Abstract

This paper reflects on some key elements of a sophisticated Internet network within a healthcare organization of which I have regular access to. The paper begins by introducing several challenges within networks as such, including their availabilities within healthcare organizations. The paper continues by shedding the light on the infrastructure of these networks, while maintaining the focus on one key component of these sensitive networks. Performance is then discussed while questioning the security of the network. The paper concludes by addressing security concerns with several protocols that are available for use within these networks. Although this paper is based on the hospital Internet network that I have regular access to, I expanded my research by looking into peer-reviewed articles, consequently keeping a general format of this paper.

Keywords: health level seven, HL7, transport control protocol, TCP, Internet protocol, IP, secure sockets layer, SSL, health information systems, HIS, open systems interconnection model, OSI model, hypertext transfer protocol, HTTP, acknowledgment message, ACK message, virtual private network, VPN

Evaluation of Hospital Internet Networks Utilizing Health Level 7 Interface Engines

Introduction

Healthcare reforms have been leaning towards implementing electronic medical records within the U.S. healthcare system to reduce cost and improve patient care. However, the cost of electronic medical records is extreme, reducing their availabilities in many organizations. According to the U.S. Department of Health and Human Services (2011), the cost of implementing electronic health records could easily exceed $100,000.00 with an annual maintenance fee of about $85,000.00, which does not include the cost of Internet switches, cables, and wireless Internet connections. Much of the maintenance costs and the initial installation costs can be dramatically decreased with interoperability, which is “the ability of health information systems to work together within and across organizational boundaries” (HIMSS, 2013). With interoperability, healthcare facilities would not have to spend tremendous amounts of money in order to develop applications that would allow health information systems (HIS) within their networks to communicate with each other. According to Benson (2012), “the more people can interoperate, the more cost-effective is every new application and the larger the IT market becomes.” However, unlike the public Internet or the World Wide Web, health-based networks lack sufficient standardizations that would allow interoperability.

Healthcare organizations normally use several disparate applications for a wide variety of purposes, whether it is to care for a patient, prescribe a medication, or bill a patient for a visit. Therefore, several applications must interact with each other so that the information is readily available for physicians, nurses, or accountants. The challenges are obviously different depending on the size of the healthcare facility. A point-to-point interface may be sufficient for some small facilities but not larger ones. According to Chander (2012), “Point-to-point interfaces are designed to send data from system A to another system B through
a custom link (i.e., the interface) between the two.” Therefore, in order to establish interoperability, an interface must be built between each two systems in order for the two to exchange information. For example, in order to transfer data from one system (e.g., admitting) to two other systems (e.g., billing and lab), two separate interfaces must be built. Consequently, the number of interfaces would increase as the number of applications increase. However, what if an interface engine could exist that would understand the language of all the HIS within a hospital’s network?

**Infrastructure and Performance**

Health Level Seven (HL7) emerged in 1987 in hopes to accomplish interoperability so that disparate HIS can easily communicate patient information between each other (Shaver, 2007). This would allow several clinical units (e.g., radiology and surgery) within a hospital to easily exchange patient information – compared to paper-based systems. This would also allow healthcare professionals to exchange information despite the type of care that they provide or the software applications that they use. For example, a radiologist who uses MedicsRIS might be able to retrieve a patient’s health information that was entered by an emergency department physician using Meditech. There are several challenges that can make this extremely difficult to accomplish. Typically, the hospital would issue a request to its IT or biomedical department to develop or seek software developers who can build an interface that can understand the language of both systems in order to exchange information, which would undoubtedly be extremely costly. On the other hand, some vendors build their applications to be HL7-compatible. However, even with HL7 compatibility, further customization is still required in order to establish interoperability.

Figure 1 illustrates the data flow within a point-to-point interface and an interface engine. Figure 1 (a) illustrates how lab, pharmacy, billing, radiology, and health information systems can exchange information by simply retrieving it from the interface engine. Figure 1 (b), on the other hand, illustrates the challenges in establishing point-to-point connections among multiple applications in order to exchange information. For example, in order for billing to retrieve information from lab, a point-to-point interface must exist.

By definition, “Health Level Seven (HL7) is a standard series of predefined logical formats for packaging healthcare data in the form of messages to be transmitted among computer systems” (MedScribe, 2013). The naming behind HL7 comes from the seventh layer of the Open Systems Interconnection (OSI) model. The International Standardization Organization’s OSI model consists of 7 layers: (1) physical, (2) data link, (3) network, (4) transport, (5) session, (6) presentation, and (7) application (Kurose & Ross, 2013). Since HL7 addresses communications between
EVALUATION OF HOSPITAL INTERNET NETWORKS

Evaluation of Hospital Internet Networks Utilizing Health Level 7 Interface Engines
Marco Abuaitah © May 15, 2016

applications (i.e., the seventh layer), it was named accordingly.

A typical HL7 message includes several three-letter segments that identify their contents. The main segments are shown in Figure 2 and they include MSH, EVN, PID, nk1, and PV1. MSH represents the message header, EVN indicates the event for which the patient is visiting, PID represents the patient identification segment, NK1 contains the next of kin information, and finally PV1 includes visit-specific information such as the name of the attending physician (Balachandran, 2014). Each segment indicates what type of information should be included in that field. This would make it possible for the sending HIS and the receiving HIS to be interoperable. For example, the MSH segment (i.e., the header), includes information about which application is sending the message, which application is receiving the message, what format the message is in, and a time stamp (Murray, 2012). The “|” symbol represents a separator between the fields. For example, the patient’s name John Edwards and his date of birth 12/02/1985 would be presented as “EDWARD JOHN | 19851202”. Therefore, any simultaneous bars (e.g., “|||”) would indicate that optional fields were present. The only mandatory message segments are MSH, EVN, PID, and PV1 (Benson, 2012).

Figure 2. HL7 message. This figure illustrates the main segments on an HL7 message.

According to Scarlat (2012), “Semantics and meanings of a message are not within the scope of the OSI model.” Therefore, in order to transfer clinical data within a certain network, transmission standards are needed to address the semantic interoperability. In order to be transmitted over TCP/IP (Transmission Control Protocol/Internet Protocol), HL7 messages would need to be enclosed or framed at the session layer of the OSI model. Although it has not been formally established to be the standard for transmitting HL7 messages, the minimal lower layer protocol (MLLP) is currently the most widely used protocol to transferring HL7 messages within health systems networks (Subramanian, 2009). MLLP – also known as simply the lower layer network (LLP) – frames HL7 messages by establishing a header and a footer so that when the messages are transferred, it is known where they start and end. The coding associated with MLLP when encoding HL7 messages are “<SB>”, “<EB>”, and “<CR>” referring to the start of the block (1 byte), end of the block (1 byte) and segment separator (1 byte), respectively (Subramanian, 2009). This is illustrated in the aforementioned HL7 in Figure 2.

In order for an HL7 message to get across the network to other applications, it must first pass through the HL7 interface engine as shown in Figure 3. The engine contains a listener that continues to listen to the main database to detect any changes. A database administrator would establish this connection between the listener and the database by ensuring that the database allows data exchange with the port number at which the listener is "listening". For example, if a registrar admits a patient to the hospital by entering his or her information in an ADT (admission, discharge, and transfer) interface, the listener would detect that a new patient has been admitted to the hospital and begins to process the HL7
message to be sent to other systems. The data is then queried and processed by the HL7 builder where the HL7 message is constructed based on the specified template. Finally, the sender ensures that the HL7 message arrives at the specified destination.

**Figure 3.** Inside the HL7 Engine. This figure illustrates the process inside the HL7 interface engine.

Similar to the hypertext transfer protocol (HTTP), which establishes a protocol between a client and a server on the Internet, HL7 hopes to establish standards between a client and an Interface engine within health systems networks. Furthermore, Kabachinski (2006) expressed in the Biomedical Instrumentation and Technology journal that HL7 is much like TCP/IP and defined HL7 as “a specification for describing, formatting, encoding, and sharing of clinical and administrative data in healthcare.” In fact, HL7 runs on top of TCP. From the perspective of the OSI model, once the HL7 message is enveloped at the session layer, it will reach the transport layer where a transport layer protocol (i.e., TCP) aids in ensuring the message’s delivery, based on the message’s specified IP address and port number. A new “layer” is added to the HL7 message as it moves from the sending application to the receiving application as shown in Figure 4. Once at the network layer, IP comes into play to ensure that the HL7 message is being routed to the right destination while taking the shortest path possible. HL7 and TCP at this point are not concerned about how the HL7 messages are being routed. Once at the data link, TCP/IP may run on top of several data link protocols/infrastructure (e.g., wireless Wi-Fi, wired Ethernet, etc.) (Kurose & Ross, 2013). These second layer protocols will ensure that the HL7 message moves from one node to the next, despite the link type. Finally, the HL7 messages are translated into bits and bytes at the physical layer. According to Kurose and Ross (2013), the physical layer moves the individual bits from one node to the next.

**Figure 4.** The OSI Model. This figure generally illustrates the delivery of an HL7 message through the OSI model layers.

Furthermore, ensuring receipt of HL7 messages is accomplished by the HL7 ACK (acknowledgement) protocol. Since these messages work over TCP/IP, some ACK messages are being implemented to be sent over the same client channel where data is being sent. When a message is sent to the receiver, the receiver is expected to send back an Acknowledgment message to indicate whether or not the message was received. According to Integrating the Healthcare Enterprise [IHE] (2007), an
acknowledgment message may include positive acknowledgments (AA) to indicate that the message was received successfully, an application error (AE) to indicate a problem in processing the message, or an application reject (AR) to indicate an issue within the message segments (e.g., a missing field). For example, Figure 5 illustrates part of an HL7 indicating that the message was received successfully by the receiver application by returning AA to the sender along with the original message’s ID.

Figure 5. Part of an HL7 Message. This figure illustrates the AA in an HL7 message.

Management

Maintaining interoperability in a healthcare organization may simply require extracting information (e.g., processes logs) from the interface engine. This would allow an administrator to be able to identify an issue when it occurs. This is essentially important to avoid time-consuming HIS inspections. For example, if a healthcare provider is not able to see a patient’s information that was entered by a registrar in an ADT interface upon the patient’s admission, then the cause might be network-related, HIS-related, or engine-related. Therefore, extracting information from the interface engine would indicate whether the messages are being lost, holding up the queue, or missing the appropriate format.

One of the essential duties in managing and maintaining the hospital’s network is ensuring that the aforementioned HL7 interface engine listener is configured according to each application. Healthcare facilities may use a variety of software applications that would enable them to monitor their HL7 interfaces to make sure that their HIS is interoperable. For example, eiConsole supports TCP/IP and LLP over TCP/IP and can be configured to listen to HL7 messages over a specific port number as shown in Figure 6 (PilotFish, 2015).

Additionally, managing the entire Internet network as a whole is also essential because of the amount of devices that are contained within an individual network. Several interfaces and protocol data units (PDUs) exist that would allow managers to monitor the performance of their networks. The most common protocol for managing TCP/IP networks is the Simple Network Management Protocol (SNMP) (Windows, 2016). Several SNMP operations allow administrators to send and retrieve information to and from network devices. For example, if there is an HL7 message that had been lost or an application that is not able to display patient information, an administrator can query the devices involved in the data exchange in order to identify the problem. This is made possible by the SNMP clients located on the network devices and the SNMP manager querying the data. For example, a GET operation
would allow the SNMP manager to retrieve information about the status or a router within the network (Jiang, 2002).

**Security**

HL7 is currently being used by over 90% of the U.S. hospitals (Benson, 2012); therefore, implementing a standard for transmitting HL7 messages is extremely vital, especially when considering the security of patients’ confidential information. Some of the sensitive issues associated with HL7 question the security of the messages sent between HIS. Paper-based patient charts are only physically accessible as they are maintained in a hospital’s medical records department or a physician’s office. Therefore, an intruder or an unauthorized person would have to be physically present at these locations in order to obtain the patient information. However, the birth of electronic medical records has opened the doors for intruders to obtain medical records remotely as the information became available on the Internet. Furthermore, the growth of the number of facilities using electronic medical records places a greater emphasis on the security of electronic medical records that exchange HL7 messages. So, how secured is patient information when sent as HL7 messages over TCP/IP using LLP (Lower Layer Protocol)?

In order to be able to transfer clinical information over a network with a maximum possible security, the data must be standardized. This allows several systems, including security systems, to know what to look for to prevent intrusion. According to Al-enazi and El-masri (2013), the number of optional fields entered in a clinical system makes it harder for HL7 to have interoperable standardization. This was illustrated in Figure 2 where multiple consecutive “|” symbols were included in the HL7 message with no values in between, indicating optional fields when entering data. Therefore, enforcing the number of optional fields in an HL7 message may strengthen the security of HL7 messages when they are being exchanged. Aside from standardization, encryption is also essential when transferring data over a network weather it is a local area network (LAN) or a wide area network (WAN). Many organizations elect to use virtual private networks (VPNs) to add a level of security to their sensitive data (Covill, 1998).

According to Kurose and Ross (2013), the virtual private network, which is associated with the Link layer, simply provides business with a way to build a private network without all the physical requirements of the network setup. Taking this into consideration, it would be more secure to move HL7 messages via MLLP, and over a VPN.

Other secure transfers include the secure sockets layer (SSL). According to Kurose and Ross (2013), although this TCP enhancement (i.e., SSL) offers “critical process-to-process security services, including encryption, data integrity, and end-point authentication,” it is implemented in the application layer. Therefore, it may not be as easy, if ever, to transfer the application-layer based HL7 messages over SSL. The key concept, however, is interoperability. If in fact HL7 messages are transferred over SSL, then the challenges of interoperability would remain unresolved. Therefore, the goal is to have a secure transmission of clinical data and, at the same time, have the health information systems understand each other. Therefore, the presence of LLP allows HL7 to be encoded so that they have a header and a tailor, which identify their message start and end parameters when transmitted between
Electronic medical records. As the name may imply, Minimal Lower Layer Protocol does not provide any type of encryption, especially since it is simply an application layer protocol (HL7, 2007). According to Health Level 7 International (2007), the idea is to have a TLS-equivalent protection, which was set by IHE (IHE, 2007).

Another security measure is contributed to the aforementioned HL7 Acknowledgment protocol. Like TCP, and unlike UDP, HL7 implements an ACK message which can be contributed as a security measure because of rejecting unknown messages when recognized. According to IHE (2007), “The ACK message is in all cases an application level acknowledgement, which conveys application errors (if any) detailed by the receiving application”. For example, if an HL7 message is sent with unknown MSH content to the receiving application, the receiving application would simply reject it. The transmission of HL7 messages occurs over TCP/IP in local area networks (LANs). According to Murray (2012), “Minimal Lower Layer Protocol (MLLP), is the absolute standard for transmitting HL7 messages via TCP/IP.” Murray (2012) also reiterates that TCP/IP is a continuous stream of bytes, and that MLLP is needed in order to signify the beginning and end of each HL7 message.

REFERENCES


Evaluation of Hospital Internet Networks Utilizing Health Level 7 Interface Engines

Marco Abuaitah © May 15, 2016