GFCE Triple-I Day @INSIG2022,
September 25, Hyderabad, India

Increasing Justified Trust in the use of the Internet in India

Report by Maarten Botterman & Satish Babu

Summary

On Sunday 25 September 2022, https://insig.in/inSIG hosted the GFCE Triple-I Day for the third time in India. The workshop is initiated by the Global Forum for Cyber Expertise (GFCE), and is supported by APNIC, ICANN, Internet Society (ISOC) and its Indian chapters, as well as the Indian Ministry of Electronics and Information Technology.

This GFCE initiative is meant to facilitate awareness raising and capacity building events in different regions of the world in order to *enhance justified trust* in the use of Internet and/or email in those regions (specific priorities to be determined by stakeholders in the region). Local and regional actors are stimulated and supported in setting up and running local/regional events between regional stakeholders, bringing in local expertise, when useful. The initiative builds on the experience of two years of events around the world (2018, 2019), and is firmly embedded in the GFCE's mission of strengthening cyber capacity and expertise globally through international collaboration and cooperation.

Participants in this workshop included global and regional experts, and regional Internet stakeholder groups, including the government, business and technical community, who all contributed to finding solutions to strengthen an open end-to-end Internet. The meeting was set up as a hybrid meeting and included online participants. The outcome of the meeting is a plan to take forward, for which stakeholders are invited to participate and for which follow-up discussions should lead to a concrete and funded Action Plan (see Annex).

On behalf of GFCE Triple-I, thanks to everyone 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 workshop happen.

Satish Babu, inSIG2022 host, welcomed all. He invited ***Shri Alkesh Kumar Sharma***, Secretary from the Indian Ministry of Electronics and IT, to open the workshop and address the meeting.

The Secretary expressed his gratitude that, despite the global pandemic, we managed to stay connected. He also reminded that, while most of us are experiencing the transformative power of digital connectivity every day, there is a disproportionate access that needs to be tackled to make sure digital connectivity brings benefit to all. Region-specific capacity building efforts are key in that – customizing support to particular matters of priority. The Secretary recognized that GFCE Triple-I Workshops offer "awareness raising" and "capacity building" initiatives with the aim of "enhancing justified trust in the use of internet", and that today our world needs it more than ever before.

India is playing an important role in this with its national initiatives. Be it the Indian Government's flagship Digital India Program, which is committed to digitally empower Indian society and economy or theDigital Literacy initiative under Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA), which aims at training non-IT literate citizens to become IT literate. This is done through its efforts to bridge the linguistic gap with the platform "Bhashini" , or through its contributions to global developments, such as the GFCE and ICANN.

To be able to benefit from the Internet, addressing security and trust issues is a priority. An array of cyber safety initiatives is undertaken to address emerging security threats, their reporting and mitigation. Computer Emergency Response Team India (CERT-IN) has been at the forefront of identifying risks and liaising with public and private entities in regular cyber safety assessments of critical digital infrastructure. Further, under the Government of India's cloud policy (GI Cloud – Meghraj), great emphasis has been laid on hosting of data within the country as well as ensuring continuous security of data residing on the cloud. Data protection regulation is also underway and electronic consent framework has been published by the Government. In all of this, the Indian Ministry of Electronics & Information Technology (MeitY) remains the custodian of Information Technology Act, 2000 ("IT Act") which is a principal Act governing the entire cyberspace in India. In addition, National Internet Exchange of India (NIXI) is an active player in this process.

He emphasized that in order to benefit from the technological transformation, there cannot be a one-size-fits-all approach: it is crucial to learn from good practices and use the standards and tools that are available, today – to invest in the key infrastructure in a way that allows reaping the benefits. With that, he expressed his appreciation of the work done by GFCE Triple-I and thanked us for engaging together.

Maarten Botterman, the GFCE Triple-I facilitator, thanked the Secretary and introduced the workshop itself, reminding participants this was the third event organized by GFCE Triple-I in India, and promising to look back to the conclusions from the last in-person meeting, that took place on November 2019 in Kolkata. He reminded participants that the Internet was not built to be safe, but to be used. The role of GFCE is to contribute to a better infrastructure, making the Internet cleaner and safer to use by reducing the vulnerability and the impact of attacks.

As the Secretary had already mentioned, the Internet infrastructure is the ecosystem of protocols, standards, technology, practices and organizations that keep the internet running. An open, stable and secure internet infrastructure is key to sustaining the economic growth and social benefits that were boosted by the Internet. These internet-driven innovations require the continuation and improvement of trust in the cyber domain that is threatened by cyber-attacks (e.g. Distributed Denial-of-Service attacks), cybercrime (e.g. hacking, malware, phishing, botnets, ransomware) and unwanted messages (e.g. (e-mail) spam). The global exposure of these threats requires a collaborative, global as well as a regional/local response to secure the infrastructure that sustains the benefits of the internet.

For the regional/local response to be effective, capacity building is key. This workshop contributes to that by bringing regional/local stakeholders together with global expertise. The role of GFCE is to contribute to a better infrastructure, making the Internet safer by reducing the impact of attacks.

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

During the first block of the workshop, 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. These are also reflected in

the GFCE Triple I Handbook. Please find below a diagram indicating how these standards interrelate:

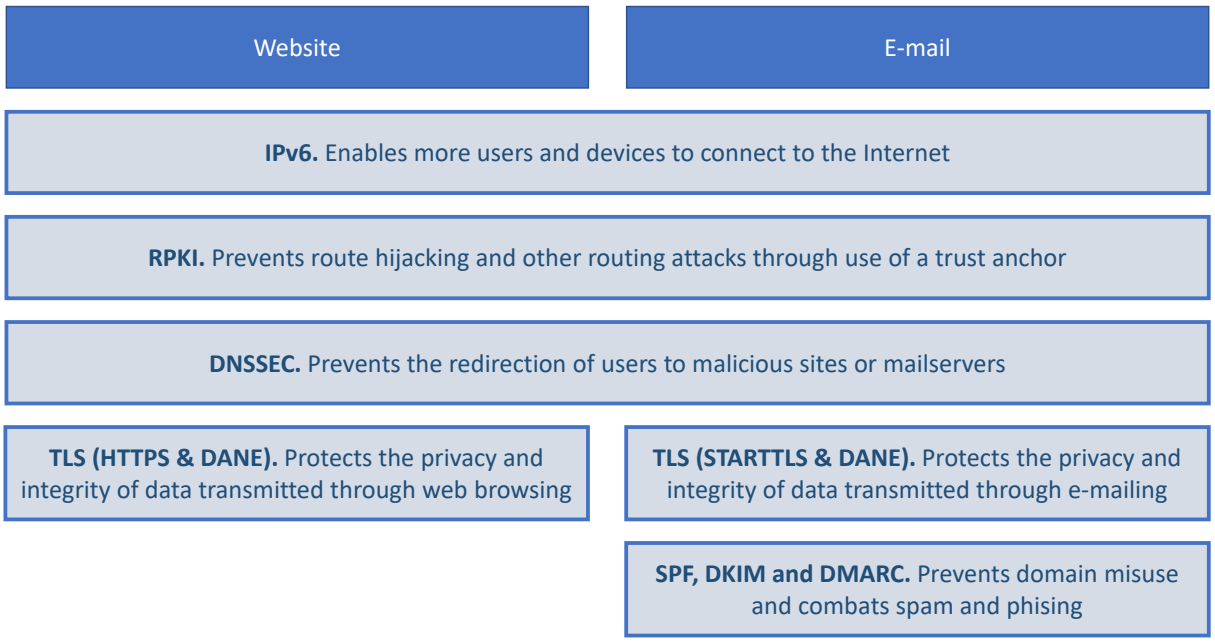

Fig.1 – today's open Internet standards

After an introduction on the value and status of different standards, we also looked into a tool developed by internet.nl that allows checking for the state of those standards – and what it takes to implement the code for local use.

On current Standards

Champika Wijayatunga (ICANN OCTO) explained that the Domain Name System (DNS), which is core to the Internet, contains a wealth of data about the connected systems – and that protection is therefore extremely important. There are several risk factors in the setup of DNS such as a hierarchical system with a "root" at the top of the hierarchy, which contains a name space of about 1500 Top Level Domain Names (TLDs). This list is used by independent root server instances around the world to perform the DNS resolution, and there are a number of measures one can take to address the associated risks:

DNS Security Extensions (DNSSEC): use public-key cryptography and digital signatures to protect the DNS data by providing (1) data origin authenticity (i.e. "Did this response truly come from the correct DNS server?") and (2) data integrity (i.e. "The data relating to the DNS server has not been modified after signing").

However, DNSSEC do not provide confidentiality for DNS data, unless combined with standards like HTTPS (DoH – RFC 8484) or TLS (DoT – RFC 7858) and achieve DNS encryption between the client and the resolver. To go beyond the protection by DNSSEC (ideally in combination with SSL/TLS or HTTPS), DNS-based Authentication of Named Entities (DANE – RFC 6698) will allow administrators of a domain name to certify the keys used in that domains' TLS clients or servers by storing them in the DNS. Thisallows domain owners to specify which Certificate Authority (CA) is allowed to issue certificates for a particular resource – as there are many CA's nowadays.

In DNSSEC deployment there are two aspects:signing of DNS data and the validation of DNS data. When it comes to DNSSEC signing, the current status with regards to Top Level Domain (TLDs) is that more than 90% of the TLD zones are signed. This includes generic, new gTLDs and a number of Country Code TLDs (ccTLDs). Some ccTLDs have not signed their zones yet, for which adoption is recommended but not obliged. Within India, DNSSEC is relatively well deployed, .IN ccTLD zone is signed, and the validation measurements are just under 60% but more is to be done to ensure better reliance – given that it will need to be used by all. Registries, Registrars, DNS Operators, Internet Service Providers and users, (be it corporate or individual users). Awareness raising is key – enabling is a necessity. Government can encourage this and lead by example. Combining DNSSEC with TLS and with DANE provides a strong integrity protection. If every network operator in the world adopted these three technologies, the Internet would be a much safer place.

Anurag Bhatia (Hurricane Electric) focused on the role of Resource Public Key Infrastructure (RPKI) and Route Origin Authorizations (ROA), discussing the challenges with routing (involving the IP addresses). He explained that, for internet routing, it is important that the IP address before and after the specific address are registered. Basically: a trust model, in which interruptions can cause disruptions – whether by purpose or by mistake. In short: through global RPKI deployment

1- Networks sign their prefixes i.e. "create ROA", and:
2- Networks validate other "networks signature".

This is to prevent "prefix hijacking" (i.e. someone originating an IP block that doesn't belong to them) and "route leaking" (i.e. announcing a route which they are not supposed to) by ensuring the integrity of the sources. Signing is one thing, however, checking whether the signature is correct closes the loop (i.e. validation). This is done by RPKI.

RPKI and ROA are high on the agenda in India, and by far most Indian Government websites are signed by RPKI ROA. However, this is not always the case, and this merits attention. Anurag built a measuring tool that now measures the RPKI deployment on a permanent base (see https://rpki/anuragbathia.com). It turns out that right now India is "on the average" – while China and Japan are lagging. Hence, more can be done by promoting signing of the routes within the country. Therefore, signing in India requires attention, but is moving forward.

A bigger challenge is validation. This occurs when everyone signs, but nobody validates, and as a consequence, the signing itself has little value. Here, progress has been made, as major (global) providers start filtering not signed routes (for list: see https://isbgpsafeyet.com). In India, some major operators are checking for signature, but not rejecting yet. As this may only be part of the chain for routing, there may still be any drop of customer traffic. This is bound to progress over time, as at some point, those operators that are not filtering will become the exception – and pressure will go up to also start filtering. APNIC and providers such as Hurricane Electric play an important role in raising attention and promoting uptake.

Sunny Chendi (Asia Pacific Network Innovation Centre - APNIC) analysed that when it comes to addresses, IPv6 is now widely deployed and the number in use is growing fast, with IPv4 addresses in scarce supply. DNSSEC, DANE, RPKI, ROA and IPv6 roll-out is very complementary and important, as to ensure integrity of routing as well as possible. As for the main challenge to implementation, Anurag quoted Geoff Huston: "*It is not a technical matter the roll-out – it is a pure financial incentive that is needed here. So, unless there is a clear value related to implementation – and it becomes more than just a cost – most operators will postpone until they cannot avoid moving forward anymore*."

However, customers feel more secure with IPv4 than with IPv6. There is still education and training required to fully understand the IPv6 protocol nuances and to ensure that security products have the same features and functionalities for protecting IPv4 and IPv6. Many products already exist to create safe, secure and trusted IPv6 networks. Therefore, APNIC and others are actively raising awareness and providing workshops for capacity building in this.

Bart Hogeveen (Australian Strategic Policy Institute - ASPI) explained that compromised email addresses can lead to effective phishing attacks (as the real owner of the email address may well be trusted) and erosion of trust. Organizations can reduce the likelihood of their domains being used to support fake emails by implementing Sender Policy Framework (SPF[1]) and Domain-based Message Authentication, Reporting and Conformance (DMARC[2]) records in their Domain Name System (DNS) configuration. Using DMARC with DomainKeys Identified Mail (DKIM[3]) to sign emails provides further safety against fake emails. Likewise, organizations can better protect

[1] 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.
[2] 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.
[3] 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.

their users against fake emails by ensuring their email systems use and apply SPF, DKIM and DMARC policies on inbound email.

In Australia, DMARC has gained a high priority as it has been recommended by the Australian Cyber Security Centre[4] following public scandals involving suspected spoofing from email addressed belonging to Australian Parliamentarians in 2019.

Using a testing tool to stimulate and support uptake of state-of-the-art Standards

In The Netherlands, a public-private collaboration is set up to select and stimulate the uptake of key standards that help use of the Internet to be more trustworthy. This multistakeholder platform meets regularly to discuss what improvements can be implemented next. A key tool to assist with the implementation is available at www.internet.nl – including code to test domains and email on their adoption of the selected standards – and what else can be done to enhance adherence to these standards.

Fig. 2: website with testing tool www.internet.nl

The code used on this website is publicly available via https://toolbox.internet.nl. It is in use in Australia, Brazil, and Denmark, and there is active interest from other parts of the world to increase its application.

[4] https://www.cyber.gov.au/acsc/view-all-content/publications/how-combat-fake-emails

Dennis Baaten (Internet.nl) is providing support to users and further development of the tool. He shared that one of the most difficult things in working with volunteers is finalising tasks, particularly when it comes to concrete work such as creating "how-to's". Practice experience has shown that it is important to have committed resources to do so – such as paid contractors or staff. Volunteers can best help by testing and providing feedback for possible further improvement.
In The Netherlands, the experience is that measuring and scoring works well to stimulate adoption, as organizations want to be seen as professional. Scoring creates transparency and provides an explanation of what can be done. Whether this is true in other cultures, too, is something to explore – as for instance the experience in Australia shows (see below).

The Public-Private partnerships underlying the Dutch Internet Standards Platform provide a solid support system, both in funding and in committing to action. The stakeholders meet regularly and share experiences and contribute to the setting up of new marketing campaigns to boost adoption. One of the lessons that can be drawn from their experience is that it is important to focus on a specific (set of) standard(s), and keep it relatively simple and straightforward. In addition, government and other stakeholders took this opportunity to work towards a "comply or explain" strategy, benefiting from the ability to measure progress on adoption of the standards through an API that makes it possible to check that specific checklist at several points in time.

Bart Hogeveen (ASPI) has been using the code to implement a test-site in Australia. His first exposure dates to 2016, and it took him about 5 years to get it implemented. Even if the internet.nl website is already in English (and could be used for checking as is), it required more than a copy/paste to implement a region-specific version.

Fig.3 – Bart Hogeveen talking during the workshop

The context for Australia is building on the 2020 Australia's Cybersecurity Strategy[5] Vision: "a more secure online world for Australians, their businesses and the essential services upon which we all depend." Nevertheless, it turned out to be hard to line up a multistakeholder support platform. For this reason, the initial focus was on setting up a public testing tool.

A main sponsor was key – this turned out to be the Australian ccTLD provider AuDA, as it perceived assisting its user base in using the Internet in a more securely as fitting to its mission. In addition to the national Cyber Security centre, there was keen interest from the Australian Small Business and Family Enterprise Ombudsman. Others were also supportive, including APNIC, although they did not play a major role.

One of the lessons learned, is that the key standards in Australia were not entirely the same as in The Netherlands. DNSSEC, for instance, was much lower on the list of priorities, and consequently, is hardly available from Internet service providers in Australia. On the other hand, secure email transport (STARTTLS and DANE) and protection against email phishing (DMARC, DKIM and SPF) have high interest and high priority, and are, consequently, wider available. Consultations took place with Industry through ACSC's Joint Cyber Security Centers, whilst also making use of the ACSC –Cybersecurity Uplift program –to harmonise and align priorities. A last key consideration in this regard was also the realization that lower priorities may not be commercially viable – in particular for small and medium businesses.

Another finding was that the Dutch stimulus of "Scoring and measuring" (i.e., blame & shame) was not acceptable in Australia since society is clearly not comfortable about sharing precise figures in this regard. Hence, for auCheck the results are displayed on a sliding scale between red and green. There wre also concerns about abuse of the check system – and a tick box was introduced to ensure awareness that this tool was only to be used for legitimate purposes.

The Australian experience shows (1) there is a lot that can be learned from other stakeholders. Good solutions for your challenges have probably been developed already (2) However, this does not mean that one-on-one implementation will work. It is recommended to consider carefully, together with other stakeholders, what is the most prevalent thing to implement in your respective region. Cultural differences, commercial/technical context, legislation, as well as practical experiences will all impact what is needed most, and what would succeed best.

Example given was the emphasis on DMARC (and DKIM, SPF) in Australia, because spoofing had had a great impact on the Australian society in the past. Whereas, for instance, in The Netherlands, there is more emphasis on DNSSEC/DANE … following serial disruptions of financial services (banks, etc.) some years ago. In general, governments get active when such disruptions take place and may trigger action through (a) legislation -requiring certain level of use

[5] https://cyber.gov.au

of standards; (b) stimulation -through awareness campaigns and/or subsidies); and (c) leading by example -adapting to new standards and leading the way, also requiring such services from upstream and downstream providers.

When comparing the experiences from the Netherlands and Australia, a common denominator is that adaption of new standards requires an investment by those in the value chain that need to adapt their systems. For this, there needs to be a concrete purpose. Whereas for some it may be a more strategic reason (e.g. longer term view, market leadership) for others the costs may be a big threshold – in particular for smaller players that have no direct interest in leading the way or may not have been yet for not having adapted their systems. A clear example of financial stimulus was the discount given by SIDN (i.e. the Netherlands ccTLD, holding .NL) to registrars/ISPs selling domain names and signing them with DNSSEC. .NL is now one of the leading domains in terms of adoption of DNSSEC.

Reasons for adoption of state-of-the-art standards are different for different stakeholders in the Internet value chain.

For Internet providers, the interest is that trust in the Internet will lead to higher uptake, thus more demand for the services. A trusted Internet is in the interest of all players, yet leading organizations are likely to invest more as their interest is higher and they can afford to invest in improvement of services.

For the government, the incentive is in empowering the users for local and global interaction, both for societal purposes and economic/market/trade purposes. For instance, Digital India is a good example of an initiative that recognizes the value of a well-functioning, safe Internet environment for the citizen. In addition, the Indian government is active at global level (e.g. in ICANN, GFCE, OEWG, …).

In the end, the key is with the users, whether commercial or non-commercial organisations, or individuals. For users to benefit most from the Internet, it is important to know they are safe, and can trust the connections to services offered on the Internet. By making users aware of the risks and measures, users will stand up and ask their suppliers to provide services they can rely upon. Websites like internet.nl and auCheck in Australia help users better understand what the situation is.

BLOCK II - Inspiration from Good Practice Actions

The second block of the day, presentations and discussions were held on a number of global and regional good practices. The afternoon session was initiated by ***Merike Kaeo***, providing an overview of the importance of cyber hygiene and trust building in cyberspace. This was followed

by an update by ***Ram Krishna Pariyar*** (ISOC) on Mutually Agreed Norms for Routing Security (MANRS), a global initiative that helps reduce the most common routing threats. ***T. Santosh*** (Ministry of Electronics and IT – MEITY) provided an overview of the Indian Multilingual Internet Initiative, ***Sarmad Hussein*** (ICANN) highlighted ICANN's support in this, and introduced the activities of UASG, and ***Ajay Data*** (Chairman UASG) ended with a call for more effort to ensure Universal Acceptance of Internationalized Domain Names, also in non-Latin scripts.

Following on, ***Rowena Schoo*** (DNS Abuse Institute) reflected on efforts done by industry leaders contributing to a safer Internet, and ***Champika Wijayatunga*** (ICANN OCTO) explained how ICANN helps in this, by providing information on facts (DAAR) and good practices (KINDNS).

Cyber Hygiene

Cyber hygiene is about "automating the boring" as security includes a lot of detailed actions where human error often causes issues. ***Merike Kaeo*** (Doubleshot Security) explained that today, stakes are high since the criminal community has increasingly sophisticated and automated tools to carry out attacks that have greater impact on the victims. For example, ransomware-as-a-service has created a viable business for criminals who use various types of malware designed to encrypt files on systems to render them unavailable and unusable until a ransom is paid.

In a 2018 visit to India with government, business and educational leaders, Merike participated in a series of events pointing at the importance of cyber hygiene and understanding organizational security risks. A critical fundamental step for ensuring cyber hygiene is to have an Incident Response Plan in place – a crisis plan for when critical digital assets are under attack. This plan would include assigning roles and responsibilities for those who have authority to take action and escalation processes/procedures for notifying key individuals. Also important is to know which external entities to go to for help, especially upstream and downstream ISPs if there is a need for any traffic filtering during a Distributed Denial of Service (DDoS) attack. In other words, it is important to e know who to go to, and who to ask for help – upstream and downstream. Additionally, making sure there are trusted offline backups for critical assets and that these backups can be reliably used to restore critical services, since some attacks will cause backups to be damaged during the restauration process. Finally, the last step is to, when a evaluate and learn after a crisis– there is always room for improvement.

Another aspect to consider is that vulnerabilities are unavoidable. When discovered, organisations should act as rapidly as possible to evaluate and then remediate/patch those vulnerabilities. This should be handled on a day-to-day basis and can be automated with existing tools.

Added essential Security Controls include:

- User Authentication/Authorization;

- Device Authentication/Authorization;
- Access Control (Packet/Route/URL);
- Data Integrity;
- Data Confidentiality;
- Auditing / Logging;
- DoS Mitigation

There is always a balance to be sought between convenience and security and privacy. Automated tools are key to provide convenience for security and privacy functionality – but when things go wrong, you need to understand what has been automated to know how to troubleshoot and fix issues in a timely manner. Protocols interrelate, and it is important to understand the interdependencies between the technologies that protect routing, DNS and email. This can also help prioritize deployment strategies.

There is no such thing as 100% security – it is all about risk management and the right balance needs to be found between convenience, security and privacy. Technologies and standards will continue to evolve, and it is important to review policies and procedures on an annual basis and review any risk decisions to see if the risk appetite has changed as a result of changing circumstances and business priorities.

The discussion was raised whether IPv6 was less easy to secure than IPv4. Merike explained that IPv6 differs from the IPv4 protocol in many ways but primarily it is the multiple addresses per interface and more automation than with IPv4 that create the differences to be considered from security perspective. In addition, while some organizations may believe that they are not utilizing IPv6 – they may well be subject to IPv6 based attacks if their ISP or equipment vendor has enabled IPv6 by default. It is also important to check what type of IP traffic is being utilized in your networks. All traffic, especially for routing, DNS and email, should be cryptographically protected. Cryptographic protection can be for integrity or confidentiality and technological capabilities need to be understood.

With digital identities, it is essential to keep credential lifecycle management in focus. Many focus on security aspects for creating and distributing credentials, but it is critical to also consider processes and procedures to securely distribute, store, recover, change, renew, revoke and destroy credentials. Credential compromise is often a first step to more impactful cyber-attacks which is why the entire lifecycle for credentials needs concerted focus. Multifactor credentials must be used so that compromising a single credential will not be so impactful.

Vendors usually design for the lowest common denominator – and defaults need to be evaluated to ensure they are appropriate for a given environment.

Merike emphasized that to create and build an environment with effective fundamental cyber hygiene, a culture that builds and maintains trust is required – and even more so: a culture of commitment. Blaming and shaming does not work in many cultures around the world – an environment where it is encouraged to point out security risks and create transparency of issues and how to mitigate risks in a positive manner is usually more effective. In practice, administrators tend to want to trust your staff and business partners, but, as humans, we are prone to making mistakes, and it is important to audit what we believe to be in practice. Trust, but verify.

When building out a digital economy, governments can help with awareness raising on popular social outlets such as television, radio and social media, aimed at different groups in society, emphasizing some fundamental online behavior risks and how to avoid those risks. The foundation for safe use of the Internet is the understanding of insecure behavior and practices, and what users can do to use the Internet in a safer manner. Bringing together different stakeholders to coordinate and work together is essential. In fact, bringing stakeholders together to learn from some of the already publicized attacks (within India, or beyond) tends to be very helpful.

Advancing Routing Security

Ram Krishna Pariyar (ISOC) made a presentation on measures that can be taken on a voluntary basis by industry players: the Mutually Agreed Norms for Routing Security[6] (MANRS), which is a campaign originating from ISOC aimed at best practices adoption for prevention of routing incidents.

Routing is a key element of making the Internet work. There are ~70,000 core networks (Autonomous Systems) across the Internet, each using a unique Autonomous System Number (ASN) to identify itself to other networks. Routers use Border Gateway Protocol (BGP) to exchange “reachability information” - networks they know how to reach. Routers build a “routing table” and pick the best route when sending a packet, typically based on the shortest path.

Border Gateway Protocol (BGP) is based entirely on trust between networks. It was created before security was a concern, and assumes all networks are trustworthy. There is no built-in validation that updates are legitimate. This chain of trust spans continents, and there is a clear lack of reliable resource data.

In 2019 alone, over 10,000 routing outages or attacks – such as hijacking, leaks, and spoofing – led to a range of problems including stolen data, lost revenue, reputational damage, and more. About 40% of all network incidents are attacks; 3.8% of all Autonomous Systems on the Internet

[6] https://www.manrs.org

were affected. Incidents are global in scale, with one operator's routing problems cascading to impact others. With that, insecure routing is one of the most common paths for malicious threats.

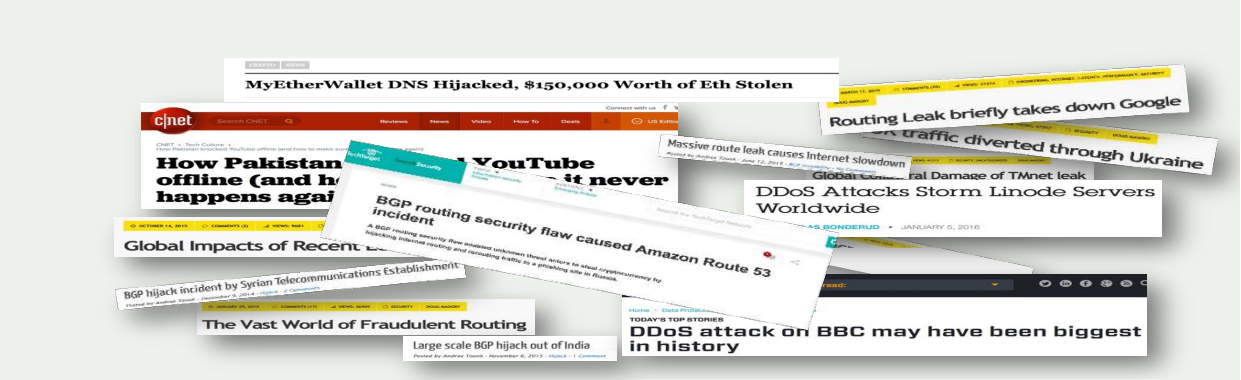

Fig. 4 – clipping of relevant articles in newspapers – courtesy ISOC

Attacks can take anywhere from hours to months to recognize, and inadvertent errors can take entire countries offline, while attackers can steal an individual's data or hold an organization's network hostage. Being vigilant and having procedures in place is therefore key.

MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure. MANRS recommends four simple but concrete actions that network operators must implement to improve Internet security and reliability:

Fig. 5 MANRS Actions for Network Operators (source: ISOC)

Network operators have a responsibility to ensure a globally robust and secure routing infrastructure. Network's safety depends on a routing infrastructure that eradicates damaging

actors and accidental misconfigurations that wreak havoc on the Internet. The more network operators work together, the fewer incidents there will be, and the less damage they can do.

As previously discussed, there needs to be an incentive for network operators to invest. Recognizing this, Ram indicated the following reasons for network operators, but also Internet Exchange Points and Content Delivery Networks (CDNs) and Cloud Providers to adopt MANRS as working practice:

1- It signals an organization's security-forward posture and can eliminate SLA violations that reduce profitability or cost customer relationships;
2- It reduces routing incidents, helping networks readily identify and address problems with customers or peers.
3- It improves network operations by establishing better and cleaner peering communication pathways, while also providing granular insight for troubleshooting.
4- With all this, it addresses many concerns of security-focused enterprises and other customers.

In line with what Merike mentioned: security is a process, not a state. MANRS provides a structure and a consistent approach to solving security issues facing the Internet. Adopting MANRS improves the security and reliability of the global Internet routing system, based on collaboration among participants and shared responsibility for the Internet infrastructure. MANRS sets a new norm for routing security: joining a community of security-minded organizations committed to making the global routing infrastructure more robust and secure.

Ram concluded with a quote from Jane Addams (Noble Peace Prize Winner): "*The good we secure for ourselves is precarious and uncertain until it is secured for all of us and incorporated into our common life*." It is therefore great to see that the commitment to adopt MANRS is truly growing throughout the industry. Today, already more than 750 Autonomous Servers (ASs) are signed up, and more are to follow.

India's Multilingual Internet and the importance of Universal Acceptance

T. Santhosh (Ministry of Electronics and IT – MEITY) introduced the roadmap to universal acceptance and a multilingual Internet, as supported by the Indian government. In order to bring in more users to the Internet, there is a need to serve those that only speak in the local language, as well. The objective is to achieve "Universal Acceptance" (UA) leading to acceptance of Internationalized Domain Names (IDNs) equally by all Internet-enabled applications, devices, and systems – irrespective of the script used.

Currently, India has 15 IDN ccTLDs (.bharat) available, covering 22 Indian languages representing 11 scripts. As per the reports of the Universal Acceptance Study Group (UASG), the

global Email address internationalization (EAI) acceptance rate is currently close to 8%, and India's EAI acceptance rate is around 11%.

Though the national Internet Exchange of India offers domain names in 22 official Indian languages, very few people can actually access the Internet in their native languages. The Indian government agrees with ICANN that many of the next billion Internet users will require to be enabled to do so in their own language. Although India is a multilingual country, and 92% of the population is non-English, 50% of India's population is not yet online. We believe that providing access to the Internet for those users will require technological solutions apart from merely internationalized or multilingual content. Localized Domain names and email addressed that resolve need to be part of these solutions.

T. Santhosh continued explaining that the Top Level and Internationalized Domains have evolved and matured enough as far as technology is concerned and that they just need to be rolled out. Services that work are crucial for increasing business and will benefit from being able to reach more people online when also available in IDNs. This is true for both commercial services by businesses, as for government services, thus creating inclusiveness and better adoption.

In order to further prepare a roadmap, a multistakeholder Committee was set up under chairmanship of Anil Kumar Jain, CEO of National Internet Exchange of India (NIXI). The work will be executed with active participation of stakeholders in the country including government, academia, and civil society, along with the support of the UASG. The Working group started their operations in January 2022. The first phase is a focus on "Universal Acceptance" – the second phase will focus on integration of IDNs, and also will consider voice-based interaction. Subcommittees have been set up to tackle all key areas that are affected by the wish to go multilingual:

- Hardware (keyboards, etc.);
- Email (resolving);
- Websites (resolving);
- Software/OS (capacity building);
- Security Devices (e.g. dealing with spam etc.);
- Browsers;
- Apps and Social Media platforms.

The Committee decided to develop a short-term plan, a medium-term plan and a longer-term plan. Capacity-building will be an underlying aspect throughout this whole process:

1- Short term: All Government websites to have Internationalized Domain Names including all the resources,"linkification" to IDN in the website contents (mygov.in site Hindi content on the Hindi IDN website);

2- Mid-term: All Government applications to be in at least three languages - i.e. English, Hindi, and the regional language of the State. If it is a Government of India (GOI) app, it should be in English and all official languages (and hosted on the specific language website);
3- Longer term (more than 1 year): Acceptance and processing (sending of EAI L1 level compliance plus creation of mailboxes for email service providers (all IDNs serve the respective languages and scripts – and resolve).

Ultimately, catalyzing the multilingual and inclusive Internet will help bring the next billion users online, of which 500 million in India, and empower the use of local language identities– in particular those that are non-English.

Sarmad Hussain (ICANN) complemented the presentation by T. Santhosh pointing at the global level attention for IDNs, originated around 2010, which started with different country-code Top Level Domains in IDNs. In 2012/2013, ICANN also announced generic top level domain round. This has enabled TLDs to be available in a wide variety of scripts across the world – Indian scripts, but also Chinese, Arabic, Cyrillic etc.

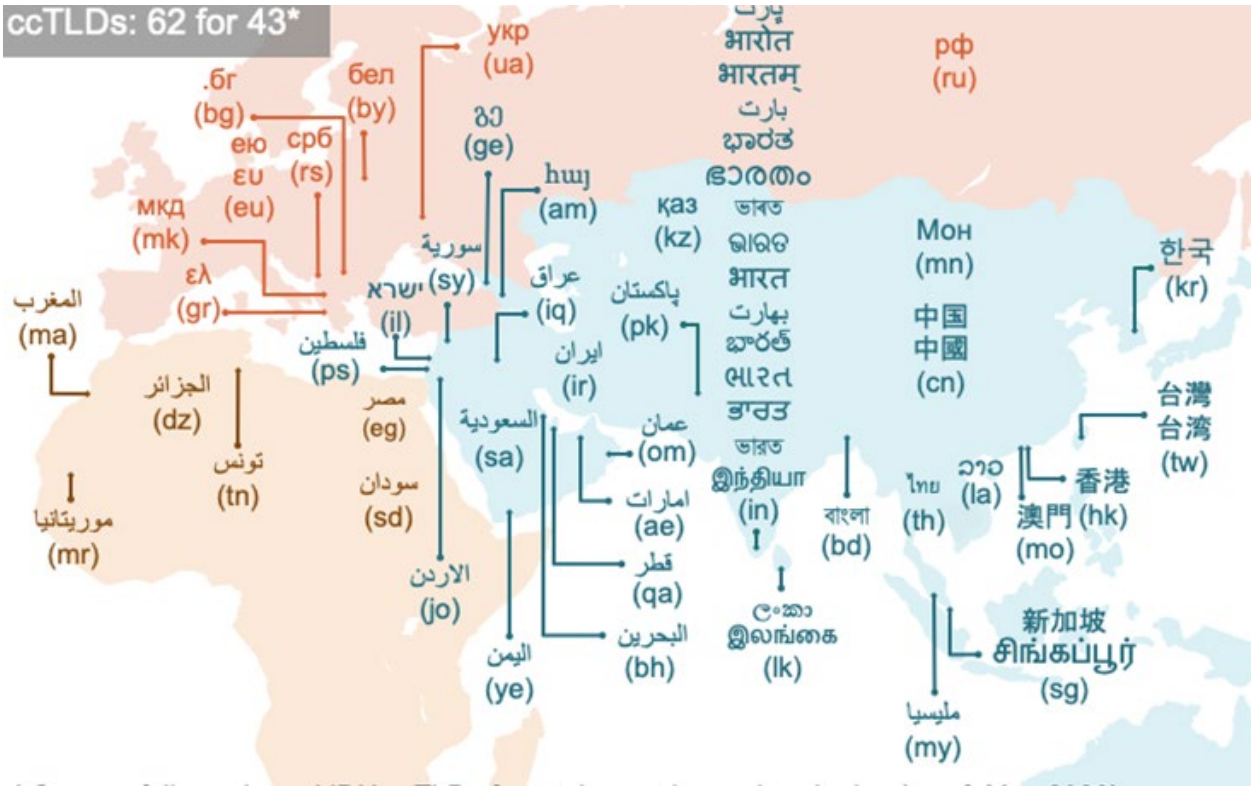

Fig.6 – successfully evaluated IDN ccTLDs (ICANN, as of May 2020)

This has created new opportunities, but also new challenges as the DNS and internet routing were based on 2 or 3 characters behind the dot, and in Latin characters. All systems and software applications need to adapt – and this requires a willingness to invest in current running systems, for which some companies are better prepared than others.

What has been observed is that from the global top 1000 websites, those using internationalized email addresses currently still stand at less than 10%. In India, this is slightly higher, raising to 11 or 12%. Looking in the zone file data in new TLDs, we found more than 35 million MS records that aim at mail servers. When we ping those with Chinese email addresses, about 20% would accept it. Therefore, efforts are progressing, but a lot remains to be done in this area. For further information on this, please see here: UASG039.

Fig.7 – UASG goal is to have all domain names and email addresses work in all software applications.

The UASG has identified multiple stakeholders and invited them to the table to address these issues together. The stakeholders in focus include:

- Technology Enablers: Organizations producing relevant standards and best current practices and providers of software programming languages, tools, and frameworks.
- Technology Developers: Organizations and individuals developing and deploying online applications and services using programming languages, tools, and frameworks.
- Email Software and Service Providers
    - Email Software Providers: Organizations and individuals providing the different applications, tools, and utilities for the email ecosystem.
    - Email Service Providers: Organizations and individuals providing services for the email ecosystem.
    - Email (and System) Administrators: Organizations and individuals deploying and administering email-related software and services.
- Government Policy Makers: Government officials generating demand for UA-ready products and services by updating accessibility standards and procurement processes.
- Academia: University programs offering IT-related degree programs.

The UASG meets on best ways forward: it reviews applications, helps raise awareness, conducts capacity building trainings, and develops tools and code that is made available to all (see for instance: https://uasg.tech/eai-check/). It also actively reaches out to application developers and

email service providers to address the issues found. See for more information www.uasg.net or www.icann.org/ua. ***Ajay Data*** (Chair UASG) also shared a video that explains the issues relating to UA: see here. He insisted that cooperation and coordination are needed to make this work. A Global Universal Acceptance Day will be organized on 16 February 2023 – ~~the~~ GFCE is invited to contribute to this.

Addressing DNS Abuse

Rowena Schoo (PIR, DNS Abuse Institute) explained that PIR and others had set up the Institute to address concerns for DNS abuse inside and outside of the ICANN community. Addressing DNS abuse challenges that are global in nature requires collective solutions. The institute focuses on education, collaboration, and innovation. The institute adopted a very open way of working, and is willing to work with all stakeholders

Two actions have been launched:

1- "Netbeacon": designed to address two problems:
   a. On the side of the sender: aiming at addressing difficulties when reporting abuse. In other words, signaling abuse is one thing, whereas having the technical knowledge to determine what is happening is more complex. Currently, there are no standards for evidence, and no consistent implementation of procedures.
   b. On the side of the registrar: reports of abuse are brutal, often duplicative, unevidenced, not about the domain of the receiver of the complaint or unactionable.

Netbeacon is a free service, easy to use site to report abuse aimed to help improve the quality of reports and reduce barriers to action. It is aimed at registrars that have an obligation to react to abuse. When a report comes in, Netbeacon checks a number of reputation blocklists, and adds that to the complaint that is sent forward to the registrar. Right now, the service is up and running, and according to Rowena, registrars report back that it truly helps to action.

2- Measuring DNS Abuse: as a separate aspect from Netbeacon, this part of the work of the Institute is aimed at helping the industry receive high quality reports. The objectives of these are:
   a. to reduce DNS abuse
   b. Enabling focused conversations and identifying opportunities for reducing abuse.
   c. Both celebrating good practices and identifying weaknesses.

The Measuring is carried out by an independent institute, KOR Labs (University of Grenoble), optimized for accuracy and reliability – thus comparability over time. It is not an attempt to measure all harm across all of the Internet and the focus is on selected harms and their features:

- Prevalence of phishing and malware across the DNS ecosystem (high level statistics);

- Where has mitigation occurred, and how long did it take to mitigate;
- Distinguishes compromised vs. malicious.

The decision to focus initially on phishing and malware only, is because the Institutebelieves that they can get very well-evidenced information. A first monthly interactive report is published (one month behind the measurement). Over time, the Institute aims to become more granular. Rowena calls for everyone to sign up for NetBeacon, and check out the measurement project.

Finally, she recognized that it is hard to agree on the levels of harm inflicted – hence the rigidity in measurement approach to ensure the data are reliable – even if not all may draw the same conclusions from these facts.. The Institute is currently focused on being as accurate as possible. When that leads to a change of methodology, they will consider very much how to represent the different measurements over time. Overall, the Institute is making a useful contribution to a better understanding of part of the issues in this area through its measurement activities.

ICANN services to help fight DNS Abuse

Champika Wijayatunga (ICANN OCTO) introduces Domain Abuse Activity Reporting (DAAR), a measurement tool focused on DNS abuse measurement, and KINDNS, which focuses on best current practices.

Currently, DAAR data helps to report based on all TLDs ICANN has data for, which is all of the gTLD domains, and a few volunteers ccTLD domains (currently 1144 TLDs representing about 215M names). Daily scores are made available to the participating TLDs via the Monitoring System API (MoSAPI), which allows both a global comparison of monthly statistics as well as an individual comparison (for own TLDsonly). Data from the zone file is combined with listings from various vetted “security threat” Reputation Block Lists and includes Spam; Malware distribution; Phishing; and Botnet Command and Control.

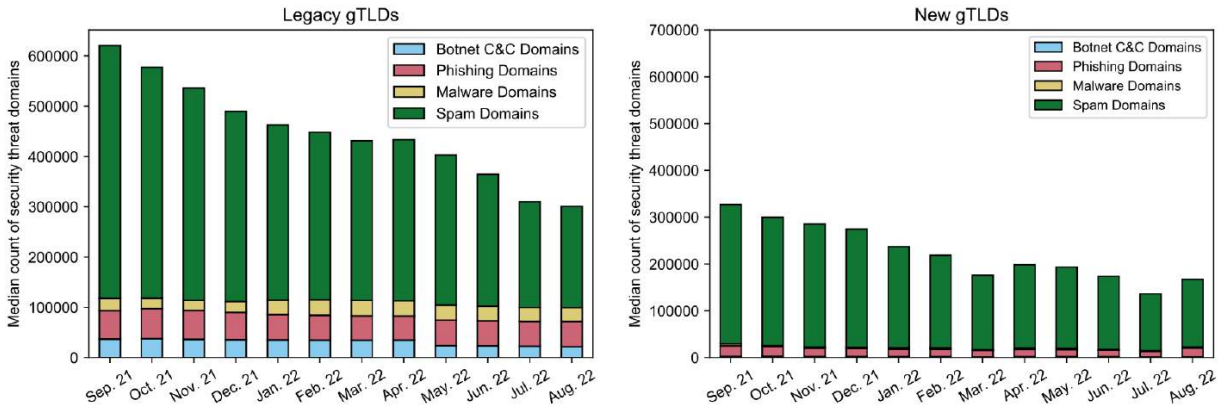

Fig.8 Breakdown of domains identified as security threats across all DAAR threat types over time.

As explained – the DAAR data are primarily based on the gTLD data, as there is a contractual relationship with the gTLDs. However, ccTLDs have also been invited to participate and provide their zone files to the DAAR System, albeit on a voluntary basis.. Every ccTLD that joins the project would be able to receive DAAR data daily via ICANN's Monitoring System API (MoSAPI), as well as the customized monthly individual reports. Currently, the following ccTLDs are participating: .au, .se, .tw, .cl, .nu, .ee, .tz, .gt, .sv, .mw, .gg, .je, .ch, .ke, .in, .ca, .li, .co, .fo, .fr, .pt. More ccTLDs are welcome to use DAAR as a service.

Moreover, KINDNS focuses on sharing good DNS practices. The acronym stands for **K**nowledge-sharing and **I**nstantiating **N**orms for **D**NS (Domain Name System) and **N**aming **S**ecurity. It is an initiative to produce a simple tool that can help a wide variety of DNS operators, from small to large, to follow both the evolution of the DNS protocol and the best practices which the industry identifies for better security and more effective DNS operations.

By joining the KINDNS initiative, DNS Operators are voluntarily committing to adhere to the identified practices and act as “goodwill ambassadors” within the community.

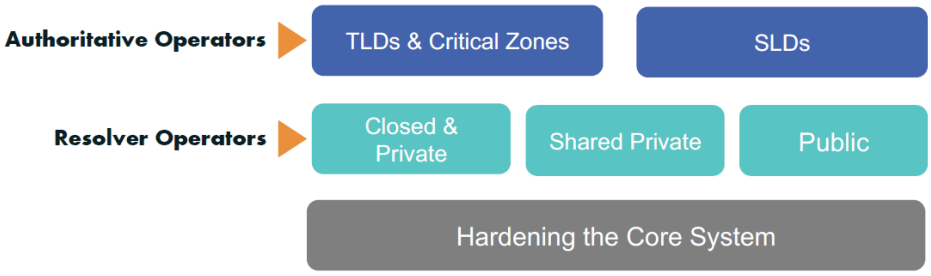

Fig. 9 – KINDNS targeted Operators source: ICANN)

Operators in each category can self-assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices. Self-Assessments will be anonymous, and a report can be directly downloaded from the web site https://www.kindns.org . Operators can enroll to participate in one or multiple categories covered by KINDNS. Participation in KINDNS means voluntarily committing to implementing and adhering to agreed norms and practices, and de facto participants become goodwill ambassadors and promote practices.

In conclusion, KINDNS is a clear contribution to doing things better, together – as does Netbeacon, MANRS, internet.nl and the measurements shared. There are also other examples of community initiatives such as the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), an international network with the aim to reduce botnets, malware, spam, viruses, DoS attacks and other online abuses. The M3AAWG makes best practices documents and abuse information available that could serve as a good resource for local action, and this is next to all CSIRT operations and collaboration around the world. Altogether, it is clear how the industry is

getting more tools and is doing more every day to address the challenges end users are confronted with.

Altogether, DNS abuse exists, even when the identified abuse seems to be declining (spam, botnets) or at least not growing (phishing, malware). Activities coordinated by ICANN and the DNS Abuse Institute help the industry get a feel for where things happen and building capacity and sharing good practice to address issues arising, are important as to ensure we can continue to rely on the DNS in the years to come – with new opportunities, there will always be new potential threats to address – physical world, and online world alike.

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

During this block, conclusions were drawn, and potential actions were developed with the aim of increasing trust in the use of the 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.

Conclusion 1 – Standards matter – incentives are needed to move the needle

Whereas the Internet wasn't built to be safe, originally, and its use moved well beyond the imagination of many of those involved early on, a lot of progress has been made and a number of important measures are now available to ensure the use of the Internet is much safer than it used to be. A combination of the standards also proposed by GFCE Triple-I make a lot of sense. However, it requires an investment of effort, time and money, to upgrade the systems and make use of state-of-the-art standards, in what partly is an industry built on low margins and high turnover.

Conclusion 2 – Incentives are needed to move the needle, as the cost goes before the benefit

It is therefore important that incentives are created for service providers to step up their game and offer state-of-the-art services and do so in a safe and secure way. Different incentives to create and/or be aware of:

1- For those that take the interest of their users at heart: lead the way and offer the best possible service that users are willing to pay for. In order to ensure it is "worth their while" there are ~~two~~ kinds of measures:

a. Helping to make it easy to implement new standards and processes based on good practice experiences (e.g. sharing of code) Global actors such as ICANN, ISOC, and the Regional Internet Registries are active in this by developing and offering code, sharing data, and collecting, validating and sharing best practices;
b. Helping to make end users aware of the value of updated services, thus making it extra attractive for them to use such a service – possibly even against additional costs/higher prices for safer use. Awareness raising campaigns and news messages may help. Also, governments can play a role by leading by example;

2- For those that are "just doing their work": requiring application of safer standards and procedures across the industry. Next to voluntary initiatives, within ICANN and RIRs this can be done by creating policies requiring specific actions. We also see governments stepping up and developing legislation on areas where there are concerns – other governments reach out and work with stakeholders to promote good practice, subsidize awareness activities and development of useful tools, and lead by example by using state-of-the-art standards within government services (and requiring it from their suppliers).

Conclusion 3 – Awareness is Key

In the end, the key is with the users, whether commercial or non-commercial organisations, or individuals. For users to benefit most from the Internet, it is important to know they are safe, and can trust the connections to services offered on the Internet. By making users aware of the risks and measures, users will stand up and ask their suppliers to provide services they can rely upon. Websites like internet.nl and auCheck in Australia help users better understand what the situation is.

We also reviewed actions that were called out during the last GFCE Triple-I workshop in 2019, updated them in the light of recent developments.

PROPOSED ACTION 2019: *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.

UPDATE 2022: Anurag Bhatia has developed such a tracker, and this one is now available from his website https://rpki.anuragbhatia.com. Anurag calls for volunteers to help progress this further. Next to this, internet.nl is offering code to measure application of RPKI/ROA to specific websites.

PROPOSED ACTION 2019: *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.

PROPOSED ACTION 2022: work towards deployment of the compliance testing tool in India. following the presentations from Dennis Baaten and Bart Hogeveen, the interest for a local version gets reconfirmed. However, taking into account this does require a real effort, there is no volunteers to lead on this. Participants do promise to explore how this can be progressed.

PROPOSED ACTION 2019: *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.

PROPOSED ACTION 2022: following the presentations and discussions during the day, Amitabh Singhal volunteered to take the lead and develop an Action Plan for Raising Awareness of Security Standards for the purpose of enhancing justified trust in the use of the Internet in the region.

Recognizing that policy and legal measures already exist, he suggests to take the following steps:

1- Bring all stakeholders on a common platform;
2- Initiate & Ramp up Conversations and Awareness;
3- Maintain & operate the Common Platform;
4- Setting up an Indian platform for checking on the state of protection of websites and mail servers, and advising & implementing security protocols, wherever found missing;
5- Conduct regular Online and Offline campaigns - Build a Roadmap with Yearly Plans, programs & tasks.

Anand Raje and Satish Babu volunteered to work with Amitabh towards further developing the Action Plan (For current outline see Annex I to this report). They will reach out to potential contributors and look forward to connecting to others that are willing to help make this happen. Please contact Amitabh Singhal when you or your organization wants to help.

For more information about GFCE Triple-I, including results of earlier events, please check out the GFCE website. Contact Maarten Botterman if you have specific questions about GFCE Triple-I, and if you are interested in improving the trusted Internet experience in your region.

Annex I – Initial Terms of Reference for an Action Plan for Raising Awareness on Security Standards (RPKI, DANES, TLS, STARTTLS, DMARC, DNSSEC, MANRS, etc.)

Based on the discussions, a number of people are planning to take forward an awareness raising activity, both informing stakeholders about the need to adopt security standards and providing assistance in doing so, effectively. An initial plan will be developed and (co-)funding will be sought. Contributions are welcome.

Initiator/coordinator: Amitabh Singhal

A. Trust Issue runs Deep:

(i) Cybercrime victim India among top five victims of cybercrime: FBI report
May 30, 2022 - Updated 08:24 pm IST…Among the complaints received, ransomware, business e-mail compromise schemes, and the criminal use of cryptocurrency were among the top incidents reported (BusinessLine News Report).

(ii) Phishing/Vishing/ Smishing/Pharming was the top crime type with 323,972 reports received in 2021. It was followed by Non-Payment/Non-Delivery, Personal Data Breach, Identity Theft and Extortion with 82,478, 51,829, 51,629 and 39,360 reports received, respectively (Hindu Businessline Report).

(iii) 5 of the top cybercrimes affecting businesses and individuals in 2022:

- Phishing Scams.
- Website Spoofing.
- Ransomware.
- Malware.
- IoT Hacking

(iv) 87% of Organizations suffer DNS Attacks: Zero-day attack. The attacker exploits a previously unknown vulnerability in the DNS protocol stack or DNS server software.

- Cache poisoning. ...
- Denial of service (DOS). ...
- Distributed Denial of Service (DDoS). ...
- DNS amplification. ...
- Fast-flux DNS.

B. Need for Safer Internet is a necessity - Potential STEPS

1. Bringing all stakeholders on a common platform;
2. Initiating & Ramping up Conversations and Awareness;
3. Maintaining & operating the Common Platform;

4. Setting up an Indian platform for checking on the state of protection of websites and mailservers, and advising & implementing security protocols, wherever found missing;
5. Regular Online and Offline campaigns - Build a Roadmap with Yearly Plans, programs & tasks.

C. Some Operational Methods:

1. Live Measure, Monitor, Analyze traffic and Develop Database of Breaches/Incidents (e.g. use and further develop Platforms like AIORI, etc.);
2. Investigate & Pinpoint the security gaps - technical/human;
3. Provide an online platform that stakeholders can use to check the state of protection;
4. Recommend Appropriate Steps to concerned stakeholders (operators, pvt/public orgs,

D. Policy & Legal Measures Exists:

India already has policies and laws to recognise and report breaches

1. Harmonization between current policies/laws and actual practices needed.
2. Propagate voluntary Enforcement of mitigating actions/ramping up security protocols or via regulatory actions where/if needed.

E. Stakeholders:

1. Telecom Operators
2. ISPs
3. Data Center/Cloud Service providers
4. E-Commerce Platforms - Both govt and private sector
5. Domain Registries & Registrars/DNS Service providers
6. CDN operators
7. Govt, Public sector and private Enterprises
8. LEA entities at both Central and State levels
9. Security/threat mitigation service providers
10. Central Govt and State Govt Ministries and Departments (MeITY, CERT-IN, Deptt of Telecom, State TERM Cells), etc.
11. IXP operators
12. Any other

ANNEX II – Workshop Agenda

GFCE Tiple-I Workshop

25 September 2022, International Institute of Information Technology, Hyderabad, India

Time (IST)	Session	Speakers
10:00-10:30	Opening Session	Welcome: Satish Babu, inSIG2022
	Inaugural Address:	Alkesh Kumar Sharma, Secretary, MeitY, Govt of India
	Introduction and moderation: Maarten Botterman, GFCE Triple-I	
Part 1: Internet Standards		
10:30-12:30	DNSSEC, DANE	Champika Wijayatunga, ICANN OCTO
	RPKI/ROA	Anurag Bhatia, Hurricane Electric
	IPv6	Sunny Chendi, APNIC
	DMARC/DKIM	Bart Hogeveen, ASPI
	The online platform to support standards implementation Bart Hogeveen, ASPI	
	Dutch Platform Internet standards Dennis Baaten, Internet.nl	
	Open Q&A	
12:30-14:00 Lunch break		
Part 2A: Internet Hygiene		
14:00-15:00	The importance of cyber hygiene and resilience when going online	Merike Kaeo, Double Shot Security, Estonia
	MANRS	Ram Krishna Pariyar, ISOC
	India's Multilingual Internet Initiative T. Santhosh, Govt of India	
	Universal Acceptance Sarmad Hussain, ICANN, and Ajay Data, UASG	
Part 2B: Good Practices and Success Stories		
15:00-16:00	DNS Abuse	Rowena Schoo, DNS Abuse Institute
	DAAR, KINDNS	Champika Wijayatunga, ICANN OCTO
Part 3: Towards Action Items		
16:00	Moderator: Maarten Botterman, GFCE Triple-I	
17:50	Close of Session/Vote of Thanks InSIG	