Celebrating 10 Years 2005–2015

VOLUME 11, ISSUE 2 • NOVEMBER 2015

IETF® Journal

A report from IETF 93, July 2015, Prague, Czech Republic. Published by the Internet Society in cooperation with the Internet Engineering Task Force.*

INSIDE THIS ISSUE

Internet Society™

FROM THE EDITOR'S DESK

By Mat Ford

THE INTERNET ENGINEERING TASK FORCE RETURNED TO THE STUNNING CITY OF Prague for our 93rd meeting, which was hosted by Brocade and the Czech domain registry CZ.NIC. In this issue of *IETF Journal* we share highlights of the week-long meeting and attempt to convey the spirit of the many people and discussions that make up an IETF meeting.

Our cover article provides an update on the status of exciting new work to simplify the deployment of security technologies on the Internet. We also have an article about the IETF Hackathon (page 14), a great introduction to the fast growing world of NETCONF and YANG (page 12), and a report on the live video Q&A session with Edward Snowden that took place prior to the meeting (page 11).

You can find out what ideas the community had for improving IETF educational and mentoring programs in our readout from the EDUNEXT BoF (page 16), and learn about one of the technology demonstrations on show during the Bits-N-Bites session (page 20).

Our regular columns from the IETF, IAB, and IRTF chairs, and coverage of hot topics discussed during the plenary meetings wrap up the issue. For more details of the Internet Area of the IETF in particular, a Working Group summary report is available at https://wiki.tools.ietf.org/area/int/trac/wiki/IETF93.

We are hugely grateful to all of our contributors. Please send your comments and suggestions for contributions to ietfjournal@isoc.org. Subscribe to the hardcopy or email edition by contacting us at https://www.internetsociety.org/publications/ietf-journal/ietf-journal-subscription.

ACME: BETTER SECURITY THROUGH AUTOMATION

By Richard Barnes

IT IS INCREASINGLY IMPORTANT TO ENSURE THAT ALL INTERNET APPLICATIONS RECEIVE certain minimum security assurances [RFC 7202]. For many years now, the IETF has required that the protocols it publishes have built-in security mechanisms [RFC 3552]. In order for users to benefit from these mechanisms, however, they need to be deployed by the operators of Internet applications.

Continued on page 4

MESSAGE FROM THE IETF CHAIR

By Jari Arkko

Jari Arkko, IETF Chair

IETF 93 IN PRAGUE WAS A RECORD MEETING IN TERMS OF ATTENDANCE: 1,384 PEOPLE from 65 countries were on site, and many more attended remotely. While our European meetings are always popular, this kind of attention is a testament to both how we are growing and the variety of interesting projects underway.

Another striking aspect of this meeting was the amount of coding that was done. The IETF Hackathon was held the weekend prior to the meeting (page 14); so many people showed up, we could barely fit them in one room. We also had a ETSI Plugtest to test 6TISCH protocol implementations, the Code Sprint to work on tools for the IETF, and the CrypTech meeting to hack on open-source hardware designs (page 9). I estimate over 150 people participated altogether—many were first-timers to the IETF, others were from major open source efforts, such as OpenDaylight, OPNFV, and RIOT. We look forward to more coding activities in the coming meetings. When you book your tickets to Yokohama, make sure to include time for some programming the weekend before the meeting: 31 October–1 November.

IETF 93 in Prague was a record meeting... While our European meetings are always popular, this kind of attention is a testament to both how we are growing and the variety of interesting projects underway.

The IAB technical plenary addressed vehicular networking (page 3). Christoph Sommer and William Whyte explained how networking in vehicles is developing and the security challenges it brings. I found this topic interesting, as I recently have been working on some related prototyping. It will be fascinating to see how the area develops in the future. I can see both local applications that run between vehicles, as well as Internet-based applications that use it to communicate with Internet-based servers or connect vehicles.

This was the first meeting of the NETVC Working Group. This group works on video codecs for Internet applications, the basis of browsers and other applications being able to exchange video streams in an efficient and interoperable manner. Work on security and privacy continued, essentially touching all the Working Groups to some extent.

The Bits-N-Bites event was very active this time. I spent some time trying to understand how I could install and test one of the open source projects that participated. This is the sort of thing that is exceptional at Bits-n-Bites: you can talk directly to effort leaders and programmers, and obtain first-hand knowledge.

We also had occasion to observe ways in which the IETF meeting is intentionally different than a traditional industry conference. Although promotional models are still common at some trade shows, they were not received as a constructive addition to the technical Bits-n-Bites session. The IETF failed to be clear enough that this wasn't

Continued on page 5

Recent IESG Document and Protocol Actions

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

WORDS FROM THE IAB CHAIR

By Andrew Sullivan

Andrew Sullivan, IAB Chair

IT IS ALWAYS SURPRISING TO ME HOW LITTLE TIME THERE SEEMS TO BE BETWEEN IETF meetings, at least by the time the meeting is upon us. IETF 93 in Prague was no exception. Still, the Internet Architecture Board (IAB) had plenty to report to the community.

Plenaries and IAB Engagement with the Community

We have heard people say that plenaries are too long and include too much reporting. Yet the plenary, the reporting we do, and our open microphone sessions are our basic accountability mechanisms. In Prague, the plenaries were in the morning. We shortened the technical plenary by 30 minutes to give people more "hallway time," and the session turned out to be somewhat crowded. But we're going to try again in Yokohama, in a combined plenary with the Internet Engineering Steering Group (IESG). While we don't expect to do this every time, we think it is worth trying these different approaches to see whether we can concentrate on protocol work, keep the meeting week as short as possible, and still engage with the IETF community.

One of the IAB's jobs is to be the interface between the IETF and other standards bodies. We were pleased to welcome Mr. Houlin Zhao, Secretary-General of the International Telecommunications Union (ITU). We don't expect regular visits of other standards bodies to the technical plenary; so we were happy that Mr. Zhao came, and we look forward to future successful collaboration with the ITU.

[W]e think it is worth trying these different approaches to see whether we can concentrate on protocol work, keep the meeting week as short as possible, and still engage with the IETF community.

Appeal

The IAB handles appeals when someone disagrees with an IESG appeal decision. The IAB takes this job seriously. Part of that job is to ensure that participants work within the IETF processes. In this case, the IAB concluded that the appellant needed to work within those other processes. See the full decision at https://www.iab.org/appeals/2015-2/response-draft-ietf-ianaplan-icg-response/.

When You Speak, We Listen

Because the IAB supervises the Request for Comments (RFC) Editor (via the RFC Editor Program and the RFC Series Oversight Committee), we publish documents pertinent to the RFC series. A recent change to the RFC series was the addition of Digital Object Identifiers (DOIs). The IAB asked for comments early, but DOIs were implemented before the IAB proceeded with publication of draft-iab-doi-04. It seemed to many that the IAB was asking for rubber-stamp feedback. That was not the goal, but we could have done better and we're grateful for the comments. In the future, we will use the following new process for developing these RFCs:

1. The proposal for the relevant change will be an Internet Draft (I-D) that outlines the plan and so on. We will process this like any other IAB stream document, with the appropriate community comment period. The draft will

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.

ACME: Better Security through Automation, continued from page 1

Deployment of security technologies presents several serious challenges for operators. The requirement for server authentication in Internet applications is especially challenging in operations. Most server authentication is based on the notion of a digital certificate [RFC 5280], a signed statement associating a domain name with the public key of a public/private key pair. Such a credential is a statement by a Certificate Authority (CA) that the holder of the corresponding private key can legitimately represent that identity.

Before making such a statement, the CA must verify that the holder of the private key is also the holder of the claimed identity, and it is this process that accounts for much of the cost and risk associated with setting up a secure Internet application.

This process is highly manual today: Informal usability tests by the authors indicate that it takes a skilled administrator 1–3 hours to complete these steps. Clearly, this is not scalable to contexts involving many domains or many certificates for the same domain.

To achieve more universal security, the certificate management process needs to be automated. We need a single protocol that can be integrated into application servers that need certificates, so that these servers can auto-configure themselves for secure operation.

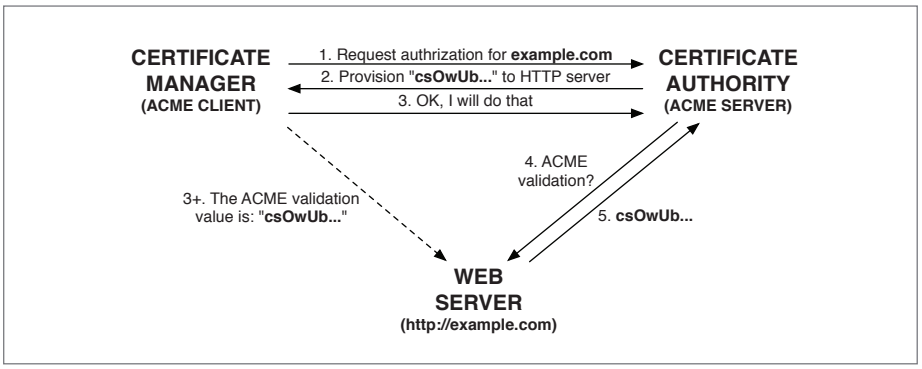
Some CAs do expose automated issuance APIs that support some issuance scenarios, such as CloudFlare's UniversalSSL service. But to date, these APIs have remained specific to each CA, which prevents the development of tools that can work with multiple CAs. The IETF ACME WG is working on a common protocol for managing certificates, known as the Automated Certificate Management Environment (ACME).

ACME is a simple client-server protocol based on HTTP. The client represents the applicant for a certificate (e.g., a web server operator), and the server represents the CA. The goal of ACME is to enable the CA to verify that the applicant owns some number of domains, and then to enable the applicant to request certificates for those domains.

ACME uses an extensible set of so-called challenges to allow the CA to verify an applicant's ownership of a domain name. When an applicant requests authorization for a domain, the CA challenges him to do something that only the domain owner should be able to do:

- Provision a file to an administrator-controlled directory on a web server
- Provision a certificate for an HTTPS virtual host
- Provision a DNS record

Once the applicant has chosen a challenge and notified the CA, the CA verifies that the challenge has been fulfilled, for example, by making an HTTP or DNS query to fetch the record that should have provisioned. If the expected value was provisioned, the CA knows that the domain owner has authorized this applicant to act on his behalf.



Overview of How ACME Validates Domain Ownership

Note that this challenge process only verifies that the applicant has practical control over a domain, which is not always the same as being the domain owner. For example, a DNS or web hosting provider might be able to use these techniques to get certificates for a customer's domain.

In addition, since the CA's validation queries are done over nonsecure channels, the CA is vulnerable to things like DNS poisoning attacks. For better or worse, this reflects the state of the art in the public key infrastructure today (regardless of ACME), so at least it's no worse. And the standardization ACME provides could make it easier to do validation from multiple perspectives, reducing the chance that an attacker can falsely demonstrate control of a domain.

Once an applicant has proved that he holds some set of domains, issuing certificates is simple. The applicant creates a Certificate Signing Request [RFC 2986] that expresses the public key and set of domains that the certificate should contain, and the CA responds with the certificate.

The separation between authorization and certificate issuance means that it is easy for an applicant with multiple domains to mix-and-match names in different certificates. For example, a web hosting provider that bundles 20 domains to a server could do one authorization transaction for each domain, then allocate those domains to server certificates in whatever way makes sense for the deployment environment.

All of this work on automation is at an early stage. ACME is being deployed by Let's Encrypt (https://letsencrypt.org/), a newcomer to the CA market, but it will likely need some adaptation through the IETF process before it can be taken up by other CAs. There's still a lot of opportunity for CAs and server operators to shape the ACME protocol to meet their needs by contributing in the working group.

Message from the IETF Chair, continued from page 2

appropriate. I have asked the IETF Administrative Oversight Committee to develop policies and practices to ensure that future meetings have clear guidelines to communicate expectations to sponsors and exhibitors.

We also had a visit from ITU Secretary-General, Houlin Zhao at the technical plenary. He put on the IETF t-shirt from his previous visit; we gave him a Hackathon t-shirt from this IETF. I'm looking forward to the code focus at ITU and the collaborative spirit that Zhou clearly represents.

A side event at IETF 93 (outside the meeting and organized by individuals) was a screening of the movie, *Citizenfour,* followed by a Q&A with Edward Snowden. Our local sponsor, CZ.NIC, gave us a warm Czech welcome at our social event at the Žofín Palace. The event ended with fireworks!

Finally, I thank all the participants, our hosts CZ.NIC, Brocade, and all the other sponsors for their help in making IETF 93 work so well. This was one of our best meetings. As always, there is still much to do. Most of the work at the IETF happens on the lists and virtual meetings, so for now, it is time to go back to those. Our next face-to-face meeting is in Yokohama. Interestingly, OpenStack and W3C are also meeting there around the same time, so I'm looking for even more possibilities for joint work.

Fireworks conclude the IETF 93 social event at the Žofín Palace.

Words from the IAB Chair, continued from page 3

call out areas that could vary due to implementation. When the comment period is over, we will proceed as usual toward publication (assuming it is warranted).

2. Implementation will follow the resulting RFC, but any variances due to implementation will be called out to the community on relevant IETF lists.
3. When everything is ready, a new I-D will be prepared to obsolete the earlier RFC and document what happened. It will be subject to community comment just to ensure it conforms with what people think has been implemented.

More changes will come as the RFC series evolves. We're listening carefully to ensure we're managing this well.

Other Highlights since IETF 92

The IAB made a statement on Trade in Security Technologies, and sent comments to the US Bureau of Industry and Security. The IAB also sent comments to the US Office of the Chief Information Officer and to the Internet Corporation for Assigned Names and Numbers (ICANN) Cross Community Working Group on Enhancing ICANN Accountability. We undertake these sorts of communications as part of our job to interact with external bodies. You can see all of our communications at https://www.iab.org/documents/correspondence-reports-documents/.

In the long run, attack response must grow as vigorously as the capabilities of Internet attackers.

With the Internet Society and in collaboration with FIRST 2015, the IAB sponsored the Coordinating Attack Response at Internet Scale (CARIS) workshop. The IAB undertakes workshops like this as part of its external liaison responsibility and because we are supposed to offer architectural guidance for the Internet. Attack response on the Internet is a critical part of the operational environment. The workshop aimed to strengthen the links among different organizations across the attack-response community. In the long run, attack response must grow as vigorously as the capabilities of Internet attackers. Kathleen Moriarty, a Security Area Director and the program chair for the workshop, gave a quick report about the workshop during the IETF 93 technical plenary. Look for the workshop report Internet Draft in an I-D repository near you.

The IAB also announced the Managing Radio Networks in an Encrypted World (MaRNEW) workshop (see page 18), which was held on 24–25 September. The IAB will share more on it at IETF 94.

References

[1] https://www.iab.org/documents/correspondence-reports-documents/2015-2/iab-statement-on-the-trade-in-security-technologies/.

VEHICULAR NETWORKS ARE EXPECTED TO SAVE LIVES BUT CARRY PRIVACY RISKS

By Carolyn Duffy Marsan

VEHICULAR COMMUNICATIONS SYSTEMS, WHICH HOLD THE PROMISE OF preventing crashes and saving lives, are poised for wide-scale deployment during the next decade. IETF 93's technical plenary session discussed the underlying networking technologies and protocols required by vehicular communications, as well as related privacy and security challenges.

Cristoph Sommer, assistant professor at the University of Paderborn, opened the discussion with an overview of the status of vehicular communication systems deployment, including the standards that have been developed to support these systems and field trials conducted to date.

Vehicular communications refer to networked vehicles talking to each other and to roadside nodes for safety warnings and traffic information. For example, when a vehicle brakes suddenly, it would automatically warn the cars behind it to stop as a way of preventing rear-end collisions.

Sommer said the idea for vehicular communication systems date back to the 1970s, but it wasn't until mobile networking became ubiquitous in the 1990s that systems such as General Motors' OnStar and BMW Assist became viable.

"After 2000, the sharp increase in computing power made it possible to deploy fully distributed and highly reactive ad hoc systems that allow cars to directly communicate to other cars on the road," Sommer said. "This generated a number of activities, including lots of coordinated research programs... between the biggest manufacturers in the United States, Europe, or Japan. That culminated in numerous large-scale field trials that concluded this technology is hugely beneficial."

The US National Highway Traffic Safety Association (NHTSA) concluded that two simple applications—intersection movement and left turn assist—could prevent 500,000 crashes and save 1,000 lives annually. In August 2014, NHTSA said it is going to propose rulemaking for all new vehicles to be equipped with vehicular networks by 2020. Indeed, some US car manufacturers say they will deliver this technology as early as 2017.

The US National Highway Traffic Safety Association concluded that two simple applications ... could prevent 500,000 crashes and save 1,000 lives annually.

Meanwhile, innovators like Google are developing autonomous driving systems, which would enable self-driving cars or platooning, where a vehicle driven by a human is followed closely by several autonomously driven vehicles that accelerate or decelerate based on the lead car's actions.

"Vehicle networking represents the third evolution in networking," Sommer said. "The first was traditional wired networks with nonmoving, static configurations. The second was mobile ad hoc networking, based on wireless mobile technology and dynamic configuration. The third is vehicular ad hoc networks, which are a completely new field of deployment."

The lower level network protocol for vehicular communications already has been developed: Dedicated Short Range Communication (DSRC), which is the underlying "wire" for these applications. DSRC comprises extensions to the IEEE 802.11 standards for wireless communication. DSRC uses: 802.11e for quality of service; 802.11j-2004 for half-clocked operations, which are a more robust form of communication; and 802.11p for operation in the 5.9 GHz band and a new mode called OCB for Outside the Context of a Basic Service Set.

"OCB mode allows devices at all times to transmit frames addressed to a wildcard service and to always receive wildcard service packets," Sommer explained.

Sommer said the 5.9 GHz band is reserved for vehicular communications, with the United States dedicating seven channels for communication and Europe dedicating five channels. While these channels have no licensing costs, they have strict usage rules to ensure that only vehicular networks operate on these frequencies.

Sommer said IP-based communications only fit into a small space in the vehicular networking paradigm because routing requires too much network overhead for most applications. Only entertainment applications might support data streaming to cars, he said.

"It's a necessity to assemble a new stack that needs to meet lots of old challenges, such as multicast, low load, and low delay, and new challenges such as highly dynamic topology, safety, partitioning, and complex mobility," Sommer said.

Three standards have been developed to meet the challenge of vehicular networks:

- **IEEE 1609 WAVE, for Wireless Access in Vehicular Environments, is being adopted in the United States.** The WAVE stack features: a physical layer; a MAC (Media Access Control) layer with channel coordination; an LLC (Logical Link Control)

layer; and finally the Wave Short Message Protocol or WSMP. Sommer said it is possible that IPv6 and TCP/UDP could ride upon the LLC layer, but more development is needed to make that happen. WAVE supports single or multiple radio devices, with single radio devices periodically tuning to the Control Channel (CCH) to ensure receipt of important messages.

- **ETSI ITS G5, or Intelligent Transportation Systems, is being adopted in Europe.** This standard focuses more on multiradio scenarios, with one radio always being tuned to the CCH. This stack features Cooperative Awareness Messages, which are periodic messages about speed and location of surrounding vehicles. ITS G5 stack consists of physical and MAC layers based on IEEE 802.11p, with Decentralized Congestion Control (DCC) that handles traffic management tasks for the access layer, the networking and transport layer, and the facilities layer. This standard also features Geonetworking, which enables disseminating information to an area determined by a particular latitude and longitude.
- **ARIB T109, or 700 MHz Band Intelligent Transpot Systems, which was designed in Japan.** Sommer didn't describe this standard in detail.

"The outlook for vehicular networking leaves us with a lot of applications, but each is tailor made to a specific use case with each also using a very different part of the network," Sommer said.

Among the applications for vehicular networking that Sommer cited along with the corresponding standards were: electronic payment through IEEE 1609.11; traffic signal timing through SAE SPAT; periodic broadcast safety messages through ETSI CAM and IEEE/SAE BSM; and geo-based broadcasting of warnings using ETSI DENM.

"Aside from all of these apps, vehicle networking opens up a whole lot of opportunities with one of the biggest being the merging of in-vehicle and vehicle-to-vehicle communication," Sommer said. "This will be the first time we can do sensor data fusion of local vehicle sensors and sensors in other vehicles. So if another car tells me there is an obstacle in the road, I might try to double-check using my computer vision system."

After Sommer concluded his talk, William Whyte, chief scientist of Security Innovation, discussed the security and privacy aspects of vehicular networking.

Whyte said vehicular networking has all the security challenges typical of networks, such as confidentiality, integrity, authenticity, authorization, and nonrepudiation, as well as cryptography requirements. However, vehicular networking adds privacy concerns such as not wanting to enable tracking or traffic analysis.

"If you have this radio in your car—and the plan in the United States is that cars will be mandated to be equipped with these radios in 2020 or 2022—you don't want that radio to give you automatic speeding tickets. You don't want wide-scale tracking to be possible," Whyte explained.

In addition, vehicular networking involves constrained devices in terms of size, power, storage, and connectivity, which puts limits on the hardware-based security capabilities. The communications are constrained because there are a limited number of 10 MHz channels.

"If you have 200 or 300 vehicles in an area, and they all have you communicate at the same time, you need to make sure the communications overhead is not too much," Whyte said.

Whyte identified several security-related efforts within the IETF that may overlap with vehicular networking, due to similar certificates, automated certificate issuance, and certificate management.

"One thing I hope we will do in the next few years is work more closely with existing technologies and existing technology groups to make sure that we don't reinvent the wheel," Whyte said.

In terms of the vehicular networking trust model, the plan is to use IEEE 1609.2 and ETSI TS 103 097 certificates. The signed PDUs (Protocol Data Units) are authorized by certificates, with Service Specific Permissions within applications. The Certificate Authority ensures that the sender is entitled to those permissions. The receiver checks that the PDU is consistent with permissions.

For example, emergency vehicles would have special permissions to allow them to send messages to other vehicles saying essentially "get out of my way," Whyte explained.

In terms of security performance, vehicular network standards use Elliptical Curve Digital Signature Algorithm (ECDSA) with 256-bit curves for cryptography. Due to the significant security overhead of the

Continued on next page

Attendees listen attentively at a packed IAB Technical Plenary.

Vehicular Networks Are Expected to Save Lives but Carry Privacy Risks, continued

digital signatures, IEEE permits implicit certificates with no explicit signatures to improve performance, while ETSI uses only explicit certificates.

Another performance concern is that the system can handle 600 incoming messages per second. While the EU is using hardware acceleration to improve performance, the United States is filtering messages and using butterfly keys, which are a one-time request to the certificate authority to generate a certain number of distinct certificates.

Whyte said new legislation will be needed to prevent vehicles from being tracked. One technical way to minimize tracking is for a vehicle to receive multiple certificates for an application so that it can be tracked here and there but not on all points in between. Another privacy threat is that an insider at the Certificate Authority (CA) could track a vehicle, or the CA could be hacked.

One precaution is that vehicular networks won't reveal information about the previous movement of a vehicle. "If a car is stolen in June, it can be tracked going forward, but not the movements before," Whyte said.

The ETSI model requires that all packets sent over geonetworking are signed at the geonetworking layer; this indicates that the sender has permissions to ask that a packet is forwarded. In addition, packets are verified before forwarding. By preventing unauthorized requests for forwarding, congestion is reduced.

"This is a further optimization because if you're signing at the network layer anyways, you don't need to sign at the application layer," Whyte said.

Vehicular networks carry advertisements for services, such as high-speed towing or electric vehicle charging, but the network protocols assume a buyer beware strategy. Plus, if hardly anyone uses a service, the buyer's privacy might be at risk.

"One outstanding research area in privacy is… if you have multiple apps such that the combination of them is a fingerprint for your device," Whyte said. "The device should support some kind of separation such as a separate virtual device for each of the apps. It has yet to be seen if that works."

Whyte said that the key security system challenges in preparing vehicular networks for deployment in the next decade are working within channel capacity and processing constraints, while supporting different trust levels and protecting privacy against likely attacks. The future, however, involves integrating vehicular networks into the general Internet of Things security framework.

The future, however, involves integrating vehicular networks into the general Internet of Things security framework.

"Vehicular networks will be a subset of machine-to-machine systems; in general, we will be moving into their frameworks over the next few years to make sure we can scale," Whyte said. "We need to manage congestion in adversarial settings as DoS attacks might have real impact in the future. And we need to harmonize policy about which applications can use which channels."

At the end of the formal presentations, IAB member Russ Housley moderated a question-and-answer session.

Allistair Woodman asked whether the information collected when a vehicle crosses a bridge or tunnel or pays a toll can be subpoenaed and used against the driver.

"The governments are aware that they are mandating this and looking on very suspiciously at the privacy concerns," Whyte said. "The whole purpose is to save lives. If 1 percent of people turn it off to avoid being tracked, there is a 2 percent drop in effectiveness. Everyone takes seriously the idea that information won't be used by law enforcement and won't be subpoenable."

Christian Huitema asked if there are any plans to bring the technology developed for vehicular networks into other domains such as the IETF.

"The technology is all public, and none of it is subject to patent," Whyte said. "We're building PKI to the capacity of issuing 1,000 certs a year to every vehicle on the road. That massive scale should be possible to support other uses. I'd be very interested in exploring other uses."

Finally, Charlie Perkins asked if there is a difference in the networking protocols for car with drivers and self-driving cars.

"On the application layer, there will be huge differences depending on who the information is for, whether a human or an autonomous vehicle," Sommer said. "But at the physical layer and the MAC layer, they don't care."

ITU Secretary-General Shares His Vision

At the conclusion of the IAB plenary session, ITU Secretary-General Houlin Zhao addressed the audience. He emphasized the importance of a strong relationship between the ITU and the IETF.

"I would like to strengthen cooperation between the ITU and the Internet Society, the IETF, the IAB, and ICANN for the benefit of our global families," Zhao said, adding that he is focussed on helping the many people who are not yet Internet users. "I encourage you not only to talk about new technologies for those who are already connected, but also encourage you to find innovations for those not connected with technologies that are physical and sustainable."

CRYPTECH AT IETF 93

By Karen O'Donoghue

MOST PEOPLE THINK OF THE IETF AS SOFTWARE AND PROTOCOLS, BUT AT IETF 93, a CrypTech workshop gave participants the opportunity to work together on open source hardware: cryptographic engines developed by a multinational team designed to restore the public's trust in cryptography.

What Is the CrypTech Project?

The CrypTech project was motivated by the loss of trust in cryptographic algorithms and products resulting from revelations of pervasive monitoring and potentially compromised algorithms and products. It evolved out of discussions within the IETF and Internet Architecture Board (IAB) community.

CrypTech was founded as an independent international development effort to create trusted, open source designs and prototypes of an inexpensive hardware cryptographic engine. The first output from CrypTech will be a trusted reference design for a Hardware Security Module (HSM, a specialized device used to securely store the public/private key pairs used with digital certificates, most commonly used in Secure Sockets Layer/ Transport Layer Security (SSL/TLS). CrypTech's open source HSM can be used as the basis for commercial products; CrypTech supports the Internet community by providing an open and auditable alternative to existing crypto devices. CrypTech's first use case is for HSMs. However, there are other applications for this type of technology. The CrypTech development model is based on a composable system that lets the designer select the bare minimum of components needed, thereby further reducing the risk and attack surface of a CrypTech-based device.

CrypTech supports the Internet community by providing an open and auditable alternative to existing crypto devices.

CrypTech is starting from the bottom up by implementing a wide variety of cryptographic algorithms to be loaded into a specialized Field Programmable Gate Array (FPGA), designing the hardware required for a true random number generator (TRNG), building high-assurance auditing and management tools for key and cryptographic operations, and writing the necessary support software to link the CrypTech HSM to existing public key infrastructure (PKI) applications such as DNSSEC and RPKI.

By moving the research and development (R&D) associated with hardware PKI to the Internet community, CrypTech can dramatically reduce costs. This gives enterprises the opportunity to make much greater use of cryptographic hardware, thus increasing overall security compared to software-based key management.

Why Hardware?

CrypTech's goal of designing a hardware cryptographic device is significantly more complicated than writing open source software. Because the project must integrate both hardware and software components, there are also real materials costs that most open source projects don't incur. For example, CrypTech has to build a tamper-proof system, so that if the hardware falls into the wrong hands or under physical attack, the device won't release the keying material.

CrypTech is also building a true random number generator that requires some specialized hardware components to be a source of "randomness." Cryptographers have always been critical of algorithmic methods of generating random numbers; poorly written random number algorithms have been critical factors in security failures. A true random number generator is an important building block in a secure cryptography infrastructure. CrypTech's initial TRNG has been tested by a number of reputable sources and the reports are amazingly positive.

The most significant hardware component in the CrypTech project is the use of an FPGA for crucial cryptographic

Stephen Farrell (center), research fellow at CONNECT, with other participants during CrypTech at IETF 93.

Continued on next page

WHAT IS A HARDWARE SECURITY MODULE?

A hardware security module (HSM) is a specialized device designed to securely store the public/private key pairs used with digital certificates. An HSM provides significant additional security for enterprise PKI and CAs because it removes the need—and the risk—of storing keys on disks or in memory.

When an HSM safeguards a private key, it must also be able to perform cryptographic operations with those keys. For example, when a CA needs to sign a digital certificate, it sends the information to the HSM and requests that the HSM create the digital signature. The HSM signs the certificate, and sends back the result.

Storing keys out of reach of any application ensures that they are never exposed outside of the HSM and cannot be stolen, as they cannot be retrieved from the HSM.

HSMs implement a combination of storage, cryptographic, and auditing functions, including:

- Key storage, backup, and management, including hardware tamper resistance.
- Accelerated cryptographic processing, including common hash and encryption algorithms.
- A true random number generator.
- System management and integrity, including logging, authentication, and auditing.

functions. When an encryption or hash algorithm is written in software and built into a general-purpose central processing unit (CPU), or loaded into a general-purpose computer, such as a Windows or Linux system, it remains very vulnerable to attack. Software can be changed, often very subtly. Memory contents can be read during operations. Even the length of time to perform operations can be measured and reveal information. However, when the cryptography is performed in a dedicated hardware device, completely inaccessible to the normal operating system, these weaknesses are reduced significantly.

The CrypTech Workshop at IETF 93

From its very beginnings, the motto of the IETF has been "rough consensus and running code." The weekend preceding IETF 93 was filled with activities that highlight the development of open source running code including the Code Sprint, the Hackathon (page 14), and finally the CrypTech (www.cryptech.is) workshop. All of these activities involved open source software, but CrypTech also included open-source security hardware.

During this workshop, participants were able to configure their own prototype hardware based on CrypTech designs and software. Participants were able to bootstrap the cryptographic services on the prototype hardware, configure it to use PKCS11 for communications to a server, configure OpenDNSSEC to get its keys from the CrypTech prototype, and finally use the system to perform DNSSEC zone signing.

An overview of CrypTech, including results from the workshop, was discussed in the IETF Security Area Advisory Group (SAAG) and IRTF Crypto Forum Research Group (CFRG) sessions. Detailed questions about the status of implementation, including specific algorithm support, illustrated the interest in and relevance of the effort.

Hardware at use during CrypTech at IETF 93.

In addition, George Michaelson summarized his workshop experience and posted photos in a detailed blog post at https://blog.apnic.net/2015/07/21/its-alive-blinkenlights-in-cryptech-ietf93/.

Community Support for CrypTech

Open source has been one of the major success stories of the Internet, and open source software is part of every piece of hardware and software produced today. The CrypTech project is no different: by bringing an open source philosophy to cryptographic software and hardware, the plan is to increase trust and transparency, offer alternatives to commercial products, and reduce costs. To learn more about CrypTech, including how you can help support this important effort, visit https://cryptech.is.

During this workshop, participants were able to configure their own prototype hardware based on CrypTech designs and software.

SNOWDEN MEETS THE INTERNET ENGINEERING TASK FORCE

By Mark Nottingham

Based on a 20 July 2015 post on https://www.mnot.net/blog/2015/07/20/snowden_meets_the_ietf.

DURING IETF 93, APPROXIMATELY 170 PARTICIPANTS ATTENDED A SCREENing of *Citizenfour,* the movie about Edward Snowden's revelations and the information that led the IETF to declare such pervasive monitoring as an attack on the Internet itself. The audience, the very people who design and maintain the Internet, watched the movie intently, their eyes glued to the screen; not a laptop was open.

There was also a surprise guest: Edward Snowden via video chat. After a standing ovation, Snowden shared his perspective on the very technology we're defining—from DNSSEC and DANE to WiFi privacy. Audience questions were answered, and we got a rare insight into both his motivations and the technical capabilities and mindsets of those performing the pervasive monitoring attack.

Audience members say that they were impressed by the depth of his thinking. Several times he cautioned against making the Internet "anti-NSA" (National Security Administration); instead, he says our focus should be on making the user our primary stakeholder. His statement especially resonated for me because last week when we were discussing the Unsanctioned Web Tracking finding in the TAG (W3C Technical Architecture Group), Tim Berners-Lee exhorted us to design for the Web we want, not just the Web we have today.

A Word about How It Happened

This was not an official IETF event; rather, it was entirely an effort of individuals working within the rules for requesting a room at IETF meetings. When we floated the idea originally, some folks were uninterested; they thought that everyone who wanted to see the movie already had. In fact, we received enough donations to cover the screening and to make a 670 Euro donation to the Courage Foundation (https://courage-found.org/)—a fantastic result.

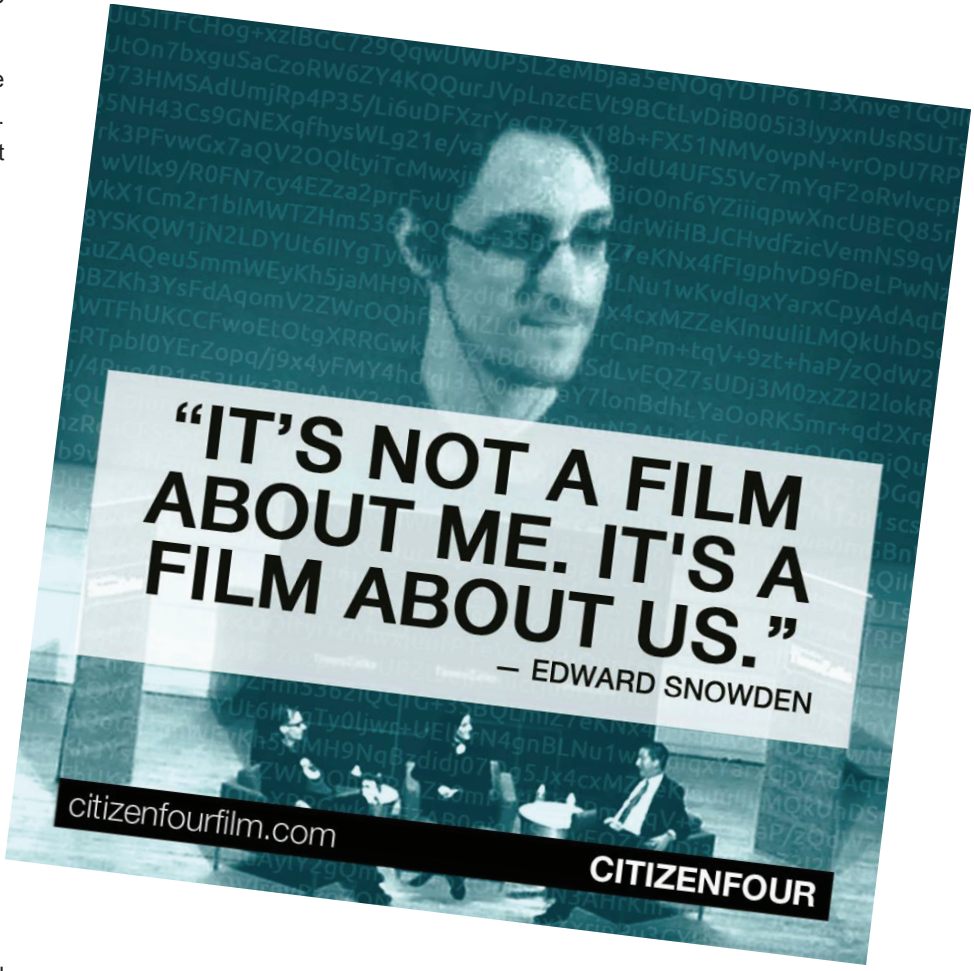
Many thanks to Daniel Kahn Gillmor for arranging the Q&A session and to Jake Applebaum and Laura Poitras for facilitating the screening.

Snowden shared his perspective on the very technology we're defining—from DNSSEC and DANE to WiFi privacy.

Links

Video: https://www.youtube.com/watch?v=0NvsUXBCeVA&feature=youtu.be

Transcript: https://gist.github.com/mnot/382aca0b23b6bf082116a transcript



YANG AND NETCONF/RESTCONF GAIN TRACTION IN THE INDUSTRY

By Mahesh Jethanandani and Benoît Claise

IN 2003, REQUEST FOR COMMENT (RFC) 3535, "OVERVIEW OF THE 2002 IAB Network Management Workshop"[1] documented the outcomes of a dialog between network operators and protocol developers about focusing the IETF on future network management work. The workshop identified 14 operator requirements and identified 'ease of use' as a key requirement for any new network management system. This ease of use includes an ability to manage a network, not just a device in the network, and asserts that there should be a clear distinction between the configuration, operational, and statistical information of the device. The requirements also include the ability to stage a configuration, validate it before committing, and roll back to the previous configuration in case of failure.

These 14 operator requirements led to the creation of the NETCONF Working Group (WG) that same year, the NETMOD Working Group in 2008, and the development of core data models for network management. The work resulted in XML-based Network Configuration Protocol (NETCONF) RFCs 6241, 6242, 6243, and 6244 in 2011 (respectively revised from 4741, 4742, 4743, and 4744), and the associated data modeling language YANG RFCs 6020 and 6021 in 2010.

Over the last couple of years, NETCONF and YANG have gained traction in the networking industry. They've moved from the definition phase into the implementation phase. At the IETF, the number of YANG models under development has seen incredible growth. New YANG models are being developed in the Operations and Management (OPS) area, as well as in the Routing (RTG), Internet (INT), Transport (TSV), and Security (SEC) areas. But the most impressive YANG model adoption comes from the open source OpenDaylight project, where the Lithium release has seen the publication of more than 480 YANG models[2].

Other Standards Development Organizations (SDOs) have also initiated YANG model development projects. For example, Metro Ethernet Forum was an early pioneer in developing Service OAM (SOAM) Fault Management (FM) and Performance Management (PM) YANG models; it is currently working on service-level YANG models[3] (figure 1). In addition, the Institute of Electrical and Electronics Engineers (IEEE), has approved a project for 802.1x and 802.1q models, with interest in developing an 802.3 model. Similarly, the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) is seeing interest in the development of a G.8032 model. Models from all the SDOs can be found in GitHub (https://github.com/YangModels/yang).

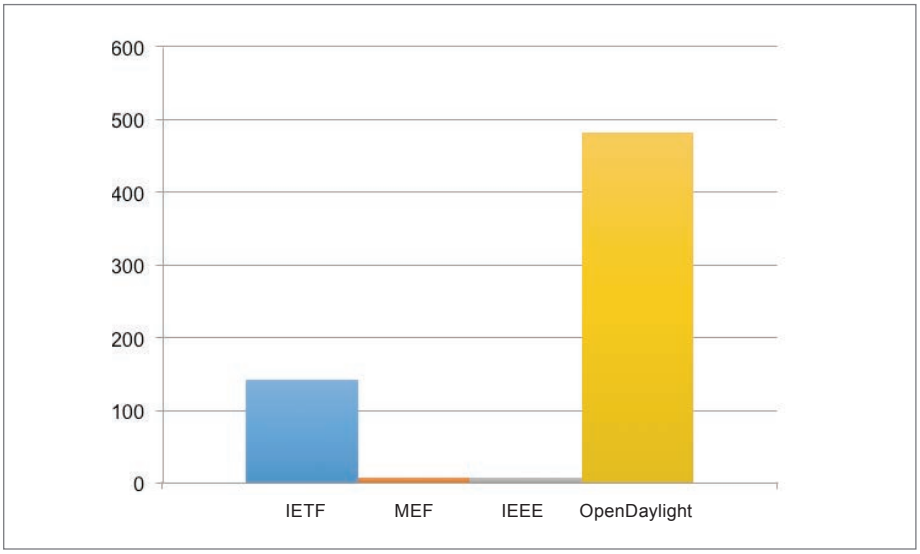


Figure 1. YANG Models in the Industry

The rapid growth in the number of YANG models is not without its challenges, primary among them is the coordination of models. While all models do a great job of defining how particular features can be configured or monitored, they also must interact with models being developed in both the IETF and other SDOs. The first practical coordination is happening in the routing area undertaken by the Routing Area YANG Coordination Forum[4]. Coordination of the YANG development work in the IETF and other SDOs falls under the umbrella of the Operations and Management Area (OPS) area director, Benoît Claise, with the help of the YANG Model Coordination Team[5].

IETF Working Groups that cover aspects of YANG model development include:

- LIME (OAM YANG models)
- L3SM (L3VPN service YANG model)
- SUPA (consistent policy YANG models)
- I2NSF (security-related YANG models)

To help with the development of YANG models, the YANG doctors[6] are available both via email and during the week of IETF meetings in YANG advice/editing sessions. In addition, there are several tools available for the development and compilation of YANG models (see http://trac.tools.ietf.org/area/ops/trac/wiki/YangModelCoordGroup for a complete list).

Probably the most important tool is pyang, a python-based YANG compilation tool that does syntactic checking and enables

generation of output formats, such as UML, a tree based model, YIN, and so forth. These tools must be run with an IETF option set in order to check for YANG guidelines in RFC 6087. Many YANG models still don't compile correctly (see http://www.claise.be/IETFYANGPage-Compilation.html). An online, graphical equivalent of the pyang tool is found at http://yangvalidator.com; it takes a YANG file or an IETF draft/RFC, extracts the model, and then validates the model.

The rapid growth of YANG models is not without its challenges, primary among them is the coordination of models.

Thanks to the extent of the development and implementation experience of some YANG models, the NETMOD WG has been getting feedback on YANG 1.0. Based on the feedback, a YANG version 1.1 is currently being finalized. This new version is a maintenance release of the YANG language; it addresses ambiguities and defects in the original specification.

With NETCONF and YANG specified, operators can start using them for configuration and monitoring. Some operators, however, have already started to use the proprietary REST APIs provided by different vendors to manage their networks. RESTCONF is a REST-like protocol running over HTTP for accessing the data defined in YANG. The REST-like API is not intended to replace NETCONF, but rather provide a simplified interface, thereby meeting a need of application developers. For that reason, the NETCONF WG decided to add support for the RESTCONF protocol in its charter. RESTCONF supports two encoding formats: XML and JSON.

Although often overlooked as a capability, devices can also send notifications defined in the YANG model. The newly adopted NETCONF charter includes an update to the NETCONF Event Notifications[7] and the development of a subscription-and-push mechanism that allows client applications to request notifications about changes in the data store. These capabilities will open NETCONF to the world of telemetry: pushing data towards the network management system (NMS) applications.

One result of the popularity of YANG is that now operators wanting to develop their own protocol for management use YANG as the data modeling language. This includes CoMI, which defines a management interface for constrained devices. Even among existing protocols NETCONF and RESTCONF, there are different encodings (e.g., XML and JSON) for YANG models.

Ultimately, what counts is the data models. There is a clear need across the industry for standard data models in order to ease the management and, more precisely, the programmability of multi-vendor networks. YANG has clearly positioned itself as *the* data model language for these standard models. It is up to us at IETF to coordinate all the YANG models if we want them to work seamlessly together.

References

1 http://tools.ietf.org/html/rfc3535.

2 http://www.claise.be/YANGPageMain.html.

3 https://wiki.mef.net/ (requires login).

4 http://trac.tools.ietf.org/area/rtg/trac/wiki/RtgYangCoord.

5 http://www.ietf.org/iesg/directorate/yang-model-coordination-group.html.

6 http://www.ietf.org/iesg/directorate/yang-doctors.html.

7 http://datatracker.ietf.org/doc/rfc5277/.

GOING MAINSTREAM: A RECAP OF THE IETF 93 HACKATHON

By Charles Eckel

Originally published at https://communities.cisco.com/community/developer/opensource/blog/2015/08/03/going-mainstream--recap-of-ietf-93-hackathon.

IETF 93 IN PRAGUE KICKED OFF WITH A HACKATHON THE WEEKEND OF 18–19 July. Following the success of the first IETF Hackathon at IETF 92, Cisco DevNet and the IETF teamed up again to host it.

More than 135 participants formed into 18 teams and worked across 15 different technologies. Among the participants were many first time IETFers from various open source communities and universities. This was great to see, given the stated goals of the Hackathon to bring running code back into the IETF, bridge the gap between open source and open standards, and introduce more developers and young people to the IETF. It was a huge success by these and other measures, and established the Hackathon as a valuable and vibrant addition to the IETF community going forward.

The Hackathon featured technology relevant to many IETF working groups (e.g., 6TISCH, ACE, BIER, DANE, HOMENET, HTTPBIS, MPTCP, NETVC, NETCONF, SFC, and SIDR) and corresponding open source projects (e.g., Dalla, Kea, OpenDaylight, OpenDNSSEC, OPNFV, Quagga, RIOT, and SPUDlib).

How Does It Work?

The event began at 09:00 with technology champions introducing each technology and proposing sample projects. Next, champions and participants self-organized into teams, including some with participants from multiple IETF Working Groups and open source communities. This mix of people, ideas, and cultures gave rise to some of the most interesting projects and highlights the opportunity for long-term benefits that extend well beyond those achieved over the weekend.

The energy in the room was contagious. Motivated by altruistic aspirations, participants worked cooperatively and diligently to develop the standards that provide the Internet's foundation, as well as the open source implementations that validate these standards and make them easier for others to use.

Raspberry Pis were among the many tech goodies available to win.

Those who didn't have other IETF activities stayed for dinner, and many worked late into the night—well beyond the advertised closing time of 21:00. But this is not to say that the day was void of fun. There was, of course, plenty of that.

There was no loss of enthusiasm the next morning; many people arrived before the advertised start time of 09:00. A few new faces arrived; they were welcomed and either plugged into existing teams or formed new teams.

The Presentations

By midafternoon Sunday, the teams presented their accomplishments to the judges: Jari Arkko, IETF chair; Ray Pelletier, IETF administrative director; Rick Tywoniak, director of Cisco DevNet; and Martin Thomson, IETF draft author and tireless contributor. The judges were left with an unenviable task given the vast array of projects, including tests, experiments, implementations of protocols, and new services. At stake were bragging rights and first dibs on tech goodies, such as Raspberry Pis, Arduinos, and IoT accessories, and tickets donated by Brocade to the IETF's social event.

Among the winners were three projects that the judges awarded "Best of Show":

- ACE–Key Technology Award
- DNSSEC–Broadest Coverage Award
- HOMENET–Best WiFi Router Feature Award and Cool Kids Award

Bits-N-Bites

The awards ceremony concluded the Hackathon, but the payoff for all the great work was yet to come. Hackathon projects were shared more broadly with the IETF

Results and insights from the projects were fed into Working Group sessions held throughout the week.


Hackathon participants worked cooperatively in teams.

Participants at the second IETF Hackathon make their presentations.

community at an extremely well-attended Bits-N-Bites session.

Results and insights from the projects were fed into Working Group sessions held throughout the week. One of the best examples was from the NETVC Working Group meeting. According to Nathan Egge of Mozilla, "Over the course of two days a team of 11 participants (both local and remote) hacked on the Thor and Daala codebases, open source video codecs that have been contributed by Cisco and Mozilla respectively to the NETVC Working Group. The results of the Hackathon included adding support for Thor to the AreWeCompressedYet.com testing framework, running four experiments using Thor's motion compensation within Daala, and fixing a long-standing issue in Daala by adding the CLP post-processing filter from Thor. Cisco committed changes to Daala and Mozilla committed changes to Thor, which shows the collaborative spirit of the IETF. Having a Hackathon is an excellent way for new ideas to be tested out in running code, and NETVC will be back for the IETF 94 Hackathon in Yokohama."

The complete set of technologies and projects, as well as photos and a video summary are available via the event Wiki at https://www.ietf.org/registration/MeetingWiki/wiki/93hackathon.

From the main Hackathon page (https://www.ietf.org/hackathon/) it is easy to navigate to information about all of the IETF Hackathons. The IETF and open source communities are encouraged to reference these sites to help with their ongoing work.

What's Next?

The IETF has already announced a Hackathon at IETF 94 in Yokohama, and Cisco DevNet is on board to sponsor it again. In addition, the Hackathon is now a regular part of IETF meetings. Sponsorship opportunities exist for anyone wanting to show their support for this important effort. Contact Ray Pelletier for details.

Stay Informed

To stay informed about past and future IETF Hackathons, subscribe to hackathon@ietf.org.

It was a huge success by these and other measures, and established the Hackathon as a valuable and vibrant addition to the IETF community going forward.

Some participants appear to think they are not worthy, but their work proved them wrong.

IETF 93 BOF: EDUNEXT

By Mirjam Kuehne

IN *IETF JOURNAL,* VOL. 10, ISSUE 1, I WROTE ABOUT THE ACTIVITIES OF THE IETF Education Team (http://ietf.org/edu/). Since then, in addition to organizing the Sunday tutorials and Working Group (WG) chair sessions, we've reviewed our portfolio, our training methods, the audiences we've reached, and the topics we've covered. It brought up a number of questions: Should we keep the Sunday tutorials? Should we provide more online training in the form of short, topical videos? Are webinars the way to go? How do we reach other audiences, such as the open source community? Should we review our charter or does it already cover both current activities and possible changes and adjustments in the future? Finally, and most important, some Edu Team members will retire soon—how will we find new members?

[In] addition to organizing the Sunday tutorials and Working Group (WG) chair sessions, we've reviewed our portfolio, our training methods, the audiences we've reached, and the topics we've covered.

In addition, we began collaborating more with the IETF mentoring program and looking at ways to more effectively collaborate and share resources. Would it make sense to merge the Edu Team and the mentoring program?

Our discussions culminated in both the organization of the EDUNEXT Birds-of-a-Feather (BoF) session at IETF 93 chaired by Dan Romascanu and myself, and an Internet Draft written by Nalini Elkins and myself in preparation for the BoF.

The main goal of the EDUNEXT BoF was to obtain input from the community on the aforementioned questions—for both the Edu Team and the mentoring program. The BoF was very well attended; it started with a description of the activities of the Edu Team and the (much younger) mentoring program. The remaining time was spent in active, sometimes heated, and chaotic discussion. It was great to see how passionate people are about the IETF, sharing knowledge, and integrating newcomers into the process. We also had a number of newcomers share their experiences; everyone was a newcomer once and can remember how it felt to attend their first IETF meeting—I certainly do!

Most of the session was dedicated to the mentoring program; it only recently started and is still defining its mission and goals. But, the Edu Team also got a lot of attention. For example, interesting ideas were raised about regional mentorships and remote training hubs. By the end of the session, we had answers to most of the questions we'd posted at the beginning of the BoF.

- Keep the Sunday tutorials, but consider providing shorter training sessions (shorter than two-hour slots).
- The Edu Team charter is good. It enables both process oriented and technical tutorials, and therefore needn't be adjusted.
- Continue to provide technical tutorials (not only process-oriented).
- Don't only target newcomers; also target existing participants, Working Grop chairs, and area directors.
- Consider providing content that is more digestible over the Internet, such as videos and webinars.
- Gather more feedback after each tutorial.
- Follow up with newcomers after their first IETF meetings to find out what worked for them and what didn't.

There was strong sentiment that the Edu Team should not merge with the mentoring program at this stage. First, the mentoring program needs to better define its goals, plus it needs both a charter and a mailing list. Also, participants felt that it is not clear what newcomers need. There is more than

Mirjam Kuehne, EDUNEXT BoF chair, presents the BoF poster.

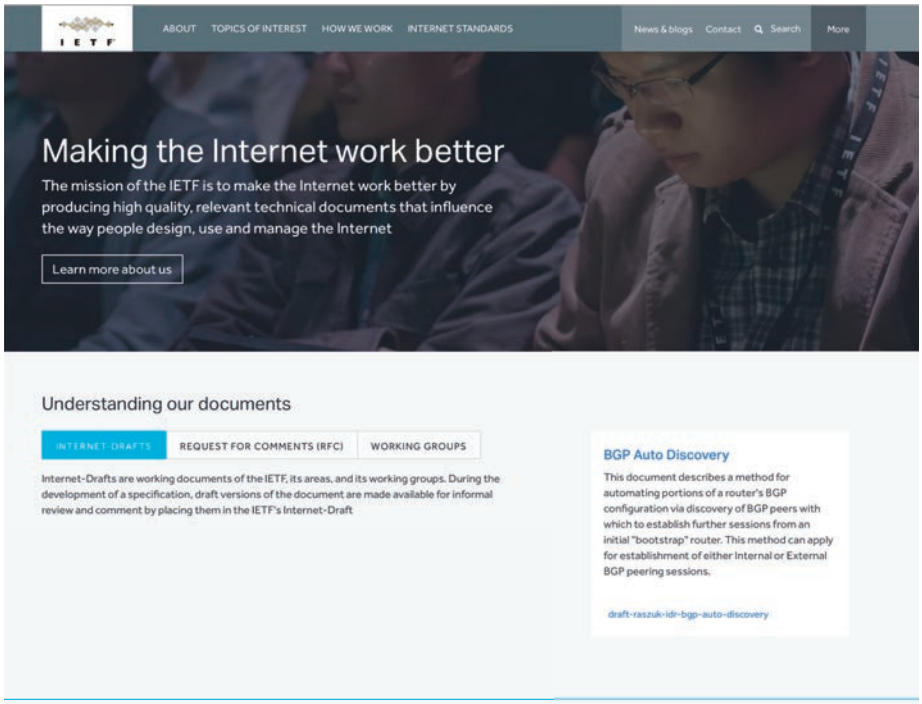
We also had a number of newcomers share their experiences; everyone was a newcomer once and can remember how it felt to attend their first IETF meeting—I certainly do!

one type of newcomer—each individual comes to the IETF with a different background and different goals. Jari Arkko, IETF chair and the area director who oversees the activities of the Edu Team and the mentoring program, will work with the mentoring team to further define their activities.

Throughout the process, Arkko was extremely supportive and helpful. It is good to see that our activities are deemed valuable and useful, and that they are becoming more visible in the overall IETF structure.

I'm very happy that we found two new members: Karen O'Donoghue and Dan Romascanu. Nalini Elkins will stay on the Edu Team to ensure continued positive collaboration between the mentoring program and the Edu Team. And Greg Wood agreed to be on the Edu Team during the IETF website restructuring process (and hopefully longer). A list of Edu Team members can be found at http://ietf.org/edu/team-members.html.

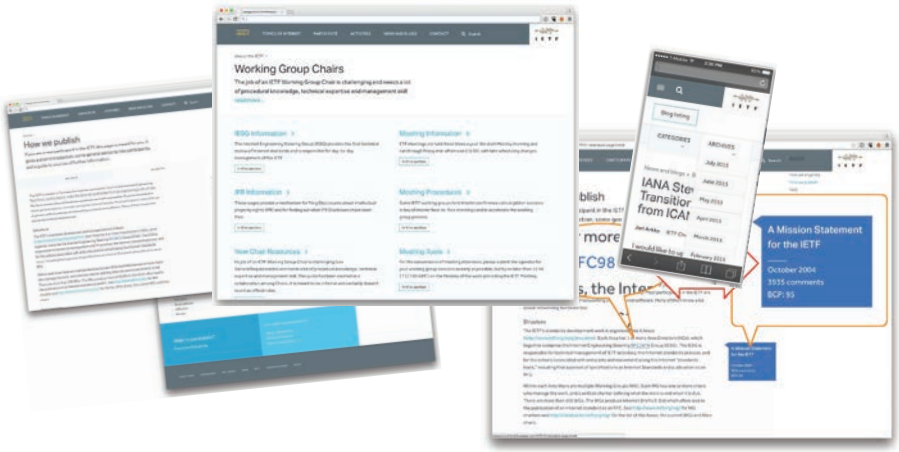
Thanks to all who participated in the BoF preparations and in the BoF session. And thanks for all the good suggestions. Please don't hesitate to contact us at edu-team@ietf.org with your questions, comments, concerns, criticism, or suggestions. There is also a public mailing list at edu-discuss@ietf.org.



IETF WEBSITE REVAMP: FIRST PEEK AT IETF 93

DURING THE IETF 93 ADMINISTRATIVE PLENARY, COMMUNITY MEMBERS GOT their first look at updated designs for the new public-facing IETF website (https://www.ietf.org). The design was developed based on usage data of the current IETF website, input from the target audiences, and consultations with the IETF Community Review Committee. The updated design aims to be widely usable, including being accessible on mobile, and working well over low-bandwidth/high-latency network connections.

Torchbox, the UK-based vendor selected for the project, was on hand at IETF 93 to answer questions from meeting attendees. The project remains on schedule, with plans to roll out the final site after IETF 94. Meanwhile, work is underway to further test the design, including its accessibility, and to smoothly migrate content to the new platform. On the current timeline, the website's new look will be in place by the beginning of 2016.



MARNEW WORKSHOP EXPLORES THE CHALLENGES OF ENCRYPTION

By Karen O'Donoghue

THE IETF AND THE IAB HAVE LONG BEEN ENGAGED IN ACTIVITIES TO REBUILD user trust and strengthen the Internet in the face of pervasive monitoring and potential product vulnerabilities. The Managing Radio Networks in an Encrypted World (MaRNEW) workshop (https://www.iab.org/activities/workshops/marnew/) was the latest in a series of collaborative activities.

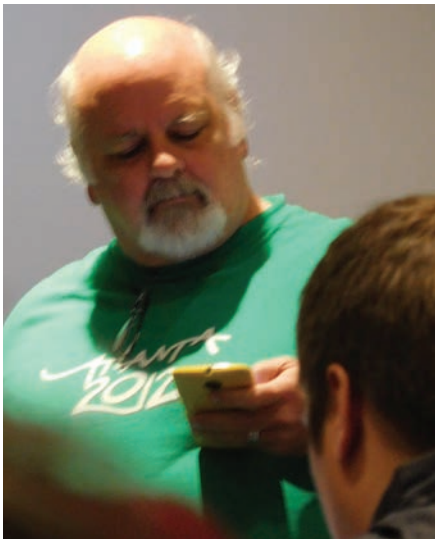
In November 2014, the Internet Architecture Board (IAB, www.iab.org) issued a Statement on Internet Confidentiality (https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/). This statement encouraged the widespread use of encryption to provide confidentiality and to improve the overall security of the Internet. One area of concern regarding this statement was the possible difficulty in the deployment of widespread encryption. Most of these concerns appeared to be overstated. The amount of deployed encryption appears to be rising steadily in most deployment scenarios. However, concerns remain in mobile environments. The MaRNEW workshop brought together the IETF and Groupe Speciale Mobile Association (GSMA) communities to discuss these challenges and to explore possible near-term and longer-term solutions.

Jianjie You, MaRNEW panelist, shares her observations with workshop particpants.

Held in Atlanta, Georgia, 24–25 September 2015, the workshop was jointly sponsored by the IAB, the Internet Society (www.internetsociety.org), AT&T (www.att.com), and the GSMA (www.gsma.com). Approximately 50 experts from around the world representing a variety of constituencies, including browser vendors, content providers, content delivery networks, equipment vendors, and mobile operators, gathered to better understand the unique challenges presented by the mobile environment and to explore ways to address these challenges.

[T]he problem isn't encryption itself, but rather current management and optimization techniques that don't work well (or at all) in the presence of encryption. New or different ways to optimize the customer experience are needed.

The workshop started with a couple of discussions to set the stage: an overview and process background from both the IETF and GSMA communities, followed by a session devoted to deployment considerations from IETF and GSMA perspectives. Next was a session on trust models and user choice that explored some of the perspectives and tradeoffs. The two sessions that followed explored sending data up and down for network management benefits. That was followed by sessions on application models, transport issues, and policy/regulation. The early sessions were challenging and all paths seemed to lead back to transport issues. However, by the end of the second day, several key themes emerged.



Spencer Dawkins, IETF Area Director, consults his notes while moderating a panel at the MaRNEW workshop.

Key Themes

One primary observation was that the problem isn't encryption itself, but rather current management and optimization techniques that don't work well (or at all) in the presence of encryption. New or different ways to optimize the customer experience are needed. Topics like cooperative resource management and content delivery network (CDN) improvement were identified as key solutions. A possible new protocol for keyless SSL to make distributed CDN deployments easier was identified as near-term work.

There was also momentum gathering around the fact that the problem isn't

MaRNEW photos: Olaf Kolkman

fully understood, and additional metrics and data that characterize how various optimization approaches work would be helpful. A framework for gathering and sharing operational data was discussed. The baseline against which new solutions would be measured is past resource management algorithms in an unencrypted world. There is a strong need for better testing and analysis tools.

Next Steps

Minutes from the workshop will be available on the MaRNEW workshop website in early November (https://www.iab.org/activities/workshops/marnew/). A draft report is planned by the end of the year; it will also be available on the MaRNEW website. A preliminary report from the workshop will be discussed at the Security Area Advisory Group (SAAG) meeting during the upcoming IETF 94 meeting in Yokohama.

While waiting for these more comprehensive reports and analyses, a couple of early summaries have been published. Natasha Rooney, a workshop cochair, provided a summary for the IETF chair blog at http://www.ietf.org/blog/2015/09/impressions-from-the-marnew-workshop/. Also, Dirk Kutscher, one of the energetic participants, has posted his perspective on the workshop at http://dirk-kutscher.info/publications/managing-radio-networks-in-an-encrypted-world-2/.

The following pointers provide perspective from the GSMA and W3C:

- Network Management of Encrypted Traffic, GSMA, Feb 2015, http://www.gsma.com/newsroom/wp-content/uploads/WWG-04-v1-0.pdf.
- The W3C Tag Finding on “Securing the Web”, January 2015, https://w3ctag.github.io/web-https/.

All in all, it was an intense two days of discussion. By the end, there was general consensus on some near-term work items and an agreement that further discussion and analysis is required.

IRTF UPDATE

By Lars Eggert

DURING IETF 93 IN PRAGUE, EIGHT OUT of the nine chartered Internet Research Task Force (IRTF) research groups (RGs) held meetings:

- Crypto Forum (CFRG)
- Global Access to the Internet for All (GAIA)
- Internet Congestion Control (ICCRG)
- Information-Centric Networking (ICNRG)
- Network Function Virtualization (NFVRG)
- Network Management (NMRG)
- Network Coding (NWCRG)
- Software-Defined Networking (SDNRG)

In addition to the meetings of those already chartered research groups, three proposed research groups held meetings. A proposed Human Rights Protocol Considerations Research Group (HRPC) held its second public meeting. The proposed “Thing-to-Thing” research group (T2TRG), related to Internet-of-Things networking, held a second, longer meeting the weekend before the IETF, in addition to a shorter session held during the week. And lastly, the third proposed research group, “How Ossified is the Protocol Stack?” (HOPSRG), discussed measurements at its first face-to-face meeting.

At the IRTF Open Meeting, two of the five winners of the 2015 Applied Networking Research Prize (ANRP) presented their research: Haya Shulman analyzed the deficiencies of Domain Name System (DNS) privacy approaches; João Luís Sobrinho designed a route-aggregation technique that allows filtering while respecting routing policies. For more about the ANRP winners, see page 22.

2015 ANRP winners, Haya Shulman and João Luís Sobrinho

The nomination period for the 2016 ANRP awards is now closed. The ANRP is awarded for recent results in applied networking research that are relevant for transitioning into shipping Internet products and related standardization efforts. You are encouraged to nominate relevant scientific papers that you have recently authored or read for consideration. Please see https://irtf.org/anrp for details.

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

BITS-N-BITES DEMOS ULTRA-LOW DELAY FOR ALL

By Bob Briscoe

AT THE BITS-N-BITES SESSION AT IETF 93 IN PRAGUE, SOMETHING QUITE remarkable was demonstrated: a streamed football match that you could pan and zoom with finger gestures on a touch screen—and still get (high definition) HD at full zoom. The app in itself was pretty neat, but the responsiveness was the remarkable thing; it seemed to stick to your finger as you panned or pinched. As you'd expect, attendees had some pretty pointed questions for those responsible: Reducing Internet Transport Latency (RITE), a team of European Internet researchers whose goal it is to remove the root causes of unnecessary latency over the Internet. The initiative is funded by the European commission under the fp7-ICT programme.

Through a dashboard you could click to add up to 100 parallel Web flows per second, and you could start dozens of downloads to pile on even more load.

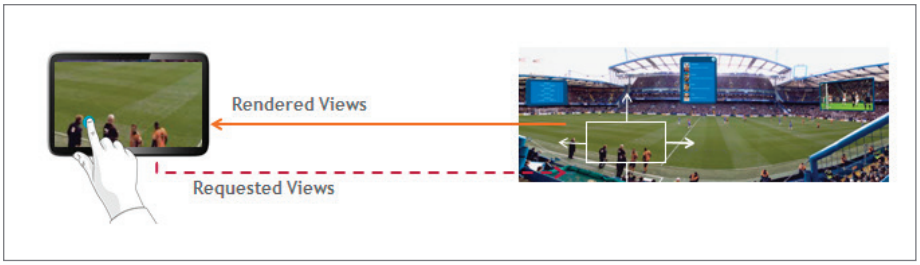


Figure 1. Requested and Rendered Views of Streaming Football Match

Was it cached locally?

No. Each client was feeding the finger gestures to a remote proxy, which, which was generating the HD scene on the fly for that user from a panoramic video of the whole stadium.

Was it just a short cable?

No. Earlier in the week, in the active queue management (AQM) Working Group (WG), the same technology had been demonstrated using remote login on Bell Labs' broadband testbed. They were streaming from a proxy in a data centre to a home network across real core, backhaul, and digital subscriber line (DSL) access network equipment—overall 7ms base round trip delay—the sort of base delay you should get to your local content delivery network (CDN). For Bits-N-Bites, they were using netem to emulate the same delay.

Was this Diffserv quality of service (QoS)?

No. That was the remarkable thing. Diffserv only gives QoS to some at the expense of others. This was for all traffic, even under high load. Through a dashboard you could click to add up to 100 parallel Web flows per second, and you could start dozens of downloads to pile on even more load. Not only did the pan and zoom responsiveness stay 'finger-sticking' good, but a chart on the dashboard showed that all the other flows were seeing the same ultra-low queuing delay. It measured the queuing delay of each packet—not just the video but all the Web flows and downloads. The worst delay was so low you could hardly see the plot—just a couple of pixels.

Had they just configured very shallow buffers?

No. The dashboard showed the link was fully utilized.

Figure 2. Dashboard View

So what was the magic under the covers?

Quite simply, all they were doing was not using regular Transmission Control Protocol (TCP) (no New Reno, no Cubic). Instead, they had switched the stacks at both ends to what they called a scalable TCP, with no need to change the apps. They said any scalable TCP will work, as long as it uses explicit congestion notification (ECN) as well. For scalable TCP, they were using Data Centre TCP (DCTCP) unmodified, which Microsoft deployed since Windows Server 8, and there's a Linux version too.

Then they had set the bottleneck queue to ECN-mark packets above a shallow step threshold. Access link capacity is typically the bottleneck for DSL, cable, and cellular. So, for their downstream DSL case they only needed this marking at the Broadband Network Gateway (BNG, a.k.a., BRAS or MSE). The same in the home gateway ought to sort out the upstream, as well.

Incremental Deployment?

Could we have this Nirvana on the public Internet? Surely any "classic" TCP flows from older machines would introduce queuing delay that would ruin everyone else's perfect day. Also, "scalable" TCPs are much more aggressive than classic TCPs. So whenever the two competed, you would expect classic TCPs to get only a small share of the capacity.

This was where the demo got really interesting. Using the dashboard, you could add classic flows, too. But it didn't affect the ultra-low queuing delay of the scalable packets at all. And the queuing delay of the classic flows wasn't compromised either—it was no worse than it would have been if all the load had been classic.

Most impressive, all the flows still shared out the capacity roughly equally, as if they were all the same type of TCP. But there was no per-flow scheduling—indeed, they weren't inspecting anything above the Internet Protocol (IP) layer.

Could we have this Nirvana on the public Internet? Surely any classic TCP flows from older machines would introduce queuing delay that would ruin everyone else's perfect day.

How did they do that?

They classified classic traffic into a separate queue to prevent it delaying the scalable traffic. Then, they coupled dropping and ECN-marking between the two queues, marking scalable flows more aggressively to exactly counterbalance their more aggressive response to the marks. This required a square relationship, which they coded really neatly; they just compared the queuing time against one random number for marking and against two for drop. They have a nice aide-mémoire for this: "Think twice before dropping."

Sunsetting TCP?

Back in 2012, when the IETF embarked on the real-time comms in Web browsers (RTCWEB) effort, it was known that queuing delay and jitter would often degrade RTCWEB. An Internet Architecture Board (IAB) workshop led to the birth of the RTP Media Congestion Avoidance Techniques (RMCAT) and the active queue management (AQM) WGs. RMCAT would avoid real-time traffic adding to the problem, and AQM would at least remove unnecessarily long queues by tackling so-called buffer-bloat. But the elephant in the room was TCP. Per-flow queuing was included in the AQM charter as a way to isolate a delay-sensitive flows from TCP, but it was hedged round with caveats, given the implication that the network would have to identify transport-layer flows, and decide on their relative capacity shares, not to mention the extra cost—a thousand-odd queues for a typical residential access.

The technology shown in Prague gives us a new component, using just two queues; a sort-of semipermeable membrane that partitions off the harmful delay of classic TCP without prejudging where to partition the bandwidth.

The demo showed that the Internet could be so much better without classic TCP. It demonstrated that a superior scalable class of TCP algorithms already exists. And it showed the path to get from here to there. It was the IETF at its best.

For more information about RITE, see http://riteproject.eu.

The technology shown in Prague gives us a new component, using just two queues; a sort of semi-permeable membrane that partitions off the harmful delay of classic TCP without prejudging where to partition the bandwidth.

2015 ANRP winner, João Luís Sobrinho

2015 ANRP winner, Haya Shulman

APPLIED NETWORKING RESEARCH PRIZE WINNERS ANNOUNCED

By Mat Ford

THE APPLIED NETWORKING RESEARCH PRIZE (ANRP) IS AWARDED FOR recent results in applied networking research that are relevant for transitioning into shipping Internet products and related standardization efforts. The ANRP awards presented during IETF 93 went to the following two individuals:

- **Haya Shulman.** For analysing the deficiencies of DNS privacy approaches in the paper, "Pretty Bad Privacy: Pitfalls of DNS Encryption."

  Read the full paper at https://www.ietf.org/mail-archive/web/dns-privacy/current/pdfWqAIUmEl47.pdf.

- **João Luís Sobrinho.** For designing a route-aggregation technique that allows filtering while respecting routing policies in the paper, "Distributed Route Aggregation on the Global Network."

  Read the full paper at http://www.cs.princeton.edu/~jrex/papers/dragon14.pdf.

Shulman and Sobrinho presented their findings to the Internet Research Task Force open meeting during IETF 93.

Slides are available at https://www.ietf.org/proceedings/93/slides/slides-93-irtfopen-1.pdf and https://www.ietf.org/proceedings/93/slides/slides-93-irtfopen-0.pdf.

Thanks to Meetecho, audio and video from the presentations is available at http://recordings.conf.meetecho.com/Playout/watch.jsp?recording=IETF93_IRTFOPEN&chapter=chapter_1 (from 00:17:45).

The call for nominations for the 2016 ANRP award cycle is now closed. ANRP winners for 2016 will be announced prior to each of the three IETF meetings scheduled in 2016. Join the irtf-announce@irtf.org mailing list for all ANRP related notifications.

INTENT-BASED NETWORK MODELING

By Bert Wijnen, Tianran Zhou, Susan Hares, and Dr. Pedro A. Aranda Gutiérrez

PROPONENTS OF INTENT-BASED NETWORK MODELING (IBNEMO) HELD two bar–Birds-of-a-Feather (BoF) meetings during IETF 93 in Prague. Many people are interested in standardizing a minimal language capable of expressing intent in networking configurations and work on this topic is ongoing via various projects using the OpenDayLight platform. Our aim is to define a minimal set of commands that can cover 80 percent of the intent expressions needed in network configurations (Figure 1).

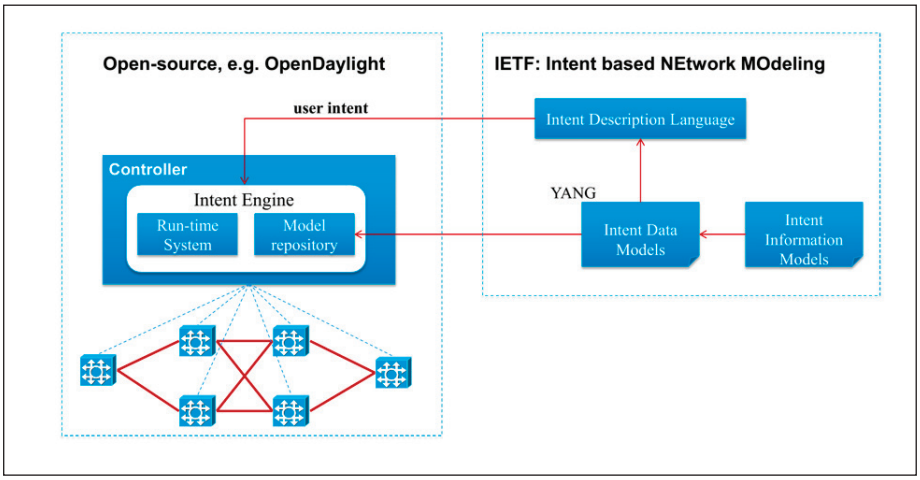


Figure 1. The Minimal Set of Commands that Can Cover 80 Percent of the Intent Expressions Needed in Network Configurations

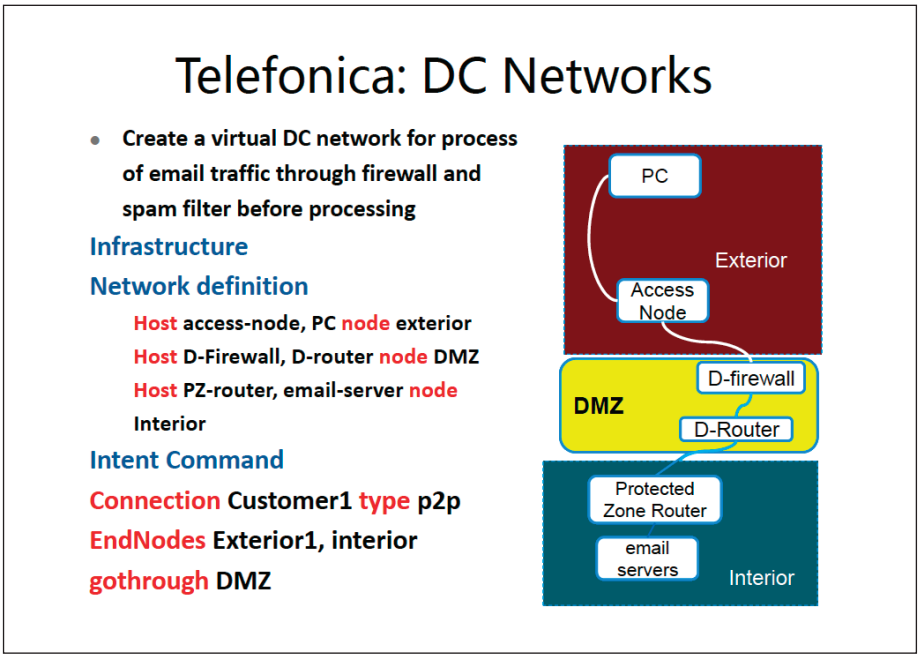


Figure 2. Example of IBNEMO at Work in the Context of the European Union-Funded Collaborative Research Project, NetIDE

Many people are interested in standardizing a minimal language capable of expressing intent in networking configurations and work on this topic is ongoing.

See https://tools.ietf.org/html/draft-hares-ibnemo-overview-00 for an Internet-Draft that includes both an overview of IBNEMO and a problem statement.

The meetings attracted 15–20 people in each of two sessions. Sue Hares gave an overview and an explanation of the aims of IBNEMO and presented her Internet-Draft. Dr. Pedro A. Aranda Gutiérrez from Telefónica, I+D shared an example of IBNEMO at work in the context of the European Union-funded collaborative research project, NetIDE* (Figure 2). And Tianran Zhou from Huawei demonstrated an early implementation of IBNEMO.

A number of good questions were raised that in turn encouraged us to help newcomers better understand the technology. We also concluded that there is a need for more awareness and interest in the technology before trying to establish an IETF Working Group.

If you are interested in IBNEMO technology, please join our mailing list at https://www.ietf.org/mailman/listinfo/ibnemo. A fuller report of the bar-BoF can be found at https://mailarchive.ietf.org/arch/msg/ibnemo/69t80ww_gkWuEuxetugQxkgMSlg.

We plan to have presentations or BoFs at the Réseaux IP Européens (RIPE) and North American Network Operators' Group (NANOG) meetings to spread the word about this interesting new work.

**The NetIDE Project is cofunded by the European Commission DG CONNECT in FP7 under grant agreement 619543.*

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 review the BoFs that took place during IETF 93, including their intentions and outcomes. If you're inspired to arrange a BoF meeting, please read RFC 5434, "Considerations for Having a Successful Birds-of-a-Feather (BoF) Session."

Captive Portal Interaction (capport)

Description: Captive portals are used to control wireless Internet access in many locations (e.g., coffeeshops, hotels). With the ongoing move to a more secure Internet, the interception techniques employed by these portals become increasingly problematic. The user experience also leaves much to be desired. This BoF meeting sought to understand if there is sufficient energy to work on the problem and design a protocol for interacting with captive portals.

Proceedings: https://www.ietf.org/proceedings/93/minutes/minutes-93-capport

Outcome: The meeting attracted a number of relevant technical experts who write code for captive portals or operating systems that have to deal with captive portals. More work is required to both narrow the scope of the problem and obtain more data about the types of captive portals and the extent of their deployment. A taxonomy document may be a good first step.

Education and Mentoring Next Generation (edunext)

Description: This meeting was to obtain community input on the future direction of the IETF education (http://www.ietf.org/edu/) and mentoring (https://www.ietf.org/resources/mentoring-program.html) activities.

Proceedings: https://www.ietf.org/proceedings/93/minutes/minutes-93-edunext

Outcome: Lots of good ideas were proposed and discussed to improve both the education and mentoring programs. See the article on page 16 for details.

Deterministic Networking (detnet)

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

Proceedings: https://www.ietf.org/proceedings/93/minutes/minutes-93-detnet

Outcome: A very well-attended meeting that strongly supported the need for open standards in this space. A large number of use cases were identified and discussed leading to some concerns about the need to narrow the scope of proposed work items to make them tractable. There was support in the room for the IETF to work on this problem in a DETNET WG. (The DETNET WG was chartered on 5 October 2015, http://datatracker.ietf.org/wg/detnet/charter/.)

European Goldfinch (Carduelis carduelis)

Eurasian Kestrel
(Falco tinnunculus)

Simplified Use of Policy Abstractions (supa)

Description: The SUPA WG defines a data model to be used to represent high-level and possibly network-wide policies that, in turn, can be input to a network management function (within a controller, an orchestrator, or a network element). Processing that input likely results in network configuration changes. SUPA, however, does not deal with the definition of the specific network configuration changes; it deals with how the configuration changes are applied (e.g., who is allowed to set policies and when and how the policies are activated, changed, or deactivated).

Practically, SUPA defines base YANG data models to encode policy that will point to device-, technology-, and service-specific YANG models developed in other working groups. The WG focuses on a single management domain, and is designed to work with device, protocol, network, and service-data models.

Proceedings: https://www.ietf.org/proceedings/93/minutes/minutes-93-supa

Outcome: A reasonably well-attended meeting that identified work for the IETF and demonstrated that the right people to do the work are available. Further discussion is required to narrow the scope and clarify expectations for a working group on this topic. (The SUPA WG was chartered on 2 October 2015, http://datatracker.ietf.org/wg/supa/charter/.)

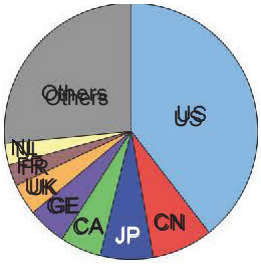
Interface to Network Security Functions (i2nsf)

Description: The primary goal of I2NSF is to define an information model, a set of software interfaces and data models for controlling and monitoring aspects of physical and virtual network security functions (NSFs). Other aspects of NSFs, such as device or network provisioning and configuration, are out of scope. Controlling and monitoring of NSFs should include the ability to specify, query, monitor, and control the NSFs by one or more management entities. Since different security vendors support different features and functions on their devices, I2NSF will focus on flow-based NSFs that provide treatment to packets/flows, such as IPS/IDS, Web filtering, flow filtering, deep packet inspection, or pattern matching and remediation.

Proceedings: https://www.ietf.org/proceedings/93/minutes/minutes-93-i2nsf

Outcome: The charter for this proposed WG is now more focussed than when this proposal was first made at IETF 91. Lots of support was shown in the meeting for forming a working group and several meeting participants indicated that they were interested in either implementing or deploying an I2NSF solution. (The I2NSF WG was chartered on 18 September 2015, http://datatracker.ietf.org/wg/i2nsf/charter/.)

IETF 93 AT–A–GLANCE



Participants: 1,384

Newcomers: 204

Number of countries: 65

IETF Activity since IETF 92 (22 March–19 July 2015)

New WGs: 12

WGs closed: 8

WG currently chartered: 143

New and revised Internet-Drafts (I-Ds): 1739

RFCs published: 116

- 76 Standards Track, 5 BCP, 6 Experimental, 27 Informational

IESG Restructuring

Restructuring complete

- Seven areas: ART, GEN, INT, OPS, RTG, SEC, TSV
- IESG working on experiments around moving more work from ADs to WGs and the community

IANA Activity since IETF 92 (March–June 2015)

Processed 1,458+ IETF-related requests, including:

- Reviewed 97 I-Ds in Last Call and 118 I-Ds in Evaluation
- Reviewed 110 I-Ds prior to becoming RFCs, 57 of the 110 contained actions for IANA

Added 12 new registries since IETF 92 (March–June 2015)

- gmpls-wson, precis-parameters, precis-tables-6.3.0, rdap-asn, rdap-dns, rdap-ipv4, rdap-ipv6, gmpls-wson, precis-parameters, precis-tables-6.3.0, babel, ppspp, security-label-format-selection, battery-technologies, scim

SLA Performance (January–June 2015)

- Processing goal average for IETF-related requests: 99%

IANA and DNSSEC

- As of 15 July 2015, 834 TLDs have a full chain of trust from the root. http://stats.research.icann.org/dns/tld_report/.

RFC Editor Activity since IETF 92 (March–15 July 2015)

Published RFCs: 135

- 108 IETF (12 IETF non-WG), 2 IAB, 4 IRTF, 9 Independent

IETF MEETING CALENDAR

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

IETF 95	**Date** 3–8 April 2016 **Host** TBD **Location** Buenos Aires, Argentina	**IETF 97**	**Date** 13–18 November 2016 **Host** TBD **Location** Seoul, South Korea
IETF 96	**Date** 17–22 July 2016 **Host** Juniper Networks **Location** Berlin, Germany	**IETF 98**	**Date** 26–31 March 2017 **Host** TBD **Location** Montreal, QC, Canada

Special thanks for hosting IETF 93

BROCADE

cz.nic | CZ DOMAIN REGISTRY

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

Afilias Google Microsoft

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

Afilias cisco comcast ERICSSON Google

ICANN JUNIPER NETWORKS NBCUniversal RIPE NCC

pub-IETFJv11.2-20151022-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
IETF Journal adheres to the *Oxford English Dictionary*, 2nd Edition.

IETF Journal

Internet Society
Galerie Jean-Malbuisson 15
1204 Geneva, Switzerland