The Internet Engineering Task Force

Security Area

Kathleen Moriarty
Stephen Farrell

Security Area Directors
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](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

- Perpass@ietf.org mailing list is used to discuss initial ideas and develop drafts or form working groups as appropriate.
IETF Work related to PM and Opportunistic Security

- **Using TLS in 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 (DPRIVE)**
  - Reducing exposure of sensitive names found in DNS
Emerging Work Areas

- End-to-end Security for email (EndyMail)
  - Multiple solutions, early days, will involve much debate with emerging solutions
  - Many problems to solve
Thank you!