International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Survey on Privacy Preservation of Sensitive Data

Uma Ashok Huljanti[1], Dr. Srinivas Narasim Kini[2]

Savitribai Phule, Pune University, Pune, India

[1]ME Computer Student (Engineering), Dept. of Computer Engineering, JayawantraoSawant College of Engineering,Pune University, Pune, India, 414007

[2]Assistant Professor, Computer Engineering, Dept. of Computer Engineering, JayawantraoSawant College of Engineering, Pune University, Pune, India 414007

Abstract: ***As the Internet grows and network bandwidth continues to increase, administrators are faced with the task of keeping confidential information from leaving their networks. In various data-leak cases, data loss is caused mainly by human mistakes. Recently government organizations show that the numbers of data-leak instances have grown quickly. One of the important issues in the information security research is data leakage or data loss especially caused by insider threat as insider threats have potential to inflict severe damage to the organization's resources, financial assets and reputation. However privacy and secrecy consideration can prohibit the organizations from willing to share the data from each other and this is one of the major tasks in the information security.In literature various papers address the problem of data leakage caused by human mistakes in the field of information security. This paper reviews the different methods used for mitigating data leakage and misuse detection. As per literature, need to develop an effective model for detecting data leakage in the field of information security.***

Keywords: Data leakage, Data misuse, Insiders, Network Security, Privacy.

1. Introduction

Organization's data is very important and proves as a main constituent in embodying the core of the organization's power and this power should be preserved and maintained. On the other side, this data is required for daily working on different processes. Consumers within the organization such as employees or partners perform different procedures on this data and may be exposed to the important information while accessing the data. Due to this processing and action, it maylead to data leakage and misuse.

Detecting and preventing data leaks perform some steps such as data-leak detection [1], data In short, the risk to data security from insider's threat is becoming more and more critical because of the endless use of the computers and also communication systems. Various methods have been proposed for defending data from outer attacks but those mechanisms fail to protect data from authorized users who may misuse their privileges in carrying out malicious activities.

2. Literature Survey

In the recent years, several methods have been proposed to deal with the problem of data leakage and misuse in database systems, especially caused by the insider.

H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda, [2] author proposed new system called Panorama to detect malware. Proposed system is designed in such way that it can automatically analyze samples for malicious data access and processing behavior. As per the observation proposed system successfully detected all the malware samples and had very few false positives. The malware samples comprises of a wide range of different classes of malware, such as keyloggers, password sniffers, packet sniffers, stealth backdoors, rootkits and spyware. Benefits of Panorama, yields zero false negative and very few false positives. Fine-grained taint analysis suffers from significant performance degradation.

K. Borders, E. V. Weele, B. Lau, and A. Prakash [3], author introduced a new paradigm for protecting confidential files on a personal computer called Storages Capsules. Proposed approach is motivated by encrypted file containers which allow a compromised machine to securely analyze and revise sensitive files without being able to steal secret data. Protection is provided by proposed scheme by separating the user's primary operating system in a virtual machine. While it is accessing private data or files, the Capsule system turns off the primary OS's device output, and when it is finished reverts its state.

Main advantage of proposed system is that they work with current applications running on commodity operating systems. A. Nadkarni and W. Enck [4], author identify the data intermediary problem as a growing concern for modern operating systems and proposed new security framework called Aquifer used for preventing accidental information disclosure in modern operating systems. Application developers in Aquifer define privacy margins that defend the entire user interface workflow defining the user task.

If a process does exist or is not part of the current UI workflow, Aquifer terminates the process. At the last author provide proof-of-concept implementation of Aquifer and integrate it with Android operating system.

J. Jung, A. Sheth, B. Greenstein, D. Wetherall, G. Maganis, and T. Kohno [5], Privacy Oracle is used over a wide range of applications and information leaks. Author proposed two fold contributions, first for discovering information leaks new technique is proposed called Privacy Oracle system which applies the black-box differential fuzz testing technique and second contribution is case study of leaks of

personal information and search three different types of information leaks.

Author discovers similar leaks based on the differential testing technique in which change in the application inputs are mapped to change in the application outputs.

Y. Jang, S. P. Chung, B. D. Payne, and W. Lee [6], author proposed the new framework Gyrus which monitors the user interactions for common tasks such as sending email, instant messaging, online social networking, and online financial services. Contribution consist of two fold approach, first they capture the users interactions with an application and second they validate resulting system output can be mapped back to the users interactions.

Gyrus builds on policy what you see is what you send (WYSIWYS). Framework is implemented on virtualization environment and successfully stops malware from sending unintended content over the network. Advantages of proposed system are stops malware from sending unintended content over the network, challenging for future attack, very efficient and no delay to the users.

K. Xu, D. Yao, Q. Ma, and A. Crowell [7], in this paper author proposed new technique called DeWare that is Detection of Malware. This technique is used for detecting the onset of infection carried through susceptible applications. Proposed system is used to provide protection for a personal computer, as well as for diagnosing and evaluating untrusted websites for forensic purposes. DeWare can be easily deployed and used in Windows.

Table 1: Literature Survey

S. No	*Paper*	*Proposed*	*Advantages*	*Disadvantage*
1	Capturing system-wide information flow for malware detection and analysis [2].	Author proposed new system called Panorama to detect malware. Proposed system is designed in such way that it can automatically analyze samples for malicious data access and processing behavior	Advantage of proposed system that yields zero false negative and very few false positives	Fine-grained taint analysis suffers from a significant performance degradation that is a slowdown by a factor of 20.
2	Protecting confidential data on personal computers with storage capsules [3].	Author introduced a new paradigm for protecting confidential files on a personal computer called Storages Capsules.	Main advantage of proposed system is that they work with current applications running on commodity operating systems.	Slowdown during the remove phase is due primarily to disk performance limitations in virtual machines.
3	Preventing accidental data disclosure in modern operating systems [4].	Proposed new security framework called Aquifer used for preventing accidental information disclosure in modern operating systems.	In proposed approach Aquifer, application developers that protect the entire user interface workflow	If a process does exist or is not part of the current UI workflow, Aquifer terminates the process.
4.	Privacy oracle: A system for finding application leaks with black box differential testing [5].	Author proposed two fold contributions, first for discovering information leaks new technique is proposed called Privacy Oracle system which applies the black-box differential fuzz testing technique and second contribution is case study of leaks of personal information and search three different types of information leaks.	Privacy Oracle discovered many small and previously unrevealed information leaks.	Limitations of proposed method are Message reordering, Encrypted connections and Traffic randomization.
5.	Gyrus: A framework for user-intent monitoring of text-based networked applications [6]	Paper proposed the new framework Gyrus which monitors the user interactions for common tasks.	Advantages of proposed system are stops malware from sending unintended content over the network, challenging for future attack, very efficient and no delay to the users.	limitation of Gyrus is that it cannot protect an application where user-intended text is represented in a proprietary format or in some complicated encoding on the traffic.

3. Architectural View

The owner sends the data to the client system .while sending the data to client over the network traffic attacker may attack the sensitive data traveling over the network to avoid this type of leakage of sensitive data we are using the “Data Leak Detection system”(DLD).

The working of DLD as follows:

1) Data owner Preprocess and Compute the finger prints of sensitive data
2) After that it send the finger -prints or packet to the packet analyzer. the packet analyzer analyze the sensitive data and check for any leakage of sensitive data .and if any data loss or changes in original data occur then packet analyzer report to the organization about leakage of original sensitive data.
3) and if there is no leakage in sensitive data then the analyzer send the data packet to the packet sniffer which contents the data without any loss or leakage in it. After that it will send to the corresponding client system.

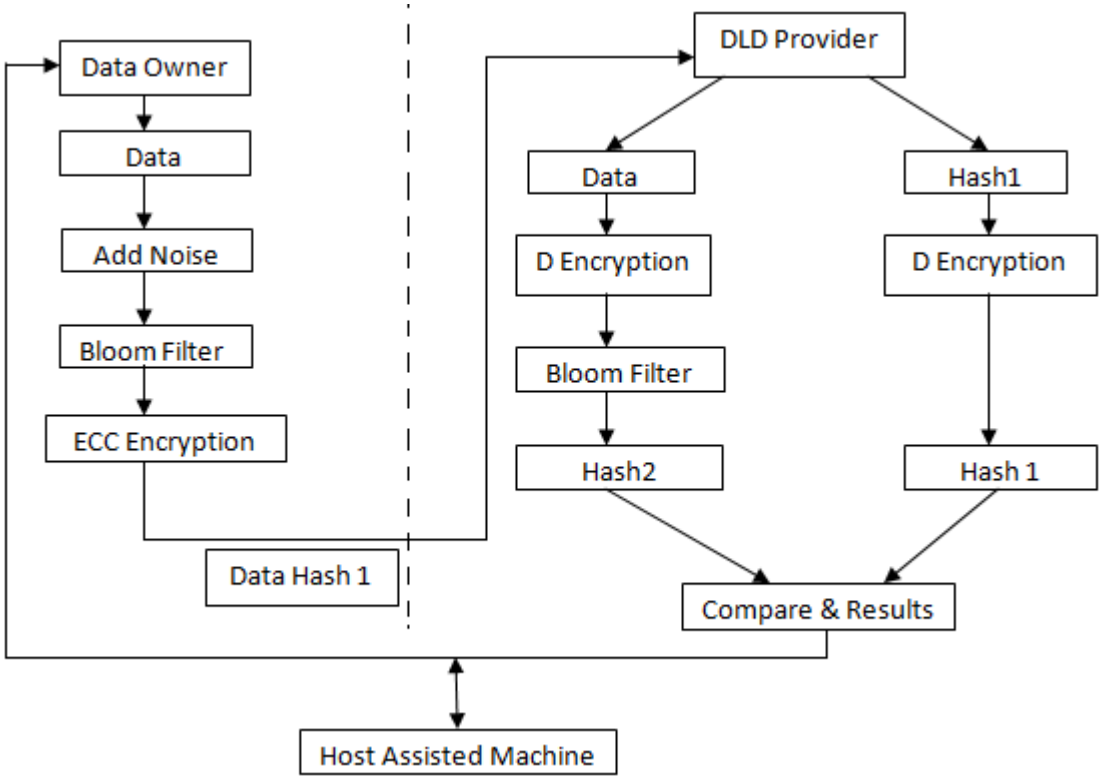

Figure 1: System architecture

4. Conclusion

This paper presented an all-inclusive survey on the data leakage and misuse in the field of information security. The main features, the advantages and disadvantages of each technique are described. Various papers address the problem of data leakage caused by human mistakes in the field of information security. This paper reviews the different mechanisms used for mitigating data leakage and misuse detection. But still none of the techniques gives the sensitivity level of the damage caused to data while providing the data to the insider. As per survey, there is strong need to focusondata leakage and misuse in the case of datasecurity. In Propose work, we develop robust technique for detection or avoidance of data leakage and misuse in the information security.

References

[1] XiaokuiShu, Danfeng Yao, Member, IEEE, and Elisa Bertino, Fellow, IEEE, "Privacy-Preserving Detection of Sensitive Data Exposure ", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 10, NO. 5, MAY 2015.

[2] H. Yin, D. Song, M. Egele, C. Kruegel, and E. Kirda, "Panorama:Capturing system-wide information flow for malware detection and analysis," in Proc. 14th ACM Conf. Comput. Commun.Secur., 2007, pp. 116–127.

[3] K. Borders, E. V. Weele, B. Lau, and A. Prakash, "Protecting confidential data on personal computers with storage capsules," in Proc. 18th USENIX Secur. Symp., 2009, pp. 367–382.

[4] A. Nadkarni and W. Enck, "Preventing accidental data disclosure in modern operating systems," in Proc. 20th ACM Conf. Comput.Commun.Secur., 2013, pp. 1029–1042.

[5] J. Jung, A. Sheth, B. Greenstein, D. Wetherall, G. Maganis, and T. Kohno, "Privacy oracle: A system for finding application leaks with black box differential testing," in Proc. 15th ACM Conf. Comput.Commun. Secur., 2008, pp. 279–288..

[6] Y. Jang, S. P. Chung, B. D. Payne, and W. Lee, "Gyrus: A framework for user-intent monitoring of text-based networked applications," in Proc. 23rd USENIX Secur. Symp., 2014, pp. 79–93..

[7] K. Xu, D. Yao, Q. Ma, and A. Crowell, "Detecting infection onset with behavior-based policies," in Proc. 5th Int. Conf. Netw. Syst. Secur., Sep. 2011, pp. 57–64..

[8] X. Shu and D. Yao, "Data leak detection as a service," in Proc. 8th Int. Conf. Secur. Privacy Commun.Netw., 2012, pp. 222–240.

[9] K. Borders and A. Prakash, "Quantifying information leaks in outbound web traffic," in Proc. 30th IEEE Symp. Secur. Privacy, May 2009, pp. 129–140.

[10] Identity Finder. Discover Sensitive Data Prevent Breaches DLP Data Loss Prevention. [Online]. Available: http://www.identityfinder.com/, accessed Oct. 2014.

Author Profile

Ms.Uma Ashok Huljanti,is currently pursuing M.E (Computer) from Department of Computer Engineering, JayawantraoSawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. She received her B.E (Infornation Technology) Degree from BIGCE Solapur. Solapur University Solapur, Maharashtra, India -413003. Her area of interest is cloud computing, network security.

Prof. Dr. Srinivas Narasim Kini, received his PhD Degree from Cochin University of Science and Technology, Thrikkakara, South Kalamasserry, Cochin**.** He received his M.E (Computer) Degree from B.M.S. College of Engineering, Basavanagudi, Bangalore, India. He received his B.E (Computer) Degree from K L E Society's College of Engineering Udyambaug Belgaum, India. He is currently working as Asst Prof (Computer) at Department of Computer Engineering, JayawantraoSawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007. His area of interest is network security,Data Mining etc.