GFCE Triple-I Day @INSIG2019, November 14, 2019, Kolkata, India

Report Maarten Botterman

Summary

On Thursday 14 November, 2019, INSIG hosted the GFCE Triple-I Day for the second time in India. This workshop is initiated by the Global Forum for Cyber Expertise (GFCE), is hosted by Indian School for Internet Governance (INSIG) , and is supported by APNIC, ICANN, Internet Society (ISOC) and its Indian chapters West-Bengali Chapter, and the Dutch Ministry of Economic Affairs and Climate.

Aim of the workshop is to look for ways forward towards Capacity Building for a more trusted Internet experience 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.

With thanks to all who helped make this happen, and with special thanks to Satish Babu and Anupam Agrawal and people from the Indian ISOC Chapters for their support from the outset to help make this happen.

Maarten Botterman, the GFCE Triple-I facilitator, opened the workshop introducing Paul Wilson, Director General of APNIC. APNIC (Asia Pacific Network Information Centre, pronounced A-P-NIC) is an open, member-based, not-for-profit organization, whose primary role is to distribute and manage Internet number resources (IP addresses and AS numbers) in the Asia Pacific region's economies. Paul emphasized the importance of capacity building, as to maximize the opportunity of local economies and societies to benefit from what the global Internet has to offer. APNIC has been supporting the GFCE since early on, and also supports and organizes other capacity building activities in the region.

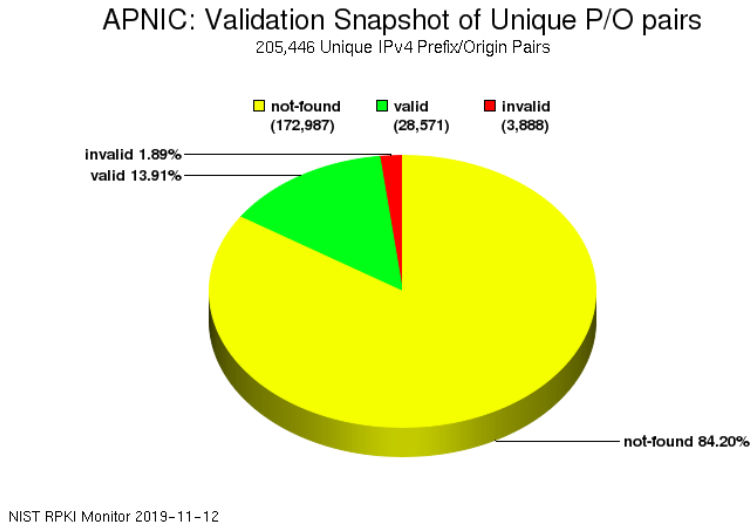
Maarten Botterman followed the opening remarks explaining that Internet was not built to be safe, but to be used. The role of GFCE is to contribute for a better infrastructure, making Internet cleaner by reducing the impact of attacks.

BLOCK I - Better Use of Today's Open Internet Standards

During the first block the focus was on the use and usefulness of Open Internet Standards such as DNSSEC/TLS/DANE, RPKI/ROA, DMARC/DKIM/SPF and IPv6. These standards are globally accepted and represent state-of-the-art insights that, when applied, can already help reduce the risks of using the Internet and email, today.

David Huberman (ICANN OCTO) expanded on the importance of cryptographic assurance for the Internet's system of unique identifiers. In his opinion, all network operators should adopt RPKI[1], DNSSEC[2], and DANE[3]. RPKI is a system of cryptographic signing and validation that secures the Internet's routing system by helping to prevent route hijackings. DNSSEC offers the same security, but to the Domain Name System. DANE leverages DNSSEC and is aimed as a replacement for the system of Certificate Authorities that we use today to sign and validate SSL certificates used in TLS. If every network operator in the world adopted these three technologies, the Internet would be a much safer place.

Simon Sohel Baroi (Fiber@Home Global) agreed with David on the importance of adoption of such state-of-the-art standards. He also expanded on RPKI by explaining how routing works, and why an extra validation is necessary: Route Origin Authorizations (ROA) provides a way to further integrity of routing by have routings authorized by a trusted instance.



[1] Resource Public Key Infrastructure (RPKI), also known as Resource Certification, is a specialized public key infrastructure (PKI) framework designed to secure the Internet's routing infrastructure.
The RPKI architecture is documented in RFC 6480.
[2] The Domain Name System Security Extensions (DNSSEC) stands for a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks.
[3] DNS-based Authentication of Named Entities (DANE) is an Internet security protocol to allow X.509 digital certificates, commonly used for Transport Layer Security (TLS), to be bound to domain names using Domain Name System Security Extensions (DNSSEC).It is proposed in RFC 6698 as a way to authenticate TLS client and server entities without a certificate authority (CA). It is updated with operational and deployment guidance in RFC 7671

The current situation in APNIC (and similarly world-wide, as that the percentage of validated domains is under 15% - and less than 20% of domains can be validated. Aim is to ensure that further introduction of standards will lead to a much lower percentage of not found pairs. Further introduction of such validation is a priority in the APNIC region.

On Email Authentication, it was said that there are several technical methods that work at "internet scale" to verify that several million emails a day are sent by the entity that claims to have sent them - for example SPF[4], DMARC[5], DKIM[6]. These ensure that the email is not forged and "authenticate" the email. What they don't do is confer any "reputation" on the email such as about whether it is a phish, spam, malware or legitimate mail. Email authentication mechanisms, combined with widely used in-house and publicly available reputation services, are a key strategy in spam filtering at scale. Up and beyond this, more work is currently underway on AS-Path Validation (BGPsec[7]) to further prevent attacks on BGP.

The pace of IPv6 deployment is a bit mixed in India. At one end we have large mobile networks which are very aggressively working on it while on the other hand on fixed-line networks it's almost non-existent. Due to the concentration of traffic and support of IPv6 by the content networks, it very much makes sense now for the fixed-line players to deploy IPv6. We expect to see a stronger growth on IPv6 as CGNAT[8] becomes a bottleneck.

BLOCK II - Inspiration from Good Practice Actions

The second block of the day, we had presentations and discussion of a number of global good practices and good practices from the region that are deemed potentially relevant for capacity building and to inspire action in the region.

Anti-abuse work

The first subject discussed was Anti-abuse work. 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) and prompt

[4] Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of the email. Sender Policy Framework is defined in RFC 7208 dated April 2014.
[5] Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email authentication protocol designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. DMARC is defined in RFC 7489, dated March 2015.
[6] DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect forged sender addresses in emails (email spoofing), a technique often used in phishing and email spam. DKIM is defined in RFC 6376, dated September 2011; with updates in RFC 8301 and RFC 8463.
[7] Border Gateway Protocol Security (BGPsec) is a security extension of the Border Gateway Protocol defined in RFC 8205, published in September 2017.
[8] Carrier-grade Network Address Translation (CGN) s an approach to IPv4 network design in which end sites, in particular residential networks, are configured with private network addresses that are translated to public IPv4 addresses by middlebox network address translator devices embedded in the network operator's network, permitting the sharing of small pools of public addresses among many end sites.

incident response (by Computer Security Incident Response Team, or CSIRTs) will help to contain damage by being able to alert users and actively take measures against the abuse. Globally, and in the region, working groups have been set up to actively detect and fight abuse by raising awareness on the key issues at hand, and take action to fight this abuse, together. One example is the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) is an international network with the aim to reduce botnets, malware, spam, viruses, DoS attacks and other online abuses. M3AAWG makes best practices documents and abuse information available that could serve as a good resource for local action

This fight is one that requires all hands on deck, as measures taken to fight abuse can lead to new abuse. A clear example is that the spammers were the first ones to implement DKIM and DMARC – origin can be validated but does not say anything about the trustworthiness of that origin or that specific message content. Sivasubramanian Muthusamy (nameshop) pointed out that DNS Security measures such as filtering or content take down, often worked in a manner that greater harm is done to the Internet than the problem being solved. He argued that this makes it important to emphasize the need to cause a shift in thinking that Internet Security measures are best left to the multi-stakeholder process, whereby swifter decisions could be taken in critical situations, and with concern for the Internet, in a manner that the measures taken do not harm the Internet. The meeting did not conclude on how to run such a process, as there is formally nothing in place to do so, on a global level. Suggestions ranged from asking ICANN to step in - but that is beyond its mandate, which is to focus on security and stability of the DNS: a mandate that does not extend to the applications or content on top of that- to industry self-regulation, to establishment and adoption of global guidelines. There was no clear conclusion on the way forward, recognizing the challenges with different alternatives, other than that abuse enabled by the Internet is an issue that deserves the highest attention.

Simon Sohel Baroi (Fiber@Home Global) made a presentation on such measures that can be taken on a voluntary basis by industry players: the Mutually Agreed Norms for Routing Security (MANRS), which is a campaign originating from ISOC aimed at best practices adoption for prevention of routing incidents. MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure. Israel discussed main motivation factors that led to this call for action, such as incident statistics, headlines and common attacks. MANRS recommends four simple but concrete actions that network operators must implement to improve Internet security and reliability:

1. Filtering: Prevent propagation of incorrect routing information
2. Anti-spoofing: Prevent traffic with spoofed source IP addresses
3. Coordination: Facilitate global operational communication and coordination between network operators
4. Global Validation: Facilitate validation of routing information on a global scale

A good discussion took place during this segment with contributions from other participants. MANRS could be used as a competitive differentiator and reduce the number and impact of routing incidents. ISOC has also been promoting webinars for spreading information.

One of the aspects of the digital world is that there will always be incidents, and in order to address those there is an important role for sharing of information and coordinated action. This was also confirmed by Vivek Nigam (APNIC), Anupam Agrawal (ISOC) and Tathagata Datta (Director, Praxis business school).

IDN, UA, and confusability

IDNs will play an important role for new generations of Internet users in the region. However, with extending the Domain Name System to use new scripts, new challenges come up that relate to acceptance by systems of those scripts, and new opportunities for abuse through confusability of different characters. Ajay Data (Universal Acceptance Study Group UASG) explained that it all starts with awareness, and that by agreeing on LGRs confusability is addressed in the best possible way through bottom-up processes with the stakeholders on specific IDNs. Creating awareness about Internationalized Domain Names (IDN), Email address internationalization (EAI) and Universal Acceptance (UA) is key, as this will serve the next billion users, world-wide as well as in the region. Confusability and Security issues around IDNs are also being addressed by building community consensus, globally.

Secure IoT deployment: global insights in the way forward

There is a high need for ensuring and enhancing security of IoT devices, as IoT is becoming part of the fabric of society, and we become increasingly dependent on the functioning of IoT ecosystems. Up to recently, security measures were exceptional, and often insufficient, but awareness is now raising with both manufacturers and users (including governments) that we need to improve on this – even when this means that the initial costs for deploying devices would go up. Other stakeholders in the value chain also have their role to play, such as access providers that should develop and adopt methodologies to early detect attempts to abuse the access of IoT devices to the Internet. Maarten Botterman pointed at the seminal work done by Information Society (ISOC) on the topic, and reminded the case of Mozilla and ISOC writing to Amazon asking to sell IoT devices with minimum levels of security. He also pointed at the DC IoT work on Building Global Trust in the Internet of Things, explaining 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 to help to create a free, secure and enabling rights-based environment: a future we want.

IX supporting secure/clean communications

As more interconnection grows, the dependency on IXP route servers is increasing. IXPs can play a good role in the routing security by implementing IRR as well as RPKI based filtering for their members As the interconnection at IXPs grows, the dependency on the IXPs route server will further increase and it will become very important for IXP operators to maintain basic routing hygiene by filtering on the basis on IRR and RPKI. Automation via tools like a routeserver and IXP manager further help in better routing hygiene implementation across the internet exchanges.

Block III: Planning for a More Trusted Internet: Marketplace for Action

During this block, conclusions were be drawn and possible actions will be developed aimed at increasing trust in the use of Internet and email in the region. The discussion was facilitated by Maarten Botterman. He invited members of organizations to express their ideas. Events like this GFCE Triple-I workshop, that brings multiple stakeholders together to discuss different aspects from Internet related activities that relate to each other, and that call for action, are incredibly important in this

During the workshop it was found that RPKI in combination with ROA makes a lot of sense, yet requires more action to increase the number of validated domains.

PROPOSED ACTION: *setup a RPKI deployment tracker, together*. A number of volunteers proposed to work together with a focus on India as tracking global status will just add too much of data and will make it non-actionable. A proposal is currently under development, tentatively pursuing the following steps:

1. Data collection of Indian prefixes from global table and check ROA status;
2. Presentation: initially with a basic webpage as well as a regular email to INNOG mailing list. This webpage can show top ASNs based on the prefixes and their ROA status as well as highlight cases of ROA invalids for the country.

It is important to find authorative ways to inform end users so they can make smarter choices. IN this there is two ways forward:

1- In general, for faster adoption of state-of-the-art global Internet security standards it is useful to have a way to test it, and share guidance on implementation. Maarten Botterman presented the Compliance testing tool at Internet.nl (developed by NLnet Labs and the Dutch Platform Internet Standards). Internet.nl is a user friendly way to test adoption of standards with Compliance test, exclusively security standards, and provide suggestions for possible improvements. It was created to be an user led demand tool that anyone can use to test its connections. Tests covers measurements on Connection, Web and Email.

PROPOSED ACTION: *explore using the compliance testing tool in the region*. The tool is currently available in Dutch and English at www.internet.nl, and the code is available as Open Source so it can be applied, regionally, in regional context and additional languages. However, this would require local action to implement the source code in a local setting.

2- For many end users, going to another website to test websites on their adoption of up-to-date security standards ia a step too much. It should be explored how secure connections can be made recognizable using visible information in website.

PROPOSED ACTION: *explore ways to make the level of security more visible to end users* when using websites. There was not a concrete proposal, yet it was said this would require collaboration with browser suppliers. In addition, it would be important to get information on security issues out to the larger public.

Internet exchanges can also play a role in keeping the Internet more secure by working together and use good practices. Participants found that in India, there is room for improvement, and better collaboration.

PROPOSED ACTION: *collaborate for development and adoption of national good practices:* reach out to NIXI to develop a national collaboration towards IX good practice standards development and adoption. It was suggested to also involve neighbouring countries in this.

At the end of the workshop, the INSIG Organizers suggested the GFCE Triple-I workshop to organize again a workshop in conjunction with INSIG2020.

PROPOSED ACTION: set up more GFCE Triple-I type workshops in the region. The workshop again generated useful insights that will be brought further through the Indian regional ISOC chapters and other participants. Question was whether in 2020 GFCE would be prepared to again help make a Triple-I workshop possible, in conjunction with INSIG2020.

For more information about GFCE Triple-I, including results of earlier events, please go to the GFCE Triple-I pages. If you are interested in improving the trusted Internet experience in your region.

-=(ends)=-