Chapter 1
A Review on Digital Sphere Threats and Vulnerabilities

Muthuramalingam S.
Thiagarajar College of Engineering, India

Thangavel M.
Thiagarajar College of Engineering, India

Sridhar S.
Thiagarajar College of Engineering, India

ABSTRACT

Digital Sphere is a global network which consists of all the resources that are required for the users, who connected with the digital network. It connects the entire world through the digital technologies. The digital network includes services, applications, and web page files. By connecting, to this network, people from one end in the world can able to communicate and share their knowledge across the world. Global communication and sharing may allow an unknown person which can disrupt the services. This chapter proposes a review on the threats and vulnerabilities related to the digital sphere network with value added security guidelines and countermeasures given to overcome such issues.

1. INTRODUCTION

A Global network with full of digital resources are provided to the requested users by connecting them to the digital world is called as digital sphere. It plays a significant role in the IT by shaping up into the reality, due to the increased dependency of users with the recent trends of evolving digital technologies. This sphere contains various varieties of data such as academia, media, social media, journalism, search engines and the computing technologies with enormous data centres, where the data retrieved by the sphere users in the form of web pages, applications, files and other such formats through the browsers with the help of protocols. Several organizations prefer to share or store their resources and run their business completely through digital sphere. By this, the customers of digital sphere are satisfied with variety of resources from various organizations. With the increased usage and the mobility of users, the services provided as applications, which is globally acceptable and accessible by the authorized users at anywhere and anytime.
The global acceptability and usability of the network consists of some security breaches which may lead to security attack by the unauthorized users. Cyber incidents are frequently occurred and rises costlier damage. The foremost problem and a challenging issue of the cyberspace (Lehto 2015) is that it has no borders or defined jurisdiction. It provides a open land for actors, who are playing a role of malicious access are left out without any judiciary actions and without being detected. Sophisticated number of recent cyber attacks and the attention given by the media to this arena shows that the importance of security in this sphere. However, the experienced person’s interest on the cyber space and the money invested by the industrialist on various aspects does not seem to become more secure. Since, digital sphere is a widely used cyber space and open for anyone, the analysis of various threats and attacks is essential to determine the appropriate countermeasures and guidelines.

The rest of the chapter covers Background, Threats, Vulnerabilities and attacks of digital sphere with Solutions and Recommendations, Future works and Conclusion.

2. BACKGROUND

The security in the cyber space needs to attain a desired state, in-order to grant secure access to the users who are able to travel along the cyber world without having worry about security breaches. The word cyber is originated from the Greek word kybereo it specifies- to steer, to guide, to control. At the end of the 1940’s, Norbert wiener an American mathematician, began to use the word cybernetics to describe computerized control systems. According to the wiener’s statement cybernetics deals with sciences that address the control of machines and living organisms through their communications and from the given feedback.

Major challenge drivers in the cyber world are time, data and network. In today’s world, (i) for a single minute, 2,16,000 photos are shared through instagram, (ii) Upload rate of video into the YouTube site increased in every 3 days (iii) Within a minute 70 new domains are registered and created 572 new websites (iv) At the same time face book, twitter, emails are also posing their increased rate in the internet (Gao, 2011). That is face book receives 1.8 million likes, 1, 80,000 more tweets taken by twitter and 204 million emails are sent and received by Gmail. and (v) Chatting over Skype are taken by the relatives and friends are taken is equivalent to 1.4 million minutes. Compared to the previous year’s Internet usage is drastically increased (Woollaston 2013).

According to the U.S News Briefs, unauthorized access to the network becomes a major issue than denial of service attacks. With the increased device usage and growth of cyber space, most of the people needs to access all the services through unauthorized privileges. The FBI investigating that the criminals having target to the selected regional offices computer systems including intrusions into public switched networks, major network intrusions, privacy violations and other crimes (IT Professional 2005).

Recent attacks performed by attackers are using the botnet a kind of unauthorized access. With the botnet, an attacker accessed the user database of an online website T35.net which is a personal and business hosting web services for many users. (Department of Justice 2010, Online).

Botnets are the background process that has collection of software agents that run automatically to command large number of computers that allow the criminals enter into the cyber network to conduct spreading of large scale infection program, spam mails, credential theft and personal information theft. That also performs the transformation of malware from one to other (Pinguelo and Muller, 2011).