GFCE TRIPLE - I

GFCE Triple-I Workshop @InSIG2018, 12 October 2018, New Delhi

Summary

On Friday 12 October, preceding the India School on Internet Governance 2018 (INSIG2018), the Indian Ministry of Electronics and IT (MeitY) hosted the GFCE Triple-I Internet Infrastructure Security Day. The Dutch Ministry of Economic Affairs and Climate as a member of the Global Forum on Cyber Expertise coordinated this initiative to look for ways forward towards more trusted use of Internet and email in the region. Participants in this workshop were 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 opened by Shri Ajay Sawhney, Secretary of the Indian Ministry of Electronics & Information Technology (MeitY). He emphasized that, since 2015, the GFCE has provided a valuable space to ensure that all nations can embrace an ever-expanding cyberspace.

The Secretary also underscored that India sees cyberspace as an ecosystem that emerging digital nations can leverage to transform the lives of the people through good governance. A trusted ecosystem is a prerequisite in order to encourage the people to embrace the Internet and to enable them to make extensive use of it to effect change in their lives. A platform like the GFCE's Triple-i initiative is important, since it helps create an ecosystem that enables efficient international cooperation in building cyber capacities.

India is aligned with and supportive of the three key priorities identified by the GFCE Secretariat during 2018 as being crucial for the further development of the GFCE. These three key priorities are:

1. Development of GFCE Working Groups along the lines of the five prioritized themes of the Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building;
2. Establishment and development of a Global Cyber Capacity Building Knowledge Partner Network, which is essential for the contribution of practical knowledge and implementation expertise to the GFCE network;
3. Further internationalization of the GFCE and the Secretariat.

The Secretary was pleased to note the organization of the workshop on "Building a trusted Internet-together" at MeitY in Delhi as a reiteration of the importance of

India's positive role on the GFCE and in furthering of the GFCE's and India's joint initiatives, efforts and agenda for Global Cyber capacity Building.

Following this, Dr. Govind welcomed participants on behalf of the Indian School on Internet Governance, co-organisers of this event, together with MeitY and Internet Society (ISOC).

After that, GFCE Triple-I facilitator 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 Olaf Kolkman (CITO ISOC), Anurag Bhatia (Hurricane Electric), and Jitender Kumar (Afilias) talked about the use and usefulness of Open Internet Standards such as DNSSEC, TLS, DANE, DMARC, DKIM, SPF and IPv6. All in the room were invited to participate and ask questions or contribute where useful.

Initially we talked about IPv6, recognizing the India, as such, has a high level of use of IPv6 compared to other countries in the world. IPv6 availability and use as such help open

DNSSEC and TLS are important in ensuring integrity of routing and of the data exchange itself. 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 had been taken into use.

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, the software code will be made available for usage in other countries/regions in the world, within the coming month. This raises a possibility for an Indian collaborative platform to provide a similar service specifically for India – whereas it is already possible today for any organization to check websites and email addresses using English.

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, on DDOS attack mitigation; Olaf Kolkman on application of MANRS by ISPs and why this matters; and Dr. Ajay Data, Data Xgen Technologies Pvt Ltd, on IDN/UA and trust aspects related to that. In addition, Cristian Hesselman, Olaf Kolkman and Maarten Botterman introduced a discussion on different aspect of trusted IoT.

Cristian Hesselman 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.

Ajay Data has been championing IDN introductions as he believes this will be a major support for many Indians that currently do not use the Internet, yet. A big challenge in this is Universal Acceptance, i.e. that Internet systems recognize the characters used in IDN addresses. At the same time, IDNs come with extra challenges with regards to confusability. Some IDN characters look exactly like other characters in other IDN sets, yet have a different ascii code. This results in addresses that look the same to humans to be different for machines, with all possible consequences for abuse. Addressing this is a major topic for those involved in progressing IDNs. According to Ajay, trusted Internet with IDN is very much possible and possibly more guaranteed than current state of security issues faced by the industry and end users. The work of LGR (label generation rules) ensure that similar looking top level domain names and mix script within top level is not allowed. If the similar guideline principals are also followed by registries and registrars, this will ensure more trusted and secure internet. In the meanwhile, new IDN tables continue to be developed and made available as to ensure more people can benefit from what the Internet has to offer – also those that would not use English or other Latin script based character sets.

MANRS stands for Mutually Agreed Norms of Routing Security (MANRS) and the need for a culture of collective responsibility whereby best practices on routing security are shared among the stakeholders. Route hijacking, route leaks, IP address spoofing, and other harmful activities can lead to DDoS attacks, traffic inspection, lost revenue, reputational damage, and more. These incidents are global in scale, with one operator's routing problems cascading to impact others. MANRS is a global initiative, supported by the Internet Society, that provides crucial fixes to reduce the most common routing threats. Olaf Kolkman introduced the why and how of MANRS with a Pecha Kucha presentation: 20 slides of 20 seconds each. He explained the Internet "hourglass model" in which it is the IP layer that basically connects all what we do with it (applications) with the infrastructure that enables this (infrastructure layer). A clear example of a way forward by better collaboration and adoption of good practice.

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. Many internet-connected devices, and in particular those sold to, 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. 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. ISOC recommends the adoption the OTA IoT Trust Framework as a guideline for safer IoT implementation. In this it is also crucial that not all responsibility for security is dumped upon the users/consumers – they often cannot be expected to have the skills and/or means. According to the IGF DC IoT, Internet of Things Good Practice aims at developing IoT systems, products, and services taking ethical considerations into account from the outset, both in the development, deployment and use phases of the life cycle, thus to find an ethical, sustainable way ahead using IoT helping to create a free, secure and rights enabling based environment. 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. A key element here is that the large base of already installed "Things" is likely to remain active for many years to come even if not complying with the newest insights. This will put some burden on the network to help protect abuse of older devices through filtering and routing. Time to act and adopt approaches like the SIDN SPIN initiative: a system for Security and Privacy for In-home Networks that aims to reduce the security risks that these devices pose to core internet systems, service providers, and end-users.

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 brainstorm session focused on answering the question:

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

Using the Open Access method for organizing this slot, three main topics were selected and consequently discussed amongst delegates:

(1) DDOS Radar

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.

<u>Actions suggested in the group were:</u>

- Implementation of DNSSEC;
- Awareness raising on the issues, both with ISPs, businesses, and the greater public;
- Developing guidelines for device manufacturers, connection providers; and cloud providers;
- Coordination of ISPs.

The initiative could be coming from the CERT community, or the ISP community, or in fact the business community – yet will require collaboration across sectors, as has been demonstrated in The Netherlands….

(2) IDN awareness and introduction (including Universal Acceptance)

IDNs play a major role in the Indian context and further preparation for uptake and universal acceptance needs to be made. As with IPv6, we may see that it will take some time before the new users (those that have not used the ascii based networks, yet) will truly join and start to trust and benefit from it. Preparation is key, and perseverance is necessary.

<u>Actions suggested in the group were:</u>

- Awareness raising;

- Promotion of use; content creation in the different scripts; application development offering services in the different scripts; search engine support of the different scripts;
- Education of use.

Content in local scripts could be highly stimulated if more public information becomes available in local scripts, as a first step. Also local initiatives will be important to make people aware and do handholding while discovering the potential of this new world that previously was not accessible – as it required mastering the English language.

(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. The SPIN approach proposed by SIDN is one of the examples that may help move the needle, and a broad group of people have worked at the IETF to develop a means to automate learning what access a device needs by use of a Manufacturer Usage Descriptions (MUD).

Actions suggested in the group were:

- Find out more from practices in other countries, including SPIN;
- Awareness and education on IoT: There is a role for educators to train developers on IoT design and security implementation around IoT .
- Creating a legal framework and setting up Standards: There is a role for Regulators, users, IoT manufacturers and consumer standards bodies to collaborate together to come up with regulation and policies on IoT devices to protect consumers from insecure devices. This should include policies of what type of IoT devices can be allowed into a country and ensure that the devices conform to security principles and technologies as well as how the data on IoT devices should be secured
- The Open Standards Organizations (like the IETF and IEEE) will play an important role in defining the standards that ensure interoperability of the IoT devices

Whereas there was not a clear commitment by specific actors, there was a broad interest to contribute to this. Possibly, setting up a nation-wide, multistakeholder project on this would help.

(4) Introduction of internet.nl tool

The old Internet standards cannot meet the modern safety requirements. This means that we have to start using new, smarter standards that keep our internet reliable. Many modern Internet Standards are available – yet not always in use, yet. Our access, hosting and email providers should take care of implementing modern internet standards and setting them correctly. The www.internet.nl website allows to check whether the Internet in use is up to date, for website, email and internet connections. Whereas anyone mastering the English language can use this website to check connections, it was also announced that the source code for the checks will shortly become available for use by third parties in other parts of the world. This would allow the possibility of creating a specific regional platform with reference to regional service providers in helping to move things forward.

Actions suggested in the group were:

- Exploring whether an Indian Internet platform can be brought together that would be willing to develop an Indian website using the source code from Internet.nl.

This action will require collaboration between several parties – and as the source code as such is available and this is a shared concern, the main requirement is someone to step up and champion this.

Conclusions

Many of the good practices presented on subjects like Open Standards adoption, joint DDOS mitigation, further IDN introduction accompanied with increasing Universal Acceptance, and IoT security were well received by a good part of the over 50 participants from the region that participated during the day. During this day delegates learned how much examples of practice and global resources are already there to help in taking local action, and expressed the intent to further local implementation of global good practices.

A lot of emphasis is on awareness raising – both within the industry 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.

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

For more information: maarten@gnksconsult.com.