http://doi.org/10.17576/apjitm-2022-1101-03
Asia-Pacific Journal of Information Technology and Multimedia
Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik
Vol. 11 No. 1, June 2022: 26 - 38

Received: 10 July 2021
Accepted: 29 November 2021
Published: 30 June 2022

THE IMPLEMENTATION STRATEGY OF DNSSEC IN STRENGTHENING DIGITAL GOVERNMENT SECURITY IN MALAYSIA

AHMAD SYUKRI ABDULLAH
SITI HANOM MARJUNI
MASTURA MUKHTAR

ABSTRACT

DNS is a well-known and important protocol on the Internet. Its main function is to translate domain names and Internet protocol addresses to allow users to access the Internet. However, it was created without consideration of security factors. Due to the vulnerabilities found in the DNS, it is often the main target of hackers for carrying out DNS spoofing attacks. To overcome this problem, DNSSEC is introduced. DNSSEC uses cryptographic public keys to create digital signatures in DNS and provides the origin authority, data integrity, and authenticated denial of existence. Therefore, in order to improve the security features of the domain in Malaysia, the implementation of DNSSEC is first performed on the domains of the Government of Malaysia. In this paper, we describe the DNSSEC implementation strategy which was performed on the Malaysian Government's domains under the administration of MAMPU. This DNSSEC process took almost a year to implement and it involved a total of 439 domains. With the implementation of DNSSEC on the .gov.my domain names, the level of security is enhanced, and it brings a significant impact on the digital transformation and digital transactions that are provided by the Government of Malaysia to its people.

Keywords: DNS, DNSSEC, DNS security, network security

INTRODUCTION

Optimising shared services and strengthening cyber security are one of the strategic thrusts in the aspirations of the Digital Government in Malaysia. This thrust focuses on efforts to improve cybersecurity to ensure a secure and reliable service access environment to protect personal data and information privacy (MAMPU, 2016).

In strengthening the public sector cyber security towards a safe and reliable environment, the Domain Name System (DNS) governance should be given priority to minimise the impact and effect of cyber-attack threats. DNS is a standard mechanism for translating domain names and Internet Protocol addresses. It is a key component of the critical infrastructure of the internet and its function is very important to enable users to access the internet network. However, the DNS is designed for the availability of internet network access with no consideration of security (Antić, 2014). It has no authentication mechanism and is often the main target of internet attacks by cyber criminals (Southam, 2014) especially DNS cache poisoning attacks (Kaminsky, 2008; Antić, 2014).

To improve the security of the DNS server, Domain Name System Security Extensions (DNSSEC) have been introduced. DNSSEC uses cryptographic public keys to create digital signatures in DNS (Arends *et al.*, 2005). Although the DNSSEC standard was introduced in 2005, its implementation is still not comprehensive either in the government or private environment. This article presents the implementation of DNSSEC on the domains of the Government of Malaysia as a secure Digital Government initiative to support the national digital economy in increasing public confidence in the services provided by the Government.

BACKGROUND

The DNS was created in the 1980s to make the Internet more accessible. It is frequently referred to as a telephone directory that translates the domain name to an IP address, thus allowing the browser to access the Internet resources. However, the main vulnerability in DNS is security (Kim and Reeves, 2020). Since DNS does not provide any mechanism for verifying the correct translation of IP addresses, DNS can be manipulated or intercepted by attackers. This can result in users receiving misleading information. The discovery of this vulnerability was revealed by Chad R Dougherty (2008) who asserted that existing DNS protocols could cause DNS cache poisoning attacks. DNS cache poisoning or also known as DNS spoofing is an attack technique that can result in the network traffic being diverted to another computer and returning the wrong IP address (Roopam and Sharma, 2014; Dissanayake, 2018).

DNS spoofing is a type of cyber-attack that exploits vulnerabilities found on DNS servers by intercepting and redirecting communication paths from legitimate servers to fake servers. Without realising, users are redirected to fake websites that allow attackers to spread malware, steal user information and so on. Usually, attackers use the Man-In-The-Middle (MITM) technique to create DNS spoofing attacks. The attack process of DNS spoofing can be summarised into the following steps: (1) the attacker injects a fake DNS entry into the DNS server; (2) the user issues request to the real website from the DNS server; and (3) the DNS server resolves the user's request to fake websites. Unfortunately, users who are affected by such attacks would be redirected to fake websites and they might be tricked into giving up their user credentials such as usernames and passwords. Figure 1 shows how an attacker exploits DNS spoofing.

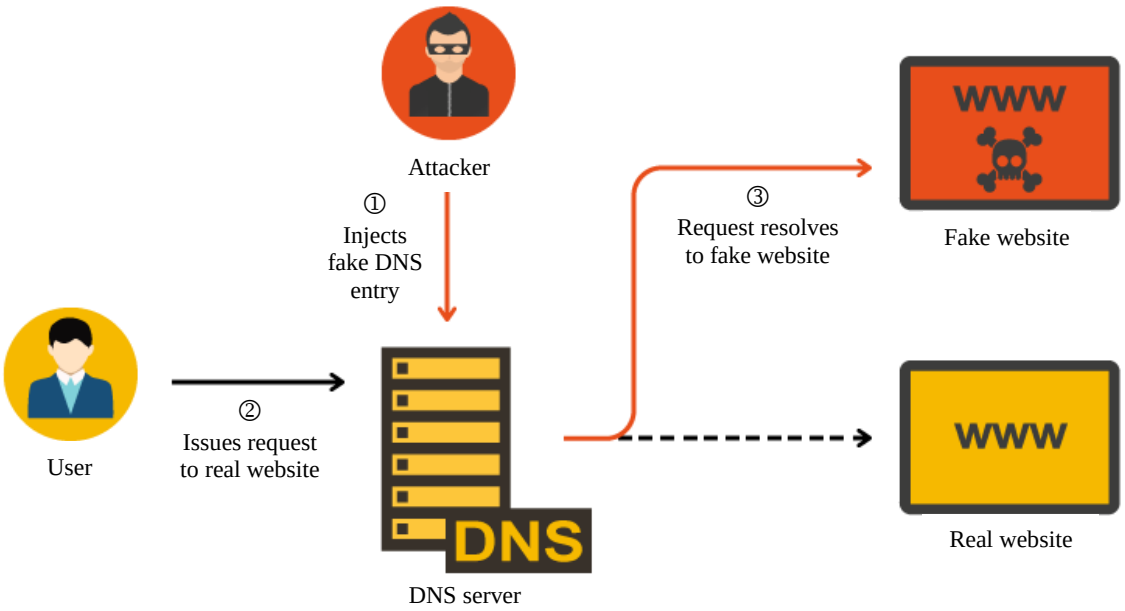

FIGURE 1: DNS spoofing example (*DNSSEC*, 2021).

DNSSEC was therefore created to protect against DNS security threats such as MITM and DNS spoofing. Despite its effectiveness, many organisations have not yet adopted DNSSEC because it is challenging to establish and manage the life cycle of domains. As of October 10, 2021, the average percentage of DNSSEC validation worldwide is 26.90% (APNIC, 2021). Chung (2017) in his research mentioned that the rate of DNSSEC deployment is still low. He concluded that the low rate is caused by (1) users' lack of awareness of DNS

vulnerabilities; (2) the lack of support from domain name registrars to deploy DNSSEC; and (3) users having to pay a higher price as a premium package to get DNSSEC support. In fact, DNSSEC support from domain registrars is quite low (Chung *et al.*, 2017). They revealed three possible reasons: (1) their customers believed that DNSSEC will cause problems in domain name resolution for endpoints that do not support DNSSEC; (2) DNSSEC is an optional service and to enable it, customers have to pay for the service; and (3) requests for records in DNSSEC domains may take longer to resolve due to DNS resolution performance.

RELATED CASE STUDY

Attacks on DNS are nothing new, but they are common. To give an idea of how this attack occurs in the real world, some of the most well-known DNS attacks to date are described below.

MALAYSIA AIRLINES

On January 26, 2015, the official website of Malaysia Airlines (MAS) was hacked by a group calling themselves the "Cyber Caliphate". On the morning of that date, users browsing www.malaysiaairlines.com were directed to a website displaying a MAS Airbus A380 aircraft with the message "404 - Plane Not Found" and "Hacked by Cyber Caliphate". Later, the MAS website was once again hacked and this time a picture of a lizard wearing a hat, tuxedo, monocle and smoking a pipe cigarette was featured with the message "Hacked by Lizard Squad – Official Cyber Caliphate".

MAS confirmed that its DNS had been compromised causing users to be redirected to the hacker's websites; however, the MAS database was not affected (Avineshwaran, 2015; Harjani, 2015; Raghuvanshi, Purnell and Ng, 2015). The airline resolved the issue with its service provider and the system became fully operational again within 22 hours (Avineshwaran, 2015; Hamzah and Carsten, 2015).

BRAZILIAN ISP

A series of major DNS poisoning attack was launched in early November 2011 against several Brazilian Internet Service Providers (ISPs). When users tried to access websites such as Google, YouTube, Gmail, Facebook, Hotmail and other popular global and local websites, a pop-up message appeared telling the users to download and install the supposed "Google Defence" software required to use the websites (Constantin, 2011; Fisher, 2011; Zorz, 2011). Unfortunately, Kaspersky's heuristic engine had identified this file as a Trojan banker and several malicious files and exploits were hosted on the same IP address, targeting users from Brazil exclusively (Assolini, 2011).

Kaspersky's global research director, Dmitry Bestuzhev, claimed that this type of attack may occur anywhere in the world and is mostly caused by vulnerabilities on the part of the ISP, and that more attacks like this will be seen in the future (Constantin, 2011). He added that implementing DNSSEC which is a security extension that uses digital signatures to verify the validity of DNS responses is a solution to DNS poisoning attacks and that all ISPs should implement it (Constantin, 2011; Kovacs, 2015).

AMAZON WEB SERVICES

A DNS spoofing attack against Amazon's web service on April 24, 2018, had resulted in users accessing the MyEtherWallet website being diverted to a phishing site. Amazon's cloud DNS service known as Route 53 provides commercial DNS services to large accounts like Instagram, Twitter and CNN, including MyEtherWallet. The Ethereum blockchain wallet

developer confirmed that the attackers redirected the DNS to a bogus website masquerading as the real MyEtherWallet website (MyEtherWallet, 2018). Not only that, the attack used the vulnerabilities in the Border Gateway Protocol (BGP) routing security to advertise spoofed network routes from exploited BGP servers (Beaumont, 2018; Loshin, 2018; Naik, 2018).

The attackers were able to steal over $150,000 in Ethereum from the users' cryptocurrency wallet during the two-hour attack (Floyd, 2018; Loshin, 2018; Nichols, 2018). It was reported that this was not due to security vulnerabilities in the MyEtherWallet platform but vulnerabilities in the DNS servers which the hackers found (MyEtherWallet, 2018). In this incident, the MyEtherWallet was targeted not only through DNS spoofing attack but also phishing attack and BGP hijacking.

DNS SPOOFING PREVENTION TECHNIQUES

When it comes to preventing DNS spoofing, end user protections are limited. Server and website providers have more capabilities for defending themselves and their clients. In order to keep everybody secure, both parties must strive to avoid spoofing. Since the DNS protocol was developed without strong security mechanisms, this weakness is often taken advantage of by attackers who use it to launch malicious attacks.

According to Herzberg and Shulman (2012), most resolvers rely on non-cryptographic validation. To overcome this, users can use end-to-end encryption method via virtual private network (VPN). This service provides an encrypted tunnel for all web traffic as well as access to private DNS servers that only accept end-to-end encrypted requests. As a result, the servers are more resilient to DNS spoofing, and attackers' requests cannot be interrupted as they will not be able to duplicate the real website's unique security certificate (Kaspersky, 2021). Another way to protect against DNS spoofing attack is to install a firewall on the network infrastructure (Agarwal *et al.*, 2017). However, the firewall application should be constantly updated to avoid vulnerabilities.

The long-term solution to DNS spoofing is to improve DNS security by enabling DNSSEC (Chung *et al.*, 2017; Nikkhah *et al.*, 2017; Adiwal, Rajendran and Shetty, 2018; Dissanayake, 2018; Grothoff *et al.*, 2018; Rao and Sathish, 2018). DNSSEC was established by Internet Engineering Task Force (IETF) to enhance the DNS protocol by adding two critical features: (1) data origin authentication and (2) data integrity protection. To implement it effectively, DNSSEC introduced public key cryptography and digital signatures (Chetioui *et al.*, 2012; Zou *et al.*, 2016; Plageras *et al.*, 2018). It was proposed to identify forged DNS response which involved digital signing of DNS responses to authenticate and protect data integrity (Roy Arends *et al.*, 2005).

THE FUNCTION OF DNSSEC

The realisation of the implementation of DNSSEC on the domain name allows the DNS resolver to authenticate the DNS queries and respond with the authenticated DNS data to the client by using the cryptographic digital signature. The digital signature signed on the DNS data helps assure trust for the users that the questioned DNS data they have received are originally provided by the authoritative DNS servers and that the DNS data have not been manipulated by the bad actor in transit. Maintaining the trust of the domain name on the internet is essential for entities as it creates a significant impact on the entity's reputation and image.

With the introduction of DNSSEC, several new types of DNS resource records are created and these will be used in parallel for the domain name with a DNSSEC-enabled state. The use of DNSSEC key terminology in the DNSSEC implementation is described below:

1. RRSIG (Resource Record Signature): An RRSIG record holds a cryptographic signature for the resource record set or RRset in the zone file, for example, the RRSIG for the RRset A, AAAA, MX, CNAME etc.
2. DNSKEY record: A DNSKEY record stores the public key. There are usually two DNSKEYs per zone, for the zone signing key (ZSK) and key-signing key (KSK). The DNS resolvers use the DNSKEY records to verify that the digital signature in RRSIG is valid.
3. DS record: The DS record proves a linkage between a parent zone and child zone. The DS record must be added on the parent zone and contains a hash of the public KSK DNSKEY from the child zone. The DS record points to the next key in the chain of trust.
4. NSEC/NSEC3 record: The NSEC/NSEC3 record provides the authenticated denial of existence of the DNS records.

Zone signing is the main process in DNSSEC management. In DNSSEC, each zone has at least one public-private key pair. The private key is held by the administrator of the zone and kept secret. Meanwhile, the public key is added to the zone file with the new type of resource record, namely the DNSKEY record.

The private key is used to sign the resource records set in the zone file and later produces the digital signature that will be used by the DNS resolver to verify that the source of the DNS data queried by the user is genuinely generated by the authoritative DNS server. Each digital signature of the RRset is added to the zone with the new resource record, namely as a DNSKEY record.

Using the example of abc.gov.my, after the zone has been signed, the administrator of the abc.gov.my zone (the child zone) submits a copy of the public key called the DS record to the administrator of .gov.my (the parent zone) through the self-managed domain management system. Then, the .gov.my zone's administrator signs the .gov.my zone, which subsequently produces the RRSIG proof that the newly added DS record is authentic. It should be emphasised that the process of submitting the DS record must be achieved to establish the level of security between the parent and child zone.

Although the domain is secured with DNSSEC, the Secure Sockets Layer (SSL/HTTPS) is similarly important. This is because both the DNSSEC and SSL/HTTPS execute different functions of security and these two technologies complement each other in improving security. DNSSEC provides solutions to real problems without the need for encryption. This means that with the implementation of DNSSEC, all queries (lookups) related to DNS records will be verified before the answer can be accessed by the users, while the SSL/HTTPS function encrypts the network traffic to ensure all internet activities on the website are secured (no spying on the internet activity).

DNSSEC uses a chain of trust structure that starts with the top domain names, namely root (.) until the actual or final domain name is queried. To achieve effective implementation of DNSSEC, DNSSEC needs to be enabled at every level of the domain name starting from the root (.) zone until the final domain name.

DNSSEC IN THE MALAYSIAN GOVERNMENT DOMAIN

According to Mukhtar (2020), research on DNSSEC for .my domain was conducted in 2009 by MYNIC as the official .my domain registry recognised by Internet Corporation for Assigned Names and Numbers (ICANN). Initial study began by conducting an in-house study on the development of DNSSEC for .my domains. It was subsequently followed by a presentation of the myDNSSEC testbed at ICANN, DNSSEC workshop and the myDNSSEC public trial. In

2011, DNSSEC was successfully deployed and signed for .my and this resulted in the DNSSEC chain of trust from root (.) to .my to be established. This was followed by the full operation of the myDNSSEC system which began accepting the Delegation Signer (DS) records for the .my domain names such as .com.my, .gov.my, .edu.my and others.

The implementation of DNSSEC on the Malaysian Government domains was presented through the Cabinet Notes in July 2019. This included all .gov.my domains owned by the Ministry, agencies under the Ministry and the State Government. In December 2019, the Malaysian National Security Council issued a letter of instruction on the implementation of DNSSEC for all active domains registered by the Government under the management of MyGov*Net administered by MAMPU (Basir, 2019). This involved 402 of the 1,190 Government domains registered with MYNIC in 2019 (MYNIC, 2021).

The initial process of this implementation began with a series of discussions between MAMPU and MYNIC. This collaboration simplifies the strategies to facilitate the operation of DNSSEC by:

1. Providing intensive technical training to the technical contact of government agencies.
2. Providing technical guidance and actual hands-on on how to configure and implement DNSSEC on domain names.
3. Providing awareness on DNSSEC and DNS Security and Analytics, its functions, and the importance of the implementation.

METHODOLOGY

To expedite the implementation of DNSSEC on all Government domains, focus was given to all Government domains under the supervision of MyGov*Net which is centrally managed by MAMPU. The strategy used is listed below.

1. DNSSEC awareness
   All network administrators in each Ministry were briefed about DNS security and the importance of DNSSEC. During the briefing, active and inactive domains were verified by the network administrators. During this implementation, a total of 402 domains were identified as active domains.
2. Migration to DNSSEC server
   All verified domains were to migrate from the existing DNS server to the new DNS server configured with the DNSSEC protocol. Figure 2 shows the overall flow chart for the DNSSEC migration.
3. Notification and verification from MYNIC
   For security reason, MYNIC would contact the network administrator when there are changes to the nameserver records during the DNSSEC process. A notification via e-mail would be sent to the network administrator for each domain that had successfully enabled the DNSSEC.

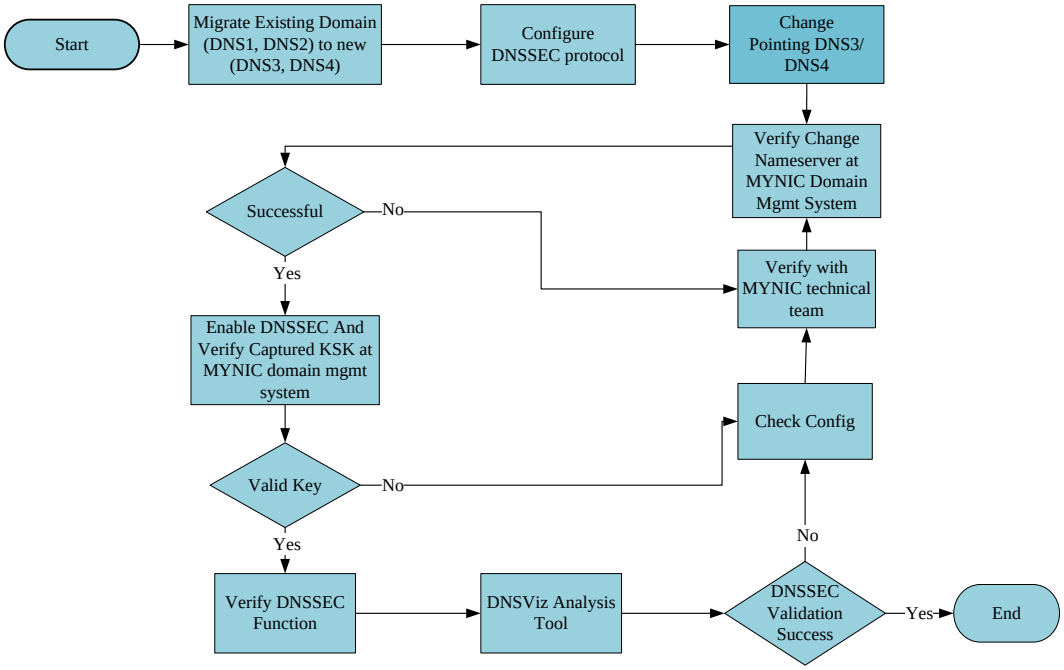

FIGURE 2: DNSSEC activation process.

DNSSEC VALIDATION

The most convenient way to validate DNSSEC is to use online tools. ICANN (2012) suggested three tools: (1) DNSViz; (2) DNSSEC Analyzer; and (3) Internet.nl. Based on these tools, we were strongly recommended to use the DNSViz and DNSSEC Analyzer. Both tools visualise the status of the DNS zone, the DNSSEC chain of trust for domain names, and its resolution path in the DNS namespaces. In fact, these tools are capable of detecting misconfiguration in each zone. Figures 3 and 4 show examples of successful DNSSEC validation using the DNSViz and DNSSEC Analyzer. Meanwhile, the Internet.nl checks to see if the Internet connection is up to date. It can also perform DNSSEC validation, but it is not as detailed as the DNSViz and DNSSEC Analyzer.

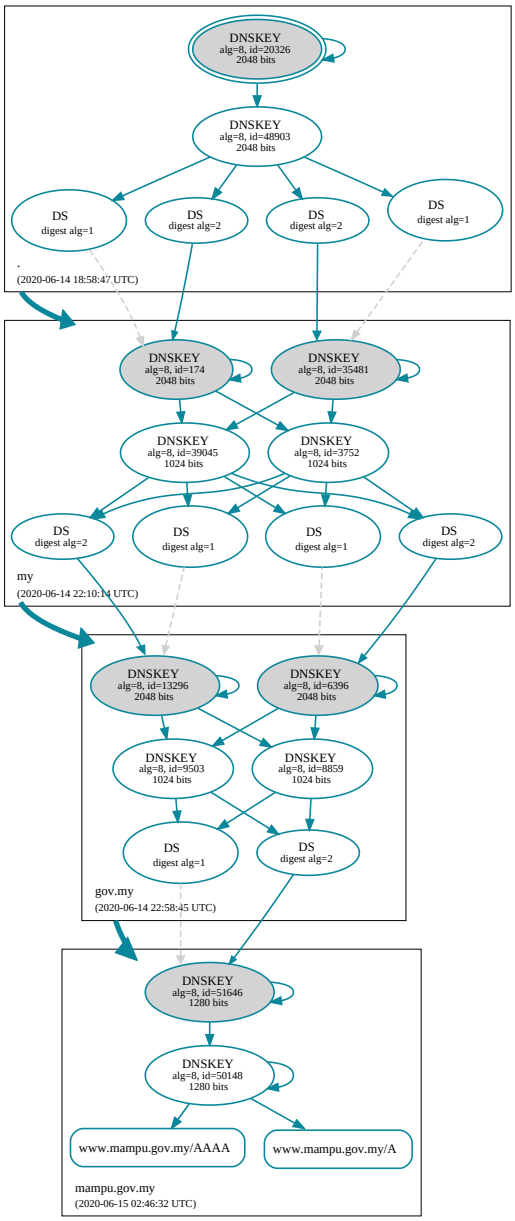

FIGURE 3: DNSSEC chain of trust for www.mampu.gov.my using *DNSViz* (2021).

.	Found 3 DNSKEY records for . DS=20326/SHA-256 verifies DNSKEY=20326/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=20326 and DNSKEY=20326/SEP verifies the DNSKEY RRset
my	Found 2 DS records for my in the . zone DS=174/SHA-256 has algorithm RSASHA256 DS=35481/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=26838 and DNSKEY=26838 verifies the DS RRset Found 6 DNSKEY records for my DS=174/SHA-256 verifies DNSKEY=174/SEP DS=35481/SHA-256 verifies DNSKEY=35481/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=174 and DNSKEY=174/SEP verifies the DNSKEY RRset
gov.my	Found 2 DS records for gov.my in the my zone DS=6396/SHA-256 has algorithm RSASHA256 DS=13296/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=17781 and DNSKEY=17781 verifies the DS RRset Found 6 DNSKEY records for gov.my DS=6396/SHA-256 verifies DNSKEY=6396/SEP DS=13296/SHA-256 verifies DNSKEY=13296/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=6396 and DNSKEY=6396/SEP verifies the DNSKEY RRset
mampu.gov.my	Found 2 DS records for mampu.gov.my in the gov.my zone DS=40306/SHA-1 has algorithm RSASHA256 DS=40306/SHA-256 has algorithm RSASHA256 Found 1 RRSIGs over DS RRset RRSIG=64368 and DNSKEY=64368 verifies the DS RRset Found 2 DNSKEY records for mampu.gov.my DS=40306/SHA-1 verifies DNSKEY=40306/SEP Found 2 RRSIGs over DNSKEY RRset RRSIG=5208 and DNSKEY=5208 verifies the DNSKEY RRset dns2.gitn.net.my is authoritative for www.mampu.gov.my www.mampu.gov.my A RR has value 43.251.19.58 Found 1 RRSIGs over A RRset RRSIG=5208 and DNSKEY=5208 verifies the A RRset
mampu.gov.my	dns1.gitn.net.my is authoritative for www.mampu.gov.my www.mampu.gov.my A RR has value 43.251.19.58 Found 1 RRSIGs over A RRset RRSIG=5208 and DNSKEY=5208 verifies the A RRset

FIGURE 4: DNSSEC chain of trust for www.mampu.gov.my using *DNSSEC Analyzer* (2020).

RESULTS AND DISCUSSION

The DNSSEC process began on October 7, 2019, and was completed on August 27, 2020, with 439 domains involved, and this exceeded the initial target of 402 domains. Table 1 shows the categories and number of domains that have been successfully implemented with DNSSEC.

TABLE 1: Category and number of domains

Category	No. of Domain
.gov.my	412
.org.my	3
.com.my	4
Total	439

The implementation took nearly a year to complete. It should be noted that it is possible to complete the implementation process within a short period of time. However, these processes were delayed because of the COVID-19 pandemic that had made technical work difficult because of the work from home requirement. Among the challenges experienced included the difficulty to get accurate administrative contact, outdated information in the "whois" database, and having to perform the activation processes remotely. Figure 5 shows the number of domains implemented with DNSSEC over the 10-month period.

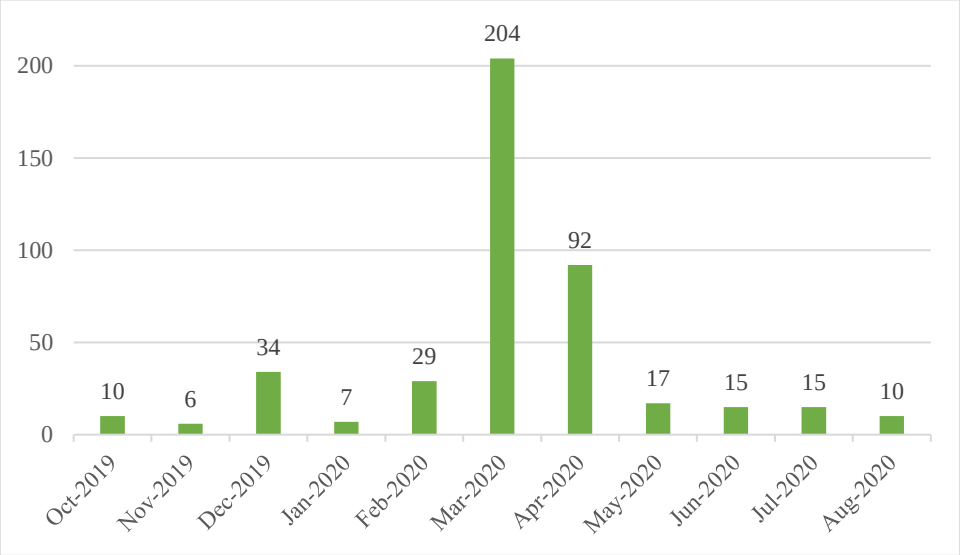

FIGURE 5: Number of domains implemented with DNSSEC over the 10-month period.

As of September 30, 2021, a total of 320,515 .my domains are registered with MYNIC but only 883 domains (0.28%) have been DNSSEC activated (MYNIC, 2021). These figures indicate that the deployment of DNSSEC in Malaysia is still low. In fact, during the briefing, it was discovered that the majority of users were unaware of DNSSEC. This finding is in line with Chung (2017) and Hampton (2017) who found that one of the reasons for the low rate is the lack of user awareness on DNS security. Additionally, domain registrars need to support DNSSEC, and the service should be provided for free in order to maintain DNS security. Most of this service requires an additional fee (EasyDNS, 2021; GoDaddy, 2021) or the DNSSEC may be provided for free but not the key management (Amazon, 2021). As a result, many users tend to delay implementation of DNSSEC (Senior, 2013).

The next plan in the implementation process is to execute DNSSEC on the remaining Government domains that have yet to be created. However, the current situation of the COVID-19 pandemic meant that the process would be quite difficult to implement. Nonetheless, we are confident that it can be performed even if it takes a long time to complete. The Government is committed to the implementation of DNSSEC to ensure digital Government security in Malaysia. Cyber security features are constantly enhanced in the Government's ICT infrastructure system in order to strengthen the protection of the Government's ICT assets and to increase the people's confidence in the digital services offered. Meanwhile, the deployment of DNSSEC is also extended to the private sector. Priority is given to the critical national information infrastructure sector and this DNS security awareness programme is indeed at its height of implementation.

CONCLUSION

DNS spoofing is a serious problem that can strike any organisation and it can endanger national security. This problem thus demands that the website architecture is protected in every aspect and related modules. DNS resolution occurs before the user interacts with the website and if the DNS is hijacked by a hacker, the user is likely to interact with a fake website. Even if a website is protected with a firewall, users are still at a high risk of exposure to security issues if the DNS architecture is not protected.

The implementation of DNSSEC has increased the level of security and data integrity of domain names from vulnerabilities in DNS. DNSSEC is an effective method to protect the security of the DNS infrastructure and this in turn prevents and protects users from being redirected to fake websites. DNSSEC should be a key requirement to protect consumers in the digital services era. Although the deployment of DNSSEC is still low, its implementation needs to be carried out in order to maintain the DNS security environment. A comprehensive awareness campaign is needed so that all users understand the importance of the issue.

REFERENCES

Adiwal, S., Rajendran, B. and Shetty, P. (2018) 'Domain Name System (DNS) Security: Attacks Identification and Protection Methods', in *International Conference on Security & Management (SAM18)*. Las Vegas, USA.

Agarwal, S. *et al.* (2017) 'A Case Study Solution to DNS Cache Poisoning Attacks', *International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)*, 3(36), pp. 91–97.

Amazon (2021) *Amazon Route 53 pricing, Amazon*. Available at: https://aws.amazon.com/route53/pricing/ (Accessed: 18 September 2021).

Antić, Đ. (2014) 'DNSSEC Deployment and Challenges', in *Sinteza 2014 - Impact of the Internet on Business Activities in Serbia and Worldwide*. Belgrade, Serbia, pp. 678–682. doi: 10.15308/sinteza-2014-678-682.

APNIC (2021) *DNSSEC Validation Rate by country (%), APNIC*. Available at: https://stats.labs.apnic.net/dnssec (Accessed: 10 October 2021).

Arends, R. *et al.* (2005) *DNS Security Introduction and Requirements*.

Arends, Roy *et al.* (2005) *Protocol Modifications for the DNS Security Extensions RFC 4035*. Available at: https://datatracker.ietf.org/doc/rfc4035/.

Assolini, F. (2011) *Massive DNS poisoning attacks in Brazil, Kaspersky Lab*. Available at: https://securelist.com/massive-dns-poisoning-attacks-in-brazil/31628/ (Accessed: 14 September 2021).

Avineshwaran, T. (2015) *MAS: Website was compromised by 'cyber caliphate', The Star*. Available at: https://www.thestar.com.my/News/Nation/2015/01/26/MAS-website-compromised-cyber-caliphate/ (Accessed: 11 September 2021).

Basir, M. R. (2019) 'Pengukuhan Keselamatan Nama Domain Kerajaan Melalui Pelaksanaan Domain Name System Security Extensions (DNSSEC)', *National Security Council*.

Beaumont, K. (2018) *Hijack of Amazon's internet domain service used to reroute web traffic for two hours unnoticed, Medium*. Available at: https://doublepulsar.com/hijack-of-amazons-internet-domain-service-used-to-reroute-web-traffic-for-two-hours-unnoticed-3a6f0dda6a6f (Accessed: 15 September 2021).

Chad R Dougherty (2008) *Vulnerability Note VU#800113 - Multiple DNS implementations vulnerable to cache poisoning, Carnegie Mellon University*. Available at: http://www.kb.cert.org/vuls/id/800113.

Chetioui, K. *et al.* (2012) 'Security of the DNS Protocol - Implementation and Weaknesses Analyses of DNSSEC', *International Journal of Computer Science Issues*, 9(2), p. 3.

Chung, T., Rijswijk-Deij, R. van, Chandrasekaran, B., *et al.* (2017) 'A Longitudinal, End-to-End View of the DNSSEC Ecosystem', in *26th USENIX Security Symposium*. Vancouver, BC, Canada:

USENIX Association, pp. 1307–1322. Available at: https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-%0Achung.pdf.
Chung, T., Rijswijk-Deij, R. van, Choffnes, D., *et al.* (2017) 'Understanding the Role of Registrars in DNSSEC Deployment', in *Internet Measurement Conference (IMC'2017)*. London, United Kingdom: Association for Computing Machinery. doi: https://doi.org/10.1145/3131365.3131373.
Chung, T. (2017) *Why DNSSEC deployment remains so low*, *APNIC*. Available at: https://blog.apnic.net/2017/12/06/dnssec-deployment-remains-low/ (Accessed: 13 June 2021).
Constantin, L. (2011) *Brazilian hackers use DNS poisoning to infect users with banking Trojan*, *InfoWorld*. Available at: https://www.infoworld.com/article/2620826/brazilian-hackers-use-dns-poisoning-to-infect-users-with-banking-trojan.html (Accessed: 14 September 2021).
Dissanayake, I. M. M. (2018) 'DNS Cache Poisoning: A Review on its Technique and Countermeasures', in *2018 National Information Technology Conference (NITC)*. Colombo, Sri Lanka: IEEE.
DNSSEC (2021) *Imperva*. Available at: https://www.imperva.com/learn/application-security/dnssec/ (Accessed: 7 June 2021).
DNSSEC Analyzer (2020) *VeriSign, Inc.* Available at: https://dnssec-analyzer.verisignlabs.com/www.mampu.gov.my (Accessed: 10 June 2021).
DNSViz (2021) *Sandia Corporation*. Available at: https://dnsviz.net/d/www.mampu.gov.my/dnssec/ (Accessed: 10 June 2021).
EasyDNS (2021) *DNS PRO Managed Anycast DNS*, *easyDNS*. Available at: https://easydns.com/dns/pro/ (Accessed: 18 September 2021).
Fisher, D. (2011) *Major DNS Cache Poisoning Attack Hits Brazilian ISPs*, *Threatpost*. Available at: https://threatpost.com/major-dns-cache-poisoning-attack-hits-brazilian-isps-110711/75859/ (Accessed: 14 September 2021).
Floyd, D. (2018) *$150K Stolen From MyEtherWallet Users in DNS Server Hijacking*, *CoinDesk*. Available at: https://www.coindesk.com/markets/2018/04/24/150k-stolen-from-myetherwallet-users-in-dns-server-hijacking/ (Accessed: 15 September 2021).
GoDaddy (2021) *Enable DNSSEC in my Premium DNS account*, *GoDaddy*. Available at: https://my.godaddy.com/help/enable-dnssec-in-my-premium-dns-account-6420 (Accessed: 18 September 2021).
Grothoff, C. *et al.* (2018) 'Towards Secure Name Resolution on the Internet', *Computers & Security*, 77(1), pp. 694–708. doi: 10.1016/j.cose.2018.01.018.
Hampton, N. (2017) *Why isn't everyone using DNSSEC?*, *APNIC*. Available at: https://blog.apnic.net/2017/06/28/isnt-everyone-using-dnssec/ (Accessed: 14 June 2021).
Hamzah, A.-Z. A. and Carsten, P. (2015) *Malaysia Airlines website targeted by hacker group 'Cyber Caliphate'*, *Reuters*. Available at: https://www.reuters.com/article/us-malaysia-airline-cybercrime-idUSKBN0KZ08E20150126 (Accessed: 11 September 2021).
Harjani, A. (2015) *Malaysia Airlines says website not hacked*, *CNBC*. Available at: https://www.cnbc.com/2015/01/25/malaysia-airlines-site-hacked-by-cyber-caliphate.html (Accessed: 11 September 2021).
Herzberg, A. and Shulman, H. (2012) 'Security of Patched DNS', in *European Symposium on Research in Computer Security*. doi: 10.1007/978-3-642-33167-1_16.
ICANN (2012) *DNSSEC Tools*, *ICANN*. Available at: https://www.icann.org/resources/pages/tools-2012-02-25-en (Accessed: 25 September 2021).
Kaminsky, D. (2008) 'Black Ops 2008: Its the End of the Cache As We Know It', in *Black Hat Conference*. Japan. Available at: http://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf.
Kaspersky (2021) *What is DNS Cache Poisoning and DNS Spoofing?*, *Kaspersky Lab*. Available at: https://www.kaspersky.com/resource-center/definitions/dns (Accessed: 9 October 2021).
Kim, T. H. and Reeves, D. (2020) 'A survey of domain name system vulnerabilities and attacks', *Journal of Surveillance, Security and Safety*, 1, pp. 34–60. doi: 10.20517/jsss.2020.14.
Kovacs, E. (2015) *Cybercriminals Use DNS Poisoning in Brazilian Boleto Fraud Scheme*, *Security Week*. Available at: https://www.securityweek.com/cybercriminals-use-dns-poisoning-brazilian-boleto-fraud-scheme (Accessed: 15 September 2021).

Loshin, P. (2018) *BGP routing security flaw caused Amazon Route 53 incident, TechTarget*. Available at: https://searchsecurity.techtarget.com/news/252439945/BGP-routing-security-flaw-caused-Amazon-Route-53-incident (Accessed: 15 September 2021).
MAMPU (2016) *Public Sector ICT Strategic Plan 2016–2020*. Putrajaya.
Mukhtar, M. (2020) 'Adoption DNSSEC to Secure e Government Services', in *vTechDay ICANN 68*. Kuala Lumpur: Internet Corporation for Assigned Names and Numbers (ICANN).
MyEtherWallet (2018) *Official statement regarding DNS spoofing of MyEtherWallet domain*. Available at: https://www.reddit.com/r/MyEtherWallet/comments/8eloo9/official_statement_regarding_dns_spoofing_of/ (Accessed: 15 September 2021).
MYNIC (2021) *Statistics*. Available at: https://mynic.my/media/statistics/ (Accessed: 7 July 2021).
Naik, A. (2018) *Anatomy of a BGP Hijack on Amazon's Route 53 DNS Service, Cisco*. Available at: https://www.thousandeyes.com/blog/amazon-route-53-dns-and-bgp-hijack (Accessed: 15 September 2021).
Nichols, S. (2018) *AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet, The Register*. Available at: https://www.theregister.com/2018/04/24/myetherwallet_dns_hijack/ (Accessed: 15 September 2021).
Nikkhah, M. *et al.* (2017) 'A Statistical Exploration of Protocol Adoption', *IEEE/ACM Transactions on Networking*, 25(5), pp. 2858–2871. doi: https://doi.org/10.1109/TNET.2017.2711642.
Plageras, A. *et al.* (2018) 'Efficient IoT-based Sensor BIG Data Collection-Processing and Analysis in Smart Buildings', *Future Generation Computer Systems*, 82, pp. 349–357. doi: 10.1016/j.future.2017.09.082.
Raghuvanshi, G., Purnell, N. and Ng, J. (2015) *Malaysia Airlines Website Hacked by Group Calling Itself 'Cyber Caliphate', The Wall Street Journal*. Available at: https://www.wsj.com/articles/malaysia-airlines-website-hacked-by-group-calling-itself-cyber-caliphate-1422238358 (Accessed: 11 September 2021).
Rao, R. V. and Sathish, M. G. C. (2018) 'A Survey of Analysing the Internet DNSSEC traffic for resolving platform optimisation and performance improvement', *Asian Journal of Engineering and Technology Innovation (AJETI)*, pp. 197–199.
Roopam and Sharma, B. (2014) 'Review Paper on Prevention of DNS Spoofing', *International Journal of Engineering and Management Research*, 4(3), pp. 164–170.
Senior, C. (2013) *Recent Domain Name System Attack Highlights Need for DNS Security Extensions (DNSSEC), BlueCat Networks*. Available at: https://en.prnasia.com/releases/global/Recent_Domain_Name_System_Attack_Highlights_Need_for_DNS_Security_Extensions_DNSSEC_-82913.shtml (Accessed: 18 September 2021).
Southam, M. (2014) 'DNSSEC: What it is and why it matters', *Network Security*, 2014(5), pp. 12–15. doi: https://doi.org/10.1016/S1353-4858(14)70050-9.
Zorz, Z. (2011) *Brazilian ISPs hit with massive DNS cache poisoning attacks, Help Net Security*. Available at: https://www.helpnetsecurity.com/2011/11/07/brazilian-isps-hit-with-massive-dns-cache-poisoning-attacks/ (Accessed: 14 September 2021).
Zou, F. *et al.* (2016) 'Survey on Domain Name System Security', in *2016 IEEE First International Conference on Data Science in Cyberspace (DSC)*. IEEE. doi: 10.1109/DSC.2016.96.

Ahmad Syukri Abdullah
Dr Siti Hanom Marjuni
ICT Infrastructure Shared Services and Security Development Division,
Malaysian Administrative Modernisation and Management Planning Unit (MAMPU).
syukri@mampu.gov.my, hanom@mampu.gov.my

Mastura Mukhtar
MYNIC Berhad
mastura@mynic.my