

Department of Computer Science and Engineering
Data Science



2022 2028
Semester: VI Subject: CSS Academic Year: 2023 - 2024
SSL -> SECURE SOCKET LAYER:
It is an internel protocol for secure exchange of information between Neb Browsen and Web Server.
- elle col are as follows:
The services provided by SSL are as follows:
-> Authentication
→ Confidentiality
It was a protocol
-> Handshare
-> Record Prolocol
-> Alexi Protocol
Handshake Protocol:
TI underages 4 sleps:
* Establish security capabilities.
* Server authentication and key techange.
* Establish security capabilities. * Server authentication and key Exchange. * Client authentication and key Exchange.
* Finish.
Oland. Establish security capabilities.
and Client Clant 1111 Server.
RNc. RNc., RNs.
* Finish. Slept: Establish security capabilities: RNa. Client Hello RNa., RNs. PNs. Server Hello RNa., RNs.
4 14 11
The dient Hello consists the following:
Varian Number.
Paralow Number of Chient (PNc) -> It is generated
bused on date and times lamp.
Client Hello consists the following:- The dient Hello consists the following:- Version Number. Random Number of Chient (RNc) -> It is generated based on date and times lamp.

Subject Incharge: Prof. Sarala Mary Page No. 4





Semester: VI Subject: CS.S Academic Year: 2028-2024
Session id -> if id = 0 then connection not yet established if id = non-zero then connection a established.
if id = non-zero then connection a established.
Supported by the client
-> Compression method: The compression algorithm that client
supports
The client will send all the above information to server. Server Hello:
Manual Property of the Control of th
The cerrer hello consists of the following:
-> Version Number -> The server will choose the version.
-> Server generated Rendom Number (RNs).
-> Server Lession id.
-> Cipher suite-> Choose single eigher suite which the
come relect I m the dist send earlier by the client
-> Compression Algorithm -> Server selects from the list that
is sent by the client.
The above informations are send to client.
Stepa: - Server Authentication and Key Exchange.
Client Color + Server.
RNc, RNs. 1. Certificate. RNc, RNs.
2. Server Kay Exchange
3. Certificale Request Dephonal. 4. Server Hellodone
4 - Server Hello done

PARSHWANATH CHARITABLE TRUST'S



Subject Incharge: Prof. Sarala Mary Page No. 3

A.P. SHAH INSTITUTE OF TECHNOLOGY

Department of Computer Science and Engineering
Data Science



Department of CSE-Data Science | APSIT

	Semester: VI Subject: CSS Academic Year: 2028-2029
	Semester: VI Subject: CSS Academic Year: 2028-2024 1. Server sends Digital Certificate which contains public key of corres.
	key of server.
	2. If server does not send certificale then only the put
	POLITIES FOR ALL DON ATVIDUACES ICCI.
	3. The server can request for dients digital certification
	4. Client can now verify and proceed.
	4. Client can now verify and proceed. Step 3: Client Authentication and key Exchange.
	DN DN 1 1. Certificate 12 motional.
	PUs - public 2. Client key Exchange RNC, RNs. key of Server
100000	kay of Server - Could's le Voust (DA)
(Generale 3. Certificate Venify. Depremaster, Prs) premaster premaster premaster premaster premaster
	D (PNc, premaster) = KNC.
	(RNc, pre-master) if RNc = RNc - valid.
h	Master secret key, Maretin correl key Cummerine
•	a) Client key Exchange: -> Client creates pre-master key.
	-> Client creates pre-master key.
	Premaster-key is encupted by public key of server and encupted pre-master key is send to server.
ć	encupléed pre-master key is send to server.
	Server will decrypt using his own private key. 3) Certificate Verification:
	3) Certificate Verification.
	townt grandom number of client using pro-master key
	I II- and an
	3) Certificate Verification: > Encupit Handom number of client using pre-master key not send to server.



PARSHWANATH CHARITABLE TRUST'S

A.P. SHAH INSTITUTE OF TECHNOLOGY

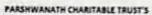
Department of Computer Science and Engineering
Data Science



Semester: VI Subject: CSS Academic Year: 2023- 2024 The server will decrypt if wing pre-master key and get the random number of client -> It RNc & equal to the sandom Number which he has already received, then it it is right client Both client and server will generate mouster secret key and symmetric key by the below method: Bre-master secret | Chien | Random Number | Server Random Number (ENE) Apply message Digest Algorithm. Master Secret Key. The master secret key is used to generale symmetric key.

Master secret key Client Random No. (ENC) Server Random No.

PNS. Apply Message Digest Algorithm. Symmetric Key his own private Res







Semester : VI	Subject :(222	Acadomic Vosc 20 29 20 20
Step 4. Enich.			Academic Year: 20 28 - 20 24 -
	lient		Server.
RNc, RNs,	1. Change cip	her specification	PAL PALO
PUs,	2. Finished	supinded .	premaster, master secret key, Symmetric key.
Media and Bou	3. Change Ci	pher specification	master secret key,
Commetric Kou	4. Frished	, ,	Symmetric key.
Symmetone 1-3	Commence and	The use of the	
Alte generating	all nequire	d keys, th	e final confirmation
message is send.	to both client	I and server	e final confirmation
RECORD PROTOCOL	L:		MAC is appointed to
	L L nat	encruption	and decryption of
the record proto	col does no.	and griton	and decryption of
the dala			
Commission Contraction	en Louis vista	Applicat	ion Data
	:	111111111111111111111111111111111111111	to the property of the
		Tmame	otation.
		Fragme	taile of sit a
43 0	rossion.	in the law	
Comp			A
MAC	MA to me sou	C-> Messag	e Authentication Code
Add	litton of	Market Dry	
	The state of	Oumm	otorc Key.
IIII Enc	uption done	uning agricult	Industry of
1			
Ap	pend Header		TOTAL TOTAL
Himmin	· Slamin		

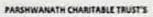
PARSHWANATH CHARITABLE TRUST'S



A.P. SHAH INSTITUTE OF TECHNOLOGY



Semester: VI Subject: (SS Academic Year: 2023-2029
The following slips are followed in necord protocol-
-> The Application data is divided into fragina
using bragmentation technique. I mented data to
wring fragmentation technique. Apply compression algorithm on fragmented data to compress the alater.
compress the date.
-> MAC is generated through the confict. MAC. The
compress the abolic . MAC is generated through the compressed date: The meester secret key is used to generate MAC. The MAC is appended to check the integrity of message.
MAC is appended to check the integrity of message. MAC is appended to check the integrity of message.
The data along with the MAC is encupted using the generated symmetric key.
the generaled symmetric key.
the generated symmetric hay. I header is appended to the encuppted date. The
header consists of content type, major and minor version,
compression length etc.
In the other end it is decaypted wing symmetric
compression length etc: In the other end it is decupted wing symmetric integrity key and master secret key is used to check integrity
of the data
ALERT PROTOCOL: Types of Error
Sereily Cause
Byle 1 Byle 2
Type of From
Warning Falal -> I No certificate
Bad record MAC. Buc certificate
TIONAL NAME OF THE PARTY OF THE
Subject Incharge: Prof. Sarala Mary Page No. 6 Department of CSE-Data Science APSIT







Semester : VI	Subject :	088	Acad	lemic Year: 2028- 2024
→ When either	the client	or the	server det	edi an error
→ When either the detecting pa party.	arly sends a	en aleit	message 1	ō the oother
party.	0		0	
→ 对 出 日 日 年	alal error.	then com	nmunicatio	n is closed.
→ Jf H å f	erning, the	n error i	i resolved	and if i
continued.	0			