# Analysis and Study of Network Security at Transport Layer

Hiren Parmar
Ph.D. Student of
Saurashtra University
Rajkot

Atul Gosai, PhD
Associative Professor
Saurashtra University
Rajkot

## ABSTRACT
In this technology era every applications depends on networks, it may be local or Internet, Intranet or Extranet, wired or wireless. All networks require strong security consideration to ensure confidentiality and integrity of communication. This paper discusses network security and related issued specifically at Transport layer, which enables true end to end communication between peers. As security is never 100%, security threats and vulnerability continues growing and becomes major concern for business and industries. Transport layer security concern with authentication, confidentiality, integrity and availability [1] [2]. In this paper we tried to discuss different security issues at transport layer, evaluating existing security mechanisms and standards. In fact, found the de-facto standards of web security used all over the world to secure e-commerce, online-banking are also found insecure. In other word, "security needs continuous improvement for better security". Major security issues at presents are various kinds of man-in-the-middle (MITM) attacks, authentication related attacks, Distributed Denial of Service (DDoS) attacks and security association related attacks need serious considerations. Further gives direction on how to improve and strengthen security.

## General Terms
TLS – Transport Layer Security
SSL – Secure Sockets Layer
MITM – Man-in-the-middle attack
DoS – Denial of Service
DDoS – Distributed Denial of Service
TCP – Transmission Control Protocol
UDP – User Datagram Protocol
AES – Advanced Encryption Standard
GCM – Galois Counter Mode
HSTS – HTTP Strict Transport Security
RSA – Rivest Shamir Adleman
CA – Certificate Authority
BEAST – Browser Exploit Against SSL / TLS
IPS – Intrusion Prevention System
PKI – Public Key Infrastructure
CBC – Cipher Block Chaining
HTTPS – Hyper Text Transport Protocol Secure (over SSL)

## Keywords
Security, Transport layer, DoS, DDoS, MITM, SSL/TLS Authentication, Confidentiality.

## 1. INTRODUCTION
Network has enabled lot of application that now a day all most all application depends on it and required security. Network security is concern with protecting data during transmission. Today, all network connected with internet, it may be LAN, Internet, Intranet and extranet. During transmission there are many types of attacks can happens on data like release of message content, Traffic analysis, masquerade, reply, modification of message and denial of service etc.[3].

To detect, understand and mitigate complex network security one should go through layer architecture of OSI reference model. It has seven layers; each layer has its own independent task. In this paper we are discussing issues related to transport layer only because of four reasons

1) Lower layer security (network layer) must be applied at every network node (less secure, slower, much more complex) compare to upper layer security (transport layer) need be applied only at End points (more secure, faster and less complex) [4].

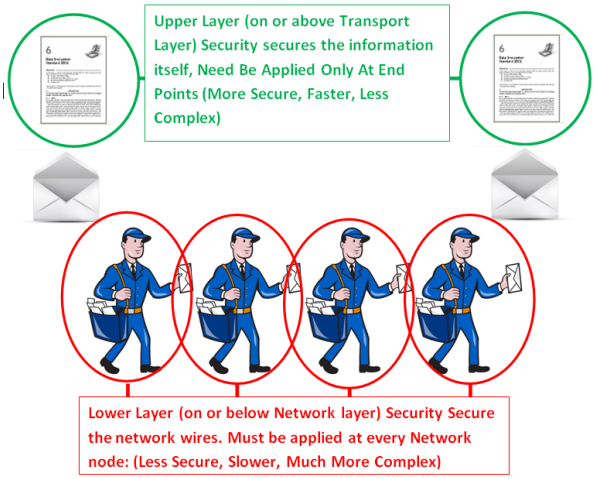


**Figure 1: Comparison of Security at network (lower) layer v/s Transport (upper) layer [4]**

2) Transport layer provides general security regardless of media, access method, topology and types of network.

3) It is below application layer so one can easily develop different applications based on security provided at transport layer like e-mail, e-commerce, web application etc.

4) Implementing IPv6 standard for TCP/IP network solves many security related issues at network layer by using IPSec protocol compulsory.

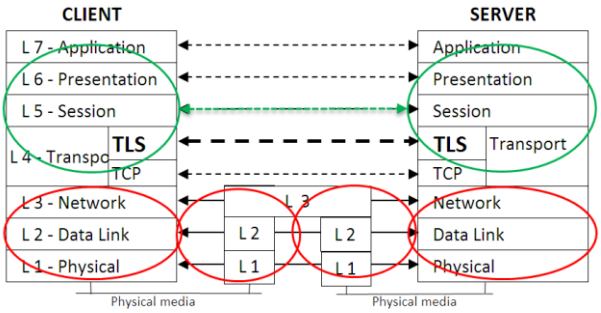


**Figure 2: Position of Transport Layer and it Security in reference to OSI model [2]**

## 2. BASIC NETWORK SECURITY REQUIREMENT

Security is described through accomplishment of some basic security properties, namely, confidentiality, integrity, availability, authentication and accountability (nonrepudiation)[3][5]. All security threats and attacks can be classified under following properties in broad sense.

### 2.1 Confidentiality

It is a property of protecting the data from all users other than those intended by the owner of the information. The non intended uses are generally called unauthorized users. It fall under passive attach. Passive attach is hard to detect but easy to apply using Cryptography and/or Stenography [5]. We can ensure confidentiality using cryptography encryption so that during transit one can see it but not know it.

### 2.2 Integrity

Ensuring integrity means protecting information from unauthorized altering. It falls under active attack. You cannot stop user to alter data but detection of this alteration is very easy. Once detected user can solve the issue like not accept such packet. We can compute on time hash as sender side before sending packet over network. Then at receiver side also calculate hash based on received message and then check both hash, if same than no break but if not same then stop the communication.

### 2.3 Availability

Availability ensuring reliable and timely access to and use of information and service is not denied to legitimate/authorized user. It is the property of protecting information from non-authorized temporary or permanent with holding of information [3]. Availability concern at almost all layers of OSI. Now a day attack on availability increases very fast and mitigating it at particular layer is very hard. But here we talk availability issues only at transport layer which can mitigate by selection appropriate security solutions like firewall, intrusion detection system etc.

### 2.4 Authentication

It is property through which we can verify or check genuine entity. It ensures that user is who they identify themselves and that each inputs arriving at the system comes from a trusted source [3]. Authentication can be ensuring by many techniques like, login-password, biometric, Certificate based, OTP etc.

### 2.5 Accountability

It concern with the tracing actions of entity uniquely. Accountability concern with keeping record and audit checking about non-repudiation, isolate fault, IDP, recovery and legal action. As we know security never 100% achievable we have to trace possible breaches. It is very essential for forensic evident and/or analysis also [3].

## 3. NETWORK SECURITY ATTACKS AT TRANSPORT LAYER

### 3.1 Eavesdropping attacks.

Unauthentic listening conversion of entities without knowing them [6]. To mitigate eavesdrop we should always communicate securely (using cryptographic solutions) so even if attacker successfully get or listen the data but not read its or its meaning.

### 3.2 Port scan attack.

A port scan is one of the most popular techniques attackers use to discover active services they can be break. All machines connected to a network run many services and each service are uniquely identified by assigning unique port number. In port scanning we sends a fake message to each port and observe its response. Based on response we can know direct or indirectly that the port is active or not and also it's related weakness [8]. Port scanning is a pre-attack, information collection phase. Hacker must know the IP address and port status to start attack. By using appropriate firewall, IDS we can protect ourselves. We should configuring appropriate rules, blocking unwanted port and allowing only solicited traffic to protect.

### 3.3 Reply attack.

In this attack attacker can saves the communications of the legitimate user, similar to an active Man-In-The-Middle (MITM) attack. Where as in the MITM attack changes the content of the message before sending it on, a reply attack only saves the message and then sends it later against [19]. He can then resend this packet for getting unauthentic access or monitory benefits like paying amount twice to beneficiary account. He can also use stored massages for impersonation. By using appropriate timestamp mechanism [19] we can mitigate it to some extent.

### 3.4 Man-in-the-Middle attack.

According to RFC 2828, a MITM is an active attack. It intercepts and modifies selectively data to masquerade as one or more of the entity involved in a communication [9]. Major characteristics of MITM attacks are (i) that they represent adaptive active attacks, and (ii) that they target the association between the communication entities [25]. It is very hard to detect and avoid MITM attacks. We should use strong mutual authentication techniques, proper configuration of client and server handshake mechanism we can reduce change to get attacked.

#### *3.4.1 TCP Session hijacking.*

The attacks exploit the communication session established between the host that starts the session and target host or between devices is session hijacking. It is a type of MITM attack. When transport layer is not encrypted, all communication between the website and client is sent in clear-text which leaves it open to intercept, injection and redirection.

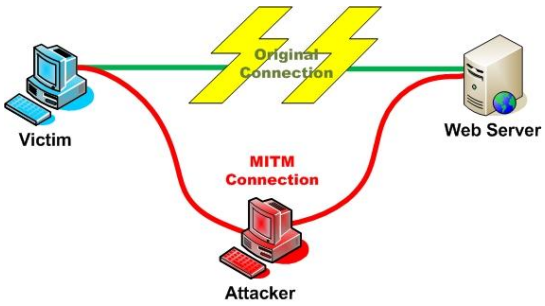


**Figure 3: MitM attack [8]**

As we all know, session involves dialogues related to connection set up, maintained, and terminate. Session hijacking can be done by spoofing and guessing a sequence number of the target host or by cookie stealing, which is used by TCP [5][6]. By using cryptography solution and insist only to communicate securely in encrypted form.

## 3.5 Land attack.

An attacker sends stream of TCP_SYN packets with the same source and destination IP address and TCP port numbers. The victim system will be rebooted or crashed [8].

## 3.6 Denial-of-Service attack.

These attacks try to overwhelm the network or server resources so that legal users or hosts cannot get service timely. Instead of using one computer, a more sophisticated DDoS (Distributed denial-of-service) attacks may use hundreds or thousands of computers (Zombies, and botnet). DoS attacks are as follow:

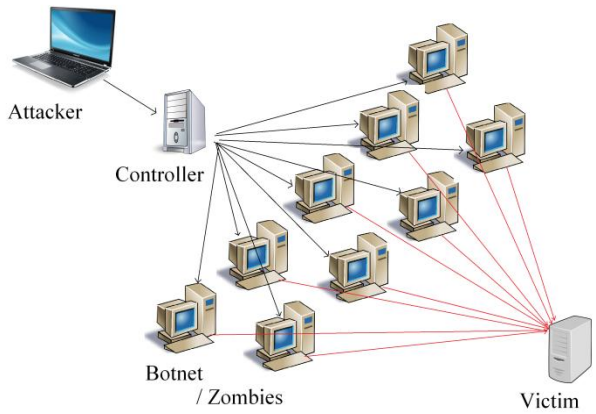


**Figure 4: A sophisticated DoS attack using large Botnet (Known as DDoS) [21]**

### *3.6.1 TCP SYN floods.*

An old and the most common network attacks is DDoS attack based on TCP SYN floods. We all know TCP setup connection by 3-way handshake mechanism and this type of attacks exploits it for attacks. Any device, network including a firewall are susceptible to the SYN flood attack.

### *3.6.2 UDP flood attack.*

In UDP flood attack an attacker sends a UDP packet to any port randomly on the victim system. On receives a UDP packet, it will think what application is waiting on the port. After sometimes it know that actually there is no application waiting for it and so it generate an appropriate ICMP packet indicating "destination unreachable" to source. Attacker can send continuously lot of UDP packets on victim's port, this way gradually system overwhelmed and go down [8].

Following are the attacks on security standards which forces us to understand attacks and improve network security by mitigating them.

## 3.7 Authentication gap in TLS renegotiation.

The authentication gap exit during the renegotiation process in the SSL 3.0 or higher and TLS 1.0 or higher protocols are vulnerable to a set of related attacks. It can allow MITM attack operating at or below TCP layer to inject a chosen plaintext prefix into the cipher text stream, often without detection. This becomes serious security defect for all protocols which uses TLS (including HTTPS) [22] [23].

## 3.8 Man-in-the-Middle against SSL/TLS.

SSL/TLS was used to mitigate risks for web transactions by providing endpoint authentication and encryption. As we do communication through SSL/TLS we are safe is the only belief. It is discovered in last 2000 the feasibility of mounting an MITM attack on the protocol.

### *3.8.1 Using SSL strip.*

It is possible to perform MITM attack by using SSL Strip [6]. SSL/TLS security stops major attacks so if we can remove it from the path we can perform many types of attack. In SSL stripping attacker change unsecure applications layer protocols that request the use of TLS for securely, like HTTP pages and traffic. "SSL stripping" was first introduced by Moxie Marlinspike [10]. It is like a more generic "downgrade attack".

### *3.8.2 Using Triple Handshakes*

If a TLS client connects to a malicious server with right credential, the client can be impersonated by the server, at any other server. This way the malicious server performs a MITM attacks on three successive handshakes [9].

In this attack the attacker can act as proxy to cause two TLS connections to share secret. Successful attack can leads to a many types of exploits like MitM, break secure renegotiation etc. [18] [19].

### *3.8.3 Faulty SSL client implementation*

MS IE, allow for transparent SSL MITM attacks when the attacker has any CA signed certificate. Even on unprotected systems an attacker can preload his own trusted root authority certificates [8]. One such example is superfish adware in Lenovo consumer laptops violate SSL [36].

### *3.8.4 An insecure key exchange.*

TLS security mainly depends on key, need to exchange and authentication carried out at initializing secure connection. As we know security of cryptography based on its key and not on its procedures or algorithms. So any insecure exchange of key can lead to very powerful and dangerous MITM attack. Web generally use third party certificate for securely exchange keys and authentications. Security of such certificate is ensuring by Public Key Infrastructures (PKIs), which has trusted authorities and its chains for distribution and validation of such certificate. In the recent years, security concerns regarding PKI usage have arisen: regardless of the position in the CA hierarchy tree, certificates can be issued for entities. Even attacks on CAs to generate valid certificates, enabling man-in-the-middle attacks. We can also maliciously use intermediate CAs, sub CA to perform planned attacks through ad-hoc certificates is also dangerous and are very hard to detect [24].

Present PKI infra for TLS is prone to MITM attacks so we need new mechanisms for detection and avoidance of those attacks [24].

## 3.9 Denial-of-Service attack against SSL/ TLS.

Here we will discuss DoS related attacks against security protocols.

### *3.9.1 SSL flood.*

SSL flood exploits the security protocols for attacks. SSL stands for Secure Socket Layer, an attacker sends lots of secure connections request and call for negotiation to victims. As we know to connect securely entities has to exchange and agreed on many security parameters, it also generate computational overheads. These SSL floods bypass firewall, IPS (intrusion prevention system) and can overwhelm server or even overflow state full firewalls [7].

### *3.9.2 SSL renegotiation attacks.*

This attack is so powerful that it can exploit the cryptography property of SSL. Even attacker with low powerful device compare to unprotected server can also took successful attack, as it only requires 1/10 of the processing / computational power [7].

## 3.10 Attacks on RC4.

TLS (and previously, SSL) uses RC4 algorithms in its cipher suits for many years for security. RC4 is even today, used by many e-commerce and online banking industries. Like SBI, Kotak, BOI all banks uses RC4 based crypto suite. Recent cryptanalysis results exploit biases in the RC4 key stream to recover encrypted data. Current study show it practically exploitable, only requires 2^26 session or 13x2^30 encryption [11] [12].

## 3.11 Compression Attacks: TIME, CRIME, BREACH.

The CRIME attack allows an active attacker to decrypt cipher text (specifically cookies) when TLS-level compression used. The TIME & BREACH attack use compression made at HTTP-level to recover secret data from the HTTP response [13] [14].

## 3.12 BEAST attack.

Browser Exploit against SSL / TLS, (BEAST), demonstrates a weakness in the SSL protocol. It enables attackers to decrypt data passing between a web server and an end-user browser. The BEAST attack uses TLS 1.0 implementation of cipher block chaining (CBC) to decrypt parts of a packet, especially cookies when HTTP runs over TLS. [15].

## 3.13 Padding Oracle Attacks.

All encryption algorithms fall under block cipher or stream cipher. This padding attacks only concern to block cipher in which encryption algorithm converts whole block (8 byte or 16 bytes) and if message is smaller than block then we have to padding it. While "oracle" gives answer for valid or invalid block in given cipher. Using this answer attacker can create algorithms decrypting any cipher text of CBC mode [35]. The MAC-then-encrypt design traditionally believed secure is one of the reasons that enable this attack in all current versions of TLS. Lucky Thirteen attack is also sophisticated variance of timing side-channel attack though which we can decrypt cipher text arbitrary [16][17].

## 3.14 Theft of RSA Private Keys.

We can able to get the server's private key when TLS is used with non-Diffie-Hellman cipher suites. One we get private key we can use it to decrypt any session (past or future) initiated with that server. Many popular network sniffer softwares (like Wireshark) use such techniques to inspect TLS protected connections.

# 4. CURRENT RELATED WORKS

All solutions on network security involve using some kind of Cryptographic techniques, authentication mechanisms, third party validation and verification techniques etc.

Network security concern with securely transfer of data between nodes. We can achieve confidentiality using encryption-decryption, cryptographic method so that even someone gets the data during transit it cannot read or misuse it. We can achieve integrity by adding hash (one way function to create compressed fix size message) with the message so that received can know the message which he receives not tempered during transit as we cannot stop integrity attack, person can change data even he could not read or understand it. Generate secure pipe (tunnel) during communication over insecure public network so nobody can tap it. Availability attributes concern to many related issues like physical factor, external factor, software and hardware. Physical and external factor is out of our scope. We here discuss DoS and DDos related issues which affects availability. Majority solutions of DoS and DDoS is to monitor traffic, detect pattern from it and stop task/communication not following standard practice which is performed by firewall, IDS, IPS solutions available in market[7]. There is lot of techniques available for Authentication mainly login-password, smart card, OTP, third party Certificate, biometric, secret ques.-ans., graphical, hiding data behind images and many more.

We are also using SSL/TLS [27], DTLS [28] the most popular de-facto security standards used by almost all secure applications and application layer protocols. Though security standards itself not secure [34] as different attacks [G] to [M] on it. There are different types of solutions and suggestion reviewed as below:

For SSL/TLS renegotiation related issues, both clients and servers must implement the renegotiation info extension, as defined in [29].

SSL Stripping attacks are happens because unencrypted initial access to web server. To avoid such kind of attack we must use HTTP strict Transport Security (HSTS) [31].

On reviewing attacks on RC4, it cannot able to providing a sufficient security for TLS sessions so we should avoid it to use RC4 based crypto suit [32].

By simply disabling TLS, HTTP-level compression we can mitigate TIME attack. We have no solution for BREACH attach at TLS level so some higher level (application-level) mitigation are needed [30]. To avoid compression related attack TLS-level compression should be disabled because it is subject to security attack as the CRIME attack [26].

The issues related to BEAST attack on TLS 1.0, Cipher Block Chaining (CBC) mode. We should avoid cipher suits using CBC mode.

MCA-then-encrypt construction is responsible for padding oracle attack. It is suggested to use Encrypt-then-MAC construct which is more secure [33]. Further, another solution of Lucky13 attack by authentication using AES-GCM.

To counter Triple Handshake attack, the [16] suggested following possible solutions i) binding the master secret to the full handshake ii) binding the abbreviated session resumption handshake to the original full handshake.

RSA private keys need better protection by using OS or dedicated hardware protection. We should always insist to use cipher suites that offer "forward secrecy". Because forward secrecy protects our sessions from passive attacks, even though, attacker successfully get private key [30].

To mitigate all above attacks we are using above concepts and follows the security standards, guidelines and suggestions of NIST, IETF[26].

## 5. CONCLUSIONS

Day by day application works on network increasing drastically, now all most all gazettes depend on network/internet. This new application and devices raise many security related issues. As number of network enabled devices increases, so, the requirement of application based on network increase. As a result, the footprint of network becomes very large and need complex security solutions. We have to continuously strengthen the security, and security standards which we are using today for tomorrow. We have seen that what we believe best security before 2013, has lot of vulnerability today.

As in chain weakest part becomes the strongest level of security same in network weakest point becomes the strongest security. SSL/TLS the most secure web security protocol has lot of vulnerability and need quick solutions. We have to think seriously about this. Major problems related to transport layer and its security standard SSL/TLS is based on weak cipher support, poor negotiation, weak authentication and integration and miss configuration. Mainly we are facing man-in-the-middle and Denial of service attacks at transport layer. Man-in-the-middle attack is not a simple single attack; it requires breaking all Confidentiality Integrity Availability (CIA) security attribute to successfully attack. Once it becomes successful then nothing can be secure over net. Same as Denial of service (DoS) and Distributed Dos (DDoS) attacks also increasing drastically. It is about to impossible to avoid because it follow standards practice for attack.

After reviewing all relevant research papers on Security at Transport Layer, we would like to suggest areas which need improvements. We need strong cipher suits, authentication methods using multifactor authentication and integrating quantum cryptography into TLS. We can develop software solutions that overcome mis-configuration and compliance related issues of clients, and servers. Further we strongly believe that the certificate based server authentication is done improperly by the ordinary user that we can improve. We should avoid uses of CBC mode, RC4 based cipher suits and TLS compression until its solutions found. Integrate all best of the class security solutions to make overall security stronger and reliable for long time. Day by day attacks and its techniques becomes matured, intelligent and at upper layer in the stack.

## 6. REFERENCES

[1] Glenn berg 1998 MCSE Training Guide Network Essential (Second edition), page no. 48-55.

[2] C.Machael Chernick, Charles Edington III, Matthew J.Fanto, Rob Rosental, 2005 Computer Security, NIST guidelines for the selection and use of TLS implements, page no. 4-6, June 2005.

[3] William Stallings 2011 Network Security Essential Applications and standards, 4th Edition, page no.9-11.

[4] By Daniel E. Nordell 2012 Terms of Protection, IEEE power and energy magazine, page 21, January/February 2012.

[5] Ranayiotis Kotzanikolaou and Christos Douligeris 2008 Chapter 1, Computer Network Security ; Basic background and current issues, Page no. 9, 2008.

[6] Chris Sanders 2010 Understanding Man-In-The-Middle Attacks - Part 3: Session Hijacking http://www .windowsecurity.com/articles-tutorials/authentication_and_ encryption/Understanding-Man-in-the-Middle-Attacks-ARP-Part4.html, Published on 5 May 2010.

[7] David Holmes 2013 Mitigating DDoS Attacks with F5 Technology, Tech Brief. F5 Technology, https://f5.com/resources/white-papers/mitigating-ddos-attacks-with-f5-technology.

[8] The Open Web Application Security Project (OWASP) 2015 over Man in the middle attack, https://www.owasp.org /index.php/Man-in-the-middle_attack, last revision 8/4/2015.

[9] Internet Security Glossary 2000 http://www.ietf.org /html/rfc2828, RFC 2828, May 2000.

[10] Marlinspike, M., 2009 owner of throughtcrime.org, demonstration of HTTPS stripping attacks, "sslstrip", http://thoughtcrime.org/software/sslstrip, February 2009,

[11] Nadhem J. AlFardan, Daniel J.Bernstein, Kenneth G. Paterson, Bertram Poettering , Jacob C.N. Schuldt, 2013 "On the security of RC4 in TLS", 22nd USENIX Security Symposium, 2013.

[12] Christina Garman, Kenneth G. Paterson, Thyla van der Merwe 2015 Attacks only Get better: Password recovery Attacks against RC4 in TLS, March 16, 2015.

[13] Tal Be'ery, Amichai Shulman 2013 "A perfect CRIME? Only TIME will Tell", Black hat Europe 2013.

[14] Yoel Gluck, Neal Harris, and Angelo (Angel) Prado 2013 "BREACH: Reviving the CRIME Attack", http:// breachattach.com,2013.

[15] Thai Duong, Juliano Rizzo 2011 "Here Come The Ninjas", "Browser Exploit Against SSL/TLS", http://packetstormsecurity.com/files/105499/Browser-Exploit-Against-SSL-TLS.html.

[16] Nadhem J. AlFardan and Kenneth G. Paterson 2013 "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols", 2013 IEEE Symposium on Security and Privacy.

[17]Bodo Moller, Thai Duong, Krzysztof Kotowicz 2014 "This POODLE Bites: Exploiting the SSL 3.0 Fallback", https://www.openssl.org/~bodo/ssl-poodle.pdf, September 2014.

[18] Bhargavan K., Delignat-Lavaud A., Fournet C., Pironti A. And P.Strub 2014 "Triple handshakes and cookie cutters: Breaking and Fixing Authentication over TLS, https://secure-resumption.com/tlsauth.pdf

[19] Mark Ciampa 2005 , Security+ Guide to Network Security fundamentals, 2nd edition, Western Kentucky University Chapter 2: Attackers and Their Attacks.

[20] Athar Mahbood and Dr. Nassar Ikram 2004 "Transport Layer Security (TLS) – A network Security Protocol for E-commerce" Technocrat PNEC Research Journal, 01/2004 http://www.researchgate.net/publication/216485703_Transport_Layer_Security_(TLS)--A_Network_Security_Protocol_for _ E-commerce.

[21] Lasote 2014 Our first DDoS attack!!, http://blog. biicode.com/first-ddos-attack/, BIICODE Blog, Posted on August 12, 2014.

[22] Marsh Ray 2009 "Authentication Gap in TLS Renegotiation, Oracle http://www.oracle.com/technetwork/ java/javase/documentation/tlsreadme2-176330.html.

[23] National cyber-alert system 2011 Vulnerability summery for CVE-2009-3555, National Vulnerability Database, http://web.nvd.nist.gov/view/vuln/detail? vulnId=CVE-2009-3555, Auguest 2011.

[24] Enrique de la Hoz, Rafael Paez-Reys, Gary Cochrane, Ivan Marsa-Maestre, Jose Manuel, Bernardo Alarcos 2014 "Detecting and Defeating advanced Man-In-The-Middle Attacks against TLS", 2014 6th International Conference on Cyber conflict, 2014.

[25] Rolf Oppliger, Ralf Hauser, David Basin 2006 "SSL/TLS session-aware user authentication – Or how to effectively thwart the man-in-the-middle", Elsevier, Science Direct, Computer Communication 29.

[26] Y. Sheffel, R. Holz, P. Saint-Andre May 2015 Recommendation for secure use of TLS and DTLS, http://www.ietf.org/html/rfc7525, RFC 7525.

[27] Dierks T., and E. Rescorla 2008 " The Transport Layer Security (TLS) Protocol Version 1.2", http://www.rfc-editor.org/info/rfc5246, RFC 5246, August 2008.

[28] E.Rescorla, N. Modadugu 2012 "Datagram Transport Layer Security Version 1.2", http://www.rfc-editor.org/info/rfc6347, RFC 6347.

[29] E. Rescorla, M. Ray S. Dispensa, N.Oskov 2010 "TLS Renegotiation indication extension", http://www.rfc-editor.org/info /rfc5746, RFC, 5746.

[30] Y. Sheffel, R. Holz, P. Saint-Andre 2015 "Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS)", http://www.ietf.org/html/rfc7457, Feb. 2015.

[31] J.Hodges, C. Jackson, A. Barth. 2012 "HTTP Strict Transport Security (HSTS)", http://www.ietf.org/html/ rfc6797, RFC 6797, November 2012.

[32] A.Popov 2015 "Prohibiting RC4 cipher suites", http://www.ietf.org/html/rfc7465, RFC 7465, February 2015.

[33] P.Gutmann 2014 "Encrypt-then-MAC for TLS and DTLS", http://www.ietf.org/html/rfc7465, RFC 7366, September 2014.

[34] Web Application Security Consortium 2004 "Insufficient Transport Layer Protection" Threat Classification, http://projects.webappsec.org/w/page/13246945/ InsufficientTransportLayerProtection, WASC-04.

[35] Microsoft Israel's blogging Community 2010 padding oracle "ASP.net vulnerability explanation", http://blogs.microsoft.co.il/linqed/2010/09/19/padding-oracle-aspnet-vulnerability-explanation/.

[36] Trend Micro SecurityLabs 2015 Superfish Adware in Lenovo Consumer Laptops Violates SSL, Affects Companies via BYOD, http://www. trendmicro.com/vinfo/us/security/ news/cybercrime-and-digital-threats/ superfish-adware-in-lenovo-consumer-laptops-violates-ssl.