

Meeting the EHR Privacy Challenge

Delivers Confidentiality and Gets Compliance for Free

Poy Chen
FrontOne Limited
poy.chen@frontone.com

Abstract:

Electronic Health Record (EHR) refers to an individual patient's medical record in digital format. With the promise to improve the quality of health care services, promote a more integrated approach to care and offer consumers an opportunity to better manage their own healthcare. EHR systems are interconnecting public and private health providers and providing remote access to patient records remotely and through the internet. However, citizens are concerned about the privacy of personal and medical information, if the recent data breaches within financial institutions, the retail industry, and from government databases are indicators, strengthening the security of EHR system in compliance with privacy requirement is a technologically challenging undertaking.

This paper presents a fresh approach in the way to securing the data, protecting digital identity, delivering data confidentiality; with an aim to provide readers a different perspective, on how EHR system's privacy objective can be met, and steps may be required to safeguarding EHR confidentiality.

© FrontOne Limited. 2007-2009. Important Notice: This document is for private viewing only. It is not intended for reproduction or public distribution. For permission to publish or electronic distribution of this article, please contact FrontOne Limited, PO BOX 17385 Green Lane, 117-125 St Georges Bay Road, Parnell Auckland New Zealand. email: info@FrontOne.com

Introduction:

Governments around the world are embarking on healthcare reforms in the efforts to provide better service to its citizen and containing blooming healthcare cost. EHR system can help to increase efficiency and reduce overall healthcare costs; as a result, a global trend of building national EHR system.

Security, integrity and privacy of personal medical data is of utmost importance, and whilst many research projects worldwide are investigating the application of new technologies to pervasive healthcare solutions, security and reliability of these technologies is an area that requires further exploration¹.

EHR System and Security Requirements

Encryption is a term often associated with IT security. Data that require protection is usually encrypted. Encryption makes plain text unreadable to anyone except those possessing special knowledge, usually referred to as a **key**. Therefore, the security of the Key is part of the overall EHR system security.

With the goal of *offer front-line healthcare staff with direct access to accurate and complete patient information, leading to better treatment decisions, improved patient safety and ultimately increased efficiency and effectiveness of a nation's health system²*, EHR system must provide secure access to EHRs medical practitioners and delivers to where it is needed efficiently. According to Digital Preservation Europe, the main characteristics that a Healthcare network security system should provide are:

- a. User authentication to verify requests for access to data
- b. User authorisation to permit access to data
- c. Ensuring confidentiality of data transmitted over the communications network.
- d. Integrity of data

There are many of solutions currently in the market that can provide one or more of the above requirements with a wide range of strength and capabilities. Most of these solutions are based on traditional security models and many have proven to be insufficient in meeting the security and privacy need of modern computing era. If we are to avoid the mistakes of the past, the experience of recent data breaches from within as well as other industries, a new approach is required.

¹ http://www.digitalpreservationeurope.eu/publications/briefs/security_aspects.pdf

² Realizing the Goal of EHR in the United States – Sierra Systems.pdf (<http://www.sierrasystems.com>)

Security Vulnerabilities and Challenges

The modern attacks are focused on circumventing security measures provided as part of the EHR (or Information) system by impersonating the authorised users (identity theft) or leveraging the legitimate user credential (man-in-the-middle attacks). As a result, the most basic part of the EHR delivery system is also the most vulnerable - identifying the authorised users and delivering contents.

EHR system security is like a train, which consists many parts; “a chain is only as strong as its weakest link”. The weakest link in current EHR system security is the Digital Identity that is used to facilitate remote access to the system.

There is fundamental difference in Digital Identity and User Authentication, Digital Identity is defining what (the user is) and User Authentication is a process to determining how (to identify user with what).

The Security Challenge

EHR system exists for the purpose to provide **authorise user access to confidential EHRs**. Unless it sets a strong foundation by choosing a Digital Identity that is strong and has high integrity, all other security measures will be compromised. In other words, you won't want to build a safe without an equally strong lock.

Digital Identities Cross Road

Authentication is the process that verifies the identity of people that access personal medical data contained in the EHR. Traditionally, the process is initiated on the input of the system user's identity and is completed when the identity is recognized. The identity which the system has been relied on such as username and password is now been recognised as unacceptable due to its high vulnerability to identity-based attacks. However, there is no suitable alternative that meet meets the need of high integrity and is scalable at low cost.

In addition, the traditional authentication process known as “Log in” or “sign on”, granting user access to all privileged resources, once the user is authenticated. In essence, this gave the attacker the reward to exploit system vulnerabilities, committing identity theft (social engineering, Malwares data breaches) and session hijacking attacks.

Client Side Attacks

The strong authentication strategy driven by the government legislation to safeguard consumer interest saw the introduction of two-factor authentication solutions. These measures have increased the barrier of attacks which has made some measurable difference in reducing e-fraud, in particular when the

requirement of one-time-password is enforced. As a result, attacks become more targeted and are shifting their focus to attacking the **transaction data** instead. These sophisticated attacks are categorised as Man-In-The-Middle and Man-In-The-Browser.

The Man-In-The-Middle (MITM) Attack

In terms of IT security, MITM attack often acts as "transparent proxy" or "intercepting proxy", which captures all data (also known as cache) on route to the user. For HTTP traffic, it is very simple to do, for secure data such HTTPS, the intercepting proxy have the capability of re-encrypt data on-the-fly.

The Man-In-The-Browser (MITB) Attack

MITB is a MITM attack in browsers. It is a Trojan that infects a web browser and has the ability to modify pages, modify transaction content or inject additional transactions, all in a completely covert fashion invisible to both the user and host application.

Architecture Weakness

The existing network and internet security are provided on each system layer. Layered Security approach continuously increases the complexity of a system; because there is no coordination between each security layer and it is impossible for any layer to defend attacks that exploit the weakest link - between layers or vulnerabilities in selected layers. An example of this is Silentbanker,³ a MITB attack that bypasses all security measures successfully, and conducts fraudulent transactions by leveraging the legitimate user's authentication and modifying transaction data on-the-fly. Another example is in the form of deep packet inspection application, used in Intruder Detection System (IDS), where all data are decrypted, unpacked and inspected. Even though IDS is built for defence, unfortunately, attacks also in possession of such technology.

The enemy of information security is complexity. Why do information security problems persist? According to Bruce Schneier, an internationally renowned security technologist and author - it is due to the continuous demands and supply of new functionalities; the information security has improved at a slower pace than the increase of system complexity.

Observations

Based on the definition of 'information security', the job is not done until the user gets the data confidentially. For that reason, security must start at the user and ends with the data confidentially. There are many reasons why we can't start

³ https://forums.symantec.com/symant/blog/article?blog.id=malicious_code&message.id=185&jump=true#M185

afresh to build a new system from ground up to address many of these problems, but if we can identify what the core issue is, better processes can put in place to work within the existing infrastructures, to achieve both goals: security and privacy. In our opinion, common deficiencies in current systems are:

Dependency on static user identities: Static identity is difficult to protect, especially in remote applications such as web applications; this dependency is a core reason on exponential increase in data breaches and identity theft activity.

Undefined end point: The true end point of information system is the user not the client application. The layered solutions designed to work within the applicable layer. For example, SSL is used to encrypt data between two ports and it will pass to the next layer decrypted, because it has completed its task. It has no awareness where the real destination is. Anyone with suitable capability along the route (such as transparent proxy attack) can pronounce itself as the destination to intercepts the information. This inability to communicate between security layers is a major reason why security vulnerabilities persist.

Security of the security key (certificate): While encryption can enhance security of data, selecting a suitable encryption system is not a simple task. It first has to be capable of securing both the data on rest and on the move. Secondly, security vulnerability also exists in the **distribution of security key**.

New Security Focus

To be effective, a security solution must be simple and can be managed from a secure source.

Dynamic Identity: Unlike a static identity which can be easily tracked and stolen; dynamic identity changes every time it is used. Dynamic Identity renders social engineering attacks irrelevant as static user data become worthless to underground economy.

Continuous mutual authentication: Continuous Mutual Authentication technology re-authenticates user periodically or with every request, defeating identity based attacks and mitigating insider and network based threats.

User Centric security: User Centric security delivers data confidentiality by encrypting user data with user specific security key. This process ensures secure, application-to-user delivery of EHR data that is complementary to TLS/SSL security and overcomes the transport layer security vulnerability.

JANUS Solution

JANUS is an innovative Information Security framework that provides strong authentication (ID sentry), client side UI protection and transaction integrity verification (Data Sentry).

JANUS is built with patented technologies. The core technology is “Message Dissemination”, which allows JANUS the ability to create and to use dynamic and unpredictable messaging system to communicate discretely, and reduce the system’s surface that is potentially exposed to hostile environments.

The complementary “Human Factor Authentication” (HFA) technology provides the factor needed to enable more individualised measures to strengthen the last end of security and user input integrity. It empowers the user to authenticate the server and be in control of how he/she is identified to JANUS through a dynamic, continuous and mutual authentication processes.

The concept of Dynamic Identity and Continuous Mutual Authentication is also achieved with the availability of 3AKey. 3AKey is a dedicated security device that facilitates security related activity as well as transaction signing behind the scenes on behalf of the user.

Data Sentry provides support for end-to-end transaction security (from start until the transaction is completed). Data Sentry consists of a communication agent that is randomly selected in every transaction and is dynamically configured to carry out client side and/or server side functions to verify the data integrity of transaction being performed by the user.

Defeating Identity Theft

In this threat model, the user identity is acquired from insiders, data breaches or social engineering attacks. For enterprises, some of attacks could be from formal employees or contractors that have knowledge of the system. At present, most if not all identities used in computer systems are static. Once the identity is compromised, the attacker impersonate the authorise user and the system won’t know the difference. It takes an average of 18 months or more to discover an identity theft if financial related e-fraud is involved; there will be much longer if identity theft is used in data theft.

At present time, identity based attacks are financially focused. However, it could be used in economic espionage by launch user Denial of Service attacks. There is nothing any of traditional security measures such as Firewall and IDS can do because the system accepting authentication request involuntary, and is making binding decision based on the data provided.

To defeat identity based attacks, the most efficient way is to change the way authentication is conducted. JANUS ID Sentry is designed to accomplish this task.

3AKey is the world first distributed local authentication technology embedded as a HID security token. With 3AKey, the authentication is conducted in reverse order as authentication will be initiated from the server. Once the application determined that the user is requesting privileged contents; the application will engage JANUS to facilitate mutual authentication with 3AKey before the requested information is delivered. The process is completed seamlessly in the background:

1. JANUS makes an authentication query to the 3AKey;
2. 3AKey generates a Dynamic ID based on the previous transaction ID and the new and unique session ID;
3. JANUS derives the identity of the target 3AKey and creates a Server's self-authentication Token with a request for identity verification back to the 3AKey;
4. 3AKey responds with the One-Time identity (token) to verify itself if the Server Access Token is indeed valid, or a random number if the Server's self-authentication Token is invalid;

3AKey provides the means to carryout multi-factor mutual authentication in a single device in one operation (in this order):

1. the application verifies the computer terminal
2. the application verifies the user's computer profile at the local host
3. JANUS identifies 3AKey
4. the 3AKey validates JANUS;
5. the identity of the 3AKey is verified by JANUS;
6. Application is notified the status of user authentication;

If the requested content warrants a higher security measure, the application would require the user to complete a Localised User Authentication (LUA) before continuing the transaction.

Whenever the 3AKey is removed from the host, the connection to the application server will be terminated automatically.

The above processes achieved the following goals:

- ❖ User privacy fully protected,
- ❖ Identity theft prevented,
- ❖ Identity based attack prevented,
- ❖ Data access exclusivity can be guaranteed.

Defeating MITM, MITB and emerging Client side Attacks

In this threat model, the attacker resides along the path of the user and application server. This can be achieved with a specialised toolkit such as “attacking proxies” or as a Trojan resides inside the browser in a form of browser extension/BHO/Plug-in/Add-On. Both above attacks have the capabilities to bypasses all web application security measures including TLS/SSL and two-factor authentication. The attacker captures the user’s identity or modifies data on-the-fly.

JANUS deploys Data Sentry toolkit to defeat client side attacks.

JANUS Data Sentry: Data sentry is a selection of security module or agents with various function and capabilities. When the application has identified data that require protection, special controls are created dynamically and purposely configured JANUS agents are embedded with the contents. After the user defined the transaction and before sending the data to the application server for process, the JANUS agent creates a keyed-HMAC from the protected data and sends it to JANUS directly. Before the application commits to the transaction, it creates and sends a Keyed-HMAC to JANUS from the data received from the user. A transaction proceeds only if JANUS confirms that it have received a matching pair of Keyed-HMAC.

Should attacker acts to interrupt the direct message transmission to JANUS, or tampering the transaction, it will be invaliding the transaction.

JANUS UI Sentry: There is potential risk of attacks that has higher level of machine intelligence which is capable of emulating some user behaviours.

Safeguard Data Confidentiality

Today, majority of applications rely on a third party application to provide protection to those data in transit, and TLS/SSL is a popular choice but it has its limitation, and has been reported to be vulnerable to MITM and MITB attacks.

Another choice is to encrypt the all data and deliver as an encrypted file but this has limited usability as it is not scale well as it need special purpose-built application and the distribution of security key is anther security challenge. More importantly, this type of encryption solution is not integrated with Strong Authentication solutions. When data is protected by security key or certificate, the user is required to provide the password to decrypt the file or message, it exposes the weakness and vulnerability of the entire system (Feds use keylogger to thwart

PGP, Hushmail⁴) - an unacceptable security risk. However, web applications do not fit in this security model as data must be made available 99.999% of the time and accessed by general purpose software such as web browsers.

JANUS provides two confidential Data Services:

- ❖ Data Confidential with 3AKey;
- ❖ Data Confidential with Safekey;

When application is used with 3AKey, the client side application retrieves encryption key from the 3AKey whereas Safekey will be completing the encryption and decryption within, reducing the demand on client side application and strengthen security. The confidentiality is assured as data is delivered encrypted with security key specific to the authenticated device and session.

Unlike other solutions that require complex security management system, 3AKey and JANUS shares a cryptography secret and it is self-managed. Dynamic encryption key is created for the unique session and unique 3AKey, thus providing higher security at a lower cost.

User Cases

According the June 2009 publication of healthcareitnew.eu, a research that is done in UK recently found that almost two-thirds (65 percent) of the patients said they were happy for their records to be stored this way, and thought the computer technology was acceptable. However, they did express concerns about security, confidentiality and the potential exploitation of their records.⁵

How do the above mentioned JANUS and 3Akey address the security and privacy concerns and bridge the gap in the trust and confidence in the EHR systems?

3AKey itself does not have security or privacy risk as it contains no personal or medical information. The patient's personal information and EHR are centrally located with strict access control, based on the privacy guide line of the system and with explicit authorisation of the patient. Some of these consents are obtained while visiting Doctor or Hospital and other could be acquired online. If a web portal is made available to patients, the facility should be available to allow patients to manage their own privacy information and to provide or withdraw some of their consents. This type of interaction would help to build trust and confidence in EHR system. With this background, 3AKey is most suitable Digital Identity platform for

⁴ http://news.cnet.com/8301-10784_3-9741357-7.html

⁵ <http://healthcareitnews.eu/content/view/1484/42/>

the modern EHR system. The following sample applications illustrate its merits and benefits:

EHR Web Portal

Web has been adopted as medium of choice for commerce in the last 15 years due to its reaches and low cost delivery platform. Accessing the one patient one record EHR system through the internet makes technological and economic senses especially sufficient security and privacy is assured. FrontOne JANUS and FrontOne 3AKey can deliver significant benefits over other solutions that are currently available in both areas:

- ❖ Integrity: EHR system and 3AKey would mutually authenticate each other when a user request is made, therefore impossible for duplicate login. This access exclusivity ensures the integrity of EHR system is maintained in high standard. It protects every user in every step and ensuring the confidential data is delivered to those needed to know and have authorised. (In contrast, other authentication solutions would permit multiple concurrent sessions and multiple locations or because the systems were unable to maintain high access integrity)
- ❖ Confidentiality: 3AKey has the capability to provide user centric data protections by encrypting data with dynamic encryption key for each and every session. User delivers and receives confidential data with unique and dedicated 3Akey.
- ❖ Simplicity: Every user including patients can use 3AKey without the need of training, it is simply plug in to work and pull out to leave the EHR system. The EHR system can implemented to take a snap shot on the work in progress and restore the session automatically on return.

With these capabilities, the web portal will be highly secure with no compromise on privacy. All functionalities within the EHR system can be delivered in this popular and low cost platform.

Electronic Prescription Management (EPM)

EPM system consists of a central prescription repository; it helps the administration of prescriptions and drugs while increases efficiency, reduces potential adversary in drug misuse and saving medicine costs.

While sending a prescription via email directly to pharmacy for dispensing improves efficiency, this type of service lacks integrity and is of concern for its security and confidentiality claim. Email is known to be insecure thus poses significant risk to privacy, placing the security responsibility (verifying the authenticity of the prescription email and the authenticity of the person collecting the prescribed medicine) to the shop keeper/Drug dispenser.

An EPM system built with JANUS and 3AKey technology will be able to address both security and privacy concerns. The prescriptions will be stored in a centrally located and secure database and access is only provided to those authorised medical professionals.

If the feature is made available, the EPM system would be able to issue patients with 3AKey to access his/her private online medical portal automatically and in confidence. From the portal, the patient will be able to see what the current treatment plan is and have access to relevant information on medicine and advice that could assist the recovery. For those patients that meet the basic knowledge criteria would be able to make new prescription request, or order the delivery of medicines already in the treatment plan. This will speed up its management and will save bureaucratic tasks to the healthcare providers and reducing unnecessary travel for the patient.

Electronic prescription database will be a valuable tool in assisting doctors to provide better diagnostic and derive better treatment plans. When a doctor receives a prescription request from patient, the information from the pharmacy would also be available. The completeness of both the treatment record and medicine dispensing history can help doctor to escalate treatment, stay in course or request the patient to visit a medical facility.

When the patient goes to the pharmacy they present his/her 3AKey to the computer terminal that is connected to the EHR system. The chemist retrieves the electronic prescriptions from the database and dispenses the medicine to the patient with confidence.

Accessing and Delivery of Diagnostics Result

Diagnostics help to derive correct treatment and accessing a diagnostic result quickly to save lives. However, if the information is not identified correctly or when it falls into the wrong hands, there are adverse consequences.

EHR system will helps to manage the information accuracy and provide accessibility. With the authorisation policy and patient's consent in place, the diagnostic result which is in electronic form can be delivered to the Doctor immediately. 3AKey will help to maintain its security and confidentiality:

1. Place the diagnostic result to a central repository with the authorisation of the practitioner's 3AKey to ensure its authenticity;
2. EHR system notifies the availability of the Diagnostic result by email or SMS; or encrypt the EHR message and push it to the Doctor's computer terminal if it is already online (go to 5);

3. The Doctor insert his/her 3AKey and access the information;
4. The EHR system validate the 3AKey automatically and encrypt the EHR message with a dynamic key specific to the receive 3AKey;
5. The Doctor acknowledge the receipt of the message, thus enable the software at the terminal retrieves decryption key from the server and 3AKey to decrypt the message.

In summary, all above described systems and services meet the highest security and privacy requirement in any country to date. With this strong foundation, the EHR system will be able to grow and deliver other financial and medical services for the benefit of the wide community.

Conclusion

All patients as well as system users have a right to privacy and may thus reasonably expect that confidentiality and protection of their personal information will be rigorously upheld by all healthcare professionals. This expectation is also valid as regards electronic health record (EHR) systems.⁶

Privacy principles need to be embedded in the operational design of EHRs and everyone using EHRs must have a common understanding of their privacy obligations. A coherent legal framework to appropriately protect the privacy and confidentiality of personal health records is therefore an essential building block for EHRs⁷.

The innovative solution described in this paper shown its effectiveness in solving a variety of seemingly unsolvable problems, delivering security, privacy and confidentiality without impacting on usability.

From an economic perspective, deploying JANUS and 3AKey will save organisations money. More importantly, it delivers the EHR confidentiality that all stakeholders wants and gets the privacy compliance for free.

Biographical Note

Poy currently works at FrontOne Limited; he is the founding Director and the inventor of Message Dissemination and Human Factor Authentication technology - the foundation technologies of 3AKey and JANUS solution. Poy's profession interests are in electronic, information and communication security, he is the architect of JANUS and the lead designer of 3AKey.

⁶ ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf

⁷ <http://www.healthissuescentre.org.au/documents/items/2008/05/206744-upload-00001.pdf>