the IETF® Journal

Volume 10, Issue 1 • July 2014

Inside this Issue

*A report from IETF 89, March 2014, London, England. Published by the Internet Society in cooperation with the Internet Engineering Task Force**

From the Editor's Desk

By Mat Ford

The 89th meeting of the Internet Engineering Task Force was hosted by the Internet Corporation for Assigned Names and Numbers (ICANN). Our cover article in this issue highlights the challenges of making Internet connectivity available to all people around the globe. The Global Access to the Internet for All (GAIA) proposed research group is a new initiative hoping to find a home in the Internet Research Task Force—we wish them luck in their important work.

We have articles about the transport services Birds-of-a-Feather, a behind-the-scenes look at the team that organizes the pre-IETF educational tutorials, and the RFC series editor, Heather Flanagan, offers an update on the work to modernise the format of the RFC series.

We also include an article on the Internet Architecture Board (IAB)- and World Wide Web Consortium-hosted pre-meeting workshop on strengthening the Internet against pervasive monitoring, celebrate the most recent winners of the Applied Networking Research Prize, and document the Internet Society panel event on the evolution of the end-to-end principle.

As always, we have our regular columns from the IETF, IAB, and Internet Research Task Force chairs, and coverage of hot topics discussed during the plenary meetings. 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/IETF89.

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 www.internetsociety.org/publications/ietf-journal/ietf-journal-subscription.

Researching Global Access to the Internet for All (GAIA)

By Arjuna Sathiaseelan

The Internet has crossed new frontiers—access to it has gotten both faster and relatively cheaper, with novel applications and services being offered every day. As a result, today's Internet represents a critical infrastructure enabling remote health care, education, employment, e-governance, digital economy, social networks, and more. As such, Internet access should be

Continued on page 4

Message from the IETF Chair


Jari Arkko, IETF Chair

By Jari Arkko

For me and many others, IETF 89 started during the previous week with a workshop organised by the Internet Architecture Board (IAB) and the Word Wide Web Consortium (W3C) on improving privacy on the Internet. Similarly, as the IETF meeting was ending, several design team meetings and workshops were just getting started. It never ceases to amaze me how much energy our community has.

The London meeting was one of the best-attended IETF meetings in recent history. We had 1,400 participants on site and many more connected remotely. Participants came from 60 countries and a variety of backgrounds. In addition, the Internet Society's Public Policy Fellowship Programme, which brings policymakers and regulators to IETF meetings, had a record 30 participants, all very active.

The March meeting also saw changes in IETF leadership: Alia Atlas, Alissa Cooper, and Kathleen Moriarty joined the Internet Engineering Steering Group (IESG), and Mary Barnes, Ted Hardie, Joe Hildebrand, and Brian Trammell joined the Internet Architecture Board (IAB). Thank you all for volunteering, and many thanks also to the members who stepped down.

Each meeting holds something of interest to everyone. I found the following noteworthy:

- Topics related to strengthening the security and privacy of the Internet continue to draw attention. The pre-meeting STRINT workshop attracted 100 participants and more than 60 papers. More would have joined us, but there was no space. During the meeting, various working groups continued the discussion. The Using TLS for Applications (UTA) working group (WG), which was specifically created to address issues surrounding pervasive monitoring, had its first meeting. The Transmission Control Protocol Maintenance (TCPM) WG discussed a proposal to add opportunistic keying mechanisms directly onto the TCP protocol. And the Encryption of Domain Name System (DNSE) Birds-of-a-Feather (BoF) considered the possibility of adding confidentiality support to DNS queries. Finally, there is an ongoing effort to review old specifications for areas that might benefit from better privacy and data minimisation.
- Projects related to key components of the web platform continued. The Transport Layer Security (TLS) WG has been rechartered to work on TLS 1.3, a redesign of the TLS protocol that provides security and efficiency benefits. The Hypertext Transfer Protocol Bis (HTTPBIS) WG continued another redesign effort around HTTP 2.0, which may enable the use of TLS even for http uniform resource identifiers (URIs) and provide limited protection against passive attacks. Work on HTTP 2.0 is nearing completion.
- The WebRTC work on real-time communications from browsers continued. The group has deferred a controversial mandatory-to-implement video codec question, but is making excellent progress in all other areas.
- The IETF has worked on various aspects of the Internet of Things for years. A new proposal was discussed in the Authentication and Authorization for Constrained Environments (ACE) BoF, which addressed how to authorise different smart objects and their users to do the actions that they are allowed to do.

Continued on page 4

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


Russ Housley, IAB Chair

By Russ Housley

This is my third contribution to *The IETF Journal* as chair of the Internet Architecture Board (IAB). Pervasive monitoring and Internet governance were discussed in many sessions.

IAB Statement on Pervasive Monitoring

At IETF 88 in Vancouver, the IAB held a technical plenary in which pervasive monitoring was discussed. The IAB, like many others who attended the session, believes that pervasive monitoring represents an attack on the Internet. Their view is supported by the fact that, during such monitoring, large amounts of information that is intended to be confidential is gathered and aggregated by third parties. Such broad-scale attacks undermine public confidence in the Internet infrastructure, no matter the intent of those collecting the information.

In response, the IAB encourages individuals to take practical measures to limit pervasive monitoring within their environments.

The IAB, like many others who attended the session, believes that pervasive monitoring represents an attack on the Internet. Their view is supported by the fact that, during such monitoring, large amounts of information that is intended to be confidential is gathered and aggregated by third parties.

Strengthening the Internet (STRINT) Workshop

The IAB and World Wide Web Consortium (W3C) held a workshop called Strengthening the Internet Against Pervasive Monitoring (STRINT)[1] in London on 28 February 2014. The workshop assembled 100 participants and was supported by the EU FP7 STREWS project[2]. Discussions covered terminology, the role of user interfaces, classes of attack mitigation, specific use cases, and transition strategies. The workshop ended with a few high-level recommendations outlined in the report at https://datatracker.ietf.org/doc/draft-iab-strint-report.

Sessions at IETF 89

During IETF 89, the IAB hosted two sessions. The first, rfcform, gathered input from the community for the RFC Series Editor on the proposed publication of RFCs in formats other than plain text. The second, igovupdate, gathered input from the community on the evolution of the IANA protocol parameter registries.

First-hand comments confirm that ICANN's administration of the protocol parameter registry functions works well for both the Internet and the IETF. We are pleased with the publication and maintenance of the protocol parameter registries and with the coordination of the evaluation of registration requests through the IANA function provided by ICANN.

Continued on page 5

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.

Researching Global Access to the Internet for All (GAIA), continued

universal in terms of availability and ability to contribute to the wider community, thereby enabling true digital inclusion to all.

Although this vision is shared among both major stakeholders and global governments, the reality of today's Internet and its level of digital inclusion is confronted by a growing digital divide—increasing geographic and socioeconomic challenges between those with sufficient access to the Internet and those who cannot afford access to its services.

Geographic Challenges

Access problems often occur with sparsely spread populations in physically remote locations—it is simply not cost effective for Internet service providers (ISPs) to install the required infrastructure for broadband Internet access to these areas. Coupled with the physical limitations of terrestrial infrastructures (mainly due to distance) to provide last mile access, remote communities using wired technologies also incur higher costs for connection between the exchange and backbone network because the distances are larger. A large exchange may accommodate many users and allow for competition between service operators; in contrast, a rural/remote broadband often does not offer economies of scale, and raises the costs per user. Most important, in many developing countries, poor connectivity between ISPs is so prevalent that local traffic is routed over expensive international links in an effort to ensure that it successfully reaches even destinations within the country of origin.

These kinds of geographic challenges motivate questioning the way we do things, such as insisting on end-to-end delivery, versus promoting more localized communication. The result is a socioeconomic obstacle: mainstream business models don't work.

Socioeconomic Challenges

Addressing digital exclusion due to socioeconomic barriers is critically important. The United Nations revealed the vast global disparity in fixed broadband access by showing that in some countries the access to fixed broadband costs almost 40 to 100 times the national average income. This problem is also applicable to developed countries where individuals are unable to pass a necessary credit check or are living in circumstances that are too unstable to commit to lengthy broadband contracts.

[T]he reality of today's Internet and its level of digital inclusion is confronted by a growing digital divide—increasing geographic and socioeconomic challenges between those with sufficient access to the Internet and those who cannot afford access to its services.

There are both research and policy challenges to the realization of a future Internet capability that offers appropriate access to all parts of society. It will require proactive collaboration and a shared vision among researchers, corporations, community groups, and governments, as there can be no single solution that is enforced on all types of users in all locations.

Global Access to the Internet for All

The proposed IRTF Global Access to the Internet for All (GAIA) research group aims to:

1. Create maximum visibility and interest among the community on

Continued on page 6

Message from the IETF Chair, continued

- Internet governance has been a hot topic around the world—at the IETF we are focused on technology, but we also care that governance associated with the Internet is both stable and reliable. In addition, we are directly impacted by the protocol parameters registry function at the Internet Assigned Numbers Authority, which records all the assignments of protocol-related constants. At the IGOVUPDATE session, Olaf Kolkman spoke about the protocol parameters registry, its evolution, and the principles under which the IAB has guided this evolution. After some amendments, the room voted unanimously to continue to operate under these principles.
- Network node configuration is becoming increasingly dominated by Network Configuration Protocol (NETCONF)/YANG-type solutions rather than Simple Network Management Protocol (SNMP)-based solutions. The Internet Engineering Steering Group (IESG) issued a statement to make sure WGs take note of this.
- As an open organisation, anyone can join IETF discussions. While this is a good thing, it can present challenges. A recent discussion on our mailing list raises the question of how to deal with repetitive postings and impolite messages.

After each meeting, these and other topics continue to be discussed on our mailing lists. Join the discussions at www.ietf.org.

Finally, many thanks to our host, ICANN, as well as to BT for our connectivity, and to Comcast for sponsoring the welcome reception.

Session discussions led to the following guiding principles for IAB efforts that impact IANA protocol parameter registries. These principles must be taken together; their order is not significant.

1. **The IETF protocol parameter registry function has been and continues to be capably provided by the Internet technical community.**

   The strength and stability of the function and its foundation within the Internet technical community are both important given how critical protocol parameters are to the proper functioning of IETF protocols.

   We think the structures that sustain the protocol parameter registry function needs be strong enough that they can be offered independently by the Internet technical community, without the need for backing from external parties. And we believe we largely are there already, although the system can be strengthened further, and continuous improvements are being made.

2. **The protocol parameter registry function requires openness, transparency, and accountability.**

   Existing documentation of how the function is administered and overseen is good [RFC 2860, RFC 6220]. Further articulation and clarity may be beneficial. It is important that the whole Internet community can understand how the function works, and that the processes for registering parameters and holding those who oversee the protocol parameter function accountable for following those processes are understood by all interested parties. We are committed to making improvements here if necessary.

3. **Any contemplated changes to the protocol parameter registry function should respect existing Internet community agreements.**

   The protocol parameter registry is working well. The existing Memorandum of Understanding [RFC 2860] defines "the technical work to be carried out by the Internet Assigned Numbers Authority on behalf of the Internet Engineering Task Force and the Internet Research Task Force." Any modifications to the protocol parameter registry function should be made using the IETF process to update RFC 6220 and other relevant RFCs. Put quite simply: evolution, not revolution.

4. **The Internet architecture requires and receives capable service by Internet registries.**

   The stability of the Internet depends on capable provision of not just IETF protocol parameters, but IP numbers, domain names, and other registries. Furthermore, DNS and IPv4/IPv6 are IETF-defined protocols. Thus we expect the role of the IETF in standards development, architectural guidance, and allocation of certain name/number parameters to continue. IP multicast addresses and special-use DNS names are two examples where close coordination is needed. The IETF will continue to coordinate with ICANN, the RIRs, and other parties that are mutually invested in the continued smooth operation of the Internet registries. We fully understand the need to work together.

5. **The IETF will continue management of the protocol parameter registry function as an integral component of the IETF standards process and the use of resulting protocols.**

   RFC 6220 specifies the role and function of the protocol parameters registry, which is critical to IETF standards processes and IETF protocols. The IAB, on behalf of the IETF, has the responsibility to define and manage the relationship with the protocol registry operator role. This responsibility includes the selection and management of the protocol parameter registry operator, as well as management of the parameter registration process and the guidelines for parameter allocation.

6. **The protocol parameters registries are provided as a public service.**

   Directions for the creation of protocol parameter registries and the policies for subsequent additions and updates are specified in RFCs. The protocol parameters registries are available to everyone, and they are published in a form that allows their contents to be included in other works without further permission. These works include, but are not limited to, implementations of Internet protocols and their associated documentation.

Highlights since IETF 88

The IAB published RFC 7101,[3] "List of Internet Official Protocol Standards: Replaced by a Web Page."

The IAB published RFC 7094,[4] "Architectural Considerations of IP Anycast."

The IAB appointed two people to the ICANN Technical Liaison Group: Warren Kumari for a two-year term and Daniel Migault for a one-year term.

References

1. www.w3.org/2014/strint/
2. www.strews.eu/
3. www.rfc-editor.org/rfc/rfc7101.txt
4. www.rfc-editor.org/rfc/rfc7094.txt

Researching Global Access to the Internet for All (GAIA), continued

the challenges in enabling global Internet access.

2. Create a shared vision among researchers, corporations, and non-governmental and governmental organisations on the challenges.
3. Articulate and foster collaboration among them to address the diverse Internet access and architectural challenges.
4. Document and share deployment experiences and research results to the wider community through scholarly publications, white papers, and Informational and Experimental RFCs, etc.
5. Have a longer term vision on influencing standardisation efforts at the IETF that could potentially change the Internet landscape to be more inclusive.

Exploration Areas

Addressing the geographic challenges

In rural and remote areas, both the service requirements and the delivery mechanisms to customers are often different than those in cities. For instance, while cities might call for densely connected options for delivery, such as DSL and fibre optical lines, remote areas are likely to rely more on wireless-based access to the Internet via wireless mesh, satellite, or TV white space options to bridge distances not seen in cities.

The reluctance of economically motivated network operators to provide wired and cellular infrastructures to rural/remote areas has led to several community led initiatives to build large-scale, self-organized, and decentralized community wireless networks that use WiFi mesh technology due to the reduced cost of using the unlicensed spectrum. These community wireless mesh networks have self-sustainable business models, which provide more localised communication services, as well as Internet backhaul support via peering agreements with traditional network operators who see such networks as a way to extend their reach at a lower cost. There also are community-led wireless initiatives such as crowd-shared wireless networks, in which home broadband owners share a portion of their home broadband with friends, neighbours, or other users either for free or as part of a service offering by the ISP.

The ability of the satellite to provide global coverage makes satellites a key enabling technology to provide broadband access and to gather and deliver critical information to areas and locations that cannot be reached by other wired or wireless technologies.

Recent years have also seen a rise in innovative ways of providing broadband Internet access via dynamic spectrum sharing, including the successful TV white space (TVWS) trials in Malawi, Kenya, and South Africa, which use the white spaces left by the termination of analog TV broadcasting, and which hold promise as an access technology for providing long-distance wireless broadband Internet access. In addition, companies such as Facebook and Google are exploring ways to connect remote communities via unmanned aerial vehicles (UAVs) and balloons.

Finally, satellite technology is being viewed as a key access technology to provide ubiquitous Internet access. The ability of the satellite to provide global coverage makes satellites a key enabling technology to provide broadband access and to gather and deliver critical information to areas and locations that cannot be reached by other wired or wireless technologies. The two-way satellite market has undergone dramatic changes over the last 10 years in terms of IP adoption, coupled with the move to higher capacity Ku/Ka bands. The satellite industry can now provide a lower-cost "broadband" IP-based service that was not possible only a few years ago. Low-earth-orbit satellites, such as Cubesats and Picosats, can now be launched into orbit to provide a communications infrastructure (especially for emergency communications) at a relatively lower cost.

GAIA will explore and document the diverse set of characteristics and integration challenges of these technologies via measurement studies and deployment experiences. GAIA will also explore the regulatory and political obstacles of deploying some of these access technologies (e.g., spectrum regulation), as well as the challenges in deploying Internet Exchange Points (IXPs) in developing regions.

A Common Platform

GAIA will take a longer-term approach to exploring new architectures that would make the Internet more flexible and accessible. We hope to use well-researched practices, results, and working platforms from related IRTF groups in key networking areas, such as Delay Tolerant Networking (DTN) including Opportunistic Communications, Information Centric Networking (ICN) and Software Defined Networking (SDN) to explore innovative architectures that will enable new methods of access to Internet services over a wide range of connectivity options at lower cost and better efficiency in terms of performance, network utilisation, and energy.

GAIA will enable an inclusive vision, in which multiple transmission technologies, novel architectures, and new access models are integrated into a single platform. Such connectivity inclusion

GAIA will enable an inclusive vision, in which multiple transmission technologies, novel architectures, and new access models are integrated into a single platform. Such connectivity inclusion has the potential to reduce transmission costs and increase efficiency, flexibility, and dependability, and the common platform will help overcome any socioeconomic obstacles to economically sustainable global access for all.

has the potential to reduce transmission costs and increase efficiency, flexibility, and dependability, and the common platform will help overcome socioeconomic obstacles to economically sustainable global access for all.

Addressing the socioeconomic challenge

Internet access can be made more affordable by coupling social and economic incentives with a common platform that enables these incentives to spur innovation for a wide range of new business models: more-localized communications, opportunities for nongovernmental organizations and local governments (driven by social rather than economic goals) to become virtual network operators, revenue creation from currently underutilized infrastructures, time-shifted services, and micropayments and reverse payment models (e.g., remote doctors pay for more capacity or Quality of Service to video conference patients). To promote some of these new models, we need to address both technological and regulatory/policy challenges (e.g., net neutrality and tiered services).

It is important to emphasize that there also is room for innovation and experimentation in policy. The major obstacles to more persistent and affordable access in sub-Saharan Africa, parts of Asia, the Middle East, and other regions are not technological but regulatory. We need to create a regulatory space for new business models and wireless technologies that also requires innovation.

The diversity of its members help make GAIA a suitable forum in which to discuss, collaborate, and disseminate the aforementioned issues.

Next Steps

Today, the GAIA group has more than 100 members. Its mailing list is at http://irtf.org/mailman/listinfo/gaia.

The first GAIA meeting was held at the IETF 89 meeting in London. It included several presentations from members (academia, industry, and nongovernmental organisations) that showcased the diversity of problem areas, projects, and solutions. The next GAIA meeting will be collocated with ACM DEV 5 in December 2014.

The group is currently finalising the topics of interest, and will ask to be formally chartered by the IRTF next year. Members aim to keep the proposed charter as more exploratory considering the diverse set of challenges that need to be addressed.

Internet Society Panel: Evolution of the Internet's End-to-End Architecture

By Carolyn Duffy Marsan

On 4 March, concurrent with the IETF 89 meeting in London, the Internet Society held a panel discussion about the Internet's underlying end-to-end principle—and whether it's worth retaining.

The end-to-end principle, which is defined as smart endpoints and a dumb network, has been a guideline for Internet engineers for decades. The principle originated from the idea that it was best not to put too much functionality in a communications network, and instead to implement functionality in applications residing at the endpoints. Over the years, the Internet's end-to-end principle also proved valuable in maintaining openness, increasing reliability, and enabling new service development.

Leslie Daigle, chief Internet technology officer for the Internet Society, opened the discussion by questioning whether or not the end-to-end principle can survive in an era of pervasive monitoring.

"Revelations of pervasive monitoring, and any number of reactions to these revelations, may or may not take us in directions that are less than optimal for the end-to-end principle, such as the drive for localization of data for services

Audience members at the Internet Society Panel discussion

Continued on next page

Internet Society Panel: Evolution of the Internet's End-to-End Architecture, continued

Fred Baker, Cisco Fellow and former IETF chair

that are meant to be global or madly encrypting everything, everywhere, all of the time," Daigle said.

She opened the discussion by asking a panel of experts: "Does the end-to-end principal matter in today's Internet and going forward? If the answer is yes, and I heartily hope it is, how does it matter?"

Fred Baker, a Cisco Fellow and former IETF chair, argued that the Internet has never been a truly dumb network.

"When the application gives the network an address and says, 'Please send this parcel of information over there,' it doesn't tell the network how to get it there. The network is presumed to have the intelligence to get it there," Baker explained.

He argued that what the end-to-end principle defines is a system in which a lower layer of the network should always do what the upper layer expects it to do. He added that the end-to-end principle should be violated only if there is good reason with measurable benefit.

"I don't think it's fair to call the network stupid, but I also don't want it to be smart," Baker said. "The statement of the end-to-end principle as I would understand it is that the network should be predictable. It should do what I expect it to do."

Having a predictable network benefits both network operators and users, Baker explained. It enables network operators to route traffic in the manner that they prefer and to fix problems as they occur. It also allows users to accomplish their tasks.

"The network might be behaving intermittently, where sometimes I can get a packet through and sometimes I can't. That causes users to call somebody," Baker said. "That's the case we don't want to happen. If I'm an operator, and I'm trying to run a network, that costs me money. If I'm a user, and I'm trying to get a file from here to there, then I'm unable to do what I set out to do."

"I don't think it's fair to call the network stupid, but I also don't want it to be smart," Baker said. "The statement of the end-to-end principle as I would understand it is that the network should be predictable. It should do what I expect it to do."

—Fred Baker, Panelist

Baker says one challenge on the horizon for the end-to-end principle is when carriers treat their Internet capacity as a private resource, what he refers to as "walled gardens." This trend decreases interoperability, he warned. However, he said one positive shift is the pressure carriers feel to simplify their networks and adopt IPv6.

Andrew Sullivan, an IAB member and Dyn principal architect, said the end-to-end principle is a challenge for Internet infrastructure companies that provide DNS or email services to corporate customers by deploying smart middle boxes inside what is supposed to be a dumb network.

Infrastructure operators "rely on this predictable network," Sullivan said. "But we also have to alter network behavior based on the user because our customers are only going to buy stuff from us if it is roughly as good as if they were running it themselves. We don't want to put something at every point of presence because the whole point of this is that we're going to make money based on the economies of scale. We end up having to modify network behavior. The difficulty is there are a lot of us, and we're all doing it at once."

Sullivan said he is hoping the Internet engineering community will create protocols that improve how infrastructure operators modify network behavior.

"One thing that I hope will emerge, although this might be wishful thinking, is that we develop protocols that give enough hints that we can do the stupid DNS or email tricks in the

Andrew Sullivan, panelist, IAB member, and Dyn principal architect (foreground)

Harald Alvestrand, panelist and former IETF chair

> "I have to extend trust to the network and to some degree do it blindly. I will extend the absolute minimum amount of trust that I can get away with. I will take resources I can get away with. And if I don't get the network behavior I'm expecting, I will do what it takes to make things work."
>
> —Harald Alvestrand, Panelist

middle without being really harmful," Sullivan said. "But we need protocols that allow you to make intelligent decisions in the middle and allow the infrastructure to give different kinds of tailored responses in an effort to make that experience as good as possible and make the latency as low as possible."

Sullivan pointed out that today's Internet applications don't operate according to the assumptions that were in place when the end-to-end principle originated. He explained that applications are no longer using a client/server model, where there are clear endpoints with a network in between. Instead, Internet applications are stitched together on-the-fly from components scattered around the network.

"The network needs to be able to stitch the stuff together or you don't have an application at all," he added.

Harald Alvestrand, a former IETF chair who works for Google, said the end-to-end principle is challenging for applications because they don't have a direct relationship with the network. Instead, they have direct relationships with users and their own backend resources.

"For an application, the network is not my friend," Alvestrand said. "None of the operators have my wellbeing at heart… and none are under my control. But I depend on the network infrastructure to reach my customers. If the network goes away, I have no purpose in life."

Alvestrand explained that applications use the network in an end-to-end fashion, but that involves traversing over a network that it doesn't control.

"I have to extend trust to the network and to some degree do it blindly," he said. "I will extend the absolute minimum amount of trust that I can get away with. I will take resources I can get away with. And if I don't get the network behavior I'm expecting, I will do what it takes to make things work. If I could wish for what the network would do for me, me being an application, I would wish for consistency that at least if things go haywire, let them go wrong in only one way."

> Sullivan said he is hoping the Internet engineering community will create protocols that improve how infrastructure operators modify network behavior.

ISOC Panel audience members

Going forward, Alvestrand recommended that the network use the end-to-end principle to remain simple.

"From the application perspective, I want to extend trust to the minimal amount possible and deliver a service to the user because that is my purpose," Alvestrand said.

All of the panelists asserted that the end-to-end model is important for future protocol development.

The end-to-end model as an enabler of a predictable network "is terribly important because the network operators can't deliver a service they can sell if that's not true," Baker summarized.

Alvestrand said the principle helps hold back the floodgates of complexity and keep the network as simple as possible.

"We need to make it happen in practice because it's one of the guidelines for protocols and services," Alvestrand said. "If you can't elucidate the specific function for what the ends are, your design is wrong."

Sullivan added that end-to-end is a pragmatic principle. "I think the economic pressure is there to keep this as one of the core principals of how we build this network," Sullivan said.

Getting Educated: Meet the IETF Edu Team

By Mirjam Kuehne

Most people have heard of, or perhaps even attended, the tutorials that take place the Sunday before each IETF meeting. But few know that it is the all-volunteer IETF Edu Team that decides which tutorials are provided and how they are organised. Following is a sneak peek at the team behind the tutorials.

The goals of the IETF Edu Team are stated in its charter:

The Education (Edu) Team manages the internal educational activities of the IETF with the goal of improving the effectiveness of IETF operations. We strive to improve the effectiveness of IETF leaders and participants by offering training sessions and educational materials that clarify their roles and responsibilities and prepare them to be more effective in their roles.

To fulfill the goals of the charter, the team offers two types of tutorials:

1. Process-oriented tutorials, such as newcomers tutorials, tutorials on how to use IETF tools, and tutorials on how to write an RFC.
2. Technical tutorials, such as tutorials on those technical topics widely relevant for IETF participants, including privacy, security, routing, and wireless. Specifically, the team aims for topics on which specialist knowledge might affect the work of multiple different working groups.

Anyone may suggest a tutorial. The IETF chair and IESG members propose tutorials when they feel there is a need for certain topics. In addition, tutorials that have not been presented in a long time and may be useful for new participants are often presented a second time.

The Edu Team recently began offering area-overview tutorials designed to both educate newcomers about the scope and activities of certain areas and offer long-standing participants updates on areas they don't actively follow. So far, the following area-overview tutorials have been organized. The team plans to continue these tutorials at IETF 91 in Honolulu and beyond. Check the agenda pages for topics.

- IETF 88–Introduction to the Real-Time Applications and Infrastructure Area (RAI)
- IETF 89–Introduction to the Applications Area (APP)
- IETF 90–Introduction to the Operations Area (OPS)

Tutorials are presented by IETF participants who are experts in their fields, and they are free to registered IETF attendees. As dictated by its charter to "present topics that assist IETF participants in building better protocols," the Edu Team does not provide general technical tutorials. All tutorials specifically focus on what IETF participants need to know in order to build better protocols.

At each IETF meeting, the Edu Team also organises an informational lunch where working group (WG) chairs can discuss topics of mutual interest. WG chairs are invited to suggest topics for forthcoming sessions.

The Edu Team is now considering whether or not to take on other projects, such as the mentoring programme, additional training for WG chairs, and review of IETF website content. It is actively seeking new, energetic members who are interested in helping with these activities. If you have feedback for the team or are interested in joining it, please contact edu-team@ietf.org or speak to any of its members during the next IETF meeting.

A list of tutorials slated for the next IETF meeting are included on the registration pages and on the meeting agenda. Slides and recordings from recent tutorials can be found at www.ietf.org/edu.

Donald Eastlake teaches the Wireless Tutorial at IETF 88. *Photo by Peter Lothberg*

The Edu Team

Cochairs
Mirjam Kuehne and Radia Perlman

Members
Jari Arkko
Scott Bradner
Brian Carpenter
Avri Doria
Russ Housley
Thomas Narten
Alice Russo
Margaret Wasserman

IAB Technical Plenary Debates the Opportunities and Challenges of Internet Payment Systems

By Carolyn Duffy Marsan

In response to an increase in the number of financial transactions being conducted over the Internet, the Internet Architecture Board held a technical plenary discussion about the challenges facing Internet-scale payment systems such as Bitcoin at the IETF 89 meeting in London.

Malcolm Pearson, director of development for e-commerce at Microsoft China, said Internet payment systems are in a similar situation to that of email 25 years ago, with each vendor having its own standards until the Simple Mail Transfer Protocol (SMTP) and Secure/Multipurpose Internet Mail Extensions (S/MIME) protocols emerged.

Malcolm Pearson, panelist and director of development for e-commerce at Microsoft China

"I'm hoping we get the same kinds of benefits out of the convergence of protocols around payments," he added.

Pearson pointed out that online payment systems face many challenges, including the fact that countries have their own currencies, as well as cultural differences regarding how people make gifts and payments, and whether they prefer cash or credit. Internet-based payment systems need to take these differences into account, as well as complex scenarios such as subscriptions, usage-based pricing, consumer-to-consumer payments, returns and cash settlements, and tax and financial reporting.

Pearson said he sees many productivity advantages to having standards for online payment systems that can provide secure interactions between merchants, users and payment sources. This is especially true in countries where large portions of the population don't have bank accounts or credit cards.

"Another very interesting tension is between security and convenience," Pearson said. "In North America, I can supply a credit card to a merchant I trust, and they will even keep track of this for me, and they'll make it very easy for me to make subsequent charges on this… But in China, if you provide that kind of experience, many users will reject it and feel that you're not providing enough security."

Pearson said he sees many productivity advantages to having standards for online payment systems that can provide secure interactions between merchants, users and payment sources. This is especially true in countries where large portions of the population don't have bank accounts or credit cards.

"There are statistics that say that in a lot of these emerging markets, without an e-commerce system, people spend two working days a month just dealing with bringing cash to family members or paying bills, which is a big load," Pearson said. "There's some good we can potentially do by solving this problem."

Pearson pointed out that online payment systems have to deal with varying timeframes, from several days to reconcile a subscription service to a few minutes to handle a restaurant bill to an immediate response for online gaming.

One scenario that's on the rise is mobile billing, which allows a customer to purchase an item from a website or store and use their mobile device as an e-wallet. Some mobile billing networks use Short Message Service (SMS) for authentication, while others use the mobile network or Subscriber Identification Module (SIM) card in the device to authenticate the transaction. Quick Response (QR) codes offer another layer of protection as they provide the mobile network operator with some validation that the user was present when the purchase was made.

"Authentication can be tied around the mobile device and then transferred to the carrier," Pearson said. "The carrier has good ways to be able to trust the mobile device and then pass on strong proof to the merchant that funds are available."

Issues to consider with mobile billing include whether possession of a device is enough to authenticate a transaction given that devices can be stolen or hacked. Another issue is the popularity in some countries of cash kiosks and retail centers, where customers pay for online purchases rather than using credit cards.

Pearson said e-wallets have the potential to address these issues because they behave like a bank account and can be funded through cash kiosks, mobile

Continued on next page

IAB Technical Plenary Debates the Opportunities and Challenges of Internet Payment Systems, continued

networks, and credit cards. "E-wallets could be relevant in North America as well as emerging markets," he added.

Pearson said there are opportunities for standardization within the online payments area where the IETF might contribute. These include invoices, user authentication, source payment authorization, cash reconciliation, and financial reporting.

"One place where we've been applying pressure is just to do cash reconciliation protocols, just getting the file formats converged," he said. "We have found that the participants are pretty willing to play. So there is, in fact, hope that the parties do want to work towards convergence."

Next up at the plenary was Steve Kirsch, founder and CEO of OneID, who gave a talk in which he debunked 15 myths in the area of secure payment authentication.

Kirsch argued that popular crypto methods such as Public Key Infrastructure, RSA Crypto, and EMV (Europay, MasterCard, and Visa) standards aren't as safe as Internet engineers believe.

"Authentication and secure payment authorization are almost the same thing," Kirsch said. "So we can use the same protocols, and it is just what we sign that's different. So I'm going to be talking about identity and about secure authorization. But they're really interrelated."

Kirsch's first myth is that there is no way to fix mass password and credit card breaches. The problem, he said, is that both passwords and credit cards are shared secrets. Further, half of Internet users have one password for all of their accounts.

"The solution to this breach problem is that we just get rid of all the shared secrets… and replace them with digital signatures," he said, adding that digital signature technology has been available for many years but that companies and individuals are not motivated enough to adopt them despite major losses from data breaches.

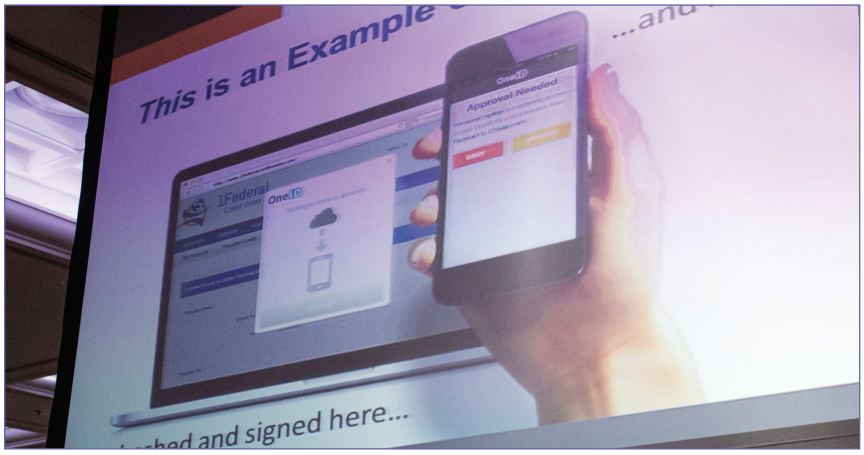
The second myth is that adopting two-factor authentication eliminates password breaches. Kirsch said that while this technology prevents key-logging attacks, it is not a remedy against mass breaches because it ends up being another shared secret. "Users hate it," he added.

Myth number three is that out-of-band two-factor authentication must be safe because banks use it. "The problem is that it's in-band two-factor authentication," Kirsch said. "You're entering code on the same computer as user name and password. If I compromise that computer, you're done."

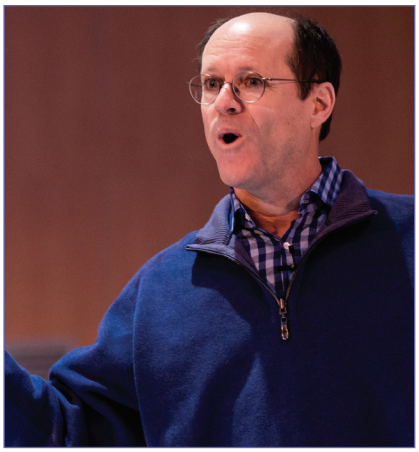
Kirsch also debunked the myth that biometrics will solve this problem. While they are useful locally, he said, the reader has to be controlled at all times.

Another myth Kirsch addressed is that it's impossible to store credit cards in a secure manner. He argued that there are secure Payment Card Industry (PCI) compliant vaults that use a crypto secret on the user's device to encrypt

Pearson said there are opportunities for standardization within the online payments area where the IETF might contribute. These include invoices, user authentication, source payment authorization, cash reconciliation, and financial reporting.



Technical Plenary presentations included debate over the safety of online payments and passwords.


Steve Kirsch, panelist and founder/CEO of OneID

the card. When a purchase is made, the user's device asks for encrypted card data, decrypts it, and passes it to the merchant.

Kirsch argued that passwords are not inherently bad; they just aren't used appropriately. What's wrong with today's Internet security systems is that passwords are used as shared secrets, which leaves them open to a breach.

"The right way to use passwords is to never disclose them and never share them off your local device," he said, adding that passwords should be combined with random data and then used as a signing key.

Additionally, Kirsch argued that popular crypto methods such as Public Key Infrastructure (PKI), RSA Crypto, and EMV (Europay, MasterCard, and Visa) standards aren't as safe as Internet engineers believe. Instead, he recommends using elliptic curve cryptography (ECC) and its companion digital signature algorithm (ECDSA).

Kirsch debunked the idea that the FIDO (Fast IDentity Online) Alliance will solve this problem because it is developing online identity technology that addresses authentication only, not authorization of transactions. "If you lose your device, you're screwed," he said.

Further, Kirsch argued that Internet users should not trust most federated identity providers, including Facebook, Google, and LinkedIn. However, Kirsch said that there are trustable federated identity providers where security is guaranteed by the architecture and ECDSA replaces shared secrets.

Audience members questioned panelists during the Technical Plenary's Q&A period.

"There is no single point of compromise because it uses multiple digital signatures," Kirsch said.

Another myth that Kirsch debunked is that trustable federated identity service is too hard to use and not as safe as proprietary identity systems. He argued that these services are as easy to use as Facebook and are immune to all known threats.

Kirsch argued that an IETF standard is not necessarily the best way to fix the online security problem. He pointed out that the IETF itself is using computer security technologies that are outdated, such as passwords for its mailing lists.

As far as Bitcoin is concerned, Kirsch said that nothing on the horizon looks lethal for this technology, but that there is also no evidence that it is going to be the future of online payments.

"The winner will be digitally signed end-to-end secure transactions," he said, adding that he favors open application programming interfaces (APIs) and a simple technique for transferring money.

Kirsch concluded that it is likely Bitcoin will be regulated in the future. But until then, he warns against storing Bitcoins in services that use in-band two-factor authorization because these systems are a type of shared secret and are susceptible to mass breach and malware.

STRONG GROWTH IN APPLIED NETWORKING RESEARCH PRIZE NOMINATIONS

Mat Ford (left) with winner Keith Winstein (center) and Lars Eggert, IETF chair (right)

The Internet Research Task Force (IRTF) reported that it received the largest-ever number of nominations for its Applied Networking Research Prize, a three-year-old program supported by the Internet Society.

The IRTF received 46 nominations—up from 36 last year—for the prize, which is given to academic researchers to recognize the best new ideas in networking, and bring them to the IETF and IRTF meetings. The IRTF chose six winners for 2014, and two winners spoke at the London meeting: Kenny Paterson from the University of London discussed new attacks on Transport Layer Security (TLS); and Keith Winstein from Massachusetts Institute of Technology spoke about a new transport protocol to support interactive applications over cellular networks. Read the related article, "ANRP Prizewinners Present on Breaking Internet Security and Making Videoconferencing Work Better," on page 17.

STRINT Workshop Focuses on Pervasive Monitoring

By Karen O'Donoghue

The past year has brought a series of revelations that have focused the entire Internet community on the topics of privacy and pervasive monitoring. Although some of the vulnerabilities have been known and some of the capabilities suspected, the depth and scale has come as a shock to many.

Two days prior to IETF 89, approximately 100 experts from the broader Internet community gathered for a workshop to discuss Strengthening the Internet (STRINT) against pervasive monitoring. The workshop focused on the ongoing issue of pervasive monitoring, its impact on the global Internet, and possible responses in various communities.

The primary goal of the STRINT workshop was to explore future work with the IETF and the World Wide Web Consortium (W3C) to address pervasive monitoring. Within that framework, the workshop also hoped to arrive at some agreement on threats, mitigations, trade-offs, architectural weak points, and potential work items and actions both within the Internet technical community (IETF, Internet Architecture Board, Internet Research Task Force, and W3C) and beyond.

The IAB plenary held at IETF 88 in Vancouver[1] concluded with a broad consensus that pervasive monitoring is an attack. This consensus has been subsequently documented as "Pervasive Monitoring Is an Attack," BCP 188, RFC 7258[2]. The STRINT workshop started with that consensus and proceeded to discuss the scope and implications of pervasive monitoring on the global Internet, possible near term actions for both the IETF and W3C communities, and harder topics for further discussion and analysis.

> [T]here is general agreement that there are technologies and tools that have been developed that would improve the state of privacy and security in the Internet.

Workshop Goals and Structure

The STRINT workshop was jointly sponsored by the IAB[3] and the W3C[4] with hosting support from the European Union STREWS project[5]. All interested parties were invited to submit position papers and participants were selected from that set, resulting in a capacity crowd. The agenda and submissions are available on the workshop website[6].

The highly popular, pre-meeting STRINT workshop was standing room only.

The workshop comprised a series of sessions with short kick-off presentations followed by moderated discussions. Topics for the sessions included workshop goals, threat models, usage of existing security tools, policy implications, improved tools, metadata, and deployment. The final sessions were a series of breakouts on research, clients, defaults, and terminology. A draft report detailing the results of the workshop is available[7].

General Observations

While it is not possible to summarize all the discussion and results from the workshop, key themes from the workshop are discussed below.

First, there is general agreement that there are technologies and tools that have been developed that would improve the state of privacy and security in the Internet. For example, well-implemented cryptography can be effective, and more use of it would improve security and privacy.

This raises the question of why existing technologies and tools that have already been developed don't get deployed and used. Cost is an argument often used against cryptography; however, costs are significantly declining. Another concern is the difficulty with deployment and use. The technical community could do more to make the tools easier to use and ensure that the default settings provide the highest levels of protection using well respected algorithms.

Additionally, the community as a whole could benefit from more examples of how to do things correctly, including examples of good software configurations to facilitate the deployment and use of existing technology. And to

[T]he community as a whole could benefit from more examples of how to do things correctly, including examples of good software configurations to facilitate the deployment, and use of existing technology.

help the developers who are often not security experts, the community should consider the development of examples of quality code for product development.

Near-Term Actions

In addition to the general observations above, the workshop identified specific activities for the IETF.

1. *Not surprisingly, terminology is a problem.* The term opportunistic encryption has been used in a number of IETF discussions related to pervasive monitoring. However, that terminology is used differently in related communities, causing confusion. To reduce this confusion, consensus needs to be reached on generic terminology.

A well-utlized whiteboard illustrates the collaborative nature of the STRINT workshop.

Subsequent to the STRINT workshop, the Security Area in the IETF has pursued this topic with the latest state being discussed on the SAAG mailing list (saag@ietf.org) and in draft-kent-opportunistic-security "Opportunistic Security as a Countermeasure to Pervasive Monitoring"[8].

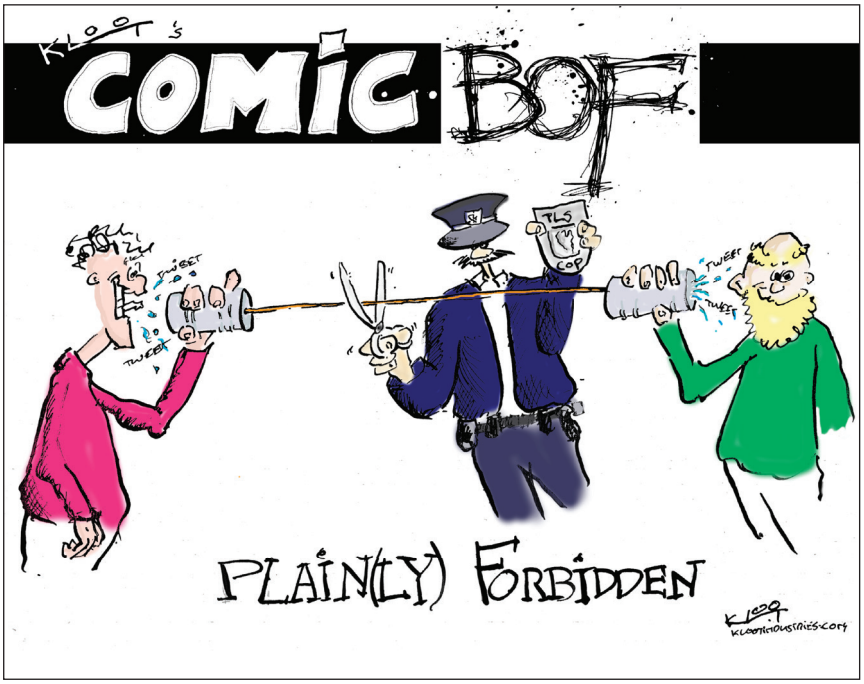
2. *A documented threat model would be helpful.* There is already an excellent start for that document in draft-barnes-pervasive-problem "Pervasive Attack: A Threat Model and Problem Statement"[9]. This will be used as the starting point and developed in the IETF.

Longer-Term Challenges

This brings us to some of the tougher challenges identified during the STRINT workshop. Most of these challenges represent significant tensions between legitimate competing concerns.

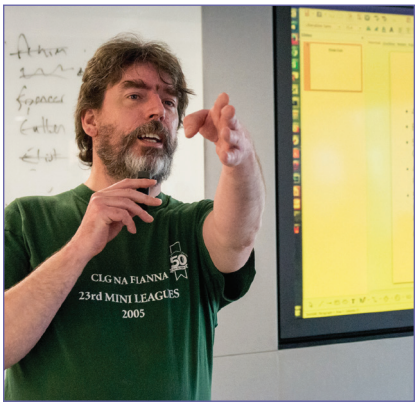
1. *The tension between the desire to deploy more encryption and the difficulty that this deployment creates for network operations.* Some visibility into traffic is necessary to optimize network performance and troubleshoot problems. However, that same visibility provides a wealth of information about the source and nature of communications even when the actual data itself is encrypted. Exacerbating this issue is the fact that traffic analysis is not well understood in the Internet community. Additional research and the development of techniques like data minimization are needed. In another example of this first tension, devices like captive portals and firewalls have legitimate roles to play in deployed networks but may not be distinguishable from a man-in-the-middle attack. Policies associated with using these devices may limit or prohibit the use of encryption.

2. *The tension between privacy and business models.* Many products and services in today's Internet are provided on a low- or no-cost basis. The information gathered in the process of providing the service is a valuable commodity, and the cost associated with providing the service is offset by the value of the information gathered. In this case, the business model is in direct conflict with the proposed mechanism for enhancing privacy.



Continued on next page

STRINT Workshop Focuses on Pervasive Monitoring, continued



Stephen Farrell, IETF security area director and research fellow in the school of Computer Science and Statistics at Trinity College, Dublin

3. *The last significant challenge discussed herein is the problem of user interfaces.* Existing user interfaces are a significant barrier to the adoption of many security technologies. If the security mechanism stands between an operator or a user and his desired objective, it needs to be easily understood and used. That is often not the case. Internet users have long since been conditioned to hit the OK button without fully understanding the implications of their decisions. A user cannot be expected to fully understand the intricacies of certificate models and encryption in order to be protected by the security mechanism. The IETF and W3C have long considered user interfaces to be primarily outside their scope; however, the time may have come to better integrate these topics into the discussion.

Finally, while the STRINT workshop was primarily a technical meeting, there was some discussion of the interdependency of technology and policy in addressing pervasive monitoring. Better communication and understanding between the two communities could lead to technical and policy approaches that are viable and support each other instead of working against each other.

Ongoing Related Activities

Beyond the STRINT workshop, the IETF and the W3C are both responding to pervasive monitoring with renewed focus on privacy and security.

The IETF has revived an effort to provide adequate privacy reviews to protocols under development. This will be part of the existing security review process and be informed by "Privacy Considerations for Internet Protocols"[10]. At some point, the IETF may update the existing security considerations document "Guidelines for Writing RFC Text on Security Considerations"[11] to better address pervasive monitoring. In addition to review of emerging protocols, there is a new effort to review existing RFCs for any privacy or pervasive monitoring concerns. A mailing list has been established (ietf-privacy@ietf.org) and a wiki page has been set up to track any issues identified during the course of these reviews (https://trac.tools.ietf.org/group/ppm-legacy-review/).

> [T]he STRINT workshop showed that there is an energized and passionate community. This community, while not in total agreement, does have rough consensus on some general principles, near term actions, and longer-term efforts that would help to mitigate pervasive monitoring.

On the working group front, a new working group in the IETF has been chartered to look at the use of Transport Layer Security (TLS) in application protocols, Using TLS in Applications (UTA). Several other working groups and Birds-of-a-Feather sessions are looking at this issue with renewed energy.

In the W3C, the Privacy Interest Group continues to provide overarching privacy review for W3C recommendations[12]. In addition, a Web Security Interest Group[13] has been established to advance security in W3C recommendations.

Conclusions

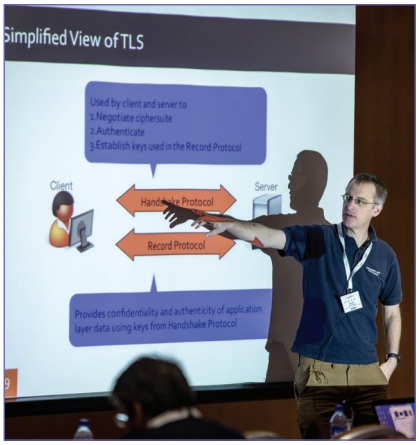
While it has been a tough year for privacy and security in the Internet, the STRINT workshop showed that there is an energized and passionate community. This community, while not in total agreement, does have rough consensus on some general principles, near term actions, and longer-term efforts that would help to mitigate pervasive monitoring. All of this is encouraging for the improvement of overall security and privacy for the global Internet.

References

1. www.internetsociety.org/publications/ietf-journal-march-2014/iab-plenary-debates-attacks
2. Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack," BCP 188, RFC 7258, May 2014. (www.rfc-editor.org/rfc/rfc7258.txt)
3. www.iab.org
4. www.w3.org
5. www.strews.eu
6. www.w3.org/2014/strint
7. https://datatracker.ietf.org/doc/draft-iab-strint-report
8. https://datatracker.ietf.org/doc/draft-kent-opportunistic-security
9. https://datatracker.ietf.org/doc/draft-barnes-pervasive-problem
10. Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols," RFC 6973, July 2013.
11. Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations," BCP 72, RFC 3552, July 2003.
12. www.w3.org/Privacy
13. www.w3.org/Security/wiki/IG

ANRP Prizewinners Present on Breaking Internet Security and Making Videoconferencing Work Better

By Mat Ford



Kenny Paterson, ANRP winner, presents his work on finding and documenting new attacks against key Internet security protocols.

The first Applied Networking Research Prize of 2014 was presented to Kenny Paterson for finding and documenting new attacks against key Internet security protocols. In their paper, "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols" *(Proc. IEEE Symposium on Security and Privacy,* pp. 526-540, San Francisco, CA, USA, May 2013), Paterson and his coauthor, Nadhem Al Fardan, demonstrate practical attacks against Transport Layer Security, a fundamental security building block for much of today's online activity.

Paterson's presentation to the Internet Research Task Force open meeting in London gave great insight into the techniques he and others have developed to leverage seemingly tiny differences in the timing of protocol operations to reveal plaintext, and thereby break the security of the transaction. There is now a real need for constant-time, constant-memory access implementations to be confident that such potential implementation weaknesses have been completely eliminated.

Paterson noted the importance of the virtuous cycle that sees widely used security protocols gaining a high profile in the research community, leading to more analysis and more development work to patch weaknesses as they are discovered and ultimately stronger security protocols for everyone. Responsible disclosure practices and close collaboration with the IETF were key aspects in this instance. Paterson's slides are available at www.ietf.org/proceedings/89/slides/slides-89-irtfopen-1.pptx, and audio from the presentation is available at www.ietf.org/audio/ietf89/ietf89-viscount-20140305-0900-am1.mp3 starting at 00:18:25.

Trying to conduct a videoconference over a cellular network from a moving car "wasn't working very well" for Keith Winstein, so he started trying to find a solution to the problem. The result was a new transport protocol called "Sprout" and the paper he and his coauthors wrote earned Winstein the second Applied Networking Research Prize for 2014.

Winstein won his award for designing a transport protocol for interactive applications that desire high throughput and low delay. In their paper, "Stochastic Forecasts Achieve High Throughput and Low Delay over Cellular Networks" *(Proc. 10th USENIX Symposium on Networked Systems Design and Implementation (NSDI),* Lombard, IL, USA, April 2013), Winstein and his coauthors, Anirudh Sivaraman and Hari Balakrishnan, describe Sprout, a transport protocol that works well over cellular wireless networks, where link speeds change dramatically with time, and current protocols build up multi-second queues in network gateways.

Winstein won his award for designing a transport protocol for interactive applications that desire high throughput and low delay.

Motivated by his subpar videoconferencing experience, Winstein and his team developed a novel end-to-end transport protocol that maximizes throughput while simultaneously bounding the risk of delay by modeling the variation in link speed based on observations of packet arrival times. The model is then used to predict the future link speed.

The results are compelling: experiments conducted on traces from four commercial cellular networks show many-fold reductions in delay, and increases in throughput over Skype, Facetime, and Hangout, as well as over Cubic, Compound TCP, Vegas, and Low Extra Delay Background Transport (LEDBAT). Although Sprout is an end-to-end scheme, in this setting it matched or exceeded the performance of Cubic-over-CoDel, which requires modifications to network infrastructure to be deployed.

Winstein received his award at the recent Internet Research Task Force open meeting at IETF 89 in London, where he also presented his results. Winstein's slides are available at www.ietf.org/proceedings/89/slides/slides-89-irtfopen-0.pdf, and audio from the presentation is available at www.ietf.org/audio/ietf89/ietf89-viscount-20140305-0900-am1.mp3 starting at 01:22:35.

The nomination period for prizes to be awarded in 2015 is now open and nominations can be submitted via the system at https://irtf.org/anrp/2015/.

Visiting Policymakers Tout IETF Policy Programme Experiences

By Carolyn Duffy Marsan

The Internet Society continued to engage regulators in discussions about the technical underpinnings of the Internet and the challenges facing this global network-of-networks by sponsoring policymakers to attend IETF 89.

ISOC's IETF Policy Programme facilitates exchange between government policymakers and IETF leaders by providing visiting policymakers with an overview of how the IETF works and key issues affecting the Internet's continued growth. Since 2012, the programme has hosted 69 regulators from 53 countries to attend IETF meetings.

In London, IETF leaders and policy guests explored such issues as mobility, bandwidth constraints and the emergence of new applications with this meeting's 16 sponsored policymakers. The group examined critical issues facing the Internet, including the frequency of pervasive monitoring by government agencies, the need for tighter security through encryption-based protocols, and the ongoing transition from IPv4 to IPv6.

Ihsan Durdu, an advisor to the head of Turkey's Ministry of Transport and Communications, said he didn't know much about how Internet standards were developed prior to attending IETF 89. He added that it is important to understand how Internet policy and technology are related to each other in his role as a government advisor.

"Internet policy development activities and its regulation are very much led by technological progress, and linked so much to technical standards as well as changing limitations and improved capabilities that this progress brings," Durdu said. "The dynamic and fast-changing nature of Internet technology is both improving Internet infrastructure and operations and affecting our daily life, including the way our economy, communications, banking, finance, social, and political life work and operate."

Durdu said attending IETF 89 was an "excellent chance to see how the IETF and its standards development activities work."

He said he wished all policymakers could attend the IETF Policy Programme. "This program could help open up their vision," he said. "A policy is good and healthy only if it is flexible: open to technological developments, inclusive of new standards, dynamic, and forward looking. Otherwise, it can do more harm than good to society."

Durdu said he left IETF 89 more convinced than ever that the Internet should continue to be governed by a multistakeholder model.

Salam Yamout, the National Information and Communication Technologies (ICT) Strategy Coordinator at the Lebanese Presidency of the Council of Ministers, said she wanted to attend an IETF meeting so she could understand how the Internet's leading standards body works.

I wanted to understand the charter, mandate, and structure of the IETF that … [have] issued thousands of policies and protocols that made [the Internet] usable by millions of users around the globe," she said.

She said having direct access to Internet experts at IETF 89 helped her better understand emerging technologies and related issues. "They shared with me their years of experience as insiders," she added. "I couldn't have gotten the same benefit if I had attended the IETF on my own."

Yamout said that all of the IETF Policy Programme sessions were interesting and relevant to her policy work, but she especially enjoyed visiting the London Internet Exchange Point.

"It gave me perspective on the scale of Internet operations/transactions driven by the Internet," she said, adding that the Internet is powering entire sectors of the economy. "I also appreciated the session about pervasive monitoring as it answered many questions about what really happened in the National Security Administration case. Governments are always interested in the issues of security and monitoring."

From left to right: Markus Kummer, ISOC; Issah Yahaya, Ghana; Maarit Palovirta, ISOC; Salam Yamout, Lebanon; Caroline Hammarberg, UNESCO; Małgorzata Steiner, Poland; Elizabeth Martin Nzagi, Tanzania; Daniel Obam, Kenya; Michuki Mwangi, ISOC (hidden); Catherine Farrel, Old Dog Consulting, UK; Hodge Semakula, EACO, Rwanda; Jeffrey Dogley, Seychelles; Coppens Pasteur Ndayiragije, Burundi; Ihsan Durdu, Turkey; Bakarr Tarawally, Sierra Leone; Sally Wentworth, ISOC (not pictured: Angelique Weeks, Liberia; Antony Chigaazira, Botswana; Odon Kasinki, Democratic Republic of Congo)

Transport Services (TAPS) Birds-of-a-Feather

By Michael Welzl

The Stream Control Transmission Protocol (SCTP), Datagram Congestion Control Protocol (DCCP), Multi-Path Transmission Control Protocol (MPTCP), and User Datagram Protocol-Lite (UDP-Lite) protocols and the Low Extra Delay Background Transport (LEDBAT) congestion control mechanism offer a large number of services to applications, in addition to the long-standing two services provided by TCP and UDP.

For example:

- SCTP provides reliable and potentially faster-than-TCP delivery of data chunks to applications that may be able to accept such chunks out of order.
- DCCP provides various forms of congestion control for applications that need it, but prefer their packets be dropped rather than retransmitted, as the latter can lead to delay.
- LEDBAT provides a scavenger-like background transfer mode, in which LEDBAT traffic does not get in the way of other transfers that use TCP, for instance.

As useful as these services may be, implementing them can be difficult: not all protocols are available everywhere, hence fall-back solutions are often required. In addition, some protocols provide the same services in different ways, and layering decisions must be made (e.g., should a protocol be used natively or over UDP?). As a result, some programmers resort to using TCP or implementing their own customized solution over UDP (e.g., Google with Quick UDP Internet Connections (QUIC)[1] and Adobe with Real-Time Media Flow Protocol (RTMFP)[2]), at which point the chances of benefiting from other transport protocols are lost.

The intention of the Transport Services (TAPS) initiative is to identify the services provided by IETF transport protocols and congestion control mechanisms, as well as the network requirements of applications and the APIs they use to communicate. By mapping the connections between these lists, a later working group (WG) may define services that a transport API should offer. It could then specify how these transport services can be implemented using native IETF transports and encapsulated transports, including the definition of mechanisms to validate that a transport (or transports) can be supported on a path.

The intention of the Transport Services (TAPS) initiative is to identify the services provided by IETF transport protocols and congestion control mechanisms, as well as the network requirements of applications and the APIs they use to communicate.

The TAPS initiative began in August 2013 with a mailing list and an accompanying Web page. We held a Bar Birds-of-a-Feather (BoF) at IETF 88 in Vancouver, where it was already clarified that TAPS should be careful to provide what application programmers really need, rather than being too focused on the Berkeley Sockets application programming interface (API). Accordingly, several Internet-drafts were written, including use cases and an overview of how higher level APIs could better be supported by enhanced IETF transport services. By breaking the dependency of applications on specific protocols, TAPS has the potential to make the currently rigid transport layer more flexible (figure 1). In December 2013, a presentation was given at the Internet Architecture Board (IAB) Workshop on Internet Technology Adoption and Transition in Cambridge, UK, explaining how the evolutionary benefit of TAPS is connected to its best-effort nature. These activities culminated in a BoF meeting at IETF 89. This BoF was designated "non-WG-forming" to enable the IETF community to discuss the various angles of this large problem space without having to spend time on charter wordsmithing. Discussion was lively at this two-hour long session that included 129 attendees and a debate at which more than 6,650 words were spoken at the microphone.

This BoF was designated "non-WG-forming" to enable the IETF community to discuss the various angles of this large problem space without having to spend time on charter wordsmithing. Discussion was lively at this two-hour long session that included 129 attendees and a debate at which more than 6,650 words were spoken at the microphone.

The following four individuals presented their viewpoints at the TAPS BoF:

1. Jon Crowcroft outlined the potential of this activity by calling it "socket science" and relating it to security.

Continued on next page

Transport Services (TAPS) Birds-of-a-Feather, continued

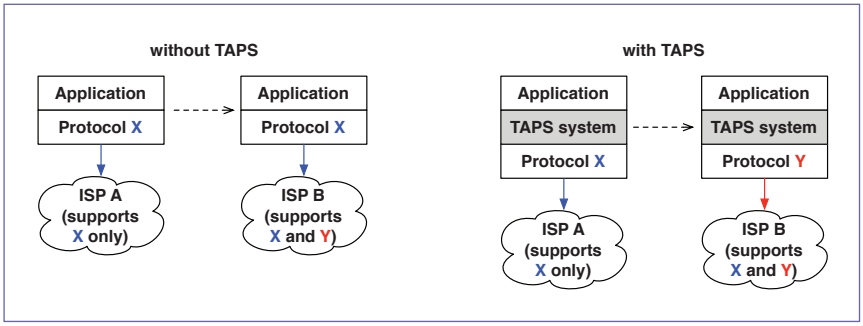


Figure 1. Without TAPS (left), the application is tied to protocol X. With TAPS (right), the application could benefit from protocol Y that is supported by ISP B.

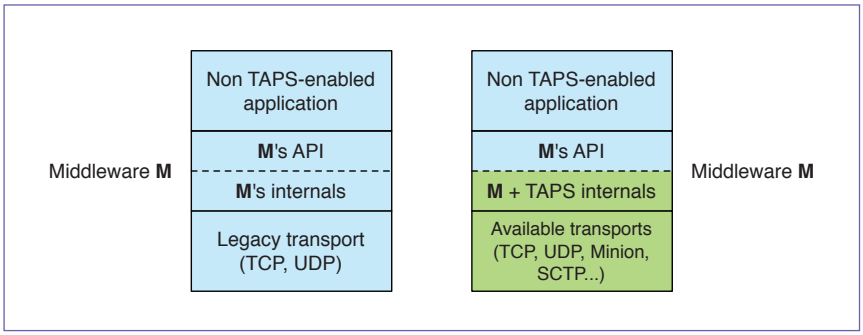


Figure 2. Before (left) and after (right) applying TAPS below a non-TAPS-enabled application. Nothing changes in the application and the middleware API that it uses.

Each presentation was accompanied by an active debate—not everyone in attendance was in agreement with every presented way of providing transport services.

2. Martin Sustrik presented how middleware, such as his own ZeroMQ, could benefit from transports other than TCP; most notably, he explained how the strict reliability of TCP is a poor match for pub/sub communication. Middleware layers are increasingly common and often have enough information about what the user is trying to achieve to be able to make informed transport choices on their behalf. Updating middleware offers an easy deployment path, in which applications could exploit some of the benefits of TAPS without having to be changed unless recompiling with a new version of the middleware (figure 2).
3. Gorry Fairhurst presented a possible implementation of TAPS.
4. Margaret Wasserman presented the API of the Multiple Interfaces (MIF) WG. This API is clearly related, and it seems obvious that a TAPS API should be somehow connected to the MIF API.

Each presentation was accompanied by an active debate—not everyone in attendance was in agreement with every presented way of providing transport services. The major concerns that were raised include:

- **Predictability.** The flexibility shown in figure 1 comes at a cost—application programmers may need a predictable behavior, whereby a certain way of using an API consistently leads to the same protocol choice underneath. It was suggested that such decisions are better made at development time than at runtime.
- **Safety.** The importance of testing was emphasized; changing the transport protocol must not break an application.
- **Binding mechanisms.** Going beyond the TAPS proposal, the support of name-based transports instead of IP-address-based transports was suggested as an option.
- **Layer versus API.** Several participants stated that TAPS should not be focusing on an API. It was suggested that (1) TAPS be thought about in terms of a layer, and (2) it be left to the operating systems that interface with applications to build the API and to produce the layer that we want with the information we want and whatever APIs are needed.

An ongoing conversation about next steps is occurring among the Transport Area (TSV) area directors (ADs) who sponsored the TAPS BoF, the Applications Area and Real-time Applications and Infrastructure Area ADs, and interested IAB members. The group's mailing list (taps@ietf.org) currently has 120 subscribers, and can be joined at https://www.ietf.org/mailman/listinfo/taps. The accompanying webpage is at https://sites.google.com/site/transport-protocolservices.

Footnotes

1. www.ietf.org/proceedings/88/slides/slides-88-tsvarea-10.pdf
2. RFC 7016, "Adobe's Secure Real-Time Media Flow Protocol"

Note: Activities of some TAPS participants (i.e., Michael Welzl and Gorry Fairhurst) were partly funded by the European Community under its Seventh Framework Programme through the Reducing Internet Transport Latency (RITE) project (ICT-317700). The views expressed are solely those of the author.

IRTF Update

By Lars Eggert

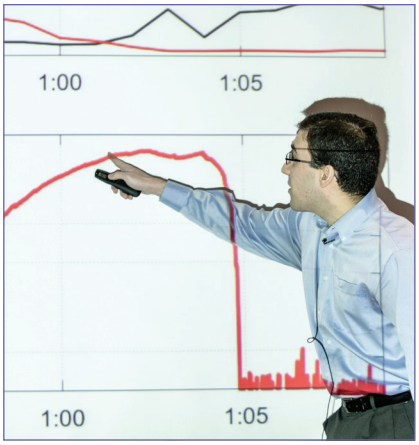
During IETF 89 in London, seven out of the nine then-chartered Internet Research Task Force (IRTF) research groups (RGs) held meetings—the highest number of meetings in recent years:

- Information-Centric Networking (ICNRG)
- Crypto Forum (CFRG)
- Internet Congestion Control (ICCRG)
- Network Complexity (NCRG)
- Software-Defined Networking (SDNRG)
- Network Management (NMRG)
- Network Coding (NWCRG)

Side Meetings

In addition to the meetings of chartered research groups, the proposed research group, Global Access to the Internet for All (GAIA), held a successful side meeting. It plans further meetings at the IETF and other events, including the ACM Symposium on Computing for Development for December 2014. The mailing list for this effort is gaia@irtf.org. For more on GAIA, see "Researching Global Access to the Internet for All (GAIA)," on page 1.

A second side meeting was held to discuss the Datacenter Latency Control research group. Proponents plan a public meeting for IETF 90 in Toronto. The mailing list for this effort is dclc@irtf.org.



Keith Winstein, one of the first Applied Network Research Prize winners of 2014, presents his research.

New RFC Published

Since IETF 88 one new RFC was published on the IRTF RFC Stream by the Scalable Active Multicast Research Group (SAMRG): RFC 7046, A Common API for Transparent Hybrid Multicast.

Applied Networking Research Prize Winners

The first two Applied Networking Research Prize (ANRP winners of 2014 presented their research at the IRTF Open Meeting at IETF 89. Kenny Paterson presented findings and documentation of new attacks against TLS and DTLS; Keith Winstein presented a transport protocol design for interactive applications requiring high throughput and low delay. For more on the ANRP winners, see "ANRP Prizewinners Present on Breaking Internet Security and Making Videoconferencing Work Better," on page 17.


Kenny Paterson (right) accepts one of the first Applied Network Research Prizes of 2014 from Mat Ford (left).

Requests and Appeals

The IRTF chair received a request from Trevor Perrin to replace one of the Crypto Forum Research Group (CFRG) cochairs. After reviewing the facts and discussing the matter with community members, the IRTF chair declined the request. The decision was appealed to the Internet Architecture Board, which upheld the decision.

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

The RFC Series and the 21st Century

By Heather Flanagan

In March 2012, I attended my first IETF meeting as RFC Series Editor. It was my first opportunity to meet directly with the community and learn what they wanted from the RFC Series. The feedback was quite clear: the old ASCII-only format was no longer sufficiently meeting the needs and expectations of the community.

In fact, questions about the suitability of the ASCII-only format started at least a decade ago. With that much history around a desire for change, I wondered why it hadn't happened sooner. The answer was quite simple—and it gave me a glimpse into just how challenging an effort this would be: many people wanted change, but there was no consensus on exactly what that change should be. Virtual wars were fought on mailing lists and in hallways as people promoted their preferred document format.

The feedback was quite clear: the old ASCII-only format was no longer sufficiently meeting the needs and expectations of the community.

My first step, after determining the priority for such an effort, was to start gathering requirements. The rfc-interest mailing list became a hotbed of conversation, and several BoFs were held at subsequent IETF meetings to both review my understanding of the community's requirements and collect more feedback. Between IETF meetings, I met with the RFC Production Center to ensure that editor requirements were also captured. The end result was the publication of RFC 6949, "RFC Series Format Requirements and Future Development." This document captured the requirements at a high level, and set the stage for making the decision to target an XML format as the canonical RFC format, with other, more human-readable formats rendered from that XML.[1] In addition, on 2 May 2013, the decision to allow non-ASCII characters and SVG artwork in a prescribed fashion was announced.

Many steps are needed to get from a declaration of intent to actual implementation. A design team was put together to help with the more detailed requirements necessary to write tools for authors and editors to create, edit, and publish documents in the new format. The team members include Nevil Brownlee (ISE), Heather Flanagan (RSE), Tony Hansen, Joe Hildebrand, Paul Hoffman, Ted Lemon, Julian Reschke, Adam Roach, Alice Russo, Robert Sparks (Tools Team liaison), and Dave Thaler.

Several Internet-Drafts have been created by design team members, including:

- The 'XML2RFC' v2 Vocabulary *https://datatracker.ietf.org/doc/draft-reschke-xml2rfc/*
- The 'XML2RFC' v3 Vocabulary *https://datatracker.ietf.org/doc/draft-hoffman-xml2rfc/*
- The Use of Non-ASCII Characters in RFCs *https://datatracker.ietf.org/doc/draft-flanagan-nonascii/*
- HyperText Markup Language Request For Comments Format *https://datatracker.ietf.org/doc/draft-hildebrand-html-rfc/*
- SVG Drawings for RFCs: SVG 1.2 RFC *https://datatracker.ietf.org/doc/draft-brownlee-svg-rfc/*
- PDF for an RFC Series Output Document Format *(in progress)*

Documenting the requirements in those drafts is a huge, critical piece of the new format effort. And there is still more to do—from prototyping code to test the requirements, to creating a digital preservation policy that describes how the RFC Editor will handle this new diversity in digital assets for future generations, to developing the actual production code that will generate the new formats.

Changing a more than 40-year-old tradition of plain text documents is not something that can—or even should—happen without a great deal of planning and testing to ensure that RFCs remain a useful way to consume information on Internet standards, best practices, experiments, and information for decades to come.

Tune in to rfc-interest and the next format BoF for an update on the status of the format effort.

Changing a more than 40-year-old tradition of plain text documents is not something that can—or even should—happen without a great deal of planning and testing to ensure that RFCs remain a useful way to consume information on Internet standards, best practices, experiments, and information for decades to come.

Footnotes

1. www.rfc-editor.org/pipermail/rfc-interest/2013-May/005584.html

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 89, including their intentions and outcomes. If you're inspired to arrange a BoF meeting, please be sure to read RFC 5434: Considerations for Having a Successful Birds-of-a-Feather (BoF) Session.

Authentication and Authorization for Constrained Environments (ace)

Description: A problem with constrained devices is the realization of authentication and authorization operations. The aim of ACE is to form a working group (WG) that will provide constrained devices with the necessary prerequisites to use REST operations in a secure way, considering such things as authorization information and the related keying material. Constrained devices will thus be enabled to authenticate operations from other (constrained or less-constrained) devices, to communicate securely with them, and to verify their individual authorization to access specific resources.

Proceedings: http://www.ietf.org/proceedings/89/minutes/minutes-89-ace

Outcome: A good discussion with some concrete problems identified, although more work is required to clearly delineate the scope of any new WG. Since the meeting, a new working group has been proposed in the Security Area (https://mailarchive.ietf.org/arch/msg/ietf-announce/xR8bmbZLOU6QR80mS-HIDVcxEJs).

Domain Boundaries (dbound)

Description: Both users and applications make inferences from domain names, usually in an effort to make some determination about identity or the correct security stance to take. Such inferences, however, are usually based on heuristics, rules of thumb, and large static lists describing parts of the Domain Name System (DNS) name space. These mechanisms are unlikely to be sustainable in the medium term as the DNS root undergoes rapid expansion. There have been some proposals to improve this state of affairs and the purpose of this BoF is to identify the problems, the work to address each problem, and to determine whether there is sufficient interest and energy to set up a working group to complete that work.

Proceedings: http://www.ietf.org/proceedings/89/minutes/minutes-89-dbound

Outcome: This is an important problem for the community to address and further work is required to come to agreement on a clearly described problem statement to help focus the effort. A discussion list has been created (https://www.ietf.org/mailman/listinfo/dbound) and a design team formed to come up with a clear problem statement and some boundary conditions.

Encryption of DNS Requests for Confidentiality (dnse)

Description: As part of the discussion about responding to pervasive surveillance and the need to make such surveillance more difficult and costly to perform, DNS has been identified as a protocol that can reveal a lot about users and their activities. Existing security solutions (like DNSSEC) do not provide confidentiality of user traffic. There have been proposals to encrypt DNS requests, to prevent information disclosure to third parties, both inside the IETF (draft-wijngaards-dnsop-confidentialdns) and outside of it (DNScurve).

European robin (Erithacus rubecula)

Continued on next page

The intention of the dnse BoF is to start from existing problem statements and to find out if something can be recommended to improve DNS traffic confidentiality. The recommendation could be an existing solution (such as IPsec) or a way to map DNS requests into a general-purpose security solution (such as Datagram Transport Layer Security (DTLS)) or the development a new standard for DNS encryption. In the last case, this may require a new WG.

Proceedings: http://www.ietf.org/proceedings/89/minutes/minutes-89-dnse

Outcome: The BoF discussion went well and triggered a second session of the DNS Operations working group to continue the discussion. A mailing list has been created (https://www.ietf.org/mailman/listinfo/dns-privacy) for focused discussion of the problem statement surrounding the addition of privacy to the DNS protocol.

Transport Services (taps)

Description: Many transport protocols and congestion control mechanisms offer services to applications in addition to the long-standing services provided by Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). For an application programmer, using protocols other than TCP or UDP is hard: not all the alternative protocols are available everywhere, hence a fallback solution must be implemented. Some protocols provide the same services in different ways. Because of these complications, programmers often resort to either using TCP or implementing their own customized solution over UDP, and the potential benefits of other transport protocols are lost.

This BoF is intended to identify the services provided by existing IETF transport protocols and congestion control mechanisms as well as network requirements for common APIs that applications use to communicate. By finding a mapping between these two lists, it is possible to define services that a transport application programming interface (API) should offer. Specifying how these transport services can be implemented using native IETF transports and encapsulated transports, including the definition of mechanisms to validate that a transport (or transports) can be supported on a path would be the next step.

For an application programmer, using protocols other than TCP or UDP is hard: not all the alternative protocols are available everywhere, hence a fallback solution must be implemented.

Proceedings: http://www.ietf.org/proceedings/89/minutes/minutes-89-taps

Outcome: This was not a working group forming BoF. The meeting included many interesting presentations and useful discussions. More focus is required with regards to a shared understanding of the issues and concrete, useful next steps. For more about the TAPS BoF, see "Transport Services (TAPS) Birds-of-a-Feather," on page 19.

Rock pigeon (Columba livia)

Tunneling Compressed Multiplexed Traffic Flows (tcmtf)

Description: RFC 4170 Tunneled Multiplexed Compressed Real-time Transport Protocol (TCRTP) defines a method for grouping packets when a number of UDP/RTP VoIP flows share a common path, considering three different layers: header compression, multiplexing, and tunneling. TCRTP optimizes the traffic, increasing the bandwidth efficiency of Voice over Internet Protocol (VoIP) and reduces the amount of packets per second at the same time. More recently, real-time services that use bare UDP instead of UDP/RTP have become popular. There is a need to replace RFC 4170 with an extended solution able to optimize these new flows, also using improved compression methods.

The BoF will discuss the proposed charter, with the aim of the creation of a WG in order to specify the protocol stack, signaling mechanisms, and maximum added delay recommendations for tunneling, compressing, and multiplexing traffic flows (TCM-TF). This BoF is intended to form a WG.

Proceedings: http://www.ietf.org/proceedings/89/minutes/minutes-89-tcmtf

Outcome: This is the second BoF of TCMTF. The problem statement was well presented and the use scenarios are quite clear. TCP is now out of scope. Discussion continues on applicability and latency considerations, but it seems that for very low bandwidth links in developing countries, a new standard here would be useful. There is a mailing list for continuing discussion (https://www.ietf.org/mailman/listinfo/tcmtf).

Virtualized Network Function Pool (vnfpool)

Description: A Virtualized Network Function (VNF) provides a network function (e.g., packet filtering at firewalls, load balancing, etc.) and is typically implemented as a software instance running on a commodity hardware server via a virtualization layer (i.e., hypervisor). This is distinct from monolithic network devices, where either a single or a number of different network functions are provided in the same specialized hardware server. There is a trend to move such network functions away from specialized hardware to commodity hardware servers, based on virtualized resources, to support VNF and further also to support Service Function Chaining (SFC). In SFC, a network service can be implemented by a set of sequentially connected VNFs deployed at different points in the network. We call a group of VNFs a VNF set, which can be used not only as an SFC, but also solely as one or more pools of VNFs.

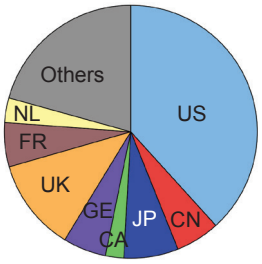
In the current charter, the WG would focus on the work around several mechanisms supporting the reliability of a VNF set: redundancy across a VNF set and stateful failover among pool members.

A VNF set can introduce additional points of failure beyond those inherent in a single specialized server, and therefore poses additional challenges on reliability of the provided services. Currently, generalized pooling and other redundancy mechanisms may be applied to address some reliability requirements of a single VNF. However, the complexity of dealing with a growing number of VNFs including stateful and stateless functions, and extending the redundancy across a VNF set (i.e., multiple pools for multiple VNFs) requires further solution development. In the current charter, the WG would focus on the work around several mechanisms supporting the reliability of a VNF set: redundancy across a VNF set and stateful failover among pool members.

Proceedings: http://www.ietf.org/proceedings/89/minutes/minutes-89-vnfpool

Outcome: A good discussion that identified a need for further work on the intended scope of any potential working group on this topic, and the need to work closely with the SFC WG to avoid any potential overlap.

IETF 89 At–A–Glance



On-site attendance: 1,364

Newcomers: 220

Number of countries: 60

IETF Activity since IETF 88 (November 2013–March 2014)

New WGs: 7

WGs closed: 0

WG currently chartered: 120

New and revised Internet-Drafts (I-Ds): 1707

IETF Last Calls: 96

Internet-Drafts submitted: 132

RFCs published: 91

- 74 IETF (61 WG, 13 Individual/AD Sponsored), 2 IAB, 3 IRTF, 12 Independent

Live and Social Media

- STRINT workshop: 525 tweets, exposure 1.352K
- IETF 89: 269 tweets on #IETF89, exposure via @IETF= 161K, exposure via #IETF89=529.6K, 73 new followers since 19 February 2014
- Facebook: 460 Likes

Mentoring Programme now has 20 mentor matches

Mailing List Discussion Style Guide: In progress

- Inspired by recent discussions on list, to promote professionalism and respect on lists and email

IANA Activity since IETF 88 (October 2013–January 2014)

Processed 1337+ IETF-related requests, including:

- Reviewed 110 I-Ds in Last Call and reviewed 131 I-Ds in Evaluation
- Reviewed 116 I-Ds prior to becoming RFCs, 63 of the 116 contained actions for IANA

SLA Performance (August 2013–January 2014)

- Processing goal average for IETF-related requests: 99%
- Currently revising the 2014 SLA between ICANN and IAOC for the protocol parameter work

IANA and DNSSEC

- 265 TLDs have a full chain of trust from the root, http://stats.research.icann.org/dns/tld_report/

RFC Editor Activity since IETF 88 (November 2013–March 2014)

Published RFCs: 91

- 35 Standards Track, 6 BCP, 4 Experimental, 46 Informational

IETF Meeting Calendar

IETF 90
20–25 July 2014
Host: Ericsson
Location: Toronto, ON, Canada

IETF 91
9–14 November 2014
Host: Cisco
Location: Honolulu, HI, USA

IETF 92
22–27 March 2015
Host: Google
Location: Dallas, TX, USA

IETF 93
19–24 July 2015
Host: TBD
Location: Prague, Czech Republic

For more information about past and upcoming

IETF Meetings

http://www.ietf.org/meeting/

Special thanks to

ICANN

for hosting IETF 89

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

Afilias Google Microsoft NBCUniversal SIDN

This publication has been made possible through the support of the following Platinum Programme supporters of the Internet Society

Afilias ARIN cable CISCO Comcast Juniper NETWORKS NBCUniversal RIPE NCC SIDN

pub-IETFJV10.1-20140701-en

Published three times a year
by the Internet Society.

Galerie Jean-Malbuisson 15
1204 Geneva, Switzerland

Email
ietfjournal@isoc.org

Find us on the Web
www.internetsociety.org/ietfjournal

Editor's Note
The IETF Journal adheres to the *Oxford English Dictionary*, 2nd Edition.

IETF Journal
IETF 89 • Volume 10, Issue 1 • July 2014

IETF Journal

Internet Society
Galerie Jean-Malbuisson 15
1204 Geneva, Switzerland