TOWARDS A SAFER INTERNET

In this briefing article, ICANN's **RICHARD LAMB** describes the technical moves to plug a longstanding security gap in the internet's 'phonebook'

There is no doubt information and communication technologies (ICT) have had a transformative effect on society. In addition to the democratising effect that has helped improve political and financial wellbeing, they have led to new approaches to business, innovation and the exchange of ideas across borders. The internet continues to provide new opportunities to improve the lives for the 3 billion or more people in the world who use it.[1]

Unfortunately, lack of security lurks behind the internet's engine of progress. The internet itself has an architecture that dates back to the 1970s[2] and assumes trust. In addition, lack of adequate regulation and cooperation (e.g. cross jurisdictional agreements to capture cyber criminals) impacts security.

For the many of us increasingly involved in fostering the internet as a safe platform, it is important to understand the layers and structures at which the internet can be 'secured'. In this article, I focus on infrastructure and less on governance. Many of the governance issues are fundamentally difficult to solve and have very long horizons. The lightweight regulatory regimes that most governments of the world have imposed on the internet already recognises the need to step carefully so as not to thwart what has made the internet a success.

This measured, long-term approach to policy and regulation for the internet remains appropriate today. However, recently at the operational, technical level there has been a fundamental improvement to the internet's architecture which has been endorsed by many governments,[3] and which can help stem the tide of abuse.

This is Domain Name System Security Extensions (DNSSEC), a mechanism to secure the internet's master phonebook – the Domain Name System (DNS), which has not changed since 1983. Often relegated to obscure technical discussions, DNSSEC has enjoyed brisk deployment and can act as a basis for securing communication across the internet.

BACKDROP

The internet was created over 30 years ago as part of an experiment on an alternative approach to communication. It sought to share physical infrastructure instead of dedicating it to conversation as a traditional phone service does. The theory was that by having multiple possible pathways over which bits of a conversation could travel, the end result would be more reliable and resilient since these bits could be rerouted on the fly around bad links. This concept of shared resources remains at the heart of the internet. It is the reason for both its success and its problems.

The early stages of this experiment involved a small group from government and academia who knew each other. Abuse was not a concern, which resulted in an open door policy for anyone associated with the work. (In college, I remember walking up to a terminal and trying to login – it simply asked me if I wanted an account and gave me one.) It was in this environment that the internet began its growth.

As it reached a wider audience, due to its underlying principles of openness, sharing, and freedom to innovate, new protocols and services were developed to run on top of this network, interconnecting other networks. In 1983, one of the very first services deployed on the internet to manage its growth was a 'phonebook', the DNS.[4]

Every machine on the internet has a numeric address. DNS is a database that allows the association of names to those internet protocol (IP)

addresses. This made it easier for people to refer to various machines when connecting to them. DNS lookups, as well as most transactions on the internet, were then made in the clear with little and no protection.

Fast forward to today's internet, where there are in excess of 3 billion users who do not know each other, and transactions are much more than just academic. The internet's infrastructure still relies on many of the same early stage protocols and services to function. Certain aspects of the infrastructure have been greatly improved, such as speed and accessibility. An example is an expansion of the addressing protocol. The explosion of the number of devices and their addressing needs is being handled with the rollout of IP version 6 (IPv6). Deployment has been steady; the original protocol, IPv4, contained 4 part numerical addresses and we simply ran out of unique addresses.

But the fundamental protocols built when trust could be assumed have not changed.

From the perspective of the average consumer, the explosion of the internet has meant vastly improved communication and convenience. For industry, the internet has provided an effective/efficient path for delivering goods and services and to target audiences, thereby increasing revenue. For both groups, securing the communication path is critical whether it be for a website, email, or an application on a mobile phone. Without a trustworthy path, confidence in the results deteriorates, resulting in consumers leaving and businesses suffering.

On the internet the first step in establishing communications is the DNS. It correlates the IP address (numbers) of the machine where a particular site is located (hosted) to the web address. For example, DNS converts www.google.com to 172.217.6.68. By nature of being one of the first services on the internet (referred to by some as the first cloud service), it is part of the internet's core infrastructure and therefore available everywhere at the furthest reaches. Recent improvements not only secure the DNS but offer a foundation to develop solutions to provide a trustworthy path within the internet.

THE DOMAIN NAME SYSTEM

The DNS was deployed to make it easier for people to identify machines on the internet. It does so by implementing a distributed database made up of files with each line associating a name to a machine IP address – much like what its predecessor, the 'host table', did.[5] However, to allow the system to scale, the DNS broke up the lookup process by sharing responsibility across multiple machines and organisations. For example, in looking up the IP address for www.google.com, the DNS would first get the IP address for the server responsible for com, then get from that server the address for the server responsible for google.com then get from that server the IP address for www.google.com.

The very first lookup for com servers is made to what are referred to as the internet's root servers. These are co-managed by the Internet Corporation for Assigned Names and Numbers (ICANN) and an international group of voluntary root server operators. Whether it be com or se for Sweden or post for the Universal Postal Union, the first stop for DNS is the root servers. Due to their role in the DNS, much interest has surrounded 'the root', so it is important to note that on the internet use of these specific root servers, or any other servers for that matter, is voluntary and only driven by choice and/or convention.

> **With the urgency to fix the DNS, DNSSEC deployment on the internet's core infrastructure went into top gear.**

In this example, the server for com is operated by Verisign (whose role is referred to as a registry). Were it www.google.se, se servers are operated by a Swedish company, IIS, under the auspices of the Swedish government. Finally the google.com servers are operated by Google and know which machine names are associated with which IP addresses inside Google.

To accelerate the speed, this chain of lookups is not done every time, but instead the result is stored in a nearby server's memory (cache) for a time so that responses are immediate. ISPs typically operate such caching servers[6] so that all their customers can benefit from the increased speed.

The critical reliance on the DNS as an identity and authentication mechanism, be it identifying a website (e.g. www.mybank.com) or identifying users (e.g. myname@mybank.com), gives one pause when contemplating that this system has not been upgraded since the trusted days of the internet decades ago. It is a testament to its creators that the basic design scaled so well, but the weight of trust placed on this humble phonebook has recently shown signs of wear. Researchers have highlighted the ease in which results from the DNS can be faked,[7] leading to impersonation or hijack, thus breaking the trust between consumer and service.

ENTER DNSSEC

In the DNS the data lookups and responses are made in the clear, i.e. are visible to anyone who can tap into any part of the path taken by your request. Since the information in the DNS is by definition, public, this openness is by design. However, since a properly placed attacker could see or guess what you are asking for, they could respond and direct you to their website. It could be, for example, a web server with deceptive content that asks for your bank username and password. The attack is amplified to cover all customers of, say an ISP, by targeting their caching servers (which would remember the forged response). Now all their customers could be hijacked. This is called cache poisoning, or spoofing.[8]

The possibility of malicious DNS responses was recognised in about 1995.[9] At that time though, other parameters in the DNS request/response transaction, such as matching request and response ID numbers, sufficed to make it difficult to carry out this type of attack.

Fast forward to 2008. A security researcher named Dan Kaminsky published a way to lie to the DNS and poison the cache that took only hours. Faster internet and computer speeds made it easy to trigger DNS requests for which an acceptable fake response could be created. Given the ever critical role the DNS plays, this became big news for the press, industry and governments.

Fortunately, by 2008 new protocols to protect the DNS – called DNS security extensions or DNSSEC – had been developed[10] and nascent efforts to deploy it were underway.[11] With the urgency to fix the DNS, thanks to Dan Kaminsky, DNSSEC deployment on the internet's core infrastructure went into top gear. The hierarchical shared nature of the DNS meant that each organisation responsible for each level of the DNS (e.g. root, com) had to deploy DNSSEC, starting with the root.

HOW DNSSEC WORKS – AND THE 'ROLLOVER'

DNSSEC is an extension to the DNS that adds cryptographic material alongside existing DNS records. It does not encrypt DNS data. It simply provides a way to verify (using digital signatures) that the data received has not been modified from its original source. Verification is typically done by the ISP's caching server or ideally on the end-user's computer for true end-to-end security.

Each organisation responsible for a level in the DNS hierarchy vouches for the identity of the next level below it. They do so using cryptography to digitally sign key material from the next level below, e.g. root signs keys from com and publishes them in the DNS; com signs keys from google.com and publishes them in the DNS; google signs keys used to sign www.google.com and publishes them in the DNS.

This creates a chain of trust for domain names protected by DNSSEC that can be verified by any caching server around the world. Even the slightest modification of the DNS response along the way will be detected. Furthermore since each key is verified by the one in the level above it, only the top root key is needed to validate the whole chain. In IT parlance, this forms a global public key infrastructure.[16]

DNSSEC is enjoying healthy deployment, so why mess with this nascent technology by changing the root key on which it relies? Two reasons: cryptographic hygiene and practice, practice, practice. Although the estimated time it might take to break the cryptography (and key length) used for the deployment of DNSSEC is in the tens of years, in the field of cryptography new vulnerability discoveries can occur any time – some published, some in the works. Therefore, a regular practice of generating a new key and rolling over to it is good practice in protecting against possible compromise. Similarly, should there be a compromise, it is critical that IT staff be familiar with emergency recovery/rollover procedures and that those procedures be tested. An emergency is not the time to learn how to change a compromised key.

It has been 7 years since the root key was generated and put into service and is now time to address these two reasons with a 'key roll'. The rollover process was carefully developed over several years by internet/DNS experts.

The current rollover process started in late 2016 with the generation of a new key. The old key will be swapped out on 11 October 2017 0000 UTC. There will be delay before any effects are felt due to memory in the caching servers.[17] Notifications of the event have been communicated widely in relevant forums, and through interactive discussions. Most systems and large operators have automated or manual processes in place already to track the rollover so ICANN and DNS experts expect no problems.

However, since this is a first time, ICANN and DNS experts will be watching the effects of this rollover closely and are ready with backup plans if required. For the end user, and hopeful engineers involved with this process, this should be a sleeper. Its anticipated success should further solidify DNSSEC as a security solution that we can all build on and benefit from.

The root was 'signed' in 2010 by ICANN and its keys are managed with international involvement and certified with annual audits;[12] 90% of the approximately 1,500 top level domains (e.g. com, se, post) have DNSSEC deployed on them.[13] Lessons from early deployments have helped to mature operations. The key used for the root is even being updated (rolled) – see box.

So the DNS is fixed and we are done – right? There's more. The DNS is not relegated to only providing IP addresses for names. It also can and does handle many other record types such as those for figuring out what machine to send email to. With DNSSEC it is now possible to cryptographically guarantee that what is published in the DNS is what everyone gets out, unmodified, globally, on every device. A by-product of securing the DNS is a global database for the secure distribution of much more than IP addresses.

For example, if I create a record with my public email key for myname@example.com in the DNS under example.com which was protected by DNSSEC, anyone in the world could look up and cryptographically verify my key and use it to send encrypted email that arrives in my mailbox without being subject to eavesdropping or modification by intermediate systems or networks.[14] Such applications for DNSSEC are already being developed and for those entrepreneurs who see these opportunities, DNSSEC doesn't just fix current issues with DNS, but provides a platform for new security products.[15]

CONCLUSION: MORE NEEDED

The internet has matured and along with it so has abuse. Built in a time of trust, new tools are now needed to combat this abuse, while allowing for adaptive and measured policy and regulatory frameworks to develop that will continue to provide a frictionless environment for the benefits of the internet-driven economy and society to develop further.

DNSSEC is a step forward in upgrading the core infrastructure of the internet to reinforce trust with cryptography and has enjoyed steady deployment and the flow of innovative ideas to secure other parts of the internet based on DNSSEC has just begun.

However, we need to do more. Without wider deployment onto popular services, the advantage now and in the future of a secured DNS will not be realised. Readers from a government or network operator who have not yet embraced DNSSEC as an important pillar in securing their cyber infrastructure should investigate and drive its implementation soonest. And if your network already implements DNSSEC, you need to make sure it is ready for the rollover.

It is the hope that thought leaders will help raise awareness to take advantage of the opportunities DNSSEC presents and beyond, contribute to the spread of a culture of information and data security so that we can continue to make the most of the internet for good.

RICHARD LAMB *is a member of ICANN's security team and has over 35 years of internet experience as engineer, entrepreneur and policy expert. He was the technical and policy architect for ICANN's root DNSSEC deployment. Prior to ICANN, he was director of global IT policy at the US Department of State.*

REFERENCES **1** See: internetworldstats.com/stats.htm **2** Internet Society (1997). Brief history of the internet. bit.ly/1hJiXRS **3** As evidenced by committed country level deployment. See bit.ly/2xPI4Br **4** IETF. Domain names – concepts and facilities. tools.ietf.org/html/rfc882 **5** See: en.wikipedia.org/wiki/Hosts_(file) **6** See: bit.ly/2wGN4n1 **7** Dan Kaminsky – flaw in DNS. bit.ly/2fiXJ4J **8** See: en.wikipedia.org/wiki/DNS_spoofing **9** Bellovin SM. Using the domain name system for system break-ins. bit.ly/2ydtm3s **10** See: ietf.org/rfc/rfc4033.txt **11** SE/Sweden and a few other registries had deployed DNSSEC by 2008. **12** The key management facility of the root zone DNSSEC key signing key (KSK). See slides at: bit.ly/2fAtljh **13** DNSSEC deployment report. rick.eng.br/dnssecstat **14** Public key email support is built into most popular email clients. Here is one example: www.akadia.com/services/email_security.html **15** How DANE strengthens security for TLS, S/MIME and other applications. bit.ly/2w60XtG **16** See: en.wikipedia.org/wiki/Public_key_infrastructure **17** Root zone KSK rollover. go.icann.org/2fz2fJ9