Cyber Security

Sweekriti Tomer, Sachin Saini
sweekirtithakur@gmail.com
sachin100494@gmail.com
CCSIT (TMU)

Abstract-As more business activities are being automated and an increasing number of computers are being used to store sensitive information, the need for secure computer systems becomes more apparent. This need is even more apparent as systems and applications are being distributed and accessed via an insecure network, such as the Internet. The Internet itself has become critical for governments, companies, financial institutions, and millions of everyday users. Networks of computers support a multitude of activities whose loss would all but cripple these organizations. As a consequence, cybersecurity issues have become national security issues. Protecting the Internet is a difficult task. Cybersecurity can be obtained only through systematic development; and techniques for countering the threats. Approaches it cannot be achieved through haphazard seat-of-the-pants methods. Applying software engineering techniques to the problem is a step in the right direction. However, software engineers need to be aware of the risks and security issues associated with the design, development, and deployment of network-based software

I. INTRODUCTION

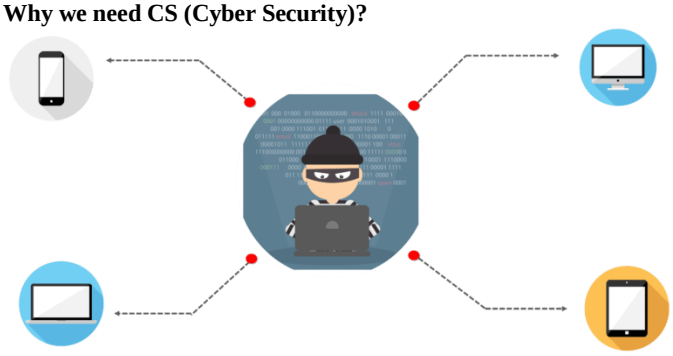
Cyber security or information technology is the area within it. its involvement to protect the computer system and to prevent unauthorized access of electronic data. its deals to protect software, hardware, networks and its information. its also protect computer system from theft or damage . in cyber security it is also known as computer security, the word authentication , authorization and auditing are like what comes in mind. authentication is a term used by server when it need to know who is accessing trying to access information or website that its present on the particular server. authorization is the process to verify access to a system has been granted.

Authentication may be done by many ways but the most common way to authenticate is the input of a username and password into a particular system. Another way of authentication can be done through the use of PIN.

For Example – A customer calls to tell the problem of troubleshoot to bypass Security to Technical Support the technical operator will ask about the pin that was set up on the client's device.

Authorization-Authorization is a term that a server uses to determine whether or not a client has permission to use a resource or access a file within that server.

Why we need CS (Cyber Security)?



Its can be rightfully told that today's generation is totally depend upon on the internet and we general users are almost ignored as to how those random bits of 1's and 0's reach securely to our computer system.

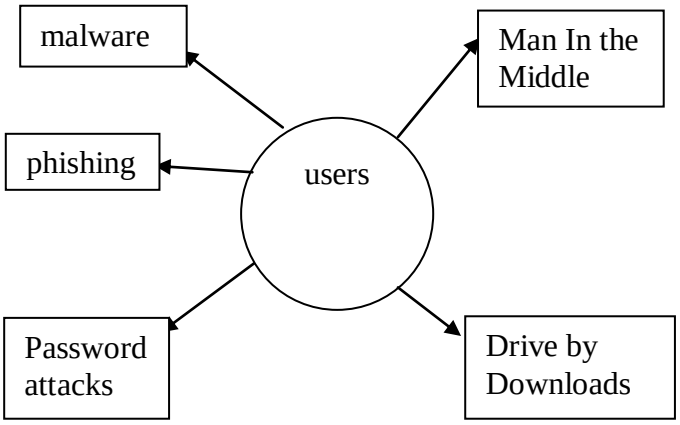
Types of Cyber Attacks in Computer System

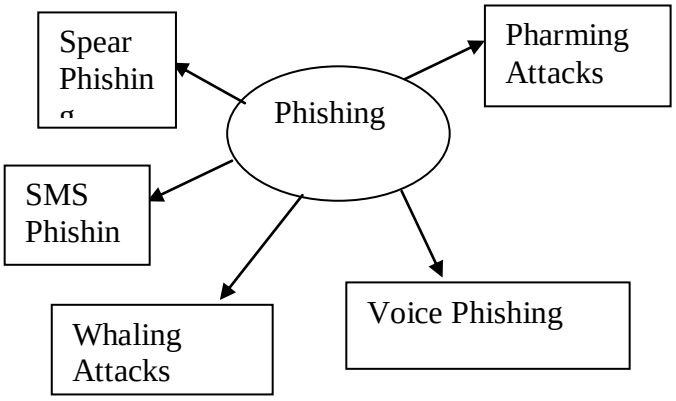
Malware

Malware

Malware is a type of software program which is harmful for computer system. This software is used to design by hackers to theft personal data of computers.

Causes of malware attacks:-





It can be various causes of malware attacks in computer system. Its main reason is downloading from internet. By using Interenet from which we download pictures ,content, videos by the help of downloading these things its very easy to come malware attacks in the computer system.

Ways to prevent from malware attacks

Songs, pictures etc is to download from trustable website. if you have to pay cost

But it will be better for your computer system.

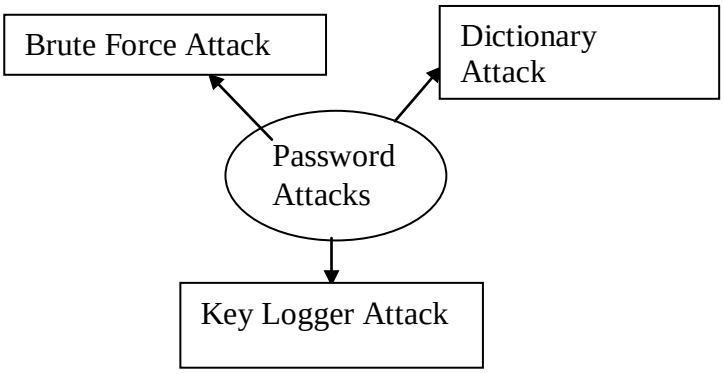
Phishing:

Phishing is type of cybercrime to theft official information like bank's account details , debit cards details. In phishing attacks the hackers send the emails to the customer to know about the information related to your bank account such as to enquire about the atm.

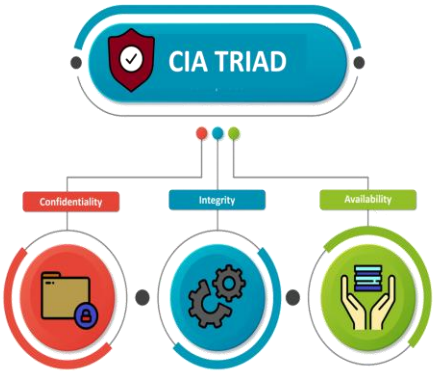
There are different types of phishing are –

Password Attacks

There are three types of password attacks



The CIA Triad



The CIA triad is an abbreviation for

C:-Confidentiality

I:- Integrity

A:-Availability

It is a design model to guide the companies and organizations to form their security policies. It is also called the AIC triad to avoid the confusion with Central Intelligence Agency(CIA). The

components of the triad are considered to be the most important and fundamental components of security.

1) **Confidentiality**

Confidentiality is to protect the personal information. Confidentiality means to kept a client's information between you and the client, and not tell others including co-workers, friends, family, etc.

2) **Integrity**

Integrity, in the circumstances of computer systems, indicate the methods of ensuring that data is real, accurate and safeguarded from unauthorized user to modify.

3) **Availability**

Availability, in the circumstances of a computer system, indicate the ability of a user to access the information or resources in a specified location and in the correct form

Conclusion

The future of cybersecurity will in one sense be like the present: hard to define and potentially unbounded as digital technologies interact with human beings across virtually all aspects of politics, society, the economy, and beyond. We built this project on the proposition that both the "cyber" and the "security" components of the concept "cybersecurity" will be in rapid motion during the back half of the 2010s. That motion is more likely to accelerate than to decelerate, but its direction varies widely among our scenarios. That is no artifact of our research process; it is the central point of the work. We hypothesize that, at some point in the not-so-distant future (if it is not already true at present), cybersecurity will be recognized widely as the "master problem" of the internet era. That puts it at the top of any list of problems that societies face, more similar to a nearly existential challenge like climate change than to an operational concern that technology companies have to manage. That recognition also will bring major changes to how human beings and digital machines interact. One purpose of these five scenarios is to point to some of the changes that may result.

References-

[1] https://www.edurka.co/blog/what-is-cybersecurity/
[2] https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html
[3] https://www.itkhj.com/phishing-hindi
[4] https://resoure.elq.symantec.com/