The SSL/TLS protocol

Myrto Arapinis School of Informatics University of Edinburgh

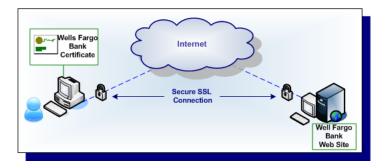
October 30, 2017

イロン イヨン イヨン イヨン 三日

1/27

SSL/TLS protocol

Goals: Confidentiality, Integrity, Non repudiation



SSL/TLS use X.509 certificates and hence asymmetric cryptography to exchange a symmetric key. This session key is then used to encrypt subsequent communication. This allows for **data/message confidentiality**, and message authentication codes for **message integrity** and thus, **message authentication**.

SSL/TLS protocol



Google

One account. All of Google.

Sign in to continue to Gmail

	•
M	lyrto Arapinis
myrto.	arapinis@gmail.com
Password	
	Sign in
leed help?	
Need help?	

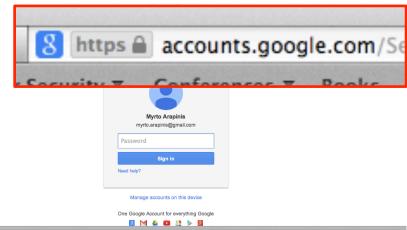
Manage accounts on this device

One Google Account for everything Google

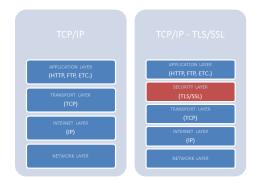


SSL/TLS protocol

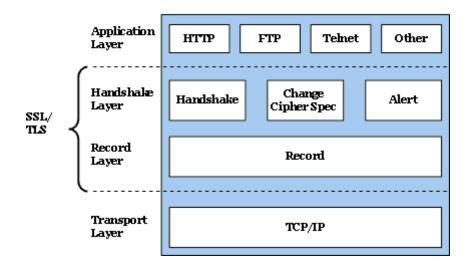




TCP/IP protocol stack



- TCP/IP provides end-to-end connectivity and is organized into four abstraction layers which are used to sort all related protocols according to the scope of networking involved
- The SSL/TLS library operates above the transport layer (uses TCP) but below application protocols



SSL/TLS handshake protocol



	f ireshark File	Edit View Go	Capture Analyze Stat	istics Tel		Wireless		Help	🗳 🕓 k 🎅 🔹 📾 52% 🖲	Wed 22:47	9 IE
● ⊖ ⊖					iii tist	Smail.pcapn	9				×
	2 🛞 🚺	S 🗙 🗋	۹ 🔶 🖉	ē 👱 1	- 1	⊕,	0,0	2 11			
Apply a	a display filter ·	<%/>								Expre	ssion +
No.	Time	Source	Destination	Protocol	Length						
	5.946868310	172.16.76.158	172.217.23.45	TCP					Win=29200 Len=0 MSS=1460 SACK_PERM=1 TS	Sval=2158060	TSecr
	5.977374146	172.217.23.45	172.16.76.158	TCP					Seq=0 Ack=1 Win=64240 Len=0 MSS=1460		
		172.16.76.158	172.217.23.45	TCP				Seq=1	Ack=1 Win=29200 Len=0		
	5.978337850	172.16.76.158	172.217.23.45	TLSv1		Client He					
	5.979058758	172.217.23.45	172.16.76.158	TCP				Seq=1	Ack=208 Win=64240 Len=0		
125	6 015001000 Cipber Suite	172 217 22 45 es Length: 30	172 16 76 159	TI Su1	2014	Server Me	110				
	v Cipher Suite										
			SA WITH AES 128 GCM SH	A256 (0xc	82b)						
	Cipher Su	ite: TLS ECDHE RSA	WITH AES 128 GCM SHA2	56 (Øxc02	f)						
			A WITH CHACHA20 POLY1			9)					
	Cipher Su	ite: TLS_ECDHE_RSA	WITH_CHACHA20_POLY130	5_SHA256	(Øxcca8)						
	Cipher Su	ite: TLS_ECDHE_ECD	SA_WITH_AES_256_GCM_SH	A384 (Øxc	82c)						
	Cipher Su	ite: TLS_ECDHE_RSA	WITH_AES_256_GCM_SHA3	84 (ØxcØ3)	8)						
	Cipher Su	ite: TLS_ECDHE_ECD	SA_WITH_AES_256_CBC_SH	A (0xc00a)						
			SA_WITH_AES_128_CBC_SH)						
			_WITH_AES_128_CBC_SHA								
			WITH_AES_256_CBC_SHA								
			TH_AES_128_CBC_SHA (0								
			TH_AES_256_CBC_SHA (0								
			AES_128_CBC_SHA (0x002								
			AES_256_CBC_SHA (0x003								
			BDES_EDE_CBC_SHA (0x00	0a)							
		Methods Length: 1									
		Methods (1 method)									
	Extensions l Extension: s										
		Extended Master Sec	ret								
		renegotiation info	ier								
		elliptic curves									
		ec point formats									
		SessionTicket TLS									
		next protocol negot	iation								
	▶ Extension: /	Application Laver P	rotocol Negotiation								
0030 72	2 10 bd 9e 00 0	30 16 03 01 00 ca	01 00 00 c6 03 r								
		7e 7a 5d 98 42 80 dd 45 fe 94 6c 41		~z] .B .ElAe*							
			03 20 33 00 41 #(.c 04e#	5.0						
0 7	Secure Sockets Laye	r (ssi), 207 bytes							Packets: 475 - Displayed: 475 (100.0%) - Load	time: 0:0.11 P	rofile: Default

Image: Image:<		Edit View Go	Capture Analyze Sta		ny Wireless Too	ls Help	B () * ? •	🖲 🏶 52% 💽 Wed 22:4	17 Q 🖃
Apply a diredum filter _ <	● ● ●				tlsGmail.pcapng				κ.
Image Image Destination Proceed Length Minimage 12 5.9775157.01 172.157.755.18 172.157.755.18 172.157.755.18 172.157.755.18 172.157.755.18	🧧 📕 🙋 🚺	🖻 🎽 🎽	۹ 🔶 🏓 🖉	🐔 🗶 🔔	. ♀, ♀,	् 🎹			
132 5,977515165 172.12.23.45 TCP \$4 558367421 Ack-18 Kin-24208 Lenne 133 5,977851565 172.27.23.45 TCP \$6 4553568 172.27.23.45 TCP 60 443-53638 Ack-18 Kin-46228 Lenne Image: Comparison of the Comparis	Apply a display filter	<%/>						🖃 👻 Ex	pression +
133 5,97837099 172.217.21.45 TLS.VL 201 Client Hello 134 5,97837099 172.217.21.45 TLS.VL 201 Client Hello 135 6,97836709 172.217.21.45 TLS.VL 201 Client Hello 136 6,97836700 172.217.21.45 TLS.VL 201 Client Hello 136 6,97836700 172.217.21.45 TLS.VL 201 State Stat									
134 5,9988578 172,127,23,45 172,167,6158 172,167,6158 172,167,6158 172,167,6158 172,172,23,45 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,16,76,138 172,112,172,128,78,128,128,128,128,128,128,128,128,128,12						K] Seq=1 Ack=1 Wi	n=29200 Len=0		
135 6.61563120 172.167.24.35 172.167.676.550 136 6.61565320 172.172.73.45 172.167.766.550 136 6.61565320 172.172.73.45 172.167.766.500 136 6.61565320 172.167.75.45 172.167.75.45 172.167.75.45 136 6.6156520 172.167.75.05 172.172.73.45 172.167.75.45 172.167.75.45 136 6.6156520 172.167.75.05 172.167.75.45 172.167.75.45 172.167.75.45 137 167.75 147.55.25 201.50 on interface 8 157.77 179.75.75.25 277.167.75.25 277.167.75.25 277.167.75.25 135.201.0000000000000000000000000000000000									•
136 6.63856425 172.17.21.45 TCP 54 35638-442 (ACC Seque28 Ack-2761 Vin-33588 Len+0 FTeme 135: 2816 bytes on uir (2522 bits), 2814 bytes capture (2522 bits) on line (Frace 8) Ethernet Frace 302 (Bet 222 bits) on line (Frace 8) Ethernet II, Src: Wware, Me: Add 2 (00:3555:06:74:02), Dist: Wware, 9:e08:82 (00:06:23:99:08:82) Internet Frace 00 Version 4, Src: 172.17.23.45 Dist: 172.16.75.188 Transsission Control Protocol, Src: Port: 443, Dist Port: 3558, Seq: 1, Ack: 286, Len: 2760 Version: 175.12 One 200 TS:12.7 Record Layer: Headback Protocol: Server Hello Version: 155.12 One 200 Version: TS: 1.2 0.63893 Version: TS: 1.2 Version: TS: 1.2 Version: TS: 1.2 0.63893 Version: TS: 1.2 Version: TS: 1.2 Version: TS: 1.2 Version: TS: 1.2 0.63893 Version: TS: 1.2						K] Seq=1 Ack=208	Win=64240 Len=0		
Frame 135: 2014 bytes on wire (22512 bits), 2014 bytes captured (22512 bits) on interface 0 Ethernet II, Srci Wanner, Brickladd (20043506: ff0:4702), Dat: Wanner, Brielsball (00042799:08:02) Internet Protocol Version 4, Src: 172,712,73,05, Dst: 172,718,76, DSt General State Lyper Variant Protocol Version 4, Src: 172,712,73,05, Dst: 172,718,76, DSt General State Lyper Variant Protocol Version 4, Src: 172,712,73,05, Dst: 172,718,76, DSt General State Lyper Variant State Lyper <tr< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr<>									
E thermet II, Src: Wware_10:7dic2 (00:50:55:16:7dic2), Doi: Vmare_9e:08:02 (00:06:25:90:08:02) Transision Control Protocol, Src Port: 433, Ds: Port: 35688, Seg: 1, Ack: 208, Len: 2760 Secure Societa Lyper Toternet Type: Hendhake (22) Version: T5 1:2 (00:838) Length: 76 * Handshake Protocol: Server Hello Handshake Protocol: Server Hello Handshake Protocol: Server Hello Handshake Protocol: Server Hello Length: 77 * Handshake Protocol: Server Hello Handshake Protocol:							61 Win=33580 Len=0		
<pre>internet Protocol Version 4, 5rc: 172.27.27.36, Dst: 177.18.76.188 Transmission Cortol Protocol, Sr Port: 43, Dst: 177.18.76.188 Secure Sockets Layer for content Protocol Version 1 Secure Hello Content Protocol Version 1 Secure Hello Indidate Protocol: Server Hello Indidate Protocol: Server Hello Indidate Protocol: Server Hello Secure Sockets Content Protocol Version 1 Secure Sockets Content Protocol Version Version: TS 1.2 (0x0383) Readow Secure Sockets Content Protocol Version 1 Secure Version Readow Secure Sockets Content Protocol Version 1 Secure Version Readow Secure Sockets Content Protocol Version 1 Secure Version Readow Secure Sockets Content Protocol Version 1 Secure Version Readow Secure Sockets Content Protocol Version 1 Secure Version Secure Sockets Content Protocol Version 1 Secure Version Secure Sockets Content Protocol Version 1 Secure Version Secure Sockets Secure Version 1 Secure Version 1 Secure Version Secure Sockets Secure Version 1 Se</pre>									
Transission Control Protocol, Src Port: 430, Bst Port: 33638, Seg: 1, Ack: 286, Len: 2760 Secure Sockets Usper * T.Skil, 2 Record Lyer: Hundhake Protocol: Server Hello Context Type: Hundhake Protocol: Server Hello Hundshake Type: Server Hello (2) Length: 72 * Handshake Protocol: Server Hello Length: 72 * Hundshake Protocol: Server Hello Coperating Server Hello (2) Length: 72 * Hundshake Type: Server Hello (2) Length: 72 * Settem Sino Length: 0 * Settem Sino Length: 74 * Extensions Length: 75 * Extensions Length: 76 * Extensions Length: 72 * Extensions Length: 72 * Extensions Length: 74 * Extensions Length: 75 * Extensions Length: 74 * Extensions Length: 75 * Extensions Length: 74 * Extensions Length: 75 * Extensions Length: 75 * Extensions Securitication_Info * Extension: Securitication Laper Protocol Repetiation * Extension: Application Layer Protocol Repetiation *					02 (00:0c:29:9e:0	98:02)			
<pre>\$ \$cccr8 5cckets Layer \$ \$ \$cccr8 5cckets Layer \$ \$ TSUL? & Record Layer: Houdshake f7dccoll: Server Hello Content Type: Houdshake (22) Version: TS 1.2 (0x830) Length: 7 \$ \$ Houdshake Type: Server Hello (2) Length: 7 Version: TS 1.2 (0x830) \$ \$ Random \$ Session To Length: 0 Compression TS 1.2 (0x830) \$ \$ Random \$ Session To Length: 0 Compression Heldon intl (0) \$ \$ Extension: record, main \$ Extension: record, main \$ Extension: server, mae \$ Extension: record, main \$ Extension: server, mae \$ Extension: server, mae \$ Extension: server, mae \$ Extension: record, main \$ Extension: server, mae \$ Extension: secver, main \$ Extension: secver, main \$ Extension: deploted M8 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 20 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 00 00 00 00 \$ So So I 20 00 00 00 00 00 00 00 00 00 00 00 00</pre>									
<pre>v T.Scil.2 Record Layer: Hundshake Proteool: Server Hello Content Type: Hundshake Proteool: Server Hello Length: 75 1.2 (Bx0838) Hundshake Type: Server Hello (2) Length: 72 Version: TLS 1.2 (Bx0838) Hundshake Type: Server Hello (2) Length: 72 Version: TLS 1.2 (Bx0838) Pandom Server June Server June June June June June June June June</pre>			t: 443, Dst Port: 35	538, Seq: 1, AG	:K: 208, Len: 2766	,			
Content Type: Handshake (22) Version: T5 1.2 (0x839) Length: 76 Handshake Protocl: Server Hello () Handshake Protocol: Server Hel									
Version: TiS 1.2 (0x8283) Length: 76 Hindshakk Protocil Server Hello Lingth: 76 Mindshakk Protocil Server Hello Lingth: 70 Session: TLS 1.2 (0x083) * Rondon Session: TLS 1.2 (0x083) * Extensions Length: 2 * Extensions Length: 32 * Extensions receptization_info * Extension: servery mane * Extension: ec.golif. Fortocil Negotization * Extension: ec.golif. Fortocil			tocot: server netto						
Length: 76 Handshake Type: Server Hello Handshake Type: Server Hello Length: 72 Server Joint 5, 1, 2 (De038) Session D Length: 0 Cipher Suite: TLS_ECONE_RSA_WITH_AES_128_GOM_SHA256 (0x-027) Compression Method: null (0) Extensions Length: 22 Extensions Length: 22 Extensions Length: 24 Extensions Length: 24 Extension: SessionTicket TLS Extension: Application Layer Protocol Negotiation Extension: Application Layer									
<pre>v Hundshake Protocol: Server Hello Handshake Type: Server Hello Length: 72 Version: T5. 12. (8x893) > Random Schart Stute: TJ.S. EURL PSA. WITH_AES_128_GOM_SHA256 (8xx82?) Compression Method: null (0) Extension: Ength: 32 > Extension: rever_name > Extension: server_name > Extension: secure TLA Code 00 00 46 03 ></pre>		L.2 (0X0303)							
Handshake Type: Server Hella (2) Length: 72 Version: TLS 1.2 (0x8383) P Rodom Comperson Method::ull (0) Extensions Length: 32 P Extensions Length: 32 P Extension: remeptiation_info P Extension: server Types P Extension: server Types P Extension: Application Layer Protocol Negotiation P Extension: ec_point_romats New 51 St 12 Ge 64 FS 22 Ge 55 F2 C2 Ge 81 Ge 64 62 St 12 Ge 64 Ge 85 St 12 Ge 64 FS 12 GE		tocol: Server Hello							
Length: 72 Version: T5.1.2 (0x0303) > Random Session TD Longth: 0 Cipher Suite: T5.1.2 (0x0303) > Estemission: Instruct, 10 Estemission: renerginate > Estemission: renerginate > Estemission: renerginate > Estemission: Renerginate > Estemission: Renerginate > Estemission: Application Layer Protocol Negotiation > Estemission: Application Diagot Bob			21						
Version: TLS 1.2 (0x038) > Random Session: ID Longht: 0 Chapter State: TLS_Inc.Edx MitH_LES_128_COM_SMA256 (0xc02f) Chapter State: TLS_Inc.Edx MitH_LES_128_COM_SMA256 (0xc02f) Extensions Length: 32 > Extensions length: 32 > Extensions increation_info > Extension: server_name > Extension: Application Layer Protocol Nepotiation > Extension: capolitation Layer Protocol Nepotiation > Extension: capolitation cayer Protocol Nepotiation > 80 St Si 12 G		Jper berrer neete (.,						
<pre>> Random Session To Length: 0 Session To Length: 0 Capter Saite: TLS_ECOME_SKAYTH_AES_128_GCM_SHA256 (0x<021) Captersion Archdo: null (0) Detensions Length: 32 Detensions Length: 32 Detensions Length: 32 Extension: Server_ame Extension: Server_ame Extension: SessionTicket TLS Extension: Application Layer Protool Negotiation Extension: cpoint_fromats Extension: cpoint_fromats Extension: cpoint_fromats Extension: cpoint_fromats Extension: content = 00 = 00 = 00 = 00 = 00 = 00 = 00 =</pre>		5 1.2 (0x0303)							
Cipher Suite: TLS_ECOME_RSA_KTIN_LSS_128_GCM_SHA256 (0xc02f) Compression Method: unll (0) Extensions Length: 32 B Extensions Length: 32 B Extension: remoti Lation_Info B Extension: SessionTicket ILS B Extension: Application Layer Protool Negotiation B Extension: Applicat									
Compression Method: null (0) Extensions: Length: 32 > Extension: server_nem > Extension: server_nem > Extension: Server_nem > Extension: Exceled Master Secret > Extension: Application Layer Protocol Negotiation > Extension: ec_point_Fronts 000 03 50 112 of 04 7 92 00 00 04 04 03	Session ID	Length: 0							
Compression Method: null (0) Extensions: Length: 32 > Extension: server_nem > Extension: server_nem > Extension: Server_nem > Extension: Exceled Master Secret > Extension: Application Layer Protocol Negotiation > Extension: ec_point_Fronts 000 03 50 112 of 04 7 92 00 00 04 04 03			TH AES 128 GCM SHA25	6 (0xc02f)					
Extension: renegatiation_info Extension: server_name Extension: server_name Extension: Extended Master Secret Extension: SessionTicket TLS Extension: Application Layer Protocol Negotiation Extension: Application Layer Protocol Negotiation Extension: Capital Contents 200 08 35 08 12 08 04 08 20 00 06 40 03									
Extension: server, name	Extensions	Length: 32							
 Extension: Extended Moster Secret Extension: SessionTicket TLS Extension: Application Layer Protool Negotiation Extensinter Protool Ne	▶ Extension:	renegotiation_info							
 Extension: SessionTicket TLS Extension: Application Layer Protocol Regotilation Extension: ec_point_formats Tot c7 79 00 00 10 00 3 03 00 4C 02 00 00 48 03	▶ Extension:	server_name							
b Extension: Application Layer Protocol Regotiation b Extension: Application Leyer Protocol Regotiation b:00 fr 0 cr 39 00 00 00 00 00 00 00 00 00 00 00 00 00	▶ Extension:	Extended Master Sec	ret						
Extension: ec_point_formats 8030 for for 77 00 00 00 10 03 03 00 4 C 02 00 00 48 03									
0830 fa f0 c7 97 00 00 10 c3 30 00 4c 02 00 00 48 03			rotocol Negotiation						
0400 05 50 51 02 00 40 47 52 32 05 50 51 02 00 40 47 52 32 03 90 11 14	▶ Extension:	ec_point_formats							
0400 05 50 51 02 00 40 47 52 32 05 50 51 02 00 40 47 52 32 03 90 11 14									
0805 35 65 35 65 35 65 35 65 35 72 97 10 83 85 <									
966 4 2 00 c0 27 4 06 40 2 0 f1 9 1.0 9 11 9 0 8 0 40 9 0 0 5									
8888 32 00 0b 00 02 01 00 16 03 03 0c 2a 0b 00 0c 26 2	0060 42 00 c0 2f 00	00 20 ff 01 00 01 0	80 00 00 00 00 B						
8090 80 8c 23 80 84 a5 30 82 84 a1 30 82 83 89 a0 83									
Secure Sockets Layer (ssl), 2760 bytes			52 05 59 80 05 ···#.						
	😑 🏋 🛛 Secure Sockets Layı	er (ssl), 2760 bytes				P	ackets: 475 - Displayed: 475	(100.0%) - Load time: 0:0.11	Profile: Default

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tor	ols Help 🗳 🕙 🕴 🛜 🐠 📾 52% 💽 Wed 22:48 Q, 📰
😝 🖯 💮 tisGmail.pcapng	2
🖉 📕 🖉 🕲 🚞 🖺 🕱 💆 🧣 🌩 🗮 🖉 💆 🛄 🍳 🍳	Q Ⅲ
Apply a display filter <\$%/>	Expression +
No. Time Source Destination Protocol Length Info	
134 5.979058758 172.217.23.45 172.16.76.158 TCP 60 443-35638 [AG	[K] Seg=1 Ack=208 Win=64240 Len=0
135 6.015031282 172.217.23.45 172.16.76.158 TLSv1 2814 Server Hello	
136 6.015054625 172.16.76.158 172.217.23.45 TCP 54 35638-443 [AG	CK] Seq=208 Ack=2761 Win=33580 Len=0
137 6.015117278 172.217.23.45 172.16.76.158 TLSv1 841 CertificateSe	erver Key Exchange, Server Hello Done
138 6.015126370 172.16.76.158 172.217.23.45 TCP 54 35638+443 [AG	[K] Seq=208 Ack=3548 Win=36500 Len=0
serialNumber: 7377627938644829374	
signature (sha256WithRSAEncryption)	
▶ issuer: rdnSequence (0)	
▶ validity	
▶ subject: rdnSequence (0)	
v subjectPublicKeyInfo	
▶ algorithm (rsaEncryption)	
v subjectPublicKey: 3082010a0282010100aa00c2a0f111bb011132301a5fcdfd	
<pre>modulus: 0x00aa00c2a0f111bb011132301a5fcdfdff7762a8fc0fd60a</pre>	
publicExponent: 65537	
▶ extensions: 8 items	
w algorithmIdentifier (sha256WithRSAEncryption)	
Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption)	
0120 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 000 0130 aa 00 c2 a0 f1 11 bb 01 11 32 30 1a 5f cd fd ff	
0140 77 62 a8 fc 0f d6 0a 85 67 fe ef cb f7 93 4e 9a wb gN.	
0150 ce 49 bc d5 8c 3b 67 b7 4f c6 a7 ab da f8 e8 04 .I;q. 0	
0160 8a 89 c6 da 99 ec 3d 42 8c 0e c0 86 0c c4 25 e3B%.	
0170 ee 93 af 17 0c b3 51 88 54 f8 86 71 bb 73 df b4Q. Tq.s 0180 cf 0e 3a e1 ab 72 f9 9e 88 78 26 5b a4 f7 d8 0drx&[
0180 cf 0e 3a e1 ab 72 f9 9e 88 78 26 5b a4 f7 d8 0drx&[0190 c2 a0 70 79 56 c2 43 07 38 de bd 15 a5 54 be 78vV.C. 8T.x	
01a0 c7 af 1a cd 3b 71 07 aa ec 2e fb 18 ee fe 78 16;qx.	
01b0 ab 5b 37 e4 97 c0 42 d6 00 48 3d 15 64 0b 76 7c .[7BH=.d.v]	
01c0 b3 8b d9 16 41 3b 4b 0d a5 f7 d8 76 d8 7c e7 4bA;Kv. .K	
01d0 ba 3e a1 a8 a4 1e 32 58 fb 4c 9d 30 01 fe 7f 90 .>2X .L.0 01e0 61 2a ec a3 d1 28 7d 57 1c 1f a7 e1 48 df 65 02 a*(\WH.e.	
01f0 75 37 2b c3 52 72 7c b6 5e be f5 ed 16 d0 bc 7c u7+.Rr . ^	
0200 ef 09 2f b5 9e 57 46 e2 f8 2c d3 ed 4a 14 7a 57/WFJ.zw	
0210 04 e4 07 8e al b4 10 fe 27 8c ca 7e e3 el b6 27 '	
0220 d7 b5 44 52 99 0b 0b 0c 92 36 47 22 0c e7 19 bdDR6G"	
0230 02 03 01 00 01 a3 82 01 67 30 82 01 63 30 1d 06	
0250 03 01 06 08 25 06 01 05 05 07 03 02 30 35 06 03+05	
Frame (841 bytes) Reassembled TCP (3119 bytes)	
O Z INTEGER (pkcs1.modulus), 257 bytes	Packets: 475 - Displayed: 475 (100.0%) - Load time: 0:0.11 Profile: Default

www.gmail.com's certificate

GeoTrust Global CA			
→ 📴 Google Interne → 📴 accounts.g	,		
Common Name	Google Internet Authority G2		
	7377627938644829374		
Version			
Signature Algorithm Parameters	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11) none		
Not Valid Before	Thursday, 6 October 2016 13:59:57 British Summer Time		
	Thursday, 29 December 2016 12:28:00 Greenwich Mean Time		
Public Key Info			
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)		
Public Key	$\begin{array}{l} 255\ \ yetes: ; AA OO (22 A OF 11 B BO (1 11 23 O (1 A 5 C O) F 77.62 \\ 356\ \ yetes: ; AA OO (22 A OF 11 B BO (1 11 23 O (1 A 5 C O) F 07.62 \\ 476\ (3 A 7 A D A A 5 5 7 F E C 16 7 7 3 A 4 5 A C 4 5 A C O 5 8 C 0 5 F 0 7 \\ 476\ (3 A 7 A D A A 5 F E 5 0 A A 9 0 C 5 A 0 7 0 3 F C 10 A 2 8 C 0 F C 0 7 6 C \\ 425\ (5 E F 3 A 1 7 O C 8 3 1 E 6 5 4 7 8 6 7 1 8 6 7 3 0 F 1 A C 7 0 F 3 \\ 510\ F 0 1 7 0 1 7 5 3 1 5 0 7 5 1 7 \\ 510\ F 0 1 7 0 1 7 5 1 5 1 7 \\ 510\ F 0 1 7 0 1 7 5 1 5 1 7 \\ 510\ F 0 1 7 0 1 7 \\ 510\ F 0 1$		
Exponent			
Key Size	2048 bits		

• • • • • • • • • • • • • • • • • • •	ed 23:02 🔍 🗄
Apply a dividyr Mitr <k></k> > Denmano Proved Length Media 106 6.43554625 172.16.76.158 172.217.23.45 TCP 54 35636-43 LCK Seq=208 Accharact Accharat Accharact Accha	
Imm Source Desination Protocol Longit Mon 135 6.051504255 172.157.7316 TC 94 35.0534431 ACK1 Seq=208 Ack-2761 Win=33588 Len=0 136 6.0511278 172.217.21.45 T17.16.77.1518 TLS.77.145 TF 94 35.0534431 ACK1 Seq=208 Ack-2761 Win=33588 Len=0 136 6.0511278 172.217.21.45 T17.16.77.1518 TLS.77.145 TF 94 35.0534431 ACK1 Seq=208 Ack-2761 Win=33588 Len=0 138 6.0511278 172.217.23.45 TLS.71.15 TLS.71.15 TLS.71.15 TLS.71.15 TLS.71.15 TLS.71.15 TLS.71.15 TLS.71.2 ACK1 Sequent Ack1 Ack1 Seq=208 Ack-2761 Win=3588 Len=0 200 Content Type: Hondshake Protocol: Client Key Exchange 401 Request 401 Request 401 Request Version: TLS 1.2 (Box883)1 Length: TA TLS.71.2 Record Layer: Hondshake Protocol: Client Key Exchange 401 Request 401 Request VE Diffic-Heltuan Client Key Exchange Length: TA 400 Red TA 401 Request 401 Request VE Signed Client Key Exchange Length: TA 400 Red TA 400 Red TA 400 Red TA <th></th>	
Tome Source Domination Protocol Longit Mo 135 6. 81354425 172.15.67.518 172.217.23.45 TP 54 35584431 ACK1 Seq=208 Ack-2761 Min=33588 Len=0 136 6. 81511278 172.217.23.45 TP 54 35584431 ACK1 Seq=208 Ack-2761 Min=33588 Len=0 138 6. 81511278 172.217.23.45 TP TLSVL 841 CertificateServer Key Exchange, Server Hello Done 138 6. 81511278 172.217.23.45 TP 43356.4431 ACK1 Seq=208 Ack-2761 Min=3588 Len=0 138 6. 8151879 172.15.76.188 172.217.23.45 TLSVL 180 Client Key Exchange, Change Clipher Spec, Hello Request, Hello Receiver, Sockast Layer * TLSVL2. Record Layer: Handshake Protocol: Client Key Exchange 451 Request 451 Request * TLSVL2. Record Layer: Handshake Protocol: Client Key Exchange 172.217.2345 172.217.2345 * TLSVL2. Record Layer: Handshake Protocol: Client Key Exchange 186.617.017.017.017.017.018.018.018.018.017.017.017.018.018.018.017.017.018.018.018.017.017.018.018.018.018.017.017.018.018.018.017.017.018.018.018.017.017.018.018.018.018.017.017.018.018.018.018.017.017.018.018.018.017.017.018.018.017.017.018.018.018.017.017.018.018.018.018.018.017.017.018.018.018.018.017.017.018.018.018.017.017.018.018.018.017.017.018.018.018.017.017.018.018.018.018.018.017.017.018.018.018.017.017.018.018.018.017.017.018.018.017.018.018.017.	* Expression
136 6.01556405 172.107.217.23.45 TCP 54 3538443 1ACK Seq=208 Ack=273 Unreal-358 Leneed 136 6.0151677 172.107.23.45 TCP 54 3538443 IACK Seq=208 Ack=273 Unreal-358 Leneed 138 6.0151677 172.107.23.45 TCP 54 3538443 IACK Seq=208 Ack=273 Unreal-358 Leneed 138 6.0151677 172.107.23.45 TCP 54 3538443 IACK Seq=208 Ack=324 Unreal-358 Leneed 138 6.0151677 172.107.23.45 TCP 54 3538443 IACK Seq=208 Ack=324 Unreal-358 Leneed 136 6.0151677 172.107.23.14 TCP 34 3538443 IACK Seq=208 Ack=324 Unreal-358 Leneed 560.075 Sockets Layer TSU:12.207.23.14 TCP 34 Becovert TSU:12.207.23.14 TCP 7 TSU:12.207.23.117.217.23.14 TCP 34 Becovert TSU:12.207.23.14 TCP 34 Becovert 560.075 Sockets Layer TUSU:12.800.071 Heavest Heavest Heavest Heavest 120.12.107.12.13.107.107.1344 FCSU FCSU Heavest Heavest Heavest 120.12.107.117.117.117.117.117.117.117.117.117	
137 6.01511228 172.217.23.45 172.16.76.158 TLSVL. 841 CertificateServer Key Exchange, Storwer leile Done 138 6.01511228 172.217.23.45 172 172.16.76.158 172.217.23.45 174 138 6.01511228 172.217.23.45 174 154 543564431 AUC(1 Seque 24431 AUC(1 Seque 24	
138 6.01370470 172.17.23.45 TCP 54 3538347 136.01370447 138 0.0137047 138 0.013	
L00 6.013370071 172.17.27.73.14 OCSP 491 Request Secure Sockets Layer File Handbake Protocol: Cllent Key Exchange Content: Type: Handbake Protocol: Cllent Key Exchange Content: Type: Handbake Protocol: Cllent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange Handbake Type: Clent Key Exchange 100 60 S 56 16 7 d 2 2 80 c 2 90 66 82 88 64 50 0 r/V, r. 1	
Secure Sockets Layer Y TLSVL2. Record Layer: Handbake Protocol: Client Key Exchange Gostent Type: Handbake (22) Version: TLS 12 (0x833) Length: 70 Y Handbake Protocol: Client Key Exchange Usersion: TLS 12 (0x833) Length: 76 Y Handbake Protocol: Client Key Exchange Network Protocol: Client Key Exchange Sockets Layer: Handbake Protocol: Client Key Exchange Network Version: TLS 12 (0x833) Length: 76 Y Handbake Protocol: Client Key Exchange Sockets Layer: Handbake Protocol: Client Key Exchange Network Version: TLS 12 (0x833) Length: 76 Y HE DIFF-Pollawa Client Protocol: Network Version: TLS 12 (0x833) Y Handbake Protocol: Client Key Exchange Network Version: TLS 12 (0x833) Y Handbake Protocol: Network Version: Y Handbake Protocol: Y Handbake Y Y Handbake Y Protocol: Y Handbake Y Y Handb	Jest
▼ TL5:1.2. Record Layer: Handshake Protocol: Client Key Exchange Context Type: Handshake Cl2:1 Version: TL5 1.2 (Book33) Length: 20 ■ Finite Headshake Type: Client Key Exchange Mandshake Type: Client Key Exchange Exclusion: Client Key Exchange Exclusion: Client Key Exchange The Version: Client Key Exchange Booksey Length: 65 ■ Exclusion: Client Key Exchange Exclusion: Client Key Exchange Booksey Length: 65 ■ TL5:1.2. Record Layer: Handshake Protocol: Chinge Client Spectra TL5:1.2. Record Layer: Handshake Protocol: Chinge Client Spectra TL5:1.2. Record Layer: Handshake Protocol: National Handshake Hessiges ■ 0 do C J M do 0 do	
Content Type: HandShake (22) Version: T5.12 (0x830) Length: 70 NandShake Protocol: Client Key Exchange NandShake Protocol: Client Key Exchange (16) is for 317 key Length: 65 Pubkey Length: 65 Pubkey Length: 65 TiSs/12 Record Layer: HandShake Protocol: Change Clipter Spec > TiSs/12 Record Layer: HandShake Protocol: Key Lipte HandShake Messages 00 00 55 65 67 7 d 20 00 67 20 00 67 20 00 00 42 dk., is	
Version: TLS 1.2 (08808) Length: 70 V Handbake Protocol: Client Key Exchange Industry Industry K Diffic-Heltman Client Params Public Protocol: Client Key Exchange Industry Robit Params Public Protocol: Change Clipher Spec Protocol: Change Clipher Spec Robit Params Public Params Pub	
Length: 70 V HandShake Type: Cluent Key Exchange HandShake Type: Cluent Key Exchange Cluength: 6 V EC D1718-Hellen Cluent Key Exchange V EC D1718-Hellen Cluent Paras V Exchange Cluent Cluent Paras V Exchange Cluent Cluent Paras V Exchange Cluent Cluent Paras V Exchange Cluent Cluent Sector Paras V Exchange Cluent Cluent Sector Paras V Exchange Cluent Cluent Sector Paras V Exchange Cluent Sector Para	
<pre>v HandShake Protocol: Client Key Exchange HandShake Type: Client Key Exchange (16) Length: 66 v EC 0171:eHellwan Client Parmas Pubkey Length: 65 Tybkey Length: 65 Tybkey Length: 65 Tybkey Zength: Clange Clipher Spec Protocol: Change Clipher Spec V Zength: Devri HandShake Protocol: Public HandShake Hessages 00 06 95 61 07 06 20 06 22 36 08 02 06 00 07.1 174.02 Accord Layer: ClangBoother Protocol: Public HandShake Hessages 00 06 95 61 07 06 20 06 22 36 08 02 06 00 07.1 174.02 Accord Layer: ClangBoother Protocol: Public HandShake Hessages 00 06 95 61 07 06 20 08 02 21 09 125 00 07.0 172.08 25 06 10 08 07 07 00 00 00 02 21 01 125 00 07.0 08 05 10 06 07 07 00 00 00 07 07.0 09 06 05 07 07 09 76 00 12 20 09 125 00 00 00 07 07 00 06 13 74 02 07 67 03 01 04 05 04 02 01 03 00 07.0 00 06 01 74 02 07 67 03 01 04 05 04 02 01 03 00 07.0 00 06 01 74 02 07 67 03 01 04 05 04 05 04 03 00 07 05 00 07 09 77 03 77 03 10 08 05 04 02 00 08 08 00 07 07 05 00 07 09 77 03 07 07 08 05 04 00 01 00 07 07 05 00 07 09 77 03 07 07 08 05 04 00 01 07 07 05 00 07 09 77 03 07 07 08 05 04 00 01 00 07 07 05 00 07 09 77 03 07 07 08 05 04 00 01 00 07</pre>	
HandSake Type: Clent Key Exchange (16) Length: 66 * EC Diffiel-Hellan Clent Params PARKey Length: 63 * Total Length: 64 * Total Length: 65 * Total	
Length: 66 v EC 51714-01Lans Client Params Pubbey Length: 65 Pubbey 2005 > TSU:2 Record Layer: Anadabae Protoci: Aligne Clipter Spec > TSU:2. Record Layer: Anadabae Protoci: Aligne Clipter Spec TSU:2. Record Layer: Anadabae Protoci: Aligne Clipter Spec 0 00 55 56 70 70 62 80 62 20 58 00 42 60 70 70 71. 0 00 55 56 70 70 62 80 62 20 58 00 42 60 70 70. 0 12 68 55 60 71 62 80 62 21 69 12 50 11 - 6. 0 00 55 56 70 72 55 53 80 80 20 80 42 50 11 - 6. 0 00 55 56 70 70 75 75 75 75 75 75 75 75 75 75 75 75 75	
* EC 51716-Hellan CLient Params Publey Length: 65 Publey Length: 65 Total: 2000: Length: 60 Total: 2000: Length: 61 Total: 2000: Length: 61 Total: 2000: Length: 61 Total: 2000: Length: 62 Total: 2000: Length: 61 Total: 2000: Length: 62	
Publicy Length: 65 Publicy VestBase VestBase <td></td>	
Nukkej Lóška (2020) Lóška (2020) <thloška (2020)<="" th=""> Lóška (2020)</thloška>	
▷ TLSJL2. Record Layer: Indhame Clpher Spec Protocol: Change Clpher Spec TLSJL2. Record Layer: Indhame Protocol: Nulley Hendbake Messages 00 00 50 55 16 7 d 2 2 00 6 2 3 06 8 0 2 5 00 7 V/ 00 00 5 55 16 0 2 2 5 5 5 0 3 6 0 2 0 2 0 1 4 5 5 5 1 5 0 0 7 V/ 00 5 5 5 16 0 2 2 5 5 5 0 3 6 0 5 0 5 1 5 1 5 1 6 0 0 0 4 2 4 1 00 5 5 6 1 6 0 2 5 5 5 0 3 6 0 5 0 1 5 0 5 1 6 2 5 1 0 1 7 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0	
 ▶ TL-X1.2 Record Layer: Handshake Protocol: Nulliple Handshake Messages ▶ 0 59 59 57 07 42 00 62 29 68 20 60 80 50 07/0, 6. ▶ 0 60 50 55 10 40 04 00 50 50 20 14 20 00 70 10 10 10 10 10 10 10 10 10 10 10 10 10	
000 000 <td></td>	
110 00 06 03 04 04 00 b0 b0 b2 ac 14 c5 bc ac bc ac bc ac bc bc <t< td=""><td></td></t<>	
2021 17.2 db 36 10.b df 7 27.4 22.2 31.6 16.1 /1.1P. 2020 17.2 db 36 bb 45 dd 40.6 bb 45 dd 40.6 bb 45 dd 40.6 2040 45.8 bb 75.4 31.4 cb 75.4 7.4 cb 75.4 7.4 cb 75.4 cb 7	
100 06 04 04 00 00 04 00 00 04 <t< td=""><td></td></t<>	
550 07 57 31 d4 c5 55 57 48 1c cf 42 27 08 77 71 .],s ₆ ,,,∧wq 650 cf 37 42 y7 83 56 9f 40 01 27 c6 44 ba 5c 130 .t.,,,K.0 770 5c 95 c7 93 52 cf 32 a1 f4 43 55 64 20 1c 5b 33, 6,,,K.0 80 54 c4 38 00 10 11 56 30 50 42 80 00 40 00 5,,,	
666 de 13 74 92 17 83 56 97 80 91 22 68 4 55 130,,, K., 6 75 56 b C 79 55 27 53 1 56 97 80 91 22 68 4 55 12 30,,,,,,, .	
777 5c 96 c7 99 36 2 f c3 1 f 4 3 55 4 6 20 1 c 55 3 \6(6(6(13) 803 51 4 8 3 50 8 1 8 1 6 1 5 3 8 0 8 1 8 1 6 3 5 8 0 2 8 0 8 0 8 0 8 0 5	
880 35 14 83 83 80 81 81 16 83 83 80 28 80 88 80 8 80 8 5	
200 16 37 73 75 62 63 4c 07 10 6c f2 83 c2 34 a3 71 .7subcLl4.q	
ana 16 37 73 75 62 63 46 67 10 6c f2 83 c2 34 a3 71 .7suocl.,l.,4.q b.	
teo da 81.62 e8b.	
CDIffe-Hellman client publicy (ssl.handshake.client.point), 65 bytes Packets: 475 - Displayed: 475 (100,0%) - Load time:	

🔹 Wireshark File	Edit View Go Ca	pture Analyze Statis	ics Telephony	Wireless Tools Help	🖸 🕓 🏄 🛜 🔶 🏭 46% (🕩 Wed 23:02 🔍 🔚
00			🚺 tist	Smail.pcapng		
	- 🗅 🗙 🖸 🖉	२ 🗢 💌 🖉 🖲	2 💷 📗	0, 0, 0, <u>T</u>		
Apply a display filter	<೫/>>					Expression
. Time	Source	Destination	Protocol Length			
136 6.015054625	172.16.76.158	172.217.23.45		35638-443 [ACK] Seq=208 Ack=276		
137 6.015117278	172.217.23.45	172.16.76.158		CertificateServer Key Exchange,		
138 6.015126370	172.16.76.158	172.217.23.45		35638-443 [ACK] Seq=208 Ack=354		
139 6.017904477	172.16.76.158	172.217.23.45		Client Key Exchange, Change Cig	her Spec, Hello Request, Hell	o Request
140 6.019370071	172.16.76.158	172.217.23.14	OCSP 491	Request		
Length: 70	ocol: Client Key Exch					
	ocol: Client Key Exch					
Length: 66	rpe, citeric Key Excha	iige (10)				
	ellman Client Params					
Pubkev Le						
		aa51d1c08e2d75d731d40d	5b5b7			
		pec Protocol: Change				
	Change Cipher Spec (2		aprox aprox			
Version: TLS 1						
Length: 1						
Change Cipher	Spec Message					
▶ TLSv1.2 Record L	yer: Handshake Proto	col: Multiple Handsha	ke Messages			
800 00 50 56 f0 7d	2 00 0c 29 9e 08 02	08 00 45 00 .PV.}.	.)E.			
810 00 a6 c3 9a 40	10 40 06 ba 02 ac 10	4c 9e ac d9@.()L			
17 2d 8b 36 01 130 8e 94 bd 4d 00	b 8f a7 2f 49 2e 21		. /I.!P.			
340 04 58 0c 88 22			Z			
50 d7 5d 73 1d 40			/.wq			
de 13 74 92 b7		4b a5 e1 30t	,.K0			
	f c3 a1 f4 43 b5 d4		c., .[3			
	1 01 16 03 03 00 28 18 79 12 f3 90 21 a7		(
	i3 4c 07 10 6c f2 83		l4.g			
b0 da 81 62 e8		b.				
🔵 🍸 🛛 Record Layer (ssl.re	ord), 6 bytes			Pa	:kets: 475 · Displayed: 475 (100.0%) · Loa	d time: 0:0.11 Profile: Defaul

miTLS, Triple Handshake, SMACK, FREAK, Logjam, and SLOTH											
i mitls.org	/pages/atta	cks									
SimSec 🔻	CSexam ▼	La cryptograts dév	oilés Cor	nferences 🔻	Resea	archProfiles 🔻	Security-Club *	Teaching 🔻	Tutoring		
		TLS miTLS	TLS miTLS Publications		acks	Code	FlexTLS	People			
			Alert	3SHAKE	VHC	SMACK Lo	ogjam SLOTH				
		Protocol Cr	yptographic	Implementatio	n De	eployment					

A Zoo of TLS attacks

Attacks on TLS that break the intuitive security property of a virtual recreation of a physically secure channel can be categorized along three dimensions.

- 1. Protocol logic vs. cryptographic design flaw
- 2. Specification/Standard vs. Implementation errors
- 3. TLS vs. Context

Flaws in the protocol logic

Attacks targeting the protocol logic may for instance cause the client and server to negotiate the use of weak algorithms even though they both support strong cryptography.

If the faulty regolation logic conforms to the specification, then the attack is on the specification test (as, e.g., sparially enabled by the False Start modification), if an implementation can be specification to biling (biling) and the program (biling) (bilinew), Langley II is an attack on the implementation. As many aspects of the standard can be underspecified or ambiguous, it is not always possible to distinguish between these two cases.

Another class of protocol logic flaws are state-machine bugs [Early CCS Attack, SMACK Attack].

The attack can also be either an attack on TLS proper, or on its context, e.g. if the attacker can just change the configuration files to deactivate strong cryptography. As the TLS standard does not describe APIs or configuration file formats, context specific attacks are always implementation specific.

The renegotiation attack [TLS_Reneg_Attack] is a logical attack on the TLS standard, where one peer believes it is running the first handshake on a connection, while the other peer is running a re-handshake. miTLS prevents the renegotiation attack by implementing the renegotiation extension.

More generally, the TLS specification is vague about how applications should handle data coming from consecutive sessions, e.g., whether it is asket to join them and consider them as a single stream, of it the user should be notified of the change of context. The renegotiation extension partially ites the problem, but it still leaves room for our elert attack, where the attacker can turn any authentic fatal attacts in to a averning atter, which get signatored by default.

Much not seriously, resuming the attacker controlled assess on a a different connection re-analyses the renegotation state. This table is a series of the state of the state

Cryptographic design flaws

Attacks exploiting cryptographic design faws may simply result from cryptanahytic progress against the cryptographic building blocks of U.S. Threy can, however, allo nesult from improper non-blackbox use of otherwise sector cryptographic constructions. An example for this is chosen ciphertext chaining (CBC) mode encrypton. Early versions of U.S. allow using trowledge of the next inflatization vector (V) to set up adaptive plaintext attacks, see, e.g. Q. penests. Lurchive for a first mention of the SEAST attack: ≣ ৩৭ে 14/27 Client and server are allowed to initiate renegotiation of the session encryption in order to:

- Refresh keys
- Increase authentication
- Increase cipher strength
- ▶ ...

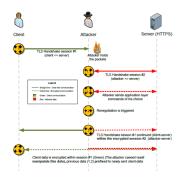
Client or server can trigger renegotiation by sending a hello meesage

イロト 不得 とくき とくき とうき

15 / 27

SSL/TLS renegotiation weaknesses

- Renegotiation has priority over application data!
- Renegotiation can take place in the middle of an application layer transaction!



(Detailed on the board)

Incorrect implicit assumtion: the client doesn't change through renegotiation

◆□ → < □ → < Ξ → < Ξ → < Ξ → Ξ → ○ Q ○ 17/27

Attacker:

GET /pizza?toppings=pepperoni;address=attacker_str HTTP/1.1
X-Ignore-This:(no carriage return)

Attacker:

```
GET /pizza?toppings=pepperoni;address=attacker_str HTTP/1.1
X-Ignore-This:(no carriage return)
```

Victim: GET /pizza?toppings=sausage;address=victim_str HTTP/1.1 Cookie:victim_cookie

```
Attacker:
GET /pizza?toppings=pepperoni;address=attacker_str HTTP/1.1
X-Ignore-This:(no carriage return)
```

```
Victim:
GET /pizza?toppings=sausage;address=victim_str HTTP/1.1
Cookie:victim_cookie
```

Result: GET /pizza?toppings=pepperoni;address=attacker_str HTTP/1.1 X-Ignore-This:GET /pizza?toppings=sausage;address=victim_str HTTP/1.1 Cookie:victim_cookie

```
Attacker:
GET /pizza?toppings=pepperoni;address=attacker_str HTTP/1.1
X-Ignore-This:(no carriage return)
```

```
Victim:
GET /pizza?toppings=sausage;address=victim_str HTTP/1.1
Cookie:victim_cookie
```

Result: GET /pizza?toppings=pepperoni;address=attacker_str HTTP/1.1 X-Ignore-This:GET /pizza?toppings=sausage;address=victim_str HTTP/1.1 Cookie:victim_cookie

\Rightarrow Server uses victim's account to send a pizza to attacker!

<ロ > < 回 > < 画 > < 直 > < 直 > < 直 > 三 の Q (C) 18/27

Twitter status updates using its API by posting the new status to http://twitter.com/statuses/update.xml, as well as the user name and password

Twitter status updates using its API by posting the new status to http://twitter.com/statuses/update.xml, as well as the user name and password

```
Attacker:

POST /statuses/update.xml HTTP/1.1

Authorization: Basic username:password

User-Agent: curl/7.19.5

Host: twitter.com

Accept:*/*

Content-Length: 140

Content-Type: application/x-www-form-urlencoded

status=
```

Twitter status updates using its API by posting the new status to http://twitter.com/statuses/update.xml, as well as the user name and password

```
Attacker:
POST /statuses/update.xml HTTP/1.1
Authorization: Basic username:password
User-Agent: curl/7.19.5
Host: twitter.com
Accept:*/*
Content-Length: 140
Content-Type: application/x-www-form-urlencoded
status=
Victim:
POST /statuses/update.xml HTTP/1.1
Authorization: Basic username:password...
```

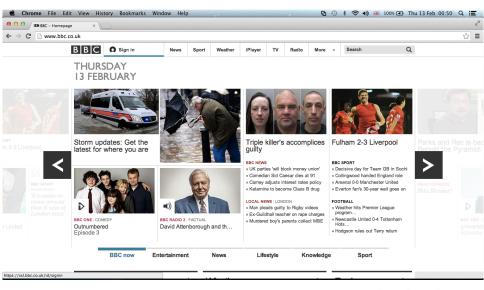
Twitter status updates using its API by posting the new status to http://twitter.com/statuses/update.xml, as well as the user name and password

```
Attacker:
POST /statuses/update.xml HTTP/1.1
Authorization: Basic username:password
User-Agent: curl/7.19.5
Host: twitter.com
Accept:*/*
Content-Length: 140
Content-Type: application/x-www-form-urlencoded
status=
Victim:
POST /statuses/update.xml HTTP/1.1
Authorization: Basic username:password...
```

 \Rightarrow the attacker gets the user name and password of the victim!

The SAML Signle Sign On (SSO) protocol

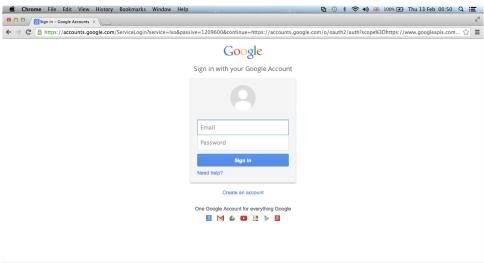
SAML SSO protocol



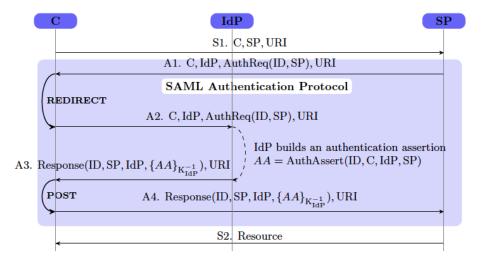
SAML SSO protocol

🗯 Chrome File Edit View Histor	y Bookmarks	Window Help						G	- * -	ê 🜒 🗄	🖶 100% 🕻	Thu 1.	3 Feb 00:5	0 Q	Ξ
\varTheta 🔿 🕤 🛛 📾 BBC - Sign in 🛛 🗙															R _M
← → C 🔒 https://ssl.bbc.co.uk/id/si									Qź	3 =					
	BBC O	Sign in Now	s Sport	Weather	IPlayer	TV More - Search Q									
		N IN BBC il	D												
	Donthave a BBC ID? Please register. Email or usemane Password						Other ways to sign in Wart be signed in to the BBC for 20 days. If cancer If cancer Bases only use block Float ways at the for over. We want have on point your attivity to Floatbook or Cancer								
	Remember of Sign in	Forgot your password? Remember me Unics if you're using a shared computer. Sign in Cancel						About BBC ID Simple Register quickly and easily to comment, add fervoirities, and more Safe We store your information securely, and we never than it without your permission.							
							Spam-fre We'll only se BBC ID help	nd you em	ails if you ask fo	r them.					
https://sil.bbc.co.uk/id/statecookie/google.com	BBC iWonde	ack Up Your become the function with the top t													

SAML SSO protocol



SAML SSO protocol (OASIS 2005)

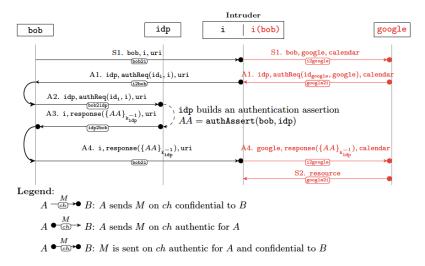


Google's SAML-based Single Sign-On for Google Applications deviates from the above protocol for a few, seemingly minor simplifications in the messages exchanged:

- G1. ID and SP are not included in the authentication assertion, i.e. AA = AuthAssert(C; IdP) instead of AuthAssert(ID; C; IdP; SP);
- G2. *ID*, *SP* and *IdP* are not included in the response, *i.e.* $Resp = \text{Response}(\{AA\}_{K_{ldP}^{-1}})$ instead of $\text{Response}(ID; SP; IdP; \{AA\}_{K_{ldP}^{-1}}).$

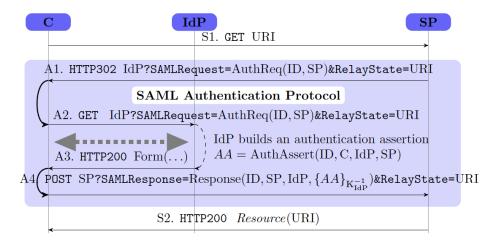
Attack Google's SSO implementation

[A. Armando, R. Carbone, L. Compagna, J. Cullar, L. Tobarra, "Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps", (FMSE'08)]



୬ <u>୦</u> ୦ 25 / 27

SAML SSO protocol (OASIS 2012)

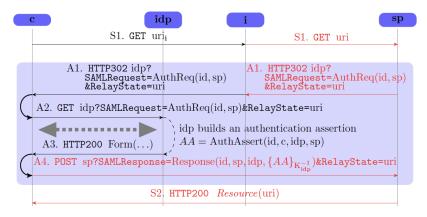


◆ □ → < ≥ → < ≥ → ≥ </p>

9 < ○
26 / 27
</p>

Attack SAML SSO protocol (OASIS 2012)

[A. Armando, R. Carbone, L. Compagna, J. Cullar, G. Pellegrino, A. Sorniotti, "From Multiple Credentials to Browser-Based Single Sign-On: Are We More Secure?", Chapter in Future Challenges in Security and Privacy for Academia and Industry]



 \Rightarrow XSS attack on SAML-base SSO for Google Apps