CENTR Tech Trends Watch

June 2021

The Tech Trends Watch is a part of CENTR's reporting on current affairs which takes into account ongoing trends in technology development from a range of standards development organisations and other technology forums. Its purpose is to trace out those trends that may have an impact on the addressing and numbering communities, and assess how those developments tie in with external stakeholders such as policy-makers and other industry sectors.

Economic incentives will bring the current generation security standards in deployment

With increasing regulatory focus on information security and cybersecurity facing registries, it is no wonder that a number of projects have emerged that aim to map the current state of security standard deployment and incentivise future deployments.

The CENTR Security Maturity Model is one self-assessment tool that can help registries establish where to focus their efforts. CENTR member SIDN has also made a more generic security maturity model for actors beyond registries that may or may not be implementing state of the art security standards.

Discussions on how to advance standards like DNSSEC, Registry Lock or the registration data access protocol (RDAP) are old in the domain name sector. Many of the standards are not new in spirit so much as in practical experience, and this was the focus of a recent CENTR IETF report.

Ulrich Wisser from the Swedish Internet Foundation explains how his registry tried to incentivise registrars to offer DNSSEC to customers by subsidising DNSSEC-enabled domains: "*The Swedish Internet Foundation places incentives to drive change. Our registrars, which are also the biggest hosting companies, get a 5% cost reduction for signed domains. This isn't much per domain (approximately €0.60), but if you sign 100k domains, it starts to add up*". The incentives caused an uptick in deployment and is now also leading to the development of better automated tools (see interview). More recently, Ulrich Wisser has also progressed with similar work on automated registry lock deployment in the ICANN ROW working group.

At least some of the open questions that are not yet ready for technical standardisation have been addressed by a CENTR effort to consolidate some of the existing models for registry lock [4]. This is especially helpful for registrars that have many different registries in their customer base, but arguably further work on implementation both of standardised models and automated tools is needed.

With automated tools for the implementation, deployment and management of mature internet security standards, better conditions have also been put in place for cooperation around putting the tools in operation. This may be an opportunity for the European internet to grow stronger around existing organisations, while increasing security and cross-border cooperation at the same time.

Next major revision of ISO27001 due in 2023

ISO27001 is one of the most commonly used information security standards in the world. Maintained by the Joint Technical Committee (JTC) 1/Standing Committee (SC) 27 at the International Standards Organisation (ISO), it lives through ten-year cycles with mid-term reviews (the last one occurring in 2017). It is also a formal standard, one that governments around the world can refer to when complying with international trade agreements and other obligations under for instance World Trade Organisation (WTO) treaties.

Preliminary work to revise the standard are already underway. Online reports suggest that the revised version will place a stronger emphasis on technical security than has so far been the case (the current version instead specifies organisational procedures, controls and risk assessments that an organisation should undertake to determine its need for technical security).

For registries, the thing to look out for is obligations on source code audits, electronic identification requirements and data integrity protection. Especially for data integrity protection, one might wonder if technologies like DNSSEC – that help secure the bond between a registrant and their domain name – would, or should, not become mandatory for future ISO27001 compliance.

A unique and global network?

Locally deployed internet standards are a new reality – every network does not need to be attached to a global and unique internet, but many of the fundamental principles of networking upon which the global and unique internet still apply. In issues ranging from the secure management of IoT devices, to security concerns and content moderation there are clear benefits from specialised networks, where actors like ccTLDs are increasingly stepping up to act as trust anchors.

For most people around the world, people experience at least some aspects of the world wide web and the internet in a similar way regardless of where they are based. The same websites are accessible, with the same domain names mapping server addresses to human language, and the same content delivery networks and undersea cables connect everything into a big whole. Technically speaking, the conversion of an internet protocol (IP) address into a domain name or the reverse, the existence of digitalised transactions and access to large numbers of websites through a web browser all work the same even when the content differs.

This is, however, not a given. Internet technologies work the same whether lots of small networks are interconnected or whether they are operating independently of one another. Indeed, for many security critical operations in internet of things, manufacturing or government affairs, isolated networks have long been preferred.

The splitting of smaller networks from the larger network is not without political and economic controversy. One negative example may be the Great Chinese Firewall, a system of technical measures designed to tailor the web and app experience of China-based individuals to the current political preferences of the government. These systems are exported to governments that want to preserve domestic political and societal conditions. They interfere with the technical function of the internet, but they also serve to isolate the countries where they are deployed from global markets, commerce and cultural exchange.

Security and sovereignty efforts, such as a recent Russian internet security law that mandates a sort of national whitelist of domain names and French attempts to solve economic grievances through liability with particularly large American websites, are feared to create similar effects. In these cases, reducing the amount

of inter-networking on the internet isolates populations from one another based on geographical origin (people living inside a country's border, for instance) rather than biographical activity (people manufacturing post-it notes, cars or preparation of regulatory decisions).

Larger reliance on wireless connectivity, whether through mobile networks or wireless local area networks (WiFi), has spurred even greater acceleration into localised network innovation. Reducing latency, increasing bandwidth and dealing with the more haphazard nature of wireless transmissions (such as packet forwarding errors due to reflections, interference or other causes) incentivises a sharp re-analysis of the core of the internet. The internet or transport control protocols, or a number of specialised protocols targeting specific communications such as security patch management, are no longer beyond reproach.

Innovations in this field can be vendor specific, or at least implemented by relatively few vendors, or brought as international standards projects. See previous text on New IP in CENTR Tech Trends 2. In any case, it is clear that we seem to be heading for a future with more localised networks, that are wireless, and that only partially re-use the technology standards that made the internet a successful, global technology.

The question seems to be which core features of the global internet will be brought into the local, specialised networks – and one contender is domain name registration standards.

For many countries around the world, a locally governed ccTLD may be the best and most reliable way of provisioning trustworthy identities to devices, both in industry, government and individual households. With a globally consolidating telecommunications sector, where only a few international corporations supply mobile network equipment and provide access services, confidence and security needs to be added from the top, by an actor sufficiently well-placed to do so. As previously mentioned by CENTR Tech Trends 1, at least two CENTR registries are already working on ways of managing internet of things devices with domain name registration technologies.

This is an opportunity not just for ccTLDs, but also for each of their respective countries and governments.

Tell us what you think!