Towards Securing Medical Documents from Insider Attacks

Maaz Bin Ahmad
Dept. of COCIS
PAF-KIET
Karachi, Pakistan

Abdul Wahab Khan
Dept. of COCIS
PAF-KIET
Karachi, Pakistan

Muhammad Fahad
Dept. of COCIS
PAF-KIET
Karachi, Pakistan

Muhammad Asif
Dept. of Electrical Engineering
CUST
Islamabad, Pakistan

***Abstract*—Medical organizations have sensitive health related documents. Unauthorized access attempts for these should not only be prevented but also detected in order to ensure correct treatment of the patients and to capture the malicious intent users. Such organizations normally rely on the principle of least privileges together with the deployment of some commercial available software to cope up this issue. But such methods can't be helpful in some of the misuse methods e.g. covert channels. As insiders may be the part of the team which developed such software, he may have deliberately inserted such channels in the source code of that software. The results may be catastrophic not only to that organization but for the patients too. This paper presents an application for securely exchange of documents in medical organizations of our country. The induction of water marking and hash protected documents enhances its security and make it fit to deploy in medical related organizations. The deployment is done in such a way that only higher management has access to the source code for reviewing. Results demonstrate its effectiveness in preventing and detecting majority of the information misuse channels.**

Keywords—covert channels; misuse; insider; medical; documents

I. Introduction

Insider [1-4] may be one of your employee, supplier, contractor, consultant or outsourced organization. The problem of insider threats detection/prevention is not a simple one to deal with, since it involves people following best practices and technology means to tackle it [5]. It looks simple to deploy principle of least privileges in medical related organizations. But this damages the organization a lot in terms of de-shaping the working environment of the organization. As there may exist a few insiders, it is not a good approach to monitor all the time other employees who are working hardly for the organization. This not only becomes a processing overhead but also creates dissatisfaction among your loyal employees. So this is not a feasible solution.

Medical related organizations also are sensitive towards insider threats. Blindly trust on user and on any commercial software may create difficulty for such organizations. Using some open source tool in this scenario may be a better choice but open source software has its own security issues. Also code revision itself is a very hectic job on someone else's code. So an application developed by trusted experts should be built for such organization which is to be reviewed only by higher expert management persons.

This paper presents an application to provide security to the viewing and exchange mechanisms of documents within the medical organizations. An application built in C# is being used to serve this purpose. Different scenarios are crafted and validated in a testing environment. Results show the usefulness of this application. In section II of the paper, the related work is presented. Section III provides the detail of the application. Section IV and V comprises of the implementation & conclusion respectively.

II. Related Work

Natarajan and hossain [6] utilized action based methodology and social network to detect the insider threats. In it the roles are assigned to the analysts. A social network is pre established for analyst and related system around him. The actions performed by analyst in each role are separately logged. Then these are compared with the expected behavior and results are collected. In this scheme there were few limitations like parameters need to be established prior and it performs slow convergence. Zhang [7] model is an active model for defense against insider threat. The model detects the insider threats in real time effectively. Artificial intelligence, graph theory and access control are used to create the model. Its plus point is that no human supervision is required. The model has several components which work differently from each other to handle the insider threats in different ways. Active defense approach manages all of these components. Information collection module comprises of sensors spread in the system. Information is gathered with the help of collection rules made by respondency module. Audit and application logs, application calling sequence, network data packets etc. are used to gather the information. Then with the help of these rules the necessary information is filtered. The information collection module then gives this information to detection module where orthodox detection tools are used in combination with detection rules. Due to their unique characters the low level insider threats are handled here properly. Then there comes sense module which analyzes abnormal events. The detection module sends those events which it thinks are suspicious but don't have unique characters to the sense module, where these events are further analyzed with the help of sense rules. So problem of false alarm is reduced here. Then there comes the respondency module which is the heart of active detection model. It may perform prediction of insider threats which would occur in the future. Intelligent techniques and insider threat previous history data helps in the prediction process. This module is also responsible for redeploying the rules for detection, sensing and information collection. This change of rules and prediction makes this model work actively against insider threat. Wang [8] security model was for sensitive nature organizations. The model was designed to stop the information theft due to insider. Encryption mechanism is the basis of this model. Trusted computing technologies work to achieve the goal. It has a core component named TPM (Trusted Platform Module) which gives the protected data like cryptographic keys and doesn't disclose the root key. Cryptographic functions like generating the random numbers, key generation of RSA (Rivest Shamir Adleman), integrity measurements etc. are also provided by TPM. Protection strength of TPM makes it impossible for someone to get wrapping keys from secured trusted platform. So the system is very secure. Wang and Puleo [9, 10] worked on the behavioral aspect of insiders. According to the research conducted, it was found that most of the insiders have one or more of the following observable behavior. These are: they have a wide range of skills, attack during their duty hours, don't share a common profile, have different motives, share their plan with co-workers, are caught by people manually and not by software or security staff etc. Profiling techniques help to detect attacks but it does work after an attack is completed. CERT (Computer Emergency Response Team) [11] discussed the organized crime approach of malicious insiders. The material for this research was collected from court documents, press releases of department of justice USA, reports of media and from interviews. They highlighted the issue of collaborative attacks where a group of insiders cooperate with each other in launching attacks. Such attacks can easily by-pass the existing security measures. So some recommendations were proposed in it to reduce chances of these kinds of attacks. E.g. detailed pre-employment screening, auditing of critical processes regularly, auditing of the database in which auditing information is stored and prefer external audits of process and system. So this methodology is policy based and emphasizes the need of having a strong security policy inside the organization. Eom et al [12] presented a document control system for military environment. This system consists of three sub-modules i.e. authentication access control and water marking. The first two modules are common to many models. The difference here is the watermarking technique. In water marking we add some information to the documents we want to protect. The document can be checked easily whether it is marked or not and accordingly its transmission is controlled. This model is very basic one and doesn't cover several illegal means related to document contents leakage e.g. copying contents of a marked document to another file, saving the water marked document on our system and later reproduce it etc. A research was conducted in order to see the insider activity in the banking and finance sector [13]. A detailed finding was described in this study. Research says that in most of the incidents observed, insiders required very little technical sophistications. Also it was observed that in most of these cases insiders planned their actions. Financial gain was the motive behind launching these attacks in most of the cases. Another interesting finding was that in all cases insiders didn't share a common profile. Several different methods and persons identified the attacks in all these cases. In these entire cases studied, victim organizations received heavy financial loss. So these were the findings obtained by studying insider threats cases in financial sector. This is a form of survey about attacks in this sector and doesn't give sufficient methodology to prevent or detect these attacks. CERT [14] studied the 123 cases of I.T sabotage and found that in all cases insider showed some suspicious behavior indicators prior to launching an attack. They developed a technical signature approach which can be applied only to a particular group of users inside the organization. In the beginning information like remote access time, protocol used in remote access is collected along with username/I.P and stored in a database. Having this information, they developed a signature. To monitor remote login these signatures are efficient but their limitation is that these cannot be applied to privileged users. Also these can only be applied to particular groups of users not to all population of users. Lizhong [15] developed a new framework in order to get and exchange only the essential information and discard the rest of information. The idea is based on the fact that normally special feature of a dataset is required rather than entire information. The proposed algorithm has the capability to process different kinds of data whether digital or continuous. Paal et al [16] targeted cross domain information exchange. As cross domain information exchange requires some kind of information flow between two domains, so it requires placing a guard between both domains which monitors and controls the flow between two domain. The main function of the guard is to provide confidentiality so they proposed a two way guard which also provides integrity.

Fisk et al [17] discussed some methods to send data between different organizations so that the overall risk of information stealing can be minimized by following these.

In short, none of these schemes targeted specifically to the medical related organizations. In medical organizations, the major requirements are to maintain up to date information about all patients, no tempering should be allowed with the prescriptions, treatment methodology should be kept confidential and fake reports and prescriptions shouldn't be generated. In order to cope up with these requirements we modified the document viewing application [19], added certain new features to it and at the end validated it with more scenarios according to the business processes of such organizations.

III. Methodology

The sensitive reports and documents are present on server in encrypted form and the other arrangements are same as mentioned in [19]. In addition to all the previous benefits of document viewing application, some more functionality is introduced in it. First of all, the confidential reports and prescriptions are hash protected. Whenever such a document is viewed, its hash value is computed and matched against the stored value at the server. If both values are same then the access is normal, otherwise the document is marked as suspicious.

As a second line of defense, all the stored medical documents are water marked. So in case of any possibility of illegal view, the user name is appended in the document who illegally viewed it. The induction of water marking also helps in the detection of forged prescription/report created by some unauthorized person.

So the proposed scheme gives the following benefits:

- User cannot copy confidential document to his/her USB
- User cannot forge any fake medical document without being noticed
- User cannot copy contents of confidential document to some other file and cannot make unauthorized changes
- Since it is our own created module, so code is available for techniques like code-analysis in order to detect covert channels
- Even if a user manages to copy some critical document from server, it cannot be decrypted on any other machine
- If any user tries to copy the contents of confidential document from his machine, he will be detected too(detection +protection)
- Supports a variety of file types like .doc/docx,.jpeg,.txt,.ppt/.pptx,.pdf and .xls/.xlsx
- Also provides Logs if any user tries to misuse the un-authorized information

As the medical documents belong to different applications e.g. MS WORD, EXCEL, POWERPOINT, TXT, PDF,JPG etc. and there may be multiple instances of the scenarios of same application. So we created different scenarios keeping in mind the business processes of medical organizations. The naming scheme is same as was discussed in [18]. These scenarios are presented for MS WORD as an example as follows:

CONF [1][1][1]:

User tries to access un-authorized Word document report of patient.

In this case, user tries to access an un-authorized MS WORD report of patient present on the server through his/her machine. If s/he manages to do so than it may result in leaking of patient secrets or may damage the security of a treatment process. Access right management and log management in the application help to prevent from it

CONF [1][1][2]:

User has read only access to a report and tries to copy its contents by selecting contents.

As the report can only be open in document viewing application, so user will not be able to do so because all such attempts are not only prevented by this application but also detected. Logs are also obtained as a result of these attempts.

CONF [1][1][3]:

User presses"prtsc" key to capture screenshot of contents of a confidential patient report.

The application has different built in checks, so it prevents the user from such kind of misuse. All of these activities are also properly logged in order to identify the intents of the users.

CONF [1][1][4]:

User tries to save read-only report to his/her machine or USB.

This scenario when simulated showed that user cannot do so because document viewing application would not allow to save confidential document to some external media.

CONF [1][1][5]:

User tries to take print of the patient confidential Report

This kind of action is also protected in the application which doesn't allow printing for such reports. So user would not be able to attack in this manner without being detected.

CONF [1][1][6]:

User tries to sniff the confidential medical documents

As the secret documents are decrypted at runtime, so if a user gets it by sniffing, he wouldn't be able to decrypt it because he doesn't know the decryption key.

CONF [1][1][7]:

User technically tries to change the code of the application or insert code with the application interface

Accessibility of source code of the application is not given to the users. Only highly privileged user have access to it. The source code is also hash protected so they also cannot make changes without being detected. Frequent code reviews also are helpful to detect such type of misuse.

CONF [1][1][8]:

User creates a forged medical prescription in order to adjust bills of misused medicines

Such kind of forgery cannot be done in the presence of this application as hash values of such documents needs to be matched from stored values on server. So such document would be detected as a fake one by this application.

CONF [1][1][9]:

User manages to open an unauthorized document and only reads it

Even only reading/opening such document doesn't go un-noticed by this application. The water marking technique introduced in the application captures the user detail that opens such a document. So it enhanced the security of the proposed application.

TABLE I. MISUSE SCENARIOS ALONGWITH DETECTION TIME & FALSE ALARMS

Scenario Application/Category	**Scenario #**	**Detection Result**	**Detection Time (sec)**	**False Alarms (%)**
MS WORD	[1][1][1]-[150][1][4]	Detected	< 1	0-2
	[1][1][5]-[150][1][5]	Prevented	-	0-1
	[1][1][6]-[150][1][6]	Prevented	-	0-1
	[1][1][7]-[150][1][9]	Detected	< 1	0-2
MS PowerPoint	[1][2][1]-[150][2][4]	Detected	< 1	0-2
	[1][2][5]-[150][2][5]	Prevented	-	0-1
	[1][2][6]-[150][2][6]	Prevented	-	0-1
	[1][2][7]-[150][2][9]	Detected	< 1	0-2
PDF	[1][3][1]-[150][3][4]	Detected	< 1	0-2
	[1][3][5]-[150][3][5]	Prevented	-	0-1
	[1][3][6]-[150][3][6]	Prevented	-	0-1
	[1][3][7]-[150][3][9]	Detected	< 1	0-2
MS Excel	[1][4][1]-[150][4][4]	Detected	< 1	0-2
	[1][4][5]-[150][4][5]	Prevented	-	0-1
	[1][4][6]-[150][4][6]	Prevented	-	0-1
	[1][4][7]-[150][4][9]	Detected	< 1	0-2
JPG	[1][5][1]-[150][5][4]	Detected	< 1	0-2
	[1][5][5]-[150][5][5]	Prevented	-	0-1
	[1][5][6]-[150][5][6]	Prevented	-	0-1
	[1][5][7]-[150][5][9]	Detected	< 1	0-2
TXT	[1][6][1]-[150][6][4]	Detected	< 1	0-2
	[1][6][5]-[150][6][5]	Prevented	-	0-1
	[1][6][6]-[150][6][6]	Prevented	-	0-1
	[1][6][7]-[150][6][9]	Detected	< 1	0-2

IV. CONCLUSION & FUTURE DIRECTIONS

Medical organizations have sensitive information and cannot rely solely on documents misuse protective tools due to covert channel presence. The proposed application modified specifically for medical organizations solved that problem while keeping false alarms as minimum as possible. The false alarms can further be minimized by placing a module for offline analysis to refine the detections of misuse. Different kinds of organizations may adopt this application by modifying it according to their business processes.

REFERENCES

[1] Blackwell C. "A Security Architecture to Protect against the Insider Threat from Damage, Fraud and Theft", CSIIRW April 13-15, Oak Ridge, Tennessee, USA 2009

[2] Bishop M, Gollmann D, Hunker J and Probst. C W. "Countering Insider Threats". Dagstuhl Seminar Proceedings 2008

[3] Phyo A H and Furnell S M. "A Detection-Oriented Classification of Insider IT Misuse". Computers & Security journal, Vol. 21, No 1. 2002

[4] "Research and Development Initiatives Focused on Preventing, Detecting, and Responding to Insider Misuse of Critical Defense Information Systems". Results of a Three-Day Workshop. Santa Monica CA, 2000

[5] Prasad R S. "Insider Threat to Organizations in the Digital Era and Combat Strategies". Proceedings of workshop icfcf09, 2009

[6] Natarajan, A., Hossain, L. "Towards A Social Network Approach For Monitoring Insider Threats To Information Security". In Not known (Eds.), Intelligence and Security Informatics : Second Symposium on Intelligence and Security Informatics, ISI 2004, Tucson, AZ, USA, Proceedings [Lecture Notes in Computer Science 3073, (pp.501-507). Nicholson Museum, University of Sydney. 2004

[7] Hongbin Zhang, Jianfeng Ma, Yinchuan Wang and Qingqi Pei. "An Active Defense Model and Framework of Insider Threats Detection and Sense". Fifth International Conference on Information Assurance and Security. 2009

[8] Wang, S.H and Li, X.Y. "A Security Model to Protect Sensitive Information Flows Based on Trusted Computing Technologies". Proceedings of the Seventh International Conference on Machine Learning and Cybernetics, Kunming, 12-15 July 2008

[9] Liu, D., Wang, X.F and Camp, L.J. "Mitigating Inadvertent Insider Threats with Incentives". School of Informatics, Indiana University 2007

[10] Anthony J. Puleo, Captain, USAF. Thesis. "Mitigating insider Threat Using Human Behavior Influence Models". June 2006

[11] "Spotlight On: Malicious Insiders and Organized Crime Activity". A technical report: CERT insider threat centre, Jan, 2012.

[12] Eom, J.H., Kim, N.U., Kim, S.H and Chung, T.M. "An Architecture of Document Control System for Blocking Information Leakage in Military Information System". International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012

[13] CERT. Insider Threat Study: "Illicit Cyber Activity in the Banking and Finance Sector". Aug., 2004

[14] Insider Threat Control: "Using a SIEM signature to detect potential precursors to IT Sabotage". CERT insider threat centre, April, 2011.

[15] Lizhong Zheng. "Lossy Information Exchange and Instantaneous Communication". MIT, Final report , 09/17/2015

[16] Paal E. Engelstad. "Security Challenges with Cross-Domain Information Exchange: Integrity and Guessing Attacks". IEEE 2015.

[17] Gina Fisk, Calvin Ardi, Neale Pickett, John Heidemann, Mike Fisk, Christos Papadopoulos." Privacy Principles for Sharing Cyber Security Data ".Department of Homeland Security Science and Technology Directorate, Cyber Security Division, via SPAWAR Systems Center Pacific under Contract No. N66001-13-C-3001, 2015.

[18] Maaz Bin Ahmad, Adeel Akram, Saeed-ur-Rehman and Hasan Islam. "Implementation of a Behavior Driven Methodology for Insider Threats Detection of Misuse of Information in Windows Environment". Information- An International Interdisciplinary journal. ISSN 1343-4500. Vol.16 No.11 Nov.2013

[19] Maaz Bin Ahmad, Muhammad Asif, SyedMashhad Mustuzhar Gilani, M. Hasan Islam, and Saeed-ur-Rehman. "A novel application to secure misuse of information in critical organizations for windows environment", Fifth International Conference on Computing Communications and Networking Technologies (ICCCNT), 2014