CURTAILING INSIDER ABUSES THROUGH RELIABLE FORENSIC EVIDENCE GENERATION IN ELECTRONIC HEALTH RECORD SYSTEMS

ISSN: 2141 – 3290
www.wojast.com

AWEH, O[1], EKONG, V. E[2*], CHIEMEKE, S.C[3]
[1]*Department of Computer Science,*
Igbinedion University, Okada, opaniaweh@gmail.com
[2]*Department of Computer Science, University of Uyo, Uyo, Nigeria.*
victoreekong@uniuyo.edu.ng
[3]*Department of Computer Science, University of Benin, Nigeria.*
schiemeke@yahoo.com

ABSTRACT

Insider security issues incidental to Electronic Health Records (EHR) systems was evaluated in this study. The motivations behind some of the malicious actions by these insiders were analyzed. The blurring of the divide between the outsider attacks and the insider abuses was highlighted to show that EHR systems present unique case scenario as a result of the requirements for remote third party contributions towards the accumulation of EHR systems information. The study then canvassed for a paradigm shift that eliminates this insider/outsider abuses in the design of EHR systems infrastructure with the objective of abstracting its overall security issues. This was done to enable infrastructure security architects to focus on reliable security designs that will check or minimize EHR threats. A novel architecture that focused on enforcing a device based authentication, generating reliable evidence to establish the culpability of offenders and the elimination of the divide between the insider and outsider users to reflect the study's paradigm shift was then designed.

INTRODUCTION

Contemporary advances and practices in healthcare delivery systems in general and patients' information management systems in particular, draws heavily from Information Technology (IT) as patient information are maintained and exchanged among users of these systems. While these emergent developments have substantially boosted healthcare delivery, they have given rise to fresh set of problems of patient health information exposure to attacks from both outsiders and insider users of such systems. These attacks or breaches come in the form of accessing information, disclosure or modification of patient's health data. As Li (2014) opined, medical data breaches are often motivated by one or a combination of identity theft and blackmail.

One major import of this trend is that, Doctor-Patient confidentiality concept, one of the hallmarks of medical practice, has come under serious compromise. This is because both authorized and unauthorized persons may now have access to patient health information. These class of problems are not new altogether, just that as medical records have become digital and mobile they have become severe source of concern to the generality of the public and hence the designers and the managers of these systems. For the designers and managers of these systems, finding appropriate responses to these problems entails evolving encompassing solutions that reasonably address the various areas of vulnerabilities. Some of the common areas of vulnerabilities incidental to patients' electronic records are discussed as follows:

(i) In a typical hospital environment, patient's information is generated at various units, before being conveyed to a central repository. It is important to note that some of these units may belong to distant third parties who provide specialized services and send in

their results online. Keeping a close tab on the procedures remains a challenge in the design of these systems.

(ii) At the patient's end, their associates have been noted to pose a source of threat. For example, there are systems with features for reaching some out patients or patients being managed from their homes using IT services. From this type of ends, some of the associates to the patient may have access to some basic information. Monitoring the possible sources of breaches at this end remains an onerous brief.

(iii) The possibility of external attacks against the hospital management system in general or the patients' health information in particular from external hackers is another area of vulnerability. When a medical data breach occurs, it simply means that patient information was, at some point in time, unsecured.

(iv) Malicious insiders are vulnerable to inducements from patient's adversaries or other motivations, some of them, financial or personal, to disclose confidential patient personal health information.

This study focuses on measures that can prevent or minimize the incident of insider abuses by prescribing a design paradigm that will increase the perceived risk of discovery for insiders who would employ brute force attack or otherwise abuse their access privileges. The proposed design paradigm will make it possible to generate and garner ample forensic evidence from the insider users of EHR systems.

American Health Information Management Association (AHIMA) (2009, 2011) and Health Insurance Portability and Accountability Act (HIPAA) (2013) articulated what Electronic Health Record (EHR) or Electronic Medical Records (EMR) systems are and what they are designed to do. In their perspective, EHR or EMR relates to the development of a comprehensive personal health information of patients with the capability for the patient and authorized users to access, retrieve, interact with and contribute to such a record.

Schultz (2012) observed that as more doctors and hospitals go digital with medical records, the size and frequency of data breaches have assumed alarming proportions. In another study, Li (2014) argues that the healthcare industry is becoming more mobile and efficient than ever before, due to the adoption of technologies such as EHR and electronic sharing, storing and accessing of medical data. This assertion was made against the backdrop of the risk of data breaches increase, and the possibility of running fowl of the requirements for compliance with guidelines, such as the HIPAA Privacy and Security Rules, which have become very difficult to meet.

INSIDER THREATS AND MOTIVATIONS

An understanding of insider threats and abuses and the motivations behind their actions is key in mitigating it. An insider attack occurs when employees of an organization with legitimate access to their organizations' information systems use these systems to sabotage their organizations IT infrastructure (Moore *et al*., 2008). The motivations for these attacks which every system conceived for EHR must take into consideration were itemized by Smith *et al*. (2010).

MATERIALS AND METHODS

This study was to provide a conceptual solution to the rising incidence of insider abuses against EHR environments. The starting point is to substantially comprehend motivations behind these abuses, study the subsisting rules and regulations designed to check or mitigate the abuses and then evaluated the subsisting forensic audit processes. Having accomplished this reasonably, we propose a workable conceptual solution that requires a paradigm shift in the security design of EHR infrastructure.

The study proposes a security design aimed at achieving the following objectives:

1. The strengthening of the subsisting authorization and other users' access control and monitoring strategies with a device based authentication mechanism. The philosophy

behind this proposition was the need to adopt an authentication device and process that could tightly bound certain actions initiated or accomplished within the EHR infrastructure environment to specific users.

2. Introduction of a honeypot as one of the backend applications. The philosophy behind this proposition was to lure prospective attackers (insiders or outsiders) off their targets and log their actions for forensic analysis.
3. Design a conventional detection systems defenses at the system level. We propose a design that concentrates its defenses at the user applications layer where most malicious activities normally occur. This way, it will run in parallel to the conventional systems.
4. Implement a design in which the system user's responsibilities and access control rights are integral parts of the systems security design. This is to make it more effective, unlike in most counter measures used for intrusion detection and prevention that work in isolation from the application access control rights and privileges and are oblivious of the user's responsibilities.
5. We strongly prescribe routine checks and constant forensic analysis of captured packets. The logic behind this prescription was premised on the fact that frequent comparison of analyzed packets will throw up irregular patterns that may necessitate elaborate investigations.

(i) **Subscriber Identity Module (SIM), International Mobile Subscriber Identity (IMSI):**
We propose the introduction of a device based authentication mechanism. The device of choice was a mobile phone SIM, IMSI. This choice was informed by the fact that IMSI is a unique authentication credential that is tightly bound to its holder. With this IMSI, access codes for accessing the EHR infrastructure at different terminals can be delivered independent of the EHR network infrastructure, thus adding another security layer to the conventional ones.

(ii) **Simple Message Service (SMS) Enabler (SMS Server):**
To send and receive access codes (tokens) in the proposed EHR infrastructure, a communication server and a mobile device authentication server to support messages exchanges between users mobile devices and EHR backend infrastructure are incorporated into the proposed system architecture. These servers make it possible to leverage SIM based IMSI as a device and also makes it possible to access Global System of Mobile Communication (GSM) networks infrastructure and its associated security schemes.

(iii) **Honeypot:**
Another integral component of the proposed conceptual solution is the honeypot. A honeypot, according to Gaonjur and.Bokhoree (2006) is a decoy computer system that uses deception to lure intruders so as to learn their behaviors. Any interaction with a honeypot is likely an unauthorized or anomalous activity (Spitzner, 2003).

DISCUSSION

The compelling reason for the proposed solution is to prevent problem behavior by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system. In the course of evolving a conceptual solution or strategy, the study introduced some devices or components and advocated for the observance of some procedures or processes. The significance of some of these introduced devices and processes with respect to their forensic evidence generation capabilities are discussed.

(i) **SIM Card IMSI**
Mobile phone SIM capabilities together with their pervasiveness and security have become a very reliable device in the development and design of trust-based applications. SIM IMSI will add an extra layer of security at the point that users attempt to authenticate, and in addition it will generate third party evidence that can be called for forensic analysis. The advocacy for the use of SIM IMSI in security systems design is very strong as can be gleaned from (Mantoro *et*

al. 2011; Kumar, 2012; Kale, *et al* 2013; Vilarinho, 2009). Mantoro *et al*. (2011) argued that SIM cards are convenient for storing security parameters essential for secure communication. They also noted that user's trust and security improvements can be achieved with a mobile phone's SIM card. Kumar (2012) proposed a solution that involved using a mobile device to authenticate a user prior to carrying out a financial transaction over the web. Kale et al. (2013) proposed a connectionless approach that included a two factor authentication scheme involving a mobile phone SIM. Vilarinho *et al.* (2009) observed that SIM cards have undergone enhancements both in the underlying hardware and their capabilities and have become a secure wireless network device

.

(ii) **Simple Message Service (SMS) Enabler (SMS Server)**

To send and receive access codes an SMS enabler must be incorporated into the system to enable secured communication with users over GSM networks. SMS enabler comes with different features, some help to track mobile devices International Mobile Subscriber Identity (IMSI) while some have the capability to also track International Mobile Equipment Identity (IMEI). They are normally used to forward and receive messages from large set of users and in the process; they maintain an elaborate information log of transactions initiated or attempted.

(iii) **Reliable Forensic Evidence Generation**

The essence of this strategy is to consciously generate and regularly extract vital information at the various identifiable user ends of the system for forensic analysis. First, the SIM cards to be used to strengthen authentication in this proposed strategy are the ones used by GSM network operators. This implies that GSM operator logs can be requested in the event of any breaches. Second, the introduced authentication server keeps an elaborate log of activities pertaining to users attempt at authentication using their SIM's. Third, there is the normal operating system log and database query transaction logs. Having all these reliable information logs guarantees the availability of ample information for forensic analysis. All these are in addition to the captured packets by the honeypot.

PARADIGM SHIFT IN EHR SYSTEMS DESIGN AND IMPLEMENTATION STRATEGIES

From the foregoing discussions a novel line of taught is apparent. This is derived from the fact that achieving the proposed objectives implies blurring, if not eliminating the distinction between external and internal users of EHR systems. This is the natural outcome of the incorporation of the components and devices and the implementation of procedures and processes suggested. The architecture of the proposed conceptual solution is illustrated in Figure 1.

The proposed architecture as depicted in Figure 1 has three identifiable segments comprising All Users/Devices, Cyberspace and EHR Backend Systems Organization. At the users/devices end, the architecture grouped all the users together. That is, there is no distinction between the insider users (malicious or not) and the outsider users (malicious or not). This position has strong philosophical underpinnings.

As indicated earlier, medical records details are accumulated from different sources, some of which are remote third party sources. For example, X-ray, Scans, Laboratory Tests, Pharmacy Units, etc. are vulnerable sources of the system. The reason being that from requested tests, prescriptions, scans and so on; experienced practitioners can accurately predict any patients' ailment. This category of users of the EHR can neither be classified as insider or outsider users of the system. Maybe we can classify them as semi insiders. This group of users apparently has some privileges in the EHR infrastructure environment.

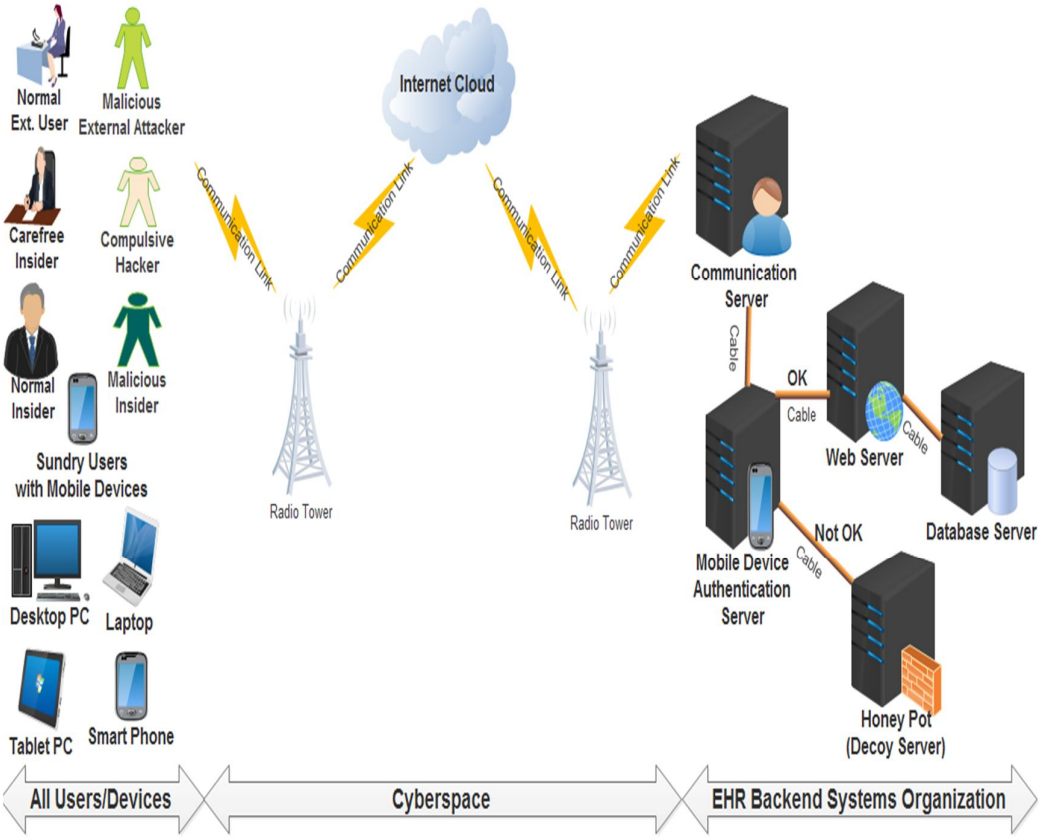

Figure 1: Proposed EHR System Architecture.

Another important point is that most insider and semi insider users of electronic information systems (including EHR users) may be relatively careless with their credentials, while some are amenable to inducements that may make them engage in malicious activities. Some others have their own motivations or may just be naturally malicious. Meanwhile, most security designs tend to focus solely or more on the external attackers, who apparently pose lesser risks to EHR systems. Therefore, canvassing for the design and implementation of EHR security system's design based on fresh perspective or fresh paradigm that eliminates the distinction between insider or outsider users of the system is not out of place considering EHR's unique nature. Eliminating this distinction is like abstracting the concept of EHR security issues or separating it as an independent concern that will encourage security architects to focus on developing reliable solution. It is imperative to note also, that with the advent of information management schemes that leverages remote data storage technologies such as cloud computing or data centers, the emphasis must be on overall security of EHR information, as all users are apparently "outsiders".

CONCLUSION

Security considerations are boosted by deterrents. Therefore awareness of the ease of being detected based on these array of forensic sources can substantially minimize the incidence of abuses. Although the proposed solution or strategy introduces some extra cost and time delays, this extra cost and delays do not compare to the cost of serious breaches that cannot be associated with any particular offender. The cost is also not comparable to that of loss of integrity and hence loss of faith by the populace in EHR systems. Adoption of this design paradigm in EHR system infrastructures will substantially curtail the rising incidence of insider

attacks and abuses in the healthcare sector. The design paradigm will also be effective in other sectors where insider threats are prevalent.

REFERENCES

American Health Information Management Association (AHIMA) (2009). Sanction Guidelines for Privacy and Security Breaches, *Journal of AHIMA*, (80) 5, pp 57–62. Available online at: http://www.ahima.org. (Accessed 21-02-2015)

American Health Information Management Association (AHIMA) (2011). Security Audits of Electronic Health Information, *Journal of AHIMA*, (82) 3, pp 46-50. Available online at: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_048702.hcsp?dDocName=bok1_048702 (accessed 19-02-2015)

Gaonjur, P. and Bokhoree, C. (2006). Risk of Insider Threats in Information Technology Out Sourcing: Can Deceptive Techniques be applied?, *Journal of Security and Management*, pp. 522 – 529.

Health Insurance Portability and Accountability Act (HIPAA) (2013). What federal rules do I need to follow to keep my patient records private and secure? Available online at: http://www.healthit.gov/providers-professionals/faqs/what-federal-rules-do-i-need-follow-keep-my-patient-records-private-and-secure (accessed 16-02-15)

Kale, R., Gore, N., Jadhav, K.N. and Shinde, S. (2013). Review paper on two factor authentication using mobile phone (Android), *Journal of Computer Engineering and Informatics*, (11), 3, pp.99–102.

Kumar, B. (2012). Secure web financial transaction methods and smart authentication with a focus on mobile devices, *Computer Science and Engineering*, (2), 6, pp.92–97.

Li, Y. (2014). How You Should – and Should Not – Be Sharing Medical Information with Patients. A Review of HIPAA Security Practices to Keep In Mind When Sharing Patient Data. Available online at: http://www.itnonline.com/article/how-you-should-%E2%80%93-and-should-not-%E2%80%93-be-sharing-medical-information-patients (accessed 15-02-15)

Mantoro, T., Milisic, A. and Ayu, M.A. (2011). Online authentication using smart card technology in mobile phone infrastructure', *International Journal of Mobile Computing And Multimedia Communications (IJMCMC)*, (3), 4, pp.67–83.

Moore, A. P. Cappelli, D. M. and Trzeciak, R. F. (2008). The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures, CERT. Program, Carnegie Mellon Software Engineering Institute.

Schultz, D. (2012). As Patients' Records Go Digital, Theft and Hacking Problems Grow. Available online at: http://kaiserhealthnews.org/news/electronic-health-records-theft-hacking/ accessed (15-02-15)

Smith, B. Austin, A. Brown, M. King, J. Lankford, J. Meneely, A and Williams, L (2010). EHR System Attacker Motivation, Challenges for Protecting the Privacy of Health Information: Required Certification Can Leave Common Vulnerabilities Undetected, SPIMACS, Chicago, Illinois, USA.

Spitzner, L. (2003). Honeypots: Catching the Insider Threat, *Conference proceedings of Computer Security Application*, pp. 170-179.

Trzeciak, R. (2012). Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks. Available online at: http://www.cert.org/insider_threat/ (Accessed 22/02/2015)

Vilarinho, T., Haslum, K. and Noll, J. (2009). Advanced SIM capabilities supporting trust-based applications, *14th Nordic Conference on Secure IT Systems, NordSec*, (5838), pp.223–238.