International Journal of Advanced Research Methodology in Engineering & Technology,
Volume 1, Issue1, December 2016

General Security Threats In Digital Platforms

Sujay B.N
Dept. of Computer Applications, Dayananda Sagar College of Arts, Science and Commerce, Bangalore, India.
Email: sujaybagur5@gmail.com

ABSTRACT

Information security is one of the major concerns in present day scenario. Everything is on the digital platform these days, which makes life simpler. But, it has a dark side as well. Information being put in digital platform makes it vulnerable and mostly easy to slide on to the hands of wrong people. People, who use the information for wrong reasons. The importance of the information security is generally neglected by normal a person who does not have any computer knowledge and often tend to make mistakes which may haunt them back with very bad episode. The paper describes the general security threats, requirements and probable solutions.

Key Words: Digital signature, Dark web, Adware, DoS, OTP

1. INTRODUCTION

We live in a world where information is everything and we call it as "The information era". Information is actually very important constraint for any organisation or an individual or a country. When it comes to securing the data, an organisation should take any measures it needs and most of them will. There are organisations and people who steal the individual data and use it for different reasons which one can't imagine.

Everyone these days have a smart phone in their pockets and most of the people are the active participants of the social media such as facebook and other platforms, by openly exposing the full control of their digital life to the people who are waiting for it.

With the growth of technology, we also have created a back-door for those threats for our data. A simple Smartphone is well enough to steal much data from an individual to fake the identity of the victim. There are places in dark web where people can buy the identity of some other person and live with it, which indeed is the identity of normal people like us. It is a place where whistleblowers get their resources to get their job done. Since the technology has become so advanced that all that is needed is a digital signature of a person to confirm the identity, which makes one's identity vulnerable. In dark web, criminals pay millions and millions of dollars just to steal the victim's identity and live the life in their names.

Advertising companies are also the organizations that need every individual's personal and intimate information. They are the source of income for the social platforms such as Facebook, Google and other organizations. "Every little footprint that we create on a digital platform matters more than one can imagine"

For example, if a pregnant women search something related to pregnancy, within an hour, her browser will be filled with ads related to pregnancy, she might also get calls/text messages regarding those advertisements.

Everyone needs the information about people and they are getting what they want since the technology is making the platform for them. They are getting the information weather we want them to have the information or not and they are using it for their profits. The threat is not only for normal people but many organisations and countries as well. There are different kinds of threats for information which is meant to be confidential.

2. SECURITY THREATS

There are different kinds of security threats in a typical web based platform, which are often neglected by normal people. These threats generally seem unimportant and that is where the attackers get their advantage.

Different types of tools the attackers use in order to get the information stolen from the victims are as follows.

Viruses: A virus is a computer program that is designed to attack on particular part of software, which can also be designed to get some actions done from the system software such as operating systems.

Worms: worms are generally transferred from one device to the other by USB sticks, which often used by the attackers without getting into the networks. This gets the work done without the victim getting connected to the internet.

Trojans: Trojans appear harmless in the beginning but it will get the job done with silence, and the user won't even get to know it. These are considered as one of the most effective tools used by the hackers to steal the data of an individual.

Adware: These are the pop-up messages that appear on browsers which are relevant based on the user's previous browsing patterns

3. SECURITY REQUIREMENT

The typical security requirement is to secure one's information completely. The normal users usually don't understand the threats they have. So, all platforms should be encrypted in such a way that there is no backdoors for the attackers.

Integrity: This is way more important, since failure to assure integrity may lead to:

a. Misappropriation of resources, i.e. someone modifying ownership records and then claiming ownership of a resource that does not belong to him, her or it (organisation).

b. Denial of service, which is an activity that results in a service provider's inability to operate within the parameters of their goal.

c. Theft of service, i.e. access to it without paying anything to the provider, which is one indeed the real threat.

Integrity concerns are more challenging as well, since in contrast to confidentiality-assurance mechanisms, the assurance of integrity has to be given in a situation of massive resource sharing.

4. RESOURCE SHARING

Big organizations usually possess thousands of computers connected together and many employees work all together. Those are generally connected by intranet network in which everyone shares single main resource. This again puts the individual employee's security. In order to overcome this situation, the organizations provide firewall where each computer can be accessed by unique ID and password.

Password protection is the obvious solution. A user has to authenticate him or her by typing in a password in addition to their account name. If the password does not match the one kept on the user database, access is denied. The problem is that a attacker could try to guess the password by fitting various bits and pieces that gormless users tend to make their passwords from: first name, date of birth, etc. So it is logical thing to try and limit the number of times a terminal allows a person to log in unsuccessfully. After three unsuccessful attempts the account is blocked and the true owner will have to contact the system administrators, authenticate him- or herself by other means (photo ID, for instance) and get the password reset.

Threat: denial of service. This generally put any organization or an individual puts in a lot of risk and frustration where the day's work is to be terminated. This usually incurs a bad loss.

Solution: Instead of blocking the account, it can be put in freeze for a particular amount of time, which is enough time for the original user to get notification and prevent the potential attack.

This may not be sufficient. The attacker can use a parallel strategy: try account 1 then 2, by the time he/she has tried all once, account 1 will be unfrozen so no delay will take place at all. If the purpose of the attack is to break into any account, no matter which (a reasonable scenario), then he/she will meet with no effective security barrier.

Advanced Solution: There can be one more password. It automatically increases the security by a layer. This ensures the security very well, it takes pretty long time for an attacker to break and enter the account of the victim.

Here the important property of the solution is that the account can only be frozen if it is already part-broken into. This takes a lot of time and the gain for the attacker is negligible: all he or she can achieve by fitting a first password to one account is win three chances (or so) to fit the second password, which is not likely to be

successful. So the cost of this exercise far outweighs the possible gain, and the attacker simply will not do it.

The user will have to be notified in case of any unsuccessful attempts to login to their account. OTP login is one other option and secured way of logging in.

CONCLUSION

Since the information is needed to be secured in all the way through normal life in this information era, it is inevitable for a person to use his details at least some point of their digital life. Some of the measures to be taken from the administrations in case of organizations, which they generally aware of and usually are one step ahead of the attackers. In case of the individuals, one should be very careful while they are browsing, and providing the information in the internet.

It is well accepted and very safe to use the anonymous and safe applications such as Tor browsers for personal browsing, which uses tor network and generally the Advertising companies will have no way to track browsing patterns of a person and send pop-ups.

In any case, either it is an individual or an organization, securing the data is highly recommended and it is wise to learn threats for information security in the internet and other digital platforms. It is also recommended to educate the normal people about these security threats, so that the style of their activity in the digital world changes for good.

REFERENCES

[1] Md Alamgir Hossain , Debabrata Samanta and Goutam Sanyal , “Eye Diseases Detection based on covariance”, International Journal of Computer Science, Information Technology, & Security (IJCSITS) , pp. 376-379, Vol2, No.2 April 2012 ISSN: 2249-9555 (Online), 2250-1355 (Print).

[2] Vijayakumar C M, Kumudavalli.M.V, Bipradip Roy, Rohit Kumar Singh, "An Overview of P2P",International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 5 , No.1 Pages : 14 - 17 (2016).

[3] Syed Khutubuddin Ahmed Khadri, Debabrata Samanta, Mousumi Paul, ” Novel Approach for Message Security”, International Journal of Information Science and Intelligent System (IJISIS), pp. 47-52,Volume 3, Number 1, 2014.

[4] Journal of Information Security and Applications by Anthony T.S. Ho

[5] Why Information Security is Hard – An Economic Perspective Ross Anderson University of Cambridge Computer Laboratory, JJ Thomson Avenue, Cambridge CB3 0FD, UK

[6] J Anderson, ‘Computer Security Technology Planning Study’, ESD-TR-73-51, US Air Force Electronic Systems Division (1973) http://csrc.nist.gov/publications/ history/index.html

[7] C Shapiro, H Varian, ‘Information Rules’, Harvard Business School Press (1998), ISBN 0-87584-863-X

[8] A taxonomy for attack graph generation and usage in network security By Kerem Kaynar, German Turkish Advanced Research Center (GT-ARC), TU Berlin, Ernst Reuter Platz 7, 10587 Berlin, Germany

[9] InfoSecurity Magazine: Scariest Search Engine on the Internet Just Got Scarier

[10] Documentary : Inside the dark web