Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-14

Manage Clipboard to Prevent Copying Important Files

Abstract--Traditional security measures have been developed to protect computer system and data within mainly against outside attackers. However, in modern world, new types of threat arise due to bribable employee. Insider threats have potential to inflict severe damage to organization's resources, financial assets and reputation. There are many types of insider threats which can break confidentiality, integrity, or availability. This paper focuses on the violations of confidentiality and integrity by privilege misuse or escalation in sensitive applications. First, we analyze and identify insider-threat scenarios that compromise confidentiality and integrity. We then discuss how to detect each threat scenario by analyzing the primitive user activities. We have implemented a threat detection mechanism by extending the capabilities of existing software packages. Since our approach can proactively detect the insider's malicious behaviors before the malicious insider's goal is achieved, we can prevent the possible damage proactively. In this paper we apply our ideas to the Windows environment as well as Linux environment.

Keywords--Active Detection, Monitoring, Insider Threats

Mrs. Nataasha Raul
Asst. Professor,
Sardar Patel Institute of Technology,
Mumbai, India
Priyank Chheda
Student,
Sardar Patel Institute of Technology,
Mumbai, India
Siddhesh Karode
Student,
Sardar Patel Institute of Technology,
Mumbai, India
Neha Lokhande
Student,
Sardar Patel Institute of Technology,
Mumbai, India

1. Introduction

In today's world, security is the biggest issue in each and every area whether it may be security for some reputed organization or for some local shopping–mart. Researcher and various vendors are developing systems like firewall, access control, intrusion detection, authentication and cryptography to protect organization's important and sensitive data from outside world. Although the primary objective of these types of system is to protect data from cyber-attack, in modern world, a new type of threat came in picture - insider threat. An insider is an individual who already possesses a certain level of privileges and trust within an organization based on their job functionalities. Now here, Outsider must gain access and privilege to a target system by implying some types of attack like social engineering in order to compromise that system, an insider generally inherits those capabilities by default due to their job functionality. According to Oak Ridge National Laboratory (ORNL), Insider sourced espionage, sabotage, and frauds are now considered as the top cyber threat. Cost estimates approach $1,000 billion/year from modification of data, security mechanism, unauthorized network connections, covert channels, and physical damage and destruction including information extrusion[8]. Hardest hit industries are banks and insurance companies with 60% of cyber-crime in banks carried out by insiders (65% being senior managers). Therefore, a great need

Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-14

still exist for a real-time, lightweight detection and mitigation system for insider misuse.

An insider threat can damage an organization in various ways, and often the damage in dollars and reputation is permanent. For instance, when an attacker exposes a bank database of credit card numbers, there will be financial loss as well as the negative impact on the bank's brand value. After the attack is being carried out, conventional forensics technologies, which help companies identify and prosecute a criminal offender. Advanced digital forensics, which monitors and audits computer systems in real-time, can be used to strike against insider misuse. However, considering the large scale of modern systems, applying digital forensics in real-time is a daunting task, since there are so many files and processes to monitor[1].

The primary objective of this research is to mitigate insider threats against sensitive information stored in the organization's computer system. In this paper, we focus on four generic threat scenarios against confidentiality and two generic threat scenarios against integrity. The detection of each threat scenario is carried outby analyzing the insider activities in terms of Copy, Rename, Print, Paste or modifying the sensitive files. We have implemented our detection or in some cases prevention mechanism by extending the capacities in Windows and Linux environments.

2. Related System Components

The information about the system components that have been used to implement the proposed system are given below. Some components described below works only with Windows operating system, some with only Linux Operating System and some works for both the Operating System. We have specially considered cost-effectiveness, reusability, compatibility, and extensibility.

2.1 File System Filter Driver

A filesystem filter driver[4] is an optional driver that adds value to or modifies the behavior of a file system. A file system filter driver is a kernel-mode component that runs as part of the Windows executive. A file system filter driver can filter I/O operations for one or more file systems or file system volumes. Depending on the nature of the driver, filter can mean log, observe, modify, or even prevent. Typical applications for file system filter drivers include antivirus utilities, encryption programs, and hierarchical storage management systems. The main disadvantage of this component is that it is not cross-platform.

2.2 System Clipboard

The clipboard[3] is a software facility used for short-term data storage and/or data transfer between documents or applications, via copy and paste operations. Clipboard is a set of functions that enable applications to transfer data within the System. It can store data in various format viz. RTF, HTML, TXT, JPG and many more for a short term period that can be easily transferred between via the Copy/Paste operations. All programs within the system have access to the temporary data buffer. Clipboard Viewer can be used to view the content of the clipboard whereas Clipboard Manager is used to manage to the data within clipboard buffer. Using Clipboard Manager, we can change the content of clipboard; we can even clear the clipboard buffer.

We use this component to check if there is any sensitive information in the clipboard or not, if there is, then we clear the clipboard so that the sensitive information doesn't get copy to an unapproved location.

2.3 Linux dmesg Command

The dmesg[9] command is used to write the kernel messages in Linux and other Unix-like operating systems to standard output (which by default is the display screen). A kernel is the core of an operating system. It is the first part of the operating system that is loaded into memory when a computer boots up (i.e., starts up), and it controls virtually everything on a system. The numerous messages generated by the kernel that appear on the display screen as a computer boots up show the hardware devices that the kernel detects and indicate whether it is able to configure them.

Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-14

dmesg obtains its data by reading the kernel ring buffer. A buffer is a portion of a computer's memory that is set aside as a temporary holding place for data that is being sent to or received from an external device, such as a hard disk drive (HDD), printer or keyboard. A ring buffer is a buffer of fixed size for which any new data added to it overwrites the oldest data in it.

We will use this utility to detect if there is any external storage device attached to the computer. We can even use this utility/component for detecting what is printing via printer.

2.4 Printer Monitoring Software

Printing (either hardcopy or softcopy) is one of the most common methods of unauthorized information leaking. Therefore, monitoring printer log is essential measure to protect the confidentiality of the organization's sensitive information. Unfortunately, there are no built-in tools in Windows or in Linux to monitor printer. Now, there are two ways to achieve this objective. One is to use the third-party software for monitoring printer logs. For Windows, we have to use SoftPerfect's Print Inspector[2] and for Linux, we can use CUPS[7] (Common UNIX Printing System) for monitoring Printer's Activity.

Another way is to create your own Printer monitoring program using dmesg and various other utility. The advantage of this method is that you can customize the program as per your need. Printing of sensitive files by unauthorized users can also be prevented.

3. Insider Threat Scenarios

There are various scenarios in which an insider can copy, modify or delete sensitive information. For example, Insider can copy data to some external device or he/she can upload that sensitive file on internet. In this paper, we assume that direct file transfer to an outside machine (e.g. via FTP, HTTP, Email attachment, etc.) can be detected and foiled by existing security mechanisms such as firewall or Intrusion detection System (IDS). There are many threat scenarios, but this paper mainly focuses on six scenarios. The threat scenarios are divided into two parts- threat scenarios against confidentiality and threat scenarios against integrity.

The threat scenarios[1] against confidentiality are as follows:

Scenario #1 – Copying a sensitive file to an unapproved location;

Scenario #2 – Renaming sensitive file;

Scenario #3 – Copying content from a sensitive file;

Scenario #4 – Printing sensitive contents;

The threat scenarios against Integrity are as follows:

Scenario #1 – Modifying sensitive file;

Scenario #2 – Deleting Sensitive file.

4. Threat Prevention

4.1 Managing clipboard for preventing Insider threats

Copying sensitive data is a threat where insider copy sensitive file and sell those data to competing company. As mentioned earlier, we are assuming that direct file transfer to an outside machine can be detected by existing security mechanisms such as firewall or IDS.

Whenever we press "*ctrl+c"* or copy any data by mouse, it is stored temporarily in clipboard. And when we press "*ctrl+v"* or click paste by mouse, whatever data present in clipboard gets pasted in specified location. For preventing copying sensitive files, we continuously check the clipboard for sensitive data or files. If sensitive data is present in clipboard, we clear the clipboard so that the insider will not be able to paste it as clipboard is empty.

In Windows, clipboard[3] management system is somewhat complicated. Windows maintains a list of clipboard viewer called Clipboard Viewer Chain[5]. This is a global list and all applications share it. Windows maintain reference to only first member in the list and member maintains its next viewer reference. If we want our application to use clipboard then we have to register our viewer to this list. When clipboard changes, Windows sends WM_DRAWCLIPBOARD message to the first member of the chain. This member has to process the event and pass it to the next member in the list whose reference it maintains.When any viewer wants to exits the chain then it should unregister itself and send reference of the next member it holds to its own reference. In this case, Windows sent WM_CHANGECBCHAIN to first member of the list which processes it and sends it forward.

To implement the above concept we maintain a list of all sensitive files. We have made this list hidden so that no one can access this list, not even authorized user. We created a program which is used to maintain the hidden list. By this program, we can add address of the file which we want to make sensitive, we can remove sensitive file status by removing name from list and even copy this sensitive file to other location. For more security, we

Proc. of the Intl. Conf. on Advances In Engineering And Technology - ICAET-2014

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-14

have carried this program in portable storage device like pen drive, so that pen drive can only be accessed by authorized user.

We have implemented the same system for preventing Scenario #3 using Python module win32clipboard[6]. In this, we continuously check the clipboard for certain keywords. If those keywords or combination of keywords are present in the clipboard, then we erase the content of the clipboard.

We can implement the same system by using Python's PySide QClipboard Library[10] making our code cross-platform. But the problem with this is that application becomes slow which is not flexible if we are monitoring large systems.

4.2 Hidden Backup to recover deleted information.

There are scenarios when completing organizations are not intend steal data; they just want to destroy it. Deleting a sensitive file can cause major losses in an organization. Therefore, it is important to find a way to prevent this threat.

By using any programming language you can check whether the file exists or not. For example, in Python, we can use the function *os.path.exists ()* to check whether the file is still there or not. If this function returns false, then the file is deleted. The problem with this method is we can only detect whether the file is deleted or not, we are not able to prevent it.

There are two methods to prevent deletion of sensitive files. First method is recovering the file from the hard disk. Whenever a file gets detected, the content of a file is not removed from the hard disk, only the reference to the file is removed. The drawback of this method is it takes a large amount of time to recover even a small file. Second method is to create a hidden backup. In this method, we can create a backup for all important files and the knowledge of this backup is only know to authorized person. And therefore only authorized person can access this backup data. To provide more security, we can create software for managing this hidden backup, so that the only way to access the backup is through software.

4.3 File System Filter Driver

As discussed earlier, a file system filter driver[4] is called on every file system I/O operation (create, read, write, rename, and etc.), and thus it can modify the file system behavior. File system filter drivers are almost similar to legacy drivers, but they require some special steps to do. Such drivers are used by anti-viruses, security, backup, and snapshot software. This is the most effective approach to prevent renaming, deleting, copying and even modifying the sensitive file from an unauthorized employee. And therefore File System Filter Driver address to problem mentioned in Scenario #1, #2, #5 and #6.

4.4 Printer Monitoring

Printing sensitive files is the most common approach by which an unauthorized person can get important information. Therefore, monitoring printer activity is essential. Unfortunately, there is no built-in application for monitoring printer. Therefore, we can use third-party software to monitor printer activity. We can use SoftPerfect's Print Inspector[2] for windows and CUPS[7] for Linux operating system. By this third-party software, we can only detect whether the sensitive is getting printed or not. But we are not able to prevent it. Another way is to create our own printer monitoring software which can detect as well as prevent sensitive file from getting printed.

5. Conclusion

In this paper we have analyzed and identified insider threat scenarios that compromise confidentiality and integrity. We then discussed how to detect each threat scenario by analyzing the primitive user activities. We have also implemented our detection mechanisms by extending the capabilities of existing software packages. In this mechanism, we were able to detect the malicious activity by the insider and were able to prevent this malicious activity to some extent.

ISBN: 978-1-63248-028-6 doi: 10.15224/ 978-1-63248-028-6-01-14

Reference

[1] Joon S. Park, JaehoYim, Jason Hallahan. Mitigating Insider threat by Active Detection.In Proceeding of Journal of Modern Internet of Things, 2013.

[2] Print Inspector. SoftPerfect, 2014.http://www.softperfect.com/products/pinspector/

[3] Windows Clipboard. MSDN, Microsoft, 2014. http://msdn.microsoft.com/en-us/library/windows/desktop/ms648709

[4] Introduction to File System Filter Drivers. MSDN, Microsoft, 2014. http://msdn.microsoft.com/en-us/library/windows/hardware/ff548202(v=vs.85).aspx

[5] Clipboard Viewer Chain. http://vikramwadnere.blogspot.in/2010/12/clipboard-viewer-chain.html

[6] Python Module win32clipboard Documentation. http://docs.activestate.com/activepython/2.4/pywin32/win32clipboard.html

[7] Common UNIX Printing System (CUPS). http://www.cups.org

[8] Intelligent Insider Threat Detection and Prevention- (IITDP) http://www.ioc.ornl.gov/factsheets/IITDP020210.pdf

[9] dmesg – Linux Command – Unix Command http://linux.about.com/library/cmd/blcmdl8_dmesg.htm

[10] Python PySide.Qtcore.QClipboard Documentation http://srinikom.github.io/pyside-docs/PySide/QtGui/QClipboard.html