
June 2012

Investigating Security Options for StudentDevelop.com and the Testing of SSL

Jude Bahanag Nunga & Okeke Godwin
Investigating Security Options for StudentDevelop.com and the Testing of SSL

Preface
Ever since the introduction of the Internet application, it has changed the way people communicate and interact to each other. With the Internet becoming more complex in its features and the services, this has led to constant evolution of threats and security flaws.

The internet standard documents RFC (request for comments) defines protocols such as TCP, IP, HTTP and SMTP. These standard internet protocols are developed by the Internet Engineering Task Force (IETF) [IETF 2007] to set guidelines on how the internet should be implemented.

There are also some set of rules such as the internet Application Programming Interface. These rules govern the way software piece should follow and also facilitates internet delivering of data to another software piece usually at the destination.

The Internet has two significant important protocols which are jointly known as TCP/IP:

- TCP (Transport Control protocol)
- IP (Internet protocol)

JUDE BAHANAG NUNGA and OKEKE GODWIN
Halmstad University,
June 2012
Investigating Security Options for StudentDevelop.com and the Testing of SSL

Acknowledgment

Special thanks and appreciation goes to you Nicolina Månsson, our program director. Your guidance and feedbacks during this thesis project has been of great value to us.

We thank you Malin Bornhager, our thesis supervisor. Your supervision and recommendations during this entire thesis project is among those great supports we have received from you over the years.

Thank you Ludvig Granberg for your technical advice to our respective questions related to the StudentDevelop platform.

As this thesis mark the end of our studies at the undergraduate level, our acknowledgement and “thank you” goes to the entire IDE department at Halmstad University.

Thank you Andrey Prokhorov for your help during the programming of the StudentDevelop web portal. Your valued contribution at the beginning helped to pave the road map for Jude Nunga to carry on with the development of the portal to this current stage.

By moving one step closer into our prospective careers and joining the corporate world, we would also like to say thank you to every lecturer and staff at the university who have contributed in one way or the other during our study years.

We also acknowledge the support and words of encouragements from our respective family and friends, it is thanks to both these encouragements and academic support from the University which has lead us this far in completing our Bachelor’s degree majoring in Computer communication.
Investigating Security Options for StudentDevelop.com and the Testing of SSL

Abstract

Security issues have become a key problem with most e-commerce platforms these days and information sent over the internet needs to be protected. When operating an e-commerce platform such as studentdevelop.com financial transactions are involved. Data communication is very vital to e-commerce and needs to be processed securely.

This thesis shall investigate Secure Socket Layer (SSL) as a possible solution to provide added security such as data integrity and confidentiality on the StudentDevelop.com web portal. This thesis shall also compare other known security suites available for use which could suit the StudentDevelop.com web platform. A vivid comparison shall be carried out to evaluate SSL and Pretty Good Privacy (PGP) with the aim of testing the preferred choice to provide encryption and data confidentiality on the StudentDevelop.com platform.

Protocols like SSL make up the next layers of mechanisms that support applications with electronic payment schemes. Cryptography being an essential security technology involving the encryption algorithm and digital signatures can provide the basic building blocks. SSL shall be tested on the StudentDevelop.com platform by installing a self-signed certificate, including a test of a digital certificate obtained from a certificate authority. In SSL, the web browser is the client and the web-site server is the server.

As a result to authenticate consumers on e-commerce platform such as studentdevelop.com, SSL increased the security for web transactions by using public-key encryption and digital certificate to achieve authentication. Encryption algorithm and digital signatures provided the basic building blocks, while SSL protocol made up the next layer of mechanisms that in return support the application layer. In the fourth coming sub chapters, we will look in to the problem description of this thesis and the investigation of security solutions for studentdevelop.com.
# Table of Contents

Preface........................................................................................................................................... 2  
Acknowledgment.......................................................................................................................... 3  
Abstract.......................................................................................................................................... 4  
Appendix.......................................................................................................................................... 7  
1  Introduction.................................................................................................................................... 8  
   1.1  Motivation and Goals ................................................................................................................ 8  
   1.2  Problem Description ................................................................................................................... 8  
   1.3  Methodology ................................................................................................................................ 8  
2  Web service technologies .............................................................................................................. 9  
   2.1  Web Development ....................................................................................................................... 10  
   2.2  Protocols and the internet ........................................................................................................... 10  
      2.2.1  The internet has three core areas ......................................................................................... 10  
   2.3  Internetworking within protocols ............................................................................................... 11  
   2.4  Elements of protocols ................................................................................................................ 11  
   2.5  The Internet Protocol Stack (IPS) ............................................................................................. 12  
   2.6  Hypertext Transfer Protocol (HTTP) ........................................................................................ 13  
      2.6.1  Uniform resource locator (URL) ........................................................................................ 13  
   2.7  File Transfer Protocol (FTP) ...................................................................................................... 14  
      2.7.1  File Transfer Protocol security threats ................................................................................. 15  
   2.7.2  Simple Mail Transfer Protocol (SMTP) ................................................................................. 15  
3  Security management .................................................................................................................... 15  
   3.1  Problems with security management ......................................................................................... 15  
   3.2  Information security ................................................................................................................... 17  
      3.2.1  Information management ..................................................................................................... 17  
4  Overview of some security infrastructures (SSL, PGP and IPSec) .............................................. 18  
   4.1  Secure Socket Layers (SSL) ..................................................................................................... 18  
      4.1.1  Secure Socket Layers Basics ............................................................................................. 18  
   4.2  Pretty Good Privacy (PGP) ........................................................................................................ 19  
      4.2.1  PGP features and their terminologies ................................................................................ 19  
      4.2.2  PGP Desktop files ............................................................................................................... 20  
   4.3  Internet Protocol Security (IPSec) ............................................................................................ 21  
      4.3.1  Comparison of some security suites .................................................................................... 22  
5  Email security ............................................................................................................................... 23
Investigating Security Options for StudentDevelop.com and the Testing of SSL

5.1 Messaging system for the StudentDevelop web portal ...........................................- 23-
5.2 Email server measuring respond time for mail server ...........................................- 24-
6 Implementation of security layer on studentdevelop.com ........................................- 24-
   6.1 Public-key infrastructure ...................................................................................- 25-
   6.2 Testing of SSL .................................................................................................- 25-
   6.3 Self-signed certificate .......................................................................................- 25-
   6.4 Deploying SSL termination devices (ISS 5.0) ...............................................- 29-
   6.5 How Secure Socket Layers works ....................................................................- 30-
7 Result .....................................................................................................................- 31-
   7.1 Result on self-signed certificate scenario .......................................................- 31-
      7.1.1 Testing SSL certificate on a local host .....................................................- 32-
   7.2 Trial certificate from a certificate authority .....................................................- 33-
8 Conclusion .............................................................................................................- 35-
   8.1 Email delay problem conclusion ......................................................................- 35-
References ..............................................................................................................- 37-
Appendix

CA  CERTIFICATION AUTHORITY
DHCP  DYNAMIC HOST CONFIGURATION PROTOCOL
FTP  FILE TRANSFER PROTOCOL
HTML  HYPERTEX Markup LANGUAGE
HTTP  HYPertext Transmission PROTOCOL
HTTPS  SECURED HYPERTEXT TRANSMISSION PROTOCOL
IP  INTERNET PROTOCOL
IPSEC  INTERNET PROTOCOL SECURITY
LAN  LOCAL AREA NETWORK
MAC  MEDIA ACCESS CONTROL
MYSQL  MY STRUCTURED QUERY LANGUAGE
MIME  MULTIPURPOSE INTERNET MAIL EXTENSIONS
PHP  PHP: HYPERTEXT PREPROCESSOR
RFC  REQUEST FOR COMMENTS
SET  SECURE ELECTRONIC TRANSFER
SMTP  SIMPLE MAIL TRANSFER PROTOCOL
SNMP  SIMPLE NETWORK MANAGEMENT PROTOCOL
SSH  SECURE SHELL
SSL  SECURE SOCKET LAYER
TCP  TRANSMISSION CONTROL PROTOCOL
TCP/IP  TRANSMISSION CONTROL /INTERNET PROTOCOL
TLS  TRANSPORT LAYER SECURITY
URL  UNIFORM RESOURCE LOCATOR
VPN  VIRTUAL PRIVATE NETWORK
Investigating Security Options for StudentDevelop.com and the Testing of SSL

1 Introduction

StudentDevelop.com is an e-commerce portal offering a suite of online tools and services that facilitates the communication and collaboration between universities, its students, and their partner companies. Developed by Jude Nunga with the aim of promoting entrepreneurship on its virtual incubator, the portal also allows students to upload and showcase their educational and commercial projects on the web. All commercial transactions will take place via the payment gateway. The portal’s collaborative tools serve as a bridge which facilitates students to add value to their resumes by working on class projects and closed commercial projects proposed by employers. By using these web services, students can get real work and valued years of experience in their specialties.

Most web applications originate from different vendors and when patched together on web systems like the WEB 2.0, they can function greatly. Even though different web applications can be put together on WEB 2.0 systems, they are usually updated separately at the respective vendors. This can be risky as it exposes the web system to security threats because the entire system does not undergo a joint system update at once. As new technologies are developed to replace older versions; security flaws in most of these technologies are detected and need to be prevented. Web construction is not deemed complete just by applying a set of rules that governs the way software piece should follow.

The protocol for payment-card transactions developed by Visa and MasterCard is SET (secure electronic transfer). Implementing a payment gateway alone on a web portal, such as studentdevelop.com, does not guarantee the portal to be secured enough to carry out financial transactions. This way, a users’ private data processed over the internet can be stolen. The self-signed SSL certificates for testing purposes are created on the IIS Server. They are useful in environments where it is not important for end users to trust your server, such as a test environment. However, ensuring security, data communication, authentication and reliability must be considered. This thesis has motivations and goals to solve some existing problems faced on studentdevelop.com which are explained at the subsequent sections.

1.1 Motivation and Goals

This thesis motivation and goal is to investigate the security options for securing studentdevelop.com and the testing of Secure Socket Layers (SSL) on its server.

As the StudentDevelop.com portal will be processing its users’ confidential data such as credit cards over the internet, client trust needs to be maintained. Implementing authentication and encryption mechanism can protect personal information over the internet.

With the use of SSL, this can increase the level of security on the web portal by providing confidentiality, message integrity and server authentication to users.

1.2 Problem Description

With e-commerce platform such as studentdevelop.com, the problem of unsecured connections which can lead to the exposure of consumers confidential data will be investigated. Besides suggesting a secure solution for processing or hiding confidential data such as credit details online, winning consumers trust and providing assurance on the portal is another problem that needs attention. This thesis will investigate the different possible security suites available for
securing e-commerce websites and select the best option for securing the StudentDevelop.com platform.

This thesis will also look into another problem faced by studentdevelop.com which involves the delay of messages sent from within the portal. Communication delay (email messaging) will be investigated to verify why it currently takes between 5 to 30 minutes for messages sent from the web portal to arrive at its destinations (usually at the external private email inbox of the receiver).

Currently the platform does not have a payment system nor can the portal guarantee a secured environment for financial transactions. When these security problems have been solved, consumers on the platform will either need to subscribe for one of the service packages offered or purchase commercial projects sold on the platform.

1.3 Methodology

The solution approach will be the implementation of Secure Sockets Layer (SSL) using Microsoft Internet Information Service (IIS 5.0 and 7.0). We will describe how SSL encryption allows users to access files, webpages, send and receive emails. We shall also test the encryption of messages and emails using PGP.

When planning the security features for an e-commerce platform, it is important for you to take into consideration your organization goals and set out policies for security management. Later in this report, we have described best practices for information security and management.

2 Web service technologies

![Web services interaction](image-url)
2.1 Web Development

PHP: Hypertext Preprocessor (PHP) is the script language used during the development cycle of studentdevelop.com. It provides the flexibility to control the web server.

As the Secure Socket Layer (SSL) ensures secure connection between the TCP and IP layers, this will not affect the use of Microsoft Internet Information Service (IIS 5.0 and 7.0) to test on confidentiality and user authentication on studentdevelop.com.

My Structured Query Language (MySQL) is used as the database system for this web portal. A database is needed for storage and to serve requested data to the browser. For this portal to provide dynamic web pages on the internet, a combination of database (MySQL), PHP code and Linux operating systems have been used.

By Hypertext Markup Language (HTML) residing inside PHP files, this makes it possible to add user details to a database, process credit card and retrieve information. Web pages were created in a programming language called HTML and, by using the World Wide Web (web), it provides access to web pages.

JavaScript is used to offer access to functions and objects. The File Transfer Protocol (FTP) program such as FireFTP is used to transfer files to and from the StudentDevelop.com web server. The Editra text editor program was the ideal editor selected for use because it highlights the syntax appropriately and it also understands HTML.

Different web browsers such as Internet Explorer, Mozilla Firefox, and Google Chrome are used for testing the web pages to make sure the pages can be accessible by different users no matter what web browsers they are using to access the web pages.

Since the web is made up of internet service (as seen in Fig 2-1) which provides access to web pages, a combination of technologies such as the internet and the web has revolutionized traditional commerce to expand on to this new infrastructure facilitating the operability of the StudentDevelop.com portal.

2.2 Protocols and the internet

2.2.1 The internet has three core areas
They include;

- Packet Switching,
- The TCP/IP communications protocol,
- Client/Server computing

James F Kurose and Keith W. Ross (2008, p. 35) defines a protocol as “ A protocol defines the format and the order of messages exchanged between two or more communication entities, as well as the actions taken on the transmission and/or receipt of a message or other event ” [1].
Michael P. Papazoglou (2008, page 57) has associated several applications and their corresponding port numbers: [2]

“Telnet corresponds to port 23
File Transfer Protocol (FTP) corresponds to port 21
Simple Mail Transfer Protocol (SMTP) corresponds to port 25
Hypertext Transfer Protocol (HTTP) corresponds to port 80
Network News Transfer protocol (NNTP) corresponds to port 119”

**Some Important port numbers as used on studentdevelop.com**
Web server is identified by port 80,
Mail server process (using SMTP protocol) is identified by port 25.

Clients and servers are end systems that run applications such as the web server and web browser programs, connecting these programs to the internet. The TCP/IP protocol is in-charge of data communication by specifying how data should be formatted, addressed and routed to ensure messages are delivered.

Among the three core concepts of the internet, we shall give some brief explanation of the most important aspect of the TCP/IP protocol and also identify their four layers. Basic knowledge of the TCP/IP protocols is vital to understand as this will give a clear picture of its connection with SSL on studentdevelop.com.

### 2.3 Internetworking within protocols (19)
Major protocol depends on other protocols in order to be able to perform fully. For example, mail servers like SMTP depends on TCP to carry out its functions, while TCP also depends on internet protocol (IP). Http depends on both Multipurpose Internet Mail Extensions (mime) and TCP.

File transfer protocol (FTP) uses the network virtual terminals from telnet to define communication on its connection and TCP to form a complete form of data communication. The internet protocol (IP) has a direct dependency on some hardware layers because it needs the hardware access or links of routers and switch to operate.

Internet protocols depend on BOOTP/DHCP just like many other protocols do depend on domain naming server (DNS) because its software implementation requires a name binding.

Complex communication data systems do not use single protocols to handle all transmission tasks. Instead they require some set of cooperative protocols which is just like the protocol suite. Sending messages from an application program on a computer to another application on another computer means transferring messages down through successive layers of protocols.

### 2.4 Elements of protocols
**Syntax:** This is a structure or format of data that shows how data are shared among end systems which are communicating between the sender and receiver.

**Semantics:** This outlines the mode of operation of data during transit. By deciding if data can be passed on to another system, including how a system defines where the information goes and whether the receiving system understand what it is getting.
Timing: This deal with calculating the time it would take to transmit a data and what size will be enough at a time without overloading the system. It also notes how fast a system can process data.

The internet standards consider protocols such as the Internet Protocol (IP) and Transmission Control protocol (TCP) as its two most important protocols. By combining protocols that operate at different layers, this will result to a group of protocols known as protocol stack.

2.5 The Internet Protocol Stack (IPS)

The internet protocol stack (as seen on Fig 2.5-1) is comprised of five layers which include; Application Layer, Transport layer, Network Layer, Link Layer, and Physical Layer.

![Internet Protocol Stack][2]

**Application layer** is in charge of protocols such as the HTTP, SMTP, and FTP. Together with network applications, all these protocols reside inside an application layer.

**Transport Layer** facilitates the transfer of data between end systems (client and server applications). Usually between the end systems, a connection must be established before data is processed. The internet uses two transport protocols known as (TCP and UDP).

TCP provides a connection-oriented service, while UDP provides a connectionless service.

To justify why TCP is used on most internet applications is due to the differences it has with UDP. TCP provides reliability with data delivery and congestion control. It is best known for its efficiency as it does not require wait times for segment acknowledgments before sending another data, thus making it commonly used by most internet applications such as FTP and HTTP.
Network Layer of the internet has several routing protocols making it a network of networks, while the internet includes an IP protocol that binds the internet together. IP protocol provides routing functions, whereas the internet components together with network layer must run the IP protocol which then routes data from one host to another.

Data link layer provides an interface to connect to network hardware and it also has several protocols such as Ethernet, WiFi and Point-to-Point protocol (PPP). Data link layer provides different services based on the link-layer protocol, thus prompting the network layer to receive different services from every data link-layer protocols.

Physical Layer involves moving individual bits within a frame across a link in a different way depending on the links transmission medium.

There are some other network functions involving translating words to network address in bits, thus translating domain names using specific application-layer protocol such as Domain Name System (DNS). Usually when the application-layer protocol is positioned in different end systems, they can interact with each other when processing data.

Protocol Layering: In software end systems, the protocols that are best suited for implementation are the HTTP and SMTP protocols. These protocols belong to the application-layer, while other protocols which are also suitable for implementation are the transport-layer protocols.

2.6 Hypertext Transfer Protocol (HTTP)

HTTP is an application layer protocol which can be implemented in both a client and a server program that run at different end systems. It uses TCP as its underlying transport protocol. A client and server program can communicate with each other through the exchange of HTTP messages [3].

James F Kurose and Keith W. Ross (2008, p. 123) states that “HTTP defines how web clients request web pages from web servers and how servers transfer web pages to clients” [3]. For example Preston Gralla (2007, p. 26) indicates that the browser releases HTTP requests to the host server and the request is broken into HTTP packets that are sent across the internet’s TCP/IP communications infrastructure to the host computer [4].

The World Wide Web is a virtual network or set of documents that is linked together on the Internet and this includes a client and server that communicate with one another using the Hypertext Transfer Protocol (HTTP) [19].

Client: Browser is a tool for retrieving, presenting, and traversing information resources on the Web. The primary purpose of a web browser is to bring information resources to the user. Servers improve efficiency by storing requested files in its cache memory.

Server: A webpage is stored at the server. Each time a client request arrives, the corresponding document is sent to the client. A server can also be more efficient through multithreading or multi-processing which can enable the server to answer to more than one request at a time.

2.6.1 Uniform resource locator (URL)

URL is a standard for specifying any kind of information on the internet. The URL defines four things: protocol, host computer, port and path.
Investigating Security Options for StudentDevelop.com and the Testing of SSL

The URL consists of the protocol, followed by a colon, then depending on the scheme; domain name (normally the host or IP address), a port number, and the path of the information it is looking for.

![Uniform resource locator](image)

**Fig 2.6.1-1**  Uniform resource locator

### 2.7 File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a protocol for transferring files over the internet. It is commonly used to download files from a server or upload to a server by making use of TCP connections [5]. FTP relies on a pair of TCP connections to perform its operation by establishing two different channels known as Control Channel and Data Channel. The files transfer as seen on fig 2-7-1 shows how files are either being uploaded or downloaded.

Control channel is identified by TCP port number 21. All the commands are sent to FTP-server via this channel. More still, the responses of the commands are received via this control channel.

Data channel make use of TCP port 20 for all data transfer between FTP client and FTP server. For example when the command for viewing directory "\List -aL" is entered, the request is sent via control channel and the response of the command is sent on the data channel on TCP port 20.

![Client/Server model](image)

**Fig 2.7-1**  Client/Server model
2.7.1 File Transfer Protocol security threats
File Transfer Protocol was not designed to be a secure protocol because it has many security weaknesses which includes; [19]
- Bounce attacks
- Spoof attacks
- Brute force attacks
- Packet capture (sniffing)
- Username protection
- Port stealing

Dos attacks being another security threat can occur in the following forms;

**Vulnerability attack:** This attack involves targeting the operating system or application running on a target client by using deceitful messages.

**Bandwidth flooding:** Over crowd the target host with a bung of packets, preventing the right packets from reaching the server.

**Connection flooding:** This involves setting up large open or fully opened TCP connection at the target client.

2.7.2 Simple Mail Transfer Protocol (SMTP)
SMTP is an application layer protocol serving email communications while acting both as SMTP client and server. Mail delivery is a fast and convenient method of transferring information and emails; this accommodates small note or large volumes of memos with a single mechanism or mode of operations. Mails are sent directly to destinations with a single timeout and retransmission for individuals signal if no acknowledgement is returned.

3 Security management
With an increase of virus and malware on the Internet these days, this proves that security management is not always sufficient. A best practice to provide security on the StudentDevelop platform is to always review and replace venerable security features and suites. With the latest version, or modified security suites in place, this can help maintain the entire security management of the StudentDevelop.com platform up to standard.

3.1 Problems with security management
**Security planning:** Many organizations tend to aim for a high degree of security or security that does not correspond to their needs. This leads to an exhaustion of available resources even before the major treat prone areas are secured. Figure 3.1-1 outlines different protocol layers and the type of security it can contain.

**Human component:** When there are system failures, human errors are always a prime subject not withstanding a lingering system problem.
Investigating Security Options for StudentDevelop.com and the Testing of SSL

<table>
<thead>
<tr>
<th>NETWORK ARCTECTURE</th>
<th>SECURITY TYPE</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Separate protocol layer</td>
<td>SSL</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>Application layer</td>
<td>S-HTTP</td>
<td>yes</td>
<td></td>
<td>yes</td>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>Integrated with core</td>
<td>IPsec</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parallel protocol</td>
<td>Kerberos</td>
<td>Yes</td>
<td></td>
<td></td>
<td></td>
<td>yes</td>
</tr>
</tbody>
</table>

Fig.3.1-1 Network security with different forms of security service
A – Full security   B – Multiple applications
C – Tailored services  D – Transparent  E – easy to deploy

By ensuring security is more efficient for the human user, the system can provide a strong backbone for a stronger protection from threats.

Security services can be added directly to a core networking protocol. IPSec is an example of such architecture because it is independent of the application protocol; so many applications may use it. Fig 3.1-2 shows an unsecured protocol with no form of security added. That is, an open browser with no security. Fig 3.1-3 shows a separate protocol layer just for security. Secure socket layer (SSL) ensures secure connection between the TCP and IP layers. In this case information from the HTTP layer is secured by the SSL layer before being transported by the TCP layer.

Adding security to applications is sometime not a good idea because it ties the security services to a single application. Each time there is a change in the application; its implications will be considered and will be modified to suit the changes.

Fig 3.1-4
The illustration shows an instance where SSL can add security not just to HTTP protocol, but to some other protocols like NNTP and FTP.
3.2 Information security

Information security refers to the confidence that un-authorized users cannot access information and services available on the network.

For almost all organization, information is the most valuable asset. The protection of business confidential information and clients’ details are very vital to any organization conducting business.

Unsecured network puts an organization at risk, thereby exposing valuable information of customers and the organization. In fact electronic transactions are only possible if the users trust the service by accepting to perform such action.

By implementing security measures and features, this does not only aim to protect and secure digital resources, however it does add value to some co-operate businesses who give assurance of online safety. It also generates business by enabling electronic transaction as a medium. [21]

3.2.1 Information management (15)

Information security is very vital and of great value to any organization or web platform. If proper security features are put in place, this can reduce threats and close flaws in a web system.

During the planning cycle for the security management of an e-commerce platform, it is advisable to consider the below approach in order to manage information security properly;

**Organization:** This mode outlines the structural and procedural organization of information security and the organization behavior in relation to security.

**Policy:** Consider setting out policies on what information needs protection and how its security can be provided and what kind of security will be used.

**Suitable Technology:** You should compare and consider technologies for use so as to be able to conduct security management efficiently, it is recommended to choose from tested and proven examples.

**The core aspect of information security**

- Assurance of data integrity,
- Freedom from un-authorized computational resources,
- Freedom from snooping or wiretapping,
- Freedom from disruption of services

**Benefits of a good security system**

- **Data integrity:** Secure system must be able to provide protection.
- **Availability:** The system must guarantee that outsiders cannot get a legitimate access to personal data (preventing hackers from getting hold of customer’s details or access).
- **Privacy and confidentiality:** No duplicates of users’ information are passed on to un-authorized users.
- **Authentication**
- **Authorization**
4 Overview of some security infrastructures (SSL, PGP and IPSec)

4.1 Secure Socket Layers (SSL)

Michael P. Papazoglou (2008, p 460) defines SSL as “SSL is an open standard Web protocol that provides server authentication, data encryption, and message integrity over TCP/IP connections” [5].

The Internet Engineering Task Force (IETF) has approved SSL as an acceptable standard protocol. SSL can be found between the lower level protocols TCP/IP and application layer or http protocols which encrypt and re-directs HTTP to the secured server usually identified on the web as HTTPS. This is the standard encrypted communication mechanism on the World Wide Web.

SSL provides authentication, confidentiality and message integrity. Its role is to perform identification and authentication of the parties involved in the communication. Authentication is achieved using public key encryption and a digital certificate issued by a trusted Certificate Authority; AT &T, GTE, CYBERTRUST, KEY Witness international, Microsoft, Thawte Consultancy and VeriSign besides others.

SSL protocol provides effective security for web transactions, while the internet architecture relies on layers of protocols building on the services of the lower layers. Different protocol layers support security services but they also have advantages and disadvantages.

4.1.1 Secure Socket Layers Basics

**Cryptography:** SSL can provide security to confidential information with the use of cryptography. Webpage vital information is encrypted across public networks to achieve a level of confidentiality. There are two types of data encryption in SSL and they include; symmetric cryptography and asymmetric cryptography [18].

Symmetric cryptography uses only one key for encryption and decryption, while asymmetric algorithm uses one key for encryption of data, and then another key for decryption. Asymmetric algorithms are more favorable than symmetric algorithms because even if the encryption key is learned in one direction, the third party still needs to know the other key in order to decrypt the message in the other direction.

With asymmetric encryption, both sides can spontaneously spawn a transaction without ever having met. This is achieved by the use of a public and private key pair. The public key of the entity is public knowledge and is used for encryption, whereas the private key of the entity remains secret and is used for decryption. Public-Key infrastructure (PKI) is the more common name for asymmetric cryptography. Although PKI is more secure, it is more expensive in terms of processing speed. The encryption and decryption of the PKI can take up to 1000 times the processing than symmetric cryptography.

**Digital Signatures:** SSL has a digital signature attached to it that will ensure its integrity. A digital signature is a hashed message with public key information. The message digest is based on the checksum of the message.

The sender and the receiver compute the message digest separately and compare the hashed results because message digest is difficult to reverse. Same results on both sides' means that the checksum was not tampered during transit.
Certificates: SSL uses digital certificates to authenticate servers. Certificates are digital documents that will attest to the binding of a public key to an individual or other entity. They allow verification of the claim that a specific public key does, in fact, belong to the specified entity. Certificates help prevent someone from impersonating the server with a false key. SSL uses X.509 certificates to validate identities. X.509 certificates contain information about the entity, including public key and name. A certificate authority then validates this certificate.

4.2 Pretty Good Privacy (PGP)
PGP defines the standards by which different programs could communicate freely but securely by using an enhanced version of the PGP protocol and a variety of different encryption algorithms which let individuals choose and make security suit them.

PGP implementation of security takes place at the application layer and this can be simpler if the internet communications are solely between two parties, email and telnet.

The sender and receiver can agree on one protocol usage for any security issues they may encounter.

PGP provides excellent levels of confidentiality, integrity, non-repudiation, and authenticity because it combines hashes, public-key encryption, and digital signatures [6].

4.2.1 PGP features and their terminologies
Codes: A code is a general term for any method of concealing the contents of a message. It is a strong form of concealing information.

Ciphers: One type of code is the cipher, which conceals the contents of a message by transforming each character in some way.

Hashes: A hash is a specialized mathematical computation performed on a message, based on one of many algorithms. Related to a cipher, a hash is a very useful tool for PGP. If the original message changes in any way, the hash of that message is completely different [7]. E8e0ee9cdc6cd03c880b5870983bb02d48fceed0 it will look this way 07937cc5fd92504006f5f192d95c8d341a26d18.

Cryptanalysis: These are ways of trying to obtain encrypted information known as cipher text, without access to that information. This is also the science of analyzing and breaking secure communication/information. Cryptanalysis involves a combination of analytical reasoning, some application of mathematical tools, pattern finding, time, determination, and luck. Attackers or hackers are known as cryptanalyst.

Integrity: Integrity refers to keeping a message unchanged. Using PGP, one can confirm that a message has not been tampered during transmission.

Confidentiality: PGP can also provide confidentiality, which means that the message contents remain private. The plaintext cannot be viewed by anyone who does not have the necessary access like keys, algorithms, and tools.

Non-repudiation: Non-repudiation means that a person cannot deny signing a particular message; this can keep track of who sent what, when it was sent and how it was sent in context of email.
Web of trust: This is the global network of people who have identified each other and digitally signed each other’s PGP keys. The Web of Trust is composed entirely of links between individuals. Everyone who is using PGP to communicate with a variety of people is connected via the Web of Trust [9].

Key servers: Key servers store PGP public keys for general public access.

Key signing: By signing another person’s key, you are affirming that you have verified that person’s identity and this is referred to as trust in the OpenPGP standard. This can actually mean trust in the PGP sense, meaning only that you trust the person’s identity.

4.2.2 PGP Desktop files
Documents which contain important information are encrypted using PGP desktop software, and then use a public key for encryption and a private key for decryption. This software ensures that information cannot be tampered even if it was emailed to a wrong user.

The PGP contains a key; a technology called non-repudiation. This means that the customer must sign, indicating that he/she has received the request/products.

According to Derek Atkins with a background from MIT’s Media Laboratory and EECS departments, at Massachusetts Institute of Technology, (MIT) viewed 22 - 03 -2012 at “http://www.mit.edu/people/warlord/pgp-class/messages.html” has listed the following step-by-step on How PGP works: [9]

Message encryption
Signing a message: pgp -sat file
  - Compute a Message Digest (hash) of the message (MD5)
  - Encrypt the hash with the signer’s Private Key

Encrypting a Message: pgp -ea file recipient(s)
  - Compress the file
  - Choose a Random Secret (IDEA) Key (session key)
  - Encrypt message in IDEA using session key
  - Encrypt session key in recipients’ Public Key(s)

Sign and Encrypt a Message: pgp -sea file recipient(s)
  - Generate a signature on the file, as above
  - Encrypt the signature and file, as above

Verifying a Message: pgp file
  - Decrypt session key using Private Key
  - Decrypt message using session key
  - Generate Message Digest of the message
  - Decrypt signature using signer’s Public Key and compare

Ascii Armor: -a
  - Takes a PGP message and wraps it in ASCII, so it can be transmitted over mail or printed.
  - Is _only_ a wrapper; the armor is not secured.
Investigating Security Options for StudentDevelop.com and the Testing of SSL

4.3 Internet Protocol Security (IPSec)

IPSec is a collection of protocols designed by IETF (Internet Engineering Task Force) to provide security for a packet at IP level. This allows a user to decide for an encryption, authentication and hashing method as desired. IPSec does not guarantee security on the webpage because it is designed for a network that runs an internet protocol packet.

IPSec is a network layer protocol which provides different security services such as; cryptographic agreement, encryption of IP datagram payloads, data integrity, and origin authentication. It is connection-oriented and can be used to communicate securely over none secure network such as the public internet. IPSec also provides secure sessions with host authentication, data integrity, and data confidentiality [10].

Security: IPSec uses digital certificates or a shared key for authentication purposes. Since IPSec operates at a lower level in a stack, it is more flexible and can protect more data above it.

Security association: IPSec requires a logical connection between two hosts using signaling protocol in other words called security association (SA).

Data protection: IPSec protects data by authenticating data received from the user, using the "Authentication Header" method or by encapsulating or encrypting the data from unauthorized user. Data encryption techniques include DES, AES and Blowfish.

IPSec, enable Internet users to carry-out email conversations and feel secure about the authenticity of their messages. IPSec offers Internet shoppers security when ordering products.
Investigating Security Options for StudentDevelop.com and the Testing of SSL

4.3.1 Comparison of some security suites
The differences between SSL and PGP are that SSL supports only the use of Digital Signature, while PGP uses public key encryption. In addition, PGP is different from SSL in that it allows you to create digital signatures by yourself.

Both SSL and PGP provide web integrity, authentication, and confidentiality in their respective ways, however they all have some differences and limitations as identified below;

Advantages of SSL
- With the use of SSL, the data are usually encrypted, and then transmitted during online transaction.
- It provides added trust to the website users and thus making a user to trust the website. It is important for a user to know that the website is secured and has been verified. One way to know if a website is SSL secured is by looking at the browser to see if the URL starts with this format "https://".
- SSL secures a private communication link or channel for the transmission of very sensitive information.

Advantages of PGP
- PGP creates both public and private keys. In order to access the private key, a password is required on every attempt to access the private key.
- When using PGP, you can either encrypt, sign messages or automatically encrypt and sign at the same time providing an extra boast of security with encryption.

Disadvantages of SSL
- SSL certificate expires after a short period of time and it requires renewals which are quite expensive.
- SSL technology can be difficult to install on a website, and at times it requires writing long software codes and installations.
- The two relevant cryptographic operations of SSL occur during the data transfer phase. When using SSL, this can dramatically slow down the web servers and as well interfere with the web portal itself.

Disadvantages of PGP [22]
- Managing keys can be challenging for users new to PGP. When keys are lost or corrupted it can be a security risk to users in a highly secure environment. These kinds of problems can lead to recipients being unable to open encrypted files.
- OpenPGP works for only PGP users; both the sender and the recipient must be using PGP. If the sender emails a file to a recipient who is not using PGP, the user cannot access the files.
5 Email security

5.1 Messaging system for the StudentDevelop.com web portal
We used PHP command to program studentdevelop.com so messages should be read externally from the web portal (read from any users personal email in-box). To do this, we used the following Php command: "mail ($to, $subject, $message)" (One line of PHP code); no need to save messages in the Data Base because messages are just sent directly to the receiver's in-box outside studentdevelop.com.

Studentdevelop.com uses two to three arrays, which are;

POST, GET and SESSION array (These three arrays are used for communicating between pages):

- Function for “POST ”, all information hidden in the system
- Function for “GET”, information are shown on the browser
- Function for "SESSION" - An array to save variables. Comparing string if exist in our system (for example domain name)

The admin can currently access the files at the server by connecting through an FTP protocol, which is a TCP/IP protocol. Example of FTP can be FILE ZILLA (FTP)

![Email security report for domain: www.studentdevelop.com](image)

Fig 5.1-1  Shows the test result using online email security grader, which shows security levels of SMTP Server for incoming and outgoing mails.
5.2 Email server measuring respond time for mail server

We ran a DNS testing using Email Server Test with the online SMTP diagnostic tool MxToolbox to check for mail blacklist and TIME TO LIVE (TTL) for packets.

However, emails are automatically sent at a preset time (via the shared hosting server) usually every 45-60 minutes. This means that if a user sends a message from studentdevelop.com; messages are kept on a queue to be delivered at the scheduled time in which messages are generally set to leave the server.

If we had programmed the system in a way that a user needed to read a message sent to them via within the web portal, then we needed to save those messages in the database. For example, one database for messages (containing who sent what, to whom, text of message, status (read/unread). However, the above alternative way for a user to receive emails externally to their private inbox was implemented mainly because the current studentdevelop.com portal uses a shared hosting plan with limited space.

6 Implementation of security layer on studentdevelop.com

To operate an e-commerce platform that processes secure data communication over the internet, encryption and authentication techniques are recommended. During the evaluation of SSL in chapter 4, we could observe that SSL protocol stands a better chance on providing added security solution for web service interaction.
Investigating Security Options for StudentDevelop.com and the Testing of SSL

Taking into consideration SSL also uses Public-Key infrastructure (PKI), StudentDevelop can be assured to attain the below functionality;

With SSL, authentication is achieved using public key encryption and a digital certificate issued by a trusted Certificate Authority. SSL is ideally suitable for use with web browsers and web server, it provides good security and does encrypts data either using asymmetric cryptography or symmetric cryptography.

6.1 Public-key infrastructure
Asymmetric encryption uses Public-Key Infrastructure (PKI) for encryption and private key for decryption which provides application and network security.

PKI supports a cryptographic public and private key which deals with confidential information while verifying digital signatures.

Basically PKI provides confidentiality, integrity, non-repudiation and authentication because it authenticates electronic transaction using digital certificate and other certificate authorities.

6.2 Testing of SSL
Before installing SSL certificate on any website, it is important you decide either to verify the certificates on the website itself (self–signed; creating it yourself/test environment) or by obtaining a certificate from a known Certificate Authority (CA) for example VeriSign, Thawte, Geotrust among others.

With regards to this thesis, SSL would be tested on studentdevelop.com by trying two possible different scenarios;

- On windows IIS 5.0 with rapidSSL certificate from a Certificate Authority
- On windows IIS 7.0 with self-signed certificate

The installation of SSL can be done in different ways as stated below;

- By using Internet Information Services (IIS) Manager Tool.
- Command line Tool.
- Graphic user interface (GUI) through Microsoft or other certificate company scripts.

6.3 Self-signed certificate
We shall use IIS manager tool and install SSL using the following four major steps;

- Download a functional certificate.
- Create an HTTPS binding on a website.
- Test by making a request to the website.
- Optionally configure SSL options; by making SSL a requirement.
Creating an SSL certificate for studentdevelop.com

Installation of self-signed certificate on client computers
With a self-signed certificate, the browser will display a warning at the start of a webpage with the server. Unless an application that uses a secured service on a server with a self-signed certificate trusts the link, exporting the certificate from the server and importing it to the client machines will solve the situation of the warning. This should only be done for internal test and development purposes, not for production websites.

To export the certificate, follow the following steps;

At the IIS Manager, open and expand the tree and right-click "Default Web Site" and choose "Properties".

In the "Directory Security" tab, and under "Secure Communications", click "View Certificate". This will then list all certificates registered on the machine, and allow you to optionally import and/or create new certificates. Refer to fig 6.3-2.

Remember that it is possible to request SSL certificate from a certificate authority like Verisign, purchase the certificate and import using this admin UI.

Alternatively, we shall create a "self-signed certificate" which is a test certificate that we can use during the development and testing of studentdevelop.com. To-do this, click the "Create Self-Signed Certificate" link on the right-hand side of the admin tool and continue as indicated below or seen on figures 6.3-3- 6.3-5:
Investigating Security Options for StudentDevelop.com and the Testing of SSL

**Opening the server port**

![Image](image1)

*Fig 6.3-2*  
Shows default port 80. To enable SSL for this website, click the "Add" button at the Pop-up’s “add binding” box to add HTTPS protocol support.

**Assigning port number**

![Image](image2)

*Fig 6.3-3*  
Assigning port number 443 and website binding
Secured port

Fig 6.3-4 The illustration shows the website binding and thus a new window with https.

Creating two random certificates

Fig 6.3-5 Shows two self-signed certificates created, one for the testing environment and one for Studentdevelop.com
Investigating Security Options for StudentDevelop.com and the Testing of SSL

The implementation of self-signed certificate
We used a newer version of Windows XP internet Information Services (IIS) such as version 7.0 which contains features such as membership-based authentication and enhanced logging system. The new FTP service offers Web administrators and web host an integrated management and configuration experience for FTP and Web sites through IIS Manager for implementing the self-signed certificate.

6.4 Deploying SSL termination devices (ISS 5.0)
The deployment of SSL on StudentDevelop.com's web environment consisted of a web server with an integrated SSL module (an SSL-enabled network interface card [NIC]). The client initiates a session with the server, and the server is directly responsible for the SSL termination.

This process adds load to the server, which is already responsible for all Hypertext Transfer Protocol (HTTP) information that is sent to and received from the client. The Web server processor is shared across both the SSL processing and HTTP processing.

Installation of SSL certificate using Microsoft internet information services (IIS 5.0)

![Access settings. Username and password settings are enabled to prevent anonymous access.](image)

Installing SSL certificate using Microsoft internet information services on older versions of Windows like XP required us to run IIS version 5.0. By using this option, it requires an administrative user access before a website can be created on the IIS tool. This is a major difference between IIS version 5.1 and version IIS 7.0 as seen on fig 6.4-1-2.
6.5 How Secure Socket Layers works

SSL has two distinct entities, server and client. The client is the entity that initiates the transaction, whereas the server is the entity that responds to the client and negotiates which cipher suites are used for encryption.

Three protocols lie within SSL, the Handshake Protocol, the Record Protocol, and the Alert Protocol. The client authenticates the server during the Handshake Protocol. When the session is initiated and the handshake is complete, the data transfer is encrypted during the Record Protocol phase. If there are any alarms at any point during the session, the alert is attached to the questionable packet and handled according to the Alert Protocol.

**SSL handshake:** The client always authenticates the server, and the server has the option of also authenticating the client. In general, web servers do not authenticate the client during the Handshake Protocol because the server has other ways to verify the client other than SSL. For e-commerce, the web-site server can verify the credit card number externally from the SSL session. In this way, the server can reserve precious processing resources for encrypted transactions.

**SSL records:** The encryption for all messaging in SSL is handled in the Record Protocol. This protocol provides a common format to frame all alert, Change Cipher Spec, Handshake, and application protocol messages. The SSL records consist of the encapsulated data, digital signature, message type, version, and length. SSL records are 8 bytes long and due to the fact that the record length is fixed, encrypted messages sometimes include padding and pad length in the frame.

**SSL alert protocol:** As mentioned earlier, the Alert Protocol handles any questionable packets. If either the server or client detects an error, it sends an alert containing the error. There are three types of alert messages: warning, critical, and fatal. Based on the alert message received, the session can be restricted (warning, critical) or terminated (fatal).
7 Result

The outcome of this thesis investigation for securing studentdevelop.com resulted to the testing of SSL on the web portal. SSL was not tested on the production website; instead it was tested at the test environment.

By deploying SSL on StudentDevelop.com, this initiates the use of a PKI for web service transaction because SSL protocol could allow the portal to expose its public key to requesters without requiring looking up the key in a public directory.

SSL then performs identification and authentication of the parties involved at the communication layer by encrypting the session so that the public key can be used to send encrypted data to the Web Service.

By using the public key alone for authentication, the identity of the private key holder cannot be guaranteed. Since SSL includes digital certificates, it became possible to verify the holder of such private key, because the digital certificate bears the identity information of the private key holder.

SSL acts as a security add-on at the studentdevelop.com portal; it encrypts and re-directs HTTP to the secured server which is usually identified on the web as HTTPS. Encryption algorithm and digital signatures provided the basic building blocks. The SSL protocol made up the next layer of mechanisms that in turn support the application layer.

The registration authorities are in-charge of verifying identities of the digital certificate holders. A challenge-response algorithm is used as a requirement for digital signature including every attempt an entity is requesting to authenticate itself. Since it is possible to retrieve a digital certificate from a public directory, a proof-of-possession (POP) is always included for the corresponding private key when using digital certificate for authentication purposes.

In order to verify the web servers’ private key, the web browser interacts with the web server to check the respond request from the web server. For authentication purpose, the web server private key is examined to verify if it corresponds to the public key in their digital certificate. After the identity of the web service provider has been verified, it is at this time a digital certificate is issued. It is the registration authority who instructs the certificate authority to issue a digital certificate. In some cases, the verification of identity and the issuance of digital certificate can be done by the same organization, otherwise by another vendor.

7.1 Result on self-signed certificate scenario

To view the self-signed certificate, you can do this by selecting from the SSL certificate drop down box list and choose one of the self-signed certificates which were created earlier; “studentdevelop” and “testing”.

HTTPS uses port number 443, while HTTP uses port number 80.
7.1.1 Testing SSL certificate on a local host
Take note that IIS has the authorization rule which prevents unauthorized access to contents even when content is moved to a different server or to a new domain.

Operational activities such as logging into the web portal and henceforth financial transaction are auto transferred to a secured server. It can be viewed on the web browser starting in this format: "https://", certifying that studentdevelop.com is secured using SSL.

Fig 7.1-1 Result shows that certificates have been created.

Fig 7.2.1-1 After the self-signed certificates are created, we opened the local host and typed http as a test in order to see the outcome.
The above message was the result we got (stating "there is a problem with this website’s security certificate"). The error appears because it is a self-signed certificate and not yet approved by a certificate authority (CA).

There are three important things that a browser usually verifies in a server certificate and if one or more of these checks is not confirmed, the browser prompts the user with warnings. The server will verify the certificate to make sure; that the current date and time within the certificate is in "Valid from" and "Valid to" the date ranges on the certificate.

The browser also checks that the certificate's "Common Name" (CN) matches the host header in the request. For example, if the client is making a request to http://www.studentdevelop.com/, then the CN must also be http://www.studentdevelop.com/.

Lastly the browser confirms to see that the issuer of the certificate is a known and trusted Certificate Authority (CA).

7.2 Trial certificate from a certificate authority
The implementation of the SSL protocol has increased the security for web transactions. This is also due to the fact that authentication is achieved using public key encryption and a digital certificate issued by a trusted certificate authority.

The implementation of SSL certificate using Microsoft internet information services (IIS 5.0) involved requesting a trial certificate from RapidSSL; a Certificate Authority.

Even though the certificate was issued by a certificate authority, we were not able to test SSL at the StudentDevelop production web site because the payment gateway of the portal has not yet been setup which is required in order to conduct financial transaction. However we could successfully implement the SSL certificate and see the result as seen below on Fig 7.2-1.
Investigating Security Options for StudentDevelop.com and the Testing of SSL

**Fig 7.2-1** Certificate information showing validity.

Confirmation message from a certificate authority attesting studentdevelop.com web portal has newly been secured with the insurance of SSL certificate.

The following certificates are correctly installed:

-----Certificate 1-----

Issued To--
Organization: *.studentdevelop.com
Organizational Unit: Domain Control Validated - RapidSSL(R)
Organizational Unit 3: GT23895939
Common Name: *.studentdevelop.com
Country: US

Issued By--
Organization: Go daddy
Organizational Unit: Go daddy Secure Certificate Authority
Country: US
Valid from Sun Jun 05 17:20:28 ET 2011 to Tue Jun 23 06:40:11 CEST 2012
Serial Number (hex): 13815e
Investigating Security Options for StudentDevelop.com and the Testing of SSL

8 Conclusion

During this thesis work, we have learned that certificate authorities are the issuers of digital certificates. Service provider like studentdevelop.com can use a valid digital certificate to provide a secure e-commerce environment which processes financial transactions.

We have come to realized that SSL is a good security add-on for e-commerce platform such as studentdevelop.com. It uses asymmetric encryption involving PKI technology for carrying out authentication on HTTP.

The reason we selected SSL over PGP is because the SSL protocol provides confidentiality using encryption mechanism to encrypt information traveling from a web browser to a web server. SSL also does it authentication using digital certificates for HTTP traffics.

From our research findings with other existing major e-commerce websites for example ebay.com, they all use SSL to secure their web pages. The Internet Engineering Task Force (IETF) has approved SSL as an acceptable standard protocol.

It is due to all these facts that consumer confidence has increased within the business to consumer (B2C) e-commerce. These days, most websites with a validated SSL certificate issued by a known certificate authority can provide their identities to consumers. Trust and assurance awareness can be identified in different ways such as a web seal sign, logo type signs stating for example; verified by “Verisign” and, in addition to the browser page starting with “https”.

Finally with all the research and investigation about the importance of SSL, we discovered that it is also possible for SSL to carry out authentication of users of a web browser for them to identify themselves to the web service provider (website). However this is not recommended for businesses as it has proven time consuming to generate a public and private key pair while looking into how to register the keys with a public key infrastructure. Overall, this still leave us with no other fact but to conclude that with e-commerce, consumers in most cases can be sure of the validated web service provider (web site). The reverse is not true.

8.1 Email delay problem conclusion

We double checked on the source codes via the control panel at the admin section of the hosting company where StudentDevelop.com portal files and source codes are stored. We could not find any fault with the source codes. Since the StudentDevelop.com platform is a legit e-commerce platform, we are not allowed to publish the result finding of the source code on this report.

After a further investigation with the hosting company concerning the shared hosting server studentdevelop.com web portal is hosted, it has been discovered that the hosting company servers are not set up for massive or instant messaging.

With regards to the result of our research findings, it included a couple of email exchange together with a phone call enquiry with studentdevelop.com hosting company. We were told that at their shared hosting server their server routes messages by giving priority to active websites hosted on their server which has a massive request demand to the mail server. Since the StudentDevelop.com platform has not been active with making such massive request to the mail server (due to it being in the development stage now), StudentDevelop.com portal files has been placed on one of the hosting company server which has a slow respond time; therefore messages are often placed on a queue.
Regarding the problem causing message delay involving sent and received messages from within the studentdevelop.com portal; this has to do with transmission delay.

With an upgrade of studentdevelop.com shared hosting plan or if the StudentDevelop.com platform can host its own private virtual server, this will provide enough data space. Once the server will have the ability to process and transmit data at a much fast rate, the server will be less busy as compared with the current shared servers.

As a proposal for future study, we suggest programming the studentdevelop.com portal or any other website in such a way that messages between two registered users connected to the portal can be sent and read within the platform itself instead of receiving messages from their external private inboxes only.

Business wise, this is a good practice as it can facilitate you to operate an active e-commerce website with users logging in to read or reply to emails thus increasing website traffic. If you were to provide just the service for users to read emails externally at their private inboxes, then users might find it hard to be able easily reply a message sent to them from within the portal and at the same time keep record of their message history inside the web portal.

To achieve the goal of having users able to read emails from within the web portal, the admin would need to create another separate database for message records storage. The reason for the current way messages are being sent and read between registered users external email accounts with regards to Studentdevelop.com is due to the portal’s shared hosting plan package. It has a limit in the database and thus the existing temporal emailing option was used to offer the possibility to communicate because the platform is still in the beta stage.
References


And


And

URL Source: http://www.faqs.org/rfcs/rfc959.html


By Derek Atkins with a background from MIT's Media Laboratory and EECS departments, at Massachusetts Institute of Technology, (MIT)


And

Web services: Principles and Technologies (2008), by Michael P. Papazoglou (Page 461)
Investigating Security Options for StudentDevelop.com and the Testing of SSL


And


[15] Privacy and security in internet-based information system, by Andreas Jacobsson


[18] Data Communication, URL source:
http://www.camiresearch.com/Data_Com_Basics/data_com_tutorial.html

[19] Internetworking with TCP/IP principles, protocols and architectures.


[22] Disadvantages of PGP, URL Source: http://www.ehow.com/list_5924278_disadvantages-pgp-encryption_.html#ixzz1QIs0bt2h