ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Protection of Smartphone, Personal Computer and Other Similar Devices from Virus Infections

Sudhakar Singh, P.K. Khare, J.M. Keller, P. Mor, M.K. Pathak

Research Scholar, Dept. of Physics and Electronics, RDVV, Jabalpur (M.P.) And Associate Professor, Dept of Physics and Computer Science, Sardar Patel College of Technology, Balaghat (M.P.), India

Professor, Dept. of Physics and Electronics, RDVV, Jabalpur (M.P.), India

Professor, Dept. of Physics and Electronics, RDVV, Jabalpur (M.P.), India

Scientific Officer, Dept. of Physics and Electronics, RDVV, Jabalpur (M.P.), India

Scholar, Dept. of Physics and Electronics, RDVV, Jabalpur (M.P.), India

ABSTRACT: The smartphones are particularly vulnerable to viruses due to their versatile communication capabilities and intermittent network connectivity. As a result, the viruses can easily spread out and cripple both the smartphone users and the cellular and telephony infrastructures. Once malware enter to the system they start to find the vulnerabilities within the operating system then perform unintended operation in the system. Most of the malwares basically attack on performance of the system, data integrity and privacy. They also play the major role in denial of service attack. These malware are also capable to infect other executable files and data. Malwares depending on their behaviour collect the information about host and harm the host computer without consent of the owner. Generally a computer virus causes damage to the host machine. The damage can be done to a number of different components of the computers operating and file system. These include system sectors, files, macros, companion files and source code. The always connected world of internet is a soft target for viruses. Viruses use internet connectivity to spread across the world faster and create havoc. Smartphones have recently become increasingly popular because they provide all in one convenience by integrating traditional mobile phones with handheld computing devices. However, the exibility of running third party softwares also leaves the smartphones open to malicious viruses. In fact, more than hundreds of smartphone viruses have emerged in the past few years, which can quickly spread through various means such as SMS/MMS, Bluetooth and traditional IP based applications. Therefore, protection of smartphone, user computer or an organization computer network from viruses is very important task.

KEYWORDS: Malware, Smartphone, Antivirus, Bluetooth, Firewall, Wi-Fi, Privacy

I. INTRODUCTION

Recently, mobile handsets are becoming more intelligent and complex in functionality, much like personal computer. Moreover, mobiles are more popular than personal computer and are being used more and more often to do business, access the Internet, access bank accounts and pay for goods and services. This resulted in an increased number of criminals who wants to exploit these actions for illegal gains. Today's malware is capable of doing many things, such as stealing and transmitting the contact list and other data, locking the device completely, giving remote access to criminals, sending SMS (Short Message Service) and MMS (Multimedia Messaging Service) messages etc. Mobile malware causes serious public concern as the population of mobile phones is much larger than the population of personal computer. Today due to flexible communication, computation capabilities and their resource constraints, mobile handsets are glued victim to malwares. A mobile handset can be attacked from the Internet since mobile are Internet endpoints or it can be infected from compromised personal computer during data synchronization and also it can have a peer mobile attack or infection through SMS/MMS and Bluetooth.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Computers are an integral part of everyday operations, organizations depend on them. A computer system failure will have a critical impact on the organization. Computer security entails the methods used to ensure a system is secure. Subjects such as authentication and access controls must be addressed in a broad terms of computer security. Today's computers are connected to other computers in networks. This then introduces the term network security to refer to the protection of the multiple computers and other devices that are connected together. In our research paper we consider only those threats which is posed by malware. Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victims data, applications or operating system or otherwise annoying or disrupting the victim. Malware is one of the major security threats in computer and network environment.

In the beginning, computers were not connected together very well and computer viruses spread extremely slowly. Files were transmitted via BBS(Bulletin Board systems) or diskette. As a result the transmission of infected files and boot sectors was geographically limited. However, as soon as connectivity increased, mostly by the use of computers in the workplace, the boundaries of computer viruses widened. First there was the local area network (LAN), then there was the wide area network (WAN) and now there is the Internet. The extensive use of e-mail has also contributed to the meteoric rise in the number of macro virus incidents. We are now living in a society in which global technology has taken the forefront and global commerce is driven by communication pathways. Computers are an integral part of this technology and so the information they contain also becomes global. Consequently, it is much easier to get a virus today than it was a few years ago. However, the types of viruses that are common today are different than those that were common two years ago. Common threat to computer system and network is malware which includes viruses, worms, Trojan and others bad type of malicious software. Viruses and Trojans are possibly the most damaging vulnerabilities that a computer system may face today. Viruses and Trojans have the ability to damage computer systems to a great extent. A virus is a small, self-contained piece of computer code hidden within another computer program. Like a real virus, it can reproduce, infect other computers and then lie dormant for months or years before it strikes. Figure 1 shows connectivity between different Electronics devices and table 1 shows comparison between Biological and Computer virus**[1][3]**.

Figure 1: Communication between different Electronics Devices

Table 1: Difference between Biological and Computer virus

Biological Virus	***Computer Virus***
Consists of DNA (Deoxyribo Nucleic Acid) or RNA(Ribo Nucleic Acid) strand surrounded by protein shell to bond to host cell.	Consists of set of instructions stored in host program
No life outside of host cell.	Active only when host program executed.
Replicates by taking over host's metabolic machinery with its own DNA/RNA metabolic machinery.	Replicates when host program is executed or host file is opened.
Copies infect other cells.	Copies infect (attach to) other host Programs.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

II. RELATED WORK

The computer systems used by business and home users have developed tremendously over the past ten years. Both system architecture and the way we use computers is totally different from the late 1980 and early 1990. But the virus problem is still there, worse than ever. As a matter of fact, viruses and worms have been able to adopt and benefit from the new features that modern computer environments offer. Virus strains do not evolve as they spread. Some argue that viruses are primitive computer based life forms, but they certainly lack one of the fundamental capabilities of living creatures to produce descendants that are slightly more adapted to a new environment than their parents. This means that as viruses cannot adapt to new system architectures, they become extinct when the number of suitable host systems decreases. New strains are always created by a human, never through natural evolution. However, the whole virus problem does adapt to new architectures and benefit from them. New viruses are written as old ones become extinct. This means that there are always new viruses that take advantage of the latest computer architectures. There are always some viruses or worms that are able to efficiently use the latest and most powerful ways to communicate, sometimes even more efficiently than the human users. Table 2 shows replication speeds for the most common virus**[1][2].**

Table 2: Replication speeds for the most common virus

Virus types	*Widespread*	*Replication media*	*Typical time needed to produce a new generation*	*Typical time to become widespread worldwide*
Boot viruses	1988 – 1995	Diskettes	Weeks	> 1 year
16-bit file viruses	1988 – 1995	Program files	Weeks	> 1 year
Macro viruses	1995-Onwards	Document files	Days	1 month
E-mail worms	1999- Onwards	E-mail messages	Hours	24 Hours
Pure worms	2001- Onwards	TCP/IP Connection	Minutes	Hours

The replication speed of viruses depends on the replication strategy and the available communication methods. Today's more powerful computer environments enable viruses and worms to spread much faster than a decade ago. Malware can come in almost any size file. To make their code easily propagated through the Internet, malware creators usually keep the files small. Malware is typically found within files that are less than one megabyte (MB) in size. According to Fortinet research, 97% of malware discovered in the past five years is below one MB in size **[2]**.
The small size of the malwares file allows malicious content to be transferred over applications such as email, peer to peer download, IM (Instance Messaging) and chat easily and executed quickly. The replication speed has increased dramatically over the past decade. This emphasizes even further the fact that anti-virus software must be kept up to date to protect the system efficiently. A typical update rate for anti-virus software has accordingly decreased from monthly or bi-monthly to daily or real time. Table 3 shows development history of malwares year wise**[1][3-7]**.

Table 3: Malicious code history year wise

Year	*Malicious code description*
1950	Bell Labs develop an experimental game in which players use malicious programs to attack each other's computers.
1975	Sci-fi author John Brunner imagines a computer "worm" spreading across networks.
1984	Fred Cohen introduces the term "computer virus" in a thesis on such programs.
1986	The first computer virus, Brain, is allegedly written by two brothers in Pakistan.
1987	The Christmas tree worm paralyses the IBM (International Business Machine) worldwide network.
1988	The Internet worm spreads through the US DARPA (United State Defense Advanced Research Project Agency).
1992	There is worldwide panic about the Michelangelo virus, although very few computers are infected.
1994	There is worldwide panic about the Michelangelo virus, although very few computers are infected.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

1995	The first document virus, Concept appears.
1998	CIH or Chernobyl becomes the first virus to paralyze computer hardware.
1999	Melissa, a virus that forwards itself by email, spreads worldwide. Bubble boy, the first virus to infect a computer when email is viewed, appears.
2000	Love Bug becomes the most successful email virus yet. The first virus appears for the Palm operating system, although no users are infected.
2001	A virus claiming to contain pictures of tennis player Anna Kournikova infects hundreds of thousands of computers worldwide.
2002	David L Smith, the author of Melissa, is sentenced to 20 months in prison by USA (United States of America) courts.
2003	The Blaster worm spreads itself across the internet via a security weakness in Microsoft software. Together with the Sobig email virus, it makes August 2003 the worst month ever for virus incidents.
2004	The MyDoom worm emerges, and currently holds the record for the fastest-spreading mass mailer worm. The Netsky worm is discovered. The worm spreads by email and by copying itself to folders on the local hard drive as well as on mapped network drives if available. Many variants of the Netsky worm appeared. The Sasser worm emerges by exploiting a vulnerability in the Microsoft Windows LSASS service and causes problems in networks.
2005	The Zlob Trojan is detected, which masquerades as a required video codec in the form of the Microsoft Windows ActiveX component. Bandook or Bandook Rat (Bandook Remote Administration Tool) is detected. It is a backdoor trojan horse that infects the Windows family.
2006	The Nyxem worm was discovered and It spread by mass-mailing. In same time low-threat trojan-horse known as OSX/Leap-A or OSX/Oompa-A was also detected. Brontok variant N was found, It was a mass-email worm and the origin for the worm was from Indonesia.
2007	Storm and Zeus was detected. Storm Worm identified as a fast spreading email spamming threat to Microsoft systems. Zeus is a trojan that targets Microsoft Windows to steal banking information by keystroke logging.
2008	MocMex, Bohmini.A, Koobface and Conficker was detected. Mocmex is a trojan, which was found in a digital photo frame in February 2008. Bohmini.A is a configurable remote access tool or trojan that exploits security flaws in Adobe Flash 9.0.115 with Internet Explorer 7.0 and Firefox 2.0 under Windows XP SP2. The Koobface computer worm targets users of Facebook and MySpac. Computer worm Conficker infects anywhere from 9 to 15 million Microsoft server systems running everything from Windows 2000 to the Windows 7 Beta.
2009	W32.Dozer and Daprosy Worm was detected. Cyber attacks occur and the emergence of the W32.Dozer attack the United States and South Korea. Symantec discovered Daprosy Worm. Said trojan worm is intended to steal online-game passwords in internet cafes.
2010	Waledac, Stuxnet, “here you have” or “VBMania” and Kenzero was detected. A botnet called Waledac sent spam emails. Stuxnet is the first worm to attack SCADA systems. The virus, called “here you have” or “VBMania”, is a simple trojan horse that arrives in the inbox with the odd-but-suggestive subject line “here you have”. Kenzero is a virus that spreads online from Peer to peer (P2P) sites taking browsing history.
2011	SpyEye and Zeus merged code is seen. New variants attack mobile phone banking information. The Morto worm attempts to propagate itself to additional computers via the Microsoft Windows Remote Desktop Protocol (RDP). Morto spreads by forcing infected systems to scan for Windows servers allowing RDP login. ZeroAccess rootkit (also known as Sirefef or max++) was discovered. Duqu is a worm thought to be related to the Stuxnet worm.
2012	Flame also known as Flamer, sKyWIper,and Skywiper is modular computer malware discovered in 2012 that attacks computers running Microsoft Windows. Shamoon is a computer virus designed to target computers running Microsoft Windows in the energy sector, Symantec, Kaspersky Lab and Seculert announced its discover it.
2013	The CryptoLocker trojan horse is discovered. Cryptolocker encrypts the files on a user’s hard drive, then prompts them to pay a ransom to the developer in order to receive the decryption key, making it the first true ransomware.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

III. VIRUSES INFECTION IN MOBILE AND COMPUTER SYSTEM

A large number of mobile devices are now part of everyday use. These include cell phones, smartphones and PDAs (Personal Digital Assistants). The functionality and applications offered by current day mobile devices are beginning to rival those offered by a traditional PC. These mobile devices are usually have some form of connectivity (e.g., GSM, GPRS, Bluetooth, WiFi). These devices have vulnerabilities like PCs, but also have some peculiarities of their own. Viruses, Worms and other malicious software have been released that exploit vulnerabilities in some of these devices. These malware can cause harm or annoyance to the users of the mobile devices. Over the past few years, there has been a substantial increase in the number of malware that have been written for mobile devices. As per, there exist at least 31 families and 170 variants of known mobile malware. Statistics have shown that at least 10 Trojans are released every week. Even though it took computer viruses twenty years to evolve, their mobile device counterparts have evolved in just a span of two years. To understand the threat that is involved, we first present the comparison of the environment for PC-based and mobile device malware. The following points illustrate the differences and similarities between mobile malware and PC malware**[2][5]**.

Vulnerabilities in PCs that have been exploited are related to vulnerabilities in the operating system or application software. Patches for such vulnerabilities are released periodically by the software vendors. The users (or administrators) of the PCs are then responsible for ensuring that these patches are applied to their systems as and when released. Though vulnerabilities for mobile devices have been found and documented, it is very difficult to "roll-out" patches to the software or firmware on the mobile devices that have already been sold. Considering that the users of mobile devices include a vast majority of people that are not security conscious, it is difficult to expect users to "apply patches" to their devices as and when the patches are released. This problem is compounded because there is no easy way to upgrade the firmware or software of a mobile device just by using the mobile device. Connectivity with a PC is usually the only way to upgrade the firmware or software.

Mobile devices such as phones are almost always switched on and stay connected to the network. Unlike a PC whose neighboring network nodes remain relatively fixed, the "neighbors" of a mobile device keep changing with every change of location of the user carrying the mobile device. As a result, for example, a single user with an infected phone entering a stadium, can potentially infect the phones of all the people within the stadium if these phones have the same vulnerability. Mobile phone users are less security conscious than the average Internet user.
Unlike PCs, several variants of mobile devices exist. This makes it difficult for the mobile malware to infect or spread to dissimilar devices. For example, a mobile worm spreading through MMS can do little if the phone it has infected does not have MMS functionality. Mobile malware have not yet caused critical harm or damage. At most they increase the user's billing, or cause the mobile phone to stop working (can be restored by a factory reset), However, as a result, there is not enough motivation, either for device manufacturers or for the users, for taking preventive action against mobile malware**.** Table 4 shows different types of malware and their description found in mobile and computer system**[4-7]**.

Table 4: Different types of Malware and their description

Name	***Description***
Virus	Attaches itself to a program and propagates copies of itself to other programs.
Boot sector virus	A virus that infects the boot record on floppies or Hard drives.
File virus	A virus that infects executable program files.
Macro virus	A virus that infects documents using application specific macro languages.
Memory resident virus	A memory resident virus remains in memory as long as the computer is turned on. This enables the virus to monitor system activities and infect other objects efficiently.
Multipartite virus	A virus that can infect several types of objects. Mostly used for hybrids that can infect both boot sectors and 16-bit programs.
Overwriting virus	A virus that overwrites the host file and destroys it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Parasitic virus	Most viruses require an object to attach themselves to. These viruses are called parasitic, as they cannot exist without their host.
Polymorphic virus	A virus that changes its own code to avoid detection.
Script viruses	A virus that replicates using scripting languages.
Stealth virus	A virus that attempts to hide its presence from Anti-virus software.
Worm	A worm is a program that actively propagates over computer Networks with or without human interaction. Mass-mailers worm (e.g. Melissa, LoveLetter, Nimda) use SMTP (Simple Mail Transfer Protocol) protocol for propagation. In memory worms (e.g. Slammer, CodeRed) proliferation over TCP/HTTP(Transmission Control Protocol /Hyper Text Transfer Protocol).
Logic bomb	Triggers action when condition occurs.
Malware	A common term for all kind of unwanted software, such as viruses, worms, Trojans etc.
Trojan horse	Program that contains unexpected additional functionality
Keyloggers	Captures keystrokes on a compromised system.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access i.e. modification of system behavior, either at a user level (e.g. user settings) or a root level (e.g. system tools or registry entries).
Zombie	Program activated on an infected machine that is activated to launch attack on other machines.
Dialer	Calling premium services, re-surging in mobile malwares.
Spyware	Monitoring of user behavior (e.g. during web browsing)
Adware	Unsolicited presentation of advertisement.
Sniffer	Capturing of network traffic, especially for passwords send in clear text.
Bug	A programming error in a computer program. Viruses are sometimes incorrectly called bugs, "the love bug" for example instead of the virus' real name VBS.Loveletter.
Hoax	A chain letter that usually circulates as an email message. Hoaxes are not related to viruses in any way, expect for the fact that many hoaxes warn about a non-existing computer virus.
Joke	A computer program that does something funny or tasteless, but does not harm the computer system.
Botnet	A botnet is a network of zombie computers under the remote control of an attacker

(i) Malware Propagation vector in Computer System

Malware propagation vectors refer to the electronic methods by which malware is transmitted to the information systems, platforms or devices it seeks to infect. Email and instant messaging applications are some of the most common vectors used for spreading malware through social engineering techniques. Any medium that enables software to be distributed or shared, however, can be a vector for malware. Examples of malware propagation or distribution vectors include the World Wide Web (WWW), removable media (such as USB-Universal Serial Bus storage keys), network-shared file systems, P2P file sharing networks, Internet relay chat (IRC), Bluetooth or wireless local area networks (WLAN).

Bluetooth is one prominent vector for malware propagation on mobile devices. Bluetooth is a wireless personal area network (PAN) that allows devices such as mobile phones, printers, digital cameras, video game consoles, laptops and PCs to connect through unlicensed radio frequency over short distances. Bluetooth can be compromised by techniques such as bluejacking and bluesnarfing and is most vulnerable when a users connection is set to "discoverable" which allows it to be found by other nearby Bluetooth devices. Therefore e-mail, web, Instant messengers, Removable media, Network shared file, P2P (peer to peer) programmes Systems, Internet relay chat and Bluetooth are called malware propagation vector **[5-7]**.

(ii) Attack vectors of mobile Malware

Today smart phone has maximum common features as personal computer so that attack vector is common as PC but more specific attack vectors for mobile malware are SMS, MMS, WiFi, Bluetooth, Vulnerabilities in the operating system.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

IV. RESULTS AND DISCUSSION

With the improvement of virus detection technologies the virus creators found it difficult to create viruses that were capable of surviving long. This situation made them to innovate new methods for the survival of their viruses. Some important stealth techniques such as encryption, polymorphism and metamorphism were developed in order to make the viruses capable of escaping conventional scanning methods. But the war between virus creators and anti-virus creators was far from being over. The anti-virus creators implemented new techniques such as heuristic scanning and emulation techniques which were capable of detecting encrypted polymorphic viruses. Some modern anti-viruses used automatic learning static, dynamic heuristics, rootkit heuristics, dynamic analysis through virtualization, dynamic analysis through bare-metal etc. methods are used to remove virus hidden anywhere in the computer. Threat mitigation are perform to detect and stop malware before it can affect its targets. Several types of security tools that can mitigate malware threats i.e. antivirus software, spyware detection and removal utilities, intrusion prevention systems (IPS), and firewalls. Antivirus software is the most commonly used technical control for malware threat mitigation. For operating systems and applications that are frequently targeted by malware, antivirus software has become a necessity for preventing incidents. To protect computer system from threat's of virus we need to choose a good quality antivirus. Presently maximum viruses are omnipotent in nature, means they does not need to execute but they automatically execute silently in system and spread from one computer to another via LAN, as email attachment, downloadable file or some external link. The common vector of viruses are External network, Guest Client, Executable file, Documents, Emails, Removable media such as CDROM or DVD ROM, Floppy disk, USB Drive, Memory card etc. To protect computer system from virus, do not assume you are not at risk, Use a pop-up blocker with your browser, Download work done only from trusted sources, Keep your software update, do not delay updates, do not automatically open attachments, Scan all incoming email attachments, do not share Memory card/ Pen drives, Track warnings and alerts, do not disable the software, use firewall for blocking suspicious program.

Although mobile phones are taking on more capabilities formerly available only on PCs, technical security solutions for mobile phones are not as sophisticated or widespread as those for PCs. This means that the bulk of mobile phone security relies on the user making intelligent, cautious choices. Even the most careful users can still fall victim to attacks on their mobile phones. To protect mobile phone, when choosing a mobile phone consider its security features and configure the device to be more secure, Configure web accounts to secure connections, Limit exposure of your mobile phone number, Carefully consider what information you want stored on the device, Carefully choose when selecting and installing apps because they can Trojan, disable interfaces that are not currently in use such as Bluetooth, infrared, or Wi-Fi, Set Bluetooth enabled devices to non-discoverable so attacker can not target your devices, Avoid joining unknown Wi-Fi networks and using public Wi-Fi hotspots and also be careful when using social networking applications**[8-10]**.

V. CONCLUSION

Many users may consider mobile phone security to be less important than the security of their PCs, but the consequences of attacks on mobile phones can be just as severe. Malicious software can make a mobile phone a member of a network of devices that can be controlled by an attacker (a "botnet"). Malicious software can also send device information to attackers and perform other harmful commands. Mobile phones can also spread viruses to PCs that they are connected to. Losing a mobile phone used to mean only the loss of contact information, call histories, text messages and perhaps photos. However in more recent years, losing a smartphone can also jeopardize financial information stored on the device in banking and payment apps as well as user names and passwords used to access apps and online services. If the phone is stolen, attackers could use this information to access the users bank account or credit card account. An attacker could also steal, publicly reveal or sell any personal information extracted from the device, including the users information, information about contacts, and GPS locations. Even if the victim recovers the device, he or she may receive many spam emails and SMS/MMS messages and may become the target for future phishing attacks.

Mobile devices are becoming smarter and more powerful. Such devices, once in widespread use, will herald the growth of using mobile devices for performing sensitive tasks such as storing sensitive data and performing eBanking transactions. Research paper show that there exist sufficient vulnerabilities in these devices that could be exploited to cause harm to the device to reveal sensitive information or to use the mobile device in a malicious way. Today's

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

smartphone has maximum common functioning feature as personal computers. So that protection from malware is more essential for smartphone and personal computers. It is therefore, easy to visualize that in the near future the threat posed by PC, mobile worms and viruses can cause considerable harm to the users of such devices. To protect communicative electronic devices from malware attack we need to install good quality antivirus and firewall, this is technical solution. We also need to follow some precaution and common sense for better protection of Smartphone, Personal computer and similar electronic devices from infection and attack of malwares.

REFERENCES

[1] White paper, "Computer Viruses from an Annoyance to a serious threats", F-Secure Corp., available on www.F-Secure.com, September 2001
[2] FORTINET White Paper, "Under Standing How File Size affects Malware detection", Available at website www.fortinet.com/sites/default/files/whitepapers/MalwareFileSize.pdf, Retrieved on dated 25-01-2014.
[3] Abraham Silberschatz , Galvin Peter B., Greg Gange , "Operating System Concepts", 8th Edition, Wiley India Private Limited, New Delhi, Published in 2010.
[4] Basandra Suresh Kumar, "Computer Today", Galgotia publication Pvt. Ltd, New Delhi, Revised Edition 2008.
[5] Peter Mell , Kent Karen , Nusbaum Joseph , "Guide to Malware Incident Prevention and Handling", NIST Special Publication, November 2005,USA.
[6] Singh Brijendra, "Network Security and Management", Prentice HallofIndia Private Limited, New Delhi 110001, Published in 2007.
[7] Stalling, William "Network Security Essentials application and standards", Third Edition, Pearson Prentice Hall, Published in 2008.
[8] Rafael Fedler, Julian Schütte, Marcel Kulicke, "Malware Protection on Android" , Fraunhofer AISEC, April 2013
[9] OUCH, "Understanding Anti-Virus Software, Newsletter", March 2011
[10] Virus Bulletin, http://www.virusbtn.com, Retrieved on Sept. 2014

BIOGRAPHY

Sudhakar Singh is a Research Scholar in the Department of Physics and Electronics, RDVV, Jabalpur (M.P.), India. He received Master of Science degree in Physics from APS University, Rewa (M.P.), India. He also obtained his Master of Computer Application (MCA) degree in 2007 from IGNOU, New Delhi, India. He has 11 years teaching and administrative experience in the Dept. of Physics and Computer Science, Sardar Patel College of Technology Balaghat (M.P.), India. He written 03 Books and 10 Research paper published in various reputed international journals. He attended various workshop /conference in IIT Mumbai and VNIT, Nagpur (M.S.), India. His research interests are Computer Security, Solid State Electronics, Communication Electronics and Space Science.