Abstract: The Internet has undoubtedly become the largest public data network, enabling and facilitating both personal and business communications worldwide. While the Internet has opened the door to an increasing number of security threats from which corporations must protect themselves. With the growth of the Internet, many applications need to securely transmit data to remote applications and computers. TCP/IP protocol is core part for the communication for any network, by means that TCP/IP with the collaboration of SSL/TLS provides the solid security. SSL is designed to resolve the security issues as an open standard. Secure Sockets Layer (SSL) is the Internet security protocol for point-to-point connections. This study focuses on the performance analysis of SSL/TLS with different protocols as well as it will lead us to learn about the limiting behavior of SSL/TLS in TCP/IP. Further, future extensions of SSL/TLS must be the part of this research.

Keywords: Phishing, Spoofing, OTP, LDAP, SSL/TLS, TCP/IP, FTP, IMAP, POP3, HTTP

1 Introduction

Securing the modern business network and IT infrastructure demands an end-to-end approach and a firm grasp of vulnerabilities and associated protective measures. Most electronic commerce (e-commerce) applications in use today employ the Secure Sockets Layer (SSL) which is now also known as the Transport Layer Security protocol (TLS), defined by the draft Internet standard RFC2246 to authenticate the server and to cryptographically protect the communication channel between the client and the server. The SSL protocol, allows mutual authentication between a client and server and the establishment of an authenticated and encrypted connection. SSL/TLS provides support for user authentication based on public key certificates. But in practice, due to the slow deployment of these certificates, user authentication usually occurs at the application layer. There are many options here; including personal identification numbers (PINs), passwords, passphrases, as well as “strong” authentication mechanisms, such as one-time password (OTP) and challenge-response (C/R) systems. In theory, the SSL/TLS protocol is assumed to be sound and secure. In practice, however, the vast majority of SSL/TLS-based e-commerce applications, employing user authentication at the application layer, are vulnerable to phishing, Web spoofing and most importantly man-in-the-middle (MITM) attacks. SSL runs above TCP/IP and below HTTP, LDAP, IMAP, NNTP, and other high-level network protocols. It was originally invented by Netscape and has become a de facto Internet standard. For the SSL 3.0 specification (also called SSL v3) in plain text form, SSL, or more specifically, the RSA public-key cryptographic operations usually used to exchange the session key at the start of a connection, is computationally intensive. It takes far more CPU time to establish an SSL connection than a normal connection.

In this study the strength of SSL/TLS is proved as a greatest protocol working with TCP/IP for secure network communication.
2 Previous Research

[Homin K. Lee et al., 2007] proved the strength of SSL (Secure Socket Layer) or TLS (Transport Layer Security) as a strongest security mechanism in client server environment publically. SSL/TLS uses cryptographic algorithms to encrypt data and communication. Homin K. Lee et al. developed a mechanism for this purpose named Probing SSL Security Tool (PSST) and checked its performance on more than 19,000 public servers. This tool checks the security by varying levels of security and changing the encryption algorithms used in SSL cryptography acceptable over the larger networks including internet. The outcomes of the tool shows an encouraging use of advanced security algorithms but there is not as fast adoption as needed.

[Rolf Oppliger et al., 2007] addressed the severe danger caused by Man in The Middle Attacks for SSL/TLS web application especially dealing financial transactions. Man in The Middle Attacks has no counter measure even for application running in support of SSL/TLS because those applications have no clear procedure for verification of user. Rolf Oppliger et al. demonstrated that their mechanism named “SSL/TLS session-aware user authentication” provides remedies to these problems. They make some variations in their mechanism and check it for user authentication. It begins with self-verification with passwords. After that improvements and expansions are discussed. Options for putting into practice their approach are also discussed.

[Zanin et al., 2007] designed a signature protocol for distributed systems especially useful for extensive and temporary mobile networks, which used encryption based on RSA algorithms. Security constraints and structural restrictions are also presented in the protocol designed, even it is very vigorous, adoptable and for scattered networks. According to researchers performance of the designed protocol can be increased to a level if the number of participants in the network is limited. Protocol proposed by Zanin et al. is robust according to them as it worked well for limited number of nodes and allow them to create suitable encrypted digital signature. An intruder is unable to break security for chosen number of participants, hence cannot disturb the performance of network or make digital signature illegal. The characteristics of this protocol are immense as compared to the limitations of less number of nodes.

[Shi qun li et al., 2008] argued the network performance degrades in the presence of SSL/TLS. Secure Socket Layer is based on encryption algorithms to encrypt data and keys. This algorithm used complex calculation which involves intensive arithmetic for keys that degrades performance, thus making SSL/TLS slowed under and loses its power in terms of efficiency while deciphering the data and keys. When number of requests to server containing SSL/TLS increases performance decreases. Shi Qun li et al. proposed a solution by suggesting modifications in RSA algorithm called “Batched RSA decryption algorithm”. This suggested algorithm increases network efficiency by offering accountably acceptable response time. At the same time deciphering process is also enhanced and accelerated, comparative to the size of b for batch. This technique is analyzed with some variations by the researchers in this study.

[Wooyoung Jung et al., 2009] worked for IPv6 security issues I wireless networks. Wooyoung Jung et al. developed a cryptographic protocol for Internet Protocol – Wireless Sensor Networks. Wireless sensor networks architecture integrating their mechanism with IPv6, are immensely used everywhere in the world. But this architecture failed to provide security, because it is a known fact that IPWSN take it as a heavy load to become accustom with cryptographic protocols of internet. These mobile networks are light Wight in hardware having RAM inn Kilobytes, and a slow processor, so it uses very light components o Secure Socket Layer (SSL) protocol. By implementing the proposed protocol in these light Wight systems, utilization of resources are low such as only 7 Kilobytes of RAM, 64 Kilobytes of flash memory for verification of user. It uses RC4 algorithm for message encryption. Session initiation of SSL handshake in this protocol take much less time and transmit a large size of data. It can be very smoothly used for domestic purposes as well as for healthcare and in army.

[Fang Qi et al., 2009] introduced that the suggested SSL session initialization can be enhanced in efficiency by secret swap over algorithm. This research at first shows that several certificates are needed in earlier version of SSL which uses batch RSA that is not practical for implementation. After that it presented only one of its kind certificate, which cope with the problem of multiple certificates. The optimized approach, concentrate over public key size to get better results, which have its foundation on the constrained model taking into account the user requirements for raking of aware security. Optimized arguments usage is also introduced while combining them with consumer needs for quality of service over internet. Constancy of the system and the bearable response time are example of QoS. At the end, by analysis and simulations shows that suggested algorithm are appraised to be practical and efficient.
[Pratik Guha and Shawn Fitzgerald, 2013] claimed that over the last few years, a number of vulnerabilities have been discovered in the Transport Layer Security protocol. The purpose of this paper is to serve as an analysis of recent attacks on SSL/TLS and as a reference for related mitigation techniques, particularly as they relate to HTTPS.

[Devdatta Akhawe et al., 2013] performed a large-scale measurement study of common TLS warnings. Using a set of passive network monitors located at different sites, they checked the population of about 300,000 users over a nine-month period. They identified low-risk scenarios that consume a large chunk of the user attention budget and make concrete recommendations to browser vendors that helped to maintain user attention in high-risk situations. They studied the impact on end users with a data set much larger in scale than the data sets used in previous TLS measurement studies. A key novelty of their approach involves the use of internal browser code instead of generic TLS libraries for analysis, providing more accurate and representative results.

3 Proposed Work

3.1 Testing Roadmap
1. Construction of hypothesis
2. Analyzing Test bed requirements.
3. Installing and configuring LAN
   - Installing and configuring Windows 2003 server on server machine
   - Installing and configuring Windows XP on client machines.
4. Installing and configuring network monitoring tools
5. Configuring security mechanisms.
6. Perform statistical analysis of LAN performance

3.2 Testing Hypothesis
1. Presence of security (SSL/TLS) affects the performance of network in terms of response time, delay, bandwidth utilization and throughput.
2. Presence of security (SSL/TLS) does not affect the performance of network in terms of response time, delay, bandwidth utilization and throughput.

3.3 Testing Procedures
Testing is done to check response time of FTP, POP3 and IMAP protocols. For each protocol two cases are made, in first case reading are taken in the presence of SSL/TLS and in second case readings are taken in the absence of SSL/TLS.

![Fig.2 SSL/TLS and TCP for Secure communication](image)

Case 1: FTP Service with Security (In the Presence of SSL/TLS)
- Configuring one machine as FTP Server with Security.
  FTP Server IP = 172.16.0.1 255.255.0.0
- Configuring other machine as FTP Client.
  FTP Client IP = 172.16.0.2 255.255.0.0
- At server side configuring a folder for FTP sharing and copying zip files of size 20, 40, 60...4000 MB.
- At client side downloading files using FileZilla and noticing response time.

![Fig.3 FTP Service in Presence of SSL/TLS](image)

Case 2: FTP Service without Security (In Absence of SSL/TLS)
- Configuring one machine as FTP Server with no Security.
  FTP Server IP = 172.16.0.1 255.255.0.0
- Configuring other machine as FTP Client.
  FTP Client IP = 172.16.0.2 255.255.0.0
- At server side configuring a folder for FTP sharing and copying zip files of size 20, 40, 60...4000 MB from client.
- At client side downloading files using FileZilla and noticing response time.
Case 3: IMAP Service With Security (In the Presence of SSL/TLS)

- Configuring one machine as E-mail Server (IMAP) with Security.
  - IMAP Server IP = 172.16.0.1 255.255.0.0
  - Installing MS Outlook at server machine.
- Configuring other machine as E-mail Client (IMAP).
  - IMAP Client IP = 172.16.0.2 255.255.0.0
  - Installing MS Outlook at client machine.
- At server side sending emails to clients and attach zip files of size 20, 40, 60 ...4000 MB.
- At client side configuring MS-Outlook to receive emails from server, and noting down response time.

Case 4: IMAP Service without Security (In the Absence of SSL/TLS)

- Configuring one machine as E-mail Server (IMAP) with no Security.
  - IMAP Server IP = 172.16.0.1 255.255.0.0
  - Installing MS Outlook at server machine.
- Configuring other machine as E-mail Client (IMAP).

Case 5: POP3 Service with Security (In the Presence of SSL/TLS)

- Configuring one machine as E-mail Server (POP3) with Security.
  - POP3 Server IP = 172.16.0.1 255.255.0.0
  - Installing MS Outlook at server machine.
- Configuring other machine as E-mail Client (POP3).
  - IMAP Client IP = 172.16.0.2 255.255.0.0
  - Installing MS Outlook at client machine.
- At server side sending emails to clients and attach zip files of size 20, 40, 60 ...4000 MB.
- At client side configuring MS-Outlook to receive emails from server, and noting down response time.

Case 6: POP3 Service without Security (In the Absence of SSL/TLS)

- Configuring one machine as E-mail Server (POP3) with no Security.
- POP3 Server IP = 172.16.0.1 255.255.0.0.
- Installing MS Outlook at server machine.
- Configuring other machine as E-mail Client (POP3).
  - POP3 Client IP = 172.16.0.2 255.255.0.0.
  - Installing MS Outlook at client machine.
- At server side sending emails to clients and attach zip files of size 20, 40, 60 …4000 MB.
- At client side configuring MS-Outlook to receive emails from server, and noting down response time.

4 Results

Data in graph shows that security increases the response time of FTP. These values are taken as mean of 5 values to show the difference in response time in the presence and absence of SSL/TLS. Security degrades performance of network.

Table 1: Sum of Response Time for FTP With Respect to Security

<table>
<thead>
<tr>
<th></th>
<th>No Security</th>
<th>SSL/TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sum</td>
<td>33460</td>
<td>33475</td>
</tr>
</tbody>
</table>

Graph for sum of response time shows the result more clearly that how SSL degrades the performance of FTP.

Table 2: Average Response Time for FTP With Respect to Security

<table>
<thead>
<tr>
<th></th>
<th>No Security</th>
<th>SSL/TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>167.300</td>
<td>167.375</td>
</tr>
</tbody>
</table>

Graph for average of response time shows the result more clearly that how SSL degrades the performance of FTP.

Fig. 7 POP3 Service in Absence of SSL/TLS

Fig. 8 FTP Response Time Graph for Data With Respect to Security

Sum of response time is taken to see the collective effect of security on response time of FTP in the absence and presence of SSL/TLS. This shows the actual effect of security on the performance of network that response time increases with security and efficiency decreases.
Graph for sum of response time shows the result more clearly that how SSL degrades the performance of IMAP.

Average of response time is taken to see the average effect of security on response time of IMAP in the absence and presence of SSL/TLS. This shows the actual effect of security on the performance of network that with security response time increases and performance decreases.

Table 4: Average Response Time for IMAP With Respect to Security

<table>
<thead>
<tr>
<th></th>
<th>No Security</th>
<th>SSL/TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>317.985</td>
<td>318.35</td>
</tr>
</tbody>
</table>

Graph for average of response time shows the result more clearly that how SSL degrades the performance of IMAP.

Table 3: Sum of Response Time for IMAP With Respect to Security

<table>
<thead>
<tr>
<th></th>
<th>No Security</th>
<th>SSL/TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sum</td>
<td>63597</td>
<td>63770</td>
</tr>
</tbody>
</table>

Data in graph shows that security increases the response time of IMAP. These values are taken mean of 5 values to show the difference in response time in the presence and absence of SSL/TLS. Security degrades performance of network.

Sum of response time is taken to see the collective effect of security on response time of IMAP in the absence and presence of SSL/TLS. This shows the actual effect of security on the performance of network that response time increases with security and efficiency decreases.
Data in graph shows that security increases the response time of POP3. These values are taken mean of 5 values to show the difference in response time in the presence and absence of SSL/TLS. Security degrades performance of network.

![POP3 Response Time Graph By Security](image)

Fig.14 POP3 Response Time Graph for Data With Respect to Security

Sum of response time is taken to see the collective effect of security on response time of POP3 in the absence and presence of SSL/TLS. This shows the actual effect of security on the performance of network that response time increases with security and efficiency decreases.

Table 5: Sum of Response Time for POP3 With Respect to Security

<table>
<thead>
<tr>
<th></th>
<th>No Security</th>
<th>SSL/TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sum</td>
<td>63595</td>
<td>63980</td>
</tr>
</tbody>
</table>

Graph for sum of response time shows the result more clearly that how SSL degrades the performance of POP3.

![POP3 Data Graph By Sum of Response Time](image)

Fig. 15 Average Response Time Graph for IMAP With Respect to Security

Average of response time is taken to see the average effect of security on response time of POP3 in the absence and presence of SSL/TLS. This shows the actual effect of security on the performance of network that with security response time increases and performance decreases.

Table 6: Average Response Time for IMAP With Respect to Security

<table>
<thead>
<tr>
<th></th>
<th>No Security</th>
<th>SSL/TLS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>317.975</td>
<td>319.9</td>
</tr>
</tbody>
</table>

Graph for average of response time shows the result more clearly that how SSL degrades the performance of POP3.

![POP3 Data Graph By Average Response Time](image)

5 Conclusion

SSL provides high-level security, but it also degrades performance of the network to some extent. Response time for FTP, IMAP and POP3 increased with SSL/TLS and performance of network degrades. Session keys at the start of the connection of SSL are usually exchanged by RSA public key cryptography operation, are computationally intensive. It takes more CPU time to establish SSL connection than a normal connection.

Other parameters such as delay, throughput and bandwidth utilization can be checked to prove the strength of SSL/TLS.
6 Future Work

The main aim behind the thesis was to check the effect of SSL/TLS on the performance of network at the cost of security. The process can be continued to check effect on other protocols like LDAP etc. Furthermore, other parameters such as delay, throughput and bandwidth utilization can be checked to prove the strength of SSL/TLS.

Performance of a secure network can increase in the presence on SSL/TLS by improving the strength of SSL/TLS without degrading performance. Cryptographic algorithm with reduced key size might be used to provide maximum security, especially the size of session keys exchanged at session establishment might be reduced which is done using asymmetric encryption.

References


