IETF
Making the Internet Work Better

Алексей Мельников
alexey.melnikov@isode.com

What is this talk about?

What is IETF?

How does IETF work?

How to participate in IETF?

Overview of some interesting technical topics being worked on in IETF

Обо мне

- Закончил факультет ВМиК МГУ имени Ломоносова
- Активно участвую в IETF с 1998 года
- 47 RFC (публикаций в IETF). Руководил несколькими Рабочими Группами (Working Groups)
- Два года был Application Area Director в IETF
- Работаю в Isode Limited (www.isode.com)

Internet Engineering Task Force

- Development of open, consensus-based Internet standards

- The mission of the IETF is to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. These documents include protocol standards, best current practices, and informational documents of various kinds. [RFC 3935]

Internet Engineering Task Force

- Разработка открытых стандартов Интернета на основе консенсуса

- Миссией IETF является создание инженерно-технических спецификаций высокого качества, с помощью которых проектирование, использование и управление Интернетом делает его работу еще лучше. Эти спецификации включают стандарты протоколов, описание лучшей текущей практики, а также информационные документы различного рода. [RFC 3935]

IETF standards make the Internet work

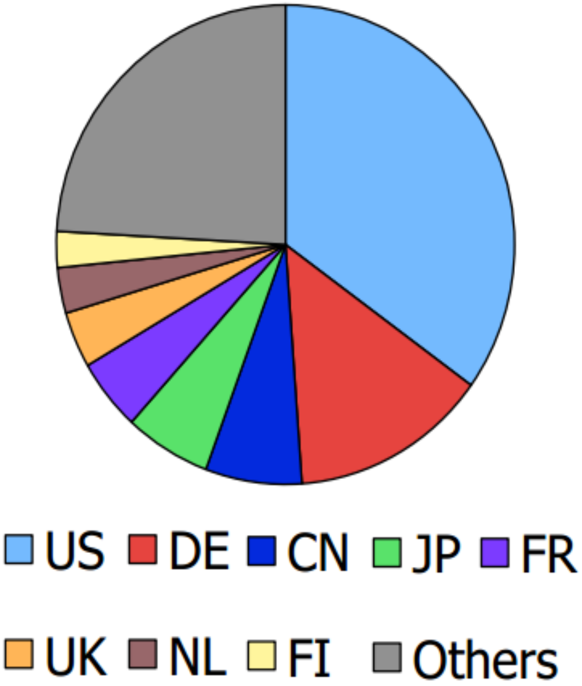
- TCP/IP
  - IPv4 (RFC791) and IPv6 (RFC2460…)
  - TCP (RFC675…) and UDP (RFC768)
- E-Mail
  - SMTP (RFC5321)
  - IMAP (RFC3501)
- Network and Routing
  - MPLS (RFC3031) and BGP (RFC4271)
- …
- DNS (RFC1034,1035…)
- DNSSEC (RFC4033-4035, …)
- Web
  - HTTP (RFC2616…)
- VoIP
  - SIP (RFC3261…) and RTP (RFC3550…)
- …

How the IETF works

- High-quality standards
  - Participants are volunteers. They serve as experts. No organizational membership.
  - Open participation and consensus based process
  - Running code
- Areas and Working Groups
  - Mailing lists with open membership
  - Most of the work is done on-line
  - 3 face-to-face meetings with remote participation
- Working specifications and standards freely available
- Maintenance responsibility
  - Standards track

IETF at a glance

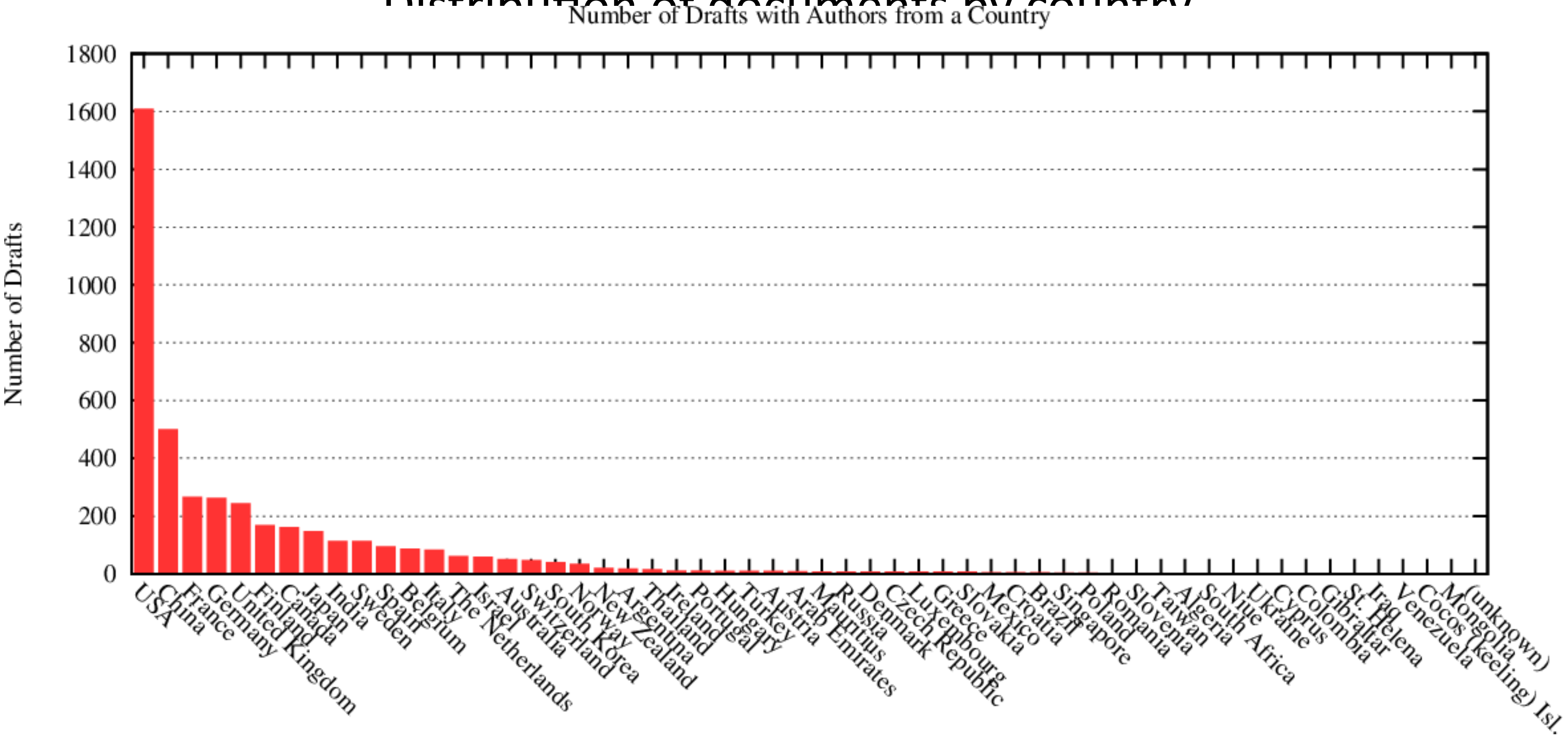
- 1000-2000 people at 3 meetings/year
  - 62 different countries represented at Berlin IETF
  - Many, many more on mailing lists
- ~120 Working Groups (WGs)
  - ~2 WG chairs each
- 8 Areas with 15 Area Directors (ADs)
- More than 7000 RFCs published
  - Internet Standards, informational and experimental documents



Participants at IETF-87
Berlin, July 2013

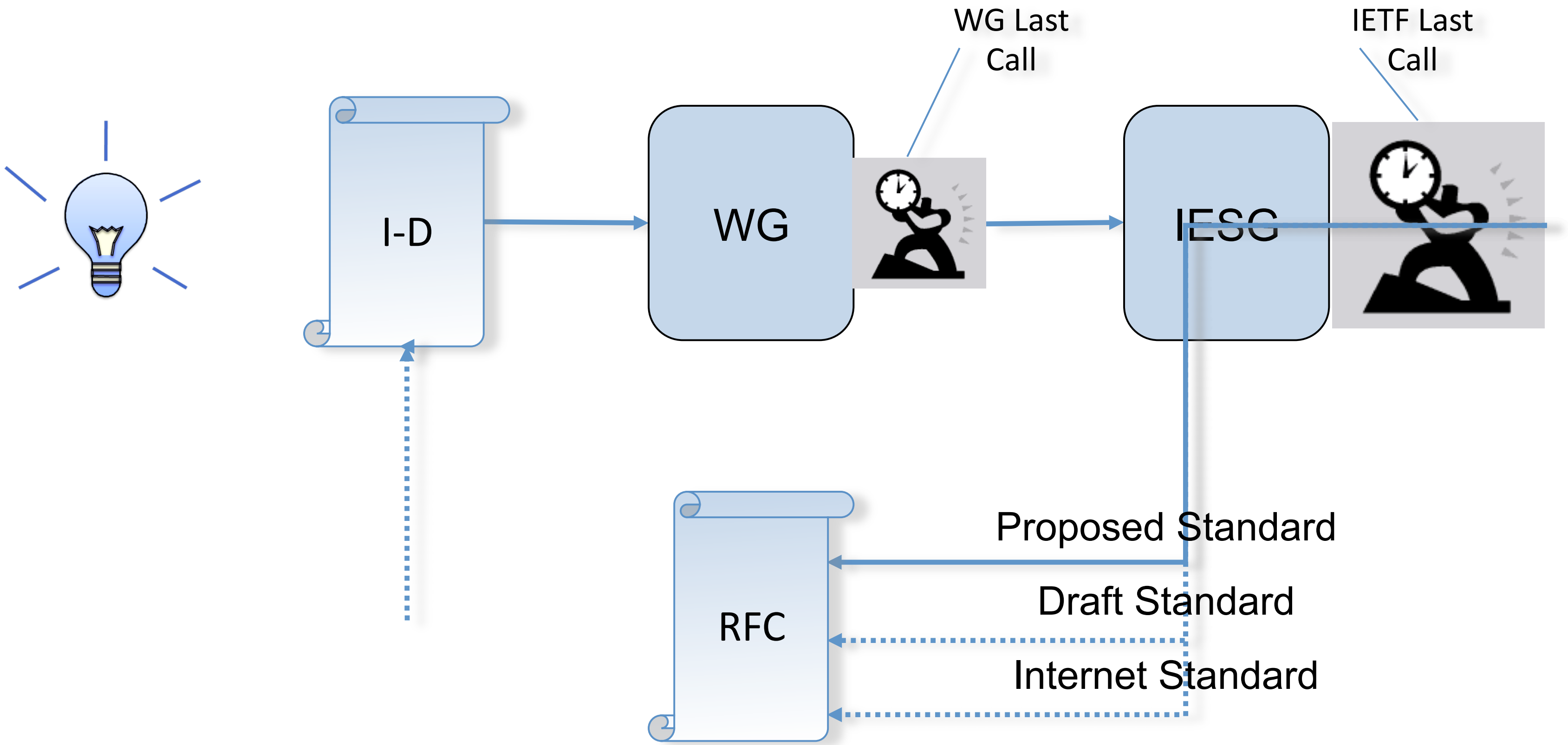
IETF by numbers: contribution

Distribution of documents by country



Source: http://www.arkko.com/

Standards process



Contributing new work (to a WG)

Check WG charters & approach chairs to ask their opinion ☑

Submit an ID (Internet Draft) to the WG ☑

- Read RFC5378 (IPR + copyright)
- draft-yourname-wgname-topic-00

Ask for feedback on ID on WG mail list ☑

Ask for time during an IETF meeting ☑

- Constructively incorporate feedback (“revise quickly, revise often”)

Eventually, ask to adopt as WG draft ☑

Continue work in WG ☑

- Note: you now become editor

Initiating new work in the IETF

Identify need

- Birds of a Feather (BOF) Session often used to demonstrate the need, a constituency, and people willing to do the work
- Compose a draft charter for the Working Group

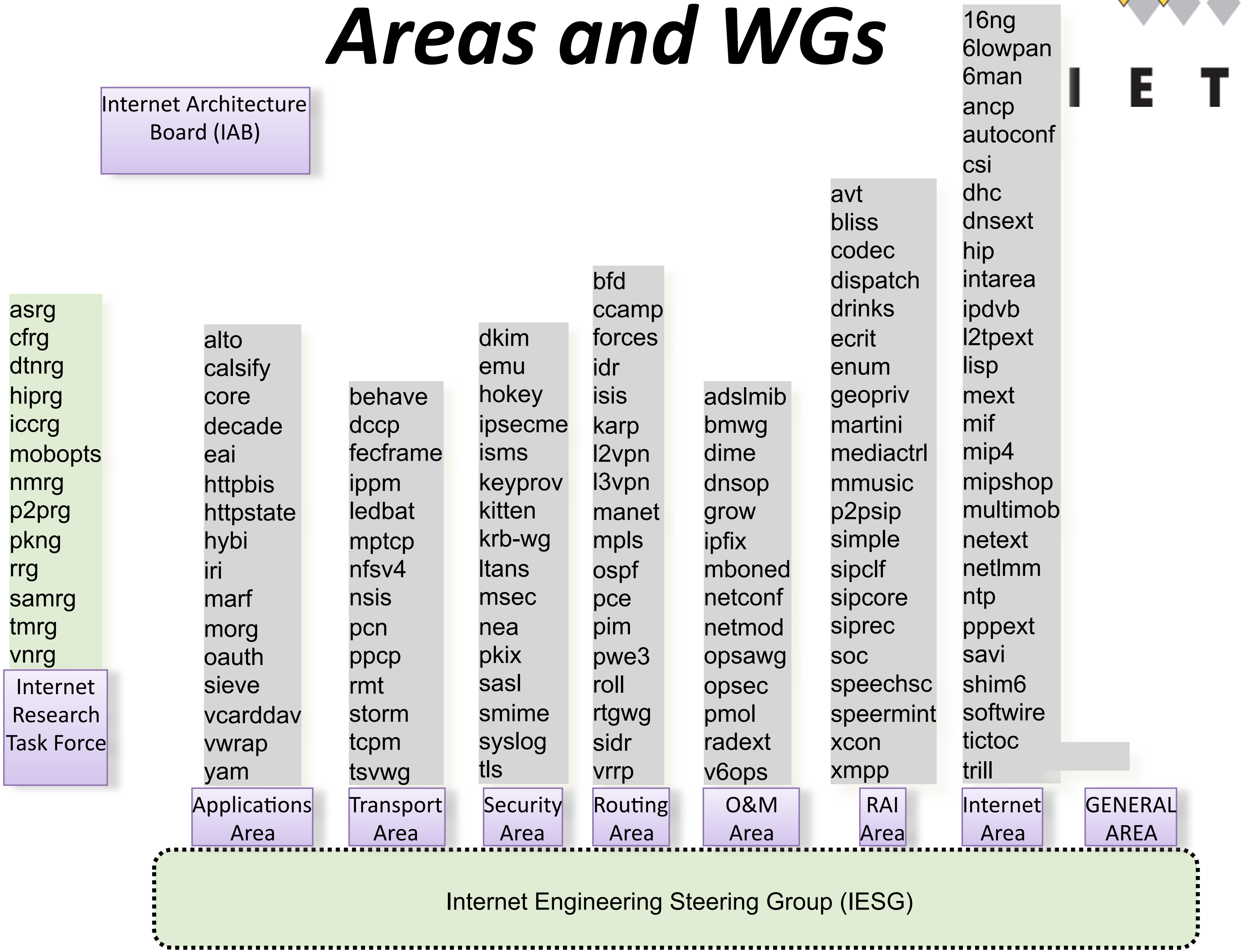
Organize Working Group

- Working Group charter approved by the IESG
- Open mail list discussions and open meetings

Organize work

- Produce documents according to the milestones

Areas and WGs



Internet Architecture Board (IAB)

Internet Research Task Force

asrg
cfrg
dtnrg
hiprg
iccrg
mobopts
nmrg
p2prg
pkng
rrg
samrg
tmrg
vnrg

Applications Area

alto
calsify
core
decade
eai
httpbis
httpstate
hybi
iri
marf
morg
oauth
sieve
vcarddav
vwrap
yam

Transport Area

behave
dccp
fecframe
ippm
ledbat
mptcp
nfsv4
nsis
pcn
ppcp
rmt
storm
tcpm
tsvwg

Security Area

dkim
emu
hokey
ipsecme
isms
keyprov
kitten
krb-wg
ltans
msec
nea
pkix
sasl
smime
syslog
tls

Routing Area

bfd
ccamp
forces
idr
isis
karp
l2vpn
l3vpn
manet
mpls
ospf
pce
pim
pwe3
roll
rtgwg
sidr
vrrp

O&M Area

adslmib
bmwg
dime
dnsop
grow
ipfix
mboned
netconf
netmod
opsawg
opsec
pmol
radext
v6ops

RAI Area

avt
bliss
codec
dispatch
drinks
ecrit
enum
geopriv
martini
mediactrl
mmusic
p2psip
simple
sipclf
sipcore
siprec
soc
speechsc
speermint
xcon
xmpp

Internet Area

16ng
6lowpan
6man
ancp
autoconf
csi
dhc
dnsext
hip
intarea
ipdvb
l2tpext
lisp
mext
mif
mip4
mipshop
multimob
netext
netlmm
ntp
pppext
savi
shim6
softwire
tictoc
trill

GENERAL AREA

Internet Engineering Steering Group (IESG)

HTTP/2.0 (HTTPBis WG)

- HTTP/1.1 update is being finalised
- HTTP/2.0 – a new mapping of HTTP semantics to TCP, with extra functionality:
  - Multiple tagged requests/responses (“streams”) that can be interleaved
  - Avoid the need for multiple TCP connections
  - Request/response HTTP headers are specially compressed to reduce bandwidth
  - Ability to prioritize requests
  - Server can push some resources to clients
  - More efficient binary message framing

IMAP QRESYNC

- Basic IMAP protocol specified in RFC 3501
- Goal of the WG – work on IMAP extensions for minimizing traffic when resynchronizing mailbox changes
  - draft-ietf-qresync-rfc4551bis-04 and draft-ietf-qresync-rfc5162bis-02
  - Example*:* INBOX with 10000 messages. Flags on 100 messages were changed. 300 new messages were delivered to the mailbox.
  - There is significant win in mobile networks when people are charged per Kbyte sent/received.

IMAP QRESYNC (continued)

- Active implementers community
  - Several open source implementations (e.g. Dovecot, Cyrus), several commercial (e.g. Gmail, Oracle, Isode)

Antispam related techniques

- SPF update (SPFBIS WG)
  - SPF allows a domain to designate certain MTAs as legitimate senders of email on behalf of a domain
  - The goal of the WG is:

Correction of errors, removal of unused features, addition of any enhancements that have already gained widespread support, and addition of clarifying language.

RFC 6686 - Resolution of the Sender Policy Framework (SPF) and Sender ID Experiments

- Talks about observed use of SPF and Sender-ID in the wide and whether there is any practical difference in using one over the other

REPUTE WG

- In the open Internet, making a meaningful choice about the handling of content requires an assessment of its safety or "trustworthiness". This can be based on a trust metric for the owner (identity) of an identifier associated with the content, to distinguish (likely) good actors from bad actors. The generic term for such information is "reputation".

Frequently used with SPF (RFC4408) and DKIM (RFC4871), but can also be applied to web pages and hosts. 2 mechanisms:

simple -- records in the DNS

extended -- a response can contain more complex information useful to an assessor, reported over HTTP using JSON encoding

REPUTE WG

About to be approved for publication:

draft-ietf-repute-model-10 An Architecture for Reputation Reporting

draft-ietf-repute-media-type-13A Media Type for Reputation Interchange

draft-ietf-repute-email-identifiers-10 A Reputation Response Set for Email Identifiers

draft-ietf-repute-query-http-11 A Reputation Query Protocol

Internationalisation

- IDN (Internationalized Domain Names)
  - Completed in 2010
  - RFC 5992 - “Internationalized Domain Names Registration and Administration Guidelines for European Languages Using Cyrillic”
- EAI (Internationalized Email) – completed in March 2013
- Precis (algorithms for string comparison which are independent of version of Unicode)
  - Replaces StringPrep (RFC 3453), which is tied to Unicode 3.2. The latest version of Unicode is 6.2 (www.unicode.org)

DANE & DNSSEC

- DANE - "DNS-based Authentication of Named Entities"
- DANE's objective:

  "Specify mechanisms and techniques that allow Internet applications to establish cryptographically secured communications by using information distributed through DNSSEC for discovering and authenticating public keys which are associated with a service located at a domain name."

RFC 6394 - "Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)"

CA Constraints – which CAs can issue certificates for a service

Service Certificate Constraints

Trust Anchor Assertion and Domain-Issued Certificates

Delegated Services

DANE & DNSSEC

- RFC 6698 - The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA

```
_443._tcp.www.example.com. IN TLSA (
        1 1 2 92003ba34942dc74152e2f2c408d29ec
              a5a520e7f2e06bb944f4dca346baf63c
              1b177615d466f6c4b71c216a50292bd5
              8C9ebdd2f74e38fe51ffd48c43326cbc )
```

<the Certificate Usage Field>

<selector: full cert/SubjectPublicKeyInfo>

<matching type> – type of a hash or specific value>

DANE & DNSSEC

- DNSSEC provides signatures over DNS records to allow applications to detect tempering with DNS records
- Together DNSSEC and DANE can be used for secure delegation, for example
  - draft-ietf-dane-srv-02 - Using DNS-Based Authentication of Named Entities (DANE) TLSA records with SRV and MX records
  - draft-ietf-dane-smtp-01 - Secure SMTP using DNS-Based Authentication of Named Entities (DANE) TLSA records

Several open source SMTP implementations already exist

DANE & DNSSEC

```
; mail domain
example.com.              MX      1 mx.example.net.
example.com.              RRSIG   MX ...
; SMTP server host name
mx.example.net.           A       192.0.2.1
mx.example.net.           AAAA    2001:db8:212:8::e:1
; TLSA resource record
_25._tcp.mx.example.net.  TLSA    ...
_25._tcp.mx.example.net.  RRSIG  TLSA ...
```

Mail for addresses at example.com is delivered by SMTP to mx.example.net. Connections to mx.example.net port 25 that use STARTTLS will get a server certificate that authenticates the name mx.example.net.

TLS

- TLS WG is performing maintenance of TLS and DTLS protocols, as well as work on TLS extensions and Cipher suites
- Recently published

  RFC 6961 - The Transport Layer Security (TLS) Multiple Certificate Status Request Extension

    - Will make certificate revocation checks work for web browsers
- Current documents:
  - An extension for multiplexing multiple protocols on a single TCP port is ready for publication (Used by HTTP/2.0)
  - draft-ietf-tls-oob-pubkey-09 Out-of-Band Public Key Validation for Transport Layer Security (TLS)

TLS

- Other related work:
- draft-popov-tls-prohibiting-rc4-00 Prohibiting RC4 Cipher Suites
- draft-agl-tls-chacha20poly1305-01 ChaCha20 and Poly1305 based Cipher Suites for TLS
- draft-sheffer-tls-bcp-01 Recommendations for Secure Use of TLS and DTLS

TLS

- Work on TLS 1.3 started. Major desired new features:

Reduce Handshake Latency

- One roundtrip for at least some initial hanshakes (currently 2)
- Zero roundtrip for rehandshake (currently 1)

Encrypt significantly more of handshake

- Protect identities and extensions

Improve Cross-Protocol Attack Resistance

- Signature in Server Key Exchange doesn't cover entire handshake

AEAD Cipher suites (+deprecate CBC?)

Bigger Random Values

Behavior Engineering for Hindrance Avoidance (Behave)

- “The working group creates documents to enable IPv4/IPv4 and IPv6/IPv4 NATs to function in as deterministic a fashion as possible.”
- Recently published documents:

RFC 6888 - Common Requirements for Carrier-Grade NATs (CGNs)

RFC 6889 - Analysis of Stateful 64 Translation

- Recently approved:

draft-ietf-behave-nat64-learn-analysis-03.txt - Analysis of solution proposals for hosts to learn NAT64 prefix

Behavior Engineering for Hindrance Avoidance (Behave)

- Work in progress:

draft-ietf-behave-requirements-update-00 Network Address Translation (NAT) Behavioral Requirements Updates

draft-ietf-behave-sctpnat-09 Stream Control Transmission Protocol (SCTP) Network Address Translation

draft-ietf-behave-syslog-nat-logging-03 Syslog Format for NAT Logging

Secure Inter-Domain Routing (SIDR)

The purpose of the SIDR working group is to reduce vulnerabilities in the inter-domain routing system. The two vulnerabilities that will be addressed are:

* Is an Autonomous System (AS) authorized to originate an IP prefix?

* Is the AS-Path represented in the route the same as the path through which the Network Layer Reachability Information travelled?

SIDR WG completed the following work:

Resource Public Key Infrastructure (RPKI). Special X.509 certificates and signed objects are used for representing resources, etc

Protocol for distribution of RPKI data to routing devices and its use in operational networks

Secure Inter-Domain Routing (SIDR)

Published in February 2012:

RFC 6480 An Infrastructure to Support Secure Internet Routing

Documents describing RPKI, repository structure used:

RFCs 6481-6491, RFC 6493

Documents describing a protocol for requesting/revoking Resource Certificates:

RFC 6492 A Protocol for Provisioning Resource Certificates

Secure Inter-Domain Routing (SIDR)

Published in 2013:

RFC 6810 The Resource Public Key Infrastructure (RPKI) to Router Protocol

RFC 6907 Use Cases and Interpretations of Resource Public Key Infrastructure (RPKI) Objects for Issuers and Relying Parties

RFC 6916 Algorithm Agility Procedure for the Resource Public Key Infrastructure (RPKI)

Recently completed by the WG:

draft-ietf-sidr-origin-ops-21 RPKI-Based Origin Validation Operation

draft-ietf-sidr-bgpsec-threats-06 Threat Model for BGP Path Security

Secure Inter-Domain Routing (SIDR)

Documents being worked on:

draft-ietf-sidr-as-migration-00 BGPSec Considerations for AS Migration

draft-ietf-sidr-bgpsec-overview-03 An Overview of BGPSEC

draft-ietf-sidr-cps-02 Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI)

draft-ietf-sidr-policy-qualifiers-00 Policy Qualifiers in RPKI Certificates

For more information on documents:

http://datatracker.ietf.org/doc/search/?sort=date&activedrafts=on&name=sidr&rfcs=on

Constrained RESTful Environments (CORE WG)

- **Goal:** to develop an easy to implement HTTP-like protocol for constraint devices like electric switches and temperature censors, i.e. for devices with limited power supply and processing capabilities.
- **Recently completed work:**
  - "Link Format" published as RFC 6690 in August 2012
  - "Constrained Application Protocol (CoAP)" approved for publication in August 2013

CORE WG (continued)

- Future work
  - “Blockwise transfers in CoAP” - how to transfer large chunks of data in an efficient manner
  - “Group Communication for CoAP” - describes how to use CoAP on top of IP multicast
  - “Observing Resources in CoAP” - specifies a simple protocol extension for CoAP that enables CoAP clients to "observe" resources, i.e., to retrieve a representation of a resource and keep this representation updated by the server over a period of time
  - “Best Practices for HTTP-CoAP Mapping Implementation” - how to implement an HTTP-to-CoAP proxy

Summary

- IETF makes the Internet work better
  - Fundamental role in Internet protocol development
- Your participation is critical to the success of the IETF
  - International scope, local relevance
  - Operator's view is always valuable
- Open, inclusive, well established structure
  - evolving together with the Internet
- More information
  - www.ietf.org