Towards an Evolvable Cyber Security Protection Profile for Electronic Medical Records to Ensure Privacy and Security

Damian Watkins, Craig Scott
Morgan State University
School of Engineering
Principle Investigator
PACER: A Homeland Security Center of Excellence
Damian.Watkins@Morgan.edu
Craig.Scott@Morgan.edu

ABSTRACT

Electronic Medical Records (EMR) provide increased productivity and convenience for patients, doctors, nurses, pharmacists, lab technicians and other medical professionals. The added accessibility to patient information introduces a multitude of security risks at various levels. The communication infrastructure may be breached by intruders from disparate countries. Loosely protected data entry terminals are susceptible to insider threats. This paper characterizes EMR systems as cyber-physical systems that must be protected by minimizing potential risks at each communications interface, data entry point, and data warehouse. A protection profile concept is discussed that provides management of risk based on known hacker modalities.

1. INTRODUCTION

The transition of patient health information to an electronic medical record (EMR) provides the benefit of increased productivity in doctors' offices and hospitals. An EMR provides increased speed and convenience as physicians begin to offer services such as instant messaging, video conferencing, and other online services to reduce the need for in-person visits. However, the expediency of medical care enabled by the digital age also presents inherent risks to the privacy of the patient as well as the integrity of the provider. Individual names, social security numbers, medical produces, and billing records that are now stored electronically as part of the EMR are also highly valued targets by hackers.

2. EMR as a Cyber-physical system

Hospital systems, health care provides, clinics, pharmacies and other entities are implementing complex, distributed software systems that handle real-time patient information. Patient vaccine, prescription, and examinations will be stored in data repositories. Current pharmacy and lab systems will be replaced by point of care on line medication administration system and an electronic medication administration record and the following nursing documentation [1]:

- Clinical Documentation
- Vital Signs, Height, Weight
- Intake & Output
- Admission History
- Assessments (Medical, Surgical, Acute Rehab, Psych, Pediatrics, Critical Care)Discharge / Transfer Documentation
- Communication to Providers
- Discharge Instruction Template
- Patient Education Communication
- Patient Access List (PAL)
- Rules based triggers i.e. admission assessment, falls, pressure ulcers, pain
- Patient Care Summary

Healthcare clinics and physician offices contain wireless networks that allow creation and storage of medical prescription information via personal digital assistants, smart phones, LCD screens, data terminals, etc.

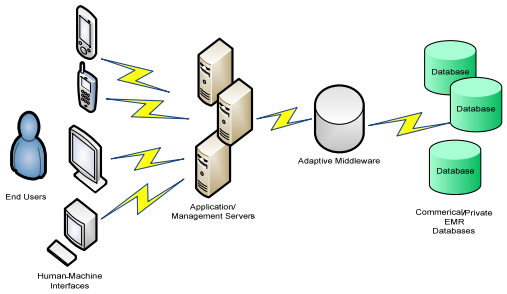

Figure 1. Cyber-physical EMR system

The addition of emerging technologies such robotic surgery and nano-electronics connected via wireless networks must be supported by a complex middleware layer. The EMR effectively becomes a cyber-physical system if it contains programming abstractions that support middleware and operating system layers for: [2]:

- Real-time Event Triggers
- Consistent views of distributed states in real-time within the sphere of influence. This challenge is especially great in mobile devices
- Topology control and "dynamic real-time groups" in the form of packaged service classes of bounded delay, jitter and loss under precisely specified conditions,
- Interface to access to the same type of controls regardless of the underlying network technology.

Figure 1, illustrates a high-level view of the cyber-physical EMR system. The core component in the diagram is the adaptive middleware between the application server and the back-end databases. The adaptive middleware contains the expert rule engines, sensor algorithms, and policy engines that govern the coordination between the computational and physical segments of the system. Results from robotic surgeries and medical scans may be transmitted, stored, and evaluated in real time. Patent medical information are contained in different forms and stored in a variety of disparate databases. In section 4, we will discuss how data from different databases with varying functions can lead to identification of an individual record by cross-correlation.

3. Cyber intrusion threats

The main threat to medical privacy is the abuse of unauthorized access by insiders and the most common threat vector is social engineering [3]. The best security training for individuals and defense-in-depth technical measures cannot protect a system where too many people have access to too much data. The following are examples of successful cyber intrusions that lead to compromised personal health information:

- October 2008 – Hackers accessed millions of patient files held by Express Scripts, Inc and threatened to expose the medical information unless a ransom was paid [4].
- April 2009 - Hackers compromised the Virginia Prescription Monitoring Program and usurped access to 8 million patient records 35 million prescription for a $10 million ransom. [5]
- May 2009 – Hackers broke into restricted databases at the University of California Berkeley and exposed the records of 160,000 college students. [6]

To protect patients, the Health Insurance Portability and Accountability Act of 1996 was enacted to require national standards for electronic heath care transactions and provides safe guards to ensure the protection of personal health information. Under the act, heavy civil and federal criminal penalties may be levied against providers if negligence is determined. For example, CVS pharmacy was required to pay $2.25 million as a settlement for violating HIPAA privacy laws [7]. Hence, risks associated with vulnerabilities exploited by cyber intrusions compromising electronic medical record systems should be managed to protect the personal health information of individuals as well as mitigate the financial losses and reputation of health care data providers.

4. Medical Inference Control

The standard methodology to protect patient information is to removed the patients name and address in attempt to make the record anonymous. This method of de-identification can be easily thwarted by complex database queries and data aggregation. For example, by searching medical procedures on a particular date and associated that information with an individual's date of birth. The patient also may be identified by cross correlating public access records with commercial database information. For example, a query that displays the records of all women aged 36 with daughters aged 14 and 1 such that the mother and exactly one daughter have a particular disease is likely to pull one individual out of millions of possibilities.

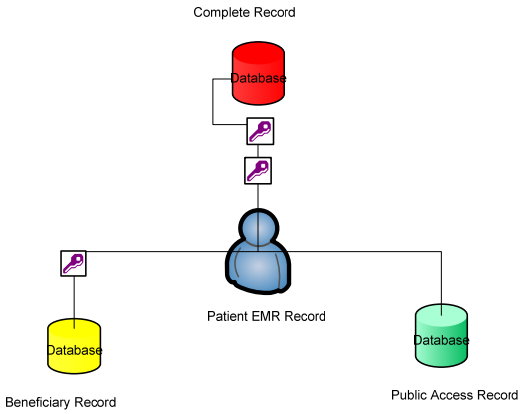

Figure 2. Patient Medical Record Versions

To control this The Healthcare Finance Administration (HCFA) maintains three types of patient medical records [3]:

- Complete medical records to bill patients
- Beneficiary-encrypted records with obscured patients' names and social security numbers
- Public access records with all information removed except demographic information

However, the HCFA methodology still does guarantee that a patient will not re-identified. The richer the dataset on a particular individual, the higher the likelihood a patient may be identified. There needs to be a method for researchers to make statistical inquiries without compromising individual's privacy. Insider threats from disgruntled employees remain a threat. Also,

data access violations from users that have transfer to a new position or department but still have privileges as well as mission creep by data entry personnel must be mitigated.

5. Protection Profile

A "living" cyber security protection profile should be implemented to manage the inherent risk associated with the changing states electronic medical record systems. It attempts to answer the question, "Who am I securing my data from and in what environment?" [3]. Security of a cyber physical system isn't a scalar methodology. The overall risk and vulnerability in the system must be quantified. A protection profile is the culmination of cyber security processes including a baseline of potential assets that are attractive to hackers, a risk assessment plan that specifies the vulnerabilities of those potential assets, and an information assurance process provides an implementation to reduce cyber risks listed in the assessment plan [8]. There has been a tradeoff between availability and security since the advent of enterprise web applications, distributed databases, and high speed data connections. Security is often the last step or omitted entirely from the product development cycle of electronic systems. Software developers hastily produce capability and leave the security of their systems as an afterthought. It can be rationalized that the proper encryption techniques to ensure privacy, firewalls to reduce port entry, and authentication modalities should provide enough protection if properly implemented. Also, opponents of increased security policy add an added layer of bureaucracy that requires additional resources. There also may be a fear that too many layers of security will adversely impact the availability of valuable information in times of emergency.

It can be argued that the ability to perform evolvable security architectures cannot be based solely on the accreditation level of electronic medical record system included as part of the enterprise infrastructure. As an alternative, the protection profile should be based on potential impacts from the five categories of attack exploits:

- Probing
- Penetration
- Persisting
- Propagation
- Paralyzation

The ability to probe including foot printing and scanning will be quantified for each component within the cyber system. Systems that are highly connected with exposure to the outside world are more susceptible to probing. Similarly, the impact of penetration depends on the access to sensitive information and connectivity to other systems. For example, an attacker may use fragmented ping sweeps to bypass firewalls and penetrate the network. Furthermore, an attacker may exploit vulnerable components via persistence using enumeration techniques to garner useful information such as the operating system a particular component may be running. An attacker may also use phishing techniques, trojans, buffer overflows, and cross-site scripting to garner user information. Attackers will plant listeners for backchannel and man-in-the middle attacks that propagate false routing information throughout the cyber network once inside the security perimeter. Also, internet worms and viruses may be propagated through websites, email, and news groups. Finally, an attacker will attempt to paralyze the cyber system if he/she is unsuccessful with hacking into the system or may wish to strategically remove a resource.

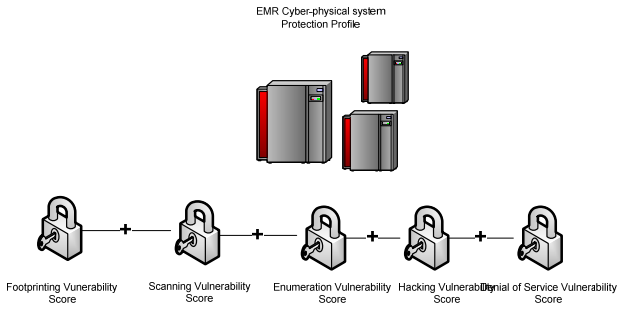

Figure 3. Cyber-physical EMR Protection Profile

Vulnerabilities in the system are the manifestation of the inherent states of the system. This includes physical, technical, organizational, and cultural weaknesses that can be exploited or otherwise adversely affected by terrorism, natural hazards, and accidents that result in harm or damage to that system [9]. Intent is the desire or motivation of an adversary to attack a target and cause adverse effects. Capability is the ability and capacity to attack a target and cause adverse effects. Threat is the intent and capability to adversely affect (cause harm or damage to) the system by adversely changing its states. Risk is the result of a threat with adverse effects to a vulnerable system. Using this approach, the evolvable protection profile minimizes the damage caused by the preceding hacking techniques. The impacts that are documented and quantified will give insight into potential strategies, exploitable vulnerabilities, and potential exploits that may be developed by cyber attackers in the future.

The use of a profile produces an adequate formulation of risks and the potential impact of those risks. As technology evolves potential exploits become increasingly sophisticated. In many cases, they include the coordination among several attackers as well as the use of bots and complex propagating worms. However, the methodology utilized by attackers has not varied only the exploits used to implement the methodology. If the potential methodologies employed to compromise EMR

systems are clearly understood, the risks and subsequent impact are much more quantifiable.

6. Penetration Testing

Rich media applications based on technologies such as Asynchronous JavaScript and XML (AJAX) are susceptible to cross site scripting, html attacks and phishing exploits where users believe they are accessing a page, but in reality they are accessing a hacker generated page. To prove this point, three prominent open source electronic medical record frameworks were installed locally and scanned for vulnerabilities:

- OpenMRS [10]
- INDIVO [11]
- openEMR [12]

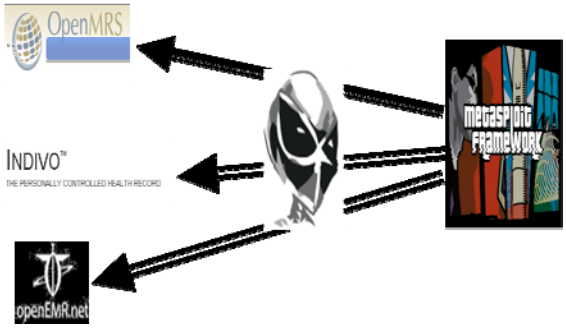

Figure 4. Experimental Penetration Test Setup

METASPLOIT [13], an open source penetration testing tool and NIKTO [14], an open source vulnerability scanner were used to scan frameworks that included a database and web application capability. As shown in Figure 4 (above), the METASPLOIT framework was used to penetration test each EMR system. All three medical record formats were installed with a generated password protected key store as well as SSL enabled web functionality. It was found that although security layers were installed, each EMR system exhibited a vulnerability to the following attacks:

- Privilege Escalation on the web server
- Cross-site scripting (XSS)
- SQL injection

Privilege escalation allows users logged into the web server to gain access to additional resources on the file system by exploiting a design flaw or bug in the software. Cross-site scripting grants an attacker the means to inject malicious code into a web page viewed by others. Finally, SQL injection attacks exploit database flaws and a lack of input validation to allow an attacker to execute database commands from the web page. In the cyber-physical EMR system that encompasses wireless connectivity to wireless devices, surgical equipment, and other medical technologies; vulnerabilities to code injection and privilege escalations are highly prevalent. This is due to the open architecture and distributed data schemes.

7. Conclusion

The Cyber-physical EMR medical system accommodates evolving technologies including sensor networks and robot surgery technologies that provide increased access to medical information. This increased access enabled in some cases by wireless technologies leads to a multitude of vulnerabilities. The development and execution of an evolvable cyber security protection profile is an effective method of managing risks based on these vulnerabilities. As a "living" document the profile may be adapted and executed to combat emerging threats presented by new technology. This will help ensure that personal heath information is protected and the health data record provider is provided indemnity from violation of the HIPAA statues.

8. References

[1] Franklin Square MedConnect Cerner Project. http://www.franklinsquare.org/npt.cfm?id=558887

[2] L. Sha, S. Gopalakrishnan, X. Lui, and Q. Wang, "Cyber-Physical Systems: A New Frontier", IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing 2008.

[3] Ross Anderson, *Security Engineering 2nd Edition, Wiley Publishing 2008*

[4] Express Scripts Press Release. http://www.esisupports.com/esisupports/esi-release111108/

[5] Health Leaders Media Release. http://www.healthleadersmedia.com/content/232554/topic/WS_HLM2_TEC/Hacker-Holding-Virginia-Health-Records-for-10-million-Ransom.html

[6] California-Berkeley news Release. http://datatheft.berkeley.edu/news.shtml

[7] HSS.gov press release. http://www.hhs.gov/news/press/2009pres/02/20090218a.html

[8] C. Schou and D. Shoemaker, Informaiton Assurance for the Enterprise: A Roadmap to Information Security, McGraw-Hill/Irwin, New York, 2007

[9] Chittister, Clyde G. and Haimes, Yacov Y. (2006) "Cybersecurity: From Ad Hoc Patching to Lifecycle of Software Engineering," *Journal of Homeland Security and Emergency Management*: Vol. 3 : Iss. 4, Article 3.

[10] OpenMRS. (http://openmrs.org)

[11] INDIVO. (http://indivohealth.org/)

[12] openEMR. (http://www.openemr.net/)

[13] METASPLOIT (http://www.metasploit.com/)

[14] NIKTO. (http://www.cirt.net/nikto2)