IETF® Journal

A report from IETF 91, November 2014, Honolulu, Hawaii. Published by the Internet Society in cooperation with the Internet Engineering Task Force.*

INSIDE THIS ISSUE

FROM THE EDITOR'S DESK

By Mat Ford

THE NERDS RETURNED TO PARADISE FOR THE IETF 91 MEETING, HOSTED BY CISCO in stunning Waikiki, Honolulu. Despite the temptation to devote the week to surfing, attendees got a lot of great work done at this memorable meeting.

Our cover article discusses the challenges for standards organisations like the Internet Engineering Task Force (IETF) in the face of agile software development paradigms. We also have articles about the upcoming IETF website revamp, a new initiative on human rights and Internet protocols, and a report on the WiFi privacy trial that ran on the meeting network in Hawaii.

You'll read about the most recent winners of the Applied Networking Research Prize, and learn about the Internet Society panel event that explored the question, Is Identity an Internet Building Block?

Our regular columns from the IETF, the Internet Architecture Board, and the Internet Research Task Force chairs, plus coverage of hot topics discussed during the meeting's plenary sessions wrap up the issue. For more details of the Internet Area of the IETF in particular, a Working Group summary report is available at http://wiki.tools.ietf.org/area/int/trac/wiki/IETF91. And last, the issue debuts a new look for the *IETF Journal*, part of a year-long celebration of the publication's 10-year anniversary.

We are hugely grateful to all of our contributors. Please send your comments and suggestions for contributions to ietfjournal@isoc.org. You can subscribe to hardcopy or email editions at https://www.internetsociety.org/publications/ietf-journal/ietf-journal-subscription.

OPEN STANDARDS, OPEN SOURCE, OPEN LOOP

by David Ward

THERE EXISTS AN UNAVOIDABLE QUESTION FOR BOTH COMMUNITY PARTICIPANTS and observers: are standards development organisations (SDOs), such as the Internet Engineering Task Force (IETF), still relevant in today's rapidly expanding environment of Open Source Software (OSS) projects?

MESSAGE FROM THE IETF CHAIR

By Jari Arkko

THE IETF 91 MEETING HAD 1,100 PARTICIPANTS FROM 50 COUNTRIES. IN ADDITION, we offered seven remote hubs throughout Latin America, and 25 presentations were held by people attending remotely. We expect remote attendance to grow even more in the future, thanks to technologies that the IETF and others have been working on. They will enable more participation and lower barriers to increased IETF involvement.

With more than 120 working groups, there are always many interesting things going on both at meetings and after them. Following are highlights of where large and important changes are happening.

Jari Arkko, IETF Chair

- **Work on the Web protocol stack improvements reached a major milestone, when the HTTP/2 specification was approved in February 2015.** The new specification builds on the foundations of existing HTTP protocols, but improves on it in many ways. For example, HTTP/2 should measurably speed page loads, and thanks to compressed headers, use less network bandwidth. I expect this technology to be in very broad use in the coming years—there are already 30 implementations and a fair amount of experience with it.

- **The IETF, the Regional Internet Registries (RIRs), and The Internet Corporation for Assigned Names and Numbers (ICANN) have been working together to transition the role of the US government in the stewardship of IANA functions to the Internet community.** In January 2015, the proposed plans for IETF and RIR parts of this transition were completed by the communities confirming how they want to address the transition. Both proposals have received positive feedback from the broader Internet community. In the case of the IETF, the plan largely is to continue with the arrangements we've already built up over the years. The community processes and roles for various organisations already work well.

- **We are seeing a surge of YANG data models submitted to the IETF.** YANG is a data modeling language for the NETCONF network configuration protocol, and these models are needed to manage network nodes in operator networks in centralised fashion. Working groups across the IETF, and particularly in the Routing Area, are working on these models to ensure that the industry has the interoperable standards it needs.

- **Work on the difficult problem of improving Internet security and privacy continues in multiple working groups.** For me, the new highlight of this effort at IETF 91 in Honolulu was the newly chartered DPRIVE working group, which addresses Domain Name System (DNS) privacy. Their meeting systematically walked through various design alternatives to enable DNS queries to be done in a private manner. Other efforts on the general problem continue, as well. The Transport Layer Security (TLS) working group is working on version 1.3 of the TLS specification, a fairly large redesign of the protocol. None of this work is easy: we need deployable security solutions, technology that enables the network to do its work while protecting privacy, and algorithms we know we can trust.

Lastly, the Internet Engineering Steering Group is working hard on ensuring that the IETF structure matches today's needs. The intent is to increase flexibility as IETF work evolves and to balance and reduce the workload across our steering group. We have changed the roles of area directors to match current work areas and have a proposal out for merging the applications and real-time applications areas.

Next up, Dallas, Texas, in March 2015. Until then, back to the mailing list for work on many of the above and other important issues.

The mission of the Internet Engineering Task Force is to make the Internet work better by producing high-quality and relevant technical documents that influence the way people design, use, and manage the Internet. See http://www.ietf.org.

Recent IESG Document and Protocol Actions

A full list of recent IESG Document and Protocol Actions can be found
at https://datatracker.ietf.org/iesg/ann/new/

WORDS FROM THE IAB CHAIR

By Russ Housley

DURING THE IETF 91 MEETING IN HONOLULU, THE INTERNET ARCHITECTURE BOARD (IAB) released a statement about Internet confidentiality; shortly after IETF 91, the IAB issued a statement about the NETmundial Initiative. After a list of highlights since IETF 90, this article repeats the previous two IAB statements without editorial comment.

Russ Housley, IAB Chair

Highlights since IETF 90

- The IAB appointed John Levine to the 2015 Internet Corporation for Assigned Names and Numbers Nominating Committee.

- The IAB published RFC 7322, "RFC Style Guide."

- The IAB reappointed Nevil Brownlee as independent submission editor.

- The IAB reappointed Lars Eggert as chair of the Internet Research Task Force.

> **The IAB now believes it is important for protocol designers, developers, and operators to make encryption the norm for Internet traffic. Newly designed protocols should prefer encryption to cleartext operation.**

IAB Statement on Internet Confidentiality

In 1996, the IAB and Internet Engineering Steering Group recognized that the growth of the Internet depended on users having confidence that the network would protect their private information. RFC 1984 documented this need. Since that time, we have seen evidence that the capabilities and activities of attackers are greater and more pervasive than previously known. The IAB now believes it is important for protocol designers, developers, and operators to make encryption the norm for Internet traffic. Encryption should be authenticated where possible, but even protocols providing confidentiality without authentication are useful in the face of pervasive surveillance as described in RFC 7258.

Newly designed protocols should prefer encryption to cleartext operation. There may be exceptions to this default, but it is important to recognize that protocols do not operate in isolation. Information leaked by one protocol can be made part of a more substantial body of information by cross-correlation of traffic observation. There are protocols which may as a result require encryption on the Internet even when it would not be a requirement for that protocol operating in isolation.

We recommend that encryption be deployed throughout the protocol stack since there is not a single place within the stack where all kinds of communication can be protected.

The IAB urges protocol designers to design for confidential operation by default. We strongly encourage developers to include encryption in their implementations and to make them encrypted by default. We similarly encourage network and service operators to deploy encryption where it is not yet deployed, and we urge firewall policy administrators to permit encrypted traffic.

The Internet Architecture Board is chartered both as a committee of the IETF and as an advisory body of the Internet Society. Its responsibilities include architectural oversight of IETF activities, Internet Standards Process oversight and appeal, and the appointment of the RFC Editor. See http://www.iab.org.
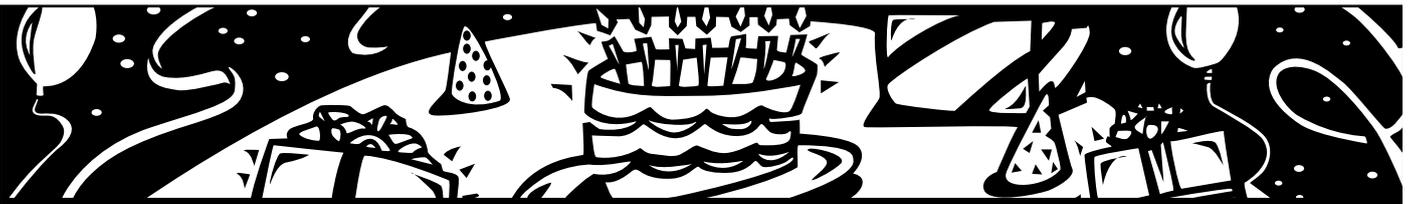
HAPPY 10TH ANNIVERSARY, *IETF JOURNAL!*

The very first issue of the *IETF Journal* was published in October 2005, just prior to IETF 64. Its editor, Peter Godwin, explained in the publication's first article, "Our aim is to provide an overview of what's happening in the world of Internet standards with a particular focus on the activities of the IETF Working Groups (WG). While we won't be able to provide in-depth coverage of every WG, each issue of the *IETF Journal* will highlight some of the hot issues being discussed in IETF meetings and in the IETF mailing lists."

Over the past ten years, much has changed in the world of Internet standards, but the goals of the *IETF Journal* remain the same. We still keep you up-to-date on what's happening at the IETF, whether you attend meetings in person or via remote participation, whether you're seeking to get up to speed after missing a few meetings or are just getting started in the IETF space.

The look of the *Journal* has also remained the same... until now. In celebration of our 10th anniversary, we've updated the layout. It's fresh, clean, modern, and we hope you like it.

Forging ahead, we are committed to upholding the *Journal*'s original goals, in addition to offering the community a sense of the diversity, breadth, and excitement of the IETF's thrice-yearly meetings. Most important, we always welcome your thoughts, feedback, content suggestions, and author contributions. Contact us anytime at ietfjournal@isoc.org.

Happy anniversary, *IETF Journal* community! We're so proud to serve you.

Words from the IAB Chair, continued

We believe that each of these changes will help restore the trust users must have in the Internet. We acknowledge that this will take time and trouble, though we believe recent successes in content delivery networks, messaging, and Internet application deployments demonstrate the feasibility of this migration. We also acknowledge that many network operations activities today, from traffic management and intrusion detection to spam prevention and policy enforcement, assume access to cleartext payload. For many of these activities there are no solutions yet, but the IAB will work with those affected to foster development of new approaches for these activities which allow us to move to an Internet where traffic is confidential by default.

IAB Statement on the NETmundial Intiative

The IAB thinks it is valuable to develop tools to support communities that can share solutions, expertise, and research related to Internet Governance. We welcomed the initial NETmundial meeting as an additional way to foster the development of a broadly based community engaged in supporting the Internet's distributed systems and methods. We believe that the recent NETmundial Initiative (https://www.net-mundial.org/press-release-1) to develop a long-running dialogue on these topics, in the form of a website and collection of materials, may be a valuable addition to the overall community efforts.

We are concerned, however, that the creation of a highly structured coordination council for the Initiative may impede the development of broad participation, and so may be premature. Because the coordination council members appear to be the responsible parties for the effort, the effort may not foster the sort of community engagement that we believe is fundamental to the Internet's distributed nature and the NETmundial principles (https://www.net-mundial.org/principles).

To make the Internet work, many people with unique perspectives of the Internet and from different communities must cooperate. We believe a broadly based dialogue among all these communities is necessary, and support any effort to enable this dialogue. The permissionless innovation given as the goal of this effort is better served by first enabling technical infrastructure to further that cooperation; that might require some lightweight administration driven by community consensus. No coordination council is needed now, and therefore the IAB will not participate in the council at this time.

Open Standards, Open Source, Open Loop, continued

For those new to the conversation, the question is not whether SDOs *should exist*—they are a political reality inexorably tied to trade policies and international relationships. The fundamental reason behind their existence is to avoid a communications Tower of Babel and to establish governance over the use of a global commercial and information infrastructure. The question is whether these organizations *have a role* in enabling innovation.

> **Software has come to dominate what we perceive as the Internet, and the agile development model has created a sharp knee in the rate of innovation over the past couple of years—innovation that needs standardization.**

SDO Challenges

SDOs, such as the IETF, must evolve their processes in order to keep up with the technological landscape and for its development processes to remain relevant.

Software has come to dominate what we perceive as the Internet, and the agile development model has created a sharp knee in the rate of innovation over the past couple of years—innovation that needs standardization. Although code is "coin of the realm" in Open Source Software (OSS) projects, code is not normative.

It is important to have SDOs and consensus-based standards. But SDOs need to realize that the OSS cycle time can create a market-based consensus to

> **To an outsider (and even some insiders), the recent reorganizing of the workgroups has the appearance of shuffling the deck chairs. It does not change our process.**

fill a standards void and that this realization may be the key to our collective futures.

There is an impedance mismatch between SDOs and OSS projects of at least 2:1 (two years to a paper standard versus one year to a product that creates a de-facto standard).

Globally, many SDOs appear incapable of defining and maintaining their boundaries, and new technology study groups are exploding across them. Every organisation is potentially—and dangerously—self-perpetuating. Few SDOs have a life-cycle plan that bounds their authority and scope as applied to new technologies.

Real coordination between SDOs is not readily detectable. This dilutes the efforts and resources of participating companies and individuals, and is creating confusion for the consumers of these technologies.

Within the IETF, we face numerous issues around our own life cycle. How much of our time are we spending on further standardization of established technology at the expense of more-pertinent and relevant working groups? How do we handle issues, technologies, and new architectures that would span our existing structure when they arise (e.g., the recent YANG model explosion across working groups)? What does the subject matter of popular, network-centric OSS projects imply might be missing at the IETF?

Most important, how do we offer startup companies, new vendors, and newly invested consumers the assurance that they have a voice, while avoiding the appearance of being an aristocracy and not a meritocracy-driven body?

> *Conway's Law: Organisations that design systems are constrained to produce designs that are copies of the communication structures of these organisations.*

To an outsider (and even some insiders), the recent reorganizing of the workgroups has the appearance of shuffling the deck chairs. It does not change our process. Conway's Law applies here.

Without more fundamental structural change, we can only expect more of the same process. The world shouldn't wait two years for a standard for Service Function Chaining, or even more years for Network Virtualization Overlays (or Network Functions Virtualization in general, which is more of a European Telecommunications Standards Institute problem).

Open Source

While there is much to say regarding the challenges that both the global SDO community and the IETF face, there also are potential risks were the OSS communities to run away with the standardization mantle.

In short, the danger is the coopting of open source due to the lack of governance. Open source software projects with poor governance risk multiple, equally bad fates.

Like the confusion stemming from the uncontrolled overlap of standards from multiple SDOs, OSS projects that overlap can also create confusion. Competition can be both unintentional (e.g., a difference in technical opinions) and purposeful (e.g., vendor freeware offered as open

Open Standards, Open Source, Open Loop, continued

source with no real community diversity to offer support alternatives, complimentary products, or hooks to other projects). The result can be multiple small communities that are underfunded or understaffed monocultures dominated by a single party.

- Good and impartial third-party governance helps avoid the creation of overlapping, nondiverse, and confusing projects.

OSS projects that don't connect to form larger architectures can create fragmentation. Fragmentation results when multiple projects each deliver part of an overall solution but cannot be used together, thereby frustrating any progress and interfering with higher-level innovation.

- Good governance creates a community that considers both the upstream and downstream connectivity of a project.

> **Good and impartial third-party governance helps avoid the creation of overlapping, nondiverse, and confusing projects.**

Security flaws can result when the project has a weak security focus, often the result of critical technology with too few reviewers and maintainers. This result recently manifested in OpenSSL (HeartBleed), and is now being addressed through the Linux Foundation Core Infrastructure Initiative (for OpenSSL, OpenSSH, and NTPd).

- Good governance establishes an effective development process—not only for new contributions, but also for maintenance, updates, and releases.

Proper governance also provides essential business, legal, management, and strategic processes that ensure a proper ownership and licensing of contributions, release management, and open community involvement. Excellent examples exist in the Linux Foundation, the Apache Foundation, and the OpenStack Foundation.

Alternative SDO Model

There have been several SDO proposals to subsume and standardize network-centric architectures developed in OSS via the endpoint/interface/application program interface (API) definition exercise. The Open Networking Foundation (ONF) is an example of an early attempt at a different hybrid model: attempting to bridge both worlds, it used the word *standard* to describe its wire protocol and the word *open* to describe its architecture.

The protocol evolved through numerous and sometimes not-backward-compatible specifications, and the organisation moved very quickly into advocacy and market development for the protocol, architecture, and OpenFlow controller (the latter activity not normally associated with a traditional SDO).

Although open-source controllers and switches were available, most were developed outside the ONF by individual interest groups. The ONF provided no reference implementation of their own.

The most important lesson from the ONF experience is fundamental to both SDOs and OSS: a truly successful ecosystem and community is created via the openness of a solution framework and via collaboration, not via ownership, and only in that way can one avoid fragmentation and confusion. Unlike in an SDO, marketing has a place in OSS projects, but should be focused primarily on community building and engagement.

Why Open API and Framework Standards Are Important

Many of the emerging OSS projects provide broadly scoped and connected solution architectures. It's important that we discuss the role of SDOs, such as the IETF, in making the connective-tissue of these new architectures normative, in order to ensure the functional interoperability that some fear may diminish in this environment. *(See https://tools.ietf.org/html/draft-opsawg-operators-ietf-00, posted by members of the Internet Society.)*

Future standards in software-driven networks will be in the form of APIs and application/service frameworks. The same reasons that the underlying Internet protocols are standardized apply to these higher-level concepts: interoperability, choice, and system design.

Standardization is necessary to vanquish the myths that a future which integrates a large amount of OSS means a future in which all software and solutions are free, and that the only viable economic model for a vendor is solely to support OSS.

On the contrary, properly designed, open, and standardized frameworks, protocols, state machines, and the like enable vendors to provide intellectual property in a modular, and, if need be, replaceable manner. There will certainly be community-supported OSS components within developing solutions, but via standardization the incentives for innovation remain for established and startup vendors.

> **Standardization is necessary to vanquish the myths that a future which integrates a large amount of OSS means a future in which all software and solutions are free, and that the only viable economic model for a vendor is solely to support OSS.**

In this way, vendor support of OSS becomes rational and credible—as does its consumption in the operator community.

Open Loop

In spite of political or economic mandates for existence, the right of any SDO to be an authority must be earned. The IETF is arguably the most appropriately focused SDO to engage in standardizing the software-driven network. The IETF is neither too broad (e.g., not involved with health and safety or environment and climate change) nor too narrow (e.g., not a single service or network domain), and the IETF experience with architecture definition, protocol development, and information/data modeling (YANG) overlaps well with the interests and outputs of network-centric OSS projects.

How to Make the IETF Relevant in this Environment

To make the IETF *the* SDO authority for new things that IT professionals and operators need, I propose that the IETF do the following.

- *Consider reforming and restructuring itself to facilitate a more agile process. Kill off what should be dead and make room for new work.* Specifically, fail fast in order to succeed faster with fewer yet better ideas that move at the speed the market moves: more Birds of a Feather meetings leading to more successful, relevant working groups with shorter lifespans, less paper to wade through, and more tangible outputs. Enable new working groups to proceed with technical work in parallel with some of the Framework, Architecture, Requirements, and Use-Case drafts that have bogged down so many people for so long. Cut the cycle time for everything (rough consensus shouldn't take two or more years).

- *Emphasize software development more in the IETF structure.* Encourage interoperability and function demon-strations all the time. Running code used to be part of the IETF mantra, but running code later is not agile. Think "hackathon" during the standards development process. From experience, the best standards have been produced hand in hand with writing the code at the same time.

> **Forcing an integration of skills and purposes changes a community with potentially bad results—collaboration, interaction, and an exchange of ideas is a better model for all of us.**

- *Engage in even more research (already a strength), thereby engaging a broader range of participants.*

- *Fix, change, or reinvent the liaison process because it will be critical to collaboration with OSS projects.* In fact, don't even use the liaison process as a model.

- *Embrace Open Source projects.* The heart of this effort will require the establishment of an open-loop engagement between the Internet Engineering Steering Group and reputable OSS foundations on productive and compatible projects. A good example of such a compatible and properly governed project is the OpenDaylight Project (Linux Foundation), which is driving the use of YANG models into the IETF as well as other open source projects.

By researching and monitoring OSS projects, we can actively invest our energy in emerging technologies instead of waiting for it to show up on our doorstep.

A feedback loop between parties will identify the areas of new and existing projects that need to be standardized, should use existing standards, or are out of compliance with standards. From a viewpoint of experience, writing code before standardizing has produced the most complete and simplistic definition of protocols.

Part of this process will require that the IETF resist the need to own or copy everything into IETF working groups. SDO geeks and OSS geeks are not the same. Paradoxically, for our purposes, code is not normative. But it's also hard to define and standardize APIs if you're not writing code. Forcing an integration of skills and purposes changes a community with potentially bad results—collaboration, interaction, and an exchange of ideas is a better model for all of us. (Note that collaboration will not work if the SDO cycle creates unnecessary drag on the OSS partner. Conversely, a non-vibrant OSS community won't be able to interact with any SDO.)

Finally, we must (1) adapt and adopt new laws, and (2) avoid Conway's Law.

> *Law of OpenSource: The quality and strength of a project is 100 percent dependent on the interests, energy, and capability of the developer community.*

> *Law of OpenStandards: The importance, validity, and timeliness of relevant specification is 100 percent dependent on the interests, energy, and compromises of those who have been empowered to manage, organize, and complete the work effort of the SDO.*

If we realize that these laws exist, we must also understand that the roles of OSS and SDOs need to change. We must set a new trajectory, move faster, and focus on building a bigger and better Internet.

IAB DETAILS TRANSPORT, SECURITY EFFORTS

By Carolyn Duffy Marsan

THE INTERNET ARCHITECTURE BOARD (IAB) HIGHLIGHTED TWO OF ITS programmes—IP Stack Evolution and Privacy and Security—during a technical plenary session held during IETF 91 in Honolulu in November.

Joe Hildebrand reported on the activities of the IAB's Internet Protocol (IP) Stack Evolution Programme, which is studying the implications of how the IP stack is evolving as a result of dual-stack communications supporting IPv4 and IPv6. Further, more applications are being built for Transport Layer Security (TLS) and Hypertext Transfer Protocol (HTTP), which add two more layers between TCP and applications.

These trends result in the IP stack evolving from a normal hourglass shape to a taller, thinner hourglass with separate stems for IPv4 and IPv6. The new IP stack makes it harder to innovate at the transport layer, Hildebrand said.

"Some things envisioned by protocol developers are not as accessible to application programmers as is desired," he said. "This means that there are not as many opportunities to add new security. Even if one fixes the interface, there is the matter of middleboxes."

Hildebrand pointed out that middleboxes aren't evil; they serve a purpose and solve a problem. Although Internet engineers prefer end-to-end communications, the majority of paths are broken due to widespread deployment of middleboxes such as network address translators (NATs).

As a starting point for its IP Stack effort, IAB is considering a proposal for a new layer on top of UDP, dubbed *udp35,* to provide a partial defense against middleboxes.

"UDP gives us a partial defense against middleboxes, provides port multiplexing and works from userspace," Hildebrand says, adding that the new UDP-based protocol would provide hooks for policy

decisions and would facilitate the evolution of Internet-over-HTTP applications.

The IAB's IP Stack Evolution Programme was formed to provide guidance and coordinate efforts by several IETF working groups: Transport Services (TAPS), TCP Increased Security (TCPINC), and Active Queue Management (AQM). The programme hopes to evolve interfaces to transport and network-layer services and improve path transparency in the presence of firewalls and middleboxes.

> **Hildebrand pointed out that middleboxes aren't evil; they serve a purpose and solve a problem.**

The IAB hosted a workshop on Stack Evolution in a Middlebox Internet (SEMI) in Zurich in January 2015. IETF participants were invited to read the workshop report when it is eventually published.

"The aim of the workshop is to get people from research and industry working in this space together to refine the scope and solution space considered by the program," Hildebrand said.

Ted Hardie reported on the IAB's Privacy and Security Programme. He noted that the programme focuses on three challenges. First, Internet protocols are developed as building blocks, thus security and privacy protections are piecemeal. Second, security approaches presume that attackers have resources on par with those available to secure the system. Third, many systems breach confidentiality to simplify the delivery of services or meet other requirements.

To address these challenges, the IAB's Privacy and Security Programme is split into three streams of work: Internet-Scale Resilience, Confidentiality, and Trust.

The Internet-Scale Resilience stream, led by Brian Trammel, is doing work on route hijacking, Distributed Denial of Service (DDoS), and related attacks. Documents are planned that will describe the available mitigations and work with related IETF programs to limit the development of protocols that offer amplification opportunities to the attackers.

The Confidentiality stream, led by Joe Hall, is working on threat models related to surveillance. An IAB statement on the applicability of cleartext protocols is in progress.

The Internet Architecture Board's Technical Plenary covered two of the organization's programmes: IP Stack Evolution and Privacy and Security.

The Trust stream, led by Karen O'Donoghue, is working on public-key infrastructure, trying to understand how to work with multiple sources of truth within a system. Planned work includes a threat-model document as well as an IAB statement on designing protocols with multiple sources of truth.

Hardie encouraged IETF participants to email the IAB's Privacy and Security Programme with relevant threats or issues raised in IETF working groups.

In administrative news, the IETF is putting its RFC Production Center contract out to bid and is experimenting with writing labs at the IETF meetings in order to help authors improve their documents.

> **Hardie encouraged IETF participants to email the IAB's Privacy and Security Programme with relevant threats or issues raised in IETF working groups.**

In addition, Sally Wentworth briefed the IETF community about the International Telecommunication Union (ITU) Plenipotentiary Conference, which featured discussions on privacy, surveillance, human rights, policy affordability, and sovereignty. She said the ITU did not expand its scope with respect to Internet operational issues. In addition, the ITU treaty and official definitions remain the same.

Wentworth believes the outreach the IETF has undertaken with policymakers over the last few years is paying off.

"The work done in home countries to bring greater knowledge about the technical work do have a bearing on how policy discussions play out," she said.

EXPERT PANEL URGES IETF TO TACKLE IDENTITY ISSUES

By Carolyn Duffy Marsan

THE INTERNET LACKS A SCALABLE INFRASTRUCTURE FOR TRUST management, and the Internet engineering community should develop technical solutions to help address this complex problem. That was the conclusion of an Internet Society-sponsored panel entitled, "Is Identity an Internet Building Block?" held 11 November 2014 concurrent with the IETF meeting in Honolulu, Hawaii.

"Identities and the attributes that relate to identities are somewhat key to establishing trust in the Internet," said Olaf Kolkman, chief Internet technology officer at the Internet Society and moderator of the panel. "When we perform any sort of communication on the Internet, identities are used for that. Attributes are used for authentication. Attributes are used as the basis of opportunistic encryption. Knowing who or what is on the other end of the line is sometimes very important."

Kolkman asked panelists to discuss what components are necessary to build a scalable, nonhierarchical and reusable trust model for the Internet.

Jeff Hodges, a PayPal engineer who spoke as an individual rather than as a corporate representative, set the stage for the discussion about identity on the Internet.

"The context of the discussion is how do we human subjects interact with various

Jeff Hodges, engineer and panelist, discussed identity on the Internet.

> **Identity involves mapping human subjects to actions, events, processes, communications channels, and physical devices. [Hodges] pointed out that identity is involved whenever you log into a website or device.**

other entities, human or not, throughout the Internet and be known as us or ourselves?" Hodges asked, adding that that this process is not necessarily under our control. "Do we have some control to assert ourselves as us?"

Identity involves mapping human subjects to actions, events, processes, communications channels, and physical devices, Hodges said. He pointed out that identity is involved whenever you log into a website or device.

"We also need to keep in mind there are various tensions and tussles involved

Expert Panel Urges IETF to Tackle Identity Issues, continued

in the areas of naming, identification, agency, autonomy, privacy, security, and such," Hodges added. "The more we work to make it smooth and seamless, we also have to take into account the individual's use case and requirements. Maybe they don't want to be identified with certain attributes, and they do want to assert other ones. How do we accommodate that and make it seamless across different modes of communication?"

Hodges said it is inevitable that devices will use biometric identification systems, and controls will be needed to determine where the information your device has about you goes. "Not everything can be enforced technological layers," he added. "We need to keep in mind that [regulation] can be a useful tool."

Natasha Rooney, cochair of the Web and Mobile Interest Group at W3C and Web technologist at Groupe Speciale Mobile Association (GSMA), provided an overview of the use cases for identity management, as well as debates around businesses involved in identity management.

Among the use cases for identity management are situations in which strict security is necessary, such as transferring money or accessing health records, while other services such as social media platforms favor speed over security. Other situations, such as purchasing alcohol or renting a car, require attribute authentication such as verifying age or a valid drivers' license.

"There is some attribute brokerage that can be done," Rooney said. "The questions are: who owns the attribute? And can you be trusted to relay that attribute?"

She pointed out that users will want anonymity in some situations.

"There are a number of services on the Internet that I don't want to know I am this exact person," she said. "We need to consider that when we talk about use cases."

Rooney said the Internet engineering community needs to ask questions about the companies that provide identity management services, including whether these companies can be trusted and how they should be handling identity management.

Natasha Rooney, Web and Mobile Interest Group cochair at W3C, Web technologist at Groupe Speciale Mobile Association, and a panelist, discussed use cases for and businesses involved in identity management.

> **"There are a number of services on the Internet that I don't want to know I am this exact person,"** she said. **"We need to consider that when we talk about use cases."**
>
> **—Natasha Roony, Panelist**

"If we're going to transport attributes over the Internet, how do we want to do that?" she asked. "How should they be secured?"

Rooney suggested that the IETF start with the simplest use case first: log in services. "Can we just get log-in right? Then would we be able to extend that?" she asked.

Leif Johansson, with the office of the chief executive officer at Swedish University Computer Network (SUNET), pointed out that identity has more aspects to it than authentication and authorization. Further, he called the push to remove middlemen from the identity management process in order to be more user centric a distraction because it has resulted in the consolidation of identity information in the possession of one or two content providers.

"I understand why *user centric* strikes a nerve with the IETF crowd because it sounds like the end-to-end principle, but the end-to-end principle is always assisted by infrastructure," Johansson said. "We don't really have the infrastructure that we need to do large-scale identity and trust on the Internet."

Johansson argued that there shouldn't be an identity layer on the Internet, rather, that identity needs to be supported at all layers.

He said the IETF should concentrate on areas where gaps exist in the identity infrastructure. In particular, he'd like to see the IETF develop a protocol like the Border Gateway Protocol (BGP) for trust and key management.

"We need an Internet-scalable mechanism for trust management," Johansson said. "I don't know what it needs to look like, but I do know we need to focus an effort and figure out a solution for this."

The panel's final speaker was Ken Klingenstein, senior director in the Internet2 Trust and Identity area. Klingenstein pointed out that the Internet engineering community is more careful about trust issues than it was 30 years ago, when the original BGP standard was so simple that it was designed on a cocktail napkin.

"It's not creative noodling on a deploying greenfield anymore," Klingenstein said. "We are taking some big beasts and making them work together and interoperate, and they don't all have the same intentions."

Klingenstein outlined several areas where new technology is being developed to

Leif Johansson, from the office of the chief executive officer at Swedish University Computer Network and a panelist, compared identity to authentication and authorization.

improve the Internet's trust mechanisms: federated and dynamic metadata, level of assurance and vectoring of trust, attributes and their metadata, reconciling regimes of privacy, managing downstream use of attributes, and scalable privacy with the federated infrastructures to support it.

"All of the scale we get is because of metadata," Klingenstein said, adding that it is a very powerful mechanism but has its own security needs. "The packets of metadata that we pass around as operators have gotten so big and so volatile that we've had to move to dynamic metadata."

Klingenstein said operators of trust infrastructure spend a lot of time on attributes.

"Privacy and scale both flow from attributes," he said. "Replacing that access control list of names with attributes gives us not only scale, but it gives us privacy. We need to know a lot of metadata about attributes, such as did you have the authority to sign that attribute and how was it bound to the individual."

Other challenges include reconciling privacy rules from country to country and managing downstream attributes. "Managing downstream use of anything is really hard. Look at the music industry," he said. "With identity, it's about making all of this scale and having the infrastructure to support it."

Klingenstein identified several building blocks for identity systems, including

> **Johansson argued that there shouldn't be an identity layer on the Internet, rather, that identity needs to be supported at all layers.**

identity providers, attribute authorities, attribute aggregators, key management, trust management, and consent management.

"We have a lot of aggregators such as portals, and they make things very tricky," he said. "If a portal is hiding many applications, I don't want to dump all of my attributes into a single location. I would like to refine my attributes and provide them on a per-application basis."

Klingenstein noted that policy issues play a role in identity management, too, including what organisations will act as registries, if there will be a registry of registries or a standard format for attributes that is consistent across registries, and how technology will be transferred to emerging nations.

"There are activities around the world trying to set the rules of the road for identity," he

added. "When I think of the purity of the IETF and ISOC, I would recommend that we stay away from [the policy issues.]"

Klingenstein noted that the research and education community has widely deployed federated identity, and that Sweden and Denmark use similar technology for commerce and for interactions between government agencies and citizens.

In the United States, the biggest deployments of federated identity are from Google, Yahoo, and Facebook. On the horizon are deployments for online medical records, and the U.S. government is supporting several pilot projects for government-to-citizen communications through its National Strategy for Trusted Identities in Cyberspace (NSTIC) activity.

Ken Klingenstein, senior director at Internet2 and a panelist, talked about the Internet community, new technologies, and public policy.

Another issue Klingenstein noted is the need for federated identity portability. "This is the ability to move my identity and my preferences for privacy management from one provider to another," he said. "If we're going to create a marketplace, we need identity portability."

In closing the discussion, Johansson emphasized his view that the Internet needs a protocol like BGP for trust. "We have a protocol that runs the network and is used to model business relationships. That is what BGP is," he said. "We don't have that for trust."

HUMAN RIGHTS AT IETF 91

By Niels ten Oever and Joana Varon

A LIVELY DEBATE ABOUT STANDARDS, PROTOCOLS, AND HUMAN RIGHTS occurred during the meeting of the Security Area Advisory Group (SAAG) at IETF 91 in Hawaii. The discussion was framed by the Internet Draft (I-D), Proposal for Research on Human Rights Protocol Considerations.[1]

The draft departs from previous work done by the IETF on privacy and Internet protocols, such as RFC 6973 on Privacy Consideration Guidelines[2], and suggests that some standards and protocols can solidify, enable, or even threaten human rights, such as freedom of expression and the right to association online. Specifically, the draft aims to establish a research group under the Internet Research Task Force to study the structural relationship and impact between Internet standards and protocols and freedom of expression and association.

A deeper rationale for the proposal was explained during the SAAG presentation, where the presenters, who are also the authors of this article, emphasized that the Internet was designed with freedom and openness of communications as core values, and questioned if these structural values can or need to be preserved on a technical level. It was argued that as the politicization of the Internet management space increases, the IETF should take an active role in promoting a more structured and holistic approach, thereby future-proofing standards and protocols and avoiding ad hoc decisions following incidents or disclosures elsewhere.

The proposal raised both eyebrows and concerns about the politicization of the work of the community. Dan Harkins posited, "Doing the human rights study will likely politicize protocols. [I don't] want the technology to have political context. Rather, I want it to be as nonpolitical as possible." Another respondent stated, "We have to stop pretending that technology is a nonpolitical decision." A round of applause followed. The presenters then clarified that their research proposal was

aimed at (1) avoiding further politicization of both protocols and the community, and (2) offering the community the time and proper processes to define its position on the interrelationship between protocols and human rights, such as freedom of expression.

> It was argued that as the politicization of the Internet management space increases, the IETF should take an active role in promoting a more structured and holistic approach, thereby future-proofing standards and protocols and avoiding ad hoc decisions following incidents or disclosures elsewhere.

Both John Levine and Alissa Cooper remarked that, in order to keep the research manageable and to keep the different rights balanced, it is crucial to start the conversation by focusing on specific human rights. The presenters reaffirmed that the primary focus will be on the right to freedom of expression and right to association. Alissa Cooper pointed to the Internet Architecture Board I-D on filtering considerations[3] and the I-D, Policy Considerations for Internet Protocols,[4] as relevant sources for future research.

> Another respondent stated, "We have to stop pretending that technology is a nonpolitical decision." A round of applause followed.

Several RFCs already make explicit statements about the objectives of the Internet, including RFC 1958 that reads, "the community believes that the goal [of the Internet] is connectivity, the tool is the Internet Protocol," and, "the current exponential growth of the network seems to show that connectivity is its own reward and is more valuable than any individual application, such as mail or the World Wide Web." This RFC notes the intrinsic value of connectivity that is facilitated by the Internet, both in principle and in practice. It also indicates that the underlying principles of the Internet aim to preserve connectivity, which is similar to a section of Article 19 of the Universal Declaration of Human Rights that defines a right to receive and to impart information.

There are also protocols that enable freedom of expression and access to information in an unprecedented way, such as Hypertext Transfer Protocol. Although RFC 7230 does not explicitly reference rights, it does form the basis for a rights-enabling architecture. The challenge of the research then is to define the specific protocol attribute(s) made by this protocol that specifically affect human rights.

Next Steps

The next major challenge lies in developing appropriate methodologies to research implicit safeguards in current standards

and protocols in order to make them explicit. Open discussions offered insights to possible methodological approaches. Richard Barnes said, "[It] seems that you are reading RFCs and that you are looking for statements on human rights that are laid out in RFCs. You might risk irritating people by reading technical documents as [if they are] political statements. It might be more useful to use RFCs as a window into the community that developed the rights that these RFCs presume."

Mark Nottingham proposed a perspective of stakeholder prioritization as described in the I-D, Representing Stakeholder Rights in Internet Protocols,[5] which is already implemented at the World Wide Web Consortium.

Useful remarks were made during the session, after the session, and on the mailing list[6], that are being used to improve the next version of the draft slated for further discussion at IETF 92 in Dallas, Texas.

This session raised considerable interest in the community. The presenters and authors of the Proposal for Research on Human Rights Protocol Considerations are continuing their research and will produce an updated I-D before IETF 92. In addition, plans for the Dallas meeting include adding another research methodology and conducting interviews aimed at deepening the understanding that area directors and RFC authors have of specific protocols and the role rights play in them.

If you have questions for the presenters or an interest in their research, please join the mailing list at https://lists.ghserv. net/mailman/listinfo/hrpc.

References

1. Proposal for Research on Human Rights Protocol Considerations, http://www.ietf.org/id/draft-doria-hrpc-proposal-00.txt.

2. "Privacy Considerations for Internet Protocols" [RFC 6973], https://www.rfc-editor.org/rfc/rfc6973.txt.

3. Technical Considerations for Internet Service Blocking and Filtering, http://www.ietf.org/archive/id/draft-iab-filtering-considerations-06.txts.

4. Policy Considerations for Internet Protocols, https://tools.ietf.org/html/draft-morris-policy-cons-00.

5. Representing Stakeholder Rights in Internet Protocols, https://tools.ietf.org/id/draft-nottingham-stakeholder-rights-00.txt.

6. https://lists.ghserv.net/mailman/listinfo/hrpc.
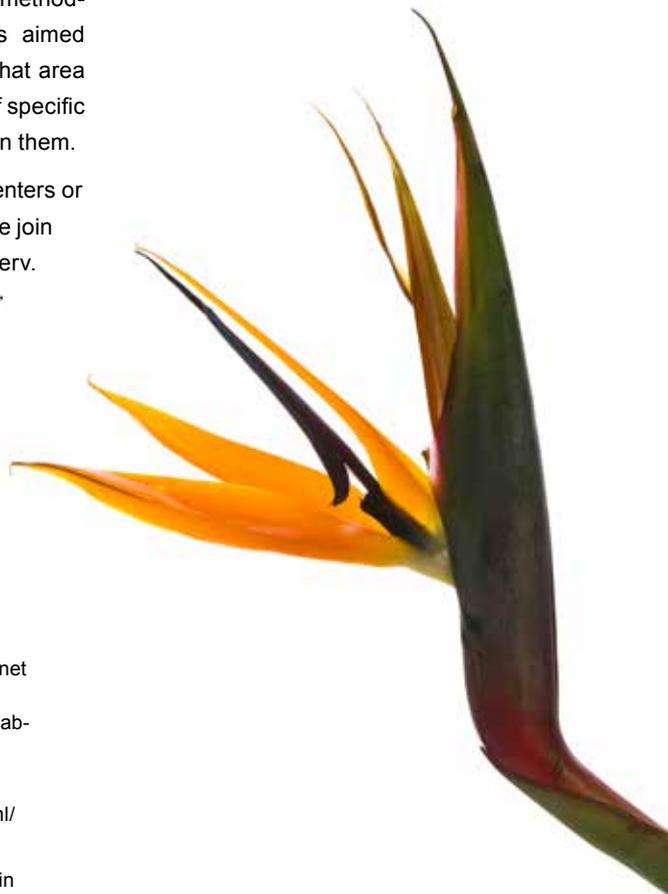
IETF WEBSITE REVAMP

After input and review by the IETF community on the scope of work, the IETF Administrative Oversight Committee (IAOC) put out a request for proposals to revamp the public-facing IETF website (www.ietf.org). Its goal is to provide the IETF with a front door to the information that its users—active IETF participants, new and potential participants, and those looking to learn more about the IETF—need to accomplish their work. Specific goals for the revamp include improving the site's ease of navigation, accessibility by mobile devices, and content maintenance. The IAOC considered several proposals and selected Torchbox (www.torchbox.com) to undertake the project.

A key aspect of the project includes engaging the IETF community as the redesign effort progresses. Key milestones and deliverables (e.g., site architecture, technology, wireframes, page design, and content updates) will be reviewed and approved by a committee chosen from IETF community volunteers.

The project will build on input and review from representatives of key audience groups on such topics as how those audiences use the current IETF Web presence, and will employ focus groups and task testing to evaluate proposed changes before they are implemented.

FRED BAKER ON 25 YEARS OF IETF, INTERNET SOCIETY SERVICE

By Carolyn Duffy Marsan

WHEN FRED BAKER ATTENDED HIS FIRST IETF MEETING IN 1989, IT comprised 150 people who were mostly researchers, operators, and vendors from the United States. At IETF 91 in Honolulu, Baker mingled with more than 1,000 attendees, including a Nigerian ccTLD operator. In a wide-ranging interview, Baker reminisced about how the IETF has changed during the past 25 years. Following are excerpts from that conversation.

Question: How was your first IETF meeting?

Fred Baker: My first IETF meeting was IETF 14 at Stanford University in June 1989. I worked for Vitalink, which made what today we might call a remote ethernet switch. I had started working on a router product. I was designing a proprietary SPF-based protocol, and an employee suggested I look into the IETF's protocol. About that time, I got a long flame from a government customer who told me in no uncertain terms that the IETF and IETF protocols including OSPF [Open Shortest Path First] and PPP [Point-to-Point Protocol] needed to be on my roadmap. I had an employee and a customer saying the IETF was important, so I showed up. IETF 14 had maybe 150 people. It was located in the basement of one of Stanford's buildings, and I think the first meeting fee was $25.

Q: What were some of the key differences between then and now?

FB: At IETF 15 in Honolulu, I tried to walk into the Open Systems Routing Working Group meeting. I was met at the door by a woman who I assumed was the chair. She told me I wasn't welcome, that it was an invitation-only meeting. That was a wake-up call for me, and it colored my participation in the IETF for a while. I was very aware of being on the outside looking in, the disliked competitor to all who sat in the room. One key difference between then and now is the openness of the process.

I dropped in on two meetings, one a BoF [Birds of a Feather] regarding the SNMP

Fred Baker at IETF 89

> **Back then, there was far more willingness to shoot from the hip. People would write up an Internet Draft, implement it, and then put it in a network. Sometimes really bad things would happen, but improvements often happened rapidly.**

MIB [Simple Network Management Protocol Management Information Base] and one on PPP. I came home from IETF 15 with two writing assignments. So there was also acceptance based on willingness to work.

Back then, there was far more willingness to shoot from the hip. People would write up an Internet Draft, implement it, and then put it in a network. Sometimes really bad things would happen, but improvements often happened rapidly. In my opinion, now it takes far too long to publish an RFC [Request for Comments]. What we really want is a happy medium.

Q: How did you go from being an outsider to chair?

FB: By November 1990, I was working at ACC, a company that built IP [Internet Protocol] routers. After that, I don't recall the strong feeling of being an outsider. Dave Crocker asked me to chair the

802.1d Bridge MIB Working Group, which was contentious. I chaired several working groups: ISDN [Integrated Services Digital Network] MIB; DS1/DS3 MIB and PPP Extensions. Someone figured out that I could chair a working group that was contentious and get results. In 1993, I chaired the Nomcom. Truth be told, in that, we were making it up as we went along. I was, of course, also doing technical work. I published 14 RFCs between 1989 and 1996.

In 1995, the Nomcom asked me to consider being the chair of the IETF. I was working at Cisco by then. Cisco told me that they would give me the leeway and financial support to do that and would back me up on my technical work. They asked only one thing: wherever my travels took me, they wanted me to be willing to talk with a customer. It seemed like a fair deal. I served in that capacity for five years. One thing I concluded is that term limits are a good thing. I was exhausted and more than willing to hand the role to the next person, whom I had been mentoring. I stayed on the IAB [Internet Architecture Board] until March 2002.

Q: What were the highlights of your tenure as IETF chair?

FB: In 1996, the IETF was pretty much the Wild West. In a certain sense, it still is. One big thing that was happening during that interval was the IETF coming of age. When I first showed up, it was 150 people, largely US researchers, but also people in

uniform, a few operators, and a few vendors. By December 2000, we had almost 3,000 people in San Diego, California, including college kids, the press, and drop-ins.

We also were starting to get on the radar at the White House. I remember meeting with a guy who worked at the equivalent of the Office of Science and Technology Policy. Our November 1999 meeting in Washington, DC, culminated in a huge discussion about wiretapping that had gone on for about a year and a half. Only about 40 percent of the messages on the Raven mailing list were from IETF people.

Another change is that we were starting to have meetings outside the United States. The first one was a happy accident. Microsoft planned to host a meeting in August 1990 in Redmond, Washington, that fell through. The University of British Columbia said they would host it, so we went 80 miles north. The next meeting outside the United States was in Amsterdam in 1993. Then we went to Stockholm in 1995, Montreal in 1996, Munich in 1997, Oslo in 1999, and Adelaide, Australia, in 2000. I thought internationalization and the willingness to go Down Under were a question of fairness to the people doing the work of the IETF.

Q: How have you been involved with the IETF since your term ended as chair?

FB: In large part, it has been technical work. I have published 54 RFCs and have 11 drafts in the mill. Organisationally, I served on the Internet Society Board from 2002 to 2008, the first four years of which I was chair. The Internet Society was changing dramatically as well. By 2002, it had organisational members that provided money and held power, chapter members who often felt disenfranchised by the Internet Society's financial woes, and individual members like myself who had little or no voice. I presided over the middle stages of change, and the recent reorganisation of the Internet Society bylaws finalized it. I think the Internet Society has

largely become what it needs to be, but still has some work ahead in terms of its consultation process.

I served on the IAOC [IETF Administrative Oversight Committee]—essentially the finance department of the IETF—at the request of the IETF from 2005 to 2010. I'm still on the IAOC's meetings committee. I cochaired two working groups: IEPrep and v6ops, and chaired the RSOC [RFC Series Oversight Committee], which was tasked with finding a new RFC Editor.
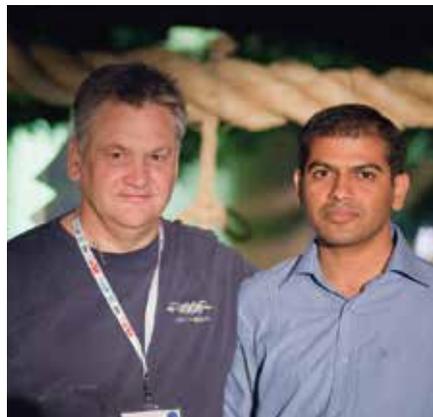
Fred Baker at IETF 76, in his role as mentor for the Internet Society Fellowship to the IETF programme

I have been involved with the IETF policy and technical fellowship programs from the beginning. They serve important roles in connecting the great wide world and the IETF. We have been able to provide education for regulators, which is important, and improve relationships with the operators and regulators who have participated. At the recent IETF meeting in Honolulu, I spoke with a woman from Nigeria and put her in contact with a person from the US Federal Bureau of Investigation who is familiar with Boko Haram and some of the issues in her country. Helping her understand the processes in the Internet was important to her job.

Q: What are some of the lessons you learned from your experiences with the IETF?

FB: If there is one thing that I have observed about the IETF from 1989 until

> I have been involved with the IETF policy and technical fellowship programs from the beginning. They serve important roles in connecting the great wide world and the IETF.

now, it is that a lot of people seem to be willing to think the worst of each other, or at least make statements to that effect. But I have found few who actually deserve that. Personal integrity goes a long way, and the people who serve in the IETF are usually examples of that kind of integrity, regardless of their quirks.

The IETF needs to think about its tone. It's not that I feel we shouldn't have knock-down, drag-out arguments if we need to have them. But we need to be a little more respectful. People need to be more accepting of each other's differences.

I do consider our open process and the accessibility of our documents—working and RFCs—to be the gold standard. But that gold doesn't shine as brightly as it needs to. In 1990, I chafed that it might take as many as six months to move a document from an Internet Draft to an RFC. Right now, I have a document in the mill that hasn't seriously changed since 2013 and is now languishing in the area director's in-basket. If we want to remain the gold standard, we need to deliver working documents with supporting prototype reference code in a finite and predictable period of time.

I also think the IETF needs to have a better working relationship with the Internet Society, which has a history of putting the IETF first, even when it was within a couple weeks of bankruptcy. The IETF has very much been a beneficiary of the Internet Society. ◆◇◆

WIFI PRIVACY TRIALS AT IETF 91 AND IETF 92

By Juan Carlos Zuniga

PRIVACY AND SECURITY ISSUES HAVE BECOME PRIORITY ITEMS FOR THE IETF, the Internet Architecture Board (IAB), and the Internet Society. Documents such as RFC 7258 and the recent IAB Statement on Internet Confidentiality (see page 3) demonstrate the community's commitment to addressing the issues and concerns raised. The goals are to fix existing Internet technologies and protocols, and to develop more-secure solutions to protect users' privacy.

Although the IETF is taking major actions on several fronts and via a host of working groups, its privacy and security efforts don't stop there. Coordination and collaboration with other standards organisations on the development of Internet technologies is a necessary next step to providing coherent solutions to today's privacy and security issues. One of the most important standards organisations is the Institute of Electrical and Electronics Engineers (IEEE), which has developed several technologies at the core of Internet connections, including IEEE 802.1 bridges, IEEE 802.3 Ethernet, and 802.11 WLAN (wireless local area network, a.k.a., WiFi).

> **Because MAC addresses, in most cases, are globally unique identifiers that can be associated to personal devices, they can become privacy risks by exposing users to unauthorized tracking.**

As part of coordinated efforts between these organisations, a joint collaboration between the IETF and the IEEE has been established and an IEEE 802 Privacy Executive Committee Study Group was created in July 2014. The group is assessing privacy issues related to IEEE 802 technologies and is planning to develop recommended practices for all IEEE 802 protocols.

One of the privacy issues identified by the group so far relates to the use of media access control (MAC) addresses in over-the-air communications. Protocols such as IEEE 802.11 WLAN openly transmit MAC addresses in several messages. Because MAC addresses, in most cases, are globally unique identifiers that can be associated to personal devices, they can become privacy risks by exposing users to unauthorized tracking.

A possible solution to this tracking issue is the use of randomized MAC addresses. Although it seems like a straightforward thing to do, several implications should be studied. MAC addresses are not only used in link-layer (i.e., layer-two) communications, but also in different higher-layer protocols, such as Dynamic Host Configuration Protocol (DHCP), Internet Protocol Version 6 Neighbor Discovery (IPv6 ND), and Address Resolution Protocol (ARP). In order to assess the implications of MAC address changes in an operating network, an experiment was suggested in which certain individuals randomized their MAC addresses while connecting to the meeting network during IETF 91 in Honolulu.

For this experiment, the first of its kind outside of a lab, a parallel network was established and a different WiFi service set identification (SSID) was broadcast during the meeting. Experiment participants were

> **Since more details and statistics are needed to continue the analysis, the group is fine-tuning the experiment for further exploration in March 2015 at both the IEEE 802 plenary meeting in Berlin and the IETF 92 meeting in Dallas.**

asked to run scripts on their computers to randomize MAC addresses when connecting to the network. The network was isolated from the rest of the IETF meeting via a different virtual local area network (VLAN) and a separate DHCP address pool. Preliminary observations indicated that several client drivers supported this technique, no major changes were required on the network configuration, and the probability of address duplication in a network of this size was negligible. Since more details and statistics are needed to continue the analysis, the group is fine-tuning the experiment for further exploration in March 2015 at both the IEEE 802 plenary meeting in Berlin and the IETF 92 meeting in Dallas. In addition, the group is developing tools to enable more users to participate in the experiment, this time also with mobile devices. All those attending IETF 92 are encouraged to participate.

MAC randomization is just one way to improve Internet privacy for nontechnical users. Watch for more collaboration and more proposals from the community in the near future.

IRTF UPDATE

By Lars Eggert
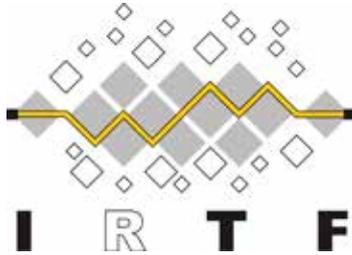
DURING IETF 91 IN HONOLULU, FOUR OUT OF THE EIGHT chartered Internet Research Task Force (IRTF) research groups (RGs) held meetings:

- Information-Centric Networking (ICNRG)
- Internet Congestion Control (ICCRG)
- Software-Defined Networking (SDNRG)
- Network Coding (NWCRG)

In addition to the meetings of already-chartered research groups, a proposed research group on Datacenter Latency Control (DCLCRG) held its second public meeting.

Another proposed research group, Network Function Virtualization (NFVRG), also held a public meeting. They subsequently held an interim meeting at the IEEE Globecom conference in Austin, Texas, in December 2014. Following both of these successful meetings, the NFVRG was officially chartered in January 2015; its charter page and additional information is available at https://irtf.org/nfvrg.

Prior to IETF 91, the Global Access to the Internet for All (GAIA) research group was also chartered. GAIA did not meet at IETF 91, but instead held two interim meetings: October 2014 in Cambridge, UK, and December 2014 with the Association for Computing Machinery Symposium on Computing for Development (ACM DEV) conference in Berkeley, California. GAIA will meet again at IETF 93 in Prague.

Since IETF 90, no new Request for Comments (RFCs) were published on the IRTF RFC Stream. This is not unusual.

At the IRTF Open Meeting at IETF 91, the final three winners of the third Applied Networking Research Prize (ANRP) of 2014 presented their research (see page 19).

- Sharon Goldberg discussed threats when BGP RPKI authorities are faulty, misconfigured, compromised, or compelled to misbehave.
- Misbah Uddin talked about matching and ranking for network search queries to make operational data available in real time to management applications.
- Tobias Flach presented novel loss recovery mechanisms for Transmission Control Protocol that minimize timeout-driven recovery.

The nominations period for the 2015 Applied Networking Research Prize (ANRP) awards closed in October 2014. The ANRP is awarded for recent results in applied networking research that are relevant for transitioning into shipping Internet products and related standardization efforts. There were 39 eligible submissions, out of which the selection committee picked five award winners for 2015. The five winners for 2015 will present their work at the three IRTF Open Meetings during the year.

Stay informed about these and other happenings by joining the IRTF discussion list at www.irtf.org/mailman/ listinfo/irtf-discuss.

INTERNET SOCIETY FELLOW TO THE IETF BRINGS LESSONS LEARNED BACK TO KENYA

By Carolyn Duffy Marsan

THANKS TO THE INFORMATION AND GUIDANCE HE RECEIVED AS A Technical Fellow at IETF 91 in Honolulu, Mwendwa Kivuva, information and communications technology administrator at the University of Nairobi, is now deploying IPv6.

Kivuva, who is also a member of the Consolidated Regional Internet Registries IANA Stewardship Proposal (CRISP) team, gained additional perspective at the meeting on the IANA transition.

Mwendwa Kivuva, one of the IETF 91 Internet Society Fellows to the IETF

Kivuva was one of 11 fellows at IETF 91. The Internet Society Fellowship to the IETF programme provides financial support for Internet technologists from emerging economies to attend IETF meetings, exchange ideas, enhance their participation in open-Internet standards development, and network with individuals from around the world with similar technical interests. The programme raises global awareness about the IETF and develops future leaders from underrepresented countries.

"Attending the IETF meeting [also] gave *me* perspective," Kivuva said. "I understood clearly the eight work areas and the working groups in each area. It was great to connect with the people who make the Internet what it is today. Initially, I wondered if I needed special training to effectively work on drafts, but I soon learned that participation becomes more effective as time goes by."

He notes that the financial support was key. "I am grateful to the Internet Society for the opportunity."

As a leading network engineer in Kenya, Kivuva was an ideal choice for the Fellowship programme. At the University of Nairobi, his work involves designing, implementing, and managing network infrastructure with a focus on security and performance. He serves as secretary general of the Internet Society's Kenya Chapter and participates in several Internet Corporation for Assigned Names and Numbers working groups. He also moderates discussions via the Kenya ICT Action Network.

Kivuva attended the newcomers' meeting, as well as meetings related to the working groups that he follows: IPv6 Maintenance (6man), IPv6 Operations (v6ops), Domain Name System Operations (dnsop), and Planning for the IANA/NTIA Transition (ianaplan).

"I realized I was stretching myself by participating in so many working groups. Going forward, I'll concentrate on only two or three working groups, then increase my engagement as I become more adept in IETF work," Kivuva said. "Since meeting people in my domain, I have a good grasp on how to participate more effectively and look forward to contributing to the mailing lists."

Kivuva was thankful for the mentorship of Fred Baker during the IETF meeting. "I liked the mentoring programme," he said. "It helped newcomers prepare so it was easier to integrate during the actual meeting. Mentors also introduce newcomers to IETF people of interest, like chairs of working groups and area directors."

Kivuva plans to bring the lessons he learned back to the network engineering community in Kenya. "Other IETF fellows from my country and I plan to have mentorship sessions at local universities and [to educate] engineering and computer science students about the work of the IETF and how they can contribute to it," he said.

> **"Initially, I wondered if I needed special training to effectively work on drafts, but I soon learned that participation becomes more effective as time goes by."**
>
> **—Mwendwa Kivuva, Internet Society Fellow to the IETF**

Kivuva encourages the Internet Society to continue funding its Fellowship to the IETF programme. "Sponsoring IETF Fellows ensures that there is diversity in the IETF," Kivuva said. "More engineers from other areas of the world, not just Europe and America, need to be brought on board. The programme offers exposure to those in developing worlds who could otherwise never attend an IETF meeting or participate in drafts or mailing lists."

APPLIED NETWORKING RESEARCH PRIZE WINNERS ANNOUNCED

By Mat Ford

Sharon Goldberg, 2015 ANRP award winner

Tobias Flach, 2015 ANRP award winner

Misbah Uddin, 2015 ANRP award winner

THE APPLIED NETWORKING RESEARCH PRIZE (ANRP) IS awarded for recent results in applied networking research that are relevant for transitioning into shipping Internet products and related standardization efforts. The call for nominations for the 2015 ANRP award cycle received approximately 40 nominations. The following three ANRP awards were presented during IETF 91.

- **Sharon Goldberg** for discussing threats when Border Gateway Protocol Resource Certification (BGP RPKI) authorities are faulty, misconfigured, compromised, or compelled to misbehave.
  Full paper: http://www.cs.bu.edu/~goldbe/papers/hotRPKI.pdf.
  Slides: http://www.ietf.org/proceedings/91/slides/slides-91-irtfopen-4.pdf.

- **Tobias Flach** for the design of novel loss-recovery mechanisms for Transmission Control Protocol (TCP) that minimize timeout-driven recovery.
  Full paper: http://nsl.cs.usc.edu/~tobiasflach/publications/Flach_Latency.pdf.
  Slides: http://www.ietf.org/proceedings/91/slides/slides-91-irtfopen-3.pdf.

- **Misbah Uddin** for developing matching and ranking for network search queries in order to make operational data available in real time to management applications.
  Full paper: http://www.cnsm-conf.org/2013/documents/papers/CNSM/p251-uddin.pdf.
  Slides: http://www.ietf.org/proceedings/91/slides/slides-91-irtfopen-0.pdf.

Goldberg, Flach, and Uddin presented their findings to the Internet Research Task Force open meeting during IETF 91. Audio and video from the presentations is available thanks to Meetecho at http://recordings.conf.meetecho.com/Playout/watch.jsp?recording=IETF91_IRTFOPEN&chapter=chapter_0, start at 00:18:50.

2016 ANRP NOMINATIONS

The nomination period for 2016 will start in the summer of 2015.
Join the irtf-announce@irtf.org mailing list to be notified when it begins.

IETF ORNITHOLOGY: RECENT SIGHTINGS

Compiled by Mat Ford

GETTING NEW WORK STARTED IN THE IETF USUALLY REQUIRES A BIRDS-of-a-feather (BoF) meeting to discuss goals for the work, the suitability of the IETF as a venue for pursuing the work, and the level of interest in and support for the work. In this article, we'll review the BoFs that took place during IETF 91, including their intentions and outcomes. If you are inspired to arrange a BoF meeting, please be sure to read RFC 5434: Considerations for Having a Successful Birds-of-a-Feather (BoF) Session.

Deterministic Networking (detnet)

Description: Institute of Electrical and Electronics Engineers (IEEE) 802 has defined Audio Video Bridging, providing time synchronization and precise scheduling for zero congestion loss and finite latency in reserved Layer-2 streams. The need for equivalent Quality of Service (QoS) features now appears in networks that include, for example, routers in addition to or instead of bridges in industrial, vehicular, or public infrastructure applications. The goals of this meeting were to consider whether to form a working group in conjunction with the IEEE802.1TSN Task Group and to specify both how to get these QoS features into routers and how new and/or existing control protocols can be used to control these flows.

Proceedings: https://www.ietf.org/proceedings/91/minutes/minutes-91-detnet

Outcome: This meeting was not intended to form a working group. Discussion concluded with a call for a clearer statement of the problems that need to be addressed and a gap analysis to understand what, if anything, is missing.

> The need for equivalent Quality of Service features now appears in networks that include, for example, routers in addition to or instead of bridges in industrial, vehicular, or public infrastructure applications.

*Black swan
(Cygnus atratus)*

Archive Top Level Media Type (arcmedia)

Description: The purpose of this meeting was to discuss registering a top-level media type for file archives, i.e. formats that package files and file metadata into a single data stream.

Proceedings: https://www.ietf.org/proceedings/91/arcmedia.html

Outcome: Participants concluded that a charter should be drafted to proceed with this work, and that a draft charter would be discussed further on the Applications Area mailing list.

Bit Indexed Explicit Replication (bier)

Description: This BoF was to discuss a new architecture for the forwarding of multicast data packets. The goal is to provide optimal forwarding of multicast packets through a multicast domain without requiring either explicit tree-building protocols or intermediate nodes to maintain a per-flow state.

Proceedings: https://www.ietf.org/proceedings/91/bier.html

Outcome: The meeting provided a good overview of the current state of multicast and the nature of the problem to be solved; and input from operators was received. Further work on use cases and a clearer problem statement is needed before this can be chartered as an IETF working group.

> The goal is to provide optimal forwarding of multicast packets through a multicast domain without requiring either explicit tree-building protocols or intermediate nodes to maintain a per-flow state.

Abstraction and Control of Transport Networks (actn)

Description: The aim of this proposed work is to facilitate centralized operation and construction of virtual networks based on multisubnet, multitechnology, multivendor domain networks. The work could enable rapid service deployment of new dynamic and elastic services, and could improve overall network operations and scaling of existing services.

Proceedings: https://www.ietf.org/proceedings/91/minutes/minutes-91-actn

Outcome: The meeting included discussion of the problem-statement draft and options for architectural approaches. Polling at the end of the meeting indicated a lot of interest in this work and a reasonable number of folks willing to actively contribute. It is not clear whether there is new protocol work here that would require the formation of a working group.

Interface to Network Security Functions (i2nsf)

Description: This non-WG forming BoF discussed interfaces for clients (especially enterprises) to request, negotiate, operate, and/or verify network security functions not physically present at the requesters' premises. Those security functions, hosted by service providers or other third parties, can be instantiated on physical appliances, or as virtual machines instantiated on common computer servers.

**Proceedings:** https://www.ietf.org/proceedings/91/minutes/minutes-91-i2nsf

Outcome: The meeting covered a lot of ground and concluded that whilst there is probably something useful here to advance into a chartered IETF working group, more refinement is required to focus on a clearly articulated and well-defined activity. Discussion will continue on the mailing list.

Blue-and-yellow macaw
(Ara ararauna)

IETF 91 AT–A–GLANCE
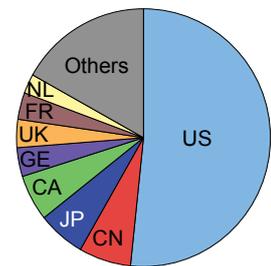
Participants: 1,100

Newcomers: 136

Number of countries: 50

**IETF Activity since IETF 90
(20 July–9 November 2014)**

New WGs: 12

WGs closed: 0

WG currently chartered: 135

New and revised Internet-Drafts (I-Ds): 1665

RFCs published: 86

• 45 Standards Track, 0 BCP, 3 Experimental,
  37 Informational

IESG Restructuring

In October 2014, the IESG announced plans to reorganise the IETF areas and working groups by summer 2015. Goals include:

• Match IETF structure to current topics

• Support growth in emerging topic areas

• Match management resources to workload

• Improve flexibility re fluctuations in workload and topics

IANA Activity since IETF 90 (July–October 2014)

Processed 1363+ IETF-related requests, including:

• Reviewed 111 I-Ds in Last Call and reviewed
  125 I-Ds in Evaluation

• Reviewed 82 I-Ds prior to becoming RFCs,
  44 of the 82 contained actions for IANA

Document collaboration with the IETF

• RFC 5226bis finished IETF Last Call on 30 October 2014.
  Authors are now addressing Last Call comments from the
  community. https://datatracker.ietf.org/doc/draft-leiba-cotton-
  iana-5226bis/.

SLA Performance (May–October 2014)

• Processing goal average for IETF-related requests: 99.5%

IANA and DNSSEC

• As of 4 November 2014, 548 TLDs have a full chain of trust
  from the root. http://stats.research.icann.org/dns/tld_report/.

**RFC Editor Activity since IETF 90
(July 2014–February 2015)**

Published RFCs: 167

• 134 IETF (13 IETF non-WG), 4 IAB, 1 IRTF, 15 Independent
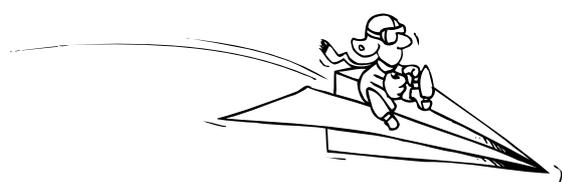
IETF MEETING CALENDAR

For more information about past and upcoming IETF meetings visit **www.ietf.org/**.

IETF 92

Date 22–27 March 2015

Host Google

Location Dallas, Texas, USA

IETF 93

Date 19–24 July 2015

Host TBD

Location Prague, Czech Republic

IETF 94

Date 1–6 November 2015

Host WIDE

Location Yokohama, Japan

IETF 95

Date 3–8 April 2016

Host TBD

Location Buenos Aires, Argentina

Special thanks for hosting IETF 91

CISCO

**The Internet Society Fellowship to the IETF,
as part of the Internet Society Next Generation
Leaders Programme, is sponsored by**

Afilias   Google

Microsoft   NBCUniversal