GFCE Triple-I Workshop @APRICOT2019, 23 February 2019, Daejeon, South Korea

Summary

On Saturday 23 February, APRICOT 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 global 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.

GFCE Triple-I facilitator Maarten Botterman highlighted the goal of the day: “What to do to improve justified trust in using the internet and email in the region” “National internet infrastructure protection, internet exchange points, registries, open source software, email security, and routing security”.

In his key note, Kuo Wei Wu warned for the danger of fragmentation of the Internet. As an example he pointed at the Chinese efforts to create a separate root server, an example that might be followed by others and thus breaking end-to-end connectivity. The YETI project is a simple way for China to make sure that if there is a war between the US and China, Internet in China would continue to work, no matter what US Government would be able to do with the root (“What if USGOV pulls .CN out of root?”). Similar efforts are underway with other governments. This would also open the door to State censorship via control of the locally available root zone. Whereas the driver may be to “assure security”, the result may be degradation of the Internet as we know it because of fragmentation.

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 Aftab Siddique (Internet Society) talked about the use and

usefulness of Open Internet Standards such as DNSSEC, TLS, DANE, DMARC, DKIM, SPF, and Jordi Palet (The IPv6 Company) about progress and application of IPv6. Application in South-East Asia is still very low, whereas application of IPv6 is eventually inevitable. All in the room were invited to participate and ask questions or contribute where useful.

DNSSEC, TLS and DANE are important in ensuring integrity of routing and of the data exchange itself. With regards to DNSSEC, todays' challenges range from the computational overhead, and the complexity of application which is not a problem for specialists, but currently a severe burden for regular ISPs. In addition, the question comes up why investment should be made if there is not a direct return. Currently, there are few direct economic incentives to justify investments. It is also not the answer to DDOS attacks, probably the main concern of ISPs at the moment. DNSSEC is thus still low down on many operators' list of priority. If we could make DNSSEC easier by being part of the "deploy and forget DNS" experience, that would have DNSSEC enabled. Clear that awareness needs to go up. With regards to SPF (HTTPS deployment), it is clear that web browser vendors and website operator have responsibilities. responsibilities, and education of end users is important. It was also noted that application of DANE would have significant added value, and is, as approach, less vulnerable than the use of CAs.

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. While the new generation of users prefers direct messaging often above email, better measures to enhance justified trust in the integrity of email and its routing continue to be important.

As for IPv6: there is no medium-long term Internet continuity without a secure IPv6 deployment. It is necessary that any work related to interned, from applications development to new product and services, and not forgetting IoT, is done with full support of dual-stack, but at the same time ensuring that it works in an IPv6-only environment. Jordi concluded that governments and regulators must ensure that public networks, at a minimum, fully support IPv6, so not tax-payers money is wasted before investment cycle requires renewing products and services. This also ensures that industries willing to participate in public tenders are also aware, creating a natural dynamic for IPv6-enabled end-user services. Finally, and not just related to IPv6, but also to secure and open deployment of IoT and Cloud-based services, he argued that governments need to actively support consumers ensuring thru open certification services, open APIs and firmware updates, their products don't go to the trash can if vendors or cloud providers vanish.

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.

Block II: Inspiration from Good Practice Actions

The second block is the space where inspirational practices and useful ways forward are shared. Ram Mohan spoke on infrastructure stability and DNS abuse and the need to address this adequately in order to avoid erosion of trust. Examples of abuse include threats: phishing, spam, malware, cryptojacking, ransomware etc. The biggest increases in 2018 and 2019 have been in (s)extortion, especially in the AP region. Next to that, specifically in the AP region, spam for dating websites are big (especially in Japan), and the total amount of spam that hits the AP region is much higher than in other regions. The estimated annual cost of cybercrime in 2018 was 600B USD. In this, romance scams alone accounted for 140B USD. The impact on infrastructure is in particular related to blocklisting of whole TLDs due to high levels of abuse, which also is impacting innocent users of those TLDs. And the same I the case with IP address blocklists. In addition, being listed on SURBL or Spamhaus as less trustworthy than a competitor leads to reputational damage. Ram Mohan argued that providing consistent and deliberate attention to abuse is key, and that just using blocklists is not enough. Modern data mining and data analysis techniques need to come into play, as a failure to remove abuse from both IP address ranges and from domain names otherwise will significantly erodes trust. That erosion of trust is the single largest factor that threatens interoperability in the end-to-end Internet, as we know it.

Dr Jeong-Min Lee from KISA spoke on “Initiatives from Korea to lessen the cybersecurity divide in developing countries.” In order to enhance the resilience against attacks in the region, the Korean CERT provides programs that can be divided into three categories of education, assessment and networking. The target participants are from the OECD DAC list of ODA recipients (see http://www.oecd.org/dac/stats/daclist.htm). Lessons learned so far are that there is a need more frequently contact, thus developing a firm communication and sharing channel, and to build up a list of successful story to enhance trust.

Taiji Kimura then presented on RPKI. He gave the example of myetherwallet.com, where mis-originated the BGP prefix was used to redirect to a phishing site. RPKI would have prevented this, and this can be strengthened by adopting Route Origination Authorization (ROA). ROA can be used to compare BGP route to find mis-originated routes. Origin validation is done by using a ROA validating server and BGP router and does not require end-user intervention, and is also increasingly used to do so (see https://rpki-monitor.antd.nist.gov/). Taiji pleaded for encouraging communicating between engineers and between tech

and non-tech persons (includes customer supporting staff), and to spread a culture of "mutual help" in BGP and Internet. In the discussion, it was concluded that renewed attention for RPKI as well as ROA is important.

Cristian Hesselman: director of SIDN Labs (the research team of the .NL operator) and SSAC Member, explained the concept of a national DDOS clearing house, 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) in the Netherlands continually collecting information on potential and active DDoS sources and automatically sharing this information with each other through the clearing house. The information consists of a digest of the DDoS traffic that a critical service provider handles (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 clearing house in April of 2018 [1] [1](at that time called "national DDoS radar") together with researcher from the University of Twente after Dutch banks and government agencies were the victim of multiple DDoS attacks earlier that 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.

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, 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. For instance, 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

[1] C. Hesselman, J. van der Ham, R. van Rijswijk, J. Santanna, and A. Pras, "A proactive and collaborative DDoS mitigation strategy for the Dutch critical infrastructure", blog, April 2018, https://www.sidnlabs.nl/a/news/a-proactive-and-collaborative-ddos-mitigation-strategy-for-the-dutch-critical-infrastructure?language_id=2

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.

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 key global Internet Standards that help make this Internet more trustworthy, when applied

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: consumers, politicians, business decision makers and service providers. When moving forward on this, the website internet.nl can be very useful, and it may be possible to set up local applications of the code that will be shared 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.

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 confirmed to be important by the well informed group of participants to this workshop during APRICOT2019.

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 add RPKI and ROA to the list of standards for which GFCE Triple-I asks for attention. In the meanwhile, NLnet Labs, the technical provider of internet.nl confirmed that RPKI and ROA will be included in the next release of the online test tool.

This was the fourth 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, especially to APRICOT, APNIC and ISOC. The results and outcomes will all be shared on the Triple-I event website.

For more information: maarten@gnksconsult.com.