 ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print)

The Significance and Future of Network Security

Nnabuife Godfrey Somtochukwu
Cranfield University, UK

Abstract
Network security is increasingly becoming ever more crucial to individuals and various administrations. An increasing number of organisations, including governmental organisations, store, manipulate and communicate valuable and confidential information electronically. However, a number of threats compromise the security of this information making network security of great importance. Through examination of the times gone by of security permits a better understanding of the emergence of security innovations and technologies. Understanding the architecture of the internet paves ways for modifications that can reduce conceivable attacks that can be sent across the network. Being aware methods, of attacks permits for suitable securities to emerge. Various administrations protect their activities from the internet through the use of encryption mechanisms and firewalls. For a better understanding and a careful evaluation, the internet, its weaknesses, threats via the internet and security technology is critically examined to reach a conclusion.

Keywords
Network Security, Internet, Cryptography, Security Technology

I. Introduction
With the rise of modern technology such as the internet and new networking technology, the world is becoming more interconnected. There is a vast amount of commercial, personal, government and military information on networking infrastructures universally [1]. Making network security one of the key factors for individuals, organisations and governments and underpins numerous objectives outlined in these bodies organisational structure, strategies, policies, aims and objectives [2-3]. Large sums of capital is spent on ensuring the robustness of information and network security, in 2014 the UK government spent over £1 billion [4]. And according to the Financial Times worldwide enterprise spending on information and network security is over £2 billion [5]. According to Dayo (2013), network security is becoming of increased standing dueto intellectual property that can be effortlessly acquired through the internet.

II. Network Security
Network security comprisesof systems or practices used to protect a computer network from unauthorized accesses, misappropriations or unauthorized alterations [6]. The first stage of this procedure is verifying a user, characteristically a username and a password are used for this: this is referred to as'one-factor authentication'[7]. In addition, depending on the level of security required, 'two-factor' or 'three-factor' authentication systemscan be used - thiscomprisesthe verification of fingerprints or security tokens[7-8]. After verification a, a firewall is used to make sure that the user accesses only the services that are authorised to them. In addition to the verification of the user, networksoughtto correspondinglydeliver security procedures against computer viruses, Trojans or worms.Antivirus software and Intrusion Prevention Systems (IPS) can be used to shield a network from viruses, Trojans and worms.Network security differs in accordance to the level of security required [9]. For instance, the level of security required by a small business will be different to that adopted by the military. Organisations tend to match their level of security in accordance to their perceived threat or the sensitivity of the information that is being protected on the network [10]. Homes or small businesses tend to have small networksso a rudimentary firewall, antivirus software and strong passwords will suffice, however a military network would need a much more secure strong firewall and proxy, encryption, strong antivirus software and a two- or three-factor authentication system and much more network security [11].

Presently there are two fundamentally diversenet works, data networks and synchronous network comprised of switches [12]. The internet is viewed to be a data network.

Since the present data network entails computer-grounded routers, information can be attained by programs, such as "Trojan horses,"planted in the routers [12]. The synchronous network that comprises of switches does not bufferd at a and consequently are not vulnerable to hackers [1]. This is why security is accentuated in data networks, such as the internet, and additional networks that link to the internet [1], [12]

II. Developing Secure Networks
When developing a secure network, the following need to be considered [12]:

- Access–official operators are provided the means of communicating to and from a particular network
- Verification–make sure the operators of the network are authentic
- Discretion–make certain that the data in the networks tays private
- Integrity–make sure the data sent has not been a ltered intransit.
- Non-refutation–make sure the operator does not disprove of making use of the network

An efficient network security strategy is designed with through understanding of security issues, risks, potential threats, required level of security, and features that brand a network susceptible to attack [12-13].

To lessen the vulner abilities found on the computer network there are various accessible products on the market. The products consist of authentication mechanisms, encryption, security management, firewalls and intrusion-detection [1],[14]. Globally individuals and organisations use a mixture of some of these products. Organisations invest in securing their intranets from threats on the internet as the internet architecture itself leads to vulnerabilities in the network [1],[15]. Having an understanding of security threats of the internet immensely assists in the emergence of innovative security approaches and technologies for networks

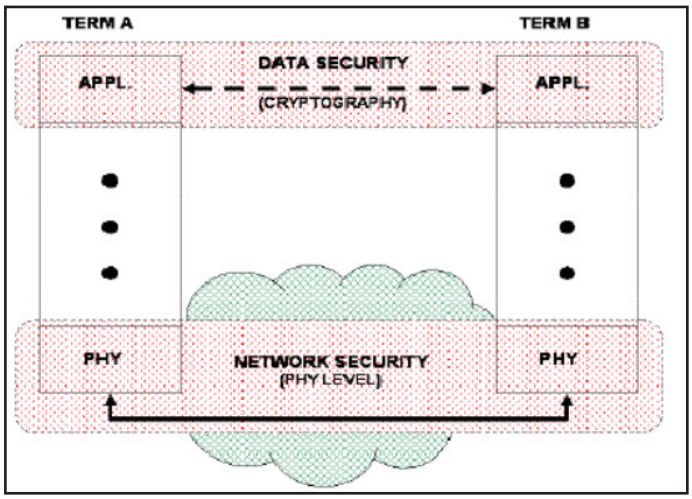

Fig. 1: Founded on the OSI Model, Data Security and Network Security Have a Differing Security Functions [1]

With internet access and internet safe guarding itself [1], [16]. It is crucial to monitor and study various types of potential threats and attacks over the internet in order to detect and guard against them [1], [17]. Daya (2013) states that intrusion discovery systems are established based on the kinds of attacks most usually used. Daya (2013) further writes that network interferences comprise of 'packets' that are presented to cause difficulties for the sub sequent reasons:

1. Acquire system data that can be exploited in future attacks
2. User sources impractically
3. Disrupt system resource's intended function

Currently typical security procedures are used on computers linked to the network. Security procedures occasionally appear as part of a single layer of the Open Systems Interconnection (OSI) network reference model. The association of network security and data security to the OSI model is revealed in Fig.1. It can be realised that the cryptography transpires at the application layer; thus, the application designers are mindful of its presence [12]. The operator can select different approaches of data security and network security is mostly contained within the physical level of the OSI.

Designs using a layered approach to secure network design have been carried out and the levels of the security model correspond to the OSI model levels. This security method leads to an operative and well-organised design which avoids some of the popular security difficulties [12].

III. Network Security Future

The field of network security is vast and forever changing as new technologies are designed to tackle existing, new and potential threats. To critically address the significance and future of network securityan analysis ofthree factors will be carried out:

A. The Evolution of Security in Networks

Arguably network security was revolutionised by the crime committed by Kevin Mitnick in the United States [1]. The crime was the largest computer-related crime in U.S. history with record losses of $80 million in U.S. intellectual property and source code from a various corporations and since then, network security came into the limelight [18]. Communal networks are being depend on to deliver fiscaland personal information Due to the evolution of data obtain able through the internet, network security is also mandated to progress in order to preserve the robustness of information security [1]. Kevin Mitnick's offense has led to corporations accentuating security for intellectual property [1],[19]. The need to keep information secure on the internet could be said to be the main driving force for information security developments [20]. Historically internet procedures were not designed to safe guard themselves, this left the internet vulnerable to attacks [1], [12]. Modern progresses in the internet architecture have made information and network security more secure[19], [21].

B. Internet Architecture and Susceptible Security Characteristics of the Internet

There are over three billion internet users worldwide and any day, there are thousands of major incidences of a security (Figure 1) [22].

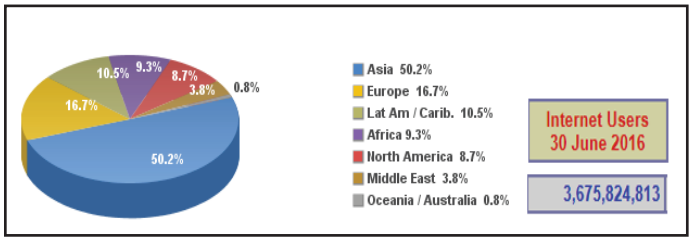

Fig. 2: World Internet Usage Statistics June 30, 2016 [38]

The uneasiness of security vulnerability on the internet has led corporations to make use of secured private intranets or networks [12]. Mechanisms at several layers of the Internet Protocol Suite were introduced by the Internet Engineering Task Force (IETF) [1], [23], [24]. The security mechanisms permit for the rational defence of information units that are transported across the network [25]. In 1988 the Morris Worm was born named after RobertMorris who was sentenced for releasing a worm that affected over 5000 internet connected computers [26]. It was in response to Morris attack that the Computer Emergency Response Team (CERT) was formed in order to make computer users aware of network security issues[1].

The security construction of the internet protocol, identified as IP Security (IPsec), is a calibration of internet security [1]. IPsec, covers the current generation of IP(IPv6) as well as the current version, IPv4 [19]). Though new systems, such as IP sec, have been established tooverwhelm the internet's finest-recognised deficiencies, they seem to be in adequate [12], [27]. Figure2 displays a graphic depiction of how IPsec's are executed to deliver secure communications [1].

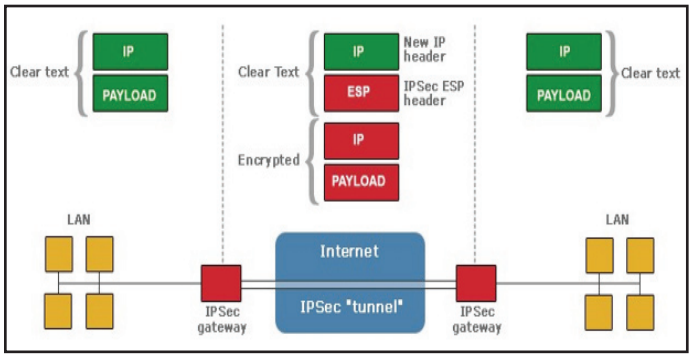

Fig. 3: IPSec

IPSec is a point-to-point procedure, on one end it encrypts and on the other decrypt sand both sides share key or keys. IPSec can

be used in binary modes, explicitly transport mode and tunnel modes [1], [6].

C. Security for Networks With Internet Access

Organisations currently use groupings of firewalls, encryption, and authentication devices to generate, intranets, that are linked to the internet but secured from it at the same time [1], [28]. However even though intranets can be swiftly setup to communicate information in a secured managed setting, the communicated information is still at risk without there being a high level of security [1], [12], [29]. If effectively managed with the right software of network security intranets are secure sources of information and communication. Never the less, the drawback of a closed intranet is that crucial information may end up not getting to the individuals that need the networks open, with the defences [10]. Examples of defences include : obligatory guidelines for staff opening of email and firewalls that pick-up and report unauthorised interference efforts [1].

With the development of new technologies cyber criminals are becoming highly sophisticated and collaborative, generating fresh security risks, whilst researchers are still discovering susceptibilities in already existing technologies [30-31]. According to Olavsrud (2015) to tackle the threat, it is essential that information security specialists understand the risks and potential risks on around, this will allow them to be in a better position to tackle network security threats. However as governments get involved in cyberspace to protect network security and impose legislation to tackle cybercrime, restrictions on activities arguably affect all organizations whether or not an organization is the intended target [30]. Olavsrud argues that even institutions not implicated in wrong doing will still be negatively impacted through collateral damage as governmental authorities' police their corner of the internet.

Conclusion

Network security is a significant sector that is progressively gaining attention as the internet rapidly expands [12]. Network technology is crucial for a wide variation of applications. Network security is imperative to information networks and applications. Though, network security is a crucial obligation in emergent networks, the lack of security methods that can be easily implemented is substantial. There is a gap in communication between the designers of security innovate or sand creators of networks. Network creation is a well-established procedure that is grounded on the Open Systems Interface (OSI) model [1], [32-33]. The OSI offers various advantages when developing networks. It proposals ease-of-use, flexibility, modularity, and standard is ation of procedures [34]. The procedures of different layers can be effortlessly joined to generate stacks which permit modular progress [1], [35]. The application of distinct layers can later be altered without making additional modifications, permitting flexibility in advancement. process [19]. In contrast to network design, secure network design is not a well-developed. There isn't a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design [36-37]

When thinking about network security, it must be highlighted that the entire network is protected and secured. Network security is not only concerned with the security in the computers at each end of the communication chain, when conveying information, the communication network must not be susceptible to attacks [12]. The network security field may have to evolve more rapidly to deal with the threats further in the future.

References

[1] B. Daya,"Network Security : History, Importance and Future," 2013.

[2] C. Yawut, P. Keawpipop,"The Future of Organization' s Computer Network Security for the Next 5 Years (2011-2015) by Using Delphi Technique," Vol. 6, No. 2011, pp. 184–188, 2015.

[3] European Commission,"Security research: Future-Bound to protect our society," 2016.

[4] Cabinet Office,"The UK cyber security strategy," 2016.

[5] Financial Times,"Corporate spending on IT security," 2011.

[6] C. Kaufman, R. Perlman, M. Speciner,"Network Security," Vol. 3, No. 8, pp. 4–8, 1995.

[7] A. Yassin, J. Yao, S. Han,"Strong Authentication Scheme Based on Hand Geometry and Smart Card Factors," Computers, Vol. 5, No. 3, pp. 15, 2016.

[8] D. W. Carman, P. S. Kruus, B. J. Matt,"Constraints and approaches for distributed sensor network security," DARPA Proj. report,(Cryptographic Technol. Group, Trust. Inf. Syst. NAI Labs), pp. 1–126, 2000.

[9] P. Golchha, R. Deshmukh, P. Lunia,"A Review on Network Security Threats and Solutions," Vol. 3, No. 4, pp. 21–24, 2015.

[10] C. Paquet,"Implementing Cisco IOS Network Security", 2nd ed. Cisco Press, 2012.

[11] G. Sadowsky, J. X. Dempsey, A. Greenberg, B. J. Mack, A. Schwartz,"Information technology security handbook", 2003.

[12] D. Gahlot, A. Thakur, A. Pokhriyal, D. Kukreti,"Network Security : it â€TM s time to take it seriously," Int. J. ofInnovative Res. Sci. Eng., Vol. 2, No. 9, pp. 613–620, 2014.

[13] A. W. Rufi,"Vulnerabilities, Threats, and Attacks," 2006.

[14] C. Kaufman, R. Perlman, M. Speciner,"Network security: private communication in a public world", second edition, 2nd ed. Prentice Hall Press Upper Saddle River, NJ, USA, 2002.

[15] P. C. Sethi, P. K. Behera,"Methods of Network Security and Improving the Quality of Service – A Survey," Int. J. Adv. Res. Comput. Sci. Softw. Eng., Vol. 5, No. 7, pp. 1098–1106, 2015.

[16] V. Nash, M. Peltu,"Rethinking Safety and Security in a Networked World: Reducing Harm by Increasing Cooperation," SSRN Electron. J., No. 6, pp. 1–30, 2005.

[17] E&Y, "Cybersecurity and the Internet of Things," E&Y, no. March, pp. 1–15, 2015.

[18] J. Christensen,"The trials of Kevin Mitnick," Mar-1999.

[19] D. K. G, M. K. Singh, M. Jayanthi,"Network Security Attacks and Countermeasures", Hershey: IGI Global, 2016.

[20] The Department of Commerce Internet Policy Task Force,"Cybersecurity, Innovation and the Internet Economy; Notice of Inquiry," Fed. Regist., pp. 1–8, 2010.

[21] M. N. Sirohi, Transformational Dimensions of Cyber Crime. Alpha Editions, 2015.

[22] BBC, "Internet used by 3.2 billion people in 2015," May-2015.

[23] L. Chen, G. Gong,"Communication System Security. Boca Raton", London and New York: CRC Press Taylor & Francis Group, 2012.

[24] K. Rose, S. Eldridge, L. Chapin,"The Internet of Things: An Overview: Understanding the Issues and Challenges of

a More Connected World," 2015.
[25] F. Mulazzani, S. a. Sarcia,"Cyber security on military deployed networks," 2011 3rd Int. Conf. Cyber Confl., pp. 1–15, 2011.
[26] J. Markoff,"Computer Intruder is Found Guilty," The New York Times, New York, 1990.
[27] C. Reynolds,"Data protection," Comput. Law Secur. Rev., Vol. 5, pp. 19–22, 1990.
[28] J. Jordan,"Extranet Security: A Technical Overview from a Business Perspective," 1997.
[29] W. Kramer,"Information and communications technology (ICT) in small business sample page proofs," Inf. Commun. Technol. small Bus., pp. 196–227, 2007.
[30] T. Olavsrud,"5 information security trends that will dominate 2016," 2015.
[31] Hewlett Packard Enterprise,"HPE Security Research Cyber Risk Report 2016," 2016.
[32] F. J. H. M. Vercoulen, M. van Wegberg,"Standard selection modes in dynamic, complex industries: creating hybrids between market selection and negotiated selection of standards," no. NIBOR / RM / 1998 / 06, 1998.
[33] R. S. Whitt,"A Horizontal Leap Forward : Formulating a New Communications Public Policy Framework Based on the Network Layers Model A Horizontal Leap Forward : Formulating a New Communications Public Policy Framework Based on the Network Layers Model," Vol. 56, No. 3, pp. 587–672, 2004.
[34] D. N. Serpanos, A. G. Voyiatzis,"Secure network design: A layered approach", Proc. - 2nd Int. Work. Auton. Decentralized Syst. IWADS 2002, no. December 2002, pp. 95–100, 2002.
[35] J. S. Heidemann,"Stackable Design of File Systems," p. xvi + 105, 1995.
[36] C. O. Lo,"Literature Integration: An Illustration of Theoretical Sensitivity in Grounded Theory Studies," Vol. 44, No. 2, pp. 177–189, 2016.
[37] T. Jaiswal, K. U. Singh, S. Sheikh,"A Novel Security Approach for Access Model," Int. J. Comput. Appl. (0975 – 8887), Vol. 138, No. 9, pp. 25–30, 2016.
[38] Miniwatts Marketing Group, "Internet World Stats: Usage and Population Statistics," 2017.

Nnabuife Godfrey Somtochukwu received his B.Sc. degree in chemical engineering from Anambra State University, Nigeria, in 2010. He obtained M.Sc. degree in petroleum and Gas Engineering from University of Salford, UK, in 2013. Currently, he is doing his doctoral research at Cranfield University, UK. His research interests include signal processing, network security, multiphase flow measurements, microwave and optical technique.