IGF Workshop 240

Building trust and confidence: implement internet standards

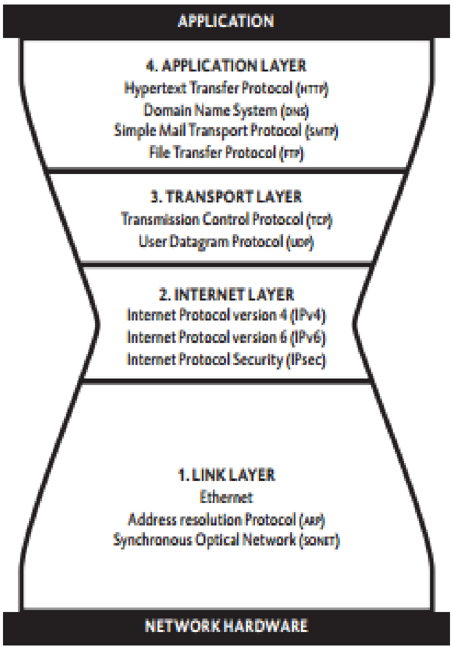
This workshop identifies good practices in speeding up implementation of internet standards, through expanding existing practices, exploring new solutions and ways of cooperation to encourage users and providers to use modern standards, as a collaborative exercise by businesses, technical community, civil society, academia and governments.

The workshop is part of the Internet Infrastructure Initiative under the aegis of the Global Forum on Cyber Expertise. The aim of this initiative is to help build a robust, transparent and resilient internet infrastructure following the experience in the Netherlands in testing and monitoring compliance with open internet standards.

Digital technologies have spread rapidly across the world, acknowledges the **WorldBank Development Report "Digital Dividends**". In many instances digital technologies have boosted economic growth, expanded job opportunities and improved service delivery. Yet their aggregate impact has fallen short and benefits are unevenly distributed in the world.

Inclusive and sustainable growth can only be accomplished within **a trusted and robust internet ecosystem**. The Internet infrastructure is its corner stone, operating based upon a set of core standards and protocols, including TCP/IP Protocol Suite, Domain Name System (DNS) and routing protocols. These layers could be regarded global public goods.

As such, the Internet only works properly if its underlying values – **openness, universality, interoperability and accessibility** – are guaranteed and if it facilitates the main objectives of data security: **confidentiality, integrity and availability**. For this purpose many open standards were developed by the technical community, to name IPv6, DNSSEC, TLS, and DKIM, SPF and DMARC.


APPLICATION
4. APPLICATION LAYER
Hypertext Transfer Protocol (HTTP)
Domain Name System (DNS)
Simple Mail Transport Protocol (SMTP)
File Transfer Protocol (FTP)
3. TRANSPORT LAYER
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)
2. INTERNET LAYER
Internet Protocol version 4 (IPv4)
Internet Protocol version 6 (IPv6)
Internet Protocol Security (IPsec)
1. LINK LAYER
Ethernet
Address resolution Protocol (ARP)
Synchronous Optical Network (SONET)
NETWORK HARDWARE

It is vital that users can rely on the fundamental Internet protocols and standards functioning properly. The problem nowadays is not the lack of those standards, but **the effective implementation** falling short. Our aim here is to

- recognise good practices on effective implementation of internet standards and related protocols with strong agenda- and policy-setting power;
- propose key activities for the Internet Infrastructure Initiative in order to act as a complementary nucleus of expertise and capacity-building support;
- Identify stakeholders and partners for cooperation.

Target audience: those stakeholders with (political) agenda-setting, regulatory and policy-setting authority.

About the Global Forum on Cyber Expertise (GFCE)

This workshop forms the kick-off of the Internet Infrastructure Initiative that was launched under the aegis of the Global Forum on Cyber Expertise (GFCE). The ambition of the GFCE is to become the global platform where public and private companies exchange expertise and best practices on cyber capacity building. The GFCE provides countries and organizations with a platform to effectively cooperate on a global level. The GFCE offers a pragmatic, action-oriented and flexible forum. Members and partners develop practical initiatives to take advantage of opportunities in cyberspace and to overcome evolving challenges in the field.

Problem setting

The availability of open internet standards is not the problem. The IETF, ISO and order standards organisations have created a vast and comprehensive compendium of practices based on rough consensus within the technical internet community. The problem rests with the implementation process. Some key challenges are:

- Different implementation approaches per country depending on infrastructure maturity;
- Effective prioritisation of standards: which are essential and which are less?
- The role of government as incentive-provider and norm-setter;
- Maturity of public-private cooperation and of multi-stakeholder eco-system;
- Achieving synergy and complementarity between various global and regional initiatives;

Outline

Following a plenary introduction and key-note, the participants will be divided into a 3 groups. Each group discusses a specific case but the entire group is confronted with the same main questions:

- What constitutes good practice in implementing open internet standards?
- What are the preconditions for effective implementation?
- Which other initiatives/activities are noteworthy and should be considered?
- Where (geographically, stakeholder group) should enhanced attention to implementing open standards be prioritised?

Through this formula of participation and interaction, we wish to discuss and identify a set of best practices. This format allows for 'smaller-group' in-depth discussions and allows each participant to also share his/her expertise and viewpoint. The groups are 'mentored' by a speaker representing one of the stakeholder communities. As a whole, the group of participants learns from the collective set of expertise present. The results of the case-studies will be reported. The online participants will discuss a case on their own facilitated by the online moderator.

Timeline and location

9 December 2016, 10:45-12:15hrs, Workshop Room 1

10:45-11:00 Introducing the GFCE Internet Infrastructure Initiative, by Bart Hogeveen (Clingendael Institute) (15min)

11:00-11.15 Key-note on open internet standards, by Olaf Kolkman (ISOC) (15min),

Break out into 3 different groups

11:15-11:45 Per group; discussing a set of key questions (30min)

11:45-12:00 Plenary: feedback and reflection by facilitators (15min)

12:00-12:15 Listing identified recommendations & concluding remarks (15min)

Break-out session group work

Issue:

We have a set of modern standards for scalable and secure internet use (see next page). How do we provide the right preconditions and incentives for organisations, companies and others to adopt these standard, even in case a direct(ly tangible) return on investment is not evident?

From your experience & point of view:

- What and where are good practices in implementing open internet standards?
- What can be good preconditions for effective implementation by organisations, public agencies, companies etc.?
- In which geographical areas is there a distinct need to address / prioritise the implementing of open standards?
- With which stakeholder groups is there a distinct need to address / prioritise the implementing of open standards?
- Which other initiatives/activities regarding implementing of internet standards are noteworthy and should be considered?

With kind support of

IPv6

The Internet Protocol (IP) is the technology underlying all traffic on the Internet. Under the current standard, IP version 4 (IPv4), every computer has a specific IP address made up of four numbers, such as 192.0.2.26. IPv4 is now 35 years old and is reaching its limits.

The biggest problem is that IPv4 can only support four billion IP different addresses. That seems a lot, but it isn't enough for a world of seven billion people, especially when you think that every connected device — desktop computers, laptops, mobile phones, webcams, central heating controllers — needs its own IP address. IP version 6 (IPv6), the successor to IPv4, solves the address shortage.

DNSSEC

DNSSEC is a security system for DNS, the internet directory that handles the translation of domain namesto IP addresses. DNS itself works fine, but the translation of a domain name to an IP address is not protected. That is a security risk, because attackers can get hold of passwords or other sensitive information by redirecting network traffic to a false IP address.

DNSSEC extends DNS with an additional security feature: a digital signature that guarantees the translation of a domain name to the correct IP address. Any internet user can check that signature automatically, and so avoid being redirected to a false IP address.

TLS

TLS is a standard for the cryptographic protection of internet connections. Most people have seen TLS, and its predecessor SSL, in action in their web browsers: by specifying the 'https' protocol in an internet destination — for example https://www.example.com/ — an internet user indicates that he wants to visit a website using a secure connection. The "padlock" icon in the browser shows that a secure connection was established successfully, and optionally provides more detailed security information. Unfortunately, just enabling TLS does not guarantee security: it needs to be properly configured as well.

DKIM, SPF and DMARC

DKIM, SPF and DMARC are three internet standards to fight phishing, spam, viruses and other nasties that are delivered by e-mail. These three standards are usually used together to validate the sender (a mail address) and the sending system (a computer) of a mail message, and to verify that the content of the message has not been altered in transit.

DKIM

DKIM secures the integrity of mail messages. It safeguards both the content and the "envelope" of every outgoing message with a digital signature. This stops attackers sending messages that pretent to be from other people (spoofing) or altering the content of a message while it is in transit.

SPF

SPF prevents "electronic mailboxes" from accepting messages delivered by unauthorised computer systems. Only messages from systems which are actually allowed to send messages for a specific domain will get through. To make this possible, a list of valid senders is published online through the DNS system. Receiving systems can use this list to validate the sender before accepting a message.

DMARC

DMARC complements the other two security standards for e-mail, DKIM and SPF. DMARC gives "electronic mailboxes" a hint on how to handle incoming mail messages that do not pass the DKIM or SPF checks. These may be discarded, for example, or be put aside. The hint is published online through the DNS system. It can additionally contain an e-mail address to which mailboxes can report rejected messages. This gives the administrator of a specific mail domain useful information about the delivery of both genuine and forged messages.