iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** XI **Month of publication:** November 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue XI, November 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

The Survey on Cyber Security

Naveen K B[1], Pranav K U[2], Reshma Narayan[3]
SJC Institute of Technology, VTU, Karnatka, India

Abstract: ***In this paper we propose a survey on the cyber security. These days there are many crimes happening in the current world. And there are various researches are going these days and this paper provides the when did the research start and what are various risks in the cyber security.***
And the advantages of cyber security, disadvantages of cyber security and the in-depth description of the security.
KEYWORDS: cyber, security, attacks, availability, secrecy, maintenance.

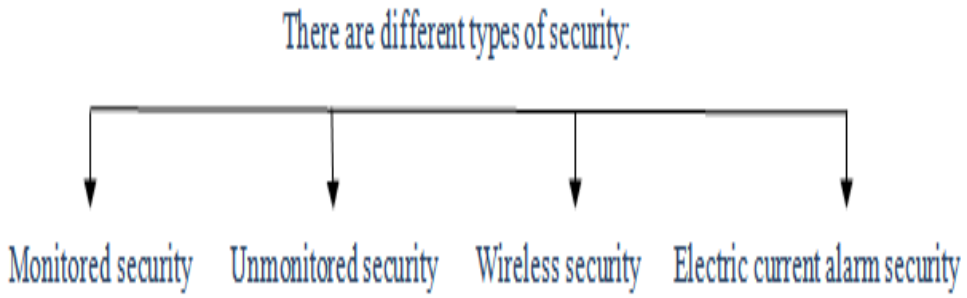
I. INTRODUCTION

A. Meaning of cyber

Related to the networks and internets involving in computers or computer networks .

B. Meaning of security

In Information technology, security is the protection of information assets through the use of technology, processes to protect networks .



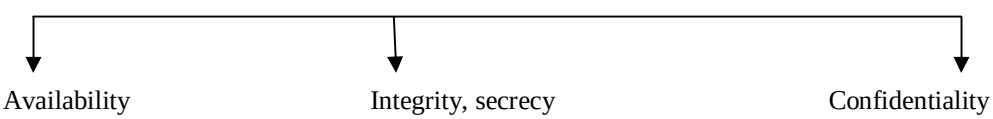
C. Meaning of cyber security

Cyber security also referred to as information technology security, in which it focuses on protecting the computers, computer networks and the computer programs. It is the body of technologies, processes which designed to protect the data from the attackers. Cyber security refers to a range in concepts including the practice protecting an organization's information, networks, computer, and resources against attacks from security and computer attacks.

In the cyber environment, the user's assets include connecting computing devices, personnel, infrastructure, applications, services and some of the telecommunication systems. Cyber security ensures the attainment and maintenance of the security properties of the user's assets against security risks in the cyber environment.

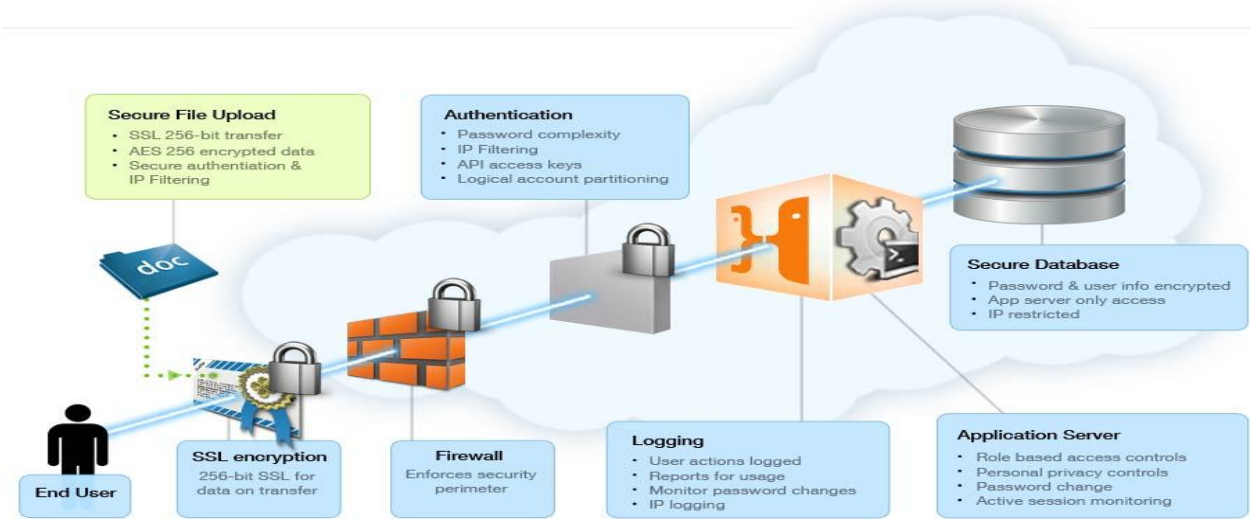
Cyber security ensures the attainment and maintenance of the security properties of the user's assets against security risks in the cyber environment.

The general security objectives are the following



Volume 4 Issue XI, November 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

II. DESCRIPTION



Nowadays , everything releases on the computers and the internet-communication (email , cell phone) , environment (digital cable , mp3's) , transportation (car engine systems , airplane navigation) , shopping (online stores , credit cards) , medicine(equipment , medical records) etc.., these all can be secured by an cyber security involves protecting that information by preventing , detecting and responding to attacks .The cyber security involves two types in the goal of protecting operation:

Corporative cyber security: availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failure with the goal of protecting an corporative operations and user's assets.	National cyber security: availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failure with the goal of protecting a nation's operations and user's assets.

In the cyber environment, the user's assets include connecting computing devices, personnel, infrastructure, applications, services and some of the telecommunication systems.And the most important aspects of cyber security is the evolving nature of security risks.

III. RISKS

There are many risks, among them very effective are viruses erasing your entire systems , someone processing into your system and alters the files, someone using your computers to attack others or someone stealing your email information and unauthorized purchases can made. But there are the steps you can make to minimize the chances.
The steps in protecting yourself to recognize the risks and become familiar with terminology:

A. Attacker or hacker

These terms are applied to the people who steal to take the weaknesses in software and computer systems for their own to gain information in the computer. Their intention is to motivate solely by curiously by their steal information. The results can range from mischief to malicious activity (stealing or altering information).

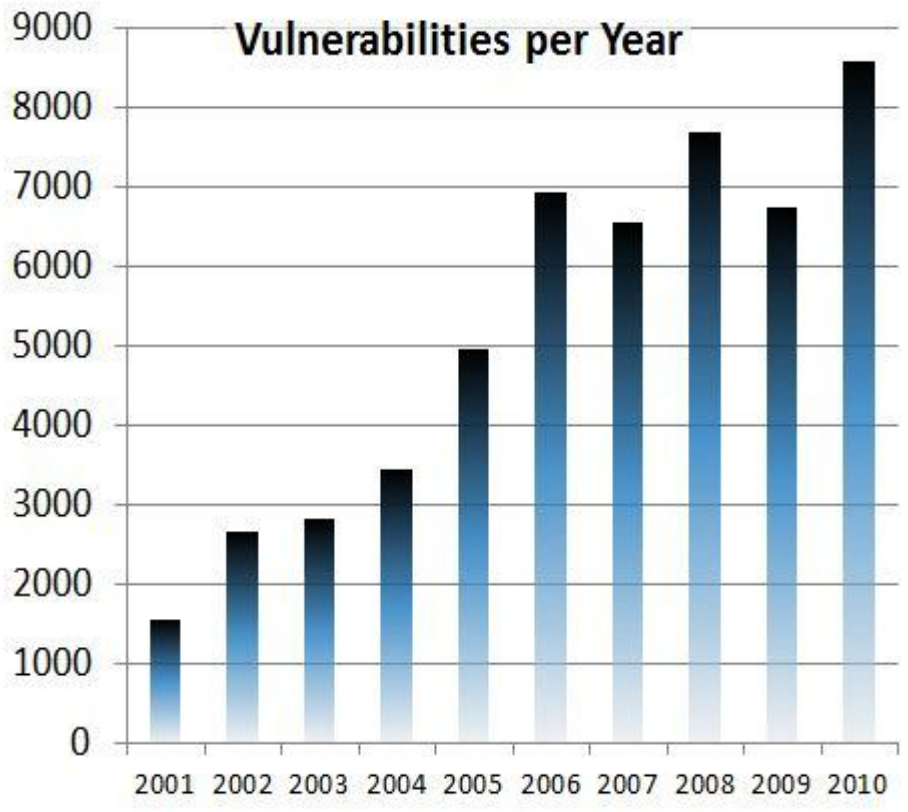
B. Malicious code

Malicious code, sometimes referred to be as malware, it includes any code that could be used to attack your computer. It might require you to do something has been infected, The malicious code will take to find and infect your computers. This code can propagates via email, websites or network based software systems.

Volume 4 Issue XI, November 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

C. Vulnerability

Vulnerabilities are caused due to the programming errors in software , attackers or intruders might have a chance of taking advantage of these errors to infect your computer , so it is very important to apply updates that address known vulnerability



Cyber security have some security standards which enable to practice safe security technique to minimize the number of successful cyber security attacks on the computer. Cyber security created recently because sensitive information is now stored on computers that are attached to the internet. Therefore, there is a need for information assurance and security

IV. HISTORY

Just a few decades ago, with the many malicious viruses and different types of aggressive malware out there today, it seems to think at the birth of networks. In fact, in early time regarding 'TALK TALK ' , this was cyber security didn't exist and it was first in a long line attacks that prompted computers scientists all around the world to take action and security measures.

YEARS	DESCRIPTION
In few decades ago	One of the most famous phreaker, was JOHN DRAPER, who made the practice of phreaking and was later he arrested and convicted due to repeated attacks on networks.
In 1980's	The 'worm' viruses became the first crime to be convicted under the 1986 computer fraud and abuse act. The worm case made a publicity after a number of early viruses had been unleashed, such a the 'brain' virus of 1986.
In 1989	Robert Morris unleashed the first computer worm on the internet, he created is widely acknowledged as the first computer worm, this is the self-propagating worm spread so aggressively and rapidly due to closing down of the internet. Other attacks have made bad sense in the internet. However the cyber crime has become more sophisticated and how security has developed in response.

In 1990's	The first viruses had went well, viral and dominates the other attacks. The virus Melissa infected many companies causing email systems around the globe. This leads to the development of the antivirus in order to prevent it. This played a huge role in forcing the awareness of computers users.
In 2000's	Rapidly the cyber –attacks became more targeted, most of us are targeted on the credit cards numbers nearly in between 2005 to 2007, Albert Gonzalez masterminded and stole information from cards of US retailer. This was the massive impact of security it losses the company from some million dollars, is the thing became more serious.
In modern days	The credit and debit cards are easily hacked and stole information and data from cards numbers. In a technical point of view, the criminals should understand that, in order to reach their goals, they would need to take an indirect route, in this case a third party supplies to the target. Using this criminals attack grabbed credit card numbers at the precise moment and memory of the system not encrypted.

Today we have reached the position in which the cyber crime is so sophisticated it seems almost impossible to prevent.

V. ADVANTAGES AND DISADVANTAGES

A. Advantages of cyber security

1) Cyber security protects systems and computers against viruses, worms, malware etc.., and other unwanted programs.
2) Cyber security improves security of cyberspace.
3) Increase in cyber defense, cyber speed.
4) Protect data and information of the company.
5) Protect networks and resources against attack from security.
6) Fight against computer hackers, intruders from being hacked and indentify theft.
7) Minimize computer crashes and freezing.
8) Gives privacy to the users of the computer.

VI. DISADVANTAGES OF CYBER SECURITY:

A. It will costly for average users.
B. Firewalls can be difficult to configure correctly.
C. Make the systems slower than before.
D. Incorrectly configured firewalls may block users from performing certain actions on the internet.
E. Need to keep updating the new software in order to keep security up to date for protecting.

VII. CONCLUSION

The cyber security risks are also widely growing field in the computer science and engineering in present days and most active research topics in the networks and the WSN mainly concentrates on how to achieve the security to the particular field .There are n number of researches are growing in this field and many algorithms are developed in this field and this paper provides the basic information regarding the what are risks and the types of attack.

REFERENCES

[1] Interpol. (2013). Cybercrime. Retrieved from http://www.interpol.int/Crimeareas/Cybercrime/Cybercrime/
[2] 2012 Data Breach Investigations Report conducted by the Verizon RISK Team (2012). Retrieved from http://www.verizonbusiness.com/about/events/2012dbir/
[3] Merriam-Webster Dictionary. (2013). Retrieved from http://www.merriamwebster.com/
[4] Changing the Game: Key findings from the PWC Global State of Information Security Survey 2013 (2013). Retrieved from http://www.pwc.com/
[5] Finding a Strategic Voice: Insights from the 2012 IBM Chief Information Security Officer Assessment (2012). Retrieved from http://www.ibm.com/ 6. Bilby, E. (2012, December 17). EU could make firms disclose network security breaches. Reuters. Retrieved from http://reuters.com/
[6] U.S. Department of Commerce, National Institute of Standards and Technology (2012). Computer Security Incident Handling Guide – Recommendations of

the National Institute of Standards and Technology (Special Publication 800-61, Revision 2). Retrieved from http://www.nist.gov/index.html

[7] European Network and Information Security Agency. (2006, May). A Step-ByStep Approach On How To Set Up A CSIRT. Retrieved from http://www.enisa.europa.eu/

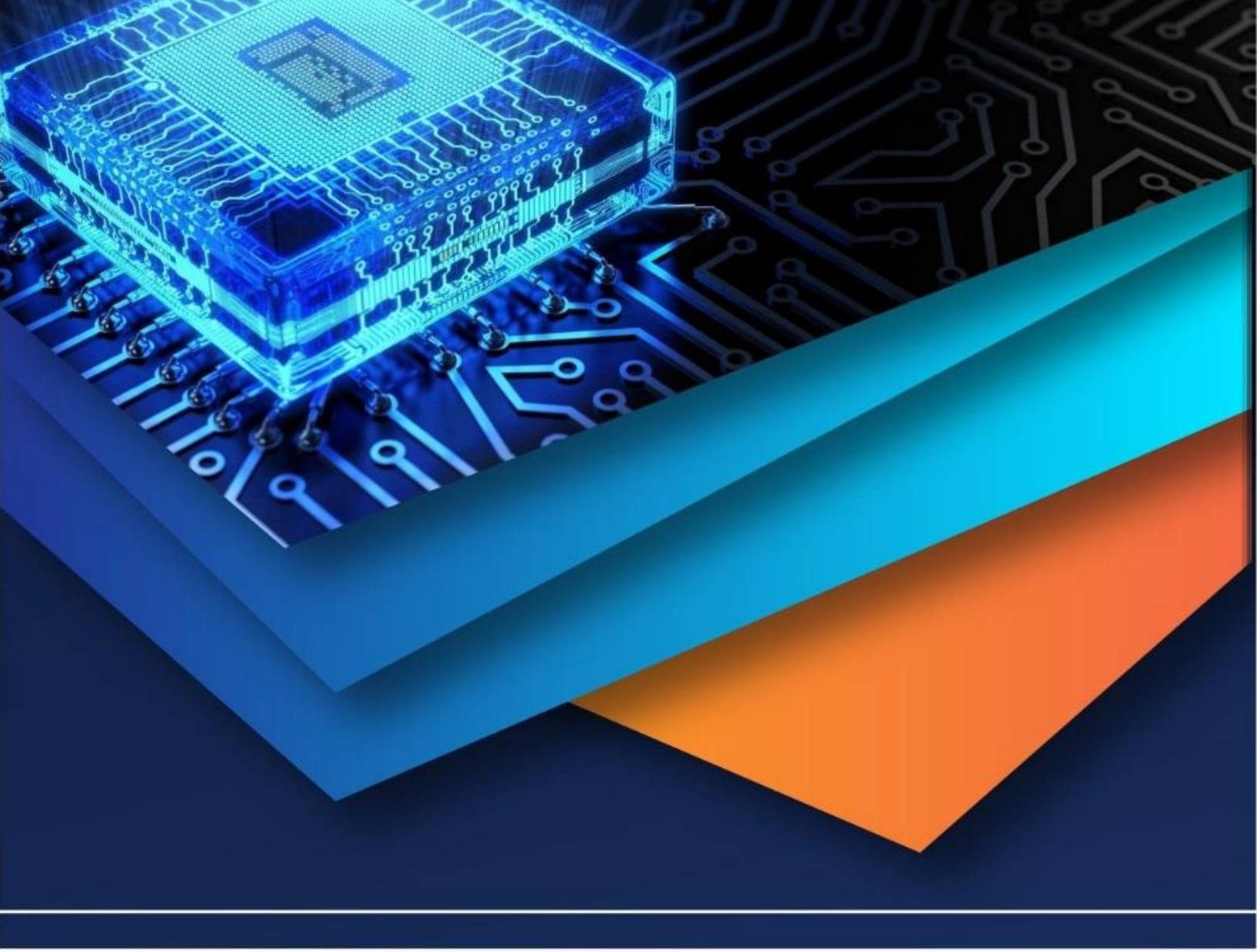
[8] European Network and Information Security Agency. (2012, December). Consumerization of IT: Risk Mitigation Strategies – Responding to the Emerging Threat Environment. Retrieved from http://www.enisa.europa.eu/

BIOGRAPHY

Naveen K B is a Student in the Computer Science & Engineering Department in SJC Institute of Technology, Chickballapur, affiliated to VTU. Pursuing Bachelor of Engineering (B.E) degree from VTU, Belgaum,. My research interests are Computer Networks (wireless Networks).

Pranav K U is a Student in the Computer Science & Engineering Department in SJC Institute of Technology, Chickballapur, affiliated to VTU. Pursuing Bachelor of Engineering (B.E) degree from VTU, Belgaum,. My research interests are Computer Networks (wireless Networks).

Reshma Narayan is an Assistant professor in the Computer Science & Engineering Department in SJC Institute of Technology, Chickballapur, affiliated to VTU. I received Master of Technology (M.Tech) degree in 2016 from VTU, Belgaum,. My research interests are Computer Networks (wireless Networks), Algorithms, web 2.0,Image Processing etc.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY