emerging Work Areas

- End-to-end Security for email
  - Multiple solutions, early days, will involve much debate with emerging solutions
  - Many problems to solve
- Network Security as a Service (NSaaS)
  - Assess policies as a tenant to a service provider, automated

How Can I help?

- Participate in the volunteer-driven IETF working groups
  - Join working group mailing list, for example: MILE@ietf.org
  - Participate in an existing thread, or start a thread on any questions based on review of an existing draft, or propose work related to MILE
  - IETF-wide meetings are held three times a year, participation can be in person or remotely
- Review background information on working groups, including implementation information:
  - List of working groups: https://datatracker.ietf.org/wg/
- Contribute to open source code implementing standards
- Provide feedback on code and associated RFCs and drafts
  - Join the Privacy/PM Review team: ietf-privacy@ietf.org
  - Or submit a ticket with your review information: https://trac.tools.ietf.org/group/ppm-legacy-review/wiki

Internet Society Fellowships to the Internet Engineering Task Force (IETF)

https://www.internetsociety.org/fellowships

- ISOC Fellowships support participation in IETF meetings by technical professionals, advanced IT students, and other qualified individuals from emerging economies who would otherwise be unable to attend.
- With an open, competitive application process, the programme selects Fellows from around the world to attend in-person IETF meetings, provides a guided introduction to the IETF, and pairs Fellows with experienced mentors.
- More than 200 Fellows since 2006 have helped build a diverse, global community of participants active in Internet protocol development.
- The Internet Society provides funding and programmatic support for Fellows.

Photo © Stonehouse Photographic /Internet Society

Pictured: Internet Society Fellows to the IETF at the 83rd IETF meeting held in Paris, France on 25-30 March 2012

Internet Society Policy Programme to the Internet Engineering Task Force (IETF)

https://www.internetsociety.org/ietfpolicyprogramme

Photo © Stonehouse Photographic Internet Society

Pictured: Internet Society Public Policy Guests at the 83rd IETF meeting held in Paris, France on 25-30 March 2012

- The ISOC Policy Programme to the IETF provides policymakers and regulators first-hand experience with and insight into the Internet technical community and IETF standards setting processes.

- The programme identifies current and emerging Internet policy leaders from countries around the world, supporting their attendance at IETF in-person meetings—including conversations with IETF leadership and deep dives into specific issues of interest with technical experts.

- More than 92 Policy guests since 2012 have participated in the programme, strengthening the shared understanding of the interplay of technical and policy aspects of the Internet.

- The Internet Society provides funding and programmatic support for the policy guest programme.

IETF®

Thank You

Kathleen Moriarty
Stephen Farrell
Security Area Directors