Journal of Computer Science 7 (11): 1691-1703, 2011
ISSN 1549-3636
© 2011 Science Publications

A New Security Model using Multilayer Approach for E-Health Services

[1]Rossilawati Sulaiman, [2]Dharmendra Sharma, [2]Wanli Ma and [2]Dat Tran
[1]School of Computer Science, Faculty of Information Science and Technology,
National University of Malaysia, 43600, Bangi, Selangor, Malaysia
[2]Faculty of Information Science and Engineering, University of Canberra,
Bruce, 2601, ACT, Australia

Abstract: Problem statement: Delivering services online is important in e-health. Services that are delivered through online communications between engaging parties, often involve sensitive information transmitted over the Internet. However, while the Internet successfully facilitates these services, significant threats also come in parallel. Network attacks, information breaches and malicious software on a computer system are common threats to the Internet. These threats can cause severe damage to computer systems and also the information. As we study current security technologies particularly that provide security to online communications, we found out that these technologies do not cater for different kinds of security needs because of the rigid way the security mechanisms are constructed. Therefore, we are interested in developing a security model that facilitates these needs, specifically in e-health. **Approach:** First, the area where different security requirements are needed are explored, such as the information classification found in ISO17799. This classification is based on the sensitivity levels of the information, where the more sensitive information requires higher security measures compared to the less sensitive information. Then, the information classification is applied to the e-health environment, so that our security model can handle the security processes for each classification. **Results:** The multilayer communication approach or MLC is the proposed security model. MLC classifies communications in e-health into five categories: Layer 1 to Layer 5 representing extremely sensitive, highly sensitive, medium sensitive, low sensitive and no sensitive data. This classification refers to the different sensitivity of the information exchanged during communications. For example, Extremely Sensitive communication involves exchanging extremely sensitive information, which requires highest security mechanisms, while Low Sensitive communication requires lower security mechanism. **Conclusion:** MLC provides five different types of security needs, where users can flexibly choose their own security preferences for their online communications, which the current technologies are lacking.

Key words: Cryptography protocols, e-health and multilayer approach, online communication, Multilayer Communication (MLC), e-health promises, diagnostic aid, security model, online communications

INTRODUCTION

The Internet plays a major role for delivering services in e-health, since it offers cheap and worldwide access. Sulaiman *et al*. (2007) discusses examples of online communications in e-health, which include videoconferencing sessions, x-ray image sharing, electronic mails, web-based applications and also software applications used with mobile devices (e.g. PDA and smart phones) to assist mobile users. Using the Internet in e-health promises to improve communication between users, because patients in rural areas can access services such as consultation sessions, diagnostic aid and remote patient monitoring (Kay *et al*., 2011; E Health News. Eu, 2011). In this study, the term “communication” is defined as a process of sharing and exchanging information between two or more parties in the e-health domain.

However, although there are many Internet-based technologies developed to facilitate the communication processes and enhance healthcare service delivery, the Internet has its own drawbacks. It is exposed to security threats, which exploit the vulnerability of computer systems. The threats include network attacks,

Corresponding Author: Rossilawati Sulaiman, School of Computer Science, Faculty of Information Science and Technology, National University of Malaysia, 43600, Bangi, Selangor, Malaysia

information breaches by intruders and malicious software or malware (Symantec Corp, 2010; Georgia Tech, 2008).

Current security technologies such as SSL/TLS, IPSec, SSH, or VPN have been robustly put into practice to provide security mechanisms to online communications. In practice, in order to use such technologies, for example SSL, one must configure the security setting and select appropriate cipher suites, which is a combination of algorithms for authentication, encryption and message authentication code (MAC), which are used to negotiate the security settings when starting a connection. However, we are interested in finding a way to provide security mechanisms that can cater for different types of security needs. For example, communications from a sender to multiple recipients can be done using different security strengths, without having to reconfigure the security setting. As to our knowledge, current security technologies only provide or can only be set to one particular value of cipher suites for every communications, that is, if one wants to have stronger or weaker security, the security must be reconfigured. We address this problem through our security model namely the Multilayer Communication (MLC).

Security technologies: There are various aspects that have been catered for in the security field, such as from monitoring the security at the network perimeter (firewalls and IDSs); securing the hosts inside the network (personal firewalls and antiviruses); to securing communications between hosts (SSL, SSH, IPSec and VPN). Here we focus our discussion in securing communications between hosts, which revolve around technologies like SSL/TLS, IPSec, SSH and VPN. These technologies have the same characteristic, which use cryptography protocols for the security processes.

Secure Socket Layer (SSL) was developed by Netscape Corporation (http://netscape.aol.com/) and later standardized and known as Transport Layer Security (TLS). It works on the transport layer of the OSI model, which means, it protects traffic in the application layer. In general, SSL's goal is to provide a secure channel between the sender and recipient. In the Initial handshake process, both sender and recipient negotiate on a cipher suite that is a set of cryptography algorithms that will be used in the communication session. The cipher suite is a composition of the public key mechanism such as RSA, a symmetric cipher (block cipher such as RC4, Triple DES, AES, IDEA, or DES) and hash algorithm such as MD5 or SHA and their associated key size.

Although SSL/TLS does not provide security automatically to an application that wishes to benefit from the SSL/TLS functionalities (to deploy SSL/TLS, the application must be specifically programmed to be SSL/TLS aware), the deployment of SSL/TLS continues to grow at a robust rate.

IP layer security or IPSec (RFCs 2401-2411 and RFC 2451) provides security protection to the Internet layer and protects all IP data packets regardless of the protection given on the application layer and transport layer. No modification or reprogramming of applications is needed if IPSec is used. IPSec uses two protocols to provide security protections, which are the Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides data integrity and authentication of origin of the IP packets. The authentication process is based on MAC, using HMAC algorithm (Krawczyk *et al*., 1997) and a secret key.

ESP on the other hand provides full confidentiality through an encryption process and an optional authentication. ESP provides an encryption mechanism to encrypt IP packets before being transmitted to the receiver host and there the packets are decrypted. This provides confidentiality to the data and prevents any eavesdropping to the data. Various types of algorithms are supported by IPSec for encryption performed by ESP such as Triple DES, RC5, IDEA, CAST and Blowfish.

Virtual Private Network (VPN) is a private and secure connection established from two connected networks from sender to recipient over the Internet. VPN works by tunnelling IP packets by adding a new header to the packet, so that it can be encrypted and authenticated. Then, at the receiving end, the packets are assembled to the original form. The receiving end can be firewalls, routers, gateway, or hosts. VPN provides a number of tunnelling protocols, such as Point-to-Point Tunnelling Protocol (PPTP), that takes place at the Data-link layer and uses TCP port 1723. It encapsulates PPP packets and transmits the packets through a tunnel over a public IP network.

PPP uses authentication protocols such as Password Authentication Protocol (PAP) and Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP). PPP provides confidentiality on the data by providing encryption using DES and 3DES.

Besides these technologies, there are also proprietary software tools that support online communications such as demonstrated by GoToMyPC (http://gotomypc.com), Groove (http://www.groove.net) and Waste (http://waste.sourceforge.net/). GoToMyPC uses multiple layers of strong passwords as authentication, data confidentiality using SSL with AES-128 bit and end-to-end authentication. Groove uses passwordbased authentication; DES and AES-192 bit algorithms to provide data confidentiality on disk; as well as to data over the network to provide end-to-end security. Data integrity is also provided using hash message and message authentication code. Waste uses TLS to provide data confidentiality and builds a web-based PKI for trust between the users.

We emphasize our research on the application/software security, which is realized by integrating the security with the applications of information systems of the health organization. This is to provide authentication, confidentiality and availability to the information, using cryptography protocols to encrypt, decrypt, sign and hash messages (Jinyuan *et al*., 2011; Zhang and Liu, 2010; Garcia-Morchon *et al*., 2009). SSL is used to established a secure network for information exchanges (Markovic, 2006; Ulieru and Ionescu, 2004). The commonly used security protection for mobile device that uses wireless LAN are user authentication and encrypted wireless network (Elkhodr *et al*., 2011; Jaizanuar, 2009; Yu *et al*., 2008; Ahmad, 2003). In addition SSL is also used on wireless devices to provide transport level security (Gupta and Gupta, 2001; Marti *et al*., 2004).

However, from studying the existing security technology, we learned that for each technology, the level of the security provided is not flexible and cannot be changed according to the organization’s need. This is because the security configuration in the security mechanisms, such as SSL is set to provide a fixed security to the user per communication session. If there is a change in the organization’s need for a higher security level for example, the SSL needs to be reconfigured at the security setting.

In general, each technology offers a list of available and supported symmetric algorithms that are used to encrypt messages in transit during the communication sessions. However, these technologies do not cater for different types of security needs in an organization. Consider that an organization uses SSL for its secure communications. If the organization needs to change the security strength of the SSL channel such as shown IBM (2009), to be stronger or weaker, it cannot be flexibly provided to the organization. The person in charge, like the Security Administrator, needs to reconfigure the systems to change the security setting.

The need for stronger or weaker security strengths is necessary in information classification standard, such as portrayed in ISO 17799, where distinguished level of security protection is needed for different types of information with different levels of sensitivity. In an organization, different types of communications carry different types of messages. These messages contain different types of information with different levels of sensitivity.

We are motivated to find the best way to secure these different types of communications in such a way that it could provide different types of security strengths to the communication, which can be selected flexibly by the user. The next section discusses the different types of information as well as information classification in further detail.

Sensitive information and the level of sensitivity: In this section, we introduce the concepts of sensitive information and the level of sensitivity of the information in greater details. Sensitive information are those that should not be revealed to public (Pfleeger and Pfleeger, 2003). Whether the information is considered sensitive, is based on the importance or the values of the information and who is communicating it. It is important for an organization to decide whether the information will cause a significant loss to the holder if it is made public. For instance, a communication that exchanges information such as a name, a place and a meeting time, are less sensitive than information that has a name, an address and types of diseases that are considered more sensitive. A third party that intercepts this conversation may correlate the information and conclude that a person with that name and address has that particular type of diseases. Such information, if revealed to public will cause embarrassment and loss of reputation to the patient.

“The desired degree of secrecy about such information is known as its sensitivity” (Economic-Expert, 2009) such as more sensitive or less sensitive. The level of sensitivity of the information can also refers to the degrees of loss or potential damage to the holder, if the information is disclosed to a party that does not have any authority to access it. The levels of sensitivity of information often relate to the classification of sensitive information.

Classification of sensitive information can be seen adopted in most governments and business-related organization around the world. Classification of information is considered important because it provides guidelines to (1) classify certain information to different levels of sensitivity and (2) protect information from any unauthorized access by providing a distinguish level of security protection to the information.

Information classification: There are existing standards for information classification. ISO provides information classification guideline in ISO 17799, which classify information as Top Secret, Highly Confidential, Proprietary, Internal Use Only and Public Documents. Each of these classifications categorizes different types of information with different levels of sensitivity. The verbatim definition of each criterion is as follows (ISO17799):

- Top secret: Highly sensitive internal documents and data. Has very restricted distribution indeed and must be protected at all times. Security at this level is the highest possible.
- Highly confidential: Information which is considered critical to the organization's ongoing operations and could seriously impede or disrupt them if made shared internally or made public. Security should be very high.
- Proprietary: Procedures, project plans, operational work routines, designs and specifications that define the way in which the organization operates. Used by authorized personnel only. Security at this level is high
- Internal use only: Information not approved for general circulation outside the organization, where its disclosure would inconvenience the organization or management, but is unlikely to result in financial loss or serious damage to credibility/reputation. Security at this level is controlled but normal
- Public documents: Information in the public domain. Security at this level is minimal.

Meanwhile, the US government categorises, sensitive information as Top Secret, Secret and Confidential. Australia and New Zealand governments have an additional criterion known as Restricted. The verbatim definitions of the information classification are as follows (EO12958, 1995; SIGS, 2001):

- Top secret: The unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe
- Secret: The unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe
- Confidential: The unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe
- Restricted: Compromise of information would be likely to affect the national interests in an adverse manner

Technology gap: From the information classifications, we can imply that (1) 'Top Secret' is the most sensitive information, or (2) 'Highly Confidential' information is more sensitive than 'Proprietary' information, or (3) 'Confidential' information is less sensitive than Secret information. We can also imply that more sensitive data has greater degree of loss or potential damage compared to the less sensitive data.

However, with the current technologies, these different types of security levels cannot be applied to the different types of communications in the example of communication scenarios described above. This is because current technologies only allow all communications sessions to be secured with the same security strength. The key lengths in the symmetric key encryption determine the strength of the encryption and thus represent the security level or security strength (Security level and security strength will be used interchangeably throughout this study) that can be provided to secure the communication. This symmetric key is selected during the configuration or set up phase. If one wants to change the security levels of the communication, one needs to reconfigure the setting.

Only one cipher is chosen for a communication session. Therefore, if a user wants to send two different messages with two different classifications to two different recipients, this user needs to use different ciphers with different security level by reconfiguring the cipher or cipher suite field. In other words, current technologies do not cater for the following requirements:

- Provide different security strengths to secure different types of communications
- Provide mechanisms to handle security for low processing devices

In the next sections we will investigate further the types of information and the sensitivity levels of the information that is transmitted during communications in e-health. Then, we proposed an information classification based on ISO17799 to classify the information in e-health.

MATERIALS AND METHODS

Communication scenarios: In this section, we construct a general or typical type of a hospital environment. For simplicity purposes, the users involved in the communication either from inside the hospital local network or from the outside network are simplified and identified as Doctor, Patient, Nurse, Social Worker (SW), Paramedic, System Coordinator (SC) and System Administrator (SyA), as shown in Fig. 1. Seven main types of communications are identified and numbered as the following.

The symbol '⇔' indicates a two-way communication. The shaded area implies communication that occurs within the hospital's local network. The communication can also occur from within the hospital to the outside network. This communication is useful particularly for users who are far away.

For example, a doctor at the hospital communicates with another doctor at another hospital; a patient or SW at home communicates with a doctor at the hospital; or a paramedic at a location of an accident communicates with SC at the hospital. The paramedic and SC work together in a distributed way. The information regarding a patient is sent by the paramedic using a PDA or a smart phone and received by SC in the hospital for further action, such as preparing for a medical team while waiting for the patient to arrive at the hospital. The public can also communicate and obtain information with the hospital, through the hospital's website. For example, to get the hospital's annual reports, available services, opening hours, public announcement and information on diseases.

Table 1 describes the different types of information being exchanged during communication in the hospital and who is communicating it. There is information that is more sensitive than the other. For instance, information that came from communications between Doctors, Patient, Nurse and Paramedic is more sensitive than information that came from SW⇔Nurse communications.

Doctors discuss about the critical level of a patient's illness. A doctor discusses with a patient about his/her detailed medical information (such as diagnosis, medical history, test results, current treatment and prescriptions) in a consultation session. A nurse communicates with a doctor regarding a patient's personal information (such as name, address, age, gender, contact person, medication). The nurse also communicates with the patient, regarding his/her medication. As for SW⇔Nurse communications, only general information about a patient is involve, such as name, contact person and a ward number.

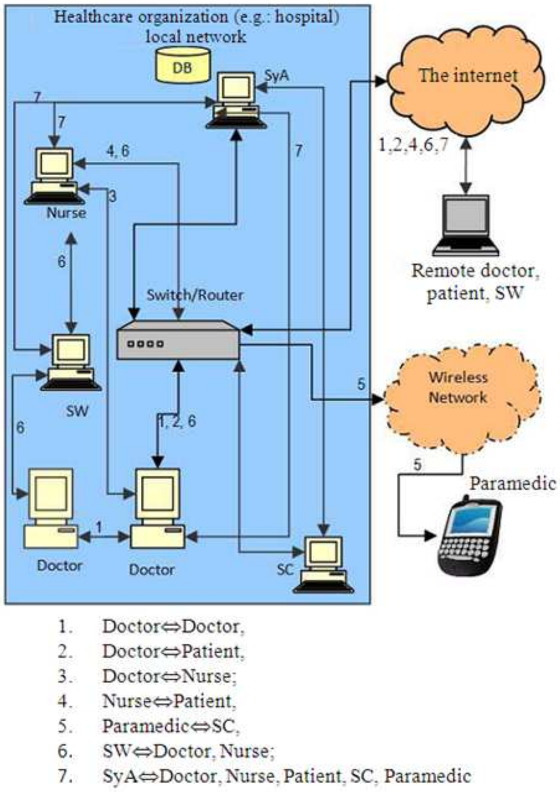

Fig.1: Different types of communications in a hospital organization

Layered approach: As we have illustrates in the previous section, there are more than one type of communications in the hospital. We could classify these communications into groups, based on the different levels of security provided to secure different levels of sensitivity of the information. The idea is comparable to the one in (IBM, 2009), to classify SSL cipher. It is based on three types of the key lengths classifications, which are HIGH, with key lengths larger than 128-bit; MEDIUM, with key lengths equal to 128-bit; and LOW, with key length smaller than 128-bit. However, this classification is limited to only three classifications, which cannot accommodate information classification such as modelled ISO17799 (2007) and SIGS (2001) described earlier.

Suppose that there are more than three types of information with different levels of sensitivity. Thus we need more than three types of communications and as a result, we need more than three types of security mechanisms. In this situation, we believed that characterizing the communications into a layered structure is the best way to cater for the security level. Therefore, based on ISO17799, we portray the security levels in a layered architecture, featured in Fig. 2.

Table 1: Different types of information exchanged between users

Communication	Types of information
Doctor⇔Doctor	Doctors communicate with each other regarding the critical level of a patient's llness and the best medication recommendation.
Doctor⇔Patient	A doctor gives consultation to a remote patient (e.g. patient at home) from hospital. Information discussed involves detailed medical information.
Doctor⇔Nurse	A nurse communicates with a doctor concerning a patient's personal information and current medical condition
Nurse⇔Patient	A nurse communicates with a patient at home concerning patient's medications.
Doctor⇔SW	A remote SW asks advise from a doctor at the hospital on a problem arises when helping a patient at home
SW⇔Nurse	A SW worker asks for patient's general information from the nurse
SW⇔Patient	A remote social worker communicates with a remote patient regarding appointmentrequest for counselling sessions
Paramedic⇔SC	A paramedic updates patient's information (such as patient's personal information, medical information: allergy, blood pressure and medical history) at a location of an accident to the database using his PDA. The information is retrieved by SC who manages the database of accident cases
SyA ⇔ All users	Concerning user accounts
Public (open channel)	With security- Any user that wants toget access or contact information to any sensitive information (e.g.: a researcher) Without security- annual reports, services available, public announcement and information on diseases

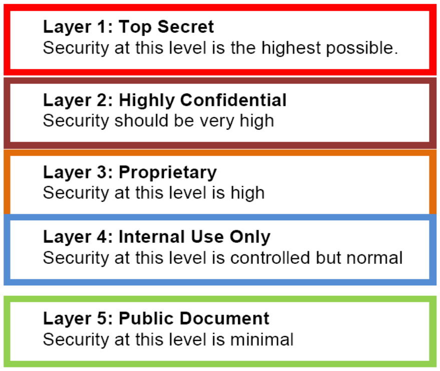
Layer 1: Top Secret
Security at this level is the highest possible.
Layer 2: Highly Confidential
Security should be very high
Layer 3: Proprietary
Security at this level is high
Layer 4: Internal Use Only
Security at this level is controlled but normal
Layer 5: Public Document
Security at this level is minimal

Fig. 2: Examples of multilayered structure

The top layer represents the most sensitive information, while the lowest layer represents the lowest sensitive information. We could adopt this characterization concept of information classification to classify online communication. Then, we can organize and apply security mechanisms with security levels appropriate to each layer. With the use of a multilayered structure it can lead to several advantages, for example modularity: security mechanisms can be captured independently based on the policy defined at every layer; and flexibility: any element of security mechanisms can be added or removed systematically when necessary, for example, we can add or remove a cipher with a certain key length to/from the layer.

Levels of sensitivity: In this section, we discuss the levels of sensitivity of the information in Table 1, which will be one step forward to establish our proposed MLC model. We examine the information and compare it with the levels of sensitivity already categorised in ISO 17799. We choose ISO 17799 as a comparison because the classification it proposed is well suited to our hospital environment. From Fig. 1, we could find that the information that is exchanged among Doctor, Patient and Nurse, includes patient's information such as patient's personal information and detailed medical information. The information can be considered as extremely sensitive (this information is considered to be equivalent to ISO17799's Top Secret.) and should not be revealed to others except for the Patients themselves, Doctors and the Nurses in charged.

Communications between Paramedic and SC can be considered as highly sensitive, as in ISO17799's Highly Confidential, because it contains information such as data collected at the site (e.g., current condition of a patient, allergy types, heart rate and blood pressure), medical history and patient's personal information. Communications between Nurse⇔SW and SW⇔Patient may result in information that fall into categories between sensitive and low sensitive, which we labelled it as medium sensitive (as in ISO17799's Proprietary), e.g.: name, contact person and ward number, appointments requests and a list of social workers that help patients either at the hospital or at home, which should be treated personal and should not be disclosed to public.

Information that falls into categories between low sensitive and no sensitive is labelled as low sensitive, as in ISO17799's Internal Use Only, like any non-medical related information, such as information about application systems or internal issues regarding the hospital. This information is still considered as internal information and should not be disclosed to public. The one that can be made public is no sensitive, as in ISO17799's Public Documents such as general information about the hospital, or general information about health, common diseases and possible treatments.

Classifying the information in the hospital: The reason why we categorize the information into its levels of sensitivity is that, from the categorization, we will construct our own security model, where we proposed suitable security mechanisms for each level of sensitivity. In the previous section, we have identified the levels of sensitivity of the information in the hospital. In our approach, we adopt the ISO 17799 standard as our basis of information classification. We have identified all entities that contribute to the hospital's information flow, either from within the organization or from the organization to the outside network (Fig. 1). We have also identified the types of information that need to be protected, such as explained in Table 1.

Now, we refer to the ISO 17799 and adopt this standard of information classification. We classify the information in e-health into five categories, together with the degree of security protection that should be applied to the information.

- Top secret: Contains extremely sensitive patient's information. The distribution of this kind of information is very restricted and must be protected all the time. Highest security protection must be applied.
- Highly confidential: Contains highly sensitive information, related to the patient's information that should not be shared internally or made public. It includes information that is obtained from mobile devices to the organization. Security should be very high and suitable for devices with limited resources.
- Proprietary: Contains medium sensitive information related to the information that is required for the operational work routines of the hospital's staff. Use by authorized personnel only. Security at this level is medium high.
- Internal use only: Contains low sensitive information, which is not approved for general circulation outside the organization. Security at this level is low.
- Public: Information that can be disclosed to public. Security at this level is minimal.

In this classification, we choose to use highest, very high, medium high, low and minimal to distinguish the degree of security or the security level provided in each categories (which is equivalent to the term used in ISO 17799, which are highest, very high, high, controlled but normal and minimal).

RESULTS

MLC-Classifying the communications: Our approach centred on how to secure communication sessions between two points, which transmit information that has different levels of sensitivity. We are interested on how to classify every communication between users in e-health, based on the levels of sensitivity of the information transmitted during the communication. By classifying the communication, we can provide flexible security mechanisms around the communication based on organizational needs. We propose the communications in e-health to be categorized into five layers, which is Layer 1 to Layer 5, based on the five classifications of information described in previous section. Table 2 shows the five types of communications in MLC. The security protection suggested in each layer is in accordance with the security provided in the ISO 17799.

Layer 1: For communication between users that exchange Top Secret information, which is extremely sensitive. The Highest protection mechanisms should be applied. The information should be protected against threats and loss and disclosed only to authorized users such as doctors, patients themselves and the nurses in charged. Any disclosure to other users must follow the patients' consent.

Table 2: Five layers of communication in MLC

Layer sensitivity	Types of data communicated	Users
Layer 1 Top secret	Contains Extremely Sensitive information: Patient's personal information and detailed medical information	Doctor⇔Doctor Doctor⇔Patient Doctor⇔Nurse Nurse⇔Patient
Layer 2 Highly Confidential	Contains Highly Sensitive information: Patient information that should not be shared internally or made public and information obtained from the paramedic at an accident spot	Paramedic⇔SC
Layer 3 Proprietary	Contains Medium sensitive information: Patient's information that is required for the operational work routines of the hospital's staff.	Doctor⇔SW Nurse⇔SW Patient⇔SW
Layer 4 Internal Use Only	Contains low sensitive information Any information that is not approved for general circulation outside the organization.	SyA ⇔ all users
Layer 5 Public	Open channel: No sensitive information such as general information on the hospital, information on health, diseases, frequently asked questions, annual reports and services available Secure open channel: any user, e.g. a researcher who wants to access or contact information to any anonymous sensitive information	The public get

Layer 2: For communication between users that exchange Highly Confidential information, which cannot be shared internally or made public. This includes information which is obtained from mobile devices to the organization. Security at this layer should be very high and suitable for devices with limited resources.

Layer 3: For communication between users that exchange Proprietary information, which is required for the operational work routines of the hospital. Security at this level is medium high.

Layer 4: For communication between users that exchange Internal Use Only information, which is related to general information about the organization's system and non-medical related information. Security at this level is low.

Layer 5: For communication between users that exchange Public information. This layer is divided into two that are with security, called secure open channel and without security, called public open channel. Security at this level is minimal. In the next section we discuss how we proposed protection mechanisms at each layer with different levels of security, by using cryptography protocols.

MLC-proposed security mechanisms: Our focus is to secure the process of message exchanges between two points, which is between a sender and a recipient in different communicating environments. Both of the users would want to make sure that the message sent or received is safe from any unauthorized access (confidentiality), not modified (integrity) and the originality of the message is guaranteed (nonrepudiation).

The sender would also want to make sure that he/she can prove that the message is from him/her (non-repudiation). The recipient would want to make sure that he/she can access the message whenever he/she needs to (availability).

The MLC is taking into account of providing flexible security protections in order to address security needs in e-health. The MLC provides three types of security mechanisms, which are data security, channel security, as well as data and channel security. Data security uses cryptography protocols such as symmetric encryption/decryption, hash function and digital signature, while channel security uses the SSL protocol. We discuss each of the MLC's security mechanisms in details in the following sections.

Mechanism1-data security: A sender wants to send a plaintext to a recipient. Both of them need cryptography protocols to secure (and recover) the plaintext. The following describes the notations used in the cryptography processes:

- Public and Private keys of the recipient (pubKr, privKr)
- Public and Private keys of the sender: (pubKs, privKs)
- Symmetric keys K;
- Plaintext, P, Hash of Plaintext, H(P)
- Digital signature, S

In our approach, we use the symmetric key encryption, hash function and digital signature to provide data security. The following describes the step-by-step process at the sender's and recipient's sides:

Cryptography Protocol at the sender side:

- Symmetric encryption: encrypts the plaintext into ciphertext using a key K. The encryption process ensures the confidentiality of the plaintext:

$$\text{Ciphertext} = E\ (P)K$$

- Hash function: Computes hash value from the plaintext, H(P). The hash value will be used by the recipient to check the integrity of the plaintext and verify whether the plaintext is tampered or not. The recipient recalculates the hash value from the plaintext retrieved from the ciphertext and compares it to the one sent by the sender. If both are matched, then the plaintext is genuine and the integrity of the plaintext is verified.
- Key exchange: The key K, should be encrypted and sent to the recipient, so that K can be used to decrypt the message at the recipient's side. In order for the sender to make sure only the recipient can recover the key, K will be encrypted with the recipient's public key, pubKr. To avoid a third party to steal and remove H(P) that is computed earlier, it can be encrypted together with K using pubKr and we name the result of the encryption as:

$$\text{Cipherkey} = E\ (K, H(P))\ \text{pubKr}$$

- Digital signature**:** In order for the sender to prove that the Cipherkey is from him/her, the sender signs it using his/her private key (privKs) to produce signature S. S = E(Cipherkey)privKs

- Send message: Afterwards, the sender can send Ciphertext, Cipherkey and S to the recipient. HTTP protocol is used to transfer message for the wired network, so that SSL can be used to secure the channel. For the wireless network, we use the Global System for Mobile communications (GSM) network, or wireless LAN (WiFi) to transfer the message.

Cryptography Protocol at the recipient side:

- To check that cipherkey is indeed come from the sender, S is verified against Cipherkey
- If Cipherkey is valid, then the following is executed
- use privKr to decrypt Cipherkey: D(Cipherkey) privKr = K, H(P)
- Then, use K to decrypt Ciphertex: D(Ciphertext)K = P
- Finally, verifies P by calculating a new H(P) from P and compare it with the one in (a). If proved valid, keep P.

Mechanism2-Channel security: In the channel security, the sender and recipient exchanges certificates and then the sender establishes SSL channel to the recipient side and simply transfer the plaintext. Certificates can be obtained through the Security Administrator in an organization, which is in charged with creating identification (Id) and a password for user accounts.

Mechanism3-Both data and channel security: When using option of both data and channel security, Sender sends all Ciphertext, Cipherkey and Signature S to the recipient through the SSL channel.

The Key size for the symmetric key encryption: The key K is an important component of an encryption process because it represents the level of security that the algorithm can provide. According to Bidgoli (2004), a symmetric cryptography system with n-bit of keys has a security level of n, if it can endure a generic attack (to find the key, when plaintext and ciphertext are known beforehand), using efforts less than the exhaustive search or 'bruteforce' attack. The selection of the key size is based on the level of security required for a cryptography system. The longer the key, the higher the security it can provide because the difficulty of trying all possible keys in the exhaustive search is directly proportional to the number of bits used (Blaze *et al*., 1996). This answers why shorter key sizes can only provide low security as it will take less time to find the key using the exhaustive search, compared to longer key sizes.

The US government policy provides recommendations on the symmetric key sizes to protect classified information namely Top Secret, Secret and Confidential information (CNSS, 2003). The Advanced Encryption Standard or AES algorithm is chosen for this purpose. AES-192 bit or AES-256 bit is chosen to secure the Top Secret information, while AES-128 bit is chosen to secure both Secret and Confidential information.

Debates on selecting symmetric key sizes for a cryptography system has been and still going on. It is important to make sure that the key size chosen for a cryptography system is proven to be strong. There are many efforts to find flaws in the key size for certain algorithms mainly using brute-force. Brute-fore attacks can be achieved by computing in parallel that is, one can easily add as many processors as desired to perform partial search of the key.

Many suggestions have been made regarding the selection of the symmetric key sizes selection. ECRYPT (2008) argued that different information has different lifespan and a key size selected to protect a particular information should be larger than the lifespan of the information. For examples, electronic banking transactions have brief security protection and private information like medical information needs protection for a lifetime of a patient.

In the late 1995, Blaze *et al*. (1996) made an adhoc report regarding the minimum symmetric key sizes required for commercial security. The report was made to discuss a solution and address the problem of inadequacy of the confidentiality protection provided by the existing key sizes. They reported that a symmetric cipher with 40-bit key does not provide any protection against brute force attack and added that the 56-bit of DES is considered inadequate, although Bidgoli (2004) argued that there was not any attack that could break DES with security level of 56, except for the exhaustive search of the key. Blaze *et al*. (1996) suggested that 75-bit key was adequate in the late 1995 based on the available equipments and time needed to find 40-bits and 56-bits keys at that time. They then proposed that 90-bit key was the minimum key size required to provide security for the next 20 years (from late 1995). ECRYPT (2008) supported Blaze *et al*. (1996)'s report and claimed that the method is still reasonable to be exercised. Bidgoli (2004) came out with a formal formulation on how to determine key sizes for symmetric key with the lifespan of the key. This formulation was an updated version of his works in 2000.

Bidgoli's work was based on the DES 56-bit key, which was first introduced in 1977. DES was first being reviewed in the year of 1982. He suggested that DES has provided adequate protection in the year of 1982. Based on this, he studied the next security level required in proportion with years. He referred to the Moore's Law which was formulated in 1965 (Fibikova and Vyskoc, 2001; Lenstra and Verheul, 2000) stating that the amount of computing power and random access memory one gets, doubles every 18 months. He then suggested that the security level should also be increased by one for every 18 months, starting from year 1982. For example, a cryptography system should use 66-bit (56-bit+10) in 10 period of 18 months (which is equivalent to 15 years) and therefore should give adequate protection in 1997 (which is obtained from 1982+15).

Bidgoli (2004) introduced a formula to find the adequate key size, K in year Y:

$$K = 56+2\ (Y-1982)/3 \qquad (1)$$

For example, in 20 years time from 2009, (which is 2029) the adequate key size is K = 56 + 2 (2029-1982) / 3 = 87, in other word, 87-bit keys should be used until the year of 2029 to provide adequate protection. We can also find Y, if given the key size K by:

$$Y = 1982+3\ (K-56)/2 \qquad (2)$$

Based on (Blaze *et al*., 1996) and (Bidgoli, 2004) works, ECRYPT (2008) recommended key sizes with the lifespan of the key, shown in the Table 3. ECRYPT (2008) reported that 80-bit key is suitable for a very short term protection against a brute-force attack and added that if an attacker is able to pre-compute the data, the 80-bit key is breakable. The report also stated that the 32 and 64-bit keys are not suitable for confidentiality protection because the 32-bit key does not offer any protection, while the 64-bit key offers very poor protection.

We calculate the lifespan for each key length using Bidgoli (2004) formulation in (2) shown in Table 4 in the last column. We compare the duration of protection given by (Bidgoli, 2004) with (Blaze *et al*., 1996), (ECRYPT, 2008) and the US Policy (CNSS, 2003). Although there is a huge gap of lifespan between ECRYPT and Lenstra formulations, we can summarize that both recommendations, as well as the US policy suggest:

- 256-bit key and 192-bit key provide highest security for a very long term protection
- 128-bit provides medium high security for a long term protection
- 112-bit provides medium security for a medium term protection and
- key bits from 80-bit provides low security for a short term protection

From the summary, we recommend the symmetric key sizes value for every player in the MLC model is provided in ranges like the following:

- 193-bit and longer: Suitable for Layer 1, to secure the Top Secret information that needs the highest security protection
- 129-bit to 192-bit: Suitable for Layer 2, to secure the Highly Confidential information that needs a very high security protection
- 112-bit to 128-bit: Suitable for Layer 3, to secure the Proprietary information that needs a medium high security protection
- 80-bit to 111-bit: Suitable for Layer 4, to secure the Internal Use Only information that needs a low security protection

Table 5 describes the recommended key sizes in each layer in MLC. The US Policy recommendation is also included for comparison purposes. The table shows that Layer 1 and Layer 2 key sizes are aligned with the US' Top Secret key sizes (192- bit for Layer 2, 193-bit and longer for Layer 1). Layer 2 supports mobile devices security and therefore, key length as low as 112-bit is supported for low processing power device. For Layer 3, we choose 112 to 128-bit key to provide medium security, which also aligned with US's Secret key sizes. For Layer 4, key sized from 80-bits to 111-bit are chosen to provide low security. By providing key length values in certain ranges, we can offer a wider range of key sizes for each layer. In summary, we conclude the security mechanism in the MLC model, which includes data and channel security as depicted in Table 6.

For channel security, cipher suites from any available provider can be used to provide protection. Table 7 provide examples of cipher suites from SunX509. Because of the limitation of the available cipher suite provided from the SSL providers, (which only provides Layer 1 with 256-bit and Layer 2 with 168/128-bit protection), we could use 128-bit cipher suites as alternatives for Layer 3 and Layer 4 as well.

Table 3: Security levels excerpt from Table 7.4 from ECRYPT (2008)

Security (bits)	Protections	Comment
80	Very short-term protection against agencies, long term protection against small organizations	≤ 4 years protection
96	Legacy standard Level	≈ 10 years protection
112	Medium-term protection	≈ 20 year protection
128	Long-term protection	≈ 30 years protections
256	Foreseeable future”	Good protection against quantum computers (Shor, 1997)

Table 4: The existing key size recommendations

Recommended key size (in bit)	Blaze	ECRYPT	US Policy	Lifespanl
75	Adequate until late 1995			≈3 years
80		≤ 4years		≈ 10years
90	Adequate until 2015 ≈ 20 years			≈ 25 years
96		≈ 10years		≈ 34years
112		≈ 20 years		≈ 58years
128		≈ 30 years	Confidential and Secret	≈ 82 years
192			Top Secret	≈ 178years
256		Foreseeab le future	Top Secret	≈ 274years

Table 5: Key size recommendation for each layer in MLC

US policy	Keylengths (in bit)	MLC	Key lengths (in bit)
Top Secret	192/256	Layer 1 (Top secret)	193 and longer
Secret	128	Layer 2 (Highly Confidential)	Wired: 129-192 Lightweight devices: 112-192
Confidentia l	128	Layer 3 (Propriety)	112-128
		Layer 4 (Internal use only)	80

Table 6: The security specifications in MLC model

Layers	Security mechanisms	Key lengths (in bit) for data security
Layer 1 (Top Secret) 193 and longer	Data and channel security	
Layer 2 (Highly Confidential)	Data or channel security *mobile devices use data security only	Wired: 129-192 Wireless:112-192
Layer 3(Propriety)	Data or channel security	112-128
Layer 4 (Internal Use Only)	Data or channel security	80-111
Layer 5 (Public)	-	ID and Password (for secure open channel)

Table 7: Cipher suites provided by SunX509 provide

256-bit	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
168-bit	SSL_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
128-bit	SSL_RSA_WITH_RC4_128_MD5, SSL_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA

For Layer 1, data and channel security are used to provide the highest protection mechanism. The key lengths for data encryption are from 193-bit and above. Layer 2 uses data or channel security only. For data security, 129-bit to 192-bit of keys are used with the wired network, while 112-bit to 192-bit of keys are chosen for the wireless network. Layer 3 and Layer 4 also provide two options either data or channel security, with key lengths of 112 to 128-bit and 80 to 111-bit respectively. For Layer 5 that is intended for public use, we could use ID and password only, to support secure open channel.

DISCUSSION

MLC Model-Justifications and Advantages: In e-ehalth, different users communicate different types of information. There is sensitive information that has to be kept confidential and there is also information that can be shared with public. Remote users such as patients can now use the Internet to communicate with their doctors and nurses from home and be part of e-health users. The MLC model provides security mechanisms to secure different types of communications among different users in ehealth according to their needs. For example, a nurse can communicate through a communication, which is secure or less secure depending on the situation. The nurse can communicate through the highest level of security when communicating with doctors or patients. Alternatively, he/she can use a medium level of security when communicating with SWs, or a minimum level of security when communicating with SA.

By using different combinations of key sizes for data and channel security, flexibile security can be provided to the health organizations. Different security strengths can be provided at each layer depending on the sensitivity of the data. The extremely sensitive information can be secured using the highest security mechanisms, while low sensitive information can be secured with minimal security mechanisms. Therefore, any excess security applied on the communication can be avoided when it is not needed. MLC satisfies the current technologies gaps and limitations, where users are now able to communicate with different types of security mechanisms suitable for their needs.

A set of encryption algorithms that are proven to be reliable by experts can be chosen to secure the layers. The selection of the algorithms can be made or decided by the Security Administrator in the organization. In MLC, there are data and channel security provided to users in such a way that the user can choose the most suitable security processes in terms of cost and efficiency. For example, the organization can choose SSL channel for the communication, which is cheaper than the data encryption, however, with a trade-off of inflexible security configuration when the user needs to change to stronger or weaker security level. Alternatively, the organization can choose to use data security only, with suitable encryption key sizes, described in Table 6. Meanwhile, when especially excess security is needed for an extremely important communication, the organization can opt for data and channel security.

In addition, communication with low processing power devices like PDAs and smart phones are provided with appropriate data security with key sizes available from 112-bit. The organization can save resources such as CPU processing power for the lightweight devices using appropriate key lengths to give better performance to the communication.

However, there is always a trade-off between strong security and performance. The longer the key lengths, the slower the performance of the security processes. Longer key length provides better security because more works and efforts are required by the attackers to find the key. Therefore, if security is important, stronger algorithms are selected with decreasing performance. Otherwise shorter key lengths with high performance can be chosen according.

CONCLUSION

From the study, we learned that current security technologies cannot cater for different kind of security needs because of the rigid way the security mechanisms are constructed. The security level or security strength in the current technologies can only be set to one particular value for all communications sessions. As a consequence, the need for a stronger or a weaker security level in different communications cannot be satisfied, without having to reconfigure the whole communication process. In other words, current security technologies did not support automatic and flexible security for different communications.

We addressed the problem by first, identifying the users and the types of communications that occurred in e-health. Then we identified the different types of information in e-health and the different levels of sensitivity of the information. We classified the information into five categories based on ISO17799 standards, which was according to the sensitivity levels. Secondly, from the classification of the information, we then categorized the communications in e-health into five categories (which we call layers later on), so that we could provide appropriate security mechanisms for each layer of the communication. Lastly, we introduced our MLC model based on five layers of communications. MLC provides two types of security mechanisms, which are data and/or channel security for wired and wireless devices, with a range of security strengths provided through the symmetric encryptions.

REFERENCES

Ahmad, Z., 2003. Wireless security in health care. Proceedings of the First Australian Undergraduate Students’ Computing Conference (AUSCC’03), The University of South Australia, pp: 1-6

Bidgoli, H., 2004. The Internet Encyclopedia. 1st Edn., John Wiley and Sons, Hoboken, N.J., ISBN: 047122202X, pp: 880.

Blaze, M., W. Diffie, R. Rivest, B. Schneier and T. Shimomura. 1996. Minimal key lengths for symmetric ciphers to provide adequate commercial security. DTIC.

CNSS, 2003. CNSS Policy no. 15, fact sheet no.1 national policy on the use of the aes to 13 protect national security systems and national security information. National Security Agency, Systems Security for the 21st Century.

E Health News. eu, 2011. Telemedicine Opportunities and developments in Member States. E Health News. Eu.

Economic-Expert, 2009. Classified information. Economic Expert.

ECRYPT, 2008. Yearly report on algorithms and keysizes (2007-2008). Katholieke Universiteit Leuven.

Elkhodr, M., S. Shahrestani and H. Cheung, 2011. Ubiquitous health monitoring systems: Addressing security concerns. J. Comput. Sci., 7: 1465-1473. DOI: 10.3844/jcssp.2011.1465.1473

EO12958, 1995. Classified national security information. Federal Register.

Fibikova, L. and J. Vyskoc, 2001. Practical cryptography-the key size problem: PGP after years. Microsoft Academic Search.

Garcia-Morchon, O., T. Falck, T. Heer and K. Wehrle, 2009. Security for pervasive healthcare. Proceedings of the 6th Annual International Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous, July 13-16, IEEE Xplore Press, Toronto, ON, pp: 1-2. DOI: 10.4108/ICST.MOBIQUITOUS2009.6962

Georgia Tech, 2008. Emerging Cyber Threats Report for 2009. SMAR Tech.

Gupta, V. and S. Gupta, 2001. KSSL: experiments in wireless internet security TR-2001-103. Tech. Report. http://dl.acm.org/citation.cfm?id=1669853

IBM, 2009. A security scan tool returns "SSL server support weak encryption vulnerability". Technote (FAQ).

ISO17799, 2007. Creating information classification criteria. ISO17799 News.

Jaizanuar, 2009. Securing Wireless Network.

Jinyuan, S., Z. Xiaoyan, Z. Chi and F. Yuguang, 2011. HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare. Proceeding of the 31st International Conference on Distributed Computing Systems (ICDCS), June 20-24, IEEE Xplore Press, Minneapolis, MN, USA, pp: 373-382. DOI: 10.1109/ICDCS.2011.83

Kay, M., J. Santos and M. Takane, 2011. mHealth: New horizons for health through mobile technologies. World Health Organization.

Krawczyk, H., M. Bellare and R. Canetti, 1997. HMAC: Keyed-hashing for message authentication. Network Working Group.

Lenstra, A.K. and E.R. Verheul, 2000. Selecting cryptographic key sizes. Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptography: Public Key Cryptography, (PKC 2000), Springer-Verlag London, UK, pp: 446-465.

Markovic, M., 2006. On secure e-health systems. Lecture Notes Comput. Sci., 4302: 360-374. DOI: 10.1007/11930242_30

Marti, R., J. Delgado and X. Perramon, 2004. Network and application security in mobile e-health applications. Lecture Notes Comput. Sci., 3090: 995-1004. DOI: 10.1007/978-3-540-25978-7_100

Pfleeger, C.P. and S.L. Pfleeger, 2003. Security in Computing. 3rd Edn., Prentice Hall Professional, Upper Saddle River, N.J., ISBN: 0130355488, pp: 746.

SIGS, 2001. Security in the Government Sector.

Sulaiman, R., D. Sharma, W. Ma and D. Tran, 2007. A Multi-agent security framework for e-health services. Knowledge Intell. Inf. Eng. Syst., 4693: 547-554. DOI: 10.1007/978-3-540-74827-4_69

Symantec Corp, 2010. Internet security threat report. Symantec.

Ulieru, M. and D. Ionescu, 2004. Privacy and security shield for health information systems (e-Health). Proceedings of the 35th Annual Hawaii International Conference on System Sciences, Jun. 7-10, IEEE Xplore Press, USA., DOI: 10.1109/HICSS.2002.994126

Yu, W.D., R. Gummadikayala and S. Mudumbi, 2008. A web-based wireless mobile system design of security and privacy framework for u-Healthcare. Proceedings of the 10th International Conference on e-health Networking, Applications and Services, July 7-9, IEEE Xplore Press, Singapore, pp: 96-101. DOI: 10.1109/HEALTH.2008.4600118

Zhang, R. and L. Liu, 2010. Security models and requirements for healthcare application clouds. Proceedings of the IEEE 3rd International Conference on Cloud Computing (CLOUD), July 5-10, IEEE Xplore Press, Miami, FL, pp: 268-275. DOI: 10.1109/CLOUD.2010.62