Glimpse on various Kinds of Security Threats

Panara Bhumita[1] Arpan Patel[2]
[1,2]Student
[1,2]Department of Computer Engineering
[1]Government Engineering College, Rajkot India [2]Government Engineering College, Gandhinagar India

Abstract— Basic introduction to what threats are, specifically security threats. Various types of it along with how they effects computer system. Explaining how encryption can be the key for solution.

Key words: Security Threats, Sensitive Data Exposure, Sensitive Data

I. INTRODUCTION

In terms of computer security, threat can be anything that contain the capability of damaging computer system. It harms the system in various ways causing the system down, malfunctioning, unauthorized access, can cause serious problems in network also and many more hazardous outputs. Threat is basically a probability i.e it may occur or may not occur [1].

II. HOW SECURITY THREATS EFFECTS OUR COMPUTER SYSTEM

At First, what is the need to deal/afraid of security threats? Why? The answer is increasing demands of protected documents/system, nowadays most of the company uses computer for storing their databases and other confidential documents. Organizations that has a computer system and sensitive information would try to protect that information from being destroyed, hacked or its integrity is maintained or not [2]. Any kind of variations such as data being stole and unauthorized changes or rather destroy of data causes huge damage and can bring the security of whole nation in danger so in certain areas such as army, government security and defense, all kinds of documents of government must be protected from all kinds of treat. All it ends at the security of our data must be maintained resolving various effort [3].

As a result to protect the information and maintaining its integrity and security from being stole one has to be aware of basic kinds of threats and its harmful effect on the systems. Below given is list of basic security threats.

III. VARIOUS KINDS OF SECURITY THREATS ARE

- Trojan
- Virus
- Worms
- Spyware
- Adware

IV. WHAT IS SENSITIVE DATA?

Sensitive data encompasses a wide range of important information that's needs to be protected to safeguard the privacy and security of an individual or an organization.

The sensitive data can include

- Banking information
- Health information
- Personal Information (DOB,SSN)
- User accounts/passwords

V. SENSITIVE DATA EXPOSURE

Many web applications do not properly protect sensitive data, such as credit cards, personal information and authentication credentials. Hence, attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Therefore Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

VI. HOW IS SENSITIVE DATA EXPOSED?

There are mainly three ways by which data is exposed. They are

A. Intrusion

Intruders can gain access To any of your sensitive data through a weakness in your computer system. To protect against this, keep your operating system updated, and use virus protection and strong passwords.[2]

B. Phishing

This is a clever method of extracting information from unsuspecting individuals. For example, an e-mail, designed to look like as if it originated from a reputable company, usually a bank or online store, will tell you that there is a problem with your account with attached links. If links appear in this kind of e-mail message, never click on them regardless of how "believable" they seem or who the source is. If you have an account with the organization, it's better to call your service representative and verify the authenticity of the e-mail. If it is legitimate, ask to complete the process by phone. This eliminates the need to send your sensitive data over an unprotected network connection.[3]

C. Social Engineering

Many times scammers attempt to gather sensitive information, such as birthplace or mother's maiden name, by posing as a representative of a legitimate organization.[4]

You should always be wary of unsolicited requests from your bank or financial institution in which you are asked for information that could potentially be used for fraudulent purposes.

IS&T never asks you to provide your username and password in e-mail or over the phone.

D. Potential Impact

The impact of the data exposure majorly depends on the type of data that has been exposed. Hence the potential of the danger reflects the sensitivity of the data, among which the major implications can be:

- Financial loss
- Identity hijacking
- Decreased brand trust (for business)

E. Preventing Sensitive Data Exposure

The first thing you have to determine is which data is sensitive enough to require extra protection.

For example, passwords, credit card numbers, health records, and personal information should be protected. When this is done, the following points need to be considered.[5]

- The data is never stored in clear text.
- The data is never transmitted in clear text. Example between database and server, or over the internet.
- Minimize the data surface area, i.e the storage and transmission of the sensitive data should as less as possible.
- The algorithms used to encrypt the data are considered strong enough.
- The generation of the keys is secure.
- Browser headers are set to not cache when the sensitive data is presented to end-user.

In addition to above threats, various other types of threats are mentioned below:[6]

- Injection.
- Broken Authentication and Session Management.
- Cross site Scripting (XSS).
- Insecure Direct Object References.
- Security Misconfiguration.
- Missing Function Level Access Control.
- Cross Site Request Forgery(CSRF).
- Using components with known vulnerabilities.
- Unvalidated Redirects and forwards.

Above details describes how the different kinds of threats are there that can harm the computer system in various drastic ways.

VII. CONCLUSION

To avoid security problems such as above described one somewhere or other encryption is helpful up-to great extent, using encryption makes data more secure and reduces the burden of security during transmission.

Because if a data that is strongly encrypted with standard or reliable algorithms that are difficult to trace the original data, such data when sent through network if get hacked by unauthorized parties then also the confidentiality of data is maintained unless they get succeed in guessing the encryption technique used while encrypting original data or rather they are capable of decrypting the data in a right manner.

Note: What is Encryption and its various algorithms along with other newly derived algorithm is mentioned in our next paper namely "Basics of AES along with newly derived encryption logics."

ACKNOWLEDGEMENT

We would like to articulate our deep gratitude to my thesis guide Asst. Prof. S. M. Bhanderi who has guided us in our paperwork. I really appreciate the keen interest for encouraging all time for our paperwork to Associate Prof. Kajal S. Patel, Professor and Head of Computer Engineering Department of Government Engineering College, Rajkot, Gujarat.

REFERENCES

[1] www.nationaldefensemagazine.org
[2] http://web.mit.edu/infoprotect/docs/protectingdata.pdf
[3] http://web.mit.edu/infoprotect/docs/protectingdata.pdf
[4] http://web.mit.edu/infoprotect/docs/protectingdata.pdf
[5] https://blog.detectify.com/2016/07/01/owasp-top-10-sensitive-data-exposure-6/
[6] https://www.owasp.org/index.php/Top_10_2013-Top_10