Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

Malware intrusion in Electronic Health Record

[1]Sowmya and [2]Dhina Suresh,
[1]Research Scholar, [2]Assistant Professor,
[1,2]Department of computer science, St. Joseph's College of Arts and Science for Women, Hosur, Tamilnadu, (India)

Abstract **-** The overall purpose of this research is to overcome the propagation of malware activities in several aspects. EHR - Electronic Health Records which is the real-time, patient – centred record system that make information available to the authorized users which includes doctors, patients and the other nursing and clinical for accessing or updating the information and maintain them frequently for patient care. Health record management is an important and challenging task. Utilization of technologies in health care, particularly the use of Electronic Health Records (EHR) offers a wide variety of benefits. Better healthcare is provided by EHR by improving all aspects of health care. Several authentications are involved in safeguarding the records for sensitive and actual data to the patients. In spite of many safeguarding technique, still there is malware function taking place in affecting the whole process. Global impact from WannaCry malware is one of the transitory issues where the maximum data are encrypted. This leads to abusing of SMB. The main aim is to overcome the malware activities by using backdoor implant tools. One of the tool called as a kill switch proved highly effective in stopping the threat. We propose a novel ABE-based framework for patient-centric secure sharing of EHRs in cloud computing environments, under the multi-owner settings. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are managed distributive by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. In the public domain, we use multi-authority ABE (MA-ABE) to improve the security and avoid key escrow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. We propose mechanisms for key distribution and encryption so that EHR owners can specify personalized fine-grained role-based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes.

Keywords - Attribute based encryption, Multi-authority, semi trusted servers

I. INTRODUCTION

Global impact from WannaCry malware is the focal point. Data from more than 250,000 computers in 150 countries are encrypted. This transitory issue is due to by installing and running of the eternal blue payload on each individual computer. The cause is abusing of SMB (server message block) vulnerability. Eternal blue propagates to vulnerable computers. Due to this propagation vulnerability exists in SMB. It leads to speculative programming error and programming weakness. The other non transitory issue is the Microsoft is unaware of this issue. SMB was developed as a feature, and features are developed in order to add value. However, there seems to have been a failure of imagination with respect to how this particular feature could be exploited. Feature architecture needs to include a rigorous, imaginative effort to identify and eliminate potential exploitable weaknesses. One of the backdoor is the "Double pulsar" even though the SMB is exploited by this backdoor; the vulnerability still exists in SMB.

Microsoft did not discover vulnerability until shadow brokers in presence. Had the vulnerability been discovered in QA testing, it could have been fixed prior to release. This is an admittedly generic solution - in order to be more specific, we would need more detailed information than Microsoft has released publicly. The NSA has an obligation to communicate with companies it exploits when it loses control of the weapons it produces. This obligation is primarily owed to the American people, and secondarily to any other innocent user that could become a victim. Microsoft is unaware of this issue until a shadow broker comes to discover it.

Eternal blue hackers threatens the user to access their own data and they are forced to pay some amount to get their data back. Some hackers release the backdoor "Double pulsar" along with the eternal blue. Some computers require authentication to install software. The main purpose of backdoor is to provide authentication. While hacking several files is leaked, "Double pulsar" is the part of leaked files. Because of this backdoor the non transitory issues are terminated because the other causal paths are more productive. The SMB exploit, currently being used by WannaCry, has been identified as Eternal Blue, a collection of hacking tools allegedly created by the NSA and then subsequently dumped by a hacking group calling itself "The Shadow Brokers" over a month ago. If NSA had privately disclosed the flaw used to attack hospitals when they found it, not when they lost it, this may not have happened.

A kill switch is a countermeasure concept of activating a single shut off mechanism for all Internet traffic. The concept behind having a kill switch is based on creating a single point of control (i.e. a switch) for a single authority to control or shut down the Internet in order to protect it or its users.

Security firm Malware bytes and Cisco's Talos security group reported that ransom ware infections appear to have slowed since the kill switch was activated [1]. The hacking tool, dubbed EternalBlue, can make it easy to hijack unpatched older Windows machines. Once Wana Decryptor has infected the first machine, it'll attempt to spread to other machines on the same local network. Then it will scan the internet for vulnerable machines.

Decryptor infects systems through a malicious program that first tries to connect to an unregistered web domain. The kill switch appears to work like this: If the malicious program can't connect to the domain, it'll proceed with the infection. If the connection succeeds, the program will stop the attack. Sinkhole – tactic researchers use to redirect traffic from the infected machines to a self-controlled system [2]. It is to prevent the use of a domain name.

Abbrevations and Acronyms

PHR, ABE,MA-ABE,AA

II. LITERATURE REVIEW

In recent years, personal health record (EHR) has emerged as a patient-centric model of health information exchange. A EHR service allows a patient to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many EHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing EHRs in cloud computing have been proposed.

While it is exciting to have convenient EHR services for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. On the one hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates. Cloud providers are usually not covered entities. On the other hand, due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviours which may lead to exposure of the PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without authorization. To ensure patient-centric privacy control over their own EHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers.

A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the EHR owner herself should decide how to encrypt her files and to allow which set of users to obtain access to each file. A EHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary[4].

III. PRECAUTIONARY MEASURES

In order to prevent the user's data from getting into unrecoverable state, users should have incremental online and offline backups of all the important data and images. In addition, all the in-built defence mechanisms and detection tools should be kept up and running all the time. Exposure to threats should be minimized, where possible, with common sense, site or IP address blocking and endpoint protection. Organizations and individuals should ensure that their electronic defence is as impenetrable as possible through the use of anti-virus, firewalls, IPS, web and mail filtering. Policies that prevent penetration should be enforced in organizations by ensuring correct system configuration and device 'hardening'. A robust and incremental back-up system of business and personal-critical details should be implemented.

Also, personnel must ensure that offline back-ups remain offline at all times so they are protected. Backups should be tested regularly to guarantee protection. Organizations should put robust policy and processes and a practical system of educating users on how to best prevent and deal with ransomware attacks in place. Ransomware attacks have become a global incidence, with the primary aim of making monetary gains through illicit means. The attack started through e-mails and has expanded through spamming and phishing. Ransomware encrypts targets' files and display notifications, requesting for payment before the data can be unlocked.

IV. PROBLEM DEFINITION

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, photographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to EHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for EHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's EHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytically and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

V. PROPOSED SYSTEM

In this paper, we endeavour to study the patient centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her EHR among a set of users by encrypting the file under a set of attributes.

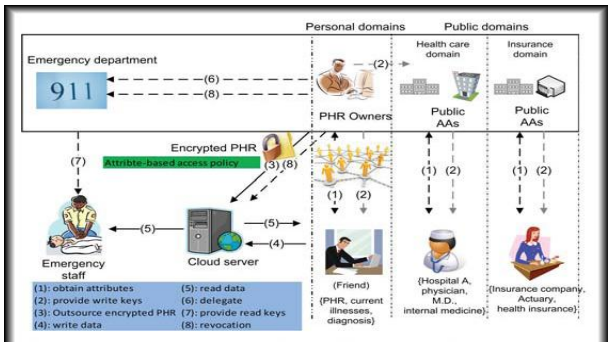

Figure1: The proposed framework for patient-centric, secure and scalable HER sharing on semi- trusted storage under multi-owner settings.

As illustrated in figure1 The proposed framework for patient-centric, secure and scalable HER sharing on semi-trusted storage under multi-owner settings, The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale EHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date. To this end, we make the following main contributions:

We propose a novel ABE-based framework for patient-centric secure sharing of EHRs in cloud computing environments, under the multi-owner settings. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are managed distributively by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain.

In the public domain, we use multi-authority ABE (MA-ABE) to improve the security and avoid key escrow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. We propose mechanisms for key distribution and encryption so that EHR owners can specify personalized fine-grained role-based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes.

CONCLUSION

This paper reviews about various malware attacks taking place in many organizations and industries which affects their growth and affects the sensitive data. As many solutions are developed to overcome these malware still there is an attack being extending in various ways.

Acknowledgement

I would like to express my sincere gratitude to my advisor Prof. Mrs. Dhina Suresh for the continuous support of my study and related research, for her patience, motivation, and immense knowledge. Her guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my study. My sincere thanks also goes to Rev. Sr. Sagaya Mary James, for their insightful comments and encouragement

References

[1] Michel khan, “PC World from IDG,” in 2017.
[2] Michel khan, “PC World from IDG,” in 2017.
[3] D. F. Sittig and H. Singh, "A socio-technical approach to preventing, Mitigating, and recovering from Ransomware attacks," Applied Clinical Informatics, vol. 7, pp. 624-632, 2016.
[4] M. Shukla, S. Mondal, and S. Lodha, "POSTER: Locally virtualized environment for mitigating ransomware threat," in 23rd ACM Conference on Computer and Communications Security, CCS 2016, 2016, pp. 1784-1786.