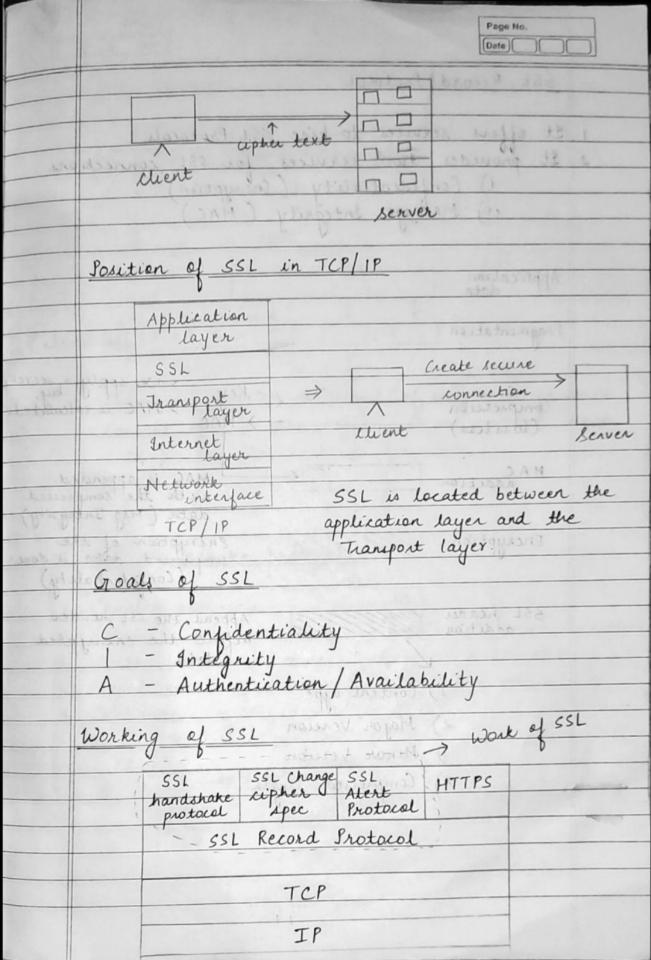
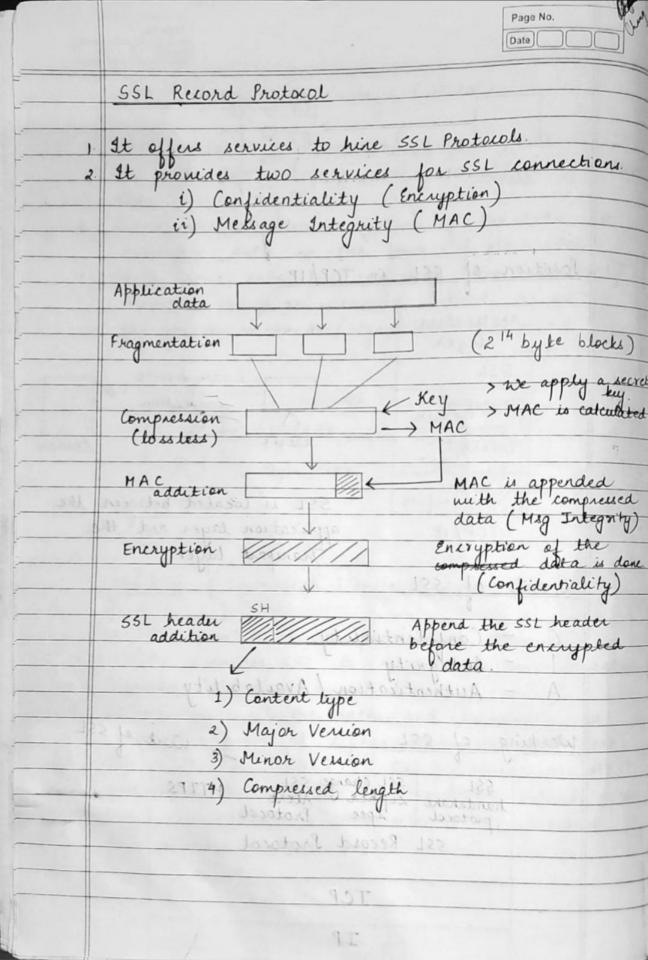
	Page No.
_	Unit-4
	<u>Oraço i</u>
9=1	Secure Socket Layer (SSL)
	TOTAL TOTAL CONTRACTOR OF THE PARTY OF THE P
j.	of SSL was released in 1995 and version 3
3	of SSL was released in 1995 and vertion 3
	was released on 1999.
2.	Internet Engineering Task Force (IETF) laurichea
	TLS (harsport hayer Security) in 2015.
3.	Internet Protocol for secure exchange of information
	between browser with softre
4.	Ironides security at transport rayer.
5.	Provides safe and secure Internet connection
6-	Data safety is a primary goal.
	3
	Hartest Ingle Patort Colar
	Client Server Server
Ma.CIA	HTTPS provides SSL to sorring the community
	1) The client sends a request to the server to
· Annu	a the secure SSL session the certificate
774	(2) The server responds by sending the certificate to the client.
3331	(3) The client then generates its session key and
13	3) The client then generates its session key and sends it to the server.
	(4) Secure SSL servion is established.

		Page No.
	HTTP (Hypertext Transfer	Protocol)
3	HTTP operates at Application It lacks the security med data. Since there is no encryption transfers data in the for screen browser. It is an insecure	layer inside TCP/IP harism to encrypt the on of the data, it um of plain text.
	Password Abe 12.74	Server
3. 4.	HTTPS (Hypertext Inanger HTTPS operates at Inansport HTTPS provides SSL to see between server and client It energypts all the data in the form of eigher It is a combination of Si Various web browsers and login credentials should u for sending the data.	layer. use the communication and transfers data text (encrypted text) SL protocol and HTTP. websites which need se HTTPS protocol





Backbone of SSL -Handshake protocol Page No. Record protocol Date Date SSL header Content Major Minor Compress. type Version Version length Minor Compressed Compressed data MAC SSL V3 Major version - 3 Minor version - 0 Compressed length - The length of compressed fragment. Content type - The higher layer protocol used to process the enclosed fragments. 55L Handshake protocol 1. a Complex protocol. 2. Establishment of secure connection between 2 entities 3. Authentication between client and server. 4 Negotiation of Encryption / MAC algorithm. 5. Exchange cryptographic keys.

simple Handshake protocol client establishment. Auth. & key exchange

Auth. & key exchange, exchange, Hand shake protocol

I and who be perforted Page No. Jankon Lower Date] Complex Handshake Protocol Client hello Share I Server hello Server certificate
Client certif. req. (
Server key exchange
Server hello done Phase 2 Client certificate Phase 3 Client key exchange change cipher spec finished (client handshake) Phase 4 change eigher spec server hardstake finished Phase 1 - 4 Parameters Jarobara Xalama 1 2. Establishment of secure consider between 2 co 1) SSL Version (version 2 or 3) 2) Session id (The id which identifies the entire Jordan Harris Senatex 3) Cipher suite (list of enyptographic algorithms)
4) Compression method (All the details that client has are sent to the server) Hand the graderal

	Page No. Date
m	Handshake protocol wes four phases to complete its cycle-
>	Share 1 - In Phase 1, both client and server send hello-packets to each other:
	Phase 2 - Server sends his certificate and server key exchange It requests for the client certificate. The server ends phase 2 by sending the "server hello done".
>	Phase 3 - In this phase, client replies to the server by sending his certificate and client exchange-key.
	Phase 4 - In Phase - 4, change eigher spec occurs and after this the hardshake protocol ends, first from the client side and then from the server side. SSL Alert Protocol
1	The primary job of the SSL Alext Protocol is to inform the lother end (server or client) about the issues in the current session level alert warring jatal type of alert
	Warning - This has no impact on the connection between sender and receiver. Only the warning

Page No).	
Date		

would be received, the communication / program will continue.

fatal - This immediately breaks the connection between sender and receiver. The communication will stop.

* Alert occurs when the two entities that are communicating face any kind of problem.

* An entity informs the other entity if it encounters any error.

	Type of Alert	Alert Message	Description
	1	close_notify	It notifies that the sender will no longer send any magi
	2	unexpected_message	incorrect message received.
-	3	bad_record_mac	wrong MAC received
	4)	bad_certificate	when the received certificate is carry

SSL change eigher specification protocol

1. It keeps the current status of the protocol (ciphen protocols) that we are using night now.

	Page No. Date
2.	It has only one message (1 Byte.)
3.	This protocol's purpose is to cause the pending state to be copied into the current state
4.	One message of 1 Byte consists of value 1. (1-1-1)
	TLS (Transport layer security)
>	TLS was proposed by IETF (Internet Engineering Tack Force) Tack Force) REC 2246 7 SSL 3.0
	TLS is defined in RFC 2246] SSL 3.0
>	It is a protocol that promate authenticular,
	privacy and data integrity between two
	communicating computer applications.
>	It is designed to promote security in
	transport layer
>	TLS was derived from SSL.
>	Encrypto the communication between web app
	and server.
>	It's the most widely deployed security
	protocol in use today and is best suite
Jan	for web browsers and other applications that
	Prequire data to be securely exchanged over
	a readox.
>	TLS is a cryptographic protocol that provides end
	to end communication settling that
>	It is a underly used protocol for interret
	communication data shaving and online transactions.
- 14	transactions.
3000	HIAC (Host Musey Arthertrope Eds) is
	a (soul made Adadhahad aces) 182 H. J. Allender alegar lager) 183

						Pa	ige No.	
						Da	te	
	G	oals of	TLS	Secure !	1 300	day	04 31	
)				V		
Record	5 (2 - 0	and identi	alitu	un 2'1	as ed we	T WINT	
- Protocol		- 4	enfidenti	and y	(HMAC)	store	
Handsha ke	5 A	A - A.	ntegrity	to 1 and		,		
Ke	6	A	ithertica	icon j avi	ailabille	y		
-	Ne	nd los	TIC.	132 3105	1 1	360377	M DAD	
-	7 16	red for	165.					
Simple		1		1		1	211	
internet		4/		1/K/		A	1	
Communica	0	Oser	Internet	> Web	(-··)	serve	r	-
- tion	-	0 1 -	Internet	V	Interret	France	Task	
-	0	2 7 55	5246	218 RIC	board	at as	211	<
- 1774	200	auther	25/2000	Hat P	dandal	Sew	11	
- 0 .	00	1 111		a widey	tob by		20 000	
Orline		Client	Internet	A	Internet		1000	
transaction	n d	X	M. see	N/w service security	Laker		1 41	<
		/ 1		(Energytion,			hort	4
			7.5	deenyptio		200	12 17	2 19
	Link	sus out	ed mon	01	He co	E10.	Caru	2
higher level 1.					-0	averal	dian	
protocol)	-	Applicati	on on	ممعد والحامو	Handshake	Charge	Alest	Abblicat
1 15.9	4	layer (+	ITTP)	- Lander	Handshake protocol	ciphel spec	Protocol	protocol
700	331	Security (SSL	hayer	- Dono	The state of the s	Prococol		,
(17	Transport	layer	ARKA ARKA	ILS	Recons	trot	col
lower)		Transport (TC	P) (TCP	A Second	
layer 1	12	rterret (ayer	no soldes				
protocol				isal and	A spalling			<
33/3	L	letwork,	nterface	-		1 6		
	3	Edwa L	20	hade state	Windows	2	7 45	2
* T	LS	Record	Protocal	410.4	Was Ad	US NOVUL	Lung	- 4
1	n 0	CI	de out	. 111	xactly.	the s	ame,	as
Н	MA	CINA	A Marie	works of difference of Author	ace be	eing >	that 1	rere
	1-1/1	Ina	or messi	ge Autho	ntication	Code) is	

Page No. Date Date used instead of MAC. Client ? Server --- Hello Get HTTP 1 K - - TIME HTTP answer Complex Client Server Server Thello, key share

2

Rey share centificate

3

Rey share centificate

get HTTP

4 -- HTTP answer

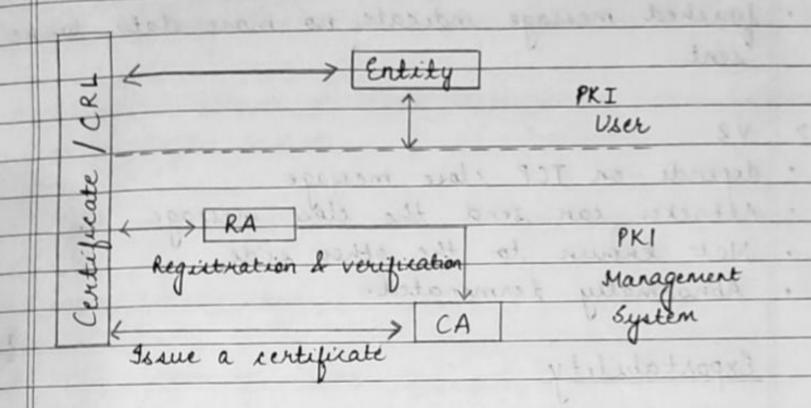
		Page No.
	Difference between 551	L & TLS
	SSL	TLS
Version	3.0	1.0 (RFC2246)
Cipher	Fortezza	X
	The state of the s	79
- bry	Message digest to	Pseudo-random Lunchas to
Cryptogr - phy Secret	Message digest to generate master secret	Iseudo-random function to generate the master secre
Record		make to
Protocol	MAC	HMAC
Alert	20da (n.)	
Protocol	"	(g) (g)
- which	No certificate alert Message"	X
	Message"	JALH 30
estiliane		
ertificate	Complex	Simple
-		

	Page No. [Date]
_	To enable all the services, digital centificates are required
>	To enable all the services, agentic
	At quarter
	A which all match to the waters of
	Public key encryption (Asymmetric key Cryptography)
-	The second of th
	Encryption B Decryption
	Plain Riblic Capter Revente Decompted Received Level Level Level
	Zender XXX
	Digital Certificate
	e se lite combintor / flectronic device
1	Small file on computer / Electronic device.
2	file extension is (. cer.)
5	It is issued by some trusted party fentity. Digital certificate establishes a relationship
	between the user and public key
5.	It requires name of the user and his public
	key.
	O .
	Sample Digital Certificate
	frankel (estaposit
	Username: abc
	Sublic key: (abc &# 12)</th></tr><tr><th></th><th>Serial no: 12345</th></tr><tr><th>-</th><th>Other information: email-id</th></tr><tr><th></th><th>Valid from: 23-04-2022</th></tr><tr><th></th><th>Valid to : 23 - 04 - 2026</th></tr><tr><th>1</th><th>Lesuer Name: Entrust, verisign</th></tr></tbody></table>

		Page No.
		Date
	all the severes and on the	to orable
	Fields of Digital Centificate	homepan
	The state of the s	
>	Version: X.509 - It defines the standigital certificate.	tandard of
	digital certificate.	
>	Signature Algo Identifier - It identifi that you have used.	es the algo
	that you have used.	
	Vser id of issuer	John William
>	CA digital Signature : used during	digital
	(Certification Authority) certificate	verification.
		D
*	de en computer / Electronic device	Home 1
	What is Certification Authority (CA)	o Filesen
V	The state of the s	
	CA are trusted agency that can is certificate	sue aignai
	0	
3335		
3333	Components of PKI	
	Components of PKI	hor go red
1.	Components of PKI Certificate Management System	hor go red
1.	Components of PKI Certificate Management System Digital Certificate	hay ag ta
1.	Components of PKI Certificate Management System Digital Certificate Validation Authority	should be the server
1.	Components of PKI Certificate Management System Digital Certificate Validation Authority	should be the server
1. 2. 3. 4.	Components of PKI Certificate Management System Digital Certificate Validation Authority Certification Authority Registration Authority	should be seen and should be see
1. 2. 3. 4.	Components of PKI Certificate Management System Digital Certificate Validation Authority Certification Authority Registration Authority	skey de sa skey skey skey skey skey skey skey skey
1. 2. 3. 4. 5.	Components of PKI Certificate Management System Digital Certificate Validation Authority Certification Authority Registration Authority End user	See of the page of
1. 2. 3. 4. 5.	Components of PKI Certificate Management System Digital Certificate Validation Authority Certification Authority Registration Authority End user	See of se

Page No.			
Date	7	7	

Architecture of PKI



CRL - Certificate Revocation hist

It is a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted.

		ige No.
-		
>	Block eigher = 40B padding in SSLV3, 44B in TLS	
-	44 B in TLS	Jan 1
-	V	
>	final block of each record is used for the next.	as IV
-	for the next.	
11	and the summer and the summer has	church!
7	Number Header data HMAC &	ura An
1	Stierroot Header data HMAC &	integrity ky
		1
	Record Record HMAC	Pad ding
	Header data	
	Record Encrypted Reader integrity-	encryption
	Acader integrity-	Key
	necord necord	- 18 4
	(the hand a second of the han	> 22 =
	Secure Electronic Transaction (SET)	
	The state of the s	Recey
>	open encryption and security specification to protect credit-card and debit-card transactions on the Internet.	2 desimed
	to protect credit - card and debit - car	d
	transactions on the Internet	2
	. Alexand	3
200	Services of SET:	
>	Provides 2 1000	2 Fach
>	Provides a secure communication channels	el
	Provides authentication by use of digi- certificates.	tal
>	Ensures confidentiality (11.	i i
March 1	only to the parties involved	e is available
	Ensures confidentiality (The information only to the parties involved in the transaction)	ie
	sample duting bendere	40
1		

			Page No.				
	SET Particip	pants:	D. Augustananijast				
i)	Card holder	(vser)	Mules selberter				
ii)	Card holder (Vser) Merchant Issuer (Financial Institution - Bank which provides Payment Land)						
iii)	Issuer / Fin	iancial Enstitution	- Bank which prov	udes			
1		payment i	aid)	21			
iv)	payment card) v) Acquirer (has relation with the merchant for processing of the payment card authorisation)						
	p)	rocessing of the	payment card				
		authorisation)	/ 0				
v)	Sayment Gat	teway - It is a	third party organises and merchant. messages on behalf	ation			
	which exis	ts between client	and merchant.				
	It processes	the payment	messages on behalf	of			
	the mercha	nt)	· ·				
- 11							
vi)	Certificate	Authority - P	whide and verific	š.			
	the digita	el certificate.	souides and verifie				
	V						
	[C. 1 41 11 1	Internet _	Menchant				
	Card Holder		1100000				
			(Internet)				
		C . 4 . W					
		Certificate Authority					
		Processing	Payment				
	Issuer		Onceony				
	Januar						
	Acquirer						
	Payment Notwork						
	(NOA)						

		Page No.
~		Requirements in SET:
~ ~ ~ ~	i) ii) iii)	No message modification Intersperability
~		Acquirer (has relation muth the merchant for expression of the payment conditions of the paymen
~_	1010	V) Soument Gateway - It is a third sorty eyen
	10 }	the present the payment mounger on boha
~ ~ ~	10	50) Centificate Authority - Broneder and veril the tripital centificate

=> SSL attacks feixed in 13-:

There are two types of attacks.

- 1) Downgrade Attack In V2 (Stripping attack). No integrity checks, i.e. Active ottocker con remove cipper suits
- In V3
- · Finished message, i.e., Digest of all the previous mersages.
- · Bosically, it is a type of cylier attack in which fockers downgrade a neb connection from the more secure HTTPS to less secure HTTP
- (2) Truncation Attack In 12 · Depends on TCP Close message Attocker con send the close mag., not known to other side & almormally term sent.

In V3

· Finished message indica ed at ata be soon on et-

- · Bosically. In a truncation attack on attacker inserts into a message a TCP code indicating the message has finished, thus preventing the recipient picking up the rest of the message.
- => Exportability -: . Neak Crypto Export Controls Strong Crypto - Complex mechanism

Im SSL V2

- · Limited to 40 bits
- · Uses 128 bit key in which.

40 bit - Secretly Encrypted with server's Public key
88 bits - Non-secret bits

· Also uses Client Moster key

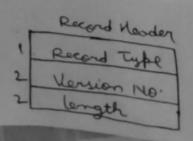
Im SSL V3

- · only 40 bits keys are allowed
- · Serveres con energht keys using 512 bit RSA keys (Normal RSA keys one 1024 bit)
- · Ethomeral key is of 512 bits
- => Encoding -: All Exchanges are in records up to 2148-216-18

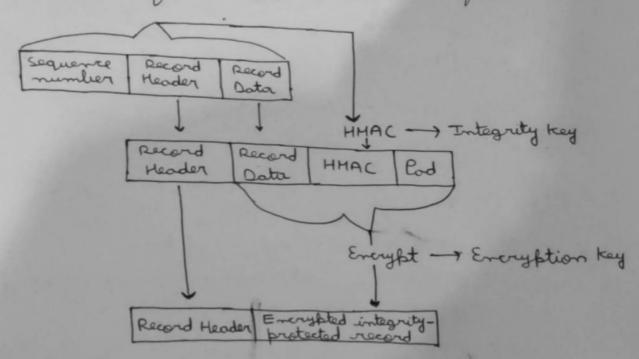
 Standard allows multiple messages in one record or multiple records
 - · Most implementations use Imag/record

Four Record Types:

- 20 = Change Cipter Sper - 21 = Polents (1= worning, 2= Fatal)
- 22 = Hondstake
- 23 = Fotal



- · Each mag. Starts with a 18 mersage-type and 3B mersage length
- => Encrypted Record Protocol -:
- · Integrity is brouided by H-MAC using the integrity key
- · Data profixed by 64 bit sequence
- Black Cipter =) 40 B Rodding in SSL V3, 44B in TLS Final Black of each record is used as IV for the next



Notwork Socuety (unit 4)

(x). Computing the keys:

Alice chooses a random number of and sends it, encuppted with Bobis public key.

Messages, both to prove the knower the keys.

- The notation f(KAvice Bob, R) means that R is cryptographically transformed with Avice and Bob's shared secret KAvice Bob.

		I want to talk, RALI'CE		al Lange e de
		certificate 1 RBab		Ben way been
Choose secrets		S Bob, keyed hash of		compute
compute	Alice		de	K = f(S, RALICE Road)
= f(S Knure Boy		keyed hash of Handshah		Thure Bob
		data protected with		The sale of the sale
		Keys derived from		7 1/11 4/17 1/17

S= Pre-matter secret

K= f(S, RA, RB)

B keys = gi (K, RA, RB)

Rs: 30 bytes

(x). client Authentication:

A process by which uses securely access a server or remote computer by exchanging a digital certificate.

-> The digital certificate is used to cryptographically bind a useris identity to a unique significate certificate.

when to provide acress control.

- Just as an organisation needs to control which hidewideral Users have access to comporate niws and vierousces, they also need to be able to identify which machines & servers have access. -) The digital certificates used for wint and device authentication may look the same as any other digital Certificate but they are direty to have different properties defending on use: -> Client Authentication can be used to prevent unauthorized access. -> It adds a second layer of security to your current username and password combination. (*) · Benofits: - Enought transactions over the notwork. - Validates the sent messaged. - Validates the use fdentity. - You can configure the certificate so that it cannot be exported to other devices, i.e. its unique to the device it is er installed on -> Seaves Litegrity & contident alify. - Chap Ro Prevents malicious attacks.