Impact of SSL Security on Bandwidth and Delay in IEEE 802.11n WLAN Using Windows 7

Samad S. Kolahi, Yuqing Cao, Hong Chen
Unitec Institute of Technology, Auckland, New Zealand
skolahi@unitec.ac.nz
caoyuqing.nz@hotmail.com

***Abstract*—**IPSec (IP Security) and SSL (Secure Socket Layer) are the main technologies for securing communications via the Internet. In this paper, we present new results on the performance of SSL using Windows 7 operating system under IEEE802.11n wireless network. Enabling IPSec security results on average approximately 50% less TCP throughout while enabling SSL security results on average approximately 96% less TCP throughput compared to open system. In IPSec, 3DES-SHA encrypted system outperformed AES128-SHA encrypted system with a maximum difference of 2.40 Mbps for packet size of 1408. However, in SSL, AES128-SHA and 3DES-SHA had almost the same performance.

1. INTRODUCTION

Network security is very important with the increased usage of computers worldwide. The goal of network security is to provide confidentiality, integrity and authentication [1].

IPSec (IP Security) and SSL (Secure Socket Layer) are the two most powerful, secure and widely used VPN (Virtual Private Networks) technologies over Internet.

There is no study in literature to compare open system (no internet security), SSL, and IPSec for 802.11n, Windows 7, and using hard routers in the experiments. In this paper, we do performance analysis and compare IPSec with SSL using IPv4 under Windows 7 and 802.11n wireless network. Systems we compared are open system, 3DES-SHA (Triple Data Encryption Standard –Secure Hash Algorithm) and AES128-SHA (Advanced Encryption Standard-Secure Hash Algorithm) encrypted systems. We measure throughput and RTT (Round Trip Time) for both TCP and UDP.

The organization of this paper is as follows. In the next section the related work of IPSec and SSL is discussed. Section three covers the experimental setup. Section four covers information regarding the traffic measurement tool and the data generating. Section five covers the results produced and the last sections include the conclusions and future works.

2. RELATED WORK

Performance evaluation and comparison of network security different operating systems has been conducted by a number of researchers. Impact of WPA2 security on IPv6 was investigated in [1-4].

In 2002, Wei and Srinivas [5] presented a study of a secure wireless LAN based on the IPSec VPN tunneling protocol. Host to host IPSec was created between an Apple computer and an IPSec gateway. Their results demonstrated that the TCP throughput without IPSec was roughly three times than that with IPSec.

In 2003, Jin-Cherng and colleagues [6] conducted an investigation on router performance when using various services and hash/encryption algorithms such as AH-MD5, AH-SHA, ESP-3DES using IPSec. They tested the throughput of router before and after implementing IPSec. Their results showed that the throughput decreased 90.02% when 3DES-SHA of IPSec was implemented and decreased 88.23% when DES-SHA was implemented.

In 2004, Khanvilkar and Khokhar [7] investigated the influence of different types of VPN technologies on network performance using 100Mb/s fast Ethernet. Their results demonstrated that IPSec had 25% bandwidth utilization while SSL had only 4% bandwidth utilization as compared to open system.

In 2009, Narayan and colleagues [8] conducted a study of network performance of three VPN protocols (PPTP, IPSec, SSL) on Windows server 2003, Windows vista and Linux operating systems. Two VPN severs acted as software routers were used to connect to networks. Their studies concluded that the SSL gave the lowest throughput in Windows environment and IPSec was the least performer in Linux environment. Throughput values varied from 15 to 95 Mbps for IPSec, PPTP and SSL in Windows environment.

In 2010, Narayan and colleagues [9] conducted a research on network performance of different IPSec algorithms, namely DES, 3DES and AES on Windows 7，XP and Vista operating systems using soft routers. Their research showed that the network performances of the tested VPN mechanisms were mostly comparable and the operating systems they were implemented on mostly gave similar throughput with a few exceptions.

In 2013, IPSec versus bandwith for Linux and Windows was evaluated in [10-11]. We have included IPsec results for Windows 7 again to show SSL impacts the bandwith much more than IPSec.

There has been no work done to date on performance of open system, SSL under Windows 7 using networks connected by hard routers. The lack of available research on impact of SSL and IPSec was the main motivation behind this paper.

3. EXPERIMENTAL SETUP

The test-bed hardware setup remained constant for all experiments conducted and the test-bed diagram is displayed as Figure 1:

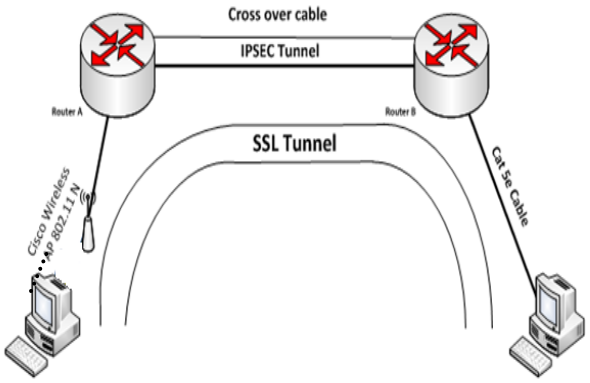

Figure 1: Network test-bed.

Two hard routers were connected via Cross over Cat 5e cable, one client machine was connected wirelessly via Cisco Linksys WAP4410N 802.11n Access Point (AP). The anther machine was directly connected to the Cisco 2811 router via Cat5e Cable.

The hardware benchmark was comprised of two computers with Intel® Core™ i5 2.80 GHz, 8.00 GB of RAM and two Cisco 2811 routers. For the efficient operation of Windows 7, an Air Live Wn-5000 wireless PCI NIC and a Western Digital Caviar 160 GB hard-drive were installed on the two workstations.

IPSec VPN is commonly setup SITE to SITE, which will establish the VPN tunnel between two routers. SSL VPN is commonly set-up Client to Server which will establish the tunnel from one computer to another via two routers.

In test-beds, Microsoft Windows 7 professional 64bit with SP1(Service Pack 1) was installed on the computer of left side and Microsoft Windows 2008 standard 64bit with SP1(Service Pack 1) was install on the receiving computer of right side.

For each test bed we implemented open system, IPSec and SSL measuring TCP and UDP throughput and RTT utilization. In all options, the wireless link had WPA2 (Wireless protected Access 2) security.

Throughput (the number of bits transmitted per unit time) depends on several factors in a network, such as process limitations and hardware design. In order to eliminate the effect of such conditions, hardware with same characteristics was used in all of the tests.

4. DATA GENERATION AND TRAFFIC MEASUREMENT TOOL

Netperf 2.4.5 [12] was selected as the tool to analyze the IPSec and SSL performances over 802.11n WLAN. Netperf can be used to measure the performance of many different types of networks. It creates and sends TCP and UDP packets in either IPv4 or IPv6 networks and provides tests for throughput and RTT.

To ensure high data accuracy, each test was repeated at least 30 runs and data averaged and runs continued until standard deviation of results was below 0.5% of the average. Each run contained at least one million packets.

5. EXPERIMENT RESULTS

The experiments were conducted to evaluate and compare the throughput and RTT for TCP and UDP on open system, SSL and IPSec (for both 3DES-SHA and AES128-SHA encrypted systems) using Windows 7 over 802.11n wireless network.

Figure 2 shows the TCP throughput comparison of open system (OS), IPSec and SSL for two encryption system. For TCP throughput, the bandwidth dropped when SSL or IPSec was implemented. IPSec systems had higher TCP throughput than SSL systems. Compared with open system, implementing IPSec made TCP throughput decrease by a maximum of 43.34 Mbps (decrease rate of 60.28%) for packet size of 1408 while implementing SSL made TCP throughput decrease by a maximum of 69.76 Mbps (97.03% decrease) for packet size of 1408. With IPSec security resulted on average approximately 50% less TCP throughout while enabling SSL security results on average approximately 96% less TCP throughput compared to open system.

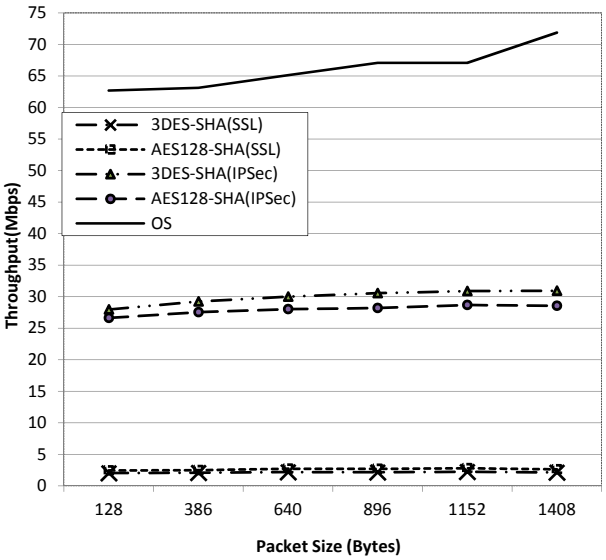

Figure 2: TCP Throughput Comparison of Open System, IPSec and SSL.

TCP throughput of IPSec was largely higher than that of SSL with a maximum difference of 28.82 Mbps for packet size 1408. In IPSec, 3DES-SHA encrypted system outperformed AES128-SHA encrypted system with a maximum difference of 2.40 Mbps for packet size of 1408. However, in SSL, AES128-SHA and 3DES-SHA had almost the same performance. Our result is similar to research results of Shashank and Khanvilkar [7]. They found that IPSec had about 25% bandwidth utilization while SSL had only 4% bandwidth utilization for fast Ethernet networks, meaning implementing SSL slows the network up to 6 times more than IPSec does.

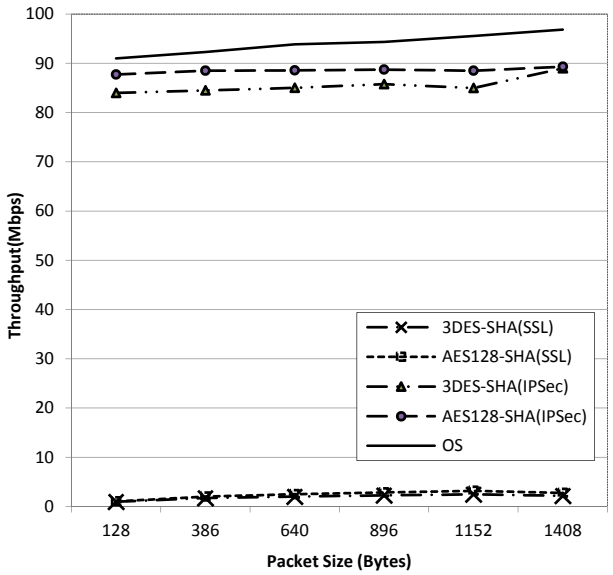

Figure 3: UDP Throughput Comparison of Open System (OS), IPSec and SSL.

Figure 3 shows UDP throughput comparison of open system, IPSec and SSL under Windows7 and 802.11n wireless network. It can be seen clearly that IPSec had higher UDP throughput than SSL. Compared with open system, implementing IPSec made UDP throughput decrease by a maximum of 10.54 Mbps (decrease of 11.03%) for packet size 1152 bytes where as implementing SSL made UDP throughput decease by a maximum of 94.66 Mbps (a decrease of 97.73%) for packet size of 1408 bytes. In addition, comparing IPSec and SSL, IPSec outperformed SSL with a maximum difference of 87.1 Mbps for packet size of 1408 bytes. In IPSec, AES128-SHA encrypted system outperformed 3DES-SHA encrypted system with a maximum difference of 3.99 Mbps for packet size of 1152 bytes. In SSL, AES128-SHA encrypted system again outperformed 3DES-SHA encrypted system with a maximum difference of only 0.7 Mbps for packet size of 386 bytes.

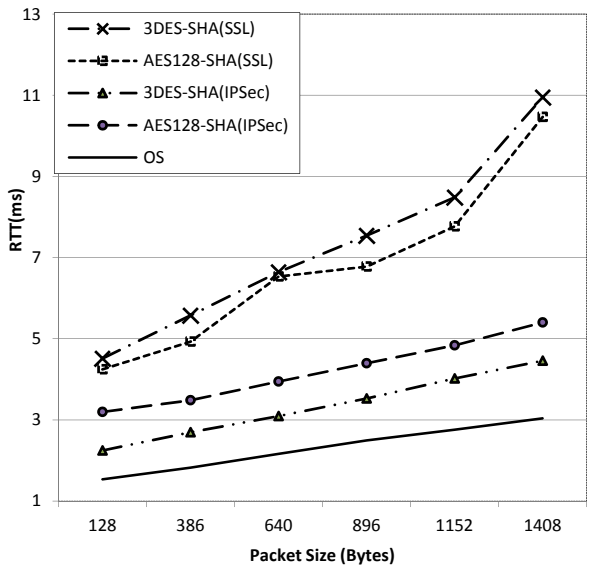

Figure 4: TCP RTT Comparison of Open System, IPSec and SSL.

Figure 4 shows TCP RTT comparison of open system, IPSec and SSL under Windows7 for 802.11n wireless network. It can be seen clearly that open system had the lowest RTT than other systems. In addition, IPSec had lower RTT than SSL. For TCP RTT, IPSec outperformed SSL with a maximum difference of 6.49 ms for packet size of 1408 bytes. In IPSec, 3DES-SHA encrypted system outperformed AES128-SHA encrypted system with a maximum difference of 0.95 ms for packet size 128. However, in SSL, AES128-SHA encrypted system had less delay than 3DES-SHA encrypted system with a maximum difference of 0.76 ms for packet size 386 bytes.

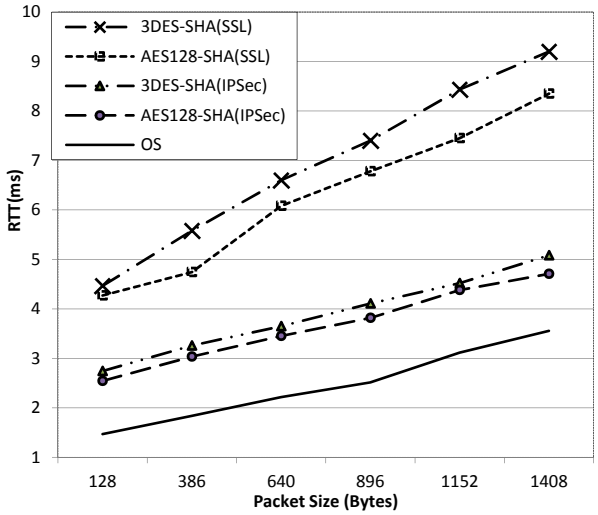

Figure 5: UDP RTT Comparison of Open System, IPSec and SSL.

Figure 5 shows UDP RTT comparison of open system, IPSec and SSL under Windows7 and 802.11n wireless network. It can be seen again that open system had the lowest RTT than other encrypted systems. In addition, IPSec had much lower UDP RTT than that of SSL. The highest RTT value was 3.5ms for open system, 9.1ms for SSL and 5.1ms for IPSec. IPSec outperformed SSL in UDP RTT with a maximum difference of 4.49 ms for packet size of 1408 bytes. In IPSec, AES128-SHA encrypted system had lower UDP RTT than that of 3DES-SHA encrypted system with a maximum difference of 0.38 ms for packet size of 1408 bytes. In SSL, AES128-SHA encrypted system again had lower UDP RTT than that of 3DES-SHA encrypted system with a maximum difference of 0.99 ms for packet size of 1152 bytes.

The UDP throughputs are higher than the TCP for all cases (open system, IPSec and SSL systems). This is due to UDP is a connectionless protocol and unlike TCP that is connection oriented, the UDP sender does not have to wait for acknowledgements because the receiver does not send any acknowledgment back to the source [13].

Figure 5 shows UDP RTT comparison of open system, IPSec and SSL under Windows7 and 802.11n wireless network. It can be seen again that open system had the lowest RTT than other encrypted systems. In addition, IPSec had much lower UDP RTT than that of SSL. The highest RTT value was 3.5ms for open system, 9.1ms for SSL and 5.1ms for IPSec. IPSec outperformed SSL in UDP RTT with a maximum difference of 4.49 ms for packet size of 1408 bytes. In IPSec, AES128-SHA encrypted system had lower UDP RTT than that of 3DES-SHA encrypted system with a maximum difference of 0.38 ms for packet size of 1408 bytes. In SSL, AES128-SHA encrypted system again had lower UDP RTT than that of 3DES-SHA encrypted system with a maximum difference of 0.99 ms for packet size of 1152 bytes.

The gain in TCP and UDP throughput and RTT values as packet size increases is likely due to the amortization of overheads associated with larger user packet sizes [14].

The lower throughput for both TCP and UDP when IPSec and SSL security is enabled (compared to open system) is due to encryption and decryption take up the CPU and memory and the data packets become longer because of higher overhead associated with encrypting [15].

6. CONCLUSION

Results showed that, for Windows 7 and 802.11n WLAN considered, enabling IPSec and SSL security can reduce bandwidth and increase delay. For IPSec and SSL, TCP throughput can decrease by a maximum of 60.28% and 97.03% respectively as compared to open system. The average bandwidth dropped was 50% (IPSec) and 96% (SSL). In UDP protocol, implementing IPSec, the throughput decrease by a maximum of 11.03% where as implementing SSL made UDP throughput decease by a maximum of 97.73%. For both TCP and USP, results showed that IPSec VPN had a much better throughput and RTT performance than SSL VPN.

7. FUTURE WORKS

In future, we plan to extend this study by incorporating more VPN technologies, such like PPTP and L2TP, and more operating systems, such as Linux. In addition, the performance comparison of IPv4 and IPv6 on different VPN technologies will be investigated.

REFERENCES

[1] P. Li, S. S. Kolahi, et al. “Effect of WPA2 Security on IEEE 802.11n Bandwidth and Round Trip Time in Peer-Peer Wireless Local Area Networks”. 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications, AINA Workshops 2011, pp. 777-782.

[2] S. S. Kolahi, S. Narayan et al. “The The Impact of Wireless LAN Security on Performance of Different Windows Operating Systems”, IEEE Symposium on Computers and Communications, 2008, pp. 260-264.

[3] S. S. Kolahi, P. Li et al. “WPA2 Security-Bandwith Trade-off in 802.11n Peer-Peer WLAN for IPv4 and IPv6 using Windows XP and Windows 7 Operating Systems”, 2012 IEEE Symposium on Computers and Communications (ISCC), 1-4 July 2012, pp. 575 – 579.

[4] S. S. Kolahi, H. Singla, et al., **“**The Influence of WPA2 Security on the UDP performance of IPv4 and IPv6 Using 802.11n WLAN in Windows 7-Windows 2008 Environment” 2011 Baltic Congress on Future Internet Communications (BCFIC Riga), 2011, p.50-53.

[5] Q. Wei and S. Srinivas, “IPSec-based secure wireless virtual private network”, MILCOM 2002. Proceedings, pp. 1107-1112.

[6] L. Jin-Cherng, C. Ching-Tien, et al. “Design, implementation and performance evaluation of IP-VPN”. 17th International Conference on Advanced Information Networking and Applications, 2003. AINA 2003, pp. 206-209.

[7] S. Khanvilkar and A. Khokhar, "Virtual private networks: an overview with performance evaluation," Communications Magazine, IEEE , vol.42, no.10, Oct. 2004, pp. 146- 154

[8] S.Narayan, K. Brooking, et al. “Network Performance Analysis of VPN Protocols: An Empirical Comparison on Different Operating Systems.” International Conference on Networks Security, Wireless Communications and Trusted Computing, NSWCTC '09, pp. 645-648.

[9] S. Narayan, M. Fitzgerald, et al. “Empirical network performance evaluation of IPSec algorithms on windows operating systems implemented on a test-bed”. IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), 2010, pp.1-4.

[10] S.S. Kolahi, Y.R. Cao, and H. Chen, “Bandwidth-IPSec Security Trade-off in IPv4 and IPv6 in Windows 7 Environment”, Second International Conference on Future Generation Communication Technologies (FGCT 2013), December 12-14, 2013, London, UK, pp. 148-152.

[11] S.S. Kolahi, Y. Cao, and H. Chen**,** “Evaluation of IPv6 with IPSec in 802.11n WLAN Using Fedora 15 Operating System”. IEEE Symposium on Computers and Communication. 2013, Split, Croatia, pp. 203-206.

[12] Netperf 2.4.5 Available: http://www.netperf.org/netperf/NetperfNew.html

[13] S.S. Kolahi and P. Li, “Evaluating IPv6 in Peer-to-Peer 802.11n Wireless LANs,” IEEE Internet Computing, Vol. 15 Issue 4, 2011, p70-74.

[14] S. Zeadally and L. Raicu, “Evaluation IPv6 on Windows and Solars,” Internet Computing, IEEE, vol.7, no. 3, 2003, pp. 51-57.

[15] E. Barka; K. Shuaib; H. Chamas, "Impact of IPSec on the Performance of the IEEE 802.16 Wireless Networks," New Technologies, Mobility and Security, 2008. NTMS '08, 2008 , pp.1-6.