HIPAA Security Mechanisms for Medical Devices

Michael A. Jofre and Dr. Eduardo B. Fernandez
FAU College of Engineering and Computer Science

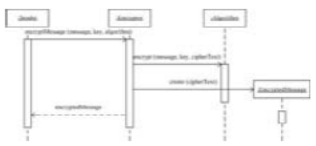
Introduction

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA Pub.L. 104-191, 110 Stat 1936, enacted August 21, 1996) has two parts, Title I and Title II. Title I of HIPAA deals with Health Care Access, Portability, and Renewability. Now the Title II of HIPAA is involved with Preventing Health Care Fraud and Abuse, Administrative Simplification, and Medical Liability Reform. Per the requirement of Title II, the Department of Health and Human Services (HHS) has advocated five rules regarding Administrative Simplification: the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule. Our discussion will focus on the possible security threats that can occur to medical devices within the parameters of the Security Rule in relation to the Required Implementation Specification and the Addressable Implementation Specifications. These devices not only perform their intended medical functionality, but they also perform other functionalities that can be affected by security threats. As a result, HIPAA's privacy guidelines need to be enforced by appropriate security mechanisms within these medical devices. Security mechanisms can be described by software patterns. A few of these patterns will be discussed, showing how they can handle such threats. We will survey existing patterns and identify which other patterns would be necessary.

Method

How can we perform the Change Cipher Specification Message Drop attack on the client/server communication protocol in order to delay the server's pending state and prevent it from sending the finished message to establish the secure communication with the client? The attack can take place because the care of the hardware and software in the medical devices might not have been properly set-up either by the manufactures, 3rd party vendors or resellers. As a result, certain security components might not have been encrypted.

Figure 1:
UC Encrypt a message



UC Decrypt a message

Figure 2: Class Diagram for SSL Client/Server Communication

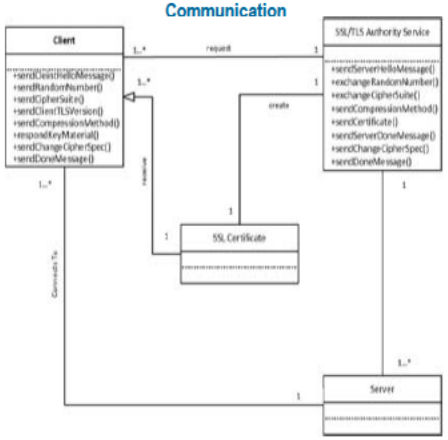
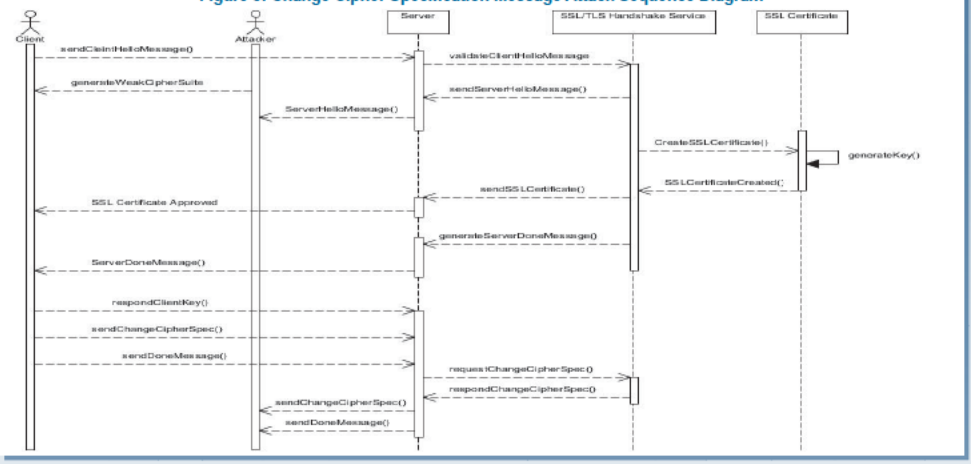


Figure 3: Change Cipher Specification Message Attack Sequence Diagram



Results

Figure 3 shows the sequence of events when the attacker is able to intercept the client Cipher Specification Message. This violates the authentication protection between the client/server communication.
Figure 2 shows the Change Cipher Specification Message Drop Attack.
Figure 1 shows a use case for the Encryption and Decryption Message sequence.

Discussion

As the overhead cost of medical devices keep rising, sometimes entities in the medical field might purchase or lease units at a much lower prices. They might not realize that the devices that they are purchasing form a reseller and/or 3rd party vendor, whether national or international, might not be HIPAA complainant. Within the guidelines of the Title II of HIPAA's Security Rule section of Physical Safeguards, it states that access to equipment containing health information should be controlled and monitored. When 3rd party vendors and resellers do not adhere to these guidelines, they create vulnerability issues that affect both smaller and larger institutions. Also, manufactures and 3rd party vendors might interpret differently the Addressable Implementation Specification. As a result, the level of security might not be enough to properly ensure medical records, but the price options look appealing. In order to have proper level of security the Required Implementation Specification needs to be enforced across to all entities. Also, liability needs to be enforced without discretion.

References

http://www.hhs.gov/ocr/privacy/index.html
http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act
http://www.healthmgttech.com/archives/
http://www.journals.elsevier.com/computer-standards-and-interfaces/