International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 533 – 536

Data Safeguarding against Internal and External Threats

Aditi S. Dixit, Abhilasha C. Devkar, Shreya S. Kela and Amruta S. Kulkarni
Maharashtra Institute of Technology, Pune,
adix981@gmail.com, abhilashadevkar@gmail.com, shreyakela02@gmail.com, amruta.kulkarni@outlook.com

Abstract **-** Today, many organisations use Information Systems to manage their sensitive and critical business related information. The need to protect such a key component of the organisation, and avoid data theft cannot be overemphasised. Data theft can be defined as the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information. The project on which this paper is based deals with the safeguarding of data against internal as well as external threats. The internal threats in this project deal with leakage of data from within an organisation by the means of mountable devices such as USB drives, while the external threats that are considered are those that corrupt data and cause its loss by means of ransomware attacks. Ransomware is malware for data kidnapping, an exploit in which the attacker encrypts the victim's data and demands payment for the decryption key. This paper describes the ways to thwart such external attacks by monitoring a set of folders for early detection of ransomware. On the other hand, internal threats are handling by means of encrypting data while transferring it over USB drives and other mountable devices.

Keywords **-** *Bitcoins, Encryption, Magic Number, Ransomware*

*****

I. INTRODUCTION

With the growing volume,velocity and variety of data, there is increased level of cyber attacks, and hence more attention is required to protect sensitive business and personal information, as well as safeguard national security.

Cyber crime is not only impacting large companies and multinational corporate who have their presence in the western hemisphere but also the Indian companies there are increasingly being targeted.

Hence, it is necessary to safeguard our computers from all types of Cyber security attacks including Ransomware attacks. The main concept behind this project can be given as follows :

- Safeguarding against Internal Threats : The software authenticates the USB drives by checking their Device ID which is unique for every device. In case of authenticated devices, the data to be copied will be transferred in encrypted format to ensure confidentiality.

- Safeguarding against Ransomware attacks : Ransomware enters the system through mails and downloads. The system warns the user before the user's crucial data gets corrupted by the ransomware, and also kills the process which is responsible.

II. RELATED WORK

Various families of ransomware and their action upon the user's data is discussed in [1]. Existing techniques work upon the principle of Anomaly based Intrusion Detection System. Anomaly based IDS studies the frequent patterns of functioning of malware and alarms the system when any different activity is observed, but this system is often prone to false positives, which is demonstrated in [2], [3], [4], [5], [6],[7]. We have used the principle explained in [8] which monitors the user's data changes instead of monitoring the processes that change the data.

The presence of data leakage is discussed in [9] which throws some light on the need for data leakage. The data leakage can be achieved through the use of USB devices. There are number of tools available in the market which try to solve the issue [10]. Our solution tries to overcome the issue by having customised solution for each individual as well as organisation based on the policy that they require.

III. IMPLEMENTATION DETAILS

I. Internal Module

In this module, the admin has to authenticate the devices and create policies according to each department based on which data can be transferred in an encrypted format, or not at all. He is the only legitimate person to add, remove or update policies. When the USB gets detected, it is authenticated and the policies associated with it are applied at the time of transferring data from desktop computer to USB.

- **Admin Module** : The Admin will get each USB registered by pressing the Save Button and then the information will be saved in the database in the form (Username, Policy Name, Device). When the user connects his USB, the Device ID will be checked internally with the existing Device IDs in the Database. Only if the Device ID of the connected USB is equal to the Device ID from the database, then the next functions are allowed or else the connected USB will be blocked.
- **Policy Creator**: The second function of the software is to set the policy for the organisation. The policy is set by the admin by selecting the file types which will be allowed to be

transferred via the connected USB. The file types will be selected department wise, since this provides more security and flexibility.

The 3 Functions which can be performed by the Admin are :

- **Add Policy**: Every time a new USB is connected the Admin will ADD the policy to the database. The admin has to add the Policy Name /Department name, Description and then select the file types which he thinks are required by the particular department. The selected file types are allowed to be transferred and the ones which are not selected will be deleted while getting transferred. On pressing the Save Button all the information will be stored in the database in the format (Policy Name, Description and all the selected file types per Department).
- **Edit Policy** : Sometimes the Department policies change and some new file types are to be added or some old ones have to be deleted. Hence, by using the EDIT option we can do this. The Search Button helps in retrieving the information from the database using the policy name i.e. the admin has to enter the name of the department and then that policy will be searched in the database and all the related information will be displayed on the screen. Then the admin has to make the required changes and then again save it. The Save option just updates the database. By pressing on the Search Button, the existing file types allowed for the computers department will be displayed. Then the changes can be made and saved to the database. The Save Button will update the database.
- **Delete Policy**: The Delete option will just delete the entry from the database. The Policy is searched by the Policy Name in the Database and if the searched Policy Name exists, then it is deleted from the Database.

- **Device ID Identification** : The first function of the software is checking the DEVICE ID for each USB. A device instance ID is a system-supplied device identification string that uniquely identifies a device in the system. The DEVICE ID has the format USBVIDv(4) PIDd(4)REVr(4) where v(4) is the 4-digit vendor code that the USB committee assigns to the vendor. d(4) is the 4-digit product code that the vendor assigns to the device. r(4) is the revision code. The Entire Device ID is always unique. The Plug and Play (PnP) manager assigns a device instance ID to each device node (devnode) in a system's device tree. Hence, by using the PNPDeviceID from Win32DiskDrive where InterfaceType='USB' we can get the unique Device ID. By clicking on the button Get Device ID we can get the unique Device ID of the connected USB.
- **Directory Watcher** : The next function of the software is to monitor the connected USB drive. The Directory Watcher is the module which is continuously running as a background process and pops up a notification saying directory changed whenever changes are made in the Drive. The changes can be like creating a folder, creating a new file, creating a file in the folder, updating the contents of the file, renaming a file or deleting the file. Any small change made in the folder will be notified.

This module is used when the user tries to copy the data to the USB. If the file type which is being copied to the USB is allowed, then the encryption function takes place which is the next function and if the file type which is being copied is not allowed, then the file just gets deleted.

- **File type Identification** : The next module is used to identify the file type by checking the header bytes of the file. This file name is retrieved from the directory watcher which continuously monitors the newly inserted drive. Generally the file type can be understood by checking the file extension but this is sometimes deceiving because the saved file extension might not be the actual file type. Hence, we have decided to check the file type using the magic bytes in the header. The magic bytes are the unique to each file header. For example, the magic bytes of png file are 0x89, 0x50, 0x4E, 0x47. Hence we read the header and compare with the magic bytes and determine the file type.
- **Extension Comparison** : The next function is used to decide whether the file type should be allowed to be transferred or not. When the type of the file which is getting copied is identified, then the software tries to find that file type in the database of the allowed file types which was chosen by the admin. If the file type which the user is trying to copy matches with any one file type from the database only the user is allowed to copy the file onto the Drive or else the copying process will be aborted.
- **Encryption**: The next function is Encryption. If the file type is of the allowed type, then the encryption module comes into picture. In the encryption module the first 512 bytes of the file header are taken as input and encrypted using the key. The key will be installed in the software itself so that no one can find and tamper the key. Key will be scrambled and stored and hence the chances of finding the original data are reduced.

- **Encryption Algorithm**

1. Select a random integer n.
2. Read the first 512 bytes of the file to be encrypted.
3. Convert the Byte into ascii and add n to it. Thus, PlainText = (PlainText + n) mod 62
4. Key is an array of unsigned long char worth 8 bytes long different per machine on which the software is installed.
5. PlainText * key = CipherText (Where * is a bitwise operation where the similar bits get transformed into false state and dissimilar bits get transformed into true state.)
6. The result obtained from the above operations is the required encrypted file.
7. Append n at the end of the file.

- Decryption Algorithm

1. Read n from end of file.
2. Remove n from end of file.
3. Read the first 512 bytes of the file to be decrypted.
4. Convert the Byte into ascii .
5. Key is an array of unsigned long char worth 8 bytes long different per machine on which the software is installed. CipherText * key = PlainText (Where * is a bitwise operation where the similar bits get transformed into false state and dissimilar bits get transformed into true state.)
6. Subtract n from the ascii of PlainText PlainText = (PlainText - n) mod 62
7. The result obtained from above operations is the Plaintext i.e. the original contents of the file are obtained.

II. External Module

This module of the software involves Ransomware Detection and Prevention.

- **Dummy Folder Creation**: In this module the first function is used to create the dummy modules at the highest level of file hierarchy. Around 5 files will be created and placed on top of the other files for protection of the other files. Once any change has been detected the folders are removed and created again.
- **Directory Watcher**: The next function is the Directory Watcher. The Directory watcher is used for notifying the changes on those dummy folders. Any changes or alteration of the dummy file will be notified and that is how we will understand that it has been attacked by a malicious process.
- **Malicious Process Identification** : If the process which alters the dummy folders is found to be running from the APPDATA Roaming folder, then it is a malicious one. Then delete the malicious process once it is found.

IV. CONCLUSION

Even today, insider intruders pose more threat to a company than outsider intruders. Our system tries to resolve both kinds of threats - internal as well as external, where the internal threat focusses on data leakage prevention through the use of USB devices and the external threat focusses on ransomware. The external threat module builds an early detection system against ransomware and the internal module assists the corporate company to have its own data access policy and the data transferred through the USB will be in encrypted format preventing it from getting leaked outside the company.

FUTURE SCOPE

- Currently, in the internal threats module, the software focusses only on the data being transferred using USB device , but the scope can be extended to cover the data transformation using emails.
- At present, in the external threats module, the software detects and prevents the ransomware attacks once the malicious software is installed on the computer. In future, the software can be enhanced such that malicious programs are detected before they are downloaded onto the computer, thus preventing ransomware attacks from their very core.
- Blacklisting of apps is one of the technique which can be implemented to accomplish this, i.e. previously downloaded malicious programs which were capable of causing ransomware attacks will not be downloaded again.
- This software can also be extended to handle different types of ransomware attacks which can enter through web browsing also.The software can also be extended to handle other types of external threats.

ACKNOWLEDGMENT

The authors would like to thank Biz Secure Pvt. Ltd. as well as Prof. Laxmi Bhagwat and Prof V. Y.Kulkarni from the Computer Engineering Department of MIT, Pune for their invaluable guidance through out the implementation of this project.

REFERENCES

[1] Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, Engin Kirda. Cutting the Gordian Knot: A Look Underthe Hood of Ransomware Attacks. IEEE, 2015
[2] V. Chandola, A. Banerjee, and V. Kumar. Anomaly detection: A survey. ACMComput. Surv, 41(3), 2009.
[3] S. A. Hofmeyr, S. Forrest, and A. Somayaji. Intrusion detection using sequences of system calls. International Journal of Information and Computer Security, 6(3), 1998.
[4] C. Warrender, S. Forrest, and B. Pearlmutter. Detecting intrusions using system calls: alternative data models. In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 1999.
[5] A. Lanzi, D. Balzarotti, C. Kruegel, M. Christodorescu, and E. Kirda. Access Miner: Using system-centric models for malware protection. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2010.
[6] A. Tang, S. Sethumadhavan, and S. Stolfo. Unsupervised Anomaly-based Malware Detection using Hardware Features. In Proceedings of the International Symposium on Research in Attacks, Intrusion and Detection (RAID), 2014.
[7] S. Axelsson. The base-rate fallacy and its implications for the difficulty of intrusion detection. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), 1999.
[8] Nolen Scaife, Henry Carter, Patrick Traynor, Kevin R.B. Butler . CryptoLock (and Drop It):Stopping Ransomware Attacks on User Data. IEEE 36th International Conference on Distributed Computing Systems, 2016

[9] Barbara Hauer. Data and Information Leakage Prevention Withinthe Scope of Information Security. IEEE Access, 2015

[10] Jasmin Jivani, Samuel Johnson, Gayatri Pandi (Jain). A Review of USB Encryption Techniques & Algorithms for Data Confidentiality. International Journal of Advanced Research in Computer Science and Software Engineering, 2015