I J C T A, 9(3), 2016, pp. 1727-1732

Security in Emerging Networks

Arya Sedigh[1], Carlene Campbell[2], Kapilan Radhakrishnan[3] and Archie Watt[4]

Abstract: The society places a great deal of trust into Internet and we all rely on this Internetwork to conduct everyday tasks such as Business Transactions, Academic Research, Social Networking and etc. It is of utmost importance that we maintain, monitor and improve our Local Networks in order to assure reliability and security of our electronic assets. The Networking technology is growing at an exponential rate and with it the attacks on structure of these technologies. As a result, it is very important that we all try our best to develop and deploy countermeasures as soon as emerging networking technologies are deployed. This paper concentrates on the security developments and the next era of technology to come while outlining the features and characteristics of an ideal network. These characteristics are ideal of many recent and upcoming networking technologies. This report identifies the epitome that Internet users hope to achieve in the future. Furthermore by in depth analysis and considerations of Past, Present and Future of the Internet, a proposal is made to better the Emerging Networks' security implementations.

Keywords: Emerging Networks, Security, Future Internetwork, Authentication, Network Security Model

1. INTRODUCTION

Computer Networks are widely used at both, personal and Enterprise levels, and it has become a necessity to ensure their safety. This is to protect our data's integrity, availability and privacy. In [1], the three forces responsible for evolution of Internetworks are outlined as traffic growth, development of new services, and advances in technology. According to the statistics published in [2] the number of Internet users over the world has increased to over 9 times of what it was on December 31st 2000, so to accommodate the increasing number of users successfully in a sound Internetwork, characteristics such as reliability, speed and security should be developed in alignment to developments of Internet infrastructure. This report contains information on recent and future developments in Computer Networks industry. Each technology is explained in terms of principle and purpose. In section II a brief history of internetworks and security implementations are presented, which is followed by analysis of a few recent and upcoming networking technologies in section III, this section also includes two proposed authentication methods for network entities and this report aims to compare and contrast the two in order to determine which is best suited for Emerging Networks. In section IV, Network Security Models (NSMs) are considered in order to anticipate their role in Emerging Networks. In section V, an addition to the structure of NSMs is proposed and finally, in section VI a comprehensive conclusion is produced covering the research conducted on Emerging Networks and their security measures.

2. HISTORY AND THE NEED FOR SECURITY

Years have passed since the introduction of Advanced Research Projects Agency Network (ARPANET) which eventually spanned across the world and was called the Internet. When Defense Advanced Research Projects Agency (DARPA) was designing ARPANET, it was merely to connect a few workstations together for basic text communication, and originally no security measures were devised for it. When the Internet

[1] School of Applied Computing, University of Wales Trinity Saint David, *Email: arya.sedigh@uwtsd.ac.uk*

[2] School of Applied Computing, University of Wales Trinity Saint David, *Email: carlene.campbell@uwtsd.ac.uk*

[3] School of Applied Computing, University of Wales Trinity Saint David, *Email: kapilan.radhakrishnan@uwtsd.ac.uk*

[4] School of Applied Computing, University of Wales Trinity Saint David, *Email: archie.watt@uwtsd.ac.uk*

became popular and the number of online hosts started to increase rapidly, the value of this Internetwork became abundantly clear to all. Big companies, banks, government bodies and even personal networks were all being interconnected on a large scale network, and this led to the need for security implementations. But security was not taken seriously until the execution of Morris Worm in 1988 which according to [3] was a self-replicating piece of code that caused overflow and disabled 1 in every 20 hosts connected to the network, this worm was programmed to take advantage of the available resources on the network and after flooding every host, the network would be paralyzed. Although this incident caused a lot of damage, some believe it was a necessity so that it could warn the Internet society on what to expect from attackers and that was the incentive behind many security implementations across the globe.

So Internet has grown a lot in the past couple of decades and has now become a place for business transactions and confidential communications, used by both public and private sectors. Authors of [5] suggest that "the biggest concern in the past and today is that the message sent is the message received and that the enemy does not intercept a message".

Since the cyber space (Internet) has become a birthplace for attacks and malicious software, some are not happy to conduct their transactions and everyday business over this internetwork and as stated in [4], "to counter this this trend, the issues of network security on the Internet must be constantly reviewed and appropriate countermeasures devised".

Furthermore, in [4] it is reported that no host is completely secure or immune to the threats over the Internet; and this, calls for a proper network security model alongside regular revisions and updates to improve its security mechanisms.

When the 'Need for Security' is looked at from an attacker's point of view, it becomes clear that attackers are constantly researching to find new vulnerabilities in Internetworks' security architectures so that they can develop new attacking techniques to exploit the weak points of networks. This argument on its own should be sufficient to satisfy the incentive behind the 'Need for a sound Internet Security'.

3. RECENT AND UPCOMING SECURITY DEVELOPMENTS IN EMERGING NETWORKS

Ever since the Internet was introduced to the world, researchers, standardization organizations and world class vendors have worked towards making this internetwork more reliable and accessible. This has been often accomplished by the introduction of new implementations like routing protocols which have made routing between networking devices faster and more secure. Authors in [6] outlined the key features of a significantly better Internet as Flexibility, Security, Mobility and Manageability.

Where the recent technologies are concerned, it is seen that the above factors play a key role in the characteristics included in their designs and implementations. A few of the recent developments in networking industry are identified below. Note that at least one of the four key features noted above, have been applied in each one:

3.1. Real-time Intrusion Detection and Prevention Systems

Intrusion Prevention and Detection Systems (IDS) & (IPS) have been around in the networking industry for a number of years, and so far they have been an important addition to the Network Security structure. The real-time IDS and IPS is now being used in the industry.

According to [7]'s observations, cited by [8], Network Security has a simple formula which is:

"Security = Visibility + Control" [7]

Not only does this formula convey how one should fortify and defend a network, it also illustrates the purpose of IDS and IPS systems:

3.1.1. Visibility

IDS deals with Visibility, since it requires all packets traversing the network to be visible, so that it can analyze and document them. IDS systems will not stop any intrusion or attack from happening, they only detect such incidents, report them immediately via email and document them, usually in a log file. This file can be viewed by the network administrators. The data gathered can then be used to identify vulnerabilities of the network, and research on how to define the correct countermeasures or perhaps rectify the security architecture of the network where required. Tripwire is an IDS software which is implemented by many companies in the commercial sector [9].

3.1.2. Control

This part of the formula is referring to IPS, as it requires access rights to the network resources. Moreover, the authors of [8] stress that, "Control is paramount to enforcement", in which enforcement is the application of policies and rules in the network in order to prevent an intrusion. Any Anti-virus or Firewall software can be named as an example for an IPS system, because what they do, is block the attacks to the network whether by filtering IP packets, or placing a suspicious file under quarantine.

3.1.3. Security

According to the above formula, if one has complete control over a network, can view and use the resources available in the network, they can secure the network in the sense that any intrusion could be detected and prevented. Analysis of the log files produced by the IDS, will help fortify the network even more.

It is now clear that security which is one of the four factors of the ideal Internet has been the foundation and goal of IDS and IPS systems all along. Also, this implementation has made the network manageable; because managing a network and going through a complex structure and different layers to find and secure vulnerabilities could be tiresome and in some cases impossible.

3.2. Authentication and Identification

The main feature used to define the following developments and proposals is Security. Out of the ideal features of future Internet, security is the most important. If it was non-existent there would not have been any such network that people trust with their private information. This section contains information on two different authentication methods. These methods are explained in detail.

3.2.1. Authentication via a Unique Identifier

Authors in [10] proposed the effective identification structure for wireline and wireless networks. The concept of Effective identification concentrates in authentication of networking devices.

Normally in a network, devices are identified and authenticated by their IP or MAC Addresses, but author of [10] proposed that if each device were to be authenticated by another unique identifier before the layer two and three connections are established, the network will be soundly fortified as outsiders wouldn't be able to access the device keys, and they will fail in attacking the networking infrastructure. Furthermore, authors of [10] believe that this method will prevent many Denial-of-Service (DOS) attacks as mostly, they try to falsify the information in IP and MAC address slots in data packets in order to conduct the attacks.

In order to develop security measures and prevent attacks in the future of the Internet, sometimes instead of new technologies and developments, simply modification of the current standards and protocols are required.

In addition to Effective Identification, the authors of [10] proposed a new **Stateful** structure for Address Resolution Protocol (ARP)ARP: Responsible for the mapping of IP to MAC Addresses.. ARP on its own is a stateless protocol, meaning if *device A* were to send an ARP response to *device B* on a network, *Device B* would simply update its ARP Cache. In this stateful structure, there is a Finite State Machine (FSM) involved which acts according to the flowchart in Figure 1;

This modification to ARP will protect devices from a forged ARP Reply message. But it will be useless if the machine had already sent an ARP Request and was waiting for a Reply. This simple modification is an example of how currently used protocols and standards could be revised and appropriated for use with a more reliable internetwork.

3.2.2. Authentication via an Identification Management System

Another method of authentication is proposed by [12] in which, a minimum of three entities are required; A host that is requesting some services, an Identification Manager (IdM) that holds the Identification information of the Host entity and also a Relying Party that fetches the Identification information from the IdM and authenticates the host before offering it services. This process is demonstrated in Figure 2:

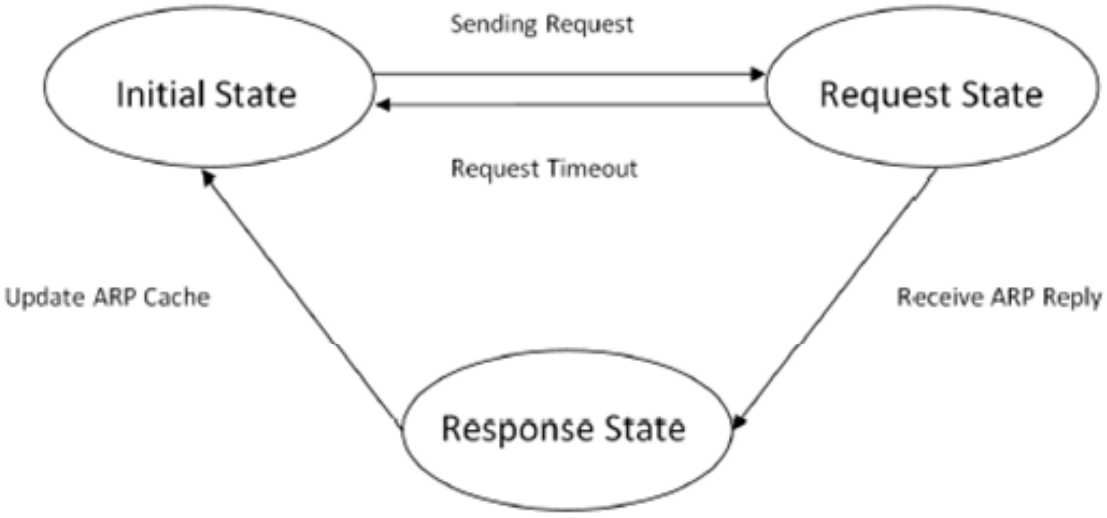

Figure 1: ARP Finite State Machine [9]

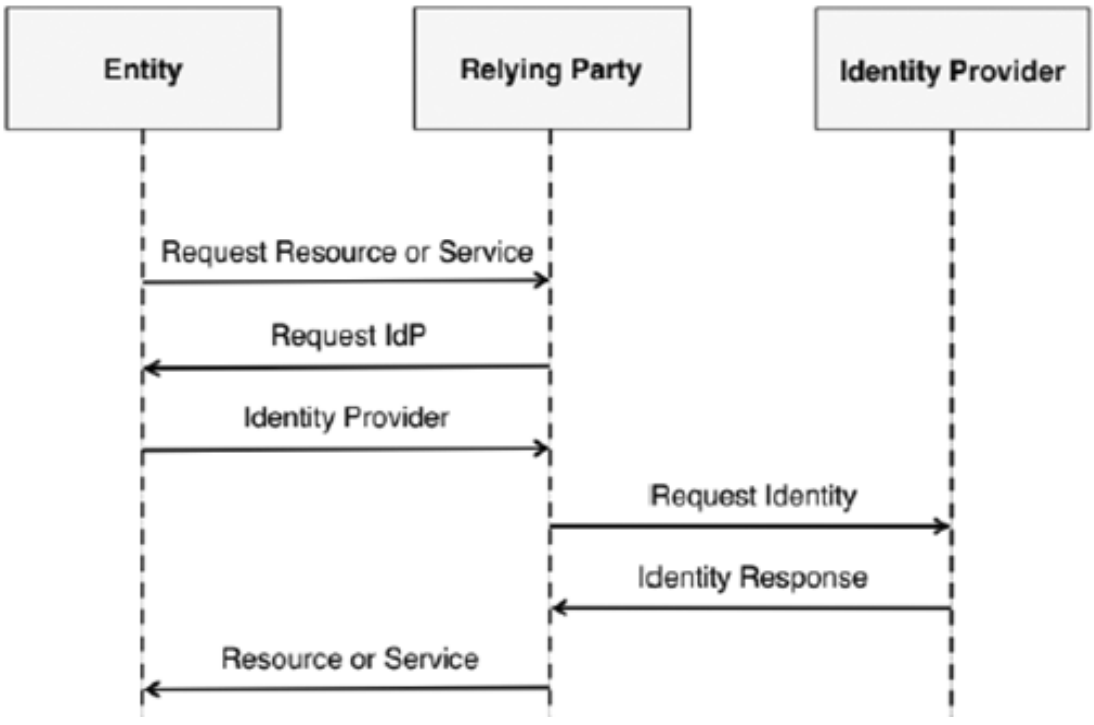

Figure 2 Entities in an IdM system [10]

4. NETWORK SECURITY MODELS IN EMERGING NETWORKS

The author of [13] suggests, Network Security Model (NSM) is defined as "A seven layer model that divides the task of securing a network infrastructure into seven manageable sections." This model is used for securing all devices in a network and there are no compatibility issues associated with it. Although this model is not a definitive guide to follow when securing a network, it still holds the potential to improve and expand to a comprehensive guide which could be implemented on a global level.

The fundamental reason why the Internet did not fail when it was deployed by DARPA was because there was a unity that connected every layer and protocol stack together, and that unity was then kept on and passed on the next generations of networking hardware and software, many new developments have been implemented since then, but they are all compatible and generic. So if we are to succeed in devising a sound NSM, we need to make sure that we use the same unity in the NSM's structure otherwise there won't be One NSM that everyone can just turn to.

Flexibility is the product of maintaining the Internet substrate and provision of Internet services, which according to [7] falls under the responsibilities of the Internet Service Provider (ISP). Since every year, new clients subscribe to ISPs, the service providers are not motivated to upgrade their physical infrastructure and therefore they just rely on the resources that are available within their physical network. Authors of [7], mentioned that to overcome this issue, Virtualization was proposed which separates the above mentioned attributes into Virtual Network Provider (VNP) and Physical Infrastructure Provider (PIP).

As mentioned in [7], VNPs have the responsibility of assigning hosts with flexible application services through employing and managing the physical resources from the PIPs. Moreover [7] believes this trend to be an absolute requirement for a healthy physical network infrastructure.

5. CONCLUSION

This report contains information on security implementations and their characteristics. From what has been gathered, it is safe to say that we established Network Security as one of the most important key factors of any Network at any time. It is also deduced that security patches and protocol amendments applied to networks tend to cause a complex structure which is becoming more and more complicated.

Having considered the current and upcoming trends in emerging networks, and defined the necessary characteristics for an ideal internetwork, it has become clear that most protocols almost satisfy the requirements of each characteristic except Flexibility. As mentioned earlier, virtualization is the solution to the problem of Internet's inflexibility, therefore ISPs should take care that while designing new technologies Flexibility should not be neglected.

6. APPENDIX

Table 1
Internet Usage Statistics [2]

World Regions	*Int, Users 2015*	*Growth (2000-2015)*
Africa	330,965,359	1321.30%
Asia	1,622,084,293	1319.10%
Europe	604,147,280	474.90%
Middle East	123,172,132	3649.80%
North America	313,867,363	190.40%
Latin America	344,824,199	1808.40%
Oceania	27,200,530	256.90%
World Total	3,366,261,156	832.50%

References

[1] W. Stallings, Data and Computer Communications. Pearson, 2007.

[2] "World Internet Users Statistics Usage and World Pupulation Stats," Feb 2016. [Online]. Available: http://www.internetworldstats.com/stats.htm

[3] H. Orman, "The Morris worm: a fifteen-year perspective," in IEEE Security & Privacy, vol. 1, no. 5, pp. 35-43, Sept.-Oct. 2003.

[4] R. Tront, J.G.; Marchany, "Internet Security: Intrusion Detection & Prevention," Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 2004.

[5] C. C. Center, "Cert coordination center reports," The Froehlich/Kent Encyclopedia of Telecommunications, 1997.

[6] H. F. T. M. Krause, Information Security Management. CRC Press LLC, 2001.

[7] J. Chen, C. Wu, M. Jiang and D. Zhang, "A Review of Future Internet Research Programs and Possible Trends," Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on, Chengdu, 2010, pp. 1-4.

[8] I. Intrusion.com, "Deploying and tuning network intrusion detection systems," corporate white paper from the product managementand sales engineering group of Intrusion.com, 2001. [Online]. Available: http://www.bandwidthco.com/whitepapers/compforensics/ids/Deploying%20and%20Tuning%20NIDS.pdf

[9] T. Holland, "Understanding IPS and IDS: Using IPS and IDS together for defense in depth," SANS Institute InfoSec Reading Room, 2004. [Online]. Available: http://www.sans.org/reading_room/whitepapers/detection/understanding-ips-ids-ips-ids-defense-in-depth_1381

[10] "Intrusion detection software." [Online]. Available: http://www.tripwire. com/data-security/incident-detection/

[11] Y. Li and K. Jiang, "Prospect for the Future Internet: A Study Based on TCP/IP Vulnerabilities," Computing, Measurement, Control and Sensor Network (CMCSN), 2012 International Conference on, Taiyuan, 2012, pp. 52-55.

[12] J. Torres, M. Nogueira and G. Pujolle, "A Survey on Identity Management for the Future Network," in IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 787-802, Second Quarter 2013.

[13] J. Backfield, "Network security model," SANS Institute InfoSec Reading Room, 2008. [Online]. Available: http://www.sans.org/reading_room/whitepapers/modeling/network-security-model_32843