ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (194-209), Month: July - September 2015, Available at: www.researchpublish.com

Internet Security and Hacked Network through OS Vulnerability

Darshan Lal Valecha

Faculty of Computer Sciences and Information Technology Institute of Business & Technology, Karachi

Abstract: **Operating Systems Vulnerabilities are the primly cause for the cyber attacks and potentially misuse of software applications. The Vulnerabilities are mostly due to unsecured OS system architecture, software development design, this is ultimately results in software development, where security is a major concern, remains mainly unnoticed. Secure System software and large refers to the process of software security. The Software security essentially focuses on developing the secure software, which generally depends on system architecture and software security assurance against the possible vulnerabilities whether this security concerned the OS Kernel. But the Kernel in customary OS terminology is a small nucleus of applications that provides only the normal resources necessary for implementing additional OS applications services. Absolute protection from them is question of ongoing research. The problem becomes more serious when it is a networked based environment. Starting from servers to clients, malwares can certainly create havoc in networked environment. Networking among computer provides malwares with an easy of transport. They can easily transfer from one system to another, thus infecting several systems in no time. Numerous technologies have been employed to counter their threat. However Immunizations with these technologies keep being devised. Present scenario calls for technologies that hit very base on which the spread of malwares in a networked environment stands. With the malware industry letting out new variants of malwares to intact large computer networks at an incredible pace, it has become imperative in the present to come up with strategies so as to counter their threats. With every new malware coming in to picture new technologies are designed to combat them and the reverse unfortunately stands true. The present scenario demands fresh technologies which strike the roots on how malwares enter a network and consequently spread inside it. The malwares have to be checked from the entry point itself because once they find a place inside the network; they can create innumerable places from them to hide. The mechanism to counter malwares in a networked environment proposed in this paper, checks the entry of malwares right from the entry point of a network itself. The architecture powered by networking among multiple OS Kernel will certainly be a progressive step in controlling the malware menace among computer networks. Even though we used process by software and also used VPN techniques because it can possible further secured as no one hacked and it's possible secure by software's technology.**

Keywords: **Computer Network Security, Invasive software's, Operating System Kernels, Malware, Threats, Architecture.**

1. INTRODUCTION

As Internet plays a more and more key functions as informatics infrastructure, Electronic Business and Electronic Payments in Internet is successes due to its something useful and it's in favor of users. International Network safety Issues are still a huge challenged, we have stills too many security events happen. The subterranean economy based on Internet Fraud is also prosperous. The WAN/ International Network being interested huge growth over the since few long time un till present, this research focusing on improving the performance of the Internet, in spite of the fact performance have its own placement in the Networks research , the offensiveness of Networks have struggled the researchers Community look like at this consistency aspect. The Domestic or International network like an organization has a large amount of

facts and figures, currently in digital form. Same on time of data transmission from one place to other place data can be hacked by unauthorized persons through Kernel or Black Hole. As similar characteristics any product tending to failure and Researchers may start to understand the significance of trustworthy communications in requested to defeat the recent crackers. The significantly now a day's security of Internet have been increased fastest during the many vulnerabilities , that can closed some of the all over the world's high class personalities profile hacked, as Amazon and Yahoo, Linux or USA Hacked Germanic Vice Chancellors Calls by any spy. Many of the assault have been also inform in CERT advisories, although information assured assumed , that peripheral Hardware responsible for encode, send bundles instructions are reliably. Researchers are questioning about assumptions since reported instances where the networks infrastructures e.g. ;(firewalls, KVM, Servers) have mutual decision by crackers anti. Therefore Internet/networks hardware's safety is obviously pressed requirements. Importantly current international attacks have been possibility of moving entirely networks Infrastructure which has important results on safety of vigorous community. Every way of our life depends on Cyberspace safe and secured operation of the system depends on. "The security of the infrastructure that needs immediate attention of the research is a pressing problem. Despite over a $22 billion a year spend on Antivirus and other security software's is going , cybercrime victims to the dangers of amateur organized groups of hackers worldwide business became a passion once was , [1] increased are ? Cyber robbers want your Bio data and financial information, and they only get it through shady web sites are going. It is well known with dignity "brand name" web site are fully protected , claims that it is now a popular marketing strategy . However, these sites or sports scores, the latest news by checking the user can affect just a computer for hidden malware being targeted to become the unwitting host is exactly why the idea is . Businesses , agencies and actually designed with security in mind, this one might have been the medical and educational institutions, many Web sites contain a wealth of personal information to target their data base 's . Currently botnets by ER per year "hijacked " as being Ease according to the US Department FBI for an average of more than one million are counters . Mass loss in the number of cases are dropped in recently years , targeted profit driven cyber attacks fortune in your company this paper will examine the nature of change itself and its employees can protect the victims of these methods is on the rise thieves who target cybercrimes,, and what can be done to prevent them . Secure system software application or system procedures. Applications software so that it permits to function appropriately under malicious attack. Today's most prevalent and a widely discussed attack exploits architectural, code-level, information leak from side channel and software verification flaws. Malicious intrudes can hack systems by exploiting these software defects. The Secure software Architecture can be achieved by imposing access control and security Kernel mechanism and Policies consists of a achieved by imposing access control and security Kernel mechanism and policies As a single-layer access control decisions to allow for precise set of rules for determining contains. Security kernel approach to an operating system (OS), in a relatively small part of the software is responsible for safety on the basis of the theory is a procedure. By the restructuring of OS security related software are all traditional design to avoid security paroles distributed in an OS kernel is reliable [2]. Period only applies to access control subjects and objects within the control, a system of layering to implement some built in support for requiring appropriate Policies. The Buffer overflows [3]. Vulnerability occurs allocated buffer. Buffer overflow vulnerabilities are very easy to exploit. Injection attack code runs with the rights of the weak programs and attackers without external assistance maintaining and let's move forward. Buffer overflow vulnerability that any other program except its caller can pass information to the [4] software can be used during the process completing section is in prison. Leak information on which it is encoded by the supervisor or other storage facilities to be provided through channels with memory through the use of a program can be through a call. The activities in the area of confinement are reported in section.

1.1 Operating System:

By early on1950's, has improved somewhat with the introduction of routine punch cards. Carried out the research laboratories of General Motors Corporation operating systems first in 1950 in the early IBM 701. For the system 50 generally ran one job at one time. This was called the treatment systems at once to stream and provided programs and data in groups or batches.

An operating system is widely has greater responsibilities and powers to work on a large scale, such as the Internet and mobile computing (Das, 2009; Kay, 2008; O 'Reilly .1995; Sun Microsystems 2002). It's just like traffic management system, and it makes sure that different programs and software packages for users and clients running at the same time do not interfere with each other. Operating systems is also responsible for security risks and ensure that unauthorized users do not access the system.

Computer's operating system (central server) being a very safe depends on a number of technologies (tools and utilities) that operate in an efficient and reliable in the clock. Operating system provides real-time access to modern resources and a number of sub-system, which is available on the operating system software on the system and external devices such as communication networks (LAN / WAN). An operating system is the most important system software and high available (program) that operate on the heart of the computer (the nucleus). The computer must have a general-purpose operating system for all programs run multiple applications at the same time another site with multiple, function, operation and services without any error. Shows the hierarchical structure of the research and technology organizations.

1.2 TYPES OF HACKING:

Maybe DNS for it is toughness, and provides lead to a variety of type of risks that a distributed database, which contains confidential **in** main three categories:

✓ Cache poisoning: general question to hasten the process, DNS servers collect general information in a cache. To change the DNS server is invalid if Information, the attacker is under the attacker's control can redirect traffic for the site plan.

✓ Server Compromise: attackers such service user's ability to modify data, a DNS server can compromise. It can be used to compromise servers DOS for cache poisoning attacks on any other server.

✓ Spoofing: In this type of attack, the attacker masquerades as a DNS server and client information wrong or potentially malicious feed. This type of attack can

Under the control of the attacker to redirect traffic to a website and launched a DOS unsuspecting client. DNS attacks, IETF to solve, collectively known as DNSSECDNS, including the expansion of the security.

2. LITERATURE REVIEW

This section is focused on Hacking and Vulnerabilities of Operating Systems and else on Network/Local or WAN (Internet) with used of different Applications. This Research Paper is includes on different parts that includes the specific targeted Area of OS and weakness of system Applications, Most Computers OS Vulnerabilities can be exploits in various of ways in Kernel . Hackers Attacks may use single specific deeds at the same limited time, a mis-configuration in one of the OS system component or even backdoor from earliest attacks. This paper will deliver detailed Information for the OS and Vulnerabilities allowed to connected to the Network, System hacking is technical used to trace the art of skulls Programming in Computer want it to do. A Hacker is the Developer who can does it very well it. A Computer Expert and average layperson typically use as conditionally to mean "System Criminals". However in reality it simply means 'Clever or Sharp programmer' with no connotation of computer programming ability or skill. They are also Occasionally broaden to mean any kind of experts, especially one who has specific some hidden known or Abort Computer coding certain amount hackers want computer done something don't , what the Genuine programmer planned . However, there was always competition between static [7] and dynamic analysis [8] arbitration, which is the best one of them, is designed to detect weaknesses before the implementation of the program code or another during the implementation of it. Thus, the aim of the researchers in the various tools that combine the approach of developing and have been very successful [9]. Although, it is known that some of the variables are weak in the program can only be detected at run-time, but mostly lacks is detected best during static analysis and striker most of the time attempted to insert his / her malicious code [10] in the source code. Also, in a number of dynamic analysis of test cases need to apply to find exactly doubled. Thus, the need to develop these methodologies that can grow insurance code of the attacker.

2.1 THE BACKGROUND OF HACKING :

Based on the idea that organizations have a hefty amount of data and also has two or three branches that are using that data. This is stored in the form of database queries. A database is a structured collection of data, usually in digital form is today. Data sets are usually available in college, (for example related aspects of the model are held, database regarding business). At the time of data transmission from one place to other place data can be hacked by unauthorized persons through hack password or attacks of data like intruder or black hole so to secure that data there are many algorithms.

DNS, is a critical infrastructure, access to servers and connections to start all over by the host is contacted. DNS attacks that include the effects of very large scale:

Denial of Service; DoS DNS hacking is one of the mainly risky effects. DoS can achieve in quite a few ways:

There is a mode of indicating that DNS is to send negative answers back. Another way is to serve the client application does not contain a server is to forward the client's request. DoS attacks on DNS servers with the maximum effect can be achieved.

Masque ring: Use of anti- communication to redirect DNS attacks, and later as a reliable company that can masquerade. If this is accomplished, an attacker, or deliberately corrupt communication intercept analysis [9] Can.

Billing information: DNS internal network threats an attacker include leakage of information. Often, the name of the host machine's operating system may be of interest to disclose the name of the project can represent.

Domain hijack your domain registration information from customers to update the stored procedures used by the compromised, attackers can take domain Registration process to capture unlawful domains.

2.2 Hacking Tools:

2.2.1 NMAP and the tradition have continued and is still number one:

NMAP best ever made so far by the security scanning and hacking tool. These applications are the top for two reasons hacking software is at the top of every list. The first of its ease of use and its wide SAGE II. As Port scanning, fingerprinting, OS detection, ping, scanning and IP range, the live hosts are to perform together, which can combine several commands in a rich command mode for advanced users provides a wide range of features like that . With most of the new Advanced Learning and security experts are recommended. Every year, Google's open source project hosting.

2.2.2 super scan:

Powerful TCP port scanner, pinged, resolver. Super Scan4 highly popular Windows port scanning tool, super scan is an update. You need a decent interface replacement for Windows NMAP, I suggest you check it, it's great. This shows a lot of information with a cool scanning experience provides.

2.2.3. NESSUS:

Nessus vulnerability scanner NMAP top of the number1 spot on the break and the only device that can reach. Because of its wide process for both network administrators and hackers is a powerful tool. Nessus weakness scanner high speed finding, configuration auditing, asset profiling, sensitive data discovery and vulnerability analysis of your property exchange, is the global leader in active scanners. Nessus scanner a whole, inside DMZs and across physically separate networks can be distributed throughout.

2.2.4. John the riper :

The fastest password cracker. It is available for Windows and several UNIX versions, and each time has been a brute force password cracker. Many flavors of UNIX (not counting the 11 official different architectures, are supported) to the currently available, DOS, WIN32. If OS and OpenVMS. The main reason is to distinguish weak UNIX password. Among many Crypt (3) out of the box support for most secret word hash types usually create on various UNIX flavors , Kerberos AFS and Windows NT,2000/XP,2003 LM hashes are .

2.2.5. WIRESHARK and kismet:

5th place 2 points to reach the number by which WIRESHARK improve. As with the fate of the 5th spot is common for Wire shark. The most preferred wireless security assessment tool and is one of this kind in this field. This tool is a must

have for all wireless junkies. Wire shark capture your network perimeter, and interactivity content searching base network protocol analyzer or sniffer that GIK is Destiny and 802.11 wireless network detector, sniffer, and intrusion detection systems. Destiny will job with any wireless card supports raw monitoring mode, and Wi-Fi 803.11c, 801.11g, and 801.11N traffic (devices and drivers permitting), which can be sniffed.

2.2.6 PANGOLIN SQL injection scanners:

This is by far a site for SQL injection attacks scans is the best scanner SQL injection. This risk is present or not to check the database to perform the test. Many popular database tools built to scan and effectively silenced for poorly configured websites works. It's a tough competition with Havji nature of the platform, but I chose this area as the winner made to Pangolin.

2.2.7 NIKTO 2:

A fresh arrival and must be. Over NIkto 270 servers in 6500 potentially unsafe files / CGIs, to ensure for older version of over 1250 servers, and version explicit problems, including comprehensive tests against web servers for objects, which perform an Open Source (GPL) web server scanner. As such, it also checks for server configuration items of multiple index files, HTTP server options, and the presence of installed web servers and software will attempt to identify. Scan items and plug-in are commonly updated and can be manually updated.

2.2.8. Low Orbit Ion Cannon*:* LOIC popular hacking group Anonymous has been called, which is an effective dos attack tool. Service goes down, so that a flood of data packets from the device to a web server can be used and it becomes inaccessible. PayPal recently this tool and many other top worldwide Web sites were used to bring down.

2.2.9. Cain and Abel:

Favorite password cracker all kinds. These new platforms are continually updated by a number of tools at its support for stiff competition this year fell in the ranks.

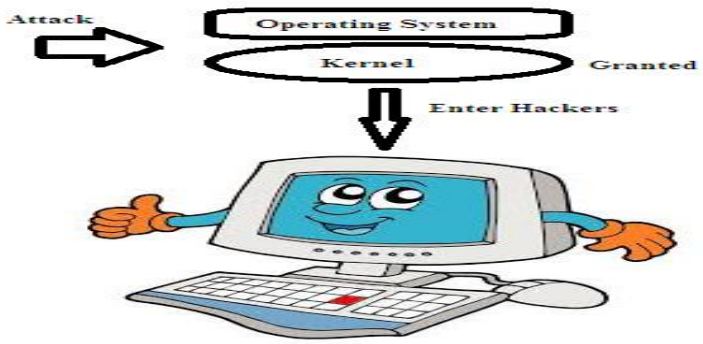
2.2.10. Hide IP:

Several tools were fighting for the last place, but high use of anonymous surfing on the 10th I finally made to put IP Hide .This is a great tool for anonymous surfing and access to copy and perform the necessary anonymity of the web testing. The closest competitor , but as the owner of the place I decided Hide IP is due to the slow pace of tar as it was .

3. METHODOLOGY

3.1 Some Vulnerability found:

As some vulnerabilities are published on 12/08/2014 in Windows 7, which was updated on 14/08/2014 as CVE-2014-4064 vulnerability type “Overflow +Info, details of this “Kernel-mode drivers in Microsoft Windows Vista SP2 or Windows Server 2008 R2 SP1 SP2 and, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 R2 and gold, and Windows RT gold and 8.1 do not properly treated using the divider combines the core of the memory allocation is formatted, which allows local users to obtain sensitive information about the addresses of the nucleus through the application developed, and is also known as "Windows kernel pool allocation of weakness." Total vulnerabilities are found in 348 in both Windows 7 and windows 8.1. The total numbers of these vulnerabilities are under solved till this time. [10]



3.2 Example of Vulnerable Program:

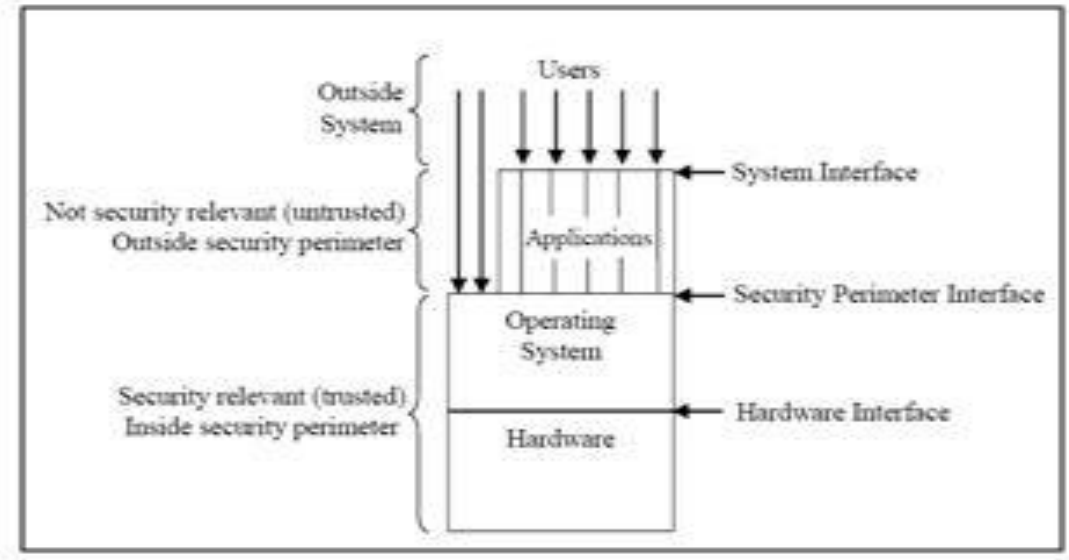
/* test.c */

```
#include <unistd.h>
Int main(int argc,char *argv[ ])
{
    Char buff [100];
/* if no argument..*/
If (argc    <2)
{
Printf ("Syntax: %s <input string>\n", argv[0]);
Exist (0);
}
Strcpy(buff, argv[1]) ;
Return 0;
}
```

This is sample program of vulnerable from reliable sources [11]

3.3 Secure System Architecture:

A computer system traditional decomposition shows the hardware, an OS and application program [12], They run concurrently and independently Proposals may be numerous. The upper layers of the interface between couples of layers of accessible works have shown that layer. There are two main interfaces. Border and perimeter security systems. OS, Collaborative Interface Framework applications on the security constraints to force the OS interface. In rules or policies that are in agreement with the hardware guarantees success with the OS at least two states, privileged, and must have unprivileged. A kernel privileged executive mode, the system is defined as a mode or supervisor mode and an unprivileged user, application or problem is referred mode. Machine running in privileged mode when software can affect any machine learning and memory in any location can access. Unprivileged mode, the software specially privileged instructions or posses software or other damage that can cause memory access in a way that has been shown to Generic Computer System Architecture



To implement the privileged and unprivileged states there are two major concerns.

3.4 Five layers of the proposed system:

1. Application layer access / user

2. OS interface / system calls

3 operating system kernel, the operating system and basic functions

4. Father and interface / firmware / BIOS, the boot kernel

5. Hardware (HW), CPUs and memory and interposers

In general, the protection can be implemented in any layer and

There will be a need for protection in each layer.

3.5 Proposed solution;

In some cases, it may be a security software application only. Even if they are designed well and was implementation Flawless, and some weakness in the lower layer operating system kernel can be used to defeat the application layer protection. L For example, considers the case of the presence of anti-tamper protection that Result in self-examination and repair of automatic data important and instructions. And this protection can be implemented purely within programs and enable the application to check own integrity and make repairs. However, if the operating system kernel has been breached, can be redirected self-examination to a different memory location, It will protect the self-selection works with incorrect Report, there will be reform.

3.6 Should govern the use of the following model:

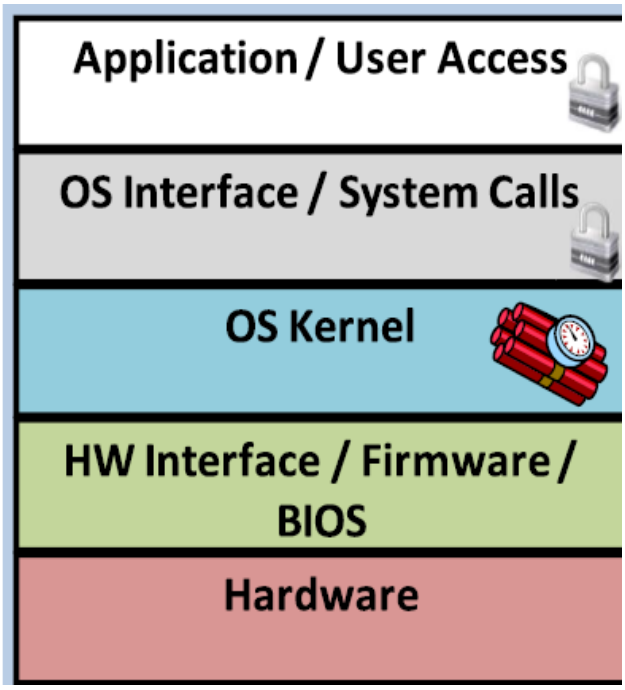
• Even with perfect protection implementation can be perfect, Likely to be defeated by the lower layer attacks.

• A loophole in a single layer can create the one above.

• Loophole could negate the lower layer protection.

• Protection should be implemented in each layer.

• Protection should be integrated in different layers.



Five layer Model as sample

3.7 Authentication:

A user to access a system files to be allowed to make important decisions about whether a system in order for the system to recognize each user must have a source. Must have a unique identifier associated with each user should be identified. With a unique identifier, a user (or more accurately. Operated by a user of a program) have described the act as a certification that is. All actions within a system as a sequence of operations on objects can be seen. Generally, an object is considered as a single file, but otherwise missed something that holds data, directories, rows, inter-process messages, network packets, input (I / O) devices including an object may be. Objects can influence access or functional entities, called subjects. A high level of abstraction, (and as a replacement for) user from users. A security mechanism in a system consists of main three tasks which access control [12]:

a. Allowed access to the items on the subject, particularly the right to determine.

b. Focuses on read access rights determine which, write, process, delete, add and access methods.

c. Subjects access rights to enforce access rights to objects .is used to support a set of security attributes. Takes place until a suitable access is not a breach of security to determine access control enforcement , it , giving access rights (as in advance) and rights (access time 's) exercise is necessary to distinguish between .

3.8 Security Policies:

In the real world, a security policy controls access to documents or other information [2]. Access control policy as a basis for making decisions on the authorization rules for determining the specific set consists of t he lack of a clear policy and shows no errors in the control system, the most security flaws is a key reason. While people generally obey a system security policy, security features obey. All systems on the basis of security features and policies are evaluated. Security kernel approach to building a system of systems is responsible for the implementation of security policy. Separately for each major OS kernel security perspective, a fairly small part of the software is accountable for safety [12]. All security related software is divided into a trusted kernel of the OS can be restructured. In most cases, the OS kernel security serves is a primitive OS. Appropriate security should be protected kernel, and the kernel should be possible to bypass access control checks. It is easy to verify the correctness of the kernel must be as small as possible. Enters the security kernel hardware's and OS software consists of a new layer. Security kernel approach to system architecture significantly the system security controls right at the user -level rise can trust.

The two main principles [9] for the design of secure systems architecture:

3.9 Minimize and isolate Security Controls:

The security of a system to achieve a high degree of confidence, Designer system design size and complexity of security related components should be minimized. Relevant parts of OS security key to minimize such an isolated part of the security relevant actions to be taken, forcing security enforcement mechanism, only a small number of different types system design is to use.

3.10 Enforce Least privilege:

Combined security mechanism related to the idea of isolating the principle of least privilege Articles should be no more than a privilege to enable them to do their jobs is necessary. In this way, very high or limit the damage caused by malicious software.

3.11 Buffer Overflow Vulnerability:

Buffer overflow vulnerabilities are very common and very easy to exploit. Injection attack code runs with the privileges of the vulnerable program and allows the attacker to self sustain and proceeds without external help. Ken Thompson [14] the principle inventor of UNIX OS also acknowledges the buffer overflow vulnerabilities in his paper "Reflections on Trusting". He has shown buffer overflow implication in C compiler which is written in its native language, Buffer overflow occurs Runs and overwrites adjacent memory buffers over the range in which a buffer while writing data. This memory is a special case of violation or corruption. Programs written in the C language [15]. Buffer overflow attacks are suffering. Also known buffer overflow.

- As I Arkanoyd steak. In some cases crash the program or functioning improperly can cause overflow.

✧ *The following as the buffer overflow vulnerability exploited by the worm can recruit: Morris worm [15] exploits a stack buffer overflow fingered by the UNIX finger daemon taken control.*

✧ *Internet Security Systems (ISS0 desktop agent using black ice stack based buffer overflow Witty worm [15] was exploited by.*

✧ *Slammer worm [16] by exploiting a stack buffer overflows in Microsoft SQL Server. Blast Worm [17] by Microsoft DCOM services stack buffer overflow exploit.*

3.12 Protection Scheme for Buffer Overflow:

Software applications can be undetected during development and testing as buffer overflows are a problem. Common C and C + + compilers when compiling the report at neither runtime buffer overflow nor buffer overflow conditions to identify possible exceptions. The possible protection mechanism [18] is

3.12.1 Stack *Buffer Overflow Detection* to Malicious code to prevent redirection of the instruction pointer Stack Buffer Overflow Detection. Stack Canaries or cookies stack buffer overflow can be used for detection .I remember just before the stack pointer back randomly, selected at the beginning of the program, which is to keep a small integer value. Carey Price will be overwritten to overwrite the return pointer is necessary in order to address more memory than most buffer overflow to overwrite memory. This value back to a normal stack pointer is not changed before using it to make sure it is checked. Between final local variables and function return address stack Push Canary. A cookie is modified, program execution stops immediately. The process of any type of malicious code is prevented.

3.12.2 ***Malicious Code Execution Prevention*** without directly detecting stack buffer overflow in the stack to prevent malicious code execution. Stack buffer overflow exploit prevention disapproved hanging from the stack into the stack memory area is to implement the policy. Non- performance processors as a support for memory pages provide descriptions. These pages can be used for storing data and code stored in the processor will not run. This "data execution prevention" method is called. OS stack and marks the pages as non- executable. Using a buffer overflow in the code that prevents an attacker from running

3.13**The Confinement Predicament:**

Data from unauthorized access or modification: The main purpose of the system for safety protection, including.

3.14*Program from unauthorized execute:*.

Further in a client-server application, there is a possibly of information leakage. The client depends on the server to provide services. He client may not trust a server and it is possible that server may record the information with some malicious intentions. There is a possibility that the server may sell this information to the interested parties, causing damage to the client. This issue can be avoided by disallowing the sever to record may information. Server can record information by writing it into an external file or communicate with other process, called collaborator. The Confinement Problem essentially can be defined as the main objective of the system to make sure that there is no way for the server to leak information to the collaborator.

◆ A confined program remains focused on the intra process calls, with a complete restriction to making calls to other programs.

◆ In a Situation in which total isolation is not practical and a call have to be invoked for another program then the called program must also be confined.

◆ In a scenario with a need of storage, preserved by the superior, a due care has to be taken to avoid any information leakage.

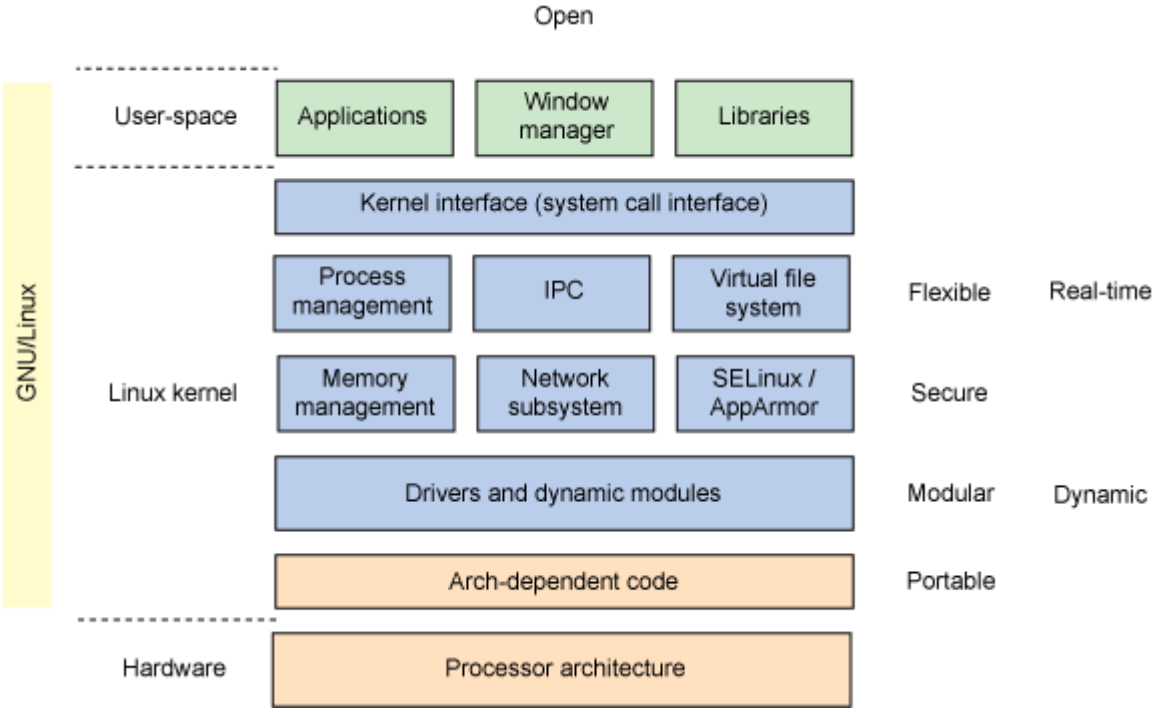
3.15**Some Architecture of Operating Systems:**

3.15.1 Linux Kernel Architectural:

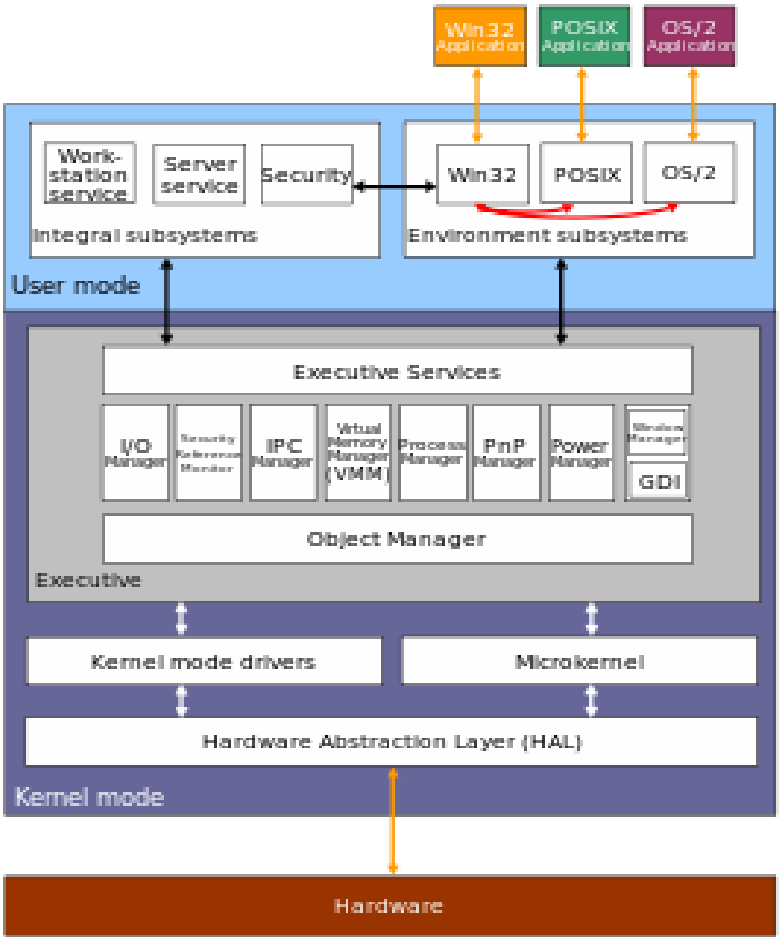
Linux kernel layer is equivalent to the basic abstract, the level of the layer between the hardware and software layers in other the system. It is built on the Android operating system on top of the Linux kernel with some changes in the architecture provided by Google. Nucleus contains a wide range of device drivers for making communication Peripheral

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (194-209), Month: July - September 2015, Available at: www.researchpublish.com

easy. Provide the nucleus of the Statute Functions such as memory management, process management, Security, and device management, network group etc. [16].

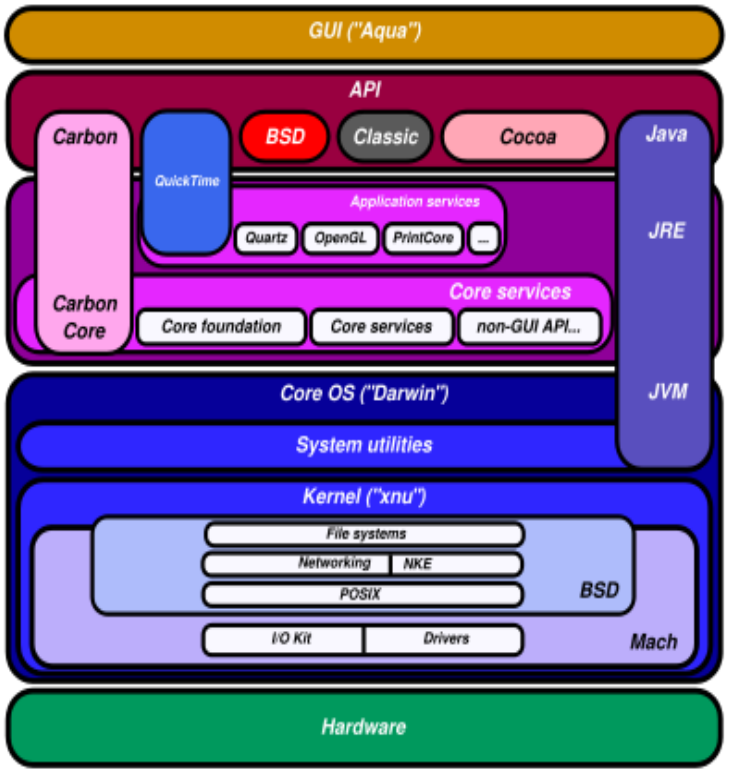


3.15.2 Windows NT Kernel Architecture:



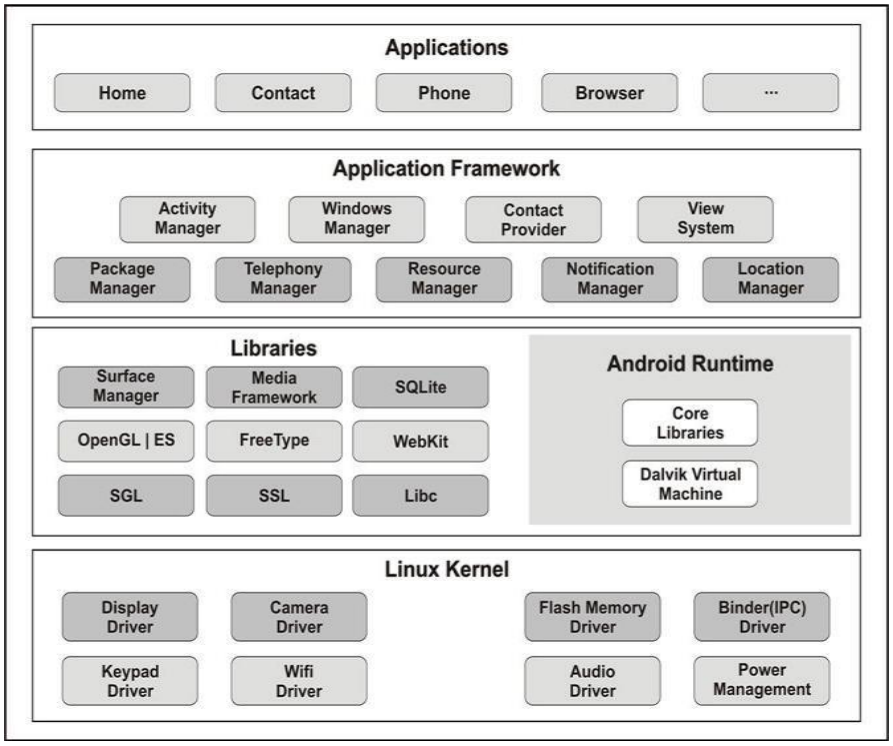
ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 3, pp: (194-209), Month: July - September 2015, Available at: www.researchpublish.com

3.15.3 Macintosh Operating System:



3.15.4 Android OS Architecture:

The main goal of the implementation of the robot is to protect the security of user data, system resources, and provide application isolation. For this, the robot updated in a timely security controls with each patch and each copy issued it. The previous versions of Android or any other security features very little to protect against attacks developed because the development is still on and it was also a very small number of people Android devices.



4. FINDING AND DISCUSSION

What is available from a number of tools in order to detect weaknesses, and some The techniques rely on fixed them, and this means is the analysis of the source code without While the application is running on dynamic techniques necessary to run it and if any one attacked on operating system , which can be tender point , that broke easily? And Selection tools are relevant to the type of application for the evaluation and programming Language and type of exposure to detect. Techniques covering all fixed Possible execution paths but require source code while dynamic techniques The difficulty of requiring the preparation of test cases and the possibility that not all And covering the tracks in the program, but the advantage that the problems, if any, are Found in the Act, respectively. Dynamic techniques have false positives also less than Stats.

Finally, the current research intends to create new ways to detect weaknesses Based on the models. In this way we can ensure the re-use of test cases and facilitate the transfer of these assertions in a specific official Programming language tool used for detection of weakness

4.1 Threats Different ways on Different Purposes:

Hacking has been around for decades. Hacker's 1983 movie War Games publicly made aware of the potential dangers, but also the official or agency to try to break into the computer and encourage their people glamorized. Some profit trading secrets and long remoteness phone codes can be stolen was the main goal of dignity. How many and much systems can be affected or damaged? The yrs 1999-2001 were banner for hackers. Immeasurable cyber crimes throughout this period there were three main importance, especially, in glamorous attack. The first $80 million in damage was caused by the Melissa virus. Then a Filipinos student "I love you" virus created, millions of PCs around the world with disabilities. Final, and definitely slightest, the Code Red worm staggering $ 2 billion in losses, resulting in Millions of Windows NT/2000 servers not infected. Incidents of anti-virus, anti- malware and other protection suites billions of dollars to equip themselves with the businesses and individuals who started a big wake-up call provided. Virus attacks almost declined by partially starting 2001 to 2007 began to fall. As a result, in modern years a growing sense of satisfaction is, users can delete all spam e- mail, downloading suspicious attachments to avoid and stay missing from websites that conscious object of morality, they will be secure. Regrettably, the nature of cyber crime is a serious change. Once a computer geek's an ego trip was fun to professional criminals an estimated $ 100 billion worldwide, has become a cash cow? Designed to damage and chaos on a large scale, significant events of the day, that is invisible to the victim targeted, stealth attacks are being replaced by. Opening one eye, for example, highly regarded, international chairman of Barclays Bank involvement. In January of 2008, the chairman of a bank card to get organized enough to get personal information. The thief then chairman of the account card used to withdraw $ 19,574, and that money is long gone until after I had no idea what was going on. 18th chairman of the world's biggest company can be targeted so simply, what wish for the normal business person? Analyst firms, corporate networks, Internet access points are not enough as many as 90 % is estimated. As a result, the Web -based attacks themselves and their employees are exposed. However, unlike Barclays Bank, for example, a well- planned attack on organized crime victims thousands of dollars for a few high-profile targets is required. Personal identification from Internet Criminals "currency" has become the smart play quietly flying under the radar and without raising any red flags from many people is to steal a small amount . Here 's an instance of how cyber criminals can do a million easy a against the law business as something harmless cleverly hide them , of course , are trying , a link to malicious software / URLs that contain a million emails sent. just 10% of recipient release the message and click the link, then, offenders will profitably infect 100,000 computers and password, social security number, credit card and bank account numbers - in the form - they are able to obtain personally identifiable information that you can use spy software to their computer, only 10 per cent, that 10,000 victims were lined up like ducks. A crime is undetected as no sense, at this point is getting greedy and makes your plan clear, and the perpetrators can benefit from it. $ 100 off any offenders from the account, the password has to be completely unnoticed. Used for each of the 10,000 victims, so that they hardly raised a finger to his mousses criminals without a cool 1 million dollars. Such types of theft only "other guy" to be and no one should get a false sense of security. Regard as the data ID stealing is one of the top growing crimes, and 10 million Americans suffer each year. T.J. retailer Only one steal MAXX, 45.7 million debit and credit card numbers were stolen , and easy for cyber criminals continue to go after the money as such threats will only accelerate .

4.2 The Herd Mentality:

Cyber criminals in a very short period of time to target the large number of victims involved, especially when there are a number of ways. Such superlative situation for these opportunities Olympics, presidential campaigns, the marvelous Bowl, and ordinary and synthetic disasters just about the world as the news coverage of national and international events, will

receive the increased traffic the site produced. Identify - legitimate business opportunities in advertising revenue as "herd mentality "while viewing, cyber thieves from Internet Criminals see an opportunity to deal in the currency. The latest details of the results of the election terrorist attack or a reputable news website visited by everyone who can steal personal and financial information, they can suffer millions within hours.

4.3 DNS Hacking:

(Sometimes referred to as DNS redirection) DNS hijack a computer's TCP / IP settings, thus invalidating the default DNS settings, pointing to a rogue DNS server, it replaces it is a kind of malicious attack. It pointed to a rogue DNS server , so that an attacker , to change its DNS settings when the computer takes control , in other words , a process known as DNS hijacking . As we all know, "Domain Name System (DNS)" its corresponding IP address "74.125.235.46" How to "google.com" as fundamental to provide a user- friendly domain name is responsible. DNS and getting a clear idea of the job you better understand about DNS hijacking can help. DNS is a fairly new concept to you.

4.4 How do abduct DNS?

It has already been mentioned, DNS user-friendly domain names to their corresponding IP addresses is responsible for matching is one. The DNS server of your Internet Service Provider (ISP) and many other private business organizations owned and maintained. By default, the DNS server your ISP's computer is configured to use. In some cases, your computer also other well-known organizations such as Google's DNS service may be using. In this case, you said to be safe and everything seems to work normally are However, your computer hacker now owned and maintained one of the rogue DNS servers so that a hacker or malware program uses, you gain unauthorized access to the computer and change the DNS settings of the situation concept . When this happens, a rogue DNS server IP addresses of malicious Web sites (such as banks, search engines, social networking sites etc.) required Web site domain names can be translated. In the address bar, type the URL of a site, as a result, you are instead intended for you, one that can be taken to a fake Web site. Sometimes, it can put in deep trouble!

4.5 What are the dangers of DNS hijacking?

DNS hijacking risks vary and can depend on the intention behind the attack. Such "open DNS" and the introduction of advertising or data collection to "HDD" Use as many ISPs DNS hijacking. These users can cause any serious damage, though it answers the DNS RFC standards is considered as a violation.

DNS hijacking attacks and other risks include the following:

4.5.1 Pharming: This is a counterfeit of a web site traffic that is redirected to another website where a variety of attacks. For example, a user who is filled with pop-ups and ads that can be redirected to a site such as Facebook.com, a social networking website that tries to. It is often to generate advertising revenue is used by the hackers.

4.5.2 Phishing*:* these users whose design (look and feel) exactly matches with the original one are redirected to a malicious Web site where the attack is a type. A user attempts to log in to their bank account when, for example, he steals login details redirected to a malicious web site can be.

4.6 How to prevent DNS hijacking?

In most cases, the attackers carry out such kidnappings for DNS as a Trojan horse malware programs make use of DNS hijacking Trojan in the video and audio codec, video downloader of you tube downloader or other free utilities are distributed as. So, to stay safe , away Free offer reliable web sites for the UN to stay is recommended . DNS Changer Trojan through fraudulent advertising revenue profits of U.S. $ 14 million to drive more than 4 million computers hijacked DNS settings that are an example of one such malware. The attackers came with the factory setting using the default password on your router settings to modify it so that it would not be possible, it changed your router's default password it is important to. For more details on this topic you hack an Ethernet ADSL Router How you can read my other post. Install a good antivirus program and keep up-to- date against any attacks from your computer can offer a great deal of protection.

4.7 Do you already suffer from DNS hijacking?

On your computer such as DNS Changer malware program is inspired by a suspect, you do not need to panic. The damage caused by such a program very simple and easy to deal with. All you have to do, just make sure you are blacklisted IPs of the DNS are not any use to verify your current DNS settings. Otherwise as directed by your ISP reset your DNS settings.

4.8 USED OF ANGRY SCANNER: Hacking the ADSL Router:

www.whatismyipaddress.com to: the risk of an ADSL router has detailed information on how to take advantage. One time the page loaded, you will find your Internet Protocol address. Angry IP Scanner down. Open Note that here you will see an option called IP range: 117.192.195.101 for suppose that your IP range to scan IP address is required to enter, you 117,192,200,255 SP is the limit as 117.192.194.0 can set some extent at least 200-300 IP addresses.

4.8.1 Tools:

Preference and choose the Ports tab. below Port selection enter 80 (we need to scan for port 80). Now, switch to the present tab option "Hosts with open ports only" select and click on OK.

4.8.2 Network Security Threats:

Different threats at each layer in OSI model can be summarized as in table.

Layers	Attacks
Physical Layer	Jamming, Tampering
Data Link Layer	Jamming, Collision
Network Layer	Spoofing or replaying information, Selective forwarding or black holes, Sink holes, Sybil attacks, Node replication attacks, Wormholes Flooding, Attacks against privacy
Transport Layer	Injects false messages , Energy drain attacks
Application Layer	Attacks on reliability

4.9 The Invisible Shield:

One said that the security measures in medicine when it comes to a situation like this is " no harm, first." - By enacting more restrictive policies for their working employee has the ability to harm. When you are trying to prevent bad in other words, do not block well.

For example, the United States Computer Emergency willingness Team java scrip, java and active4 x controls plug- INS and pop up to disabled as recommended in January of 2008. It equally benefits of some of these features, and the average user is not a realistic approach that offers more than a bunker mentality. There is a more rational approach. Their most basic level, cybercriminals to thwart the best approach may be called in three steps:

a. The friendly and incoming web traffic comes, enterprises must scan everything, and if possible, without delay.

b. For someone with a laptop, a two -factor passwords, identity based control and encryption is necessary for the employee.

c. For web developers, with security as a primary concern the design of sites and regular penetration tests must be run.

Especially for an enterprise, to one another without compromising security and performance balance that must create a secure web gateway. Such a secure gateway includes the following:

✧ To filter a huge cache determine a proxy tool scans all web traffic , content caching never affected gateway transient objects Scan for updates again.

✧ Internet is 75 +% unrated content objectionable and unproductive employee exposure, plus a real-time service to reduce the rate of URL filter.

✧ Leverage active script control features while having an allow list of approved "drive-by" updates.

✧ Anywhere on the network has an opportunity to process web content before it is heuristic and behavioral analysis engine with the best generation of online anti-malware software deployment.

✧ Leverage control features that allow active scripting in the list of the “drive-by " approved updates.

✧ Never caching confidential information, encrypted web traffic analysis for risks to increase the efficiency in the use of SSL hardware acceleration.

✧ Data loss prevention solutions such as third-party integration, an open architecture to implement gateway.

✧ Their desired policy, in addition to planning for Internet traffic exploded with full load efficiency for large -scale and secure web gateway failed tests and scenarios.

✧ Regardless of location or policy choices LAN performance and security standards.

✧ Prevention of hazards, while providing all the benefits of Web 2.0.

✧ These organizations from many different vendors of hardware and software products are faced with a myriad, but piecing together a solution to its own problems in terms of management, and product safely exceed where the difference cannot leave.

5. CONCLUSION

Secure system software environment an overview of current techniques with a focus on kernel security components is presented. Safe Kernel Programming Architecture thick implemented secure operating system kernel software security components such theory recognized for security concerns, buffer overflows and imprisonment are discussed. The main purpose of this paper threats and system software practitioner community is to raise awareness about the exploitation. Due to the risks obscuring techniques to block the implementation of a special affair. Organized cybercriminals will continue to search for vulnerable targets, and any day your company's security and malware that threatens both your wallet could bring a new wave is still. Information to steal his identity and that uses stealth weapons is a war, and the best defense, the best comprehensive offering of hardware and software solutions to protect your computer system.

REFERENCES

[1] Jim Alves-Foss, W. Scott Harrison, Paul Oman and Carol Taylor. “The MILS Architecture for High-Assurance Embedded Systems”. International Journal of Embedded Systems at http:/ /citeseerx.ist.psu.edu/viewdoc/download? doi=10.1.1. 76.6810 &rep=rep1&type=pdf

[2] Clark, D. D., and Wilson, D. R. 1987. “A Comparison of Commercial and Military Computer Security Policies.” In Proceedings of the 1987 Symposium on Security and Privacy, pp. 184-95. Washington, D.C.: IEEE Computer Society.

[3] Ames, S. R., Jr.; Gasser, M.; and Schell, R. R. 1983. “Security Kernel Design and Implementation: An Introduction.” Computer 16(7):14-22. Reprinted in Advances in Computer System Security, vol. 2, ed. R. Turn, pp. 170-77, Artech House.

[4] Steve Bellovin. “Buffer Overflows and Remote Root Exploits”.Personal Communications,October 1999. 4.Butler W. Lampson. 1973. “A note on the confinement problem”. Communication , ACM 16, 10 (October 1973), 613-615

[5] Jesse C. Rabek Roger I. Khazan Scott M. Lewandowski Robert K. Cunningham, “Detection of Injected, Dynamically Generated, and Obfuscated Malicious Code”, Copyright 2003 ACM

[6] Michael Zhivich, Tim Leek, Richard Lippmann, “Dynamic Buffer Overflow Detection”,

[7] David Evans and David Larochelle, “Improving Security Using Extensible Lightweight Static Analysis”, IEEE computer Society 2002

[8] Bas Cornelissen,Andy Zaidman,Arie van Deursen, Member, Leon Moonen, Member,Rainer Koschke, “A Systematic Survey of Program Comprehension through Dynamic Analysis”, IEEE Computer Society 2009

[9] Morrie Gasser. 1988. “Building a Secure Computer System”. Van Nostrand Reinhold Co., New York, NY, USA.

[10] https://support.microsoft.com/kb/2984615 on 12/08/2014

[11] http://www.tenouk.com/Bufferoverflowc/Bufferoverflow6.html

[12] Jim Alves-Foss, W. Scott Harrison, Paul Oman and Carol Taylor. "The MILS Architecture for High-Assurance Embedded Systems". International Journal of Embedded Systems at http:/ /citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.76.6 810 &rep=rep1&type=pdf.

[13] Ken Thompson, "Reflections on Trusting Trust", Communications of the ACM, August 1984, Volume 27, Number 8, pp. 761-763.

[14] Kernighan, B.W., and Ritchie, D.M. "The C Programming Language". Prentice-Hall, Englewood Cliffs, N.J., 1978.

[15] EUROSEC GmbH Chiffriertechnik & Sicherheit, "Secure Programming in C/C++", ver 1.0, July 2005, http:// www.secologic.org/downloads/c/051207_EUROSEC_Draft_ Whitepaper_Secure_C_Programming.pdf

[16] Android Architecture, Available at: http://www.android-app-market.com/android-architecture.html

[17] Rajib K. Mitra, (1998), "UNIX Security", online, http:// www.spy.net/~jeeb/unix_security.html.

[18] Crispin Cowan, Calton Pu, Dave Maier, Heather Hinton, Peat Bakke, Steve Beattie, Aaron Grier, Perry Wagle, and Qian Zhang. "StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks". In 7th USENIX Security Conference, pages 63-77, San Antonio, TX, January 1998.

[19] Lampson, B.W., "Dynamic protection structures", Proc. AFIPS 1969 FJCC, Vol. 35, AFIPS Press, Niontvale, N.J., pp. 27-38.

[20] "Stack buffer overflow " http://wikipedia.org/wiki/ Stack_buffer_overflow.htm (Oct. 08, 2012)

[21] Bob Page,(1988, November 7), "A Report on the Internet Worm", [online], http://www.ee.ryerson.ca/~elf/hack/iworm.html.

[22] "Witty Worm targets BlackICE PC Protection systems (ICQ_Witty_Worm)", [online], http://www.iss.net/security_center/reference/vuln/ICQ_Witty_Worm.htm.

[23] Paul Boutin, (2003 July), "Slammed! An inside view of the worm that crashed the Internet in 15 minutes", Issue 11.07, [online], http://www.wired.com/wired/archive/11.07/ slammer.html (Oct. 08, 2012).

[24] "Blaster (computer worm)", (2012 December 26), [online], http://en.wikipedia.org/wiki/Blaster_worm.

[25] http://www.codenomicon.com/resources/whitepapers/2013-ovum-whitepaper-zerodays-in-finance.pdf.

[26] http://en.wikipedia.org/wiki/Software_cracking.

[27] http://www.theatlanticwire.com/global/2013/05/china-hackers-pentagon/65628/.

[28] http://www.theblaze.com/stories/2013/06/10/tense-ed-henry-confronts-jay-carney-on-obama-22.statements-during-white-house-press-conference/.

[29] Blue Coat Cyber Crime Agency.

[30] http://www.teckh.com/?p=143.

[31] Bishop, D. Introduction to Cryptography with Java.

[32] Applets. Jones and Bartlett, Sudbury, MA, 2003.

[33] www.staysafeonline.inf.