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

Prevention of hacking in smart phones

Kavin kumar .B, C.N.Vanitha

Abstract

Our world has been facing a large amount of thread due to the insecurity in all the electronic devises. In this method the smart phone will be having a application which the phone keeps all its data in it so when someone try to hack it will be prevented. In general Hacking is like laying a bridge between the computer of the hacker and computer which is under attack .This bridge is a way by which the data is been taken from the other .So if we are able to keep the defiance mechanism which will send a virus, whenever a bridge is laid to steal the data of someone in unauthorized manner .Since when a connection is between two computer both computers can exchange any information. So the computer which is under attack can sends a virus to the hackers computer so that all the data will be infected with the virus .The virus has a tracking software or a program which can be stored in the hackers computer even the computer of the hacker have an anti virus. When the person who's computer can get the information that his / her computer was under attack and they can get the location of the hacker easily.

Key word: hacking, smart phone , prevention .

Introduction

Computer hackers are unauthorized users who break into computer systems in order to steal, change or destroy information, often by installing dangerous malware without your knowledge or consent. Their clever tactics and detailed technical knowledge help them access information you really don't want them to have.

Since a large number of hackers are self-taught prodigies, some corporations actually employ computer hackers as part of their technical support staff. These individuals use their skills to find flaws in the company's security system so that they can be repaired quickly. In many cases, this type of computer hacking helps prevent identity theft and other serious computer-related crimes. Computer hacking can also lead to other constructive technological developments, since many of the skills developed from hacking apply to more mainstream pursuits. For example, former hackers

Classifications

Several subgroups of the computer underground with different attitudes use different terms to demarcate themselves from each other, or try to exclude some specific group with whom they do not agree.

Eric S. Raymond, author of The New Hacker's Dictionary, advocates that members of the computer underground should be called crackers. Yet, those people see themselves as hackers and even try to include the views of Raymond in what they see as a wider hacker culture, a view that Raymond has harshly rejected. Instead of a hacker/cracker dichotomy, they emphasize a spectrum of different categories, such as white hat, grey hat, black hat and script kiddie. In contrast to Raymond, they usually reserve the term cracker for more malicious activity

The three phases of malware attacks

Typically an attack on a smart phone made by malware takes place in 3 phases: the infection of a host, the accomplishment of its goal, and the spread of the malware to other systems. Malware often use the resources offered by the infected smart phones. It will use the output devices such as Bluetooth or infrared, but it may also use the address book or email address of the person to infect the user's acquaintances. The malware exploits the trust that is given to data sent by an acquaintance.

Infection

Infection is the means used by the malware to get into the smart phone, it can either use one of the faults previously presented or may use the gullibility of the user. Infections are classified into four classes according to their degree of user interaction:

Monetary damages

The attacker can steal user data and either sell them to the same user, or sell to a third party.

Damage

Malware can partially damage the device, or delete or modify data on the device.

Concealed damage

The two aforementioned types of damage are detectable, but the malware can also leave a back door for future attacks or even conduct wiretaps.

Spread to other systems

Once the malware has infected a smart phone, it always aims to spread one way or another:

It can spread through proximate devices using Wi-Fi, Bluetooth and infrared;

It can also spread using remote networks such as telephone calls or SMS or emails.

EXISTING WORK

Gurpreet K. Juneja proposes :

The state of security on the internet is bad and getting worse. One reaction to this state of affairs is termed as Ethical Hacking which attempts to increase security protection by identifying and repairing known security weakness on systems owned by other parties. As public and private organizations migrate more of their critical functions to the Internet, criminals have more opportunity and motivates or encourages to gain access to sensitive information through the Web application. Thus the need of protecting the systems from the inconvenience of hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems. So, Ethical hacking is an assessment to test and check an information technology environment for possible weak links and weakness. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. This paper describes what ethical hacking is, what it can do, an ethical hacking methodology as well as some tools which can be used for an ethical hack.

Michael Bachmann proposes:

Issues concerning computer security have increased in recent years and cyber security has become a top priority for many governments, organizations, and industries. Unfortunately, the attention showed to cyber crime issues has focused primarily on the technical view of computer crime. Today, our knowledge about the persons behind the keyboards remains a puzzle. The current study focuses on one particular subgroup of cyber criminals, the illicit computer hackers. In particular, two personality characteristics commonly regard to hackers, strong preference for rational decision-making processes .

I.P.L. Png, Candy Q. Tang, Qiu-Hong Wang proposes:

They analyzed the strategic interactions among end-users and between end-users and a hacker. They show that security efforts by end users are strategic substitutes. This explains the inertia among end-users in taking precautions even in the face of grave potential consequences. Next, they analyzed the direct and indirect effects of changes in user fixing cost and the rate of enforcement against hacking. For instance, a reduction in user fixing cost would directly lead users to increase fixing effort. However, that would make them less attractive targets, and so induce less hacking.

Ms. Mayuri S. Bawane andMr. Chetan J. Shelke proposes:

In this work, the explanation is about how the computer's containing valuable information is being unsecured and the techniques to make it secure. This technique contains information on the tools and skills a hacker uses to hack the computer systems and networks. This work proposes the study of hacking; as the cost of hacking attacks continues to rise, many of the businesses have been forced to increase spending on network security.

However, hackers have also developed new skills and techniques that allow them to break more complex systems. Hacking involves affecting the computer system with virus. This work describes the various techniques of hacking and cracking, also how they work. . Today, however, hacking and hackers are most commonly associated with

malicious programming attacks on the Internet and other networks.

Proposed system:

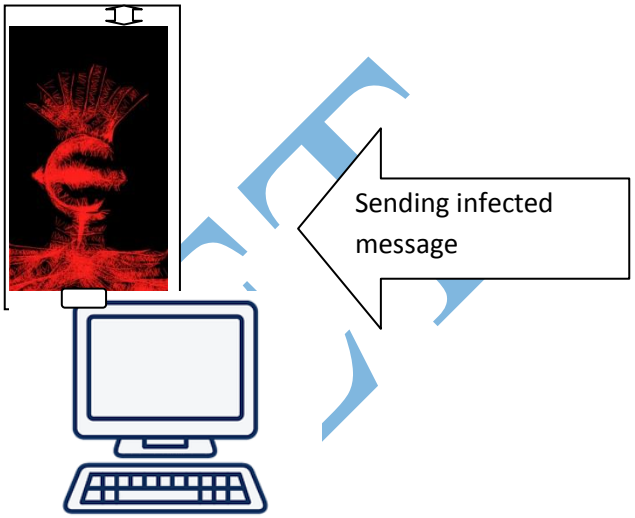
Our world has been facing a large amount of thread due to the insecurity in all the electronic devises .Our world is now in the digital era everything in this world is computerized , everything has come into our hand in the name of smart phone. Smart phone has replaced many difficult work in the computer and we keep more data in the phone .Many of the confidential data are stored in the smart phone in order to keep them safe since now a days the risk of computer hacking has increased . Additional to that the person who hacks the computer can escape easily by using a fackip address, when we try to trace the person it is difficult to find. But now even the smart phone has been hacked.

So here my idea has a solution in preventing the hacking and we can able to track the person who tried to hack or who hacked. IN this method the smart phone will be having a application which the phone keeps all its data in it so when someone try to hack it will be prevented. In general Hacking is like laying a bridge between the computer of the hacker and computer which is under attack .This bridge is a way by which the data is been taken from the other .So if we are able to keep the defiance mechanism which will send a virus, whenever a bridge is laid to steal the data of someone in unauthorized manner .Since when a connection is between two computer both computers can exchange any information. So the computer which is under attack can sends a virus to the hackers computer so that all the data will be infected with the virus.

The virus has a tracking software or a program which can be stored in the hackers computer even the computer of the hacker have an anti virus. When the person who's computer can get the information that his / her computer was under attack and they can get the location of the hacker easily.

This can be also used in computer. In phone when we get a message which is not required or which is found harmful for the data immediately triggers the defiance mechanism and it starts to work .Hacking a phone can be generally categorized in these steps

- Through messages, email, mms etc...
- hacking through the network system e.g.: through wifi connection



Mobil user
hacker's device

CONCLUTSON

Now a days many inportant informations are stored in the phone since it is easy to carrry ,many important deatiles are send through the phone . as the number of thread increases in the security of phone . this helps us to feel free from that problem because when the information is taken the information is affected with a virus so even if the virus is been removed by the anti virus the information will be not proper and the persons location will be found .

References

[1]Gurpreet K. Juneja **ETHICAL HACKING: A TECHNIQUE TO ENHANCE INFORMATION SECURITY** Vol. 2, Issue 12, December 2013

[2]Michael Bachmann1 **The Risk Propensity and Rationality of Computer Hackers**

International Journal of Cyber Criminology Vol 4 Issue 1&2 January - July 2010 / July - December 2010

[3]I.P.L. Png, Candy Q. Tang, Qiu-Hong Wang **Hackers, Users, Information Security** May 2006

[4]Ms. Mayuri S. Bawane and Mr. Chetan J. Shelke **ANALYSIS OF INCREASING HACKING AND CRACKING TECHNIQUES** Volume 3, Issue 2, February 2014