

SSL Presentation

- 1. Practical SSL With Apache and PHP
- 2. Part I: The Players
- 3. Basics: Hashing
- 4. Basics: Symmetric Encryption
- 5. Basics: Asymmetric Encryption
- 6. <u>Certificates</u>
- 7. Certificate Authorities
- 8. Transport Layer Security
- 9. TLS: What It Does
- 10. TLS: The Handshake Protocol
- 11. TLS: Server Handshake Response
- 12. TLS: Server Certificate
- 13. TLS: Server Certificate Verification
- 14. TLS: Root Certificates
- 15. TLS: Failed Verification
- 16. TLS: Client Handshake Response
- 17. TLS: Handshake Wrapup
- 18. TLS: Record Protocol

- 19. TLS: Record Protocol (cont'd)
- 20. Apache's mod_ssl
- 21. OpenSSL
- 22. PHP's OpenSSL Support
- 23. The Big Picture
- 24. Part II: SSL-enabled Webservers
- 25. HTTPS Requirements
- 26. Using PHP to simplify PKI
- 27. A Local Certificate Authority
- 28. A New Server Certificate
- 29. Global SSL Directives
- 30. A Passphrase Dialog
- 31. Apache Per-host SSL Directives
- 32. Cipher Suite
- 33. Cross Your Fingers
- 34. Revoking A Server Certificate
- 35. Part III: Application Level SSL
- 36. Example: Stored Secrets
- 37. Class openSSL
- 38. Signing
- 39. Encrypting

[Presentation]

- 40. Decrypting
- 41. Verifying
- 42. Checking The Key Passphrase
- 43. Parsing X.509 Data
- 44. Discussion
- 45. Thank You!
- 46. <u>Resources</u>
- 47. Download



Practical SSL With Apache and PHP

... and OpenSSL, mod_ssl, X.509 Certificates.

Chris Snyder and Mike Southwell New York PHP 22 November 2005



Part I: The Players

Cryptography basics

Certificates

Transport Layer Security

What you need:

mod_SSL OpenSSL toolkit PHP --with-openssl



Basics: Hashing

not reversible has native PHP support

md5('hello') : 5d41402abc4b2a76b9719d911017c592 sha1('hello') : aaf4c61ddcc5e8a2dabede0f3b482cd9aea9434d



Basics: Symmetric Encryption

Symmetric: both sides use the same key

Reversible Requires out-of-band key exchange. PHP needs mcrypt extension

3DES AES Blowfish RC4

We each have the same secret key.

You encrypt a value with this key, and send it to me. The only way to decrypt it is with our shared secret key.



Basics: Asymmetric Encryption

Asymmetric: encryption and decryption use different keys

Reversible Allows public knowledge of encryption key PHP needs OpenSSL extension

RSA

I give you my public key.

You encrypt a value with my public key, and send it to me. The only way to decrypt it is with my private key (which only I have).



Certificates

X509 Public Key Infrastructure

RFC3280 defines Certificates and Certificate Revocation Lists.

http://rfc.net/rfc3280.html



Certificate Authorities

Certificate Authorities provide secured identification of a server, and enable asymmetric encryption of messages between client and server.



Transport Layer Security

A 30-second history

Secure Sockets Layer was developed by Netscape in 1994 as a protocol which permitted persistent and secure transactions. In 1997 an Open Source version of Netscape's patented version was created, which is now OpenSSL. In 1999 the existing protocol was extended by a version now known as Transport Layer Security (TLS). By convention, the term "SSL" is used even when technically the TLS protocol is being used.



TLS: What It Does

- TLS encrypts messages.
- TLS makes message alteration detectable.
- TLS authenticates message senders/receivers.



TLS: The Handshake Protocol

SSL encrypts every transaction between the client browser and the server, which makes it possible to send sensitive information back and forth without fear that it will be readable by anybody who might intercept it. It can do this because, before it begins transferring encrypted information, the server engages in an elaborate negotiation with the client, called the Handshake Protocol. This negotiation has the following parts:

• The client sends a request to the server which, because it uses the https (as opposed to http) schema, initiates the negotiation.

🍘 ssl-aptanline.txt - Ether	real			
Flo Edit Yow Go Cap	pturo Analyzo Statistias	Holp		
	🖌 📄 🗀 🕷	0 3 3 4	\$ €	중 앞 [
Diters		-	Expression	. Dear Apply
1. (2010) A (1. (2010) A (1. (2010))	inne	Destinet on		hi i
1 0.000000 1 2 0.002545 1		Driadcast 192.138.1.102		Who has 192.168.1.17 те 192.168.1.102 192.163.1.1 is at 00:0с:41:72:8e:56
3 0.002577 1		167.205.245.81		Standard query A mail.sptonline.net
4 0,127533 1	67.208.245.81	192.158.1.102	DNS	Etandard query response A 167,206,5,250
5 0.143190 1 5 0.156568 1		167.205.5.250	TOP	[TCT Zerowindow] 3304 > https: [SYN] Sep=0 Ack=0 win=0 Len=0 https:> 3204 [SYN, ACK] Soq=0 Ack=1 Win=4380 Len=0 MSS=14±0
7 1.156678 1		167.206.5.250	TCP	3304 > https:[ALK] Eeg-1 Ack-1 w1=45505 Len-0
8 0.157/06 1	.92.165.1.102	167.206.5.250	SSEV2	ulisht Hello
9 1.276579 1		192.158.1.102	SSL	[Unneassembled Packet] 2204 - brand [a: 4] - calles ack 1481 -de 65525 - colo
10 1.276863 1 11 1.294577 1		167.206.5.250		3304 > https:[ALK] Beq-108 Ack-1461 wir-65535 Len-0 Continuation pate
12 0./25790 1		167.206.5.250		3304 > https:[ACK] Seq-108 Ack-2734 Wir-64262 Len-0
13 5.238019 1		167.206.5.250		Client Key Exchange, Change Ciphen Spec, Encrypted Handshake
14 5.256120 1 15 5.257220 1		192.158.1.102 167.206.5.250	TLS TLS	Charge C'pher Spec, Entrytted Handslake Message Application Data
10 5.277154 1		192.158.1.102	SSL	[Uniteassembled Packet]
17 5.277462 1	92.165.1.102	167.206.1.210	TCP	3304 -> https://www.sederals.ack=4237.wir=65535.i=n=0
18 5.250125 1	67.205.5.250	192.158.1.102	TIS	Continuation Cate, [Unceassembled Packet]
Internet Protoco □ Inansmission Con Source pert: 3:	: 192.158.1.102 () 7, Shc: 192.158.1 trol (mitocol, Sh 304 (3204) ht: https (443) ht: 0 (relative	00:04:41:5d:23:27), .102 (192.165.1.102), DST:	2.165.1.1 (00:00:41:72:59:56) 167.206.5.250 (167.206.5.250) nt: https (448), Seq: 0, Ack: 0, Len: 0
0000 00 0C /1 72 8		1 93 2F 08 00 45 00	or	v Ar./E.
0010 00 30 50 14 4	40 00 80 06 3a du	1 CO 48 01 66 47 CE	.CP.6	···· ·····
	01 hh eh 05 75 dt 00 00 02 04 05 b4	00 00 00 00 70 02		
	VO VO VZ V4 VE D4	OT OT OF OS		
J bestination Fort (top ds:port),	abut Incost science			
pestr attor -orc (tcp dstpcrt),	2 DYC JF: 2010 281 M:0			



TLS: Server Handshake Response

The server responds with a plain-text message consisting of the following parts:

- 1. An exchange method to be used for passing back and forth the keys to be used for encrypting information. This is typically either RSA or Diffie-Hellman-Merkle. If it is RSA, the server must send along also a Certificate (discussed below).
- 2. The type of encryption to be used (RC4 or preferably 3DES).
- The technique to be used for calculating the Message Authentication Code, a checksum appended to messages and used to verify that the message contents havenâ€[™]t been tampered with. Typically MD5 or SHA-1.

	_	nline.txt																										
Flo	Edic	Yen (Go C	apturo	Analy	20 St	ctistic	5 Hol	-																	_		
	ě.			1		ß	×	Ø	3		9 4		¢ 4	0 7	F ₹	F			(€,	Q,	Q,	++				K	
<u>Diters</u>												- 1	ixpress	ion	gear	6pply												
Nu -		Time		Since				Des	lin- t m			1	Profe	i fui	i i													
		0.0000		192.1					adca				AF. P									2.16		102				
		0.0025								3.1.10			AF.P DNS									:8e:						
		0.1275					L			1.1.1			DNS									1.205						
		8.1431								5.2			TER												ACK-		-0 Lo	en=0
		2.1565 2.1566								1.1.10			TOP IOP												380 L Len-0		PISS=_	400
	8	1.157/	16	192.1	65.1	.102		16	7,206	.5.2	5 C		SSEV	i uli	sπt	Hel	10					-						
		1.2765 1.2768								1.1.10			ICP					Pac a			=	-1.1	an		5535			
		2.2345								3.1.10			SSL		ntin.				28	4-TA	с Л.	.K-14	OT W	0		Len-o		
		0.4257								5.5.2			TCP												4262			
		5.2380 5.2561).5.23 3.1.1(TLS	C1	EIIU .	Key	EXU	he' u Sruck	le, i	C: an	ite (iphe Le.u	n Spe	≝1., < 1. 11	Encry	pted a	Harids	hake
F	Ve C · · · ·	indshal ensfion Ishen (essfion Iallian Ishen s	: TL 5000 TD 45 L	5 1.0 Leng engt ength	(CX(th: 7 h: 0 : 16)301) 75		nt Ha	110	C.)																		
		Cipher						Contra La Co																				
0200 0210 0220 0230	01 05	91 50 ta 00) 16 - A9 - 71	01 hl	0 80 n Ah	06 05	3 = 7 77 4 01 0	12 01	48 0 9e 9	08 00 01 66 99 0d 40 00	47 50	се 18 00	F	g;	: 2. 5													
0240	13		1 80 1 00	03 00	3 00	07	38 0	10 06 10 00	35 1	10 02 00 00	00	90		9														
00000	00) 3Z QQ	00 (04 0	00 0	05	00 0)0 2t	00 (00 16	00	00	.2.			·												
0070	00	00 fa	2 11	00 0	00	00	00 1 62 (15 QU	00 1	2 00	06	de																
0.90	24	61 eC	ŔŔ	ξ7 f	- Ra	ÅÅ	e7 l	4 3 8	8f :	20 of	72	ue																
Doher s	pecif	ication (ss	d.hano	shake.c	F: 28.	J DI 28	L M: 0																					
	-																											



TLS: Server Certificate

RSA key exchange enhances security by requiring the server to send a Certificate to the client. This Certificate is a binary collection of the following information:

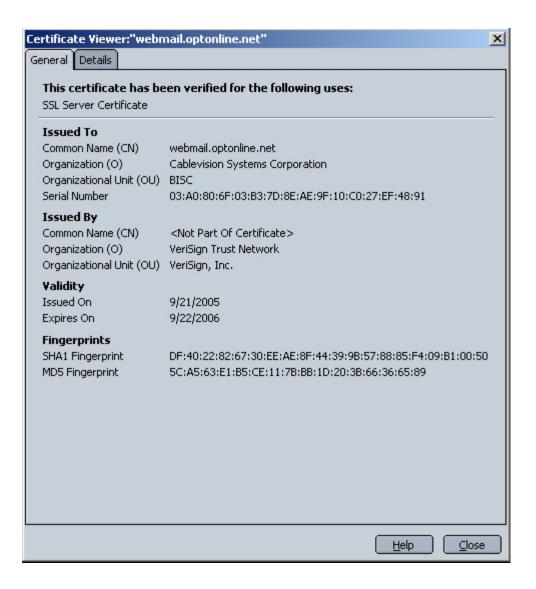
- 1. Its identity
- 2. Its own attestation that it really is who it has said
- A Certificate Authorityâ€[™]s attestation that the serverâ€[™]s attestation is true
- 4. Its public key, which may be used to encrypt the message encryption key, randomly generated by the client

🚱 ssl-aptanline.txt - Ethereal 📃	
Flo Edit Yow Go Capture Analyze Statistics Holp	
$\blacksquare \blacksquare \blacksquare \circledast \circledast \models \square \times @ 2 2 + \Rightarrow \Rightarrow 2 + [\square \exists 0, 0, 0] \blacksquare \blacksquare 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 =$	0
Expression. Dear Apply	
No - Toe Score Destination Protoni foil	
1 0.000000 192.165.1.10Z Driadcast ARP Who has 192.168.1.17 Te 192.168.1.102 2 0.002545 192.165.1.1 192.158.1.102 ARP 192.163.1.1 is at 00:00:41:72:8e:56	
2 0.002545 192.165.1.1 192.158.1.102 ARP 192.163.1.1 is at 00:00:41:72:8e:56 3 0.002577 192.166.1.102 167.205.245.81 DNS Standard guery A mail.optonline.net	
4 0.127533 167.208.245.81 192.158.1.102 DNS Etandard query response A 167.206.5.250	_
> 0.1431±0 192.16±.1.102 167.205.5.250 TCP [TCF Zerowindow] 3304 > https:[SYN] Seb=0 Ack=0 win=0 Len=0 5 0.156568 167.206.5.250 192.168.1.102 TCP rttcs > 3204 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=14±0	0
7 0.156678 192.168.1.102 167.206.5.250 (CP 3304 > https [ALK] Ecq-1 Ack-1 w1n-65535 [cn-0	
8 3.157/36 192.169.1.102 167.236.5.250 SSLV2 ulient неllo 9 3.276579 167.206.5.250 192.168.1.102 SSL [Unneassembled Packet]	
10 1.276863 192.165.1.102 167.206.5.250 (LP 3304 > https:[ALK] seq-106 Ack-1461 w17-65535 Len-0	
11 0.204577 167.205.5.250 192.158.1.102 SSL Continuation Date 12 0.425790 192.169.1.102 167.205.5.250 TCP 3304 > https:[ACK] seg-106 Ack-2734 Wir-64262 Len-0	
13 5.238019 192.165.1.102 167.206.5.250 TLS Client Key Exchange, Channe Cipher Spet, Encrypted Handshak	(e
14 5.256130 167.205.5.250 192.168.1.102 TLS Change Cipher Speck Entryptied Handslake Message Sequence homber, 1 (referitive sequence homber)	-
<pre>[Next sequence number: 1461 (relative sequence number)] Acknowledgement number: 106 (relative ack number) Header Tength: 20 bytes # Flags: 0x0018 (PS-, ACK) Window size: 4485 Checksum: 0xebsb [connect] @ [SEQ/ACK analysis] <u>[Tris is an ACK to the segment in Frame: 8]</u> [Tris is an ACK to the segment was: 0.110273000 seconds] SECURE SOCKET Layer [unreascenoled Pecket: ESL]</pre>	
0000 31 1f 30 1d 06 03 55 04 02 12 16 56 65 72 59 53 1.00Vonfs 00d0 69 67 66 20 54 72 75 73 74 20 46 65 77 77 6f 72 fon inus t wetwor 00e0 69 31 17 66 03 50 40 00 13 00 56 65 72 69 k1.0veri 00e0 53 69 67 66 2c 20 49 66 67 26 31 33 30 31 06 03 ctign, the cliptol	
01e0 60 31 17 30 15 06 03 55 04 0b 13 0e 56 65 72 69 k1.0	
00†0 53 69 67 68 20 20 49 68 63 28 31 33 30 31 06 03 insign, to d.1001 0100 55 04 06 12 20 56 65 72 60 52 60 67 68 20 49 56 invPVen feign In	
0110 74 65 77 64 61 77 69 6f 64 61 62 20 53 65 77 76 ternational very	
0120 60 72 20 45 41 20 2d 20 45 60 61 75 73 20 33 31 er CA - Class 31 0130 43 30 47 06 03 55 04 0b 13 40 77 77 72 e 76 65 IQG.U§www.ve	
10140 JZ 64 JZ 64 67 67 57 55 65 65 66 75 47 50 53 70 49 1015100,0 007075 1	
0160 41 42 49 4d 49 54 59 20 -4d 54 44 2e 28 63 29 39 - AECLITY ILTD.(d)9	
0170 - 07-20-56-65-72-69-50-6967-68-30-18-17-0d-30-35 - 7 Menipi gr005 0180 - 30-37-30-38-30-30-30-30-30-30-30-12-0d-30-36-30 - 07080000-002060	
0190 37 30 38 32 33 35 39 35 39 54 30 81 43 31 00 30 70823595 9201.0	
	-
jecure Socket Layer (sd), 1460 byta F: 261 D: 281 M: 0	



TLS: Server Certificate Verification

• The client browser recognizes the Certificate Authority and thus verifies the authenticity of the connection.





TLS: Root Certificates

It can do this because it has pre-installed certificates from many Authorities.

🕲 Certificate Manager	
Your Certificates Other People's Web Sites Authorities	
You have certificates on file that identify these certificate authoriti	es:
Certificate Name	Security Device 🖳
VeriSign, Inc.	
Verisign Class 3 Public Primary Certification Authority	Builtin Object Token
Verisign Class 1 Public Primary Certification Authority	Builtin Object Token
-Verisign Class 2 Public Primary Certification Authority	Builtin Object Token
Verisign Class 1 Public Primary Certification Authority - G2	Builtin Object Token
Verisign Class 2 Public Primary Certification Authority - G2	Builtin Object Token
-Verisign Class 3 Public Primary Certification Authority - G2	Builtin Object Token
-Verisign Class 4 Public Primary Certification Authority - G2	Builtin Object Token 🛛 🗐
VeriSign Class 1 Public Primary Certification Authority - G3	Builtin Object Token 🚽
View Edit Import Delete	
	ОК <u>H</u> elp



TLS: Failed Verification

If there is a conflict between the name on the certificate and the name of the server, the browser pops up a "Domain Name Mismatch†notice, allowing the user to decide whether to continue.

Security Error: Domain Name Mismatch	×
You have attempted to establish a connection with "mail.optonline.net". However, the security certificate presented belongs to "webmail.optonline.net". It is possible, though unlikely, that someone may be trying to intercept your communication with this web site.	
If you suspect the certificate shown does not belong to "mail.optonline.net", please cancel the connection and notify the site administrator.	
View Certificate	
OK Cancel Help	



TLS: Client Handshake Response

 Assuming the client does trust the server, it generates a random key to be used by the server for message encryption. It then encrypts that key with the serverâ€[™]s public key, and sends it back to the server.

u	: 704	Go	Capturo	Analyza	Statistic	Holp													
n a				0	A ×	i a	3	4	s 40	不力			Ð		1 🖭		4 55	×	6
	n		CC2977					_		1 1					•			v	
r:						-		<u> </u>	apression.	. Gear &	ppiy _								
-	Time		Since			Destinet		P	30030 - 2010 -	fu" i									
	0.000		192.1			Dread:				Who has						102			
			192.1				58.1.102 05.245.0			192.163 Standar									
4	0.12/	(5.33)	167.2	08.24:	.81	192.18	58.1.103	. D	NS	Etandar	d quer	y nosp	oonso A	167.2	05.5.2				
			192.1				06.5.250 8.1.103		CP CP							<u>ep-0 Ack</u> 11-4380		-0 Len	-0
			192.1				36.5.250									535 _cn=		155-14	CV
- 3	1.157	7/16	192.1	69.1.1	02		06.5.250			ulfenτ	не]]о								
			167.2				58.1.102		SL	[Unneas									
			192.1				06.5.250 58.1.102			continu			ped-to	с дек-	1461 W	1-65535	Lau-0		
			192.1				06.5.250						5eq-10	E Ack-	2734 W	1 -64262	Len-0		
			192.1				06.5.250 58.1.102									et, Endry Ke Messer		Handsh	iake
	(p.a.c	DI T		11.500.7	27.2														_
			5 1.0	(CX03)1)														_
L	Lergtr	: 13-	4				nge												
L B H 3 TL:	Length Handsh Si Reco	: 13- ak = 1 ord _	e Protoco ayen: (l: 71 Thange	iert ke Ciphe	y Excha 1 Specifi	Protoco	: Chang	≣ ⊂iph	≡r Spe:									
ا ۲۱ 🖬 ۲۱:۲۲ ا	Length Handsh Si Reco Curller	: 13- ak= ord _ u Typ	e entori ayan: (pe: Cha	nt: Cl Thange unce C	ient ke Cipher ipher S	y Excha	Protoco	: Chang	≡ ⊂iph	er Spei									
L E H TL: () V	Lengtin Haindsin Si Reido Conitien Vensfic	: 13- ak = ord _ u Typ n: u	e Protoco ayen: (nt: Cl Thange unce C	ient ke Cipher ipher S	y Excha 1 Specifi	Protoco	: Chang	≡ ⊂iph	u≘r Spe:	1								
ן ים דב: י נ נ	Lengtin Hainds f Si Rieco Conitien Vensfic Lengtin	: 13- ak= ord _ t Typ n: 11 ; 1	e Protocn ayan: (pe: Cha La 1.0	nt: 51 Change unde C (6x03	ient ke Ciphe ipher S 01)	y Excha 1 Specifi	Protoco	: Chang	≣ Ciph	≡r Spe:									
ן ד⊑: 0 ג נ ג ג ג ג ג ג ג ג ג ג ג ג ג ג ג ג ג	Length Hands T S Reco Curlen Vensfo Length Change	: 13- ak= ord _ t Typ n: tr : 1 : 1	2 ayan: (92: Iha 15 1.0 hen Spa	nt: Cl Change Inde C (CX03 ec Mes	iett ke Ciphe ipren S 21) sage	y Excha Stec F pec (20	Protoco	-	·										
ן ₪ דב: נ נ נ נ נ נ נ נ נ נ נ נ נ נ נ נ נ נ נ	Length Hands T S Reco Curler Vensic Longth Change S Reco Conter	: 13 ak= t Typ n: tt : 1 Cipl t Typ	ayer: (by: Ind to: Ind to: Ind to: Ind her Spa ayer: I be: Har	nt: cl change unde C (CX03 c Mes landsh adshak	ient ke Ciphe iphen S 01) Sage ake Pri ake Pri 2 (22)	y Excha Stec F pec (20	9755050"))	-	·										
ן דב: נ נ נ נ נ נ נ נ נ נ נ נ נ נ נ נ נ נ נ	Length Hards T S Reco Curler Vensic Length Change S Reco Conter Vensic	: 13 ak= 1 ord _ t Typ : 1 Cipl ord t Typ n: T	ayer: (be: Ind be: Ind be: Spa her Spa ayer: I	nt: cl change unde C (CX03 c Mes landsh adshak	ient ke Ciphe iphen S 01) Sage ake Pri ake Pri 2 (22)	y Excha Stec F pec (20	9755050"))	-	·										
L TL: (L (TL: () () () () () () () () () (Length Hands S Reco Longth Change S Reco Conten Verisi L Length	: 13. ak = 1 t Typ t Typ n: 1 : 1 Cipl t Typ n: Th : 32	e ayar: (be: Dha la 1.0 her Spa ayer: H be: Har la 1.0	il: fl hange mue C (CX03 ec Mes landsh adshak (CX03	iert ke Ciphe ipren S D1) Sage ake Prr ≥ (22) D1)	y Excha Stec F pe⊂ (20 toco :	Franypt	ed Hand	shake	Message	·E.								
	Length Hands T S Reco Longth Change S Reco Conten Versi L Length Do de	: 13 ak= ord _ t Typ r: 1 : 1 : Ciplord t Typ :: 32 : 32 : 32	2 offor ayar: 0 be: 10 ber Spa ayer: 1 be: Han be: Han be: 10 t 40 00	il: Cl Change Ince C (CXU3 ec Mes Iandsh Idshak (CX03 80 0	iert ve Ciphe ipren S D1) sage ake Pri e (22) D1)	y Extha Step F pec (20 then : 6 c0 aft	Fromypt	ed Hand	shake	Message									
	Length Hands T S Reco Longth Change S Reco Conten Versi L Length Do de	: 13 ak= ord _ t Typ r: 1 : 1 : Ciplord t Typ :: 32 : 32 : 32	2 offor ayar: 0 be: 10 ber Spa ayer: 1 be: Han be: Han be: 10 t 40 00	il: Cl Change Ince C (CXU3 ec Mes Iandsh Idshak (CX03 80 0	iert ve Ciphe ipren S D1) sage ake Pri e (22) D1)	y Extha Step F pec (20 then : 6 c0 aft	Fromypt	ed Hand	shake	Vessage :8	<u>P.</u>								
	Length Hands S Reco Conten Vensi D Longth Change S Reco Conten Vensi D Length Di de Di fa S S 24	: 13 ak = t Typ n: 11 : 1 Cipl n: 11 : 2 t Typ n: Ti : 32 50 C c b4 dk 60 C c	2 ayer: 0 be: 1.0 her Spa ayer: 1 be: Han 15 1.0 1 40 00 5 00 00	t: ::: hange ince C (GX03 ic Mes ic Mes	ipt (Ciphe ipter 5 51) 5age ake Pr ≥ (22) 01) 5 3e 2 0 74 4 5 01 0	y Excha Step F per (20 then : 6 c0 a8 9 f7 9e 0 86 10 9 99 94	Forrypt 00 00 01 66 a3 ba 00 00 00 27	ed Hand a7 ce 30 18 32 00 85 11	shake P.&	Message 	 								
	Length Hands S Reco Conten Vensi D Longth Change S Reco Conten Vensi D Length Di de Di fa S S 24	: 13 ak = t Typ n: 11 : 1 Cipl n: 11 : 2 t Typ n: Ti : 32 50 C c b4 dk 60 C c	2 ayer: 0 be: 1.0 her Spa ayer: 1 be: Han 15 1.0 1 40 00 5 00 00	t: ::: hange ince C (GX03 ic Mes ic Mes	ipt (Ciphe ipter 5 51) 5age ake Pr ≥ (22) 01) 5 3e 2 0 74 4 5 01 0	y Fwitha Siet F ppeu (20 thorn : 6 c0 aB 9 f2 0 0 86 10 9 99 d2 0 24 d	Foorypt	ed Hand 	5hake P.&	Message :8. :8. tI. &'. 91 IJI									
	Length Hands S S Reco Curlen Vensfic Length Change S Reco Conten Venstic Length Length Length Do de Dis fo So 24 dd Se So 24	: 13 ak = t Typ n: t : 1 Cipl nd t Typ n: Ti : 32 50 f 00 c b 50 f 00 c b 50 f 00 c b 50 f 10 d 51 d 51 d 51 d 51 d 51 d 51 d 51 d 51	2 2: nthref ayEr: (uE: Ele 	1: 1: change mice C (GX03 c Mes landsh dshac (CX03 R0 0 R0 0 R0 0 C 27 - 27 - 27 - 27 - 27 - 27 - 27 - 27 - 27 - 21 - 24 -	iert (Ciphe ipren (21) sage ake Pro- e (22) 21) 5 7 7 5 7 4 5 9 5 5 9	y Extha Step F pper (20 thron : 6 c0 a8 9 fd 4e 9 99 d2 9 7d 4e 4 02 40 1 94 3e	Fromypt 60 00 01 66 03 ba 00 00 00 27 dd c2 4a 82 08 4/	ed Hand 	shake P.& 	Message 									
	Length Hands S Reco Duriter Length Change S Reco Conter Length Conter Length Durits S Reco Conter Length Durits S Reco Conter Length Durits S Reco Conter Length S Reco S S Reco S S Reco S S Reco S S Reco S S S S S S S S S S S S S S S S S S S	: 13 ak = t Typ in: 1 : 1 Ciplord t Typ n: Typ n: Typ n: 32 50 C co b4 do b4 do b4 do 24 C do 25 C do 26 C do 27 C do 27 C do 27 C do 28 C do 29 C do 29 C do 20 C do 29 C do 20	4 2: dfnor aya::: (ye:: lha 	1: 51 hange mice C (6x03 kc Mes landshak (0x03 kc Mes landshak (0x	$r = 1 + c_{f}$ $r = 1 + c_{f}$ r =	y Firth Ster F pul (20 thron : 0 80 10 0 86 10 9 99 d2 9 7d 40 4 02 40 1 91 32 9 37 40	Franypt 60 00 01 66 03 ba 00 00 00 00 04 27 04 82 04 82 04 82 04 82 04 82 04 82 04 82 04 82 05 84 04 82 05 84 05 85 05 85	ed Hand a7 re 30 18 32 00 85 11 54 48 37 12 70 5 18 20	shake P.6 P.6 	Message 									
	Length Hands S Reco Duriter Length Change S Reco Conter Length Conter Length Durits S Reco Conter Length Durits S Reco Conter Length Durits S Reco Conter Length S Reco S S Reco S S Reco S S Reco S S Reco S S S S S S S S S S S S S S S S S S S	: 13 ak = t Typ in: 1 : 1 Ciplord t Typ n: Typ n: Typ n: 32 50 C co b4 do b4 do b4 do 24 C do 25 C do 26 C do 27 C do 27 C do 27 C do 28 C do 29 C do 29 C do 20 C do 29 C do 20	4 2: dfnor aya::: (ye:: lha 	1: 51 change (6x03 c Mes c	iP - t <pre>ciphe = :::::::::::::::::::::::::::::::::::</pre>	y Fxtha Stet F ppt (20 toto : 6 c0 a0 9 f2 6 0 86 10 9 99 d2 9 70 4e 4 02 40 1 94 3e 9 73 4e 4 02 40 1 94 3e 7 76 d 45 51	Encrypt 00 00 01 66 03 ba 00 00 d0 27 d0 27 d0 27 d4 82 08 47 df 7d 2e 14	ed Hand 37 ce 30 18 32 00 34 11 57 12 78 70 12 38	shake P.& 	Message 									
	Length Hands - Sincer Soncer Length Change Soncer Verstr Length Verstr Length Soncer S	: 13 ak = ord _ t Typ : 1 cipl t Typ rrd t Typ : 32 cipl t Typ : 32 cipl t Cipl t Typ : 32 cipl t Cipl t Cipl Cipl t Cipl t Cipl t Cipl Cipl Cipl Cipl Cipl	2 ntorn ayer: 1 ove: 11 	1:	$\begin{array}{c} c_{1} c_{1} c_{2} \\ c_{1} c_{2} \\ c_{2} \\ c_{3} \\ c_{2} \\ c_{3} \\ c_{2} \\ c_{3} \\ c_{3}$	y Firth Ster F pper (20 then : 0 80 10 0 86 10 0 86 10 0 86 10 9 99 42 9 97 40 0 45 51 7 74 40	Encrypt Encrypt 00 00 01 66 a3 ba 00 00 00 27 dd c2 4a 82 dd c2 4a 82 df 7d 2e 14 c0 73 45 ef	ed Hand 47 ce 50 18 82 00 85 11 54 48 37 12 70 75 78 20 12 3 78 20 12 3 78 3	shake P.& P.& 	Message 	н., d I 4., d I 4., с I 4., с I 4., с., с.,								
	Length Hands S Reco Longth Longth Change S Fren Length Length Length Length Length Length S 64 Hang S 74 Hang S 14 Hang S 14 Hang S 72 Hang S 72 H	: 13 ak = ord _ U Typy : 1 : Cipl ind : Cipl ind : 2 : 32 : 32 : 32 : 32 : 32 : 1 : 32 : 33 : 34 : 35	4 2: ntood aye::: (ye:: Iha 5: I.0 hen Spa ayen:: I 5: I.0 5: Constant 5:	1:	$r = 1 + c_{f}$ $r = 1 + c_{f}$ r =	y Firtha Ster F ppel (20 toro : 0 80 24 0 77 4 0 86 0 9 99 dz 9 97 dz 9 70 4 9 70 4 9 72 4 0 24 0 1 91 26 1 91 26 d 45 51 7 74 40 d 45 51 7 74 40 d 7 71 40 0 70 70	Fromypt 00 00 01 66 01 66 00 00 00 00 00 27 dd c2 dd c3 dd c3	ed Hand a7 re b0 18 a7 re b1 18 a7 re b2 00 18 a7 re b1 18 a7 re b2 00 18 a7 re b1 18 a7 re b2 00 18 a7 re b3 18 a7 re b3 18 a8 re b3	shake P.& D. 	Message 									
	Length Hands - Si Reco Curled the Length Change Si Reco Contein Length Contein Le	: 13. ak= t Type t Type rd t Type t Type bd 2 50 f t Type bd 2 50 f t 2 50 f t 5 50 f t 5 50 f t 5 50 f 5 50 f 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	2 2: nthord ayer: (ue: Ind 	1:	iP - t vi Ciphe ipren S 21) 5age ake Pr (22) 01) 6 76 7 2 (22) 01) 6 76 7 4 01 0 1 05 0 1 05 0 4 07 0	y Firtha Ster F ppel (20 toro : 0 80 24 0 77 4 0 86 0 9 99 dz 9 97 dz 9 70 4 9 70 4 9 72 4 0 24 0 1 91 26 1 91 26 d 45 51 7 74 40 d 45 51 7 74 40 d 7 71 40 0 70 70	Fromypt 60 00 01 66 03 ba 00 00 d0 27 dd C2 08 4/ dF 7/ 20 73 42 67 44 82 08 4/ dF 7/ 20 73 45 67 44 82 05 73 15 67 14 73 15 67 16 6 17 75 17 75 1	ed Hand a7 re b0 18 a7 re b1 18 a7 re b2 00 18 a7 re b1 18 a7 re b2 00 18 a7 re b1 18 a7 re b2 00 18 a7 re b3 18 a7 re b3 18 a8 re b3	shake P.& P.& 	Message 	н. с. н. н. с.								
	Length Hands - Si Reco Curled the Length Change Si Reco Contein Length Contein Le	: 13. ak= t Type t Type rd t Type t Type bd 2 50 f t Type bd 2 50 f t 2 50 f t 5 50 f t 5 50 f t 5 50 f 5 50 f 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	4 2: ntood aye::: (ye:: Iha 5: I.0 hen Spa ayen:: I 5: I.0 5: Constant 5:	1:	iP - t vi Ciphe ipren S 21) 5age ake Pr (22) 01) 6 76 7 2 (22) 01) 6 76 7 4 01 0 1 05 0 1 05 0 4 07 0	y Fxtha Stet F ppel (20 toco : 6 c0 a8 9 f2 6 0 86 L0 9 99 d2 9 7d 4e 4 02 40 1 94 3e 7 74 cc e 71 40 1 04 20 1 04 75 7 4 cc e 71 40 1 60 20 t 80 36	Fromypt 60 00 01 66 03 ba 00 00 d0 27 dd C2 08 4/ dF 7/ 20 73 42 67 44 82 08 4/ dF 7/ 20 73 45 67 44 82 05 73 15 67 14 73 15 67 16 6 17 75 17 75 1	ed Hand a7 re b0 18 a7 re b0 18 a7 re b12 a8 f 11 b4 48 37 12 a8 f 11 b4 48 37 12 a8 51 13 31 33 32 ea	shake P.& P.& 	Message 	н. с. н. н. с.								



TLS: Handshake Wrapup

At this point, the Handshake Protocol is finished. Both the server and the client know the following:

- 1. What key and encryption method to use for message encryption
- 2. What key and hashing method to use for message signing

There is, then, a great deal going on behind the scenes, which explains why SSL connections are sometimes slower than insecure ones.



TLS: Record Protocol

Now the Record Protocol starts to manage all future communication. The server finally is ready to respond to the original request, as follows:

- 1. It encrypts its http response.
- 2. It calculates a hash of its response
- 3. It appends that hash as a signature.



TLS: Record Protocol (cont'd)

Upon receiving the serverâ€[™]s response, the client does the following:

- 1. It detaches the signature.
- 2. It calculates a new hash of the response, and compares that to the detached signature.
- 3. (Assuming they match,) it decrypts the response.
- 4. It displays the requested html.



Apache's mod_ssl

Installed by default in Apache 2, and available for Apache 1.3, *mod_ssl* provides cryptography so that Apache can interact with the OpenSSL toolkit.

http://www.modssl.org/_



OpenSSL

The OpenSSL project provides a toolkit and cryptography library for implementing the TLS protocol.

http://www.openssl.org/



PHP's OpenSSL Support

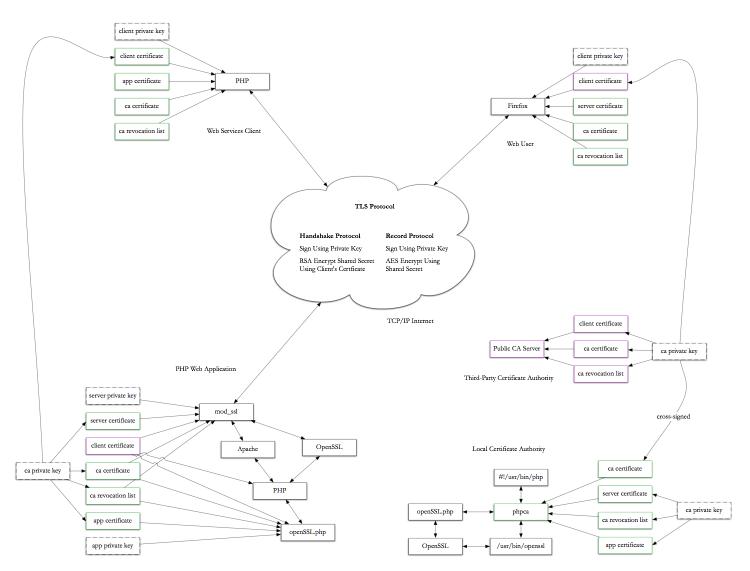
PHP reports that it must be compiled *--with-openssl* in order to use its wrapper support for OpenSSL, although that appears not to be completely true.

http://www.php.net/openssl



The Big Picture

Green parts are created by local CA, pink parts by third-party CA.





Part II: SSL-enabled Webservers

HTTPS Requests and Responses are:

- Encrypted
- Tamper-proof
- Authenticated (Server, anyway)



HTTPS Requirements

- Apache with mod_ssl
- An IP Address
- Private server key (passphrase encrypted)
- Signed Server Certificate
- (optional) Certificate Authority Certificate(s)
- (optional) PassphraseDialog script



Using PHP to simplify PKI

phpca is a command line utility to create and manage a simple Certificate Authority for use with Apache's mod_ssl.

```
./phpca <command> [<server> | "ca"]
```



A Local Certificate Authority

./phpca cagen



A New Server Certificate

./phpca newserver ssl.example.org



Global SSL Directives

##
Global SSL Directives
##
#LoadModule ssl_module modules/mod_ssl.so
Listen 443
Random number generation
SSLRandomSeed startup file:/dev/urandom 512
SSLRandomSeed connect file:/dev/urandom 512
Session Cache
SSLSessionCache none
SSLSessionCacheTimeout 600
SSLPassphraseDialog builtin
SSLMutex
file:/Applications/xampp/xamppfiles/logs/ssl_mutex
AddType application/x-x509-ca-cert .crt

Addrype application/x-x509-ca-cert .crt AddType application/x-pkcs7-crl .crl



A Passphrase Dialog

Create /root/httpdkey:

#!/bin/sh
echo 'my secret password'

Make sure only root has access:

chmod 700 /root/httpdkey

Use an external SSLPassphraseDialog:

SSLPassphraseDialog exec:/root/httpdkey

<u>Manual</u>



Apache Per-host SSL Directives

SSL Virtual Host Context ## <VirtualHost _default_:443> # General setup for the virtual host DocumentRoot "/Users/csnyder/Sites/https" ServerName localhost ServerAdmin csnyder@chxo.com ErrorLog logs/sslerror.log # SSL Configuration SSLEngine on SSLCipherSuite HIGH:MEDIUM SSLCertificateFile /etc/httpd/ssl/localhost.cert SSLCertificateKeyFile /etc/httpd/ssl/localhost.key SSLCertificateChainFile /etc/httpd/ssl/ca.cert SSLCARevocationFile /etc/httpd/ssl/ca.crl Client Authentication (Type): # #SSLVerifyClient require #SSLVerifyDepth 10 SSL Engine Options: # <Files ~ "\.(cqi|shtml|phtml|php?)\$"> SSLOptions +StdEnvVars </Files> SSL Protocol Adjustments: # SetEnvIf User-Agent ".*MSIE.*" \ nokeepalive ssl-unclean-shutdown \ downgrade-1.0 force-response-1.0 # Per-Server Logging: CustomLog logs/ssl_request_log "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"

[Presentation] Apache Per-host SSL Directives

</VirtualHost>



Cipher Suite

DIY suite-ness!

openssl ciphers -v 'HIGH:MEDIUM'

Manual



Cross Your Fingers



Revoking A Server Certificate

./phpca revoke ssl.example.org



Part III: Application Level SSL

A PHP application can use OpenSSL's RSA support to:

- Sign values to prevent tampering
- Encrypt values to keep them private



Example: Stored Secrets

On storage, application needs:

• Application Certificate (Public Key) to encrypt values

On retrieval, application needs:

- Application Private Key to decrypt values
- ...and Private Key passphrase



Class openSSL

```
include_once( './openSSL.php' );
$server = new openSSL();
$server->privateKey( file_get_contents( $server_key ) );
```

```
$server->certificate( file_get_contents( $server_cert ) );
```



Signing

\$value_signed = \$ssl->sign(\$value , \$passphrase);

Looks like:

So long, and thanks for all the fish. ----BEGIN openSSL.php SIGNATURE---e35fbZmTXYbVP33HY1CX31hxirAiENmEY4A0JHiGqPDfS87BmDQszGHF

CSvnMAyyqF70uwRYnRS+VdiDNy2y3Uh2gqB7SNGXgWZnRNsMTeGX40KX

NB5uwUQ+zNu7QjYfapQyliYoOWS5L+GcmFRHveTwAgw= ----END openSSL.php SIGNATURE----



Encrypting

Short values only! (56 chars max)

\$secret = \$ssl->encrypt(\$value, \$client_certificate);

Looks like:

Nlmc97wDavLSF7R078NcluVX8SrYMXdDFu9otugP5LDIPTW++VUQ5DOs Z9qVS9+AL01gv1H2Ub8eNRcV67WgQw/51MA92+T5KprSqV+CP/FXfcNC nd3pq/H6TkP0LTF7zX9Q7GZg/4UuMHmc9EcGHhoOxBM=



Decrypting

\$value = \$ssl->decrypt(\$secret, \$passphrase);

[Presentation] Verifying

Contents | Previous | Next



Verifying

\$verified = \$ssl->verify(\$signed_value, \$client_certificate);



Checking The Key Passphrase

\$success = \$ssl->checkKey(\$passphrase);



Parsing X.509 Data

```
$ssl->certificate( $certificate_data );
$dn = $ssl->getDN();
print_r( $dn );
```

Looks like:

```
(
   [C] => US
   [ST] => New York
   [L] => New York City
   [O] => CHXO Internet
   [OU] => Certificate Authority
   [CN] => ca.chxo.com
   [emailAddress] => csnyder@chxo.com
)
```

[Presentation] Discussion

Contents | Previous | Next



Discussion

How do you use SSL?



Thank You!

For many many more details, please consult "Pro PHP Security", published in September by Apress.





Resources

Some of the many resources used in the making of this presentation.

Cryptography

- <u>Diffie-Hellman-Merkle Key Exchange</u>
- PKCS #7: Cryptographic Message Syntax Standard
- <u>PKCS #12: Personal Information Exchange Syntax</u>
 <u>Standard</u>
- <u>RSA Cryptosystem</u>
- <u>S/MIME Specification 3.1 (RFC 3851)</u>
- Legal
 - <u>CNET: Netscape Patents Crypto Protocol (Sept. 16, 1997)</u>
 - United States Patent: 4,405,829 (RSA)
 - United States Patent: 5,657,390 (SSL)

Manuals

- mod_ssl Directives
- OpenSSL Manuals
- PHP OpenSSL Functions

Other How-Tos

- <u>Certificate Management and Generation with OpenSSL</u>
- <u>Generating an SSL Certificate with Apache+mod_ssl</u>

SSL/TLS Protocol

- <u>The SSLv2 Protocol</u>
- <u>The SSLv3 Protocol</u>
- The TLS Protocol v1.0
- X.509 Public Key Infrastructure Spec (RFC 3280)



Download

Presentation files as a **ZIP archive**.

Contents:

```
psslwap/FCNYLicense.txt
psslwap/README
psslwap/cnf_template.php
psslwap/config-dist.php
psslwap/configure
psslwap/fcnyCLI.php
psslwap/gpl.txt
psslwap/openSSL.php
psslwap/openSSLDemo.php
psslwap/openssl.cnf
psslwap/phpca
psslwap/players.png
```