International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 3, Issue 3, May 2014, 45- 50

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

ERD-OS: A MAJOR THREAT TO OPERATING SYSTEM SECURITY

JITHIN JACOB[1], PRINCE V JOSE[2], ANURAJ C. K[3] & SUREKHA MARIAM VARGHESE[4]

[1, 3]Assistant Professor, Department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering, M.G University College of Engineering, Thodupuzha, Kerala, India

[4]Professor, Computer Science and Engineering Mar Athanasius College of Engineering, Kothamangalam, Kerala, India

ABSTRACT

Emergency Repair Disks are used to recover and backup data during an operating system failure or corruption. ERD's Can by-pass installed operating system and give throughout access to the system. ERD-OS is also known by the names By-pass loader or Hacker's OS or Mini OS. Now a day this became a popular way to attack systems due to several features of ERD-OS. None of the current Operating systems are unable to withstand this attack. ERD-OS works on all systems irrespective of the operating system installed in the system. On the other hand ERD can be used as an efficient way to recover data during an operating system crash or failure. This paper gives information about ERD-OS attack and the ways to prevent the same.

KEYWORDS: BIOS, Confidentiality, ERD-Emergency Repair Disk, Integrity, OS-Operating System

INTRODUCTION

Computer security is a branch of technology known as information security as applied to computers and networks. The objective of computer security includes protection of information and property from theft and corruption, while allowing the information and property to remain accessible and productive to its intended users [1]. Operating system plays a vital role in providing the system security. Microsoft, One of the pioneer firms in operating system development gives the caption "Experiencing the Ultimate in Security and Privacy" for their operating systems like windows 7 and windows 8.

One of the main functions of the operating system is to protect data and prevent unauthorized access to data and program. Most operating systems provide some form of authentication, authorization and access control mechanisms and privilege levels to provide the user with the ultimate security and privacy that they need. There are many elements that are disrupting computer security. Any type of method /mechanism which helps to loosen the security or uncovering the protection of information and information systems by means of unauthorized access, use, disclosure, disruption, modification or destruction of data and programs can be considered as a security breach.

In some situations the faults in OS itself will lead to security breaches. To ensure reliable operation and to preserve integrity of stored information; it is necessary to discover new security breaches prevailing in a particular environment and learn their causes and implications in the environment. A good knowledge about the methods and means for security violations and proper assessment of the existing mechanisms are very essential for building secure systems and for enhancing security of existing systems. Main focus of this paper is one of the growing security concerns, improper

utilization of the emergency repair tool provided by OS vendors. Almost all commercial operating systems now in use have to bend their knees in front of Emergency Repair Disk Operating System (ERD – OS) on the aspect of security. The Evolution of the attack scenario, different perspectives of the ERD tool, working and methods to withstand ERD attack are discussed in different sections of this paper.

EVOLUTION

The corruption or failure of operating system due to any reason will impart much severe effect in large organization including data loss. In such situation the system should be restored or re – installed with a fresh operating system without losing data. Hackers OS or ERD-OS was developed with the intention of retrieving data during emergencies. ERD-OS facilitates login and access to system resources without base operating system. This is possible even in situations like operating system fails to load properly. No credentials are required to get access to the normally protected data and programs with all the privileges of an administrator. Several companies are making use the ERD-OS of Microsoft and similar products developed by them to retrieve their highly valuable data during emergencies like system crash. This ERD-OS are available in different forms and names like Emergency repair System (ERS), By-pass loader, Hacker's – OS, ERD – commander CD and By-Pass OS. Hirens boot cd is a typical example of ERD-OS / Hacker's OS.

This tool was originally used by companies to handle critical situations such as OS failure. But the problem lies in the fact that this supporting tool for handling emergencies can cause a real security threat. Hackers with wrong intention can utilize the ERD-OS for retrieving the private, highly confidential and supposed to be secured data's and programs. These Organizations were using this only in the situations where operating system fails. When this came to Hacker's side they explored ERD's as the best way to attack a system because an ERD never leaves a single trace of the attack happened to the system even if the operating system of the attacked machine is working properly. Hacker's later modified the typical traditional ERD that's being used in organizations with additional features such as password viewer (shows all the passwords and email ids used by the user in the installed operating systems), wireless key viewer (shows keys of nearby wireless network) etc.

DIFFERENT PERSPECTIVES

Hacker's View

Most systems provide tight security measures in order to protect the information from potential intrusion or disruption. The simplest way to execute an attack with an intention of information theft, corruption or disclosure is to depend on ERD. The specialty about ERD is that it never leaves a single trace to identify that the attack has happened. The attack will never change the system from its previous properties or states, which ensures that the user of the system will never detect the occurrence of an attack. Though there are several ways to execute the attack, in most of the methods, the existing credentials of the system or users get affected. This includes the modification/insertion of features like usernames and passwords. The affected user of the system can use these traces to for manual/automatic detection of the attack occurrence.

User's View

The most effective, simple and efficient way to recover and restore information and data during an operating system crash or failure is by using ERD.

ERD follows only simple steps so that a normal user with this ERD can restore or recover data easily when needed.

BACKGROUND AND RELATED WORKS

Security in computer systems is strongly related to the notion of dependability. Informally, a dependable computer system is one that we can justifiably trust to deliver its services [2]. Dependability includes availability, reliability, safety, and maintainability. However, if we are to put our trust in a computer system, then confidentiality and integrity should be taken into account. Confidentiality refers to the property of a computer system whereby its information is disclosed only to authorized parties. Integrity is the characteristic that alterations to a system's assets can be made only in an authorized way. In other words, improper alterations in a secure computer system should be detectable and recoverable. Major assets of any computer system are its hardware, software, and data. Operating system developers always try to develop operating systems that are stringent to confidentiality and integrity. However the operating systems developed till now are unable to with stand with ERD attack. All the security aspects like dependability, availability, integrity and confidentiality gets violated with ERD attack.

ERD – attack exploit the un awareness of the computer system user. Many of the users never heard about an attack like this till now. Several users are using modern security features like face recognition and finger print recognition to login in the system as an additional security measure. Many of these additional security measures are available inbuilt in modern laptops. However these additional or advanced security features like face recognition and finger print recognition based methods also gets failed in front of ERD. By using an ERD we can access the entire hard disk of the system this discloses the data of the authorized user (confidentiality fails). After accessing user data, it can be altered or even corrupted (Integrity Fails).

The ERD attack works on all systems Irrespective of the operating system installed in the machine. For example if we are using the ERD-OS of a Windows – XP or any other Windows version in a windows based machine all the drives will be accessible that is we can access all the data stored in the storage media of the machine. If we are using a windows based ERD-OS in a Linux based or Mac based machine, partition of hard disk which is formatted in NTFS or FAT is easily accessible but a non windows compactable partition cannot be accessed. Even though those non compactable partitions can be formatted with ERD-OS which will result in data loss (integrity and data availability fails).

WORKING

The ERD-OS works in a very user friendly manner, which makes hacking very easy and simple for everyone. The primary resource required for the ERD–attack is a bootable CD with ERD tool kit. So the first step towards implementing the attack is to change the BIOS settings to enable booting from the CD. Various steps associated in executing the ERD attack is enumerated below.

Step 1: Enter the BIOS setup by pressing the corresponding key (usually F2, F8, F12 or DEL)

Step 2: Go to boot device priority in Boot manager and select CD / DVD – R/RW as the first boot device.

Step 3: Save changes and exit the BIOS setup by using the corresponding key (usually F10)

Step 4: Now the System will restart and gets booted from the CD.

Step 5: The ERD – OS will now get loaded and the entire hard disk and will be accessible in a couple of minutes.

Step 6: System is now open for hacker with supervisory privileges. All the protected data and privileged programs are now accessible to the hacker without any barrier. So the hacker can retrieve, insert, modify and delete the programs and data which may lead the system to a very dangerous situation. Data manipulation operations may include

Step 7: After retrieving all the important data and completing all the intended tasks, the system can be restarted to revert the changes made in the BIOS setup.

CASE STUDY

Bit locker Drive encryption in windows 7 and windows 8. Bit Locker Drive Encryption is a full disk encryption feature included with the Ultimate and Enterprise editions of Microsoft's Windows Vista and Windows 7 and with the Professional and Enterprise editions of Windows 8 desktop operating systems, as well as the server platforms, Windows Server 2008, Windows Server 2008 R2 and Windows Server 2012. It is designed to protect data by providing encryption for entire volumes. By default it uses the AES encryption algorithm with a 128-bit or 256-bit key [3]. Bit Locker helps to protect data on lost or stolen computers by encrypting the entire system volume and any partitioned data volumes. Bit Locker provides a seamless, secure, and easily manageable data protection solution. Bit Locker enhances data protection by bringing together two major sub-functions: drive encryption and the integrity checking of early boot components. Drive encryption protects data by preventing unauthorized users from breaking Windows file and system protection on lost, stolen, or inappropriately decommissioned computers [4].

When approaching a Bit Locker encrypted drive with an ERD-OS attack, the drive never gets opened or accessible and the data is under safe custody even though we can format the entire drive or partition which is encrypted with Bit locker resulting in Data loss (Integrity and data availability fails).So in over all we can say Bit locker also fails to protect data in the system.

SOLUTIONS

The existing system is unable to prevent ERD attack completely.

Temporary methods to withstand ERD attacks

Setting a BIOS Password

The user can set a BIOS password (superior or master password). Whenever the system gets turned on, it will ask for BIOS password before booting up. The system will boot with ERD only if the password is provided correctly. But the main demerit of this method is that a BIOS password can be easily cleared. It can be cleared by removing the CMOS battery in the mother board and turning the system on. In this situation ERD attack will work well with the system. The only advantage is user can just suspect that something had happened to the system because the BIOS settings are cleared.

Smart Card Based Security Access Control

Smart cards can be used for turning the system on. Therefore a person with the original smart card can only access the system. The main demerit of this method is that cost of smart cards is very high.

There are no permanent methods to withstand ERD – attack till now.

CONCLUSIONS

ERD-OS is a very serious security threat to all operating systems. It is an excellent tool for hackers and the possibilities of misuse using ERD are endless. Using ERD technique, the attacker can gain unlimited access without any difficulty and the attack can cause loss of confidentiality, Integrity and availability of data. Current protection mechanisms in commercial operating systems are inadequate to defend against the ERD attack. Existing systems do not provide a permanent solution to defend against the ERD attack. More study and research is required for the development of effective mechanisms for the identification, detection and protection from ERD and similar attacks.

ACKNOWLEDGEMENTS

We would like to take this opportunity for expressing our profound gratitude and deep regards to all teaching and non-teaching staffs of the department of Computer Science and Engineering, Mar Athanasius College of Engineering, Kothamangalam, Kerala, Mr. Dileep Lal (Associate Professor, Department of Mechanical Engineering, Mar Athanasius College of Engineering), Mr. P. Tharcis (Head of the Department, Computer Science and Engineering, Christian College of Engineering and Technology Tamil Nadu), Mr. P.G RAJAN (Head of the Department, Science & Humanities, Christian College of Engineering and Technology Tamil Nadu) Mr. Dennis Ebenezer (Assistant Professor Department of Computer Science and Engineering, Christian College of Engineering and Technology Tamil Nadu) and Mrs. Suma Sara Jacob (Assistant Professor Department of Computer Science and Engineering, Christian College of Engineering and Technology, Tamil Nadu) for their guidance, monitoring and constant encouragement throughout the preparation of this paper.

REFERENCES

1. International Journal of Multimedia and Ubiquitous Engineering Vol. 2, No. 2, April, 2007: IT Security Review: Privacy, Protection, Access Control, Assurance and System Security.
2. IEEE International Symposium on Fault -Tolerant Computing, Pasadena, California, USA, June 27-30, 1995, Special Issue, pp. 42-54. Dependable Computing: Concepts, Limits, Challenges.
3. http://en.wikipedia.org/wiki/BitLocker_Drive_Encryption.
4. http://download.microsoft.com/ Download /9/0/ 1/9019efd5-043f-4c17-9c33-793ca68c7c78/Bit Locker_ 01_Sales_ SALES_Datasheet.pdf.

AUTHOR'S DETAILS

Jithin Jacob Former, Assistant Professor, Department of Computer Science and Engineering Mar Athanasius College of Engineering, Kothamangalam Kerala. He received his B.E Degree in computer science and Engineering from Christian college of Engineering and Technology, Tamil Nadu and M.E in Computer Science and Engineering from

Sapthagiri College of Engineering, Tamil nadu, affiliated to Anna University. Areas of interests are computer security and operating systems.

Prince V Jose is currently working as Assistant Professor in the Department of Computer Science and Engineering, Mahatma Gandhi University College of Engineering, Thodupuzha, Kerala, India. He received his B-Tech Degree in Computer Science and Engineering in 2011 from Mahatma Gandhi University College of Engineering, Thodupuzha, affiliated to Mahatma Gandhi University. He has more than 2 years of teaching experience. His area of interests include Computer Architecture, Microprocessors, Digital electronics, Operating Systems

Anuraj C.K is currently working as Assistant Professor in the Department of Computer Science and Engineering, M.A. College of Engineering, Kothamangalam, Kerala, India. He received his B-Tech Degree in Computer Science and Engineering in 2011 from Adi Shankara Institute of Engineering and Technology, Kalady affiliated to Mahatma Gandhi University. He has more than 2 years of teaching experience. His area of interests include Internet Computing, Network Security, Computer Graphics, Operating Systems.

Surekha Mariam Varghese is currently heading the Department of Computer Science and Engineering, M.A. College of Engineering, Kothamangalam, Kerala, India. She received her B-Tech Degree in Computer Science and Engineering in 1990 from College of Engineering, Trivandrum affiliated to Kerala University and M-Tech in Computer and Information Sciences from Cochin University of Science and Technology, Kochi in 1996. She obtained Ph. D in Computer Security from Cochin University of Science and Technology, Kochi in 2009. She has more than 20 years of teaching and research experience in various institutions in India. Her research interests include Network Security, Database Management, Data Structures and Algorithms, Operating Systems, Image Processing, Computational Intelligence and Information Retrieval. She has published 10 papers in international journals and international conference proceedings. She has served as reviewer, committee member and session chair for many international conferences and journals.