IHS Markit 2017 market analysis predicted annual growth of 12 percentage of the internet of things(IoT) connected devices globally, from approximately 27 billion in 2017 o 125 billion in 2030 (IHS Markit, 2017). An Internet Protocol version 4(IPv4) address is 32 bits long, yielding approximately 4 billion network addresses. In contrast, an IPv6 address is 128 bits long, allowing for more than 340 undecillion addresses (Batallaa, Binczewskib and Burakowskic, 2011). The number of network addresses IPv6 has set it as the ideal network protocol for the future of the internet.

The billions of IoT devices can be computers, smartphones, actuators, home appliances, intelligent electrical devices, and critical national infrastructures such as water purifying plants and road infrastructure. Internet Protocol Security(IPSec) is a suite of protocols and algorithms designed to secure data transmitted over the internet or any public network. Thus, providing confidentiality, integrity and authentication to the data transmitted through the IP network (Thomas and Elbirt, 2004). The two protocols defined for securing IP packets are Authentication Header(AH) and Encapsulating Security Payload(ESP). AH ensure data integrity by authenticating the sender, and it also provides replay protection.ESP provides confidentiality of data through encryption and authentication (Loshin, 2021). IPsec protects IPv4 and IPv6 data; however, it is optional on IPv4, integrated into IPv6. Regulations such as General Data Protection Regulation(GPDR) require pseudonymization of data and data privacy protection; IPv6 becomes ideal for compliance with the law. Critical national infrastructure requires a heightened amount of security against malicious attackers, such as in the attempt to increase sodium hydroxide on the water plant in the United States of America(USA) by malicious attackers (Bergal, 2021). Thomas and Elbir (2004) state that one of the most significant drawbacks of IPsec is its complexity. While IPsec's flexibility has contributed to its popularity, it also leads to confusion and has led security experts to state that “IPsec contains too many options and too much flexibility.”

Domain Name System (DNS) is a framework used to resolve internet domain names to IP addresses, and it is a vital function used by the entire internet. DNS has vulnerabilities exploitable by malicious actors such as DNS spoofing and DNS cache poisoning (Ariyapperuma and Mitchell, 2007). The risks associated with DNS poisoning and spoofing are data theft, malware infection, and halted security updates. The Internet Engineering Task proposed DNS Security Extensions (DNSSEC) Force(IETF) to solve the DNS vulnerabilities. DNSSEC, through the use of digital signatures, ensures that DNS entries are authentic and their integrity is legitimate. Some of the internet-connected devices are part of critical functions such as healthcare, and secure name resolution is essential to prevent data theft, such as redirecting an implantable device's monitoring data to the malicious host.

References :

Ariyapperuma, S. and Mitchell, C. J. (2007) ‘Security vulnerabilities in DNS and DNSSEC’, *Proceedings - Second International Conference on Availability, Reliability and Security, ARES 2007*, (January 2007), pp. 335–342. doi: 10.1109/ARES.2007.139.

Batallaa, J., Binczewskib, A. and Burakowskic, W. (2011) ‘Why is IPv6 Deployment Important for the Internet Evolution?’, *Nit.Eu*, pp. 5–15. Available at: http://www.nit.eu/czasopisma/JTIT/2011/2/5.pdf.

Bergal, J. (2021) *Florida Hack Exposes Danger to Water Systems | The Pew Charitable Trusts*. Available at: https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2021/03/10/florida-hack-exposes-danger-to-water-systems [Accessed: 21 July 202]).

IHS Markit (2017) *News Release | IHS Markit Online Newsroom*. Available at: https://news.ihsmarkit.com/prviewer/release_only/slug/number-connected-iot-devices-will-surge-125-billion-2030-ihs-markit-says (Accessed: 20 July 2021).

Loshin, P. (2021) *What is IPsec (Internet Protocol Security)?* Available at: https://searchsecurity.techtarget.com/definition/IPsec-Internet-Protocol-Security (Accessed: 21 July 2021).

Thomas, J. and Elbirt, A. J. (2004) *How IPsec works, why we need it, and its biggest drawbacks | CSO Online*. Available at: https://www.csoonline.com/article/2117067/data-protection-ipsec.html (Accessed: 21 July 2021).