GFCE Triple-I Workshop @AIS2019, 16 June 2019, Kampala, Uganda

Report by Daniel Nanghaka and Maarten Botterman

Summary

On Sunday 16 June, the African Internet Summit hosted the GFCE Triple-I Internet Infrastructure Security Day for the second year in a row. This workshop was supported by AfriNIC, AfricaCERT, AFNOG, WACREN, ICANN, Internet Society, and the Dutch Ministry of Economic Affairs and Climate. Aim of the workshop is to look for ways forward towards more trusted use of Internet and email in the region. Participants in this workshop included global and regional experts, and regional Internet stakeholder groups, including the government, business and technical community, who all contributed in finding solutions to strengthen an open end-to-end Internet.

The workshop was held in English, and contributions/questions in French were facilitated by consecutive translation in the room, as to ensure all participants can express themselves in the language (French/English) they are most comfortable in. Recordings of the life streaming of the conference can be found here.

The Workshop started with opening remarks by Maarten Botterman and Dr. Nii Quaynor. Maarten started with highlighting the World Economic Forum Global risk report 2018 with the compelling risks in the Internet infrastructure initiative. It was noted that GFCE partnership with the regional registries and has been setting up Capacity building events with this workshop being the second in Africa. The first workshop was held in Dakar (see report).

The main Purpose of the day was to derive ways to improve the justified trust in using the Internet and email in the region. There is a need to conduct an evaluation of the Internet and decision making in the internet ecosystem through proper assessment of the trends in Internet growth in Africa and through constant planning and mitigation of risk related to the Cyberspace. The nature of the space requires collaboration and cooperation working together to create a bigger space.

Mr. Nii Quaynor called for active participation, and emphasized the importance of continued joint action across the African continent. He encouraged the participants to work together on development and implementation of new actions to improve trust in the Internet in the region. He also highlighted the good experience with the AFNOG capacity building trainings.

GFCE TRIPLE - I

After that, Maarten Botterman explained the organization of the day, basically build up in three blocks: awareness raising on a number of Open Standards, and how their deployment can help enhance justified trust; inspiration by sharing of excellent practices building on this; and action planning – as in the end it is all about getting things done (capacity building towards more trusted Internet in the region.

Block I: Better Use of Today's Open Internet Standards

During the first block we focused on Open Internet standards that could already be applied today, and Alain Aina (WACREN) talked with Adiel Akplogan (ICANN) about the use and usefulness of Open Internet Standards such as DNSSEC, TLS, DANE, RPKI, ROA, DMARC, DKIM, SPF, and IPv6.

DNSSEC, TLS and DANE are important in ensuring integrity of routing and of the data exchange itself. The challenge is the overhead and action needed by all players in the value chain to be fully effective. The successful first root KSK rollover cycle completed recently was mentioned. The Resource Public Key Infrastructure (RPKI)services are implemented as a complement to the current IRR services, which solves one of the most fundamental problems: verification whether an Autonomous System (AS) is authorized to announce a specific prefix. Route Origin Authorization (ROA)'s are cryptographically signed statement that confirm the link between a set of prefixes and an origin ASN, and complement this. Eventually the goal is to have secured BGP capable routers to validate prefixes against ROA's. This will highly contribute to mitigating some of the weaknesses of the current routing system that will help reduce abuse – and more will need to be done. It was point out that based on the recent statistics published by NRO, for RPKI adoption for IPv4 and IPv6; this region is not doing badly. Effort must continue and the RPKI BoF planned for the end of AFNOG2019 was well welcomed. BCP38 and MANRS were also briefly discussed.

DMARC, DKIM and SPF are standards that help prevent email to be easily abused to confuse people with spoofing etc. There are examples of cyber extortion that could have been easily prevented when those standards are implemented by mail server operators. While the new generation prefers direct messaging often above email, better measures to enhance justified trust in email remain important.

During the discussion on the use and usefulness of these Open Internet Standards, Alain stressed the need for all to understand what is an open standard as there are many definitions when it comes to this and also lot of confusion. He referred to the recent effort by IETF, IAB, IEEE, W3C, etc.… to promote a proven set of principles that establish The Modern Paradigm for Standards. He mentioned the five (5) principles to the modern Paradigm of Standards published in RFC 6852:

1. Cooperation;

2. Adherence to Principles;
    a. Due process;
    b. Broad consensus;
    c. Transparency;
    d. Balance;
    e. Openness;
3. Collective Empowerment;
4. Availability;
5. Voluntary Adoption.

Adiel highlighted the challenge to understand what the meaning of Open standards is, and pointed out that there is a need for choosing appropriate standards that are fit for different business and economic environments. Sometime implementation of standards, as open as they can be, add operation costs that small ISPs or network operators will not be able to handle because their already tight margins. Sometimes the additional costs are real and unavoidable, but sometimes their just a matter perception and much could be done without additional costs. It is therefore important to raise awareness and share relevant good practice.

A question arose " How do we set the proper framework in the implementation of the Open Standards?" Awareness raising is deemed key in this, as is the availability of trusted sources of information on these standards and why they are needed – tailor made for different stakeholder groups. A specific point for attention is the tension between ITU led standards and the broader global Internet standards originating from IETF. In particular with 5G development and deployment, a clear way forward will be necessary. It was noted that for some governments and telecom operators, adoption by ITU of specific IETF standards will stimulate implementation. According to Michuki Mwangi, there are more manufacturers compared to implementers involved in developing standards at IETF, which sometimes leads to tension and contention around the implementation of those standards.

A challenge is lack of effective collaboration between policy makers, private operators and regulators. Business considerations shift priority based on the evolution of the markets and business models: the question raises: how do build an effective collaboration on security best practices? In the Netherlands, stakeholders from government, business and Internet industry have formed a Platform Internet Standards, where appropriate standards are discussed and agreed, and joint help is provided for further implementation of those.

A very good tool to measure the use of these standards by websites and mail servers is the website www.internet.nl. On this website, it is possible to fill in any website or email address to check whether it is up-to-date in its use of these open standards. The website also provides information on where a website fails, and what can be done to resolve this. As announced by the technical supplier NL Labs,

the software code will be made shortly available for usage in other countries/regions in the world. This raises a possibility for regional collaborative platforms to provide similar services in support of roll-out of these standards in the region – noting it is already possible today for any organization to check websites and email addresses using English and the www.internet.nl website. Daniel Nanghaka (ILICIT Africa) shared his interest to take the lead to deploy an Africa Open Standards Platform on this basis, in order to support the open Internet standard adoption in Africa.

Block II: Inspiration from Good Practice Actions

The second block is the space where inspirational practices and useful ways forward are shared. Cristian Hesselman: head of SIDN Labs (the research team of the .NL operator) and SSAC Member, explained the concept of a DDOS Radar, which facilitates a proactive and collaborative DDoS mitigation strategy. It resolves around providers of critical services (e.g., ISPs, banks, government agencies, and hosting providers) continually collecting information on potential and active DDoS sources and automatically sharing this information with each other. The information consists of a digest of the DDoS traffic that a critical service provider needs to handle (a so-called "DDoS fingerprint"). Sharing of fingerprints provides an additional layer of Internet security on top of to the (commercial) DDoS scrubbing services that service providers need to use as well, which separate DDoS traffic from benign traffic. Cristian proposed the concept of a DDoS radar together with researcher from the University of Twente after Dutch banks and government agencies were the victim of multiple DDOS attacks earlier this year. A strategy that may provide true inspiration for initiatives in other countries and regions. Several Dutch ISPs, banks, government agencies, the University of Twente, and SIDN have teamed up around the concept and are currently working to bring it to an operational system.

Abuse mitigation was the subject of a panel led by Jean-Robert Hountomey (AfricaCERT), with Yuri Ito (Cybergreen) and Adiel Akplogan (DAAR, ICANN).There is a need for resources to help detect and act against abuse as it was also mentioned that the Internet is not good or bad in itself: it is how it is used that matters. Early detection of abuse (whether purposefully or by mistake) will help to contain damage by being able to alert users and actively take measures against the abuse. Measuring abuse allows to understand where the weakest spots are, which helps prioritizing appropriate measures. Examples of global action include Cybergreen and DAAR, basically providing information to the public about specific abuse.

- Yurie Ito continued the discussion from previous session on how to motivate decision makers to adapt right actions and policies. She pointed out how to use cross-comparable statistics, data, benchmarking to draw the decision maker's right attention to assign the right resources to counter specific challenges. CyberGreen undertakes research on a country's overall Cyber Ecosystem healthiness. It also provides recommendations to improve cyber health by informing CSIRT and policy makers on the most

significant systemic risks and helps them to adapt the right security measures and policies. It does so by providing data based on its own scanning, and in that way CyberGreen is able to show comparable data that provide an excellent segue into action with a focus on those points that are recognized as abusable and harmful to global internet. CyberGreen also started national level ecosystem health-check analysis with its technical partners - analyzing not only the level of DDoS infrastructure, but email infrastructure and internet routing infrastructure. Comments and suggestions from the audience about data normalization, also how to utilize this type of statistics with other measurements such as DAAR and MANRS for collaborative analysis, and promote global best practices.

- Adiel Akplogan reported on ICANN's Domain Abuse Activity Reporting (DAAR) project. He has introduced the initiative to the audience and highlight its goal as a system for studying and reporting on domain name registration and security threat (domain abuse) behavior across top-level domain (TLD) registries and registrars. The system is not built in any way to enforce compliance. The reporting tool is aimed at the ICANN community, which can then use the data to facilitate informed policy decisions. DAAR was designed to provide the ICANN community with a reliable, persistent, and reproducible set of data from which security threat (abuse) analyses could be performed. The system collects TLD zone data, a very large body of registration data, and complements these data sets with a large set of high-confidence reputation (security threat) data feeds. The data collected by the DAAR system can serve as a platform for studying or reporting daily or historical registration or abuse activity. A monthly report is published on ICANN web site freely available for people to consult. The DAAR initiative is open to work with volunteers ccTLDs who will be interested in providing data so to measure the behavior of the TLD within the framework of DARR. ccTLDs interested can contact ICANN to have more information on how to proceed to join.

Conclusions of the panel is that understanding where abuse takes place is key knowledge for effectively addressing this. It requires reliable data from reliable sources. Global sources can play an important role in that.

Michuki Mwangi made a presentation on Mutually Agreed Norms for Routing Security (MANRS) and called upon network operators around the world to join the Routing Resilience Manifesto Initiative, and to agree to the Mutually Agreed Norms for Routing Security (MANRS) Principles. There is a clear need for a culture of collective responsibility whereby best practices on routing security are shared among the stakeholders. For consumers it is wise to choose a reliable router supplier that agrees to the MANRS Principles. Aim is to involve more ISPs in the region as to enhance reliability of the routing. He therefore invited key African players to expand on what they had done to further ensure routing security for their clients, and three people did stand up to share from their activities. Two of the three also indicated that for them the MANRS baseline was not sufficient – they went beyond the guidelines with more strict measure to prevent abuse. This

was a clear demonstration in how different networks can play and already play a role in making the Internet more secure.

The Internet of Things (IoT) comes with opportunities for citizens as well as the digital economy. This includes applications in the home as well as in infrastructures, factories, vehicles and in nature itself. Maarten Botterman pointed at the fact that many internet-connected devices, and in particular those sold to consumers, often lack basic cyber security provisions, which is an increasing concern for citizens and governments. There are basically two risks: <1> vulnerability of individual devices themselves for tampering; and <2> wider society faces an increasing threat of large scale DDOS attacks launched from large volumes of insecure IoT devices. How to reduce those risks is a high interest topic in many countries and regions. Kevin Chege expanded on the need to for the adoption of IoT trust frameworks to improve security in and around IoT, and recommended the adoption the OTA IoT Trust Framework as a guideline for safer IoT implementation. The OTA Trust Framework identifies the core requirements manufacturers, service providers, distributors/purchasers and policymakers need to understand, assess and embrace for effective security and privacy as part of the Internet of Things. Verengai Mabika reported that most of the people in Africa are consumers of IoT devices and are not involved or aware about the Security of the IoT. Reference was made to Senegal with the process on which they are doing to improve on IoT Security. More information can be found on https://iotsecurity.sn. It is important that manufactures, suppliers and users all play a role to ensure adequate security in devices, and in systems consisting of multiple IoT devices working together to deliver specific services. How to make this apply to your region is a key concern that has now high political and increasing public interest around the world. Actively finding a way forward in the region has become a priority – including the need for international collaboration. Next to awareness of better application of security and transparency rules, longer term solutions are under development, as well.

Block III: Planning for a more Trusted Internet

Following the introductions about open internet standards that can help enhance justified trust in use of the Internet and email (Block I) and the examples of good practice provided (Block II) the day was summarized with a focus on answering the question:

> *"What to do, together, to improve justified trust in using the Internet and email in the region"*

The following topics came up during the day as possible actions to pick up specifically in the region, at this point in time, in order to progress trust in the use of Internet and email in the region:

(1) Awareness raising on relevant information to key stakeholders on:

a. key global Internet Standards that help make this Internet more trustworthy, when applied;
b. abuse – where is the threat, how does it compare to other threats, and to other regions, and what can be done to mitigate abuse;

1.1 It may be worthwhile to set up local or regional Platforms with multiple stakeholders to agree on relevant and necessary Internet Standards to be implemented. Collaboration between Government, Service providers and key users is essential in this. Next to establishing "what standards are needed in the region", this includes ways to incent investments in this, both by service providers (by making it worthwhile to "keep the service clean" and implement good practice in the interest for your customers) and governments (what is the societal impact of abuse and attacks, and what can be done to mitigate this), as well as end users. Here, it was argued that too few people are aware of this, which also leads to ISPs not having a business incentive for investing in a more secure set-up of their services as customers don't ask for it, and don't value it. However: this is likely to change if abuse continues to grow, and if some service providers in the region start offering more secure services. So awareness raising needs to take place on all fronts: end users, politicians, business decision makers and service providers.

1.2 When moving forward on this, developing a regional version of the website internet.nl can be very useful, and it may be possible to set up local applications of the code that is now available under an Open Software license.

(2) DDOS mitigation through collaboration

Here, it was recognized that dealing with DDOS attacks is a key towards being able to rely on infrastructures and services – even more so for critical applications and infrastructures than for others. Whereas many companies and government recognize this already today and are building mitigation systems to reduce the risk, the big opportunity seems to be in working together, and sharing both DDOS attack sinking facilities as information about attacks, as soon as they are recognized.

(3) IoT

The number of IoT devices continues to surge with estimates indicating that the devices will number 2.5 times the population of earth by the year 2020. For these devices to be trusted and used properly, users need to be educated early on what IoT devices are as well as on the risks and opportunities IoT devices present. Manufacturers need to ensure that IoT devices are secure by design from the beginning, following broadly recognized Principles and Guidelines on IoT design such as the OTA IoT Trust Framework Guidelines. Network providers need to make sure they filter and sink abuse of the networks where that is detected. Cloud providers need to ensure adequate protection of their services as well. Overall,

next to mitigating the short term risks, longer term solutions need to be developed and adopted. For this, much can be learned from other countries.

(4) Capacity building workshop

In this context, there was mention of AFNOG capacity building workshops (Nii Quaynor, and IoT security capacity building workshop (Kevin Chege, Internet Society). In addition, most of the attendants agreed that it would be useful to bring back the GFCE Triple-I workshop in 2020, during AIS2020.

Conclusions

Many of the good practices presented on subjects like Open Standards adoption, joint DDOS mitigation, better abuse detection and prevention, and IoT security were confirmed to be important by the well informed group of participants to this workshop during AIS2019.

A lot of emphasis is on awareness raising – both within the industry, to politicians, and to the larger public. And this comes hand in hand with (intra- and cross-sectoral) collaboration, as many of the challenges faced are the same.

As for Open Internet standards, the suggestion came up to consider setting up regional or national "Platforms" of multiple stakeholders to jointly set appropriate standards for a safer use of Internet and e-mail.

This was the fifth of a series of Triple I Workshops that will be organized in different regions of the world. Big thanks to all contributors to this workshop – co-organizers, presenters and participants. The results and outcomes will all be shared on the Triple-I event website.

For more information: maarten@gnksconsult.com .