GFCE Triple-I Day @LACIGF2019, August 5 2019, La Paz, Bolivia

Report by Daniel Fink & Maarten Botterman

Summary

On Monday 5 August, the LACIGF hosted the GFCE Triple-I Day for the first time in LAC region. This workshop was supported by LACIGF (https://lacigf.org/), LACTLD (https://www.lactld.org/), LACNIC (https://www.lacnic.net/), LACAAWG, nic.br/cgi.br (https://cgi.br/), ICANN (http://www.icann.org), Internet Society (http://www.Internetsociety.org) and its Bolivian 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. The workshop was held mostly in Spanish, and partly in English

With thanks to all who helped make this happen, and with special thanks to Rafael Lito Ibarra and Miguel "Nacho" Estrada for their support from the outset to help make this happen. And we could not have done it without the invaluable support from Roberto Zambrana, Chair of the ISOC Bolivia Chapter, who helped reach out for all practical arrangements and invitations in Bolivia itself.

Maarten Botterman, the GFCE Triple-I facilitator, opened the workshop introducing Lito Ibarra as his Spanish language co-facilitator for this workshop, honoring the fact that most participants were more fluent in Spanish than English. Lito started by saying we were gathering for building capacities. LACIGF is a good venue to organize the GFCE event and exchange information related to Internet security. He invited participants to focus on ideas, plans and opportunities as outcome for the event, that should be written in a flipchart provided by organizers. He highlighted the presence of the supporting organizations and thanked to Roberto Zambrano from ISOC Bolivia for organizing the event.

Iván Zambrana, the Bolivian Vice-Minister for Telecommunications, welcomed all participants to La Paz and thanked for the effort. He stated that Bolivia has a large territory with a relatively low population challenged by basic problems like health, education, production means and so forth. He believes the Internet is a good tool to tackle these challenges and expect the workshop will bring up ideas on how to implement it. From the government's point of view, there is a need for quickly implementable solutions for Bolivian people to take advantage of the Internet and enhance security is a very important factor. He said he is ready to work together and is sure the outcomes

of the workshop will be a great hand for improving people's life in Bolivia. Maarten Botterman thanked for the Vice Minister speech saying that we are all in good hands with Vice Minister Iván Zambrana.

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.

Daniel Fink (ICANN), Mauricio Oviedo (CEO SOCIUM) and Jannett Ibañez (ADSIB / NIC Bolivia) first focused on DNSSEC, as standard that helps ensure integrity of DNS origin. Daniel explained how the standard actually works, and what was needed to get it to be in use. Other relevant implementation topics were discussed by Mauricio Oviedo such as challenges to sign second level zones and how to "change gears" on this adoption. Mauricio pointed that more information in Spanish language is necessary to enhance capacities and highlighted that administrators should be more confident and prepared to act on their systems in case of failures on the implementations. Hugo Salgado contributed saying that there are good tools to automate zone signing, but there are still technology needs for monitoring DNSSEC problems. He recommended a tool written by NIC.br. Mauricio presented the idea of offering laboratories to increase confidence in administrators. He added that high turnover in companies can also be a challenge for the stability of the implementations. A representative of a Bolivian ISP informed they have few zones in their operation, not yet signed. On the other hand, they had implemented DNSSEC in recursive servers. Their experience to overcome the lack of confidence was running tests on experimental servers before scaling to the real operations. He agrees that the fear of facing a DNS failure is critical. Jannett Ibañez presented the well-structured DNSSEC implementation plan for the .BO ccTLD. Since 2018 ADSIB / NIC Bolivia has been conducting training sessions and workshops with international experts to prepare the implementation. A good practice presented by Mrs. Ibañez is the engagement of several entities from Bolivia in a multistakeholder fashion to be involved in the plan from the beginning. A solid chronogram was presented and the signing of .BO is expected to happen on November 2019.

Lia Solis (LACNOG, ISOC Bolivia) talked about DMARK, DKIM and SPF as important standards for email integrity. Lia recommendations are to make sure:

i. adequate capacities are in place for successful implementations;
ii. planning and actions with engagement of all stakeholders and;
iii. trust by design.

She also presented statistics of global adoption of these standards as published by Gmail reports. In the second part of her presentation, Lia presented IPv6 and the benefits of its adoption such as: Better connectivity; Support to innovation; Cost reduction (due to lack of IPv4) and economic growth. According to her views, challenges for IPv6 adoption in Bolivia can be summarized in resources (human and financial), false perception that it should not be considered a problem, existing infrastructure incompatibilities and a false perception that NAT is a feasible solution for lack of IPv4 addresses. IPv6 adoption rate in Bolivia is now 13.35. During her presentation, Lia recommended that policies should be in place to boost IPv6 adoption, for example, add a requisite for domain owners to enable IPv6 when they renew their accounts. Online games consoles, nowadays operating with IPv4 only servers, should also consider IPv6 adoption as soon as possible.

Gerardo Rada (LACNIC) presented about RPKI (Resource Public Key Infrastructure), standards that are aimed at ensuring that routing is more secure. He conducted an interactive exercise to demonstrate possible problems in BGP routing such as hijacking the shortest path or a specific route. Gerardo also discussed recent cases of routing failures and introduced ROA (Route Origin Authorisations) as a way to further integrity of routing by have routings authorized by a trusted instance. LACNIC developed a tool to support these implementations, which is now available.

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. Lucimara Desiderá (Chair, LAC AAWG; Member, M3AAWG) provided a background on work currently going on in the region and world-wide, and explained how other stakeholders can benefit from this, and contribute to this. 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 icould serve as a good resource for local action. Lucimara highlighted that these abuse problems are global problems that cannot be solved by individual actors. Therefore she recommended a multistakeholder working group approach based on trust and collaborations, as adopted by M3AAWG as a good procedure to be followed in the region, including the engagement of more regional members in M3AAWG. LAC AAWG is the regional initiative to focus on this.

The NIC.br's National Program “For a Safer Internet” was presented by Lucimara in her capacity of Security Analyst at CERT.br. Firstly, CERT.br was introduced as the national body to increase the level of security and incident handling capacity of the networks connected to the Internet in Brazil. The Mirai incident compromised Customer Premises Equipment (CPEs), and Deutsche Telekom was able to remedy firmware updates in just 2 days. Unfortunately the situation in LAC

region is different, with more heterogeneous and vulnerable pieces of CPE deployed by ISP's, which was creating a challenge on how to recommend better designs to manufacturers and/or buyers. Sebastian Bellagamba from ISOC pointed that ISP's are typically sensitive to costs, where a few cents could represent huge savings in large purchases of equipment. Lucimara agreed, but added that consequences could be much worse given that some attacks have the potential to simply destroy CPE's firmware and bring the need to replace all CPE's in the network. The CERT.br National Initiative for A More Secure Internet Program tackled this challenge with the objectives of:

- Reduce Denial of Service attacks originating in Brazilian networks;
- Reduce the Prefix Hijacking, Route Leak, and IP Spoofing;
- Reduce the vulnerabilities and configuration failures in network elements; and
- Create a culture of security.
- Promoted best practices such as Hardening;
- Close open services,
- Implement Routing Security and Anti-spoofing (BCP 38).

The initiative was jointly promoted by NIC.br/CGI.br, ISOC and ISPs, Hosting and Telco Associations. Results of this initiative were encouraging with a substantial reduction in national attacks. They also received international recognition for the effort. Minimum Security Requirements for CPEs Acquisition are published by M3AAWG and LACNOG.

Israel Rosas (ISOC) made a presentation on Mutually Agreed Norms for Routing Security (MANRS), which is a campaign 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 many participants. MANRS could be used as a competitive differentiator and reduce the number and impact of routing incidents. A representative from a Bolivian ISP informed they are already implementing the good practices. ISOC has also been promoting webinars for spreading information. Lia Solis and Israel Rosas offered collaboration to anyone interested in joining the initiative.

After that, Daniel Fink reported on ICANN's Domain Abuse Activity Reporting (DAAR) project. DAAR is a database 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, but to provide transparency on weaknesses in the DNS. The reporting

tool is aimed at the ICANN community, which can then use the data to facilitate informed policy decisions. DAAR provides the ICANN community with a reliable, persistent, and reproducible set of data from which security threat (abuse) analyses could be performed, and can serve as a platform for studying or reporting daily or historical registration or abuse activity.. It 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. A monthly report is published on ICANN web site freely available for people to consult. As such, it includes data from generic Top Level Domains (gTLDs) that are contracted by ICANN, but is also 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 DAAR. ccTLDs interested can contact ICANN to have more information on how to proceed to join.

CERT collaboration

Lucimara Desidera (member of CERT.br and FIRST), explored what are today key CERT concerns and activities, how can stakeholders benefit, and what stakeholders do to help. A Computer Security Incident Response Team (CSIRT) is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity. Their services are usually performed for a defined constituency that could be a parent entity such as a corporate, governmental, or educational organization; a region or country; a research network; or a paid client. An Incident is any real or suspected adverse event in relation to the security of computer systems or computer networks. Internet has grown exponentially since 1969, as well as the occurrence of incidents since then. It became imperative that CSIRTS should work together under the principles of common goals and trust, something that is built and not mandated. As a recommendation to governments, Lucimara explained that CSIRTS should not be created from a top down approach and it should not be implemented within intelligence agencies. Maarten added that there are examples where governments did play an important facilitating approach, for instance by creating an exemplary government CERT, and allow it to play a facilitating role in the CSIRT community (such as organization of meetings, and exchange of good practice), thus supporting development of CSIRTs in a bottom-up fashion.

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. Discussion were led by Sebastian Bellagamba (Internet Society); Maarten Botterman (IGF DC IoT).

Sebastian presented the IoT Trust Framework for Privacy & Security, saying it is expected IoT devices will be 5 times the global population by 2022. That means new players joining the network along with security risks and privacy concerns. A list of challenges were identified related to manufacturers, services and consumers. The trust framework will require a collective responsibility and is a work in progress that consider 40 strategic principles necessary to address IoT security, privacy and lifecycle issues. Sebastian concluded with updates on the current work such as initiating multistakeholder processes in countries for framework's adoption, pointing the recent conclusion of process in Canada available at https://iotsecurity2018.ca .
Maarten Botterman reminded the case of Mozilla and ISOC writing to Amazon asking to sell IoT devices with minimum levels of security. He 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.

Flash contributions: other exemplary practices

Hugo Salgado Hernández (NIC Chile / LACTLD) presented the LACTLD's Anycast Cloud, an upgrade on the previous cooperation among regional ccTLD operations that offers increased resiliency and scalability features. Anycast can help reduce the impact of DDoS attacks (when a server is overloaded with requests and crashes) through better load balancing making use of other routes and servers. With anycast, requests are fulfilled by other locations during mitigation and recovery. The Anycast Cloud is available to LACTLD members where each member can install one or more nodes, rely on the cloud for their own services and save costs with a shared administration. Operations began in 2015 serving 8 ccTLDs in LAC region and 7 working instances around the continent. The project is growing to add new ccTLDs and expanding anycast instances in other regions such as Europe and the USA. Hugo concluded mentioning this is a good example of the best use of technology to save costs, integrate the region and deliver a better service to users.

Following Hugo's presentation, 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. Maarten went through some features of the tool with screenshot examples. Batch tests are available for large assessments, which, for instance, would allow to submit a list of web addresses from all government services in a country. 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. A fantastic tool indeed.

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, and Lito Ibarra. Lito started by stating that there is a chance that solutions already exist for problems we are facing. He invited members of organizations to express their ideas. Ernesto Bojorquez, president of LACTLD, thanked for the workshop and appreciated the format of the event where we could build trusted relationships for future collaborations. He predicted that this initiative could have great impacts and highlighted the importance of all standards that were discussed. Sebastian Bellagamba, Regional Director for Latin America and the Caribbean from ISOC, explained that Internet is a network of networks with immense value to the society. This value should be protected and this is a task for joint forces. 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. Nacho Estrada (LACTLD) said that silos should be broken and these events help, and should be repeated in other communities. Mauricio Oviedo expressed his concern about bad actors that are actively working, already today, to explore vulnerabilities. He believes in sharing experiences and the creation of a chain of trust, and also called for action.

PROPOSED ACTION: set up more GFCE Triple-I type workshops in the region

Users should prefer to buy better quality equipment and governments should have ways to homologate WiFi and IoT devices. Helping users understand what they get, in terms of security support, and how to guarantee that it is as stated, requires labeling and certification. Lucimara added that it's hard to homologate software in those equipment and certifications could create a false perception of security. Her recommendation is to think about processes to ensure safety in those equipment and be prepared for incidents permanently. Sebastian added that certifications processes nowadays are different from the ones used in the past. There are many more manufacturers and products available these days.

PROPOSED ACTION: plan for better ways to inform users about the risks related to devices, and how to deal with this. Collaboration in the ISOC framework for action may be a good start.

A member from ISOC Bolivia asked for a tool to measure Internet speed quality and compare broadband in Bolivia with other countries, as to inform policy making. Internet connections in Bolivia as perceived slow mostly due to incorrect configurations and unauthorized access from other users to ones connections. In addition, highly densely populated buildings faces lack of 2.4 GHz channels.

PROPOSED ACTION: analyze the real situation with regards to Internet speed, as to inform action where useful or necessary.

A member from private sector informed he is working on an innovation cluster and he believes the technologies discussed during the workshop should be shared to Bolivian tech startups. Lito Ibarra added that there is little consciousness from users on these topics and people do not see themselves as possible targets of online attacks. Asked what could be done to create more awareness for the citizens. A participant from Ecuador informed that during the recent conduction of Julian Assange from Ecuador Embassy to the authorities, several threats were published (and commented on press) against Ecuador were announced, resulting in concerns from the general population. According to him, information from media channels were not sufficiently educated to provide adequate guidance to the people. Lia Solis highlighted the importance of participation on Internet Governance fora and the topic of security are transversal to all discussions. Users should be aware of their power and be more conscious.

One participant said he would like to socialize these topics with the help of the Bolivian vice minister, Iván Zambrana, who attended most of the workshop, with high interest. It would be very important to share minimum requirements to local companies. Another participant from Bolivia asked if it would be more important to educate the population or the private sector. She believed that for security the private sector should be priority on educational programs. And as part of social responsibility, companies should educate their clients about cybersecurity. Educating the population could be one of the social responsibility forms that companies could adopt. Journalists and media should be involved in these activities.

PROPOSED ACTION: get together to create the necessary awareness campaigns, and include security thinking from the outset in education curricula.

Flipchart Opportunities

In addition, a number of ideas to take forward had come up during the day. Whereas there was no explicit commitment for action, the interest to engage in one or more of these topics was explicitly expressed:

- DNSSEC:
    - Creation of platforms for testing and monitoring DNSSEC deployments;
    - Encourage DNSSEC validation in ISP's
- Automate zone signing processes
- ISP's and companies/organizations creating ROA's for RPKI
- Get to know and promote Best Current Operational Practices (BCOPS) in Customer Premises Equipment (CPEs) for security (in English and Spanish);
- MANRS:
    - Participate in LAC AAWG meetings;
    - Implement MANRS if you manage an ASN
- Host a LACTLD Anycast node
- Test domains on up-to-date-ness of the protocols used at www.Internet.nl
- Discuss and list norms to be adopted by governments and other organizations

- Implement a trustmark initiative to ensure secure deployment of IoT, consider certifying IoT devices before they are allowed on sales platforms (considering security and firmware);
- Develop norms for quality and measurements for Internet connections;
- Maintain and increase collaboration among countries, organizations and persons, and across sectors, and develop a clear understanding of the roles in making the Internet a more trusted place for users;
- Repeat workshops like this at different occasions.

At the end of the workshop, the Chilean host of LACIGF2020 invited the GFCE Triple-I workshop to be part of LACIGF2020.

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)=-