International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp. 363-376
http://dx.doi.org/10.14257/ijsia.2014.8.3.36

Secure on Demand IP based Connection (SEDIC) for Virtual Private Networks(VPNs)

Saadiah Yahya[1], Mohamed Sulaiman Sultan Suhaibuddeen[2], Zainab Abu Bakar[2] and Ahmad Yusri Dak[2]

[1]Malaysia Institute of Transport (MITRANS), Universiti Teknologi MARA
Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA
40450 Shah Alam, Selangor, Malaysia
[2]Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA
40450 Shah Alam, Selangor, Malaysia
[1]saadiah@tmsk.uitm.edu.my, [2]msss@melaka.gov.my;{zainab; yusri}@tmsk.uitm.edu.my

Abstract

Diverse security measures are used to improve security entropy including the introduction of secure port services, better tunneling protocols and complex encryptions cryptography. Most of these do not address the fundamental of the security risk which is to avoid newly discovered exploits and protect credential from man-in-the-middle attack. In this study, experiments involving three types of existing environment, which include insecure connection as a basis, working against pre-shared key and public-key infrastructure (PKI), are being modeled. A new framework named SeDIC has been introduced to overcome the limitations and address the current security weaknesses. In this new implementation, forward secrecy is maintained since the key for authentication is only valid once and this will deny replay attack. This study proves that secure internet application is possible and the user can have the freedom to use the lowest cryptographic entropy to perform their on-line transactions. Having complex mathematical algorithms such as Elliptic Curve Cryptography (ECC) for tunneling, or even multilayer authentication system alone will not address the potential risk, besides prolonging the time for intruder in gaining unauthorized access.

Keywords: *PKI, cryptography, SeDIC, Security Measure, VPN*

1. Introduction

Confidential and sensitive application systems such as online banking and stock trading are transacted on the internet. The processes require remote management of high secure servers [1]. All services running on a server are represented by certain ports in handling the request. These open ports on servers welcome attackers to scan the port to check services for vulnerable information, especially for malfeasant motives [2-6] on zero days exploits.

2. Statement of Problems

Information flows between server and clients are open for eavesdropping by man-in-the-middle to emulate certain identity, gain secret access of unauthorized transacted information or enable hijacking of the said session as such, the current methods are arguably not secured [7-12]. Existing authentication system which use traditional Secure Socket Layer/Transport Layer Security (SSL/TLS), is also weak, where it relies heavily on user identification (ID)

ISSN: 1738-9976 IJSIA

and password upon the SSL/TLS session establishment [11, 13-16]. Speed and flexibility usually have a negative relationship with security. For a system to be secured, there is a need to impose additional overheads which are excessive and not efficient for maintaining its authentication and confidentiality [17-21].

There are various mechanisms introduced by information security technologists to ensure the communication is only experienced by the approved parties. Until now, there are no full-proof security systems that can be considered the best protection ever [22, 23]. The best technology used to perform a secure transaction at the moment is Virtual Private Network (VPN) [24, 33]. This technology has evolved from Layer 2 during Asynchronous Transfer Mode (ATM) and Frame Relay into Layer 3 which provides better flexibility and a cost-effective way of establishing secure tunnels [25].

3. The Objectives and Methods

This paper examines various security elements, ranging from VPN method, modification of Diffie-Hellman encryption algorithm [26] which provides on demand capability to the current VPN system, as well as providing better, faster yet secure tunneling between the two nodes comprising the user and the server. A new VPN variant which overcomes issues stated above is then designed and its performance is evaluated against other popular VPN technologies. Five VPN technologies namely Layer 2 Tunneling Protocol (L2TP), Generic Routing Encapsulation (GRE), Internet Protocol Security (IPSec), Open VPN and Multiprotocol Label Switching (MPLS) were being deployed for evaluation. Each of these technologies was studied in the areas of the encapsulation techniques, covering multiplexing, signaling, data security, multiprotocol support, frame sequencing, tunnel maintenance and quality of service capability. In the second objective the following four steps were set up.

i. The development of a client application which will initiate and tunnel secure connection to the server. The server port and services will only open once the client is validated.

ii. The connectivity between both of the connecting hosts, utilizes better cryptography mechanism protecting the authentication process to produce on-the-fly one time encryption key for per-session based server-client transmission.

iii. The current authentication system will be replaced by using verifier based method at both hosts and user-end instead of traditional user ID and password upon SSL/TLS establishment.

Finally, the new VPN variant performance were compared against other popular VPN technologies.

The efficiencies improvement is the key of this research, where the overall network and process overhead will be reduced which leads to faster communication transmission without compromising security

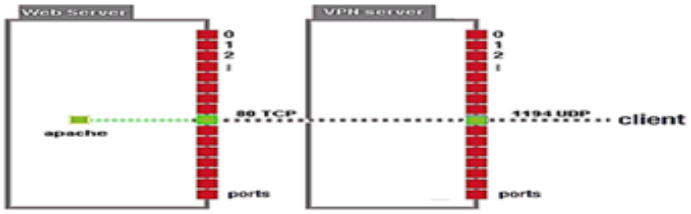


Figure 1. Typical VPN Mode - Client to Server Connection

The typical VPN connection as in Figure 1 provides an interim mediator which authenticates the client prior accessing the resource server. The concept between Plain Mode and Typical VPN Mode is the same where the running services are exposed to the client which sends a connection request. Another similarity on both of these figures is that the resource servers are running continuously even when they do not serve any connection request.

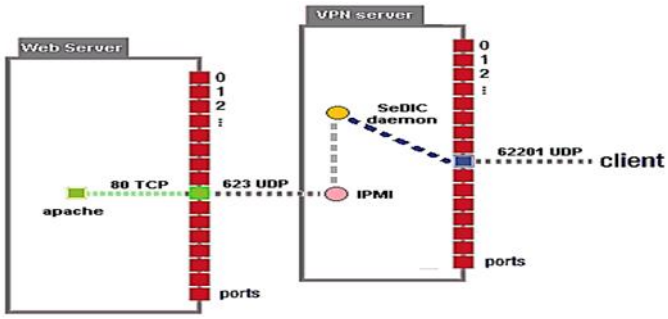


Figure 2. SeDIC Mode - Client to Server Connection

As shown in Figure 2, there are two major system enhancements that could be made in OpenVPN. This involves modification of the authentication block as well as the encryption block [27].

There are various client applications available to establish a connection from a client to the server. In order to have a secure link establishment, the best mechanism is by using certificates, which reside in the host or in a smartcard [28] Studies have shown that to perform PKI especially via asymmetrical means, this needs high overheads [29]. However, we cannot utilize the raw way of authentication via username and password, since this is the weakest authentication method, being the lowest in the entropy. Therefore, this research will modify the TLS cryptographic module library to incorporate Secure Remote Password (SRPv6) to become an alternative key exchange and encryption module. This may prove to be as good as using PKI, besides having low processing overheads. Nevertheless, the default SRPv6 has three main issues. One of which is from the server: if an attacker learns a user's SRP verifier (e.g., by gaining access to a server's password file), the attacker can masquerade as a real server to that user, and can also attempts a dictionary attack to recover that user's password [30]. Another way is from the client where an attacker could repeatedly contact an SRP server and try to guess a legitimate user's password. Thirdly, is when the client's user name is being sent as clear text in the Client Hello message.

Another security consideration is the server hosting the VPN service. Normally a hacker can easily perform a network scan to know what service is running at what port, and if there is an exploit available in any of the component, the server could be easily compromised. This research will also integrate on demand concept, by utilizing Single Packet Authorization (SPA) complementing with SRPv6. The modification shall be done at the client software as well as in the daemon running in the server, especially the user credential. The default SPA uses Phase-shift keying (PSK) which is stored in the configuration file. This research will also replace the PSK with SRP. In order to maintain the identity of the connecting host and to avoid session hijacking especially from the host under Network Address Translation (NAT), a heartbeat alike protocol is used to periodically check the authenticity of the host.

This research addresses these issues by having a separate authentication module by using SPA which first establishes a secure tunnel. The next step is renegotiating an SRP-

authenticated connection with the handshake protected by the first connection utilizing username which is being encapsulated within the SPA packet. By having on demand functionalities, rather than technically hiding the port and services, this research shall also combine an intelligent system to the network which is to 'awake' the required server upon request, by using Intelligent Platform Management Interface (IPMI) protocol.

Vanila VPN Process Flow shows the common steps of how a client is able to get authenticated prior joining the requested network. It starts when both the Client and Server negotiate for the protocol and cryptographic, followed by the authentication done by the user. Once this is done, the said client joins the remote network. In the case of SeDIC VPN Process Flow, the client will send a single packet as the passive authorization. Without the interaction of the user, if and only when the packet qualifies the required criteria, the VPN port shall be opened to undertake further active authentication from the user. Upon getting the correct credentials, the server shall send an awake signal to the requested server and later create a firewall rule so that the client could connect. Further at the specified interval, the connection will be evaluated for confirming the identity of the connecting client. If a valid response is given, the link is maintained. If there is no response given by the client, the link will be abandoned.

Testing Parameters are in accordance with RFC2544 which is the benchmarking methodology for network interconnects devices. Penetration test involves an active analysis of the system for any potential vulnerabilities which may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities using Network Mapper (NMAP), AMAP, TCPDUMP, and NetCat.

4. Experimentation and Data Collection

In order to verify the research outcome, there have been five scenarios of data collection, which are:

No VPN Connection; Vanilla VPN with symmetrical encryption Connection; Vanilla VPN with asymmetrical encryption Connection; Modified VPN with SPA; and SRP encryption Connection (SeDIC). The attributes which have been gathered from the Client CPU utilization are overhead, round-trip time, jitter, TCP throughput, server CPU utilization, probability of error, time between errors, and link utilization.

In the encapsulation process, there are potentially three compounded overheads which shall be imposed to every VPN packet encounter overhead. The first overhead derived from when every payload sent through the VPN tunnel is packed with various protocols headers and trailers to form a routable packet. The second overhead derived from the authentication and encryption ciphers used to secure the tunnel. Finally, the third overhead derived from the use of compression to reduce the amount of data transmitted [31].

5. Analysis and Results

This research had gathered various security issues derived from the evolution of computer networking and diverse secure connectivity techniques being reviewed by studying the most common VPN used comprising L2TP, GRE, IPSec, OpenVPN and MPLS. These technologies had also undergone a series of improvement to become the current version. Generally these VPN techniques share similar three building blocks which are Tunneling, Credential and Encryption. However, a majority of these technologies are confined into two ways in order to improve security, which are either having more complex mathematical

equations or producing multi-layered security. Two most common encryption methods are being evaluated, which are asymmetrical certificated based technique and symmetrical encryptions pre-shared key-based technique. A connection without any encryption is also measured for benchmarking the findings. After reviewing all the security issues, a new method SeDIC (originating from OpenVPN) was introduced and tested. The findings from the analysis of the test data revealed that SeDIC addresses all matters faced by most of the VPN techniques around.

A client which initiates a tunnel secure connection to the server only when requested was first experimented. There are two authentication techniques involved specifically on the client that will perform passive authentication using a modified SPA. Upon the valid packet, the connection port is opened for the client to further issue active authentication which eventually will establish the connection. By using this technique, an attacker will find it impossible to perform any strike due to the nonexistence of some vital information on the victim's server. Next, a better cryptography mechanism which protects the authentication process to produce on-the-fly one time encryption key for the per-session based server to client transmission was deployed. Instead of using the old Diffie–Hellman for the key exchange to take place, a new method SRP was being used. As the Diffie-Hellman system is very resource hungry, and uses the old method of authentication, where actual user credential is being transmitted across to the server. This would enable a man-in-the-middle to sniff the packet and later decrypt it in a motive to gain an authorized access to the server [30-34]. By having this key exchange protection, the information which flows between two computers is not visible for eavesdropping by the man-in-the-middle.

Experimentations were conducted based on the existing VPN technologies by using plain connectivity as the benchmark for the best scenario, a newly introduced VPN was also tested to determine its rank against the other two technologies. These test results were analyzed and measured using related statistical methods. In determining the distribution of the result, Normality Test was used; Kruskal-Wallis was deployed to validate consistencies of the test after the same tests were carried out multiple times; Dunn's Test was performed to determine the group likelihood of each VPN technologies. Cronbach's Alpha was performed in order to confirm whether the representative data were sufficient so that a general assumption can be made. The basic tool in identifying the host availability was tested using ping program where 8 ICMP packets were sent and the reply were identified.

All the available encryption systems had successfully been broken [35], therefore, this research stresses that most of the research in cryptography as well as in the security systems are either making the mathematical equation more complex or creating multi-layer security system. However, it will not stop any attacker from gaining access into the protected system, but it only delays the time taken to attack, with nowadays high performance computing system especially the GRID, it can be easily used to predict or brute force attack into any security system. In this research a new framework was designed by looking at every process so that it shall provide a real secure system. This affirms that the current SSL/TLS authentication and encryption system are weak because they use User ID and Password. The findings show that this research performs more efficient CPU utilization with better network throughput without compromising the security level of the system, this had overcome the main issue of excessive usage of computer resource which is the overhead imposed in order to maintain authentication and confidentiality system.

In performing various test, this research uses 512 bytes as the basis, the reason is that "Every internet module must be able to forward a datagram of 68 octets without further fragmentation. Every internet destination must be able to receive a datagram of 576 octets either in one piece or in fragments to be reassembled.", therefore the closes frame size is 512

bytes. All the data gathered statistically shows that the data are non-normal, where the snapshot at 512 bytes for various methods results the same results giving P-values less than 0.005

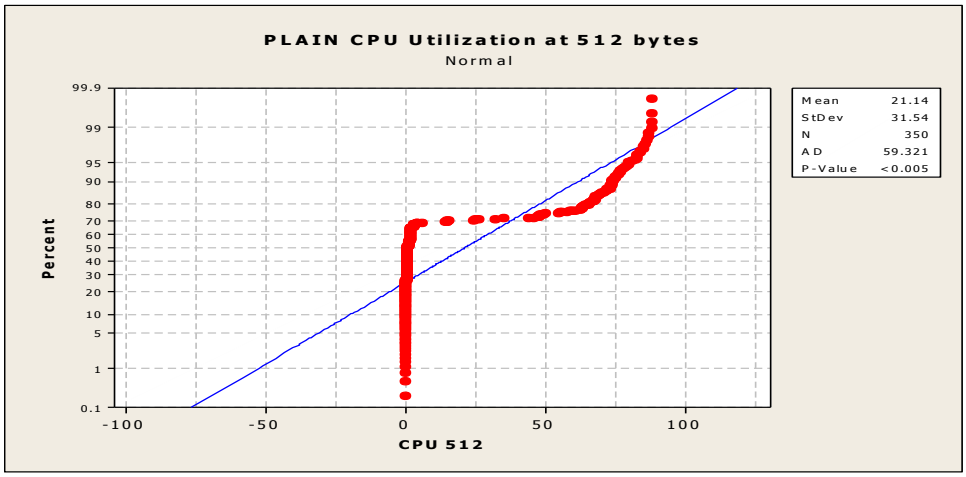


Figure 3. Normality Test on CPU Utilization at 512 bytes Frame Size on Non Secure Mode

A normality test conducted on samples data running on PLAIN system at 512 windows frame resulted P-Value less than 0.005 as Figure 3, which tells these data are non-normal. Similarly, normality test conducted on samples data running on SeDIC system at 512 windows frame also resulted with P-Value less than 0.005 as shown in Figure 4, which signifies these data are also non-normal. Normality test on CPU Utilization at 512 bytes Frame Size on Pre Shared Key Mode and on Certificate Mode also depicts non-normal data. Due to the non-normal result in the normality test, in checking the consistencies of the result, Kruskal-Wallis test is used. In this non secure analysis, the tests were conducted five times under similar testing attributes, in each test 50 CPU readings are taken, which totalling to 350 readings.

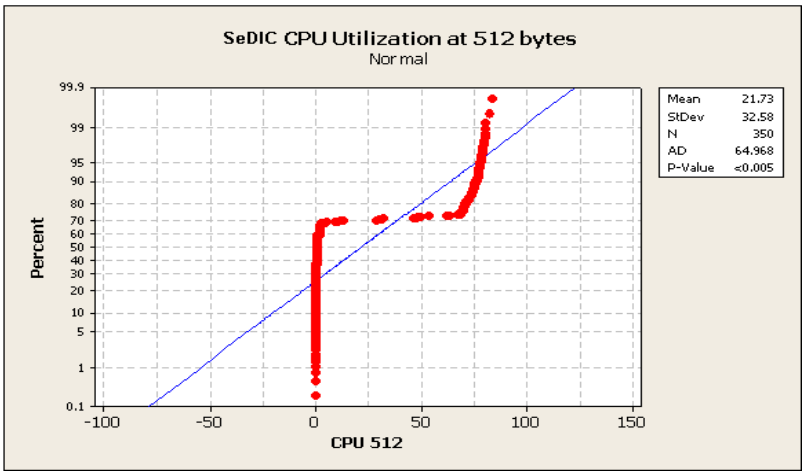
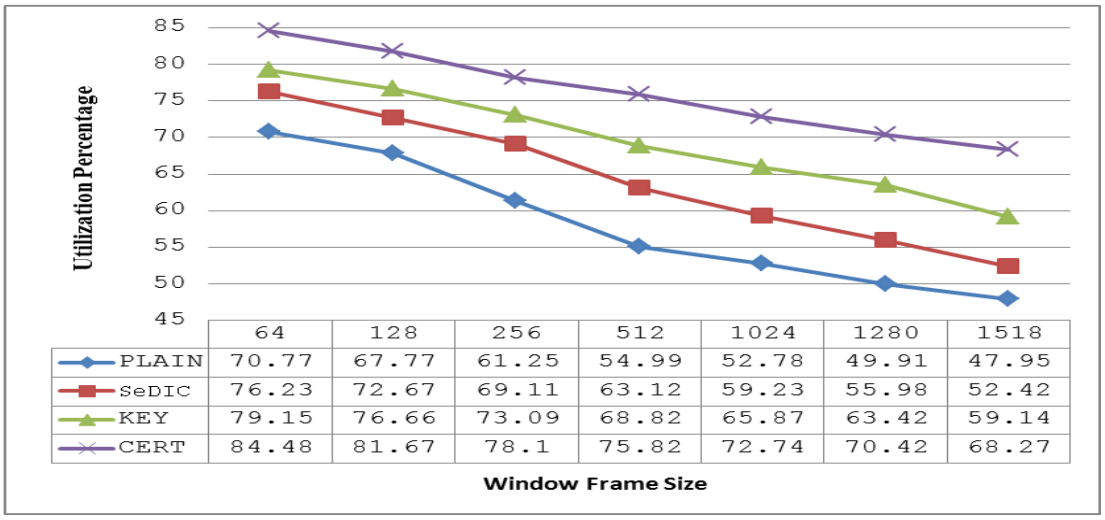


Figure 4. Normality Test on CPU Utilization at 512 bytes Frame Size on SeDIC Mode

The CPU readings on both the client and server side shows declining effect when bigger frame size allowed, as shown in Figure 5 and Figure 6, in other words the bigger the frame size are allowed, relatively the lower the CPU readings will become. Significant slope happened after 512 bytes.



	64	128	256	512	1024	1280	1518
PLAIN	70.77	67.77	61.25	54.99	52.78	49.91	47.95
SeDIC	76.23	72.67	69.11	63.12	59.23	55.98	52.42
KEY	79.15	76.66	73.09	68.82	65.87	63.42	59.14
CERT	84.48	81.67	78.1	75.82	72.74	70.42	68.27

Figure 5. Client CPU Utilization

This result as in Figure 5 shows readings of client CPU utilization at various frame size starting from 64 bytes until 1,518 bytes as a guideline from RFC1544. The best reading is SeDIC, which is a new method developed by this research; followed by KEY, which is a tunneling method which used a pre-shared key being symmetrical encryption scheme; and CERT, which used certificate based being asymmetrical encryption scheme. As can be seen in the above figure the wider the frame size, the lower the CPU utilization readings, and both PLAIN and SeDIC are able to excel better than KEY and CERT. PLAIN improves 32% from 64 bytes to 1518 bytes, SeDIC improves 31%, KEY improves 25% and CERT improves 19%. Looking at frame size columns shown in Table 1, SeDIC imposes the lowest among the other method, followed by KEY and CERT.

Table 1. Client CPU Utilization Differences

	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes	1280 bytes	1518 bytes
SeDIC	8%	7%	13%	15%	12%	12%	9%
KEY	12%	13%	19%	25%	25%	27%	23%
CERT	19%	21%	28%	38%	38%	41%	42%

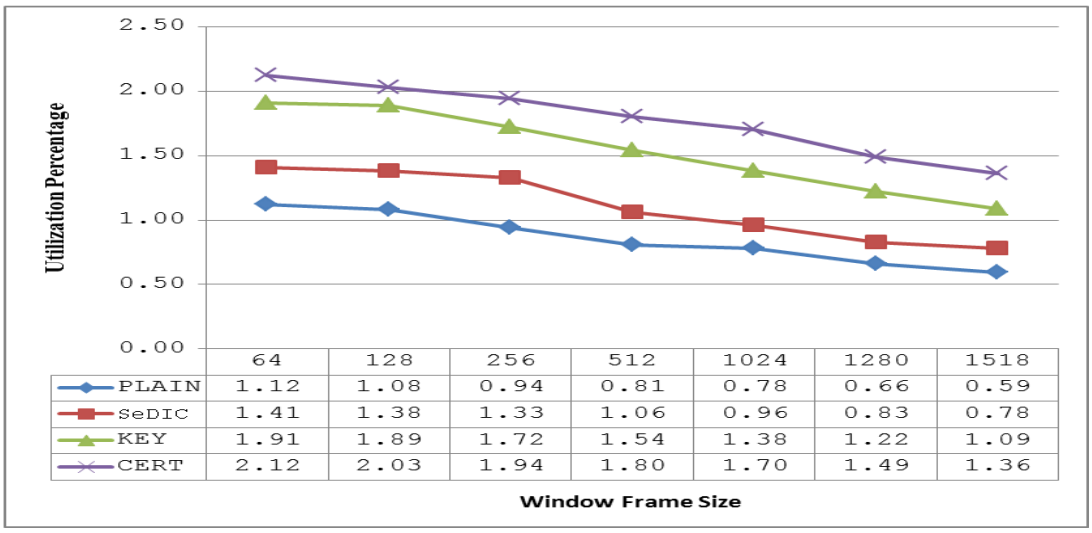


Figure 6. Server CPU Utilization

On the server side as shown in Figure 6 reflects the same pattern, where the best reading is SeDIC, followed by KEY and CERT. In term of the improvement, PLAIN as being a base point records improvement at 47% from 64 bytes frame size to 1,518 bytes frame size; followed by SeDIC at 45%; followed by KEY at 43% and CERT at 36%. As the figures shows on the client side, the server side also shows similar pattern that the lowest impact to the CPU as the table below is SeDIC followed by KEY and CERT.

Table 2. Server CPU Utilization Differences

	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes	1280 bytes	1518 bytes
SeDIC	26%	28%	41%	31%	23%	26%	32%
KEY	71%	75%	83%	90%	77%	85%	85%
CERT	89%	88%	106%	122%	118%	126%	131%

In measuring the connectivity overhead, a reading is taken for the transmission between the client and server. As shown in Figure 7, the best reading comparing with the base point of PLAIN is SeDIC followed by KEY and CERT. In term of improvement between 64 bytes frame size to 1,518 bytes frame size, PLAIN as the base improve 55%, followed by SeDIC at 51%, then followed by KEY at 42% and the last is CERT at 36%. Examining at the verticals, SeDIC impose the lowest overhead compared to KEY and CERT as table below in Table 3: Overall Network Overhead Differences.

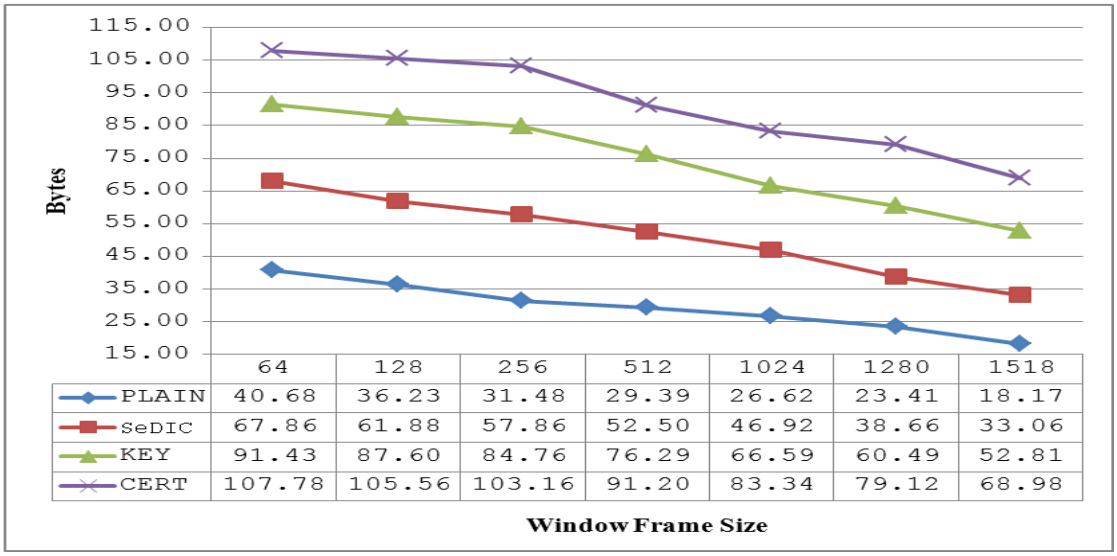


Figure 7. Network Transmission Overall Overhead

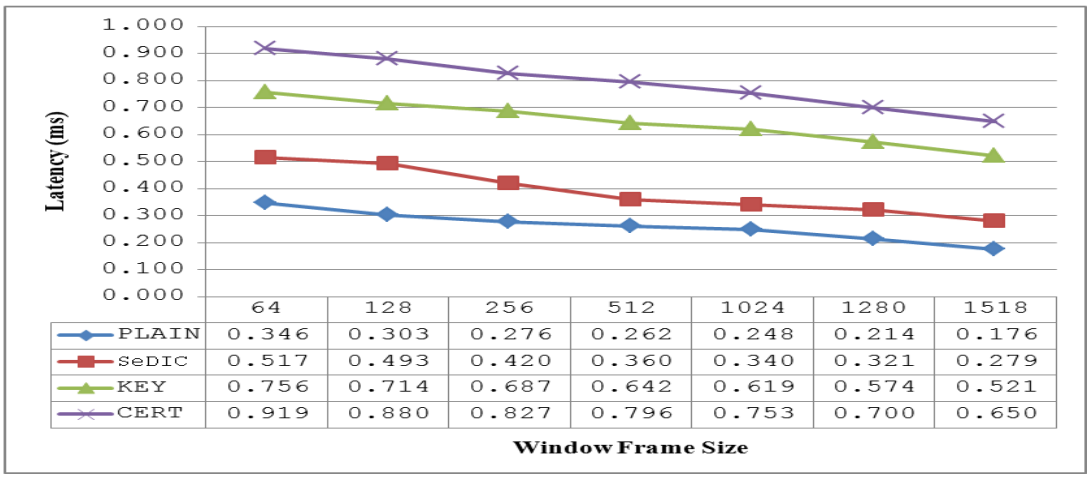
Table 3. Overall Network Overhead Differences

	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes	1280 bytes	1518 bytes
SeDIC	67%	71%	84%	79%	76%	65%	82%
KEY	125%	142%	169%	160%	150%	158%	191%
CERT	165%	191%	228%	210%	213%	238%	280%

Figure 8 shows the latency reading for the network transmission between the client and the server; again this finding also have similar pattern with the previous tests being done, compared to the base point which is PLAIN, SeDIC records the best reading, followed by KEY and CERT. The improvement between 64 bytes frame size towards 1,518 frame size shows the base point PLAIN at 49%, SeDIC at 46%, KEY at 31% and CERT at 29%. The latency readings also show at every column, SeDIC imposes the lowest impact on the network latency followed by KEY and CERT as shown in Table 4.

Table 4. Overall Network Latency Differences

	64 bytes	128 bytes	256 bytes	512 bytes	1024 bytes	1280 bytes	1518 bytes
SeDIC	49%	63%	52%	37%	37%	50%	59%
KEY	118%	136%	149%	145%	150%	168%	196%
CERT	166%	190%	200%	204%	204%	227%	269%



	64	128	256	512	1024	1280	1518
PLAIN	0.346	0.303	0.276	0.262	0.248	0.214	0.176
SeDIC	0.517	0.493	0.420	0.360	0.340	0.321	0.279
KEY	0.756	0.714	0.687	0.642	0.619	0.574	0.521
CERT	0.919	0.880	0.827	0.796	0.753	0.700	0.650

Figure 8. Overall Network Latency

6. The Significance of this Study

Both security and flexibility offered in this study makes it possible for mobile users who are on the move to access computer resources securely without the need of any additional hardware or token key. Traditionally in the market, a TAC generator gadget is used to generate the token key for the additional authentication. This gives extra hassle to users to bring and protect the said device wherever they go but will not guarantee or enhance the security after all.

Most of the studies had shown that asymmetrical encryption gives the highest security level; this type of encryption uses certificate based encryption. The higher the security is needed, the higher certificate bits should be imposed. Crypto export law had prevented higher bits rate in some developed countries. The findings of this study had shown that the certificate-based method gave a better security level compared to the asymmetrical method. This study had provided statistical data in showing efficient resource usage on both CPU and network load, without compromising the security level. Here the security is even better and the resource needed is lower than the available solutions. These findings contradict with the current assumption that the computer resource will be sacrificed in order to have a higher security level. A modification in the building blocks had made an effective security possible with very minimum overheads.

7. Conclusion and Future Work

This study has laid the building blocks of VPN and conducted comparative analysis in finding its weakness. In fulfilling the needs from this era, an on-demand concept is being introduced which gives synergy to a newly developed framework and prototype called SeDIC. This study has proven that having more complex or multi-factored authentication system does not guarantee the security. Another understanding proven otherwise is that, the higher the security, the higher resource overhead needed.

The way the client-server communication in future is foreseen will not be confined into service serving on certain ports. Instead all the traffic will be unique and authenticated at the application level from the client through the network until it reaches the resource server. The server later will validate the client request and return the entreaty with the information needed without the need of assigning fixed port-based resource serving.

At the moment, various identity validation processes are done at the silo basis where there could be validated at the operating system level, application level, network level as well as the remote resource level. On the other hand, central identity management processes are being developed either categorized as Single Sign-On or Centralized Authentication System. The new concept which is being tested by various software vendors is OpenID, but there is yet inter-operability between applications with the appliances. These missing gaps will always potentially invite attempt for unauthorized access by manipulating and planting broker agents.

This study has experimented and managed only one resource server, but in the production environment, it involves a well-connected computer grid presenting on-demand load balanced system which has the intelligence to provide a unique demand by users automatically. A trust relationship needs to exist between the client and the resource daemon, the daemon with the servers, as well as the server and other servers. Having the mobile user to securely connect into the resource server with very flexible way is foreseen as the enabler of secure cloud computing initiatives; nevertheless, the impact that it may imposed once compromised.

Acknowledgements

This research is sponsored in part of grant from Ministry of Higher Education (MOHE), Malaysia and Research Management Institute (RMI), Universiti Teknologi MARA (UiTM), Shah Alam, Malaysia for the Grant No 600-RMI.

References

[1] C. K. Tan and Capella, "Remote Server Management using Dynamic Port Knocking and Forwarding", Special Interest Group in Security and Information Integrity (SIG^2) - http://www.security.org.sg/code/sig2portknock.pdf, **(2004)**.
[2] J. Regan, "An Introduction to Using Linux as a Multipurpose Firewall", Linux Journal, Issue, vol. 71, **(2000)**.
[3] A. D. Smith and W. T. Rupp, "Issues in cybersecurity; understanding the potential risks associated with hackers/crackers", Information Management & Computer Security, vol. 10, no. 4, **(2002)**, pp. 178-183.
[4] G. Aloisio, M. Cafaro, I. Epicoco, S. Fiore, D. Lezzi, M. Mirto and S. Mocavero, "Resource and Service Discovery in the iGrid Information Service", Lecture Notes in Computer Science - Computational Science and Its Applications – ICCSA, Springer Berlin / Heidelberg, **(2005)**.
[5] K. Ingols, R. Lippmann and K. Piwowarski, "Practical Attack Graph Generation for Network Defense", Computer Security Applications Conference, 2006. ACSAC '06. 22nd Annual, Issue Date: **(2006)** December, pp. 121-130.
[6] J. Maassen and H. E. Bal, "Smartsockets: solving the connectivity problems in grid computing", Proceedings of the 16th international symposium on High performance distributed computing, ACM New York, NY, USA, **(2007)**.
[7] F. D. Li, T. Hanks, S. Meyer and D. Traina, Generic Routing Encapsulation (GRE. Retrieved 01 March 2010, from http://www.ietf.org/rfc/rfc2784.txt, **(2000)**.
[8] R. Gennaro, "Multi-trapdoor Commitments and Their Applications to Proofs of Knowledge Secure Under Concurrent Man-in-the-Middle Attacks", Lecture Notes in Computer Science - Advances in Cryptology – CRYPTO 2004, Springer Berlin / Heidelberg, **(2004)**, pp. 283-303.
[9] N. Asokan, V. Niemi and K. Nyberg, "Man-in-the-Middle in Tunnelled Authentication Protocols", Lecture Notes in Computer Science - Security Protocols, Springer Berlin / Heidelberg, **(2005)**, pp. 28-41.
[10] H. Xia and J. Carlos Brustoloni, "Hardening Web browsers against man-in-the-middle and eavesdropping attacks - SESSION: Security through the eyes of users", International World, **(2005)**.
[11] R. Oppliger, D. Basin, A. Rodenhaeuser and B. Kaiser, "A Proof of Concept Implementation of SSL/TLS Session Aware User Authentication (tls-sa)", In Braun, T. Carle, G. & Stiller, B. editors, Kommunikation in Verteilten Systemen, Informatik Aktuell, **(2007)**, pp. 225-236.
[12] G. Hao and H. Tao, "Principle of and Protection of Man-in-the-middle Attack Based on ARP Spoffing", Journal of Information Processing Systems, vol. 5, no. 3, **(2009)**, pp. 131-134.
[13] P. Persiano and I. Visconti, "User privacy issues regarding certificates and the TLS protocol: the design and implementation of the SPSL protocol", Proceedings of the 7th ACM conference on Computer and communications security, Conference on Computer and Communications Security, Athens, Greece, **(2000)**, pp. 53-62.

[14] A. Adelsbach, S. Gajek and J. Schwenk, "Visual Spoofing of SSL Protected Web Sites and Effective Countermeasures", Lecture Notes in Computer Science-Information Security Practice and Experience, vol. 3439, **(2005)**, pp. 204-216.
[15] C. Castelluccia, E. Mykletun and G. Tsudik, "Improving secure server performance by re-balancing SSL/TLS handshakes", - SESSION: Security protocols, Proceedings of the 2006 ACM Symposium on Information, computer and communications security, ASIAN ACM Symposium on Information, Computer and Communications Security, Taipei, Taiwan, **(2006)**, pp. 26-34.
[16] H. K. Lee, T. Malkin and E. Nahum, "Cryptographic strength of ssl/tls servers: current and recent practices", Proceedings of the 7th ACM SIGCOMM conference on Internet measurement - SESSION: Security and anomaly detection, Internet Measurement Conference, San Diego, California, USA, **(2007)**, pp. 83-92.
[17] R. Hauser, T. Przygienda and G. Tsudik, "Lowering Security Overhead in Link State Routing", Computer Networks: The International Journal of Computer and Telecommunications Networking Special issue on computer network security, **(1999)**, pp. 885-894.
[18] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck and M. B. Srivastava, "On Communication Security in Wireless Ad-Hoc Sensor Networks", Proceedings of the 11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, WETICE, IEEE Computer Society, Washington, DC, USA, pp. 139-144.
[19] H.-C. Speel, "Meet OpenVPN: Connecting road warriors with a full-blown open-source VPN solution", Linux Journal Article, vol. 7949, **(2004)**.
[20] T. Xie and X. Qin, "Enhancing Security of Real-Time Applications on Grids Through Dynamic Scheduling", Lecture Notes in Computer Science - Job Scheduling Strategies for Parallel Processing, Springer Berlin / Heidelberg, vol. 3834, **(2005)**, pp. 219-237.
[21] F. Qin, C. Wang, Z. Li, H.-S. Kim, Y. Zhou and Y. Wu, "LIFT: A Low- Overhead Practical Information Flow Tracking System for Detecting Security Attacks", Proceedings of the 39th Annual IEEE/ACM International Symposium on Microarchitecture, International Symposium on Microarchitecture, **(2006)**, pp. 135-148.
[22] G. C. Dalton II, K. S. Edge, R. F. Mills and R. A. Raines, "Analysing security risks in computer and Radio Frequency Identification (RFID) networks using attack and protection trees", International Journal of Security and Networks, vol. 5, no. 2-3, **(2010)** March, pp. 87-95.
[23] Y. P. Kosta, U. D. Dalal and R. Kumar Jha, "Security Comparison of Wired and Wireless Network with Firewall and Virtual Private Network", (VPN. 2010 International Conference on Recent Trends in Information, Telecommunication and Computing, Kochi, Kerala, India, **(2010)**.
[24] H. Burch and C. Chase, "Monitoring Link Delays With One Measurement Host", SIGMETRICS Performance Evaluation Review, vol. 33, no. 3, **(2005)**, pp. 10-17.
[25] V. Boyko, P. MacKenzie and S. Patel, "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman", Lecture Notes in Computer Science Eurocrypt 2000, Retrieved 15 April 2009 from http://www.iacr.org/archive/eurocrypt2000/1807/18070157-new.pdf, **(2000)**.
[26] M. Bishop, "Introduction to Computer Security", Addison Wesley, Pearson Education, **(2005)**.
[27] P. Venkateswari and Purusothaman, "Comparative Study of Protocols Used for Establishing VPN", International Journal of Engineering Science and Technology, vol. 1, no. 3, **(2009)**, pp. 160-165.
[28] M. Nazri Ismail and M. Taha Ismail, "Analyzing of Virtual Private Network over Open Source Application and Hardware Device Performance", International Journal of Computational Cognition, vol. 8, no. 2, June **(2010)**.
[29] D. M. Pointcheval and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attacks", Lecture Notes in Computer Science. Retrieved 14 April 2009 from http://www.iacr.org/archive/eurocrypt2000/1807/18070140-new.pdf, **(2000)**.
[30] M. Bellare, D. Pointcheval and P. Rogaway, "Authenticated Key Exchange Secure Against Dictionary Attack", Eurocrypt, **(2000)**.
[31] S. Khanvilkar and A. Khokhar, "Virtual Private Networks: An Overview with Performance Evaluation", IEEE Communication magazine, vol. 42, no. 10, **(2004)**, pp. 146-154.
[32] M. Bellare, R. Canetti and H. Krawczyk, "A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols", Proc. of the 30th STOC. ACM Press, New York, **(1998)**.
[33] B. Schneier, "Secrets & Lies: Digital Security in a Networked World", 1st edition, John Wiley & Sons, Inc., New York, NY, USA, **(2000)**.
[34] M. D. Abrams and H. J. Podell, "Local area networks", Abrams MD, Jajodia S & Podell HJ (eds) Information Security: An Integrated Collection Of Essays, IEEE Computer Society Press, Los Alamitos, CA, **(1995)**.
[35] M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution", CRYPTO '93, LNCS 773, Springer-Verlag, Berlin, **(1994)**, pp. 232-249.

[36] X. Wang, Y. Lisa Yin and H. Yu, "Finding Collisions in the Full SHA-1", Shandong University, Jinan 250100, China. Retrieved 18 March 2009 from http://www.infosec.sdu.edu.cn/paper/sha1-crypto-auth-new-2-yao.pdf, **(2005)**.

Authors

Saadiah Yahya is Associate Professor of Computer Sciences at MARA University of Technology, Malaysia. She has been lecturing in the University for 30 years in the area of Networking, Information System, Information Security, and Information Technology Management. Before that, she has been a mathematics and chemistry teacher at La Salle High School of Klang, Malaysia for about a year. She has a Ph. D. in Computer Sciences specializing on Computer Networking from Putra University, Malaysia. She has published 10 (7 main author and 3 co-author) academic books in the area of computer sciences and IT, written many papers in the area of computer sciences and networking. She is actively doing research in the area of computer networking and IT and currently has completed 18 researches. Seven of those researches has participated in innovation, invention, and design competition at university and international level and won numerous medals (1 gold, 5, silver, 4 bronze and a Special Award: best presenter). She involves in many important academic committee at the faculty and the university. She is also active with co-curricular activities at the University particularly for the Faculty of Computer and Mathematical Sciences and has been a head of Network Application and Communication SIG, and an advisor for student's union society at the faculty. She has been appointed as advisor and chief of panel examiners for the Ministry of Education and many industries and agencies in Malaysia. She is a Chartered *Chartered Institute of* Logistics *and* Transport *mem*ber of professional bodies. She is also a certified CCIA instructor she is married and a mother of four grownup children.

Dr Mohamed Sulaiman Sultan Suhaibuddeen sit as board of director in several government linked companies and multinational technical security company. He is currently an academic and industrial advisor for MARA Technology University. He frequently was called to give public lectures on ICT's technical and governance aspects. Proven ability to effectively plan, lead and manage business IT operations and reengineer processes to improve business performance and operational efficiencies. Recognized for excellence in developing and providing consulting services, training and management support. Proficient in identifying direction of leading-edge technologies and its application to business systems. Exposed to ISO/IEC 27001, 14000 and 9001:2000 as Management Review Board, Manual Committee and Internal Audit Team. Attended workshop and implemented Balance Score Card, Six Sigma, Blue Ocean Strategies and The International Customer Service Institute programme.

Zainab Abu Bakar is a Professor at Department of Computer Science, Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam, Malaysia. Since her completion of her doctorate in Computer Science, she has been actively involves in the research areas of Information Retrieval on text, image, map, mathematical terms, and speech; Natural Language Processing; and Semantic Web with secured research grants

Ahmad Yusri Dak received the B.Eng(Hons) Ellectrical Engineering and Master of Science(IT) from the Universiti of Teknologi MARA, Selangor, Malaysia in 1997 and 2013. He was working with several multinational company such as Telekom Malaysia(TM), Asteria Telcommunications Sdn Bhd and Celcom. He also involved in many telecommunications project such as civil, GSM, ETACS, Intelligent Networks and fixed networks. He is currently a Ph.D. candidate at the Center of Computer Technology and Networking, Universiti Teknologi MARA(UiTM), Malaysia. Current research interests include wireless network, information security and RFID and completed 15 researches project locally and internationally. Seven of those researches has participated in innovation, invention, and design competition at university and international level and won numerous medals (1 gold, 5, silver, 4 bronze and a Special Award: best presenter).