
Systems Applications Proxy Pwnage

ian@sensepost.com



about: us



Ian de Villiers



[SensePost – 2011]



What we're going to talk about

- Why this Talk ?
- The history of decompressing SAP DIAG
- Understanding the fundamentals
- New Attacks
- Conclusion



Why this Talk ?

- SAP systems carry business critical data
 - Root is nice, but it's all about the data... 😊
- Any numbers of attacks against SAP systems
 - This talk is not about them...
- Fundamental security shortcoming in the SAP GUI (DIAG) protocol
 - Unencrypted. By Default
 - Compressed
 - This is old news...



#include <Disclaimer.h>

- SAP is a behemoth
- Very little documentation out there
 - service.sap.com require user accounts ☹️
- Documentation for DIAG protocol requires NDA (apparently)... ☹️
- Custom toolsets require development
- SAP Basis version used is reasonably outdated..
 - Fine for protocol analysis
 - Some attack scenarios may not be applicable



#include <Disclaimer.h>

- SensePost Assessments
 - Covered a lot of ground...
 - ... but virtually impossible to do a complete job on something as complex
 - Research has been on an “as-time-allows” approach between projects
- Releasing tools and research as-is...
 - Let’s see some SAP 0-day in the next couple of months... 😊
- Lack of documentation means analysis is probably not spot-on



#include <Disclaimer.h>

- Planned to present with SAP on second laptop
- Some technical issues yesterday
 - Running SAP in a VM
 - Laptop is a dog in terms of speed at the moment



What we're going to talk about

- ~~Why this Talk ?~~
- The history of decompressing SAP DIAG
- Understanding the fundamentals
- New Attacks
- Conclusion



The History...

- Sniffing SAP GUI Passwords
 - Andreas Baus & René Ledosquet from Securon
 - Published 6th July, 2009
- Dealt with playing back captured packets to SAP GUI
- Decompressed data obtained from SAP GUI memory with debugger



But wait...
There's more...



The History...

- Dennis Yurichev
 - Published 2nd June, 2010
- Discovered that similar compression method was employed in MaxDB
 - Open Source MaxDB code available
- Wrote utility for decompressing SAP traffic
 - Required manual reassembly of data segments over multiple packets



The History...

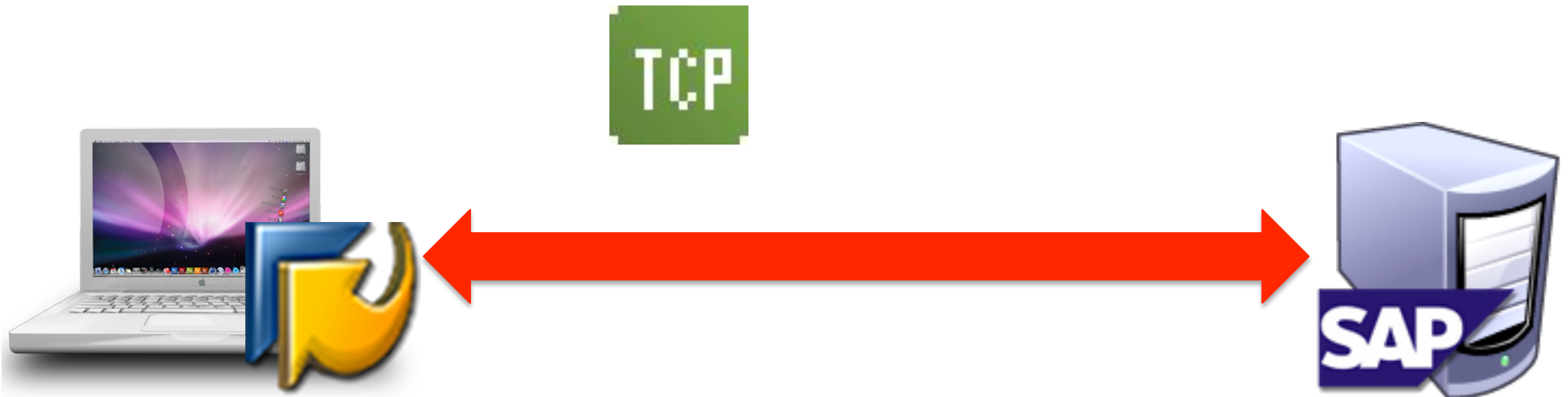
- Dennis' research required:
 - Identification of SAP compressed packets by magic
 - 0x1f @ packet.data[17]
 - 0x9d @ packet.data[18]
 - Stringing together of subsequent packets without magic at 17 and 18
 - Once complete “message” had been assembled, we could decompress the data
 - (Decompression won't work until we have the complete stream)



SAPDecompress – In Pictures



SAPDecompress – In Pictures



SAPDecompress – In Pictures

1f 9d

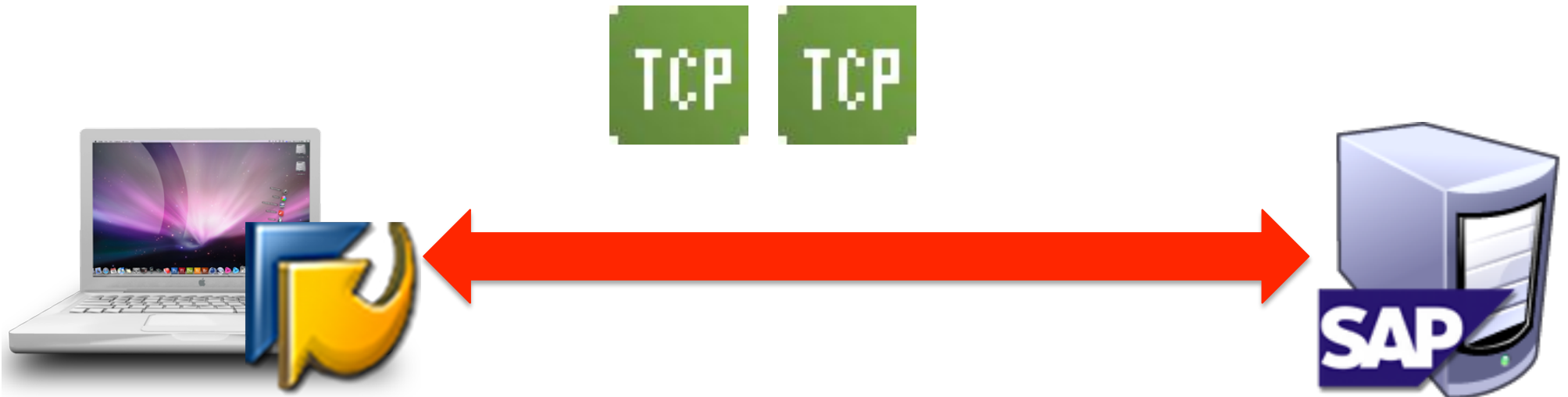
1f 9d == SAP Compressed Message Magic
At packet.data[17] and packet.data[18]

TCP

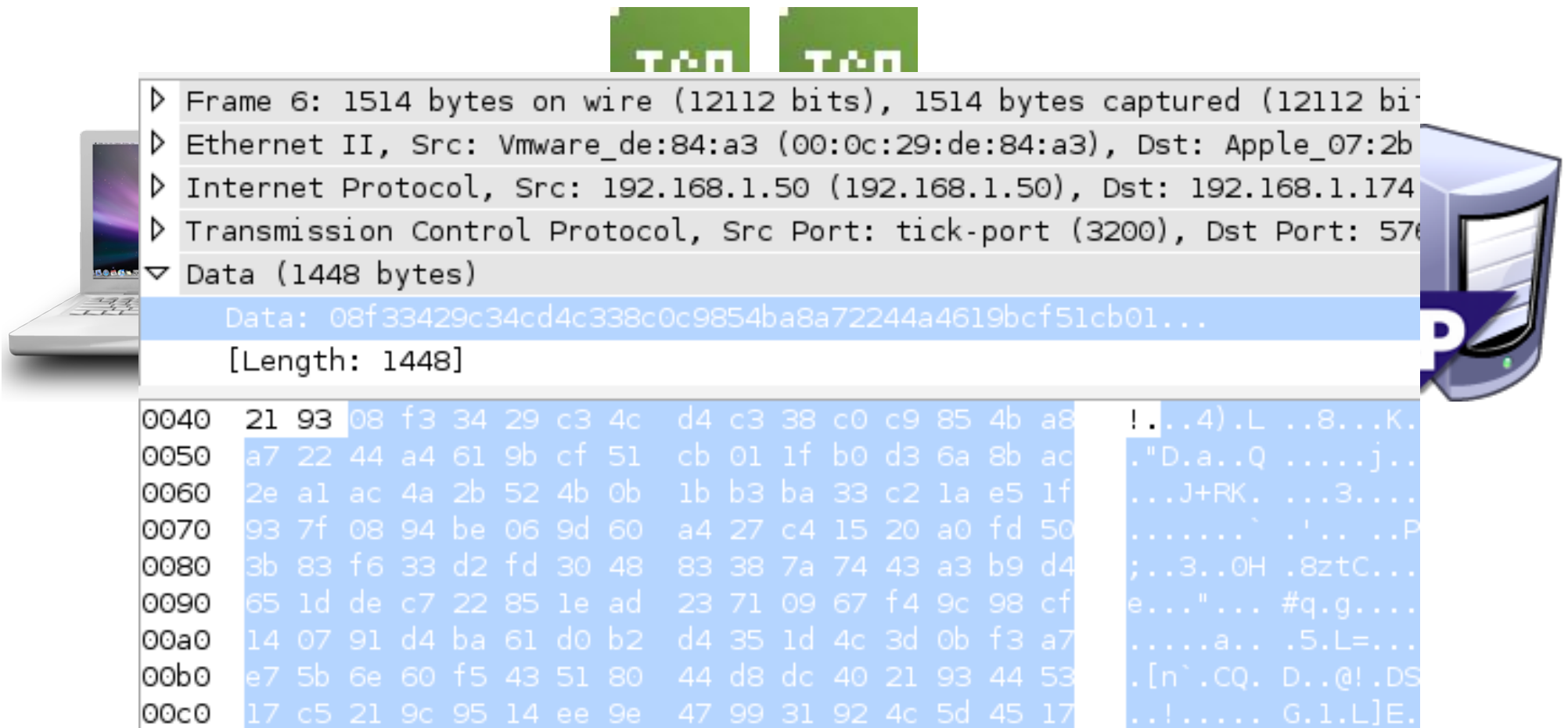
```
▶ Frame 5: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
▶ Ethernet II, Src: Vmware_de:84:a3 (00:0c:29:de:84:a3), Dst: Apple_07:2b:33:93 (08:00:27:33:93:00)
▶ Internet Protocol, Src: 192.168.1.50 (192.168.1.50), Dst: 192.168.1.174 (192.168.1.174)
▶ Transmission Control Protocol, Src Port: tick-port (3200), Dst Port: 5760
▼ Data (1448 bytes)
  Data: 0000d2a00001100000100016a240000121f9d02deacb534...
  [Length: 1448]
0040 21 93 00 00 02 a0 00 00 11 00 00 01 00 01 6a 24  !...*.. .....j$
0050 00 00 1f 9d 02 de ac b5 34 b7 71 1c e1 de 27  ..... .4.q...!
0060 41 10 a4 0e 0e 6c 47 b6 46 26 45 53 8a 49 01  A.. J.lG .F&ES.I.
0070 04 f8 90 4a e5 08 c4 43 a2 0b 7c 08 00 65 27 76  ...J...C ..|..e'v
0080 4a b5 02 86 e2 46 cb 5d 64 77 21 8a 4e 55 7c f1  J...F.] dw!.NU|.
0090 d1 b9 c6 b7 5c fc 23 52 be e6 94 5f 90 ca 25 a9  ....\.#R ..._.%
00a0 dc 73 4a 7e 40 92 9e de c7 2c c9 d8 2c 39 56 59  .sJ~@... ,...9VY
00b0 a3 92 88 ee e9 99 f9 fa 39 3d 10 8b e6 79 60 ff  ..... 9=...y`.
00c0 f9 ec df 0b 7f f9 c3 ea 9f c3 dc 6f 2e 18 5f be  ..... ..o..._
00d0 f6 e5 3f fe 75 f3 b7 1a 9b 82 64 14 cd 19 38 87  ..?.u... ..d...8.
00e0 3f a6 94 6a b9 5c 82 dd 5e 6b 0d 79 ef 02 43 de  ?..j.\. ^k.y..C.
00f0 98 5a 2d 97 2a b0 eb da 7d 6f c0 db 76 18 3a 7c  .Z..*... }o..v.:|
0100 d7 3d b0 fc a7 7c 80 42 57 81 55 4a cb 8d e5 7a  .=...|.B W.UJ...z
0110 b3 d4 68 ac 54 5a e5 7a 79 ad be 5a 2b 95 4a f5  ..h.TZ.z y..Z+.J.
0120 a5 5b 8d e6 5a b5 56 29 9a 2a 68 5b dd 9d a2 a9  .[...Z.V) .*h[...
0130 41 ee d0 76 9f 0f 03 6b 58 34 df 00 15 a6 8a a6  A..v...k X4.....
0140 82 3f 70 9f 7c f4 e3 0a 4c 2b a5 5f 7c f2 f7 bf  .?p.|... L+_|...
0150 f6 ff f9 c7 2f 3e 85 c2 f5 bf 7d fe 95 52 34 af  ..../>.. ..}..R4.
0160 41 be d7 a9 35 9a dd fb db 1f a2 d4 05 c8 29 a5  A...S... .....
```



SAPDecompress – In Pictures



SAPDecompress – In Pictures



▶ Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

▶ Ethernet II, Src: Vmware_de:84:a3 (00:0c:29:de:84:a3), Dst: Apple_07:2b:3c:ad (08:00:27:00:2b:3c)

▶ Internet Protocol, Src: 192.168.1.50 (192.168.1.50), Dst: 192.168.1.174 (192.168.1.174)

▶ Transmission Control Protocol, Src Port: tick-port (3200), Dst Port: 576 (576)

▼ Data (1448 bytes)

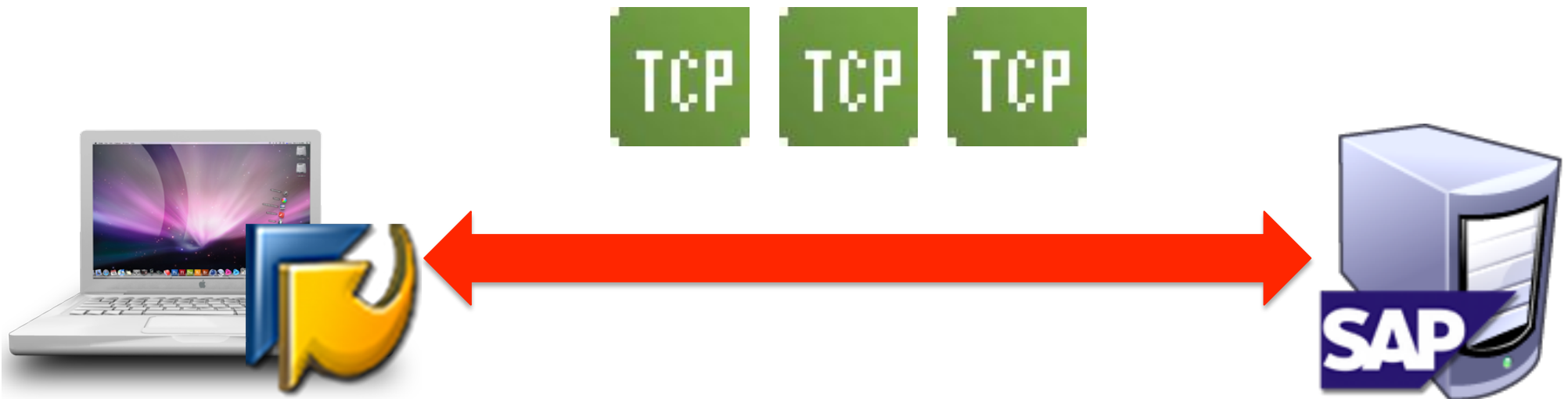
Data: 08f33429c34cd4c338c0c9854ba8a72244a4619bcf51cb01...

[Length: 1448]

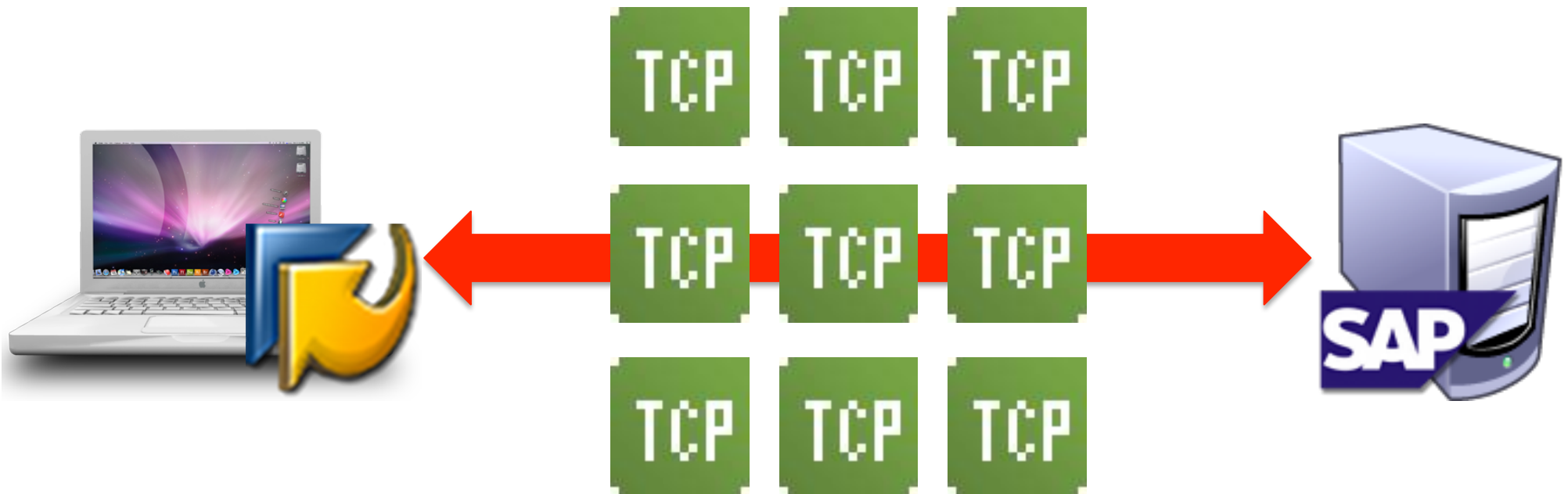
0040	21 93	08 f3 34 29 c3 4c d4 c3 38 c0 c9 85 4b a8	!...4).L ..8...K.
0050	a7 22 44 a4 61 9b cf 51 cb 01 1f b0 d3 6a 8b ac	."D.a..Qj..	
0060	2e a1 ac 4a 2b 52 4b 0b 1b b3 ba 33 c2 1a e5 1f	...J+RK. ...3....	
0070	93 7f 08 94 be 06 9d 60 a4 27 c4 15 20 a0 fd 50` .'... ..P	
0080	3b 83 f6 33 d2 fd 30 48 83 38 7a 74 43 a3 b9 d4	;..3..0H .8ztC...	
0090	65 1d de c7 22 85 1e ad 23 71 09 67 f4 9c 98 cf	e..."... #q.g....	
00a0	14 07 91 d4 ba 61 d0 b2 d4 35 1d 4c 3d 0b f3 a7a.. .5.L=...	
00b0	e7 5b 6e 60 f5 43 51 80 44 d8 dc 40 21 93 44 53	.[n`.CQ. D..@!.DS	
00c0	17 c5 21 9c 95 14 ee 9e 47 99 31 92 4c 5d 45 17	..!..... G.1.L]E.	



SAPDecompress – In Pictures



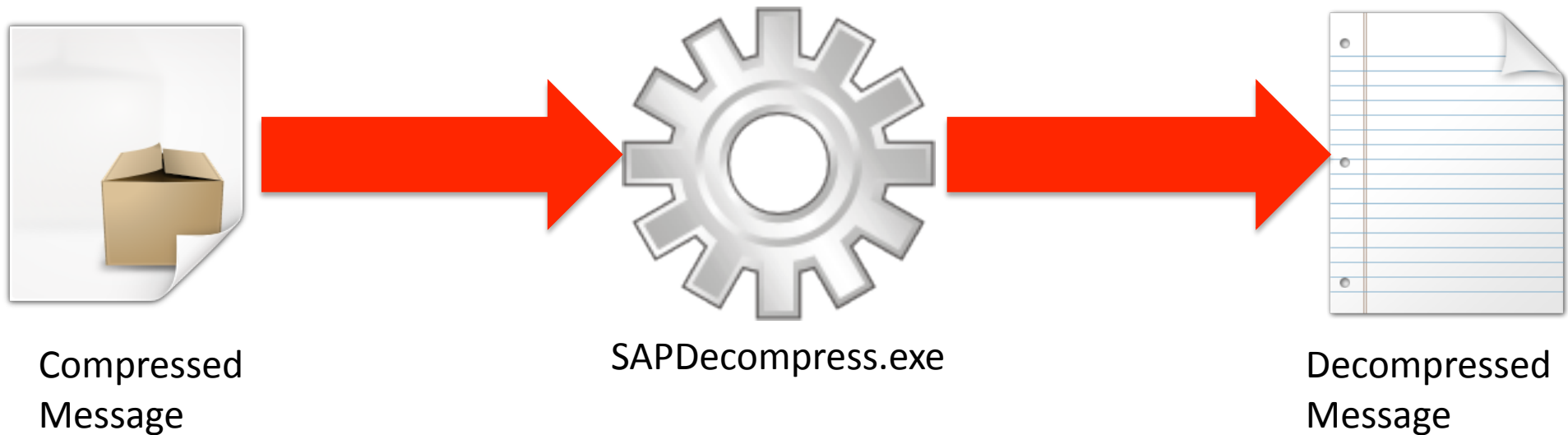
SAPDecompress – In Pictures



SAPDecompress – In Pictures



SAPDecompress – In Pictures



SAPDecompress – In Pictures

																Length: 316 Bytes	
.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f		
00.: 00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8	
01.: 12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	RÅø½\$ Eqü\ ž	
02.: d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖË# f\$ñ·· Ūi 4pË	
03.: 30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ	
04.: db	53	7f	47	e7	ae	2d	f2	c2	e5	0b	9f	f3	3d	e7	fb	ŪS Gç@-ðÄÄ Ÿó=çŪ	
05.: 65	ac	0a	07	0f	8b	17	40	08	8f	d9	b5	94	36	4c	fd	e˘ < @ Ūμ"6Lý	
06.: bb	36	a0	56	81	7c	cb	b1	51	3b	85	1c	cd	aa	0c	10	»6 V Ë±Q;... Íª	
07.: a0	04	fa	bf	5d	d4	34	28	83	49	14	a1	84	da	09	19	úž]O4(fI i„ Ū	
08.: cf	50	6b	90	d4	b1	c0	a0	01	05	80	9c	59	73	71	2e	ïPk Ö±Ä αYsq.	
09.: 11	6a	7f	5b	46	59	9d	ca	7f	d3	b9	38	53	34	8a	70	j [FY Ê Ó¹8S4Šp	
0a.: 4e	c3	cc	25	01	18												
0b.: ce	e8	be	99	40	65												
0c.: a3	ed	c6	15	f2	ca												
0d.: fe	39	be	14	bd	ae												
0e.: a4	ab	73	de	e9	3f												
0f.: 42	04	87	d3	51	c2												
10.: 7f	4a	06	eb	f0	75												
11.: d6	cc	71	45	8b	44												
12.: c7	26	43	40	06	65												
13.: 4d	2a	59	aa	13	55												

																Length: 431 Bytes	
.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f		
00.: 01	01	0f	00	00	00	00	00	00	00	00	00	00	00	00	00	#	4110
01.: 00	10	06	23	00	0f	00	00	10	0e	01	34	31	31	30	00	UTF8	720
02.: 55	54	46	38	00	10	04	09	00	03	37	32	30	10	04	19		
03.: 00	02	00	00	10	0f	01	00	10	00	00	07	00	0a	0f	00		
04.: 00	00	00	00	00	00	00	00	00	10	04	04	00	08	00	14		
05.: 00	07	00	10	00	07	10	04	17	00	02	00	1f	10	04	16		
06.: 00	02	00	13	10	05	01	00	16	00	05	00	00	02	14	11		
07.: 3d	10	5b	31	10	00	11	00	00	00	00	00	00	00	00	10	= [1	
08.: 0c	08	00	10	00	00	03	e6	00	00	07	70	00	00	03	e6	æ p æ	
09.: 00	00	07	70	10	0c	06	00	21	00	00	00	11	00	00	00	p !	
0a.: 00	00	00	00	31	00	00	01	10	00	00	00	00	00	00	00	1	
0b.: 00	00	00	00	13	00	00	00	5b	02	10	09	0b	00	0a	01	[
0c.: 00	02	00	14	00	00	00	00	00	11	00	00	00	e0	3c	3f	à<?	
0d.: 78	6d	6c	20	76	65	72	73	69	6f	6e	3d	22	31	2e	30	xml version="1.0	
0e.: 22	20	65	6e	63	6f	64	69	6e	67	3d	22	73	61	70	2a	" encoding="sap*	
0f.: 22	3f	3e	0a	3c	44	41	54	41	4d	41	4e	41	47	45	52	"?> <DATAMANAGER	
10.: 3e	0a	20	20	3c	43	4f	50	59	20	69	64	3d	22	63	6f	> <COPY id="co	
11.: 70	79	22	3e	0a	20	20	20	20	3c	47	55	49	20	69	64	py"> <GUI id	
12.: 3d	22	67	75	69	22	3e	0a	20	20	20	20	20	20	3c	4d	= "gui"> <M	
13.: 45	54	52	49	43	53	20	69	64	3d	22	6d	65	74	72	69	ETRICS id="metri	
14.: 63	73	22	20	58	33	3d	22	31	39	32	30	22	20	58	32	cs" X3="1920" X2	
15.: 3d	22	37	22	20	58	31	3d	22	37	22	20	58	30	3d	22	= "7" X1="7" X0="	
16.: 32	38	33	22	20	59	33	3d	22	31	32	30	30	22	20	59	283" Y3="1200" Y	
17.: 32	3d	22	32	30	22	20	59	31	3d	22	31	32	22	20	59	2="20" Y1="12" Y	
18.: 30	3d	22	32	38	33	22	2f	3e	0a	20	20	20	20	3c	2f	0="283"/> </	
19.: 47	55	49	3e	0a	20	20	3c	2f	43	4f	50	59	3e	0a	3c	GUI> </COPY> <	
1a.: 2f	44	41	54	41	4d	41	4e	41	47	45	52	3e	0a	0c		/DATAMANAGER>	

Compressed
Message

The History...

- Dennis Yurichev's work is *awesome*...
- My work is based very much on his discovery...



What we're going to talk about

- ~~Why this Talk ?~~
- ~~The history of decompressing SAP DIAG~~
- Understanding the fundamentals
- New Attacks
- Conclusion



The Fundamentals

- Understand the compression
- Understand the compressed protocol
 - Simplify the sniffing and decompression
- Recompression
- Understand the application protocol
 - What makes SAP GUI tick ?
- Identify SAP attack vectors not previously considered...



The Compression Algorithm

- Variants of Lempel-Ziv
 - LZC
 - LZH
 - SAP Supports both (tried and tested)



The Compression Algorithm

- Variant of Lempel-Ziv
 - LZC
 - LZH
 - SAP Supports both (tried and tested)
 - Makes one believe that SAP and MaxDB share same compression code-base... 😊



.Compression
.Decompression



.Compression
.Decompression



The Compression Algorithm

- Variant of Lempel-Ziv
 - LZC
 - LZH
 - SAP Supports both (tried and tested)
 - Makes one believe that SAP and MaxDB share same compression code-base... 😊
- Version used per message is determined by the Compression Header...
 - This is described in a minute...



The Fundamentals

- ~~Understand the compression~~
- Understand the compressed protocol
 - Simplify the sniffing and decompression
 - Recompression
- Understand the application protocol
 - What makes SAP GUI tick ?
- Identify SAP attack vectors not previously considered...



The Core, Compressed Protocol

- Easy to parse...



The Core, Compressed Protocol

- Easy to parse...



- In the absence of documentation, I've had to make my own names...

The Core, Compressed Protocol

- Easy to parse...
- In the absence of documentation, I've had to make my own names...
 - SAP Header
 - Compression Header
 - Compressed Data



The Core, Compressed Protocol

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	08	00	00	11	00	00	01	00	01	af	01	00	00	0
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Rãø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n·· Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ
04.	db	53	7f	47	e7	ae	2d	f2	c2	e5	0b	9f	f3	3d	e7	fb	ÛS Gç@-ðÃÃ Ÿó=çû
05.	65	ac	0a	07	0f	8b	17	40	08	8f	d9	b5	94	36	4c	fd	e˘ < @ Ûµ"6Lý
06.	bb	36	a0	56	81	7c	cb	b1	51	3b	85	1c	cd	aa	0c	10	»6 V Ë±Q;... Íª
07.	a0	04	fa	bf	5d	d4	34	28	83	49	14	a1	84	da	09	19	ú¿}04(/I i„Ú
08.	cf	50	6b	90	d4	b1	c0	a0	01	05	80	9c	59	73	71	2e	ÏPk Ö±À αYsq.
09.	11	6a	7f	5b	46	59	9d	ca	7f	d3	b9	38	53	34	8a	70	j [FY Ê Ó¹8S4\$P
0a.	4e	c3	cc	25	01	18	66	1b	f4	ea	f4	e7	39	ac	1c	81	NÃI% f ôêôç9˘
0b.	ce	e8	be	99	40	65	fe	ea	f4	3e	d6	2f	fc	3d	dc	ed	Îè%™@epêô>Ö/ú=Üí
0c.	a3	ed	c6	15	f2	ca	16	3c	dc	2c	b6	cb	68	b3	72	c5	£íÆ òË <Ü,†Ëh³rÃ
0d.	fe	39	be	14	bd	ae	de	b9	f5	7c	6f	ec	dd	7b	c3	c1	p9% ½@P¹õ oiÝ{ÃÃ
0e.	a4	ab	73	de	e9	3f	3c	06	3c	5a	ba	62	b1	8d	3f	85	¤«sPé?< <Zºbt ?..
0f.	42	04	87	d3	51	c2	56	6f	51	8a	08	8e	07	fe	64	d4	B ‡ÓQÃVoQ\$ pdÖ
10.	7f	4a	06	eb	f0	75	17	2d	f6	82	cf	9a	14	75	e3	50	J ëðu -ö, Ì§ uãP
11.	d6	cc	71	45	8b	44	fe	8a	ed	0a	a7	dd	14	3c	50	06	ÖÏqE< Dp\$í \$Ý <P
12.	c7	26	43	40	06	65	0c	a4	22	a4	a9	c5	4a	43	2d	4a	Ç&C@ e ¨"¤@ÃJC-J
13.	4d	2a	59	aa	13	55	b5	0e	ba	1a	3f	00					M*Yª Uµ º ?

SAP Header



The Core, Compressed Protocol

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	88	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	17	1f	9d	07	57	a5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Rãø½\$ Eqü\ ¿
	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	88	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Rãø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# f\$ñ·· Úí 4pÈ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ~° YB‡ R‡VÖ
04.	db	53	7f	47	e7	ae	2d	f2	c2	e5	0b	9f	f3	3d	e7	fb	ÛS Gç@-òÃÃ Yó=çû
05.	65	ac	0a	07	0f	8b	17	40	08	8f	d9	b5	94	36	4c	fd	e~ < @ Ûµ"6Lý
06.	bb	36	a0	56	81	7c	cb	b1	51	3b	85	1c	cd	aa	0c	10	»6 V Ë±Q;... íª
07.	a0	04	fa	bf	5d	d4	34	28	83	49	14	a1	84	da	09	19	ú¿}04(fI i„Ú
08.	cf	50	6b	90	d4	b1	c0	a0	01	05	80	9c	59	73	71	2e	ïPk Ô±Ã αYsq.
09.	11	6a	7f	5b	46	59	9d	ca	7f	d3	b9	38	53	34	8a	70	j [FY Ê Ó¹8S4Şp
0a.	4e	c3	cc	25	01	18	66	1b	f4	ea	f4	e7	39	ac	1c	81	NÃÏ% f ðèðç9~
0b.	ce	e8	be	99	40	65	fe	ea	f4	3e	d6	2f	fc	3d	dc	ed	îè¾™@epêð>Ö/ü=Üí
0c.	a3	ed	c6	15	f2	ca	16	3c	dc	2c	b6	cb	68	b3	72	c5	£íÈ òÈ <Ü,†Èh³rÃ
0d.	fe	39	be	14	bd	ae	de	b9	f5	7c	6f	ec	dd	7b	c3	c1	p9¾ ¾@P¹õ olÝ(ÃÃ
0e.	a4	ab	73	de	e9	3f	3c	06	3c	5a	ba	62	b1	8d	3f	85	ª«sPé?< <Zøbt ?..
0f.	42	04	87	d3	51	c2	56	6f	51	8a	08	8e	07	fe	64	d4	B ‡ÓQÃvoQŞ pdÖ
10.	7f	4a	06	eb	f0	75	17	2d	f6	82	cf	9a	14	75	e3	50	J èðu -ö, Ì§ uãP
11.	d6	cc	71	45	8b	44	fe	8a	ed	0a	a7	dd	14	3c	50	06	ÖÏqE< DpŞí \$Ý <P
12.	c7	26	43	40	06	65	0c	a4	22	a4	a9	c5	4a	43	2d	4a	Ç&C@ e ª"ª@ÃJC-J
13.	4d	2a	59	aa	13	55	b5	0e	ba	1a	3f	00					M*Yª Uµ ø ?

SAP Header

Compression Header



The Core, Compressed Protocol

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	17	1f	9d	07	57	a5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n·· Úí 4pÈ
	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n·· Úí 4pÈ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ° YB‡ R‡VÖ
04.	db	53	7f	47	e7	ae	2d	f2	c2	e5	0b	9f	f3	3d	e7	fb	ÛS Gç@-ðÄÄ Yó=çú
05.	65	ac	0a	07	0f	8b	17	40	08	8f	d9	b5	94	36	4c	fd	e¬ < @ Ûµ"6Lý
06.	bb	36	a0	56	81	7c	cb	b1	51	3b	85	1c	cd	aa	0c	10	»6 V Ë±Q;... í»
07.	a0	04	fa	bf	5d	d4	34	28	83	49	14	a1	84	da	09	19	ú¿]04(fI i„Ú
08.	cf	50	6b	90	d4	b1	c0	a0	01	05	80	9c	59	73	71	2e	ïPk Ö±À æYsq.
09.	11	6a	7f	5b	46	59	9d	ca	7f	d3	b9	38	53	34	8a	70	j [FY Ê Ó¹8S4\$P
0a.	4e	c3	cc	25	01	18	66	1b	f4	ea	f4	e7	39	ac	1c	81	NÄI% f ðèðç9¬
0b.	ce	e8	be	99	40	65	fe	ea	f4	3e	d6	2f	fc	3d	dc	ed	Ïè¾™@epèð>Ö/ü=Üí
0c.	a3	ed	c6	15	f2	ca	16	3c	dc	2c	b6	cb	68	b3	72	c5	£íE ðÈ <Ü,†Èh³rÄ
0d.	fe	39	be	14	bd	ae	de	b9	f5	7c	6f	ec	dd	7b	c3	c1	p9¾ ¾@D¹Ö olÝ{ÄÄ
0e.	a4	ab	73	de	e9	3f	3c	06	3c	5a	ba	62	b1	8d	3f	85	„«spé?< <Zºbt ?..
0f.	42	04	87	d3	51	c2	56	6f	51	8a	08	8e	07	fe	64	d4	B ‡ÓQÄvoQ\$ pdÖ
10.	7f	4a	06	eb	f0	75	17	2d	f6	82	cf	9a	14	75	e3	50	J èðu -ö, Ìš uāP
11.	d6	cc	71	45	8b	44	fe	8a	ed	0a	a7	dd	14	3c	50	06	ÖÏqE< Dp\$í \$Ý <P
12.	c7	26	43	40	06	65	0c	a4	22	a4	a9	c5	4a	43	2d	4a	Ç&C@ e „““@ÄJC-J
13.	4d	2a	59	aa	13	55	b5	0e	ba	1a	3f	00					M*Y» Uµ » ?

SAP Header

Compression Header

Compressed Data



The SAP Header

- Bytes [0] – [11]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ



The SAP Header

- Bytes [0] – [11]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

– Bytes [0] – Bytes [3]

- $\text{Len(Shheader)} + \text{Len(Chheader)} + \text{Len(Cdata)} - 4$

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ



The SAP Header

- Bytes [0] – [11]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

– Bytes [0] – Bytes [3]

- $\text{Len(Shheader)} + \text{Len(Chheader)} + \text{Len(Cdata)} - 4$

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

0x0000138 == 312

316 bytes – 4 bytes == 312 bytes



The SAP Header

- Bytes [0] – [11]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

– Bytes [0] – Bytes [3]

- $\text{Len(Shheader)} + \text{Len(Chheader)} + \text{Len(Cdata)} - 4$

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

316 bytes – 4 bytes == 312 bytes

0x0000138 == 312

– Bytes [4] – Bytes [11]

- Unknown (Tampering makes *no* difference)

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ



The Compression Header

- Bytes [12] – [19]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	uo	cø	z3	ve	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 7° ŸB‡ R‡VÖ



The Compression Header

- Bytes [12] – [19]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

– Bytes [12] – Bytes [15]

- Length of decompressed stream
- Little-Endian

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ



The Compression Header

- Bytes [12] – [19]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úî 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

– Bytes [12] – Bytes [15]

- Length of decompressed stream
- Little-Endian

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úî 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

0x00001af == 431



The Compression Header

- Bytes [12] – [19]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úî 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

– Bytes [12] – Bytes [15]

- Length of decompressed stream
- Little-Endian

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úî 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

0x00001af == 431

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 431 Bytes
00.:	01	01	0f	00	00	00	00	00	00	00	00	00	00	00	00	00	



The Compression Header

- Bytes [12] – [19]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

– Bytes [16]

- Version of compression (LZH / LZO)
- LZC == byte & 0x0f = 0x00
- LZH == byte & 0x0f = 0x02

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ



The Compression Header

- Bytes [12] – [19]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.	uo	c8	23	ve	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# f\$ñ•• Úí 4pÊ
03.	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

– Bytes [16]

- Version of compression (LZH / LZC)
- LZC == byte & 0x0f = 0x00
- MZH == byte & 0x0f = 0x02

```
#define CS_LZC          0x0    /* use lzc .....*/
#define CS_LZH          0x2    /* use lzh .....*/
int CsObjectInt::CsGetAlgorithm(SAP_BYTE * data)
/*-----*/
/* Get Algorithm number of compressed data */
/*-----*/ {
    return ((int) (data[4] & (unsigned char) 0x0F));
}
```



The Compression Header

- Bytes [12] – [19]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

– Bytes [17] – Bytes [18]

- Compression Magic
- Always 1f 9d

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úí 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ



The Compression Header

- Bytes [12] – [19]

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úî 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ

– Bytes [19]

- MaxBits

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Råø½\$ Eqü\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# £\$n•• Úî 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ˘° ŸB‡ R‡VÖ



Compressed Data

- Bytes [20] – [N]
 - The compressed stream

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	fc	5c	9d	bf	Rãø¼\$ Eqù\ ¿
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da	ee	0c	34	70	ca	ÖÈ# f\$ñ·· Úí 4pÈ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c	52	87	56	d4	7f	0 ~° ÝB‡ R‡VÖ
04.:	db	53	7f	47	e7	ae	2d	f2	c2	e5	0b	9f	f3	3d	e7	fb	ÛS Gç@-ðÃÃ Ýó=çú
05.:	65	ac	0a	07	0f	8b	17	40	08	8f	d9	b5	94	36	4c	fd	e~ < @ Ûµ"6Lý
06.:	bb	36	a0	56	81	7c	cb	b1	51	3b	85	1c	cd	aa	0c	10	»6 V Ë±Q;... í»
07.:	a0	04	fa	bf	5d	d4	34	28	83	49	14	a1	84	da	09	19	ú¿]04(fI i„Û
08.:	cf	50	6b	90	d4	b1	c0	a0	01	05	80	9c	59	73	71	2e	ïPk Ô±À æYsq.
09.:	11	6a	7f	5b	46	59	9d	ca	7f	d3	b9	38	53	34	8a	70	j [FY Ê Ó¹8S4\$P
0a.:	4e	c3	cc	25	01	18	66	1b	f4	ea	f4	e7	39	ac	1c	81	NÃI% f ôêôç9~
0b.:	ce	e8	be	99	40	65	fe	ea	f4	3e	d6	2f	fc	3d	dc	ed	Ïè¾™@epêô>Ö/ü=Üí
0c.:	a3	ed	c6	15	f2	ca	16	3c	dc	2c	b6	cb	68	b3	72	c5	£íE òÈ <Ü,†Èh³rÅ
0d.:	fe	39	be	14	bd	ae	de	b9	f5	7c	6f	ec	dd	7b	c3	c1	p9¾ ¾@P¹ö olÝ{ÃÃ
0e.:	a4	ab	73	de	e9	3f	3c	06	3c	5a	ba	62	b1	8d	3f	85	„«spé?< <Zºbt ?..
0f.:	42	04	87	d3	51	c2	56	6f	51	8a	08	8e	07	fe	64	d4	B ‡ÓQÃvoQ\$ pdÖ
10.:	7f	4a	06	eb	f0	75	17	2d	f6	82	cf	9a	14	75	e3	50	J êðu -ö, Ìš uãP
11.:	d6	cc	71	45	8b	44	fe	8a	ed	0a	a7	dd	14	3c	50	06	ÖÏqE< Dp\$í \$Ý <P
12.:	c7	26	43	40	06	65	0c	a4	22	a4	a9	c5	4a	43	2d	4a	Ç&C@ e „"„@ÅJC-J
13.:	4d	2a	59	aa	13	55	b5	0e	ba	1a	3f	00					M*Y» Uµ » ?



As an Aside...

- Bytes [12] – Bytes [15]
 - Length of decompressed stream
 - Little-Endian

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 316 Bytes
00.:	00	00	01	38	00	00	11	00	00	01	00	01	af	01	00	00	8
01.:	12	1f	9d	02	52	e5	f8	bd	24	0c	45	71	tc	5c	9d	bf	Råøk\$ Eqü\ z
02.:	d6	c8	23	0e	a3	a7	6e	b7	b7	1e	da						f £\$n•• Ūi 4pÊ
03.:	30	13	1f	ac	b0	09	0e	9f	42	87	0c						~° YB‡ R‡VÖ

- Field is user-controlled, but programmatic type is SAP_INT
 - Signed integer
- What if the original length was 0xffffffff ?
- (thanks Behrang Fouladi)



As an Aside...

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 360 Bytes
00.:	00	00	01	64	00	00	11	00	00	01	00	01	f3	01	00	00	d
01.:	12	1f	9d	02	52	f5	b8	f4	24	0c	05	51					Rō,ō\$ QøøÁÉ
02.:	b5	91	4b	20	28	71	61	bd	6e	8c	0b	fb	c0	04	4c	28	μ' K {qa½n(É ûÄ L{
03.:	58	11	09	0b	d4	20	24	34	ac	b4	34	a4	89	3c	42	c5	X O \$4~'4¼%<BÄ
04.:	c8	bf	75	e5	ef	70	ca	c3	c8	4d	6e	4e	f2	cd	99	39	ÈzuâÿpÈÄÈMnNòí™9
05.:	33	82	80	fd	c7	92	e7	c8	90	1c	0a	d7	96	65	a2	df	3, ýÇ' çÈ x- eçß
06.:	7b	a8	80	c9	0a	a4	b2	6d	32	b9	08	91	6a	19	01	0c	{ " È ¢²m2¹ · j
07.:	48	41	fd	df	27	cb	48	23	4f	94	21	c5	e4	23	32	9e	HAYß' ÈH#O" !Ää#2
08.:	32	b9	40	92	63	09	01	05	24	00	e9	24	eb	b0	a1	c5	2¹@' c \$ e\$è° iÄ
09.:	90	fd	eb	d2	d2	f1	28	e9	87	c6	cd	77	ca	b4	24	ce	ýè00ñ(é:ÆÍwÈ' \$Î
0a.:	a8	b8	73	59	80	c0	76	1d	f4	72	f4	87	22	53	05	28	" sY Àv örô: "S (
0b.:	1b	30	a4	0c	45	24	df	31	84	15	e8	22	11	f9	5b	24	0¼ E\$ß1, è" ù[\$
0c.:	35	68	6f	fe	32	0a	16	28	ca	1b	2e	21	7f	87	94	86	5hop2 (È .! : "†
0d.:	8b	49	38	0d	a3	d7	39	53	0e	40	63	08	23	be	27	0e	< I8 f×9S @c #¾'
0e.:	fc	ae	d6	bf	26	ef	fa	67	b0	88	c2	d9	d4	e1	d6	95	ü0Öz&Yúg° ÄÜÖäÖ
0f.:	c9	f5	60	ea	cf	46	e1	74	ec	70	6a	ba	e4	f5	9a	5a	Éö`êİFátİpjèäöš Z
10.:	bd	77	7b	6e	c7	7d	74	5b	cd	6e	4d	d5	f5	6a	e3	e9	½w{nÇ}t[İnMÖöjâé
11.:	d9	d3	c3	91	c3	fd	d9	7c	c5	63	44	b0	d5	6f	af	d9	ÜÖÄ' ÄÿÜ ÄcD° Öo`Ü
12.:	78	19	6e	11	c1	4e	b3	d7	6d	37	5e	d6	85	49	f0	b1	x n ÄN³×m7^Ö..Iö±
13.:	08	fd	88	eb	83	12	45	dd	d8	94	35	b0	1d	5e	26	b1	ý`èf EYØ"5° ^&±
14.:	36	62	3a	dc	ae	94	b8	ee	c5	06	db	24	83	47	86	d8	6b:Ü@" iÄ Ü\$fg†Ø
15.:	e8	59	31	21	dd	5a	8c	6d	a8	41	a9	eb	95	8c	78	27	èY1!ÝZ(Im"Aöè (K'
16.:	5a	d5	d8	db	55	fb	05	00									ZÖØÜUü

```
30 typedef int SAP_INT; /* Value range: */
```

– What if the original length was 0xfffff ?



As an Aside...

Length: 360 Bytes																		
.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f			
00.: 00	01	64	00	00	11	00	00	01	00	01	f3	01	00	00				
01.: 12	1f	9d	02	52	f5	b8	f4	24	0c	05	51							
02.: b5	91																	
03.: 58	11	*	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	Length: 360 Bytes			
04.: c8	bf	00.	00	01	64	00	00	11	00	00	01	00	01	ff	ff	ff	ff	
05.: 33	82	01.	12	1f	9d	02	52	f5	b8	f4	24	0c	05	51				
06.: 7b	a8	02.	b5	91	4b	20	28	71	61	bd	6e	8c	0b	fb	c0	04	4c	28
07.: 48	41	03.	58	11	09	0b	d4	20	24	34	ac	b4	34	a4	89	3c	42	c5
08.: 32	b9	04.	c8	bf	75	e5	ef	70	ca	c3	c8	4d	6e	4e	f2	cd	99	39
09.: 90	fd	05.	33	82	80	fd	c7	92	e7	c8	90	1c	0a	d7	96	65	a2	df
0a.: a8	b8	06.	7b	a8	80	c9	0a	a4	b2	6d	32	b9	08	91	6a	19	01	0c
0b.: 1b	30	07.	48	41	fd	df	27	cb	48	23	4f	94	21	c5	e4	23	32	9e
0c.: 35	68	08.	32	b9	40	92	63	09	01	05	24	00	e9	24	eb	b0	a1	c5
0d.: 8b	49	09.	90	fd	eb	d2	d2	f1	28	e9	87	c6	cd	77	ca	b4	24	ce
0e.: fc	ae	0a.	a8	b8	73	59	80	c0	76	1d	f4	72	f4	87	22	53	05	28
0f.: c9	f5	0b.	1b	30	a4	0c	45	24	df	31	84	15	e8	22	11	f9	5b	24
10.: bd	77	0c.	35	68	6f	fe	32	0a	16	28	ca	1b	2e	21	7f	87	94	86
11.: d9	d3	0d.	8b	49	38	0d	a3	d7	39	53	0e	40	63	08	23	be	27	0e
12.: 78	19	0e.	fc	ae	d6	bf	26	ef	fa	67	b0	88	c2	d9	d4	e1	d6	95
13.: 08	fd	0f.	c9	f5	60	ea	cf	46	e1	74	ec	70	6a	ba	e4	f5	9a	5a
14.: 36	62	10.	bd	77	7b	6e	c7	7d	74	5b	cd	6e	4d	d5	f5	6a	e3	e9
15.: e8	59	11.	d9	d3	c3	91	c3	fd	d9	7c	c5	63	44	b0	d5	6f	af	d9
16.: 5a	d5	12.	78	19	6e	11	c1	4e	b3	d7	6d	37	5e	d6	85	49	f0	b1
		13.	08	fd	88	eb	83	12	45	dd	d8	94	35	b0	1d	5e	26	b1
		14.	36	62	3a	dc	ae	94	b8	ee	c5	06	db	24	83	47	86	d8
		15.	e8	59	31	21	dd	5a	8c	6d	a8	41	a9	eb	95	8c	78	27
		16.	5a	d5	d8	db	55	fb	05	00								

30

– What if the original length was 0xffffffff ?



As an Aside...

```
00000000 00 01 64 00 00 11 00 00 01 00 01 f3 01 00 00 d ó
00000001 12 1f 9d 02 52 f5 b8 f4 24 0c 05 51 Rō,ô$ QøðÁÉ
00000002 b5 91 * .0 .1 .2 .3 .4 .5 .6 .7 .8 .9 .a .b .c .d .e .f .g .h .i .j .k .l .m .n .o .p .q .r .s .t .u .v .w .x .y .z Length: 360 Bytes
00000003 58 11 00 00 01 64 00 00 11 00 00 01 00 01 ff ff ff ff d yyyÿ
00000004 c8 bf 01 12 1f 9d 02 52 f5 b8 f4 24 0c 05 51 Rō,ô$ QøðÁÉ
00000005 33 82 02 b5 91 4b 20 28 71 61 bd 6e 8c 0b fb c0 04 4c 28 μ' K (qākn(E ŪÀ L(
00000006 7b a8 03 58 11 .0 .1 .2 .3 .4 .5 .6 .7 .8 .9 .a .b .c .d .e .f .g .h .i .j .k .l .m .n .o .p .q .r .s .t .u .v .w .x .y .z Length: 74 Bytes
00000007 48 41 04 c8 bf 05 33 82 0.:49 6e 74 65 72 6e 61 6c 20 54 53 4b 48 20 65 72 Internal TSKH er
00000008 32 b9 05 33 82 1.:72 6f 72 2c 20 73 65 73 73 69 6f 6e 20 74 65 72 rror, session ter
00000009 90 fd 06 7b a8 2.:6d 69 6e 61 74 65 64 20 20 20 20 20 20 20 20 20 20 minated
0000000a a8 b8 07 48 41 3.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0000000b 1b 30 08 32 b9 4.:20 20 20 20 20 20 20 20 20 20 0c
0000000c 35 68 09 90 fd 0a a8 b8 73 59 80 c0 76 1d 14 72 14 87 22 53 05 28 ,SY AV orōz S (
0000000d 8b 49 0a a8 b8 0b 1b 30 a4 0c 45 24 df 31 84 15 e8 22 11 f9 5b 24 0 E$B1, è" ù[$
0000000e fc ae 0c 35 68 6f fe 32 0a 16 28 ca 1b 2e 21 7f 87 94 86 5hop2 (E .! †"†
0000000f c9 f5 0d 8b 49 38 0d a3 d7 39 53 0e 40 63 08 23 be 27 0e < I8 t×9S @c #%'
00000010 bd 77 0e fc ae d6 bf 26 ef fa 67 b0 88 c2 d9 d4 e1 d6 95 ü0Öz&iüg° ^ÀÛôäÖ
00000011 d9 d3 0f c9 f5 60 ea cf 46 e1 74 ec 70 6a ba e4 f5 9a 5a Éö`ëİFátİpjeäöš Z
00000012 78 19 10 bd 77 7b 6e c7 7d 74 5b cd 6e 4d d5 f5 6a e3 e9 žw{nç}t[İnMÖöjâé
00000013 08 fd 11 d9 d3 c3 91 c3 fd d9 7c c5 63 44 b0 d5 6f af d9 ŪŌĀ· ĀŷŪ| Ācd° Ōo~Ū
00000014 36 62 12 78 19 6e 11 c1 4e b3 d7 6d 37 5e d6 85 49 f0 b1 x n ĀN³×m7^Ö..İö±
00000015 e8 59 13 08 fd 88 eb 83 12 45 dd d8 94 35 b0 1d 5e 26 b1 ŷ`ëf EŸø"5° ^&±
00000016 5a d5 14 36 62 3a dc ae 94 b8 ee c5 06 db 24 83 47 86 d8 6b:Ū@" İĀ Ū$fg†ø
00000017 5a d5 d8 db 55 fb 05 00 15 e8 59 31 21 dd 5a 8c 6d a8 41 a9 eb 95 8c 78 27 èY!ŸZ(Īn" A@ë (Īk'
00000018 5a d5 d8 db 55 fb 05 00 16 5a d5 d8 db 55 fb 05 00 ZŌøŪŪŪ
```

– What if the original length was 0xffffffff ?



Sniffing SAP Traffic

- SAP traffic does not lend itself very well to WireShark dissectors...
- Answer was to write a custom protocol analysis tool in Java
- Used 3rd Party pCap JNI interface
 - Allows us to use standard pCap filters / dump files
- Use custom built JNI interface built from MaxDB code



SAPCap

The screenshot displays the SAPCap by SensePost application window. The title bar reads "SAPCap by SensePost...". Below the title bar are three tabs: "SAP Connections & Messages", "Configuration & Control", and "Log".

The "SAP Connections & Messages" tab is active, showing two panes: "Connections" and "Messages".

Connections:

- /192.168.1.60:49941->/192.168.1.10:3200

Messages:

- 0: /192.168.1.60:49941 -> /192.168.1.10:3200
- 1: /192.168.1.60:49941 -> /192.168.1.10:3200
- 2: /192.168.1.10:3200 -> /192.168.1.60:49941
- 3: /192.168.1.10:3200 -> /192.168.1.60:49941
- 4: /192.168.1.10:3200 -> /192.168.1.60:49941
- 5: /192.168.1.10:3200 -> /192.168.1.60:49941
- 6: /192.168.1.10:3200 -> /192.168.1.60:49941
- 7: /192.168.1.10:3200 -> /192.168.1.60:49941
- 8: /192.168.1.60:49941 -> /192.168.1.10:3200
- 9: /192.168.1.10:3200 -> /192.168.1.60:49941
- 10: /192.168.1.60:49941 -> /192.168.1.10:3200
- 11: /192.168.1.10:3200 -> /192.168.1.60:49941
- 12: /192.168.1.10:3200 -> /192.168.1.60:49941
- 13: /192.168.1.60:49941 -> /192.168.1.10:3200
- 14: /192.168.1.10:3200 -> /192.168.1.60:49941
- 15: /192.168.1.60:49941 -> /192.168.1.10:3200
- 16: /192.168.1.10:3200 -> /192.168.1.60:49941
- 17: /192.168.1.60:49941 -> /192.168.1.10:3200

Message Overview:

Source: /192.168.1.10:3200
Destination: /192.168.1.60:49941

Buttons: Decompressed (selected), Compressed

Message Details:

Message	PARAMS	RFC_QUEUE	VERBS	VARs
000.: 43	30 41 38 30 31 30 41 30 39 30 30 34 44 39 36			Length: 46,757 Bytes
001.: 32	32 32 31 43 30 30 32 46 53 41 50 47 55 49 20 20			00A8010A09004D96
002.: 20	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20			Z21C002FSAPGUI
003.: 20	20 20 20 20 20 20 20 20 20 30 30 30 30 30 31			00000001
004.: 00	00 00 00 01 01 01 00 08 01 01 01 01 04 01 01 00			
005.: 01	01 01 01 03 00 04 00 00 02 03 01 03 01 06 00 0b			
006.: 04	01 00 03 01 03 02 00 00 00 23 01 06 00 07 00			#
007.: 0f	31 39 32 2e 31 36 38 2e 31 2e 31 30 20 20 20			192.168.1.10
008.: 00	07 00 18 00 2d 31 39 32 2e 31 36 38 2e 31 2e			-192.168.1.
009.: 31	30 20 20 20 20 20 20 20 20 20 20 20 20 20 20			10
00a.: 20	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20			
00b.: 20	20 20 20 00 18 00 11 00 01 33 00 11 00 12 00 04			3
00c.: 37	30 31 20 00 12 00 13 00 04 37 30 31 20 00 13			701 701
00d.: 00	08 00 20 77 69 6e 78 70 73 61 70 5f 4e 53 50			winxpsap_NSP
00e.: 5f	30 30 20 20 20 20 20 20 20 20 20 20 20 20 20			_00
00f.: 20	20 20 20 00 08 00 06 00 80 53 41 50 47 55 49			SAPGUI
010.: 5f	51 55 45 55 45 45 45 45 0d 09 00 00 d3 7f 7e			_QUEUEEEEE Ó ~
011.: 4b	4e 3a 11 7f 1d 0b b0 4c 43 4e 44 50 4e 3a 11			KN: °LCNDPN:
012.: 17	d3 7f 7e 17 01 11 00 06 42 43 55 53 45 52 01			Ó ~ BCUSER
013.: 11	01 14 00 03 0b ca d6 01 14 01 15 00 01 45 01			ËÖ E
014.: 15	00 09 00 06 42 43 55 53 45 52 00 09 01 34 00			BCUSER 4



SAPCap



C++



JAVA™

C++

- Jpcap
 - JNI interface for pCap
 - Responsible for reading packets
 - pCap dump files
 - Sniffing
 - Filtering packets using standard pCap filters
 - Saving information as pCap dump files

SAPCap



- SAPCap
 - Java
 - Responsible for:
 - Parsing packet data
 - Decompressing messages
 - Queue management

SApCap

C++



JAVA™

C++

- SapCompress
 - JNI interface
 - Implements MaxDB functions for decompression
 - `int[] doDecompress(int[])`

Demo: SApCap

The screenshot displays the SApCap by SensePost application window. The title bar reads "SApCap by SensePost...". Below the title bar are three tabs: "SAP Connections & Messages", "Configuration & Control", and "Log".

The "SAP Connections & Messages" tab is active and divided into two panes:

- Connections:** A list of connections. The selected connection is "/192.168.1.60:49941->/192.168.1.10:3200".
- Messages:** A list of messages. The selected message is "9: /192.168.1.10:3200 -> /192.168.1.60:49941".

The "Message Overview" section shows:

- Source: /192.168.1.10:3200
- Destination: /192.168.1.60:49941

Below the overview are two tabs: "Decompressed" (selected) and "Compressed".

The "Decompressed" view shows a hex dump of the message data. The columns are labeled "Message", "PARAMS", "RFC_QUEUE", "VERBS", and "VARS". The data is displayed in hexadecimal and ASCII. The length of the message is 46,757 Bytes.

Message	PARAMS	RFC_QUEUE	VERBS	VARS
000.: 43	30 41 38 30 31 30 41 30 39 30 30 34 44 39 36			00A8010A09004D96
001.: 32	32 32 31 43 30 30 32 46 53 41 50 47 55 49 20 20			Z21C002FSAPGUI
002.: 20	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20			00000001
003.: 20	20 20 20 20 20 20 20 20 20 30 30 30 30 30 31			
004.: 00	00 00 00 01 01 01 00 08 01 01 01 01 04 01 01 00			
005.: 01	01 01 01 03 00 04 00 00 02 03 01 03 01 06 00 0b			
006.: 04	01 00 03 01 03 02 00 00 00 23 01 06 00 07 00			#
007.: 0f	31 39 32 2e 31 36 38 2e 31 2e 31 30 20 20 20			192.168.1.10
008.: 00	07 00 18 00 2d 31 39 32 2e 31 36 38 2e 31 2e			-192.168.1.
009.: 31	30 20 20 20 20 20 20 20 20 20 20 20 20 20 20			10
00a.: 20	20 20 20 20 20 20 20 20 20 20 20 20 20 20 20			
00b.: 20	20 20 20 00 18 00 11 00 01 33 00 11 00 12 00 04			3
00c.: 37	30 31 20 00 12 00 13 00 04 37 30 31 20 00 13			701 701
00d.: 00	08 00 20 77 69 6e 78 70 73 61 70 5f 4e 53 50			winxpsap_NSP
00e.: 5f	30 30 20 20 20 20 20 20 20 20 20 20 20 20 20			_00
00f.: 20	20 20 20 00 08 00 06 00 80 53 41 50 47 55 49			SAPGUI
010.: 5f	51 55 45 55 45 45 45 45 0d 09 00 00 d3 7f 7e			_QUEUEEEEE Ó ~
011.: 4b	4e 3a 11 7f 1d 0b b0 4c 43 4e 44 50 4e 3a 11			KN: °LCNDPN:
012.: 17	d3 7f 7e 17 01 11 00 06 42 43 55 53 45 52 01			Ó ~ BCUSER
013.: 11	01 14 00 03 0b ca d6 01 14 01 15 00 01 45 01			ËÖ E
014.: 15	00 09 00 06 42 43 55 53 45 52 00 09 01 34 00			BCUSER 4



The Fundamentals

- ~~Understand the compression~~
- ~~Understand the compressed protocol~~
 - ~~Simplify the sniffing and decompression~~
- Recompression
- Understand the application protocol
 - What makes SAP GUI tick ?
- Identify SAP attack vectors not previously considered...



Recompression ?

- Core decompression functions are defined in `vpa105CsObjInt.cpp`
 - `CsDecompr()`

```
122
123  int CsObjectInt::CsDecompr(SAP_BYTE * inbuf, /* ptr input .....*/
124      SAP_INT inlen, /* len of input ....*/
125      SAP_BYTE * outbuf, /* ptr output .....*/
126      SAP_INT outlen, /* len output .....*/
127      SAP_INT option, /* decompr. option */
128      SAP_INT * bytes_read, /* bytes read .....*/
129      SAP_INT * bytes_decompressed) /* bytes decompr. */
130  /*-----*/
131  /*      Decompress                                     */
132  /*      */
133  /* Adaptive Dictionary Compression                   */
134  /*      Lempel-Zip                                    */
```

Recompression ?

- But... vpa105CsObjInt.cpp also contains function for what would appear to be compression...
 - CsCompr()

```
55
56  int CsObjectInt::CsCompr(SAP_INT sumlen,
57                          SAP_BYTE * inbuf,
58                          SAP_INT inlen,
59                          SAP_BYTE * outbuf,
60                          SAP_INT outlen,
61                          SAP_INT option,
62                          SAP_INT * bytes_read,
63                          SAP_INT * bytes_written)
64  /*-----*/
65  /* Compress a memory segmented                                */
66  /*                                                            */
67  /* Adaptive Dictionary Compression                          */
68  /*   Lempel-Zip                                             */
69  /*                                                            */
```

Recompression ?

- We modify our JNI library to make use of MaxDB code
 - doCompress()
 - doDecompress()

```
1
2 #include <jni.h>
3 #include <stdio.h>
4 #include <stdlib.h>
5 #include <assert.h>
6
7 #include "SapLib.h"
8 #include "hpa101satype.h"
9 #include "hpa104CsObject.h"
10 #include "hpa106cslzc.h"
11 #include "hpa107cslzh.h"
12 #include "hpa105CsObjInt.h"
13
14 JNIEXPORT jintArray JNICALL Java_com_sensepost_SAPProx_jni_JniInterface_ldoDecompress
15 (JNIEnv * env, jobject obj, jintArray in) {...}
82
83 JNIEXPORT jintArray JNICALL Java_com_sensepost_SAPProx_jni_JniInterface_ldoCompress
84 (JNIEnv * env, jobject obj, jintArray in) {...}
```



Recompression ?

- We now have programmatic interface to:
 - Decompress SAP traffic
 - doDecompress()
 - Useful for interception and sniffing
 - Compress SAP traffic
 - doCompress()
 - Useful for MiTM attacks
 - Useful for assessment of SAP Gui Applications



The Fundamentals

- ~~Understand the compression~~
- ~~Understand the compressed protocol~~
 - ~~Simplify the sniffing and decompression~~
- ~~Recompression~~
- Understand the application protocol
 - What makes SAP GUI tick ?
- Identify SAP attack vectors not previously considered...



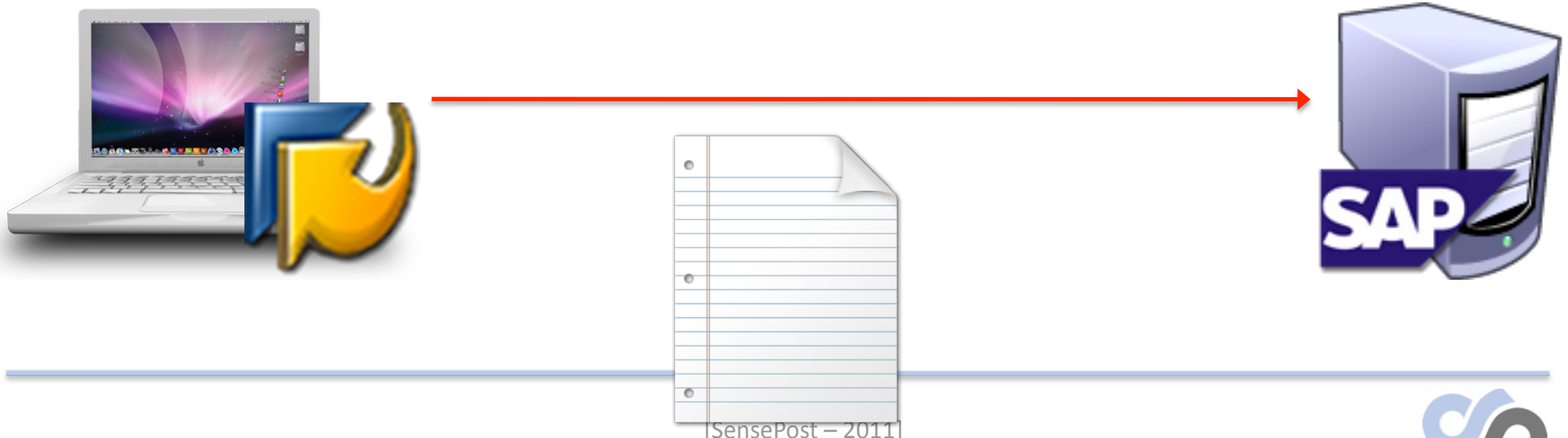
The Application Protocol

- Multiplexed
 - Single connection per-user per-location per-host



The Application Protocol

- Multiplexed
 - Single connection per-user per-location per-host
- Initial hand-shake is uncompressed



The Application Protocol

- Multiplexed
 - Single connection per-user per-location per-host
- Initial hand-shake is uncompressed
- Server response is compressed



[SensePost – 2011]



The Application Protocol

- Multiplexed
 - Single connection per-user per-location per-host
- Initial hand-shake is uncompressed
- Server response is compressed
- Uncompressed component is static
 - Terminal name
 - Options change depending on capabilities of SAP GUI (support bits)



Message Types

- Two basic Types of Messages
 - Simple Messages
 - Complex Messages
- Message structures differ in terms of direction
 - GUI -> Server
 - Server -> GUI



Simple Messages : GUI -> SAP

- Header
 - “OK Code”
 - Character Encoding
 - GUI Version
- Data
 - Input values
 - XML Stream defining screen metrics



Simple Messages : GUI -> SAP

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 499 Bytes
00.:	01	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00	█
01.:	00	10	06	23	00	0f	00	00	10	0e	01	34	31	31	30	00	# 4110
02.:	55	54	46	38	00	10	04	09	00	03	37	32	30	10	04	19	UTF8 720
03.:	00	02	00	00	10	0f	01	00	10	00	00	07	00	0a	00	00	
04.:	00	00	00	00	00	00	00	00	10	04	04	00	08	00	14		
05.:	00	07	00	10	00	07	10	04	17	00	02	00	1f	10	04	16	
06.:	00	02	00	13	10	05	01	00	16	00	05	00	00	03	1b	11	
07.:	3d	10	5b	31	10	00	11	00	00	00	00	00	00	00	10		= [1
08.:	0c	08	00	10	00	00	03	e6	00	00	07	70	00	00	03	e6	æ p æ
09.:	00	00	07	70	10	0c	06	00	21	00	00	00	11	00	00	00	p !
0a.:	00	00	00	00	31	00	00	01	10	00	00	00	00	00	00	00	1
0b.:	00	00	00	00	13	00	00	00	5b	02	10	0a	01	00	09	00	[
0c.:	00	00	00	00	00	5b	00	13	10	09	02	00	31	00	18	00	[1
0d.:	01	79	00	01	00	00	02	00	14	40	00	06	0c	00	0c	62	y @ b
0e.:	63	75	73	65	72	00	19	04	01	79	00	01	00	00	03	00	user y
0f.:	14	42	00	07	0c	00	28	6d	69	6e	69	73	61	70	10	09	B (minisap
10.:	0b	00	0a	01	00	03	00	14	00	00	00	07	00	11	00	00	
11.:	00	e0	3c	3f	78	6d	6c	20	76	65	72	73	69	6f	6e	3d	à<?xml version="
12.:	22	31	2e	30	22	20	65	6e	63	6f	64	69	6e	67	3d	22	"1.0" encoding="
13.:	73	61	70	2a	22	3f	3e	0a	3c	44	41	54	41	4d	41	4e	sap*"?> <DATAMAN
14.:	41	47	45	52	3e	0a	20	20	3c	43	4f	50	59	20	69	64	AGER> <COPY id
15.:	3d	22	63	6f	70	79	22	3e	0a	20	20	20	20	3c	47	55	="copy"> <GU
16.:	49	20	69	64	3d	22	67	75	69	22	3e	0a	20	20	20	20	I id="gui">
17.:	20	20	3c	4d	45	54	52	49	43	53	20	69	64	3d	22	6d	<METRICS id="m
18.:	65	74	72	69	63	73	22	20	58	33	3d	22	31	39	32	30	etrics" X3="1920
19.:	22	20	58	32	3d	22	37	22	20	58	31	3d	22	37	22	20	" X2="7" X1="7"
1a.:	58	30	3d	22	32	38	33	22	20	59	33	3d	22	31	32	30	X0="283" Y3="120
1b.:	30	22	20	59	32	3d	22	32	30	22	20	59	31	3d	22	31	0" Y2="20" Y1="1
1c.:	32	22	20	59	30	3d	22	32	38	33	22	2f	3e	0a	20	20	2" Y0="283"/>
1d.:	20	20	3c	2f	47	55	49	3e	0a	20	20	3c	2f	43	4f	50	</GUI> </COP
1e.:	59	3e	0a	3c	2f	44	41	54	41	4d	41	4e	41	47	45	52	Y> </DATAMANAGER
1f.:	3e	0a	0c														>



Simple Messages : SAP -> GUI

- Header
- Data
- “TH”



Simple Messages : SAP -> GUI

- Header
 - Encoding

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 9,322 Bytes
000.:	10	06	11	00	20	ff	7f	fe	2d	d8	b7	37	d6	74	08	7e	ÿ p-ø·70t ~
001.:	13	05	97	15	97	eb	f2	2f	8d	03	20	0e	00	00	00	00	--èð/
002.:	00	00	00	00	00	10	06	23	00	0f	00	00	10	0e	01	34	#
003.:	31	31	30	00	55	54	46	38	00	10	06	27	00	20	00	00	110 UTF8
004.:	10	07	02	34	31	30	33	00	55	6e	69	63	6f	64	65	4c	4103 UnicodeL
005.:	69	74	74	6c	65	55	6e	6d	61	72	6b	65	64	00	10	06	ittleUnmarked
006.:	21	00	20	31	32	39	33	35	43	45	30	35	44	46	42	46	1EBA4F0000C29DE8
007.:	31	45	42	41	34	46	30	30	30	30	43	32	39	44	45	38	4A3 NSP
008.:	34	41	33	10	06	02	00	03	4e	53	50	10	06	03	00	08	winxpsap
009.:	77	69	6e	78	70	73	61	70	10	06	19	00	02	00	19	10	"\àjûñið)
00a.:	06	01	00	02	00	00	10	06	0a	00	02	00	00	10	06	1f	P, E % TRADESH
00b.:	00	12	01	12	93	5c	e0	5d	fb	f1	ec	a4	f0	00	0c	29	OW 00 &0
00c.:	de	84	a3	01	10	06	25	00	0a	54	52	41	44	45	53	48	
00d.:	4f	57	00	10	06	13	00	08	01	30	30	00	26	30	00	00	



Simple Messages : SAP -> GUI

- Header
 - Encoding
 - Transaction ID

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 9,322 Bytes
000.:	10	06	11	00	20	ff	7f	fe	2d	d8	b7	37	d6	74	08	7e	ÿ p-ø·7ot ~
001.:	13	05	97	15	97	eb	f2	2f	8d	03	20	0e	00	00	00	00	— -èð/
002.:	00	00	00	00	00	10	06	23	00	0f	00	00	10	0e	01	34	# 4
003.:	31	31	30	00	55	54	46	38	00	10	06	27	00	20	00	00	110 UTF8
004.:	10	07	02	34	31	30	33	00	55	6e	69	63	6f	64	65	4c	4103 UnicodeL
005.:	69	74	74	6c	65	55	6e	6d	61	72	6b	65	64	00	10	06	
006.:	21	00	20	31	32	39	33	35	43	45	30	35	44	46	42	46	! 12935CE05DFBF
007.:	31	45	42	41	34	46	30	30	30	30	43	32	39	44	45	38	1EBA4F0000C29DE8
008.:	34	41	33	10	06	02	00	03	4e	53	50	10	06	03	00	08	4A3
009.:	77	69	6e	78	70	73	61	70	10	06	19	00	02	00	19	10	psap
00a.:	06	01	00	02	00	00	10	06	0a	00	02	00	00	10	06	1f	
00b.:	00	12	01	12	93	5c	e0	5d	fb	f1	ec	a4	f0	00	0c	29	"\àjûñið)
00c.:	de	84	a3	01	10	06	25	00	0a	54	52	41	44	45	53	48	P, E % TRADESH
00d.:	4f	57	00	10	06	13	00	08	01	30	30	00	26	30	00	00	OW 00 &0



Simple Messages : SAP -> GUI

- Header
 - Encoding
 - Transaction ID
 - System & Hostname

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 9,322 Bytes
000.:	10	06	11	00	20	ff	7f	fe	2d	d8	b7	37	d6	74	08	7e	ÿ p-ø·70t ~
001.:	13	05	97	15	97	eb	f2	2f	8d	03	20	0e	00	00	00	00	— -ëð/
002.:	00	00	00	00	00	10	06	23	00	0f	00	00	10	0e	01	34	# 4
003.:	31	31	30	00	55	54	46	38	00	10	06	27	00	20	00	00	110 UTF8
004.:	10	07	02	34	31	30	33	00	55	6e	69	63	6f	64	65	4c	4103 UnicodeL
005.:	69	74	74	6c	65	55	6e	6d	61	72	6b	65	64	00	10	06	ittleUnmarked
006.:	21	00	20	31	32	39	33	35	43	45	30	35	44	46	42	46	! 12935CE05DFBF
007.:	31	45	42	41	34	46	30	30	30	30	43	32	39	44	45	38	1EBA4F0000C28DF8
008.:	34	41	33	10	06	02	00	03	4e	53	50	10	06	03	00	08	423 NSP
009.:	77	69	6e	78	70	73	61	70	10	06	19	00	02	00	19	10	winxpsap
00a.:	06	01	00	02	00	00	10	06	0a	00	02	00	00	10	06	1f	" \à]ûñið)
00b.:	00	12	01	12	93	5c	e0	5d	fb	f1	ec	a4	f0	00	0c	29	P, E % TRADESH
00c.:	de	84	a3	01	10	06	25	00	0a	54	52	41	44	45	53	48	OW 00 &0
00d.:	4f	57	00	10	06	13	00	08	01	30	30	00	26	30	00	00	



Simple Messages : SAP -> GUI

- Header
 - Encoding
 - Transaction ID
 - System Name
 - Host name
 - Theme

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 9,322 Bytes
000.:	10	06	11	00	20	ff	7f	fe	2d	d8	b7	37	d6	74	08	7e	ÿ p-ø·70t ~
001.:	13	05	97	15	97	eb	f2	2f	8d	03	20	0e	00	00	00	00	— -èð/
002.:	00	00	00	00	00	10	06	23	00	0f	00	00	10	0e	01	34	# 4
003.:	31	31	30	00	55	54	46	38	00	10	06	27	00	20	00	00	110 UTF8
004.:	10	07	02	34	31	30	33	00	55	6e	69	63	6f	64	65	4c	4103 UnicodeL
005.:	69	74	74	6c	65	55	6e	6d	61	72	6b	65	64	00	10	06	ittleUnmarked
006.:	21	00	20	31	32	39	33	35	43	45	30	35	44	46	42	46	! 12935CE05DFBF
007.:	31	45	42	41	34	46	30	30	30	30	43	32	39	44	45	38	1EBA4F0000C29DE8
008.:	34	41	33	10	06	02	00	03	4e	53	50	10	06	03	00	08	4A3 NSP
009.:	77	69	6e	78	70	73	61	70	10	06	19	00	02	00	19	10	winxpsap
00a.:	06	01	00	02	00	00	10	06	0a	00	02	00	00	10	06	1f	
00b.:	00	12	01	12	93	5c	e0	5d	fb	f1	ec	a4	f0	00	0c	29	" \àj053HA
00c.:	de	84	a3	01	10	06	25	00	0a	54	52	41	44	45	53	48	TRADESH
00d.:	4f	57	00	10	06	13	00	08	01	30	30	00	26	30	00	00	OW



Simple Messages : SAP -> GUI

- Data
 - SAP Program Context & SAP Screen

069.:	53	68	69	66	74	00	10	06	06	00	02	00	c8	10	06	07	Shift	È
06a.:	00	24	53	30	30	30	20	20	20	20	20	20	20	20	20	20	\$S000	
06b.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
06c.:	20	20	20	20	20	20	01	00	00	00	00	00	00	21	00	00		!
06d.:	00	00	00	00	00	16	54	10	0c	07	00	10	00	00	00	16		T
06e.:	00	00	00	54	00	00	00	16	00	00	00	54	10	04	1a	00		T T
06f.:	01	2c	10	04	1b	00	01	45	10	04	1c	00	0c	20	20	20		, E
070.:	20	20	20	20	20	20	20	20	20	10	06	0c	00	03	30	30		00
071.:	30	10	0c	0a	00	14	53	41	50	20	52	2f	33	20	28	31	0	SAP R/3 (1
072.:	29	20	4e	53	50	20	20	20	20	10	06	0f	00	28	53) NSP (S	
073.:	41	50	4d	53	59	53	54	20	20	20	20	20	20	20	20	20	APMSYST	
074.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
075.:	20	20	20	20	20	20	20	10	06	10	00	14	30	30	32	30		0020
076.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
077.:	10	06	0d	00	28	53	41	50	4d	53	59	53	54	20	20	20		(SAPMSYST
078.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20		
079.:	20	20	20	20	20	20	20	20	20	20	20	20	20	10	06	0e		
07a.:	00	04	30	30	32	30	12	0b	01	00	00	00	56	00	1c	01		0020 v
07b.:	00	00	00	16	00	01	00	00	00	00	00	00	00	00	00	00		
07c.:	00	55	73	65	72	00	55	00	00	00	1e	02	00	00	00	16		User U
07d.:	00	02	00	00	00	00	00	00	00	00	00	00	00	53	79	73		Sys
07e.:	74	65	6d	00	79	00	00	00	1c	03	00	00	00	16	00	03		tem y
07f.:	00	00	00	00	00	00	00	00	00	00	00	48	65	6c	70	00		Help
080.:	48	00	00	12	0b	02	00	00	0c	8c	00	1e	01	01	00	00		H (E
081.:	02	64	01	01	00	00	00	00	00	00	00	00	00	00	4c	6f		d Lo
082.:	67	20	6f	6e	00	4c	00	00	00	24	01	02	00	00	12	05		g on L \$
083.:	01	02	00	00	00	00	00	00	00	00	00	00	4e	65	77	20		New
084.:	70	61	73	73	77	6f	72	64	00	4e	00	00	00	1f	01	03		password N
085.:	00	00	12	0f	01	03	00	00	00	00	00	00	00	00	00	00		
086.:	4c	6f	67	20	6f	66	66	00	4f	00	00	00	26	02	01	00		Log off O &
087.:	00	00	64	02	01	00	00	00	00	00	00	00	00	00	00	43		d C
088.:	72	65	61	74	65	20	53	65	73	73	69	6f	6e	00	45	00		reate Session E
089.:	00	00	23	02	02	00	00	00	64	02	02	00	00	00	00	00		# d



Simple Messages : SAP -> GUI

- Data
 - SAP Program Context & SAP Screen
 - Menus & Keyboard Accelerators

07c.:	00	55	73	65	72	00	55	00	00	00	1e	02	00	00	00	16	User U
07d.:	00	02	00	00	00	00	00	00	00	00	00	00	00	53	79	73	Sys
07e.:	74	65	6d	00	79	00	00	00	1c	03	00	00	00	16	00	03	tem y
07f.:	00	00	00	00	00	00	00	00	00	00	48	65	6c	70	00		Help
080.:	48	00	00	12	0b	02	00	00	0c	8c	00	1e	01	01	00	00	H (E
081.:	02	64	01	01	00	00	00	00	00	00	00	00	00	4c	6f		d Lo
082.:	67	20	6f	6e	00	4c	00	00	00	24	01	02	00	00	12	05	g on L \$
083.:	01	02	00	00	00	00	00	00	00	00	00	4e	65	77	20		New
084.:	70	61	73	73	77	6f	72	64	00	4e	00	00	00	1f	01	03	password N
085.:	00	00	12	0f	01	03	00	00	00	00	00	00	00	00	00	00	Log off O &
086.:	4c	6f	67	20	6f	66	66	00	4f	00	00	00	26	02	01	00	d C
087.:	00	00	64	02	01	00	00	00	00	00	00	00	00	00	00	43	reate Session E
088.:	72	65	61	74	65	20	53	65	73	73	69	6f	6e	00	45	00	# d
089.:	00	00	23	02	02	00	00	00	64	02	02	00	00	00	00	00	End Session
08a.:	00	00	00	00	00	45	6e	64	20	53	65	73	73	69	6f	6e	D \$d
08b.:	00	44	00	00	00	24	02	03	00	00	06	64	02	03	00	00	



Simple Messages : SAP -> GUI

- Data
 - SAP Program Context & SAP Screen
 - Menus & Keyboard Accelerators
 - Input dialogs

```
153.:00 00 00 00 00 00 00 10 0c 06 00 21 00 00 00 11 | !
154.:00 00 00 00 00 00 00 11 00 00 00 5b 00 00 00 00 | [
155.:00 00 00 00 00 00 00 11 00 00 00 5b 02 10 0a 01 | [
156.:00 09 00 00 00 00 00 00 00 00 00 12 09 02 00 00 |
157.:03 9e 00 24 00 02 7b 00 01 00 00 00 01 21 00 | $ { !
158.:12 12 00 12 43 6c 69 65 6e 74 20 20 20 20 20 20 | Client
159.:20 20 20 20 20 20 00 18 00 02 72 00 01 00 00 00 | r
15a.:00 01 21 52 53 59 53 54 2d 4d 41 4e 44 54 00 15 | !RSYST-MANDT
15b.:00 00 79 00 01 00 00 00 00 14 40 00 03 03 00 03 | y @
15c.:30 30 31 00 18 00 00 72 00 01 00 00 00 00 14 40 | 001 r @
15d.:52 53 59 53 54 2d 4d 41 4e 44 54 00 4f 00 00 78 | RSYST-MANDT O x
15e.:00 01 00 00 00 00 14 40 3c 50 72 6f 70 65 72 74 | @<Propert
15f.:79 62 61 67 3e 3c 44 65 66 61 75 6c 74 54 6f 6f | ybag><DefaultToo
160.:6c 74 69 70 3e 43 6c 69 65 6e 74 3c 2f 44 65 66 | ltip>Client</Def
161.:61 75 6c 74 54 6f 6f 6c 74 69 70 3e 3c 2f 50 72 | aultTooltip></Pr
162.:6f 70 65 72 74 79 62 61 67 3e 00 49 00 00 7f 00 | opertybag> I
163.:01 00 00 00 00 23 21 00 13 00 38 49 6e 66 6f 72 | #! 8Infor
164.:6d 61 74 69 6f 6e 20 20 20 20 20 20 20 20 20 20 | mation
165.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 |
166.:20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 |
167.:20 20 20 00 1a 00 00 72 00 01 00 00 00 00 23 21 | r #!
168.:4d 45 53 53 41 47 45 5f 46 52 41 4d 45 00 24 00 | MESSAGE FRAME $
169.:03 7b 00 01 00 00 02 00 01 21 00 12 12 00 12 53 | { ! 0
16a.:73 65 72 20 20 20 20 20 20 20 20 20 20 20 20 20 | ser
16b.:20 00 18 00 03 72 00 01 00 00 02 00 01 21 52 53 | r !RS
16c.:59 53 54 2d 42 4e 41 4d 45 00 1e 00 01 79 00 01 | YST-BNAME y
16d.:00 00 02 00 14 40 00 0c 0c 00 0c 3f 20 20 20 20 | @ ?
16e.:20 20 20 20 20 20 20 00 18 00 01 72 00 01 00 00 | r
```



Simple Messages : SAP -> GUI

- Data
 - SAP Program Context & SAP Screen
 - Menus & Keyboard Accelerators
 - Input dialogs
 - Screen Data

```
1cf.: 04 00 7a 01 07 00 00 06 00 00 21 00 84 36 00 84 z ! " 6 "
1d0.: 54 68 72 65 65 20 63 6c 69 65 6e 74 73 3a 20 30 Three clients: 0
1d1.: 30 30 2c 20 30 30 31 20 61 6e 64 20 30 36 36 2e 00, 001 and 066.
1d2.: 20 20 46 6f 72 20 61 6c 6c 20 70 75 72 70 6f 73 For all purpos
1d3.: 65 73 2c 20 30 30 31 20 73 68 6f 75 6c 64 20 62 es, 001 should b
1d4.: 65 20 75 73 65 64 2e 20 20 20 20 20 20 20 20 20 e used.
1d5.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
1d6.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
```



Simple Messages : SAP -> GUI

- “TH”
 - System Name
 - Transaction
 - Transaction ID

237.:	05	00	09	02	00	08	00	01	00	1f	00	0b	10	0a	06	00	
238.:	19	54	43	5f	49	55	53	52	41	43	4c	00	53	41	50	4d	TC_IUSRACL SAPM
239.:	53	59	53	54	00	30	30	32	30	00	10	09	0b	00	0a	01	SYST 0020
23a.:	00	02	00	14	00	00	00	00	00	12	04	18	00	00	00	b9	1
23b.:	2a	54	48	2a	02	00	b9	00	00	4e	53	50	20	20	20	20	*TH* 1 NSP
23c.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
23d.:	20	20	20	20	20	20	20	20	20	00	01	20	20	20	20	20	
23e.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
23f.:	20	20	20	20	20	20	20	20	20	20	20	53	45	53	53	49	SESSI
240.:	4f	4e	5f	4d	41	4e	41	47	45	52	20	20	20	20	20	20	ON_MANAGER
241.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
242.:	20	20	20	00	01	4e	53	50	20	20	20	20	20	20	20	20	NSP
243.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
244.:	20	20	20	20	20	31	32	39	33	35	43	45	30	35	44	46	12935CE05DF
245.:	42	46	31	45	45	41	34	46	30	30	30	30	43	32	39	44	BF1EEA4F0000C29D
246.:	45	38	34	41	33	2a	54	48	2a	0c							E84A3*TH*



Dialogs

- All input fields accept strings
 - No client-side validation
 - Data is validated on the server
- Input field lengths can be manipulated



Dialogs

- All input fields accept strings
 - No client-side validation
 - Data is validated on the server
- Input field lengths can be manipulated

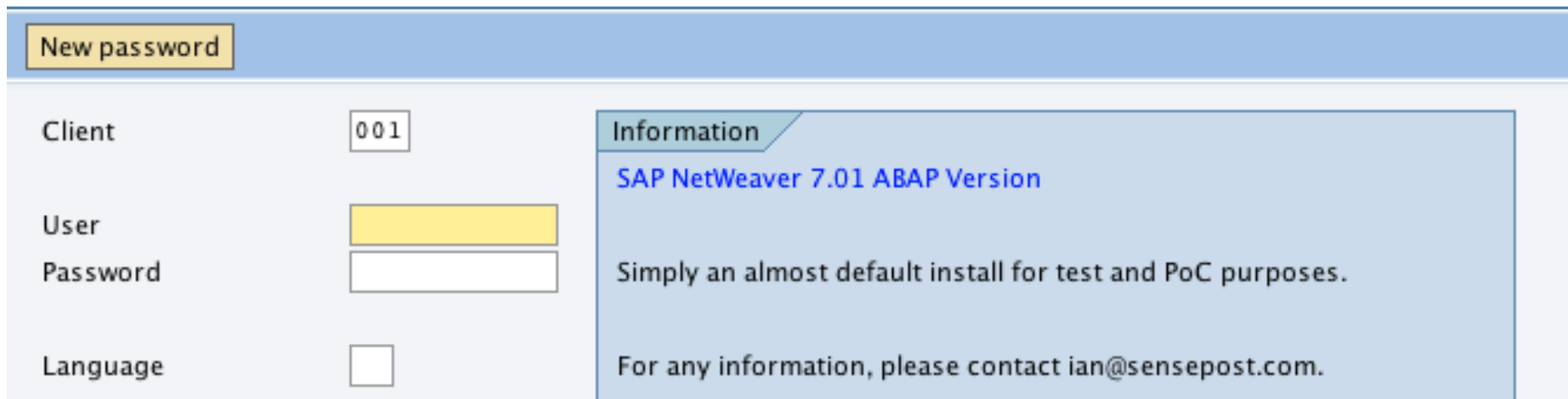
```
34.:00 01 25 52 53 59 53 54 2d 42 4e 41 4d 45 00 1c | %RSYST-BNAME
35.:00 01 79 00 01 00 00 02 00 14 44 00 0c 0c 00 0c | y D
36.:41 53 44 20 20 20 20 20 20 20 20 20 20 20 20 20 | ASD
37.:72 00 01 00 00 02 00 14 44 52 53 59 53 54 2d 42 | r DRSYST-B
38.:4e 41 4d 45 00 52 00 01 78 00 01 00 00 02 00 14 | NAME R x
39.:44 3c 50 72 6f 70 65 72 74 79 62 61 67 3e 3c 44 | D<Propertybag><D
3a.:65 66 61 75 6c 74 54 6f 6f 6c 74 69 70 3e 55 73 | efaultTooltip>Us
3b.:65 72 20 6e 61 6d 65 3c 2f 44 65 66 61 75 6c 74 | er name</Default
3c.:54 6f 6f 6c 74 69 70 3e 3c 2f 50 72 6f 70 65 72 | Tooltip></Proper
3d.:74 79 62 61 67 3e 00 12 04 03 7b 00 01 00 00 03 | tybag> {
3e.:00 01 25 00 00 12 00 34 00 18 04 03 72 00 01 00 | % 4 r
3f.:00 03 00 01 25 52 53 59 53 54 2d 42 43 4f 44 45 | %RSYST-BCODE
40.:00 3a 04 81 79 00 01 00 00 03 00 14 46 00 28 0c | : y F (
```



Dialogs

- All input fields accept strings
 - No client-side validation
 - Data is validated on the server
- Input field lengths can be manipulated

SAP



The screenshot shows the 'New password' dialog box in SAP. It features a title bar with the text 'New password'. Below the title bar, there are four input fields: 'Client' with the value '001', 'User' (highlighted in yellow), 'Password' (empty), and 'Language' (empty). To the right of these fields is an 'Information' panel with a blue header. The information panel contains the text: 'SAP NetWeaver 7.01 ABAP Version', 'Simply an almost default install for test and PoC purposes.', and 'For any information, please contact ian@sensepost.com'.



Dialogs

- All input fields accept strings
 - No client-side validation
 - Data is validated on the server
- Input field lengths can be manipulated

```
34.:00 01 25 52 53 59 53 54 2d 42 4e 41 41 45 00 41 %RSYST-BNAME
35.:00 01 79 00 01 00 00 02 00 14 44 00 ff ff 00 ff y D yy y
36.:41 53 44 20 20 20 20 20 20 20 20 20 ASD
37.:72 00 01 00 00 02 00 14 44 52 53 59 53 54 2d 42 r DRSYST-B
38.:4e 41 4d 45 00 52 00 01 78 00 01 00 00 02 00 14 NAME R x
39.:44 3c 50 72 6f 70 65 72 74 79 62 61 67 3e 3c 44 D<Propertybag><D
```



Dialogs

- All input fields accept strings
 - No client-side validation
 - Data is validated on the server
- Input field lengths can be manipulated

New password

Client	001	Information
User	ASD	SAP NetWeaver 7.01 ABAP Version
Password		Simply an almost default install for test and PoC purposes.
Language		For any information, please contact ian@sensepost.com.

Dialogs

- Length of submitted strings can be adjusted in a similar fashion...

```
0e.: 63 75 73 65 72 00 1a 04 01 79 00 01 00 00 03 00 cuser v
0f.: 14 42 00 08 0c 00 28 70 61 73 73 77 6f 72 64 10 B password
10.: 09 0b 00 01 00 03 00 14 00 00 00 08 00 11 00
11.: 00 00 e0 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e à<?xml version
```



Dialogs

- Length of submitted strings can be adjusted in a similar fashion...

```
0e.: 63 75 73 65 72 00 1a 04 01 79 00 01 00 00 03 00 cuser v
0f.: 14 42 00 12 0c 00 28 61 61 61 61 61 61 61 61 B aaaaaaaaaa
10.: 61 61 61 61 01 00 03 00 14 00 00 00 08 00 11 00 aaa
11.: 00 00 e0 3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e a?xml version
12.: 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d ="1.0" encoding=
```



Complex Messages

- Contain the same structures as simple messages...



Complex Messages

- Contain the same structures as simple messages...
- ... But include XML structure:
 - <SVARS>



Complex Messages

- Contain the same structures as simple messages...
- ... But include XML structure:

– <SVARS>

50	4c	4f	4c	45	41	01	30	00	17	00	00	00	17	05	02	PLOLEA 0
00	00	05	02	00	0b	00	04	37	30	31	20	00	0b	01	02	701
00	0e	4f	4c	45	5f	46	4c	55	53	48	5f	43	41	4c	4c	OLE_FLUSH_CALL
01	02	03	37	00	00	03	37	05	03	00	00	05	03	05	12	7 7
00	00	05	12	02	05	00	0f	45	58	43	45	50	54	5f	44	EXCEPT_D
45	53	43	52	49	50	54	02	05	02	05	00	0a	45	58	50	ESCRIP
4f	52	54	5f	58	4d	4c	02	05	02	05	00	05	53	56	41	ORT_XML
52	53	02	05	02	01	00	0a	49	4d	50	4f	52	54	5f	58	RS
4d	4c	02	01	02	03	00	01	00	02	03	3c	02	00	00	3c	ML
02	3c	05	00	07	3c	53	56	41	52	53	3e	3c	05	3c	05	< <SVARS>< <
00	08	3c	2f	53	56	41	52	53	3e	3c	05	3c	02	00	00	</SVARS>< <
3c	02	02	13	00	06	02	08	04	00	ff	01	02	13	03	01	< y
00	0a	45	52	52	4f	52	5f	49	4e	46	4f	03	01	03	02	ERROR_INFO
00	08	00	00	01	04	00	00	00	00	03	02	02	13	00	09	
04	00	04	00	04	00	20	00	04	02	13	03	01	00	06	50	P
41	52	41	4d	53	03	01	03	02	00	08	00	00	00	2c	00	ARAMS
00	01	29	03	02	03	05	00	fa	7b	02	7c	ea	00	00	05) ú{ e
f6	0c	33	00	00	12	1f	9d	02	52	a9	d9	e4	88	75	02	ö 3 R@Uä u
41	f8	2a	48	be	c0	e3	1f	0e	e0	9d	95	28	3f	b3	c8	Äø*H&Ää ä (?³È



Complex Messages

- Contain the same structures as simple messages...
- ... But include XML structure:
 - <SVARS>
- Include compressed streams:
 - PARAMS



Complex Messages

- Contain the messages...
- ... But include
 - <SVARS>
- Include commands
 - PARAMS

```
:04 00 04 00 04 00 20 00 04 02 13 03 01 00 06 50
:41 52 41 4d 53 03 01 03 02 00 08 00 00 00 2c 00 ARAMS
:00 01 29 03 02 03 02 02 fa 7b 02 7c ea 00 00 05
:f6 0c 33 00 00 12 1f 9d 02 52 a9 d9 e4 88 75 02
:41 f8 2a 48 be c0 0e e0 9d 95 28 3f b3 c8
:ca f7 bf 45 28 9a 47 8f c6 52 aa f2 24 cb 8b f9
:54 2a a0 a0 1b 66 42 88 21 c4 14 be ad ff fe fb
:4b eb 1f a0 1c be a5 af 3f fb fa e5 10 8e ee cf
:3f bf ff f5 f1 e3 ef 5f 08 ff 4a 30 ed 2c 78 a8
:61 b3 f0 4b 3d b4 70 75 f3 d7 9f 7d fd 7a b8 6c
:f9 fa b3 af df 08 af 07 3e b6 19 6c 2e 84 b1 c5
:27 5c 96 8d 2d da 3a 48 63 8b 10 c3 a0 14 0f 10
:2b da fc 46 68 62 3d 14 5d 70 87 a5 ba 58 b7 6a
:1e e8 d8 b0 6e e0 15 0f 58 b7 c3 52 0f 58 b7 a6
:79 48 4f b0 fc 08 1e 12 80 ae cd 6f 02 00 cf 8a
:2e 4c 0e 51 17 eb 66 b9 e4 ba 58 b3 29 ea 62 6e
:8f 2e 9d 33 cc d7 61 d9 7e 4b 98 03 f3 40 f7 5b
:02 f7 04 69 6c f9 71 96 8d 2d 47 67 d9 d8 32 ce
:86 73 4e 03 05 03 05 00 fa 52 0f d9 59 ea a1 38
:4b 3d d8 fe d1 3c 34 67 a9 87 ee 2c f5 80 3c 8a
:67 5f 9e ce 32 0f e5 71 96 79 28 58 37 f1 ec 2b
:c9 59 ea 21 3b 4b 3d 60 dd c4 73 b2 54 67 a9 87
:66 ac b2 2f 0a d6 4d 3c 27 cb 70 96 7a 98 c6 2a
:1e ea 13 ec bc 16 3c d4 68 ac 72 ee d4 e4 ba 6c
:2d 6a 76 96 9d 3b af 5f 69 6c 58 63 f1 ac ae d5
:59 3a b6 66 ac 52 87 2a bc 8a e7 7a 1d ce 52 0f
:d3 59 e6 a1 3d a7 1e 0a 1e 5a 74 96 79 68 c9 58
:69 1e ca 65 a5 7d 91 c4 b3 ba 65 67 a9 df 62 ac
:ba 2f 92 78 56 b7 6a ac b2 2f 5a 73 5d ba 6e dd
:59 65 5f 1c 0f 74 6c 6d e5 2c 89 35 a0 4d 67 d9
:d8 fa 63 ac 92 87 8e 9c 89 35 a0 27 67 a9 87 ec
:2c f5 80 3c 88 35 a0 57 67 a9 87 66 ac 32 0f 7b
:2d fe 47 bd 48 62 bd e8 9f 58 ea 77 18 ab 78 e8
:c8 83 58 2f c6 13 ac 4f 54 d8 68 ac b2 87 46 72
:5d 36 bf 03 05 03 05 00 fa 23 3b cb f6 d0 28 d7
```



Complex Messages

- Contain the same structures as simple messages...
- ... But include XML structure:
 - <SVARS>
- Include compressed streams:
 - PARAMS
 - RFC_QUEUE



Complex Messages

- Contain the same messages...
- ... But include X
– <SVARS>
- Include compressed
– PARAMS
– RFC_QUEUE

00	08	00	04	00	08	00	04	00	20	00	08	04	04	04	ff		y
01	04	ff	01	04	ff	01	04	ff	01	04	ff	01	04	ff	01		
04	ff	01	02	13	03	01	00	09	52	46	43	5f	51	55	4		y RFC_QUEUE
55	45	03	01	03	02	00	08	00	00	07	3d	00	00	00	1		UE =
03	02	03	05	00	fa	7b	02	7c	ea	00	00	2f	ec	b8	ad		
00	00	12	1f	9d	2	bb	7d	b3	80	8b	6a	6d	17	fd	04		
dd	2d	22	02	0d	0d	43	77	83	84	d2	48	87	84	b4			Y-"OY Cwf..OH
84	20	d2	48	09	22	22	25	a1	84	02	d2	1d	52	d2	20		OH " "i. O RO
dd	25	dd	79	47	d9	df	77	f7	3e	fb	ec	7b	f6	d9	7a		YyGÜBw+>ü1{ÖÜz
ef	be	e7	fb	e6	cf	6f	0d	8b	77	0d	6b	ad	e7	59	ef		YçÜaIo w k-cYI
cc	33	ff	f5	be	23	c9	26	ce	c7	c6	ce	26	ce	c6	0e		I3yö#É&IÇE&IE
e1	e2	92	e2	e7	61	67	63	97	66	63	e3	e6	d5	10	57		aa' açagc-fcãã W
95	d1	92	23	fb	43	d8	ae	61	07	00	00	40	20	10	80		N' #ÜC@a e
04	7d	00	c2	41	57	a0	bf	c0	00	38	00	00	04	06	82		} AAW zÀ 8
81	08	00	54	38	20	00	ba	06	82	3e	8d	12	fa	27	22		T8 e , > d."
00	93	9d	9f	83	85	9d	87	8f	85	9d	85	9d	0d	ba	1f		" Yf... † e
68	13	21	80	f9	3f	34	fe	9f	81	fe	03	36	00	c8	09		h ! ù74pY p 6 È
7d	c0	01	c0	f1	b2	b1	93	41	7f	e3	fe	b2	86	0b	40)Ä Äñ²¹" A äp²† e
02	90	b9	5b	db	7b	38	ba	dc	73	34	56	d6	50	35	66		¹[Ü{8eÜs4VÖP5f
63	fb	fd	0e	90	00	08	00	ff	eb	08	8d	d5	b4	20	5a		cüy ye Ö' Z
03	05	03	05	00	fa	10	c0	df	01	02	90	0d	80	04	3d		ú àB =
0b	45	49	65	29	55	e8	fa	0d	68	db	0d	20	36	00	41		EIe)Uèú hÜ 6 A
42	52	4b	03	a2	0e	c4	06	e2	01	c0	d0	14	03	f1	80		BRK ç Ä ä ÄÐ ñ
f8	00	20	04	fa	80	fc	8f	6d	00	64	20	d7	f5	36	2e		e ú ü m d ×Ö6.
f8	6f	39	87	07	c2	43	53	0c	5d	50	7f	c9	03	2a	10		eo9‡ ACS J P É *
04	20	90	52	35	56	d5	d2	34	96	54	94	83	28	6b	1a		R5VÖ04-T" f(k



Complex Messages

- Contain the same structures as simple messages...
- ... But include XML structure:
 - <SVARS>
- Include compressed streams:
 - PARAMS
 - RFC_QUEUE
 - VERBS



Complex Messages

- Contain messages

- ... But it

– <SVARS>

- Include compressed streams:

– PARAMS

– RFC_QUEUE

– VERBS

```
00 00 03 05 03 06 00 00 03 06 02 13 00 09 04 00 0a 00 20 00 0a 00 01 02 13 03 01 00 05 56 45 52 42 53 03 01 03 02 00 08 00 00 00 35 00 00 00 9c BS 5 VER
03 02 03 00 00 fa 7b 02 7c ea 00 00 03 76 4c 20 00 00 12 1f 9d 02 d2 8e b9 ed a8 0d 03 61 f8 55
f2 08 b1 03 01 2e 39 2c 2c 2a 7b 10 14 f5 da c4 0  t .9,,*{  oÜÄ
2e 9b 6e e2 20 27 a1 bb 6f 5f e7 28 3b 40 0e 83 ., nã 'i»o_ç(;ë f
44 57 b4 ff 0d 48 99 4f b6 ff 99 b1 9d 18 46 26 DW`ý H™D1y™t F&
64 4c 05 23 11 7b d9 fd 62 4e 64 d4 6a 5a fc e9 dL # {ÛybNdÔjzÜé
e5 d0 34 e0 91 08 3c 35 e6 44 0a b4 61 d1 ab 08 åÐ4â' <5æD `aÑ«
0e 4c 44 9f 6a c4 19 29 d0 ca e5 ef c9 38 c4 e5 LDÿjÄ )ÐÊâYÉ8Äâ
4c a8 31 27 ba 76 24 10 b4 66 7b 37 8c 98 98 12 L"1'ev$ `f{7CE`
```



Complex Messages

- Contain the same structures as simple messages...
- ... But include XML structure:
 - <SVARS>
- Include compressed streams:
 - PARAMS
 - RFC_QUEUE
 - VERBS
 - VARS



Complex Messages

- Contain message
- ... But in
 - <SVAR
- Include
 - PARAM
 - RFC_C
 - VERBS
 - VARS

06	06	03	00	01	00	ff	01	00	28	02	13	03	01	00	04	ÿ	(
56	41	52	53	03	01	03	02	00	08	00	00	01	51	00	00	VARS	Q
01	0d	03	02	03	05	00	fa	7b	02	7c	ea	00	00	06	fa	ú{	è ø
1d	62	01	00	12	1f	9d	02	af	7d	3b	ec	4d	22	8b	e2	b	};iM"<ã
30	fe	55	fa	05	4a	07	19	28	b8	c9	66	33	2d	d3	4a	0pUú	J‡ (,Éf3-ÓJ
44	60	81	ba	ea	9b	06	eb	c4	25	a9	85	50	34	bb	d9	D`	œè, èA%0..P4«Û
ec	77	5f	34	3a	e7	da	43	dc	b9	f4	2f	6f	7c	7e	c9	lw_4:	çÚCÜ¹ò/o -É
aa	c9	41	5f	3c	7b	87	99	7b	0b	47	47	df	97	7c	35	èÉA_<{‡™	GGB- 5
4a	8f	fd	14	d1	aa	a0	47	ff	74	b3	d3	76	37	69	b5	J	ÿ Ñè Gÿt³Óv7iµ
8f	4f	db	9d	e6	71	96	66	e9	71	27	e9	6e	7f	79	d2	OÛ	æq-féq'én yO
e9	76	5b	a7	db	5f	4f	bb	ff	fa	7f	01	df	b0	a0	cd	év[šÛ	O«ÿú B° Í
24	cb	fc	1c	0f	5c	4f	8a	e9	d5	60	e6	07	5f	54	41	šËü	\OšÉO`æ TA
47	7e	f6	13	69	ca	de	ef	c2	15	da	f4	63	c4	b2	a0	G-ö	iÊPIÂ ÚòcÃ²
d3	7c	7c	79	d5	6f	9c	8f	86	b3	bc	3f	2c	26	e7	b3	Ó	yOœ †³¼?,&ç³
c9	a0	41	e3	58	c1	0a	cd	5a	69	b3	d3	49	bb	89	7b	É	AÄXÁ Ízi³ÓI«%o{
11	ea	0b	82	26	6e	08	af	f6	4d	c9	4d	b0	97	70	85	è	&n`ÖMEM°-p..
f2	86	29	60	41	d3	56	e2	a6	88	66	41	13	37	c3	1e	ò†)	`AÓVã!`fa 7A
2c	28	97	bc	84	05	ed	3f	cf	2f	8b	eb	ea	31	d4	bf	,	(-¼„ í?Í/<èè1O¿
14	75	03	05	03	05	00	fa	b0	42	c5	2c	68	fa	24	71	u	ú°BÅ,húšg
53	44	0b	56	a8	1f	22	5e	10	94	4b	5e	c1	82	b6	d3	SD	v" " ^ "K^Å, 1O
c4	4d	11	cd	82	72	97	97	b0	a0	5c	f2	12	41	50	2e	ÄM	Í, r—° \ò AP.
79	05	56	a8	98	05	cd	b6	ff	e1	d1	c2	15	9a	fa	31	y	v" Í†ÿãÑÄ š ú1
62	59	d0	9b	e5	fb	c6	fd	7c	d5	58	dd	ce	37	8b	bb	bYD,	âUËÿ ÖXÝÍ7<«
c6	4d	b9	69	5c	7e	58	4c	57	b7	8b	cd	a6	5c	4f	ff	EM¹i\	-XLW·< Í \Oÿ
2c	6f	6f	fd	5f	c7	43	c1	0a	e5	67	4a	0a	41	50	6e	,	ooÿ_çCÁ ägJ APn
4a	75	f0	33	a5	03	0b	57	28	37	25	01	0b	9a	76	12	Juð3ÿ	W(7% š v
37	45	34	0b	9a	b8	19	f6	60	41	b9	e4	25	82	a0	5c	7E4	š ð`A¹äš, \
f2	0a	16	34	71	33	ec	21	58	a1	5c	f2	0a	16	94	c3	ò	4q3i!XI\ò "Ä
11	09	0b	9a	b8	19	f6	60	41	b9	e4	25	82	a0	9c	d8	š	ð`A¹äš, œø
2b	58	d0	c4	cd	b0	87	60	85	72	c9	2b	84	41	dd	10	+XDÄI°	‡`..rÉ+„ AY



PARAMS, VARS and VERBS

- Work in conjunction
- Define actions to be performed on / by objects on the GUI / Server
- Lists of “indexed data” are decompressed and parsed by ABAP to various fixed-length data structures



PARAMS, VARS and VERBS

- Parsed by ABAP into structured variables
- CASE ABAP PARAM-TYP.
 - WHEN 'S':
 - Set Value Of
 - WHEN 'G':
 - Get Value Of
 - WHEN 'C':
 - Call Method Of
- Thoughts of eval() spring to mind... 😊



PARAMS, VARS and VERBS

- Graphic example:

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 159 Bytes			
0.:	20	20	20	20	20	20	20	20	31	20	43	72	65	61	74	65	1 Create			
1.:	4f	62	6a	65	63	74	20	20	20	20	20	20	20	20	20	20	Object			
2.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
3.:	8th VARS element													20	35	20	43	C	5 C	
4.:														20	20	20	20	reateObject		
5.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
6.:	20	20	20	20	20	20	20	20	20	43	20	20	20	20	20	20	C			
7.:	20	20	38	20	53	68	65	6c	6c	45	78	65	63	75	74	65	8 ShellExecute			
8.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
9.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	43		C			



PARAMS, VARS and VERBS

- Graphic example:

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 159 Bytes
0.:	20	20	20	20	20	20	20	20	31	20	43	72	65	61	74	65	1 Create
1.:	4f	62	6a	65	63	74	20	20	20	20	20	20	20	20	20	20	Object
2.:																	
3.:	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 159 Bytes
4.:	20	20	20	20	20	20	20	20	31	20	43	72	65	61	74	65	1 Create
5.:	4f	62	6a	65	63	74	20	20	20	20	20	20	20	20	20	20	Object
6.:																	
7.:																	
8.:	72	65	61	74	65	4f	62	6a	65	63	74	20	20	20	20	20	Object
9.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
0.:	20	20	20	20	20	20	20	20	20	43	20	20	20	20	20	20	
1.:	20	20	38	20	53	68	65	6c	6c	45	78	65	63	75	74	65	8 ShellExecute
2.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
3.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
4.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
5.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
6.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
7.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
8.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
9.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	43	C



PARAMS, VARS and VERBS

- Graphic example:

```
0. .0 .1 .2 .3 .4 .5 .6 .7 .8 .9 .a .b .c .d .e .f Length: 159 Bytes
0.: 20 20 20 20 20 20 20 20 31 20 43 72 65 61 74 65 1 Create
1.: 4f 62 6a 65 63 74 20 20 20 20 20 20 20 20 20 20 20 Object
2.
3. .0 .1 .2 .3 .4 .5 .6 .7 .8 .9 .a .b .c .d .e .f Length: 159 Bytes
4.: 20 20 20 20 20 20 20 20 31 20 43 72 65 61 74 65 1 Create
5.: 4f 62 6a 65 63 74 20 20 20 20 20 20 20 20 20 20 20 Object
6.
7. .0 .1 .2 .3 .4 .5 .6 .7 .8 .9 .a .b .c .d .e .f Length: 159 Bytes
8.: 20 20 20 20 20 20 20 20 31 20 43 72 65 61 74 65 1 Create
9.: 4f 62 6a 65 63 74 20 20 20 20 20 20 20 20 20 20 20 Object
0ba.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0bb.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0bc.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0bd.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0be.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0bf.: 20 20 20 20 20 20 20 20 20 20 30 30 30 30 30 30 30 0000000
0c0.: 30 30 20 63 3a 5c 77 69 6e 64 6f 77 73 5c 73 79 00 c:\windows\sy
0c1.: 73 74 65 6d 33 32 5c 63 6d 64 2e 65 78 65 20 20 stem32\cmd.exe
0c2.
0c3.
0c4.
0c5.
0c6.
0c7.
0c8.
0c9.
```

8th element in VARS structure provides the argument...



PARAMS, VARS and VERBS

- Details on these structures can be found in ABAP code...
- Refer to ABAP Structures && where used:
 - OLE_PA
 - OLE_VERBS
 - SWCBCONT



RFC_QUEUE

- Contains META and internal table data in use by the current application / screen
- Only ever seems to appear in SAP responses
 - This assumption may be incorrect



RFC_QUEUE

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 46,757 Bytes
000.:	43	30	41	38	30	31	30	41	30	39	30	30	34	44	39	36	0A8010A09004D96
001.:	32	32	31	43	30	30	32	46	53	41	50	47	55	49	20	20	221C002FSAPGUI
002.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
003.:	20	20	20	20	20	20	20	20	30	30	30	30	30	30	30	31	00000001
004.:	00	00	00	01	01	01	00	08	01	01	01	01	04	01	01	00	
005.:	01	01	01	03	00	04	00	00	02	03	01	03	01	06	00	0b	
006.:	04	01	00	03	01	03	02	00	00	00	23	01	06	00	07	00	#
007.:	0f	31	39	32	2e	31	36	38	2e	31	2e	31	30	20	20	20	192.168.1.10
008.:	00	07	00	18	00	2d	31	39	32	2e	31	36	38	2e	31	2e	-192.168.1.
009.:	31	30	20	20	20	20	20	20	20	20	20	20	20	20	20	20	10
00a.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
00b.:	20	20	20	00	18	00	11	00	01	33	00	11	00	12	00	04	3
00c.:	37	30	31	20	00	12	00	13	00	04	37	30	31	20	00	13	701 701
00d.:	00	08	00	20	77	69	6e	78	70	73	61	70	5f	4e	53	50	winxpsap_NSP
00e.:	5f	30	30	20	20	20	20	20	20	20	20	20	20	20	20	20	_00
00f.:	20	20	20	20	00	08	00	06	00	80	53	41	50	47	55	49	SAPGUI
010.:	5f	51	55	45	55	45	45	45	45	0d	09	00	00	d3	7f	7e	_QUEUEEEEE Ó ~
011.:	4b	4e	3a	11	7f	1d	0b	b0	4c	43	4e	44	50	4e	3a	11	KN: °LCNDPN:
012.:	17	d3	7f	7e	17	01	11	00	06	42	43	55	53	45	52	01	Ó ~ BCUSER
013.:	11	01	14	00	03	0b	ca	d6	01	14	01	15	00	01	45	01	ÊÖ E
014.:	15	00	09	00	06	42	43	55	53	45	52	00	09	01	34	00	BCUSER 4
015.:	03	0b	ca	d6	01	34	05	a8	58	15	94	05	01	05	05	65	ÊÖ 4 "X " e
016.:	eb	05	05	65	0b	06	00	0b	04	01	00	03	0b	01	02	00	ë e
017.:	16	44	50	5f	50	55	54	5f	43	4c	49	45	4e	54	5f	54	DP_PUT_CLIENT T
018.:	41	42	4c	45	34	35	41	01	02	03	37	00	00	03	37	01	ABLE45A 7 7
019.:	25	00	20	31	32	39	33	35	43	45	30	35	44	46	42	46	% 12935CE05DFBF
01a.:	31	46	39	41	34	46	4f	09	0b	ca	43	32	39	44	45	38	1F9A4FO ÊC29DE8
01b.:	34	41	33	01	25	01	31	00	b9	2a	54	48	2a	02	00	b9	4A3 % 1 1*TH* 1



The Fundamentals

- ~~Understand the compression~~
- ~~Understand the compressed protocol~~
 - ~~Simplify the sniffing and decompression~~
- ~~Recompression~~
- ~~Understand the application protocol~~
 - ~~What makes SAP Gui tick ?~~
- Identify SAP attack vectors not previously considered...



SAPProx

The screenshot displays the SAP Prox application window. On the left, a log shows various messages between GUI and SRV components. The main area is titled 'SAP Connections & Messages' and contains a 'Decompressed' view of a message. The message is a 'Complete Message' with a length of 18,188 bytes. The hex dump shows the following data:

Offset	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Text
000	10	06	11	00	20	ff	7f	fe	2d	d8	b7	37	d6	74	08	7e	ÿ p-ø·7ot ~
001	13	05	97	15	97	eb	f2	2f	8d	03	20	0e	00	00	00	00	--ëo/
002	00	00	00	00	00	10	06	23	00	0f	00	00	10	0e	01	34	#
003	31	31	30	00	55	54	46	38	00	10	06	27	00	20	00	00	110 UTF8
004	10	07	02	34	31	30	33	00	55	6e	69	63	6f	64	65	4c	4103 UnicodeL
005	69	74	74	6c	65	55	6e	6d	61	72	6b	65	64	00	10	06	ittleUnmarked
006	21	00	20	44	32	38	44	35	43	45	30	30	45	38	34	46	! D28D5CE00E84F
007	31	33	38	41	34	46	45	30	30	30	43	32	39	44	45	38	138A4FE000C29DE8
008	34	41	33	10	06	02	00	03	4e	53	50	10	06	03	00	08	4A3 NSP
009	77	69	6e	78	70	73	61	70	10	06	19	00	02	00	1e	10	winxpsap
00a	06	01	00	02	00	00	10	06	0a	00	02	00	00	10	06	1f	
00b	00	12	01	d9	8d	5c	e0	72	06	f1	e4	a4	fe	00	0c	29	Û \är nãp)
00c	de	84	a3	01	10	06	25	00	0a	54	52	41	44	45	53	48	P_e % TRADESH
00d	4f	57	00	10	08	00	46	33	01	01	00	08	01	01	01	01	OW F3
00e	04	01	01	00	01	01	01	03	00	04	00	00	02	0b	01	03	
00f	01	06	00	0b	04	01	00	03	01	03	02	00	00	00	23	01	#
010	06	00	15	00	04	04	01	01	00	00	15	00	07	00	0f	31	1
011	39	32	2e	31	36	38	2e	31	2e	31	30	20	20	20	00	07	92.168.1.10
012	00	18	00	2d	31	39	32	2e	31	36	38	2e	31	2e	31	30	-192.168.1.10
013	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
014	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
015	20	00	18	00	11	00	01	33	00	11	00	12	00	04	37	30	3 70
016	31	20	00	12	00	13	00	04	37	30	31	20	00	13	00	08	1 701
017	00	20	77	69	6e	78	70	73	61	70	5f	4e	53	50	5f	30	winxpsap_NSP_0
018	30	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	0
019	20	20	00	08	00	06	00	80	53	41	50	47	55	49	00	00	SAPGUI
01a	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01b	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01c	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01d	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01e	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01f	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
021	00	00	00	00	00	00	00	00	06	01	30	00	08	53	41		0 SA
022	50	4c	4f	4c	45	41	01	30	00	17	00	00	17	05	02		PLOLEA 0
023	00	00	05	02	00	0b	00	04	37	30	31	20	00	0b	01	02	701
024	00	0e	4f	4c	45	5f	46	4c	55	53	48	5f	43	41	4c	4c	OLE_FLUSH_CALL
025	01	02	03	37	00	00	03	37	05	03	00	00	05	03	05	12	7 7
026	00	00	05	12	02	05	00	0f	45	58	43	45	50	54	5f	44	EXCEPT_D
027	45	53	43	52	49	50	54	02	05	02	05	00	0a	45	58	50	ESCRIP EXP
028	4f	52	54	5f	58	4d	4c	02	05	02	05	00	05	53	56	41	ORT_XML SVA



SAPProx



C++



- SapCompress
 - JNI interface
 - Implements MaxDB functions for decompression && compression
 - `int[] doDecompress(int[])`
 - `Int[] doCompress(int[])`

SAPProx

C++



- SAPProx
 - Java
 - Responsible for:
 - Parsing packet data
 - Decompressing messages
 - Interception
 - Compressing modified messages
 - Queue management

Demo: SAPProx

The screenshot displays the SAP Proxy application interface. On the left, a log window shows a series of messages between GUI and SRV components, including connection counts and byte sizes. The main window is titled 'SAP Connections & Messages' and contains a 'Decompressed' tab. Below this, a 'Complete Message' section shows a hex dump of network data. The hex dump is organized into columns labeled .0 through .f, with corresponding ASCII characters on the right. The message length is indicated as 18,188 bytes. The hex dump shows various control characters and data fields, including 'winxpsap', 'TRADESH', 'SAPGUI', and 'OLE_FLUSH_CALL'.

SAP Proxy

SAP Connections & Messages Configuration & Control Log

Decompressed Compressed

Complete Message PARAMS RFC_QUEUE VERBS VARS

Length: 18,188 Bytes

```
000.: 10 06 11 00 20 ff 7f fe 2d d8 b7 37 d6 74 08 7e  y p-ø·7ot ~
001.: 13 05 97 15 97 eb f2 2f 8d 03 20 0e 00 00 00 00  --ëø/
002.: 00 00 00 00 00 10 06 23 00 0f 00 00 10 0e 01 34  #
003.: 31 31 30 00 55 54 46 38 00 10 06 27 00 20 00 00  110 UTF8
004.: 10 07 02 34 31 30 33 00 55 6e 69 63 6f 64 65 4c  4103 UnicodeL
005.: 69 74 74 6c 65 55 6e 6d 61 72 6b 65 64 00 10 06  ittleUnmarked
006.: 21 00 20 44 32 38 44 35 43 45 30 30 45 38 34 46  ! D28D5CE00E84F
007.: 31 33 38 41 34 46 45 30 30 30 43 32 39 44 45 38  138A4FE000C29DE8
008.: 34 41 33 10 06 02 00 03 4e 53 50 10 06 03 00 08  4A3 NSP
009.: 77 69 6e 78 70 73 61 70 10 06 19 00 02 00 1e 10  winxpsap
00a.: 06 01 00 02 00 00 10 06 0a 00 02 00 00 10 06 1f  ù \är nãp )
00b.: 00 12 01 d9 8d 5c e0 72 06 f1 e4 a4 fe 00 0c 29  P_e % TRADESH
00c.: de 84 a3 01 10 06 25 00 0a 54 52 41 44 45 53 48  OW F3
00d.: 4f 57 00 10 08 00 46 33 01 01 00 08 01 01 01 01  #
00e.: 04 01 01 00 01 01 01 03 00 04 00 00 02 0b 01 03  1
00f.: 01 06 00 0b 04 01 00 03 01 03 02 00 00 00 23 01  92.168.1.10
010.: 06 00 15 00 04 04 01 01 00 00 15 00 07 00 0f 31  -192.168.1.10
011.: 39 32 2e 31 36 38 2e 31 2e 31 30 20 20 20 00 07  3 70
012.: 00 18 00 2d 31 39 32 2e 31 36 38 2e 31 2e 31 30  1 701
013.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  winxpsap_NSP_0
014.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  0
015.: 20 00 18 00 11 00 01 33 00 11 00 12 00 04 37 30  SAPGUI
016.: 31 20 00 12 00 13 00 04 37 30 31 20 00 13 00 08  1 701
017.: 00 20 77 69 6e 78 70 73 61 70 5f 4e 53 50 5f 30  0
018.: 30 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  SAPGUI
019.: 20 20 00 08 00 06 00 80 53 41 50 47 55 49 00 00  0
01a.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
01b.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
01c.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
01d.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
01e.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
01f.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
020.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
021.: 00 00 00 00 00 00 00 00 00 06 01 30 00 08 53 41  0 SA
022.: 50 4c 4f 4c 45 41 01 30 00 17 00 00 17 05 02  PLOLEA 0
023.: 00 00 05 02 00 0b 00 04 37 30 31 20 00 0b 01 02  701
024.: 00 0e 4f 4c 45 5f 46 4c 55 53 48 5f 43 41 4c 4c  OLE_FLUSH_CALL
025.: 01 02 03 37 00 00 03 37 05 03 00 00 05 03 05 12  7 7
026.: 00 00 05 12 02 05 00 0f 45 58 43 45 50 54 5f 44  EXCEPT_D
027.: 45 53 43 52 49 50 54 02 05 02 05 00 0a 45 58 50  ESCRIPT EXP
028.: 4f 52 54 5f 58 4d 4c 02 05 02 05 00 05 53 56 41  ORT_XML SWA
```



Attack API

- Users can write their own exploits
- In a scripting language of their choice...
 - Jython
 - Groovy
 - Jruby
 - *
- Script locations specified in configuration
- Allow for canned exploits
- (thanks Willem Mouton)



Demo: Attacks / Scripting

```
print "START : COMMAND EXEC SCRIPT"  
# The saved packet  
b = [16, 6, 17, 0, 32, 255, 127, 254, 45, 2  
0, 0, 0, 16, 6, 35, 0, 15, 0, 0, 16, 14, 1,  
105, 99, 111, 100, 101, 76, 105, 116, 116,  
56, 57, 48, 54, 70, 49, 56, 49, 65, 52, 70,  
119, 105, 110, 120, 112, 115, 97, 112, 16,  
224, 139, 63, 241, 32, 164, 252, 0, 12, 41,  
126, 92, 224, 140, 114, 241, 34, 164, 252,  
2, 0, 200, 16, 6, 7, 0, 20, 83, 69, 56, 48,  
0, 0, 0, 49, 255, 16, 12, 7, 0, 16, 0, 0, 0,  
12, 66, 67, 85, 83, 69, 82, 32, 32, 32, 32,  
32, 78, 83, 80, 32, 32, 32, 32, 32, 16, 6,  
32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32,  
32, 32, 32, 32, 32, 32, 32, 16, 6, 13, 0, 4,  
32, 32, 32, 32, 32, 32, 32, 32, 32, 32, 32,  
55, 0, 0, 16, 6, 39, 0, 32, 0, 0, 16, 7, 2,  
114, 107, 101, 100, 0, 16, 2, 5, 0, 223, 4,  
print " + SET Message:1"  
c = api.getStringInput("C:\PATH\COMMAND")  
print " + GET Command : " + c
```



What we're going to talk about

- ~~Why this Talk ?~~
- ~~The history of decompressing SAP DIAG~~
- ~~Understanding the fundamentals~~
- New Attacks
- Conclusion



New (Old) Attacks ?

- We now have a proxy for SAP GUI
 - WebScarab for SAP
- For what I believe is the first time, we get an unprecedented view into SAP GUI applications...
- ... and we know where that left us with web applications ...



New (Old) Attacks ?

- Authorisation
- Authentication



Demo: Auth*

SAP Proxy

SAP Connections & Messages Configuration & Control Log

Decompressed Compressed

Complete Message PARAMS RFC_QUEUE VERBS VARS

Length: 18,188 Bytes

```

GUI->SRV: CMP:266 bytes:DEC:30 bytes
SRV->GUI: CMP:3372 bytes:DEC:9322 bytes
GUI->SRV: CMP:360 bytes:DEC:499 bytes
SRV->GUI: CMP:239 bytes:DEC:251 bytes
SRV->GUI: CMP:226 bytes:DEC:234 bytes
SRV->GUI: CMP:513 bytes:DEC:947 bytes
SRV->GUI: CMP:460 bytes:DEC:756 bytes
SRV->GUI: CMP:16807 bytes:DEC:18188 bytes
GUI->SRV: CMP:1263 bytes:DEC:2045 bytes
SRV->GUI: CMP:3675 bytes:DEC:8695 bytes
    
```

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	
000.:	10	06	11	00	20	ff	7f	fe	2d	d8	b7	37	d6	74	08	7e	ÿ p-ø·7ot ~
001.:	13	05	97	15	97	eb	f2	2f	8d	03	20	0e	00	00	00	00	--ëo/
002.:	00	00	00	00	00	10	06	23	00	0f	00	00	10	0e	01	34	#
003.:	31	31	30	00	55	54	46	38	00	10	06	27	00	20	00	00	110 UTF8
004.:	10	07	02	34	31	30	33	00	55	6e	69	63	6f	64	65	4c	4103 UnicodeL
005.:	69	74	74	6c	65	55	6e	6d	61	72	6b	65	64	00	10	06	ittleUnmarked
006.:	21	00	20	44	32	38	44	35	43	45	30	30	45	38	34	46	! D28D5CE00E84F
007.:	31	33	38	41	34	46	45	30	30	30	43	32	39	44	45	38	138A4FE000C29DE8
008.:	34	41	33	10	06	02	00	03	4e	53	50	10	06	03	00	08	4A3 NSP
009.:	77	69	6e	78	70	73	61	70	10	06	19	00	02	00	1e	10	winxpsap
00a.:	06	01	00	02	00	00	10	06	0a	00	02	00	00	10	06	1f	
00b.:	00	12	01	d9	8d	5c	e0	72	06	f1	e4	a4	fe	00	0c	29	Û \är nãp)
00c.:	de	84	a3	01	10	06	25	00	0a	54	52	41	44	45	53	48	P_e % TRADESH
00d.:	4f	57	00	10	08	00	46	33	01	01	00	08	01	01	01	01	OW F3
00e.:	04	01	01	00	01	01	01	03	00	04	00	00	02	0b	01	03	
00f.:	01	06	00	0b	04	01	00	03	01	03	02	00	00	00	23	01	#
010.:	06	00	15	00	04	04	01	01	00	00	15	00	07	00	0f	31	1
011.:	39	32	2e	31	36	38	2e	31	2e	31	30	20	20	20	00	07	92.168.1.10
012.:	00	18	00	2d	31	39	32	2e	31	36	38	2e	31	2e	31	30	-192.168.1.10
013.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
014.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
015.:	20	00	18	00	11	00	01	33	00	11	00	12	00	04	37	30	3 70
016.:	31	20	00	12	00	13	00	04	37	30	31	20	00	13	00	08	1 701
017.:	00	20	77	69	6e	78	70	73	61	70	5f	4e	53	50	5f	30	winxpsap_NSP_0
018.:	30	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	0
019.:	20	20	00	08	00	06	00	80	53	41	50	47	55	49	00	00	SAPGUI
01a.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01b.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01c.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01d.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01e.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01f.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
020.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
021.:	00	00	00	00	00	00	00	00	06	01	30	00	08	53	41		0 SA
022.:	50	4c	4f	4c	45	41	01	30	00	17	00	00	17	05	02		PLOLEA 0
023.:	00	00	05	02	00	0b	00	04	37	30	31	20	00	0b	01	02	701
024.:	00	0e	4f	4c	45	5f	46	4c	55	53	48	5f	43	41	4c	4c	OLE_FLUSH_CALL
025.:	01	02	03	37	00	00	03	37	05	03	00	00	05	03	05	12	7 7
026.:	00	00	05	12	02	05	00	0f	45	58	43	45	50	54	5f	44	EXCEPT_D
027.:	45	53	43	52	49	50	54	02	05	02	05	00	0a	45	58	50	ESCRIP EXP
028.:	4f	52	54	5f	58	4d	4c	02	05	02	05	00	05	53	56	41	ORT_XML SVA



New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic



Demo: State & Business Logic

SAP Proxy

SAP Connections & Messages Configuration & Control Log

Decompressed Compressed

Complete Message PARAMS RFC_QUEUE VERBS VARS

Length: 18,188 Bytes

```
000.: 10 06 11 00 20 ff 7f fe 2d d8 b7 37 d6 74 08 7e  y p-ø·7ot ~
001.: 13 05 97 15 97 eb f2 2f 8d 03 20 0e 00 00 00 00  --ëø/
002.: 00 00 00 00 00 10 06 23 00 0f 00 00 10 0e 01 34  #
003.: 31 31 30 00 55 54 46 38 00 10 06 27 00 20 00 00  110 UTF8
004.: 10 07 02 34 31 30 33 00 55 6e 69 63 6f 64 65 4c  4103 UnicodeL
005.: 69 74 74 6c 65 55 6e 6d 61 72 6b 65 64 00 10 06  ittleUnmarked
006.: 21 00 20 44 32 38 44 35 43 45 30 30 45 38 34 46  ! D28D5CE00E84F
007.: 31 33 38 41 34 46 45 30 30 30 43 32 39 44 45 38  138A4FE000C29DE8
008.: 34 41 33 10 06 02 00 03 4e 53 50 10 06 03 00 08  4A3 NSP
009.: 77 69 6e 78 70 73 61 70 10 06 19 00 02 00 1e 10  winxpsap
00a.: 06 01 00 02 00 00 10 06 0a 00 02 00 00 10 06 1f  ù \är nãþp )
00b.: 00 12 01 d9 8d 5c e0 72 06 f1 e4 a4 fe 00 0c 29  P_e % TRADESH
00c.: de 84 a3 01 10 06 25 00 0a 54 52 41 44 45 53 48  OW F3
00d.: 4f 57 00 10 08 00 46 33 01 01 00 08 01 01 01 01  #
00e.: 04 01 01 00 01 01 01 03 00 04 00 00 02 0b 01 03  1
00f.: 01 06 00 0b 04 01 00 03 01 03 02 00 00 00 23 01  92.168.1.10
010.: 06 00 15 00 04 04 01 01 00 00 15 00 07 00 0f 31  -192.168.1.10
011.: 39 32 2e 31 36 38 2e 31 2e 31 30 20 20 20 00 07  3 70
012.: 00 18 00 2d 31 39 32 2e 31 36 38 2e 31 2e 31 30  1 701
013.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  winxpsap_NSP_0
014.: 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  0
015.: 20 00 18 00 11 00 01 33 00 11 00 12 00 04 37 30  SAPGUI
016.: 31 20 00 12 00 13 00 04 37 30 31 20 00 13 00 08  1 701
017.: 00 20 77 69 6e 78 70 73 61 70 5f 4e 53 50 5f 30  winxpsap_NSP_0
018.: 30 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20  0
019.: 20 20 00 08 00 06 00 80 53 41 50 47 55 49 00 00  SAPGUI
01a.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
01b.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
01c.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
01d.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
01e.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
01f.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
020.: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  0
021.: 00 00 00 00 00 00 00 00 00 06 01 30 00 08 53 41  0 SA
022.: 50 4c 4f 4c 45 41 01 30 00 17 00 00 17 05 02  PLOLEA 0
023.: 00 00 05 02 00 0b 00 04 37 30 31 20 00 0b 01 02  701
024.: 00 0e 4f 4c 45 5f 46 4c 55 53 48 5f 43 41 4c 4c  OLE_FLUSH_CALL
025.: 01 02 03 37 00 00 03 37 05 03 00 00 05 03 05 12  7 7
026.: 00 00 05 12 02 05 00 0f 45 58 43 45 50 54 5f 44  EXCEPT_D
027.: 45 53 43 52 49 50 54 02 05 02 05 00 0a 45 58 50  ESCRIPT EXP
028.: 4f 52 54 5f 58 4d 4c 02 05 02 05 00 05 53 56 41  ORT_XML SWA
```



New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic
- Validation



Demo: Validation

SAP Proxy

SAP Connections & Messages Configuration & Control Log

Decompressed Compressed

Complete Message PARAMS RFC_QUEUE VERBS VARS

Length: 18,188 Bytes

```

GUI->SRV: CMP:266 bytes:DEC:30 bytes
SRV->GUI: CMP:3372 bytes:DEC:9322 bytes
GUI->SRV: CMP:360 bytes:DEC:499 bytes
SRV->GUI: CMP:239 bytes:DEC:251 bytes
SRV->GUI: CMP:226 bytes:DEC:234 bytes
SRV->GUI: CMP:513 bytes:DEC:947 bytes
SRV->GUI: CMP:460 bytes:DEC:756 bytes
SRV->GUI: CMP:16807 bytes:DEC:18188 bytes
GUI->SRV: CMP:1263 bytes:DEC:2045 bytes
SRV->GUI: CMP:3675 bytes:DEC:8695 bytes
    
```

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	
000.:	10	06	11	00	20	ff	7f	fe	2d	d8	b7	37	d6	74	08	7e	ÿ p-ø·7ot ~
001.:	13	05	97	15	97	eb	f2	2f	8d	03	20	0e	00	00	00	00	--ëo/
002.:	00	00	00	00	00	10	06	23	00	0f	00	00	10	0e	01	34	#
003.:	31	31	30	00	55	54	46	38	00	10	06	27	00	20	00	00	110 UTF8
004.:	10	07	02	34	31	30	33	00	55	6e	69	63	6f	64	65	4c	4103 UnicodeL
005.:	69	74	74	6c	65	55	6e	6d	61	72	6b	65	64	00	10	06	ittleUnmarked
006.:	21	00	20	44	32	38	44	35	43	45	30	30	45	38	34	46	! D28D5CE00E84F
007.:	31	33	38	41	34	46	45	30	30	30	43	32	39	44	45	38	138A4FE000C29DE8
008.:	34	41	33	10	06	02	00	03	4e	53	50	10	06	03	00	08	4A3 NSP
009.:	77	69	6e	78	70	73	61	70	10	06	19	00	02	00	1e	10	winxpsap
00a.:	06	01	00	02	00	00	10	06	0a	00	02	00	00	10	06	1f	
00b.:	00	12	01	d9	8d	5c	e0	72	06	f1	e4	a4	fe	00	0c	29	Û \är nãp)
00c.:	de	84	a3	01	10	06	25	00	0a	54	52	41	44	45	53	48	P_e % TRADESH
00d.:	4f	57	00	10	08	00	46	33	01	01	00	08	01	01	01	01	OW F3
00e.:	04	01	01	00	01	01	01	03	00	04	00	00	02	0b	01	03	
00f.:	01	06	00	0b	04	01	00	03	01	03	02	00	00	00	23	01	#
010.:	06	00	15	00	04	04	01	01	00	00	15	00	07	00	0f	31	1
011.:	39	32	2e	31	36	38	2e	31	2e	31	30	20	20	20	00	07	92.168.1.10
012.:	00	18	00	2d	31	39	32	2e	31	36	38	2e	31	2e	31	30	-192.168.1.10
013.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
014.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
015.:	20	00	18	00	11	00	01	33	00	11	00	12	00	04	37	30	3 70
016.:	31	20	00	12	00	13	00	04	37	30	31	20	00	13	00	08	1 701
017.:	00	20	77	69	6e	78	70	73	61	70	5f	4e	53	50	5f	30	winxpsap_NSP_0
018.:	30	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	0
019.:	20	20	00	08	00	06	00	80	53	41	50	47	55	49	00	00	SAPGUI
01a.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01b.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01c.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01d.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01e.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01f.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
020.:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
021.:	00	00	00	00	00	00	00	00	06	01	30	00	08	53	41		0 SA
022.:	50	4c	4f	4c	45	41	01	30	00	17	00	00	17	05	02		PLOLEA 0
023.:	00	00	05	02	00	0b	00	04	37	30	31	20	00	0b	01	02	701
024.:	00	0e	4f	4c	45	5f	46	4c	55	53	48	5f	43	41	4c	4c	OLE_FLUSH_CALL
025.:	01	02	03	37	00	00	03	37	05	03	00	00	05	03	05	12	7 7
026.:	00	00	05	12	02	05	00	0f	45	58	43	45	50	54	5f	44	EXCEPT_D
027.:	45	53	43	52	49	50	54	02	05	02	05	00	0a	45	58	50	ESCRIPIT EXP
028.:	4f	52	54	5f	58	4d	4c	02	05	02	05	00	05	53	56	41	ORT_XML SWA



New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic
- Validation
- Replay



Demo: Replay

SAP Proxy

SAP Connections & Messages Configuration & Control Log

Decompressed Compressed

Complete Message PARAMS RFC_QUEUE VERBS VARS

Length: 18,188 Bytes

```
GUI->SRV: CMP:266 bytes:DEC:30 bytes
SRV->GUI: CMP:3372 bytes:DEC:9322 bytes
GUI->SRV: CMP:360 bytes:DEC:499 bytes
SRV->GUI: CMP:239 bytes:DEC:251 bytes
SRV->GUI: CMP:226 bytes:DEC:234 bytes
SRV->GUI: CMP:513 bytes:DEC:947 bytes
SRV->GUI: CMP:460 bytes:DEC:756 bytes
SRV->GUI: CMP:16807 bytes:DEC:18188 bytes
GUI->SRV: CMP:1263 bytes:DEC:2045 bytes
SRV->GUI: CMP:3675 bytes:DEC:8695 bytes
```

Offset	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	ASCII
000	10	06	11	00	20	ff	7f	fe	2d	d8	b7	37	d6	74	08	7e	ÿþ-ø·7ot ~
001	13	05	97	15	97	eb	f2	2f	8d	03	20	0e	00	00	00	00	--ëo/
002	00	00	00	00	00	10	06	23	00	0f	00	00	10	0e	01	34	#
003	31	31	30	00	55	54	46	38	00	10	06	27	00	20	00	00	110 UTF8
004	10	07	02	34	31	30	33	00	55	6e	69	63	6f	64	65	4c	4103 UnicodeL
005	69	74	74	6c	65	55	6e	6d	61	72	6b	65	64	00	10	06	ittleUnmarked
006	21	00	20	44	32	38	44	35	43	45	30	30	45	38	34	46	! D28D5CE00E84F
007	31	33	38	41	34	46	45	30	30	30	43	32	39	44	45	38	138A4FE000C29DE8
008	34	41	33	10	06	02	00	03	4e	53	50	10	06	03	00	08	4A3 NSP
009	77	69	6e	78	70	73	61	70	10	06	19	00	02	00	1e	10	winxpsap
00a	06	01	00	02	00	00	10	06	0a	00	02	00	00	10	06	1f	
00b	00	12	01	d9	8d	5c	e0	72	06	f1	e4	a4	fe	00	0c	29	Û \är nãp)
00c	de	84	a3	01	10	06	25	00	0a	54	52	41	44	45	53	48	P_e % TRADESH
00d	4f	57	00	10	08	00	46	33	01	01	00	08	01	01	01	01	OW F3
00e	04	01	01	00	01	01	01	03	00	04	00	00	02	0b	01	03	
00f	01	06	00	0b	04	01	00	03	01	03	02	00	00	00	23	01	#
010	06	00	15	00	04	04	01	01	00	00	15	00	07	00	0f	31	1
011	39	32	2e	31	36	38	2e	31	2e	31	30	20	20	20	00	07	92.168.1.10
012	00	18	00	2d	31	39	32	2e	31	36	38	2e	31	2e	31	30	-192.168.1.10
013	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
014	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
015	20	00	18	00	11	00	01	33	00	11	00	12	00	04	37	30	3 70
016	31	20	00	12	00	13	00	04	37	30	31	20	00	13	00	08	1 701
017	00	20	77	69	6e	78	70	73	61	70	5f	4e	53	50	5f	30	winxpsap_NSP_0
018	30	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	0
019	20	20	00	08	00	06	00	80	53	41	50	47	55	49	00	00	SAPGUI
01a	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01b	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01c	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01d	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01e	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
01f	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
021	00	00	00	00	00	00	00	00	06	01	30	00	08	53	41		0 SA
022	50	4c	4f	4c	45	41	01	30	00	17	00	00	17	05	02		PLOLEA 0
023	00	00	05	02	00	0b	00	04	37	30	31	20	00	0b	01	02	701
024	00	0e	4f	4c	45	5f	46	4c	55	53	48	5f	43	41	4c	4c	OLE_FLUSH_CALL
025	01	02	03	37	00	00	03	37	05	03	00	00	05	03	05	12	7 7
026	00	00	05	12	02	05	00	0f	45	58	43	45	50	54	5f	44	EXCEPT_D
027	45	53	43	52	49	50	54	02	05	02	05	00	0a	45	58	50	ESCRIP EXP
028	4f	52	54	5f	58	4d	4c	02	05	02	05	00	05	53	56	41	ORT_XML SVA



New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic
- Validation
- Replay
- Client-Side attacks



Client-Side Attacks

- Many business cases require the execution of applications on the client.
 - Provided for by ABAP
- Deprecated: GUI_RUN or WS_EXECUTE
- Current: cl_gui_frontend_services
- Newer clients still support old methods
 - Backwards compatibility
 - Do prompt when applications execute
- (thanks Steve Lord)



Client-Side Attacks

- WS_EXECUTE / GUI_RUN



Client-Side Attacks

	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 1,037 Bytes
1b.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	10	(SAPLGRAP
1c.:	06	0d	00	28	53	41	50	4c	47	52	41	50	20	20	20	20	
1d.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
1e.:	20	20	20	20	20	20	20	20	20	20	20	10	06	0e	00	00	
1f.:	04	30	31	30	30	10	06	23	00	0b	00	00	04	67	01	31	0100 # g 1
20.:	31	32	37	00	00	10	06	27	00	20	00	00	10	07	02	34	127 ' 4
21.:	31	30	33	00	55	6e	69	63	6f	64	65	4c	69	74	74	6c	103 UnicodeLittl
22.:	65	55	6e	6d	61	72	6b	65	64	00	10	02	05	00	df	04	eUnmarked 8
23.:	31	56	33	2e	34	00	4c	45	00	42	00	44	2c	00	50	20	1V3.4 LE B D, P
24.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
25.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
26.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
27.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
28.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
29.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
2a.:	20	20	20	00	58	63	3a	5c	77	69	6e	64	6f	77	73	5c	Xc:\windows\
2b.:	73	79	73	74	65	6d	33	32	5c	63	61	6c	63	2e	65	78	system32\calc.ex
2c.:	65	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	e
2d.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
2e.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
2f.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
30.:	20	20	20	20	20	20	20	20	20	00	45	00	52	00	10	06	E R
31.:	23	00	0f	00	00	10	0e	01	34	31	31	30	00	55	54	46	# 4110 UTF
32.:	38	00	10	06	27	00	20	00	00	10	07	02	34	31	30	33	8 ' 4103
33.:	00	55	6e	69	63	6f	64	65	4c	69	74	74	6c	65	55	6e	UnicodeLittleUn
34.:	6d	61	72	6b	65	64	00	10	09	0a	00	00	12	04	18	00	marked
35.:	00	00	b9	2a	54	48	2a	02	00	b9	00	00	4e	53	50	20	1*TH* 1 NSP
36.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
37.:	20	20	20	20	20	20	20	20	20	20	20	00	01	42	43	43	BC
38.:	55	53	45	52	20	20	20	20	20	20	20	20	20	20	20	20	USER
39.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	53	45	SE
3a.:	55	5f	49	4e	54	20	20	20	20	20	20	20	20	20	20	20	U_INT
3b.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
3c.:	20	20	20	20	20	20	00	01	4e	53	50	20	20	20	20	20	NSP
3d.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	
3e.:	20	20	20	20	20	20	20	20	44	44	37	45	35	43	45	30	DD7E5CE0
3f.:	38	43	37	32	46	31	32	33	41	34	46	43	30	30	30	43	8C72F123A4FC000C
40.:	32	39	44	45	38	34	41	33	2a	54	48	2a	0c				29DE84A3*TH*



Demo: Client-Side Attacks

The screenshot displays the SAP Proxy application interface. On the left, a log window shows a list of transactions between GUI and SRV components. The transaction `SRV->GUI: CMP:16807 bytes: DEC:18188 bytes` is highlighted in blue. The main window is titled "SAP Connections & Messages" and "Configuration & Control". It features a "Decompressed" tab and a "Compressed" tab. Below these, there are sub-tabs for "Complete Message", "PARAMS", "RFC_QUEUE", "VERBS", and "VARS". The "Complete Message" tab is active, showing a hex dump of the message data. The hex dump is organized into columns labeled .0 through .f, with a "Length: 18,188 Bytes" indicator. The corresponding ASCII representation is shown on the right side of the hex dump. The ASCII text includes "y p-ø·7ot ~", "ëö/", "#", "110 UTF8", "4103 UnicodeL", "ittleUnmarked", "! D28D5CE00E84F", "138A4FE000C29DE8", "4A3 NSP", "winxsap", "Û \är nãp)", "P_e % TRADESH", "OW F3", "#", "1", "92.168.1.10", "-192.168.1.10", "3 70", "1 701", "winxsap_NSP_0", "0", "SAPGUI", "0 SA", "PLOLEA 0", "701", "OLE_FLUSH_CALL", "7 7", "EXCEPT_D", "ESCRIP EXP", "ORT_XML SVA".



Client-Side Attacks

- cl_gui_frontend_services
 - Makes use of OLE

	Complete Message																PARAMS	RFC_QUEUE	VERBS	VARs
	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 159 Bytes			
0.:	20	20	20	20	20	20	20	20	31	20	43	72	65	61	74	65	1	Create		
1.:	4f	62	6a	65	63	74	20	20	20	20	20	20	20	20	20	20	Object			
2.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
3.:	20	20	20	20	43	20	20	20	20	20	20	20	20	35	20	43	C	5	C	
4.:	72	65	61	74	65	4f	62	6a	65	63	74	20	20	20	20	20	reateObject			
5.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
6.:	20	20	20	20	20	20	20	20	20	43	20	20	20	20	20	20	C			
7.:	20	20	38	20	53	68	65	6c	6c	45	78	65	63	75	74	65	8	ShellExecute		
8.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
9.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	43				C	



Client-Side Attacks

- cl_gui_frontend_services
 - Makes use of OLE

	Complete Message																PARAMS	RFC_QUEUE	VERBS	VARs
	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.a	.b	.c	.d	.e	.f	Length: 159 Bytes			
0.:	20	20	20	20	20	20	20	20	31	20	43	72	65	61	74	65	1	Create		
1.:	4f	62	6a	65	63	74	20	20	20	20	20	20	20	20	20	20	Object			
2.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
3.:	20	20	20	20	43	20	20	20	20	20	20	20	20	35	20	43	C	5 C		
4.:	72	65	61	74	65	4f	62	6a	65	63	74	20	20	20	20	20	reateObject			
5.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
6.:	20	20	20	20	20	20	20	20	43	20	20	20	20	20	20	20	C			
7.:	20	20	38	20	53	68	65	6c	6c	45	78	65	63	75	74	65	8	ShellExecute		
8.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
9.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
0bd.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
0be.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
0bf.:	20	20	20	20	20	20	20	20	20	20	20	30	30	30	30	30		0000000		
0c0.:	30	30	20	63	3a	5c	77	69	6e	64	6f	77	73	5c	73	79	00	c:\windows\sy		
0c1.:	73	74	65	6d	33	32	5c	63	6d	64	2e	65	78	65	20	20		stem32\cmd.exe		
0c2.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				
0c3.:	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20	20				



Client-Side Attacks

- SAP GUI provides number of COM libraries with potentially exploitable functions
 - Saved by the fact that the controls are not marked “Safe for Scripting”



Client-Side Attacks

ComRaider - [124 classes found to objects registered in this path]

IDEFENSE
A VeriSign Company

LABS

View

Date	GUID	ProgID	InProcServer	Description
8.30.11	{00100000-200...	SAPGUI.Menu...	c:\program files...	SAP MenuItem Class
8.30.11	{00100000-200...	SAPGUI.Popup...	c:\program files...	SAP PopupMenu Control
8.30.11	{00100000-200...	SAPGUI.Menu...	c:\program files...	SAP MenuBar Control
8.30.11	{01DD356D-02...	Sapfewut.SapD...	c:\program files...	SapDirectories Class
8.30.11	{039899B6-4B8...	SAPGUI.TextE...	c:\program files...	SAP TextEdit Control
8.30.11	{048B665E-B0...	SAPGUI.Splitter...	c:\program files...	SplitterCtrlScripting Class
8.30.11	{056DA858-0F...	sapguifocus.Fo...	c:\program files...	SAPGUI Focus Class
8.30.11	{06A45680-190...	SAPGUI.eCAT...	c:\program files...	SAP eCATT RHConnection Class
8.30.11	{0738DC8A-82...	Sapguiservices...	c:\program files...	SAPGUIServices Class
8.30.11	{0738DC8E-82...	Sapguiservices...	c:\program files...	SAPGUICtxMnuService Class
8.30.11	{07EBD6B4-B5...		c:\program files...	SAP OLE Link Server - Binary Data Object Class
8.30.11	{0A46E62E-EF...	SAPGUI.Stagin...	c:\program files...	SapStageCtrlScripting Class
8.30.11	{0B052FD7-1A...	SAPGUIServic...	c:\program files...	SAPGUI RfcService Class
8.30.11	{0C7BF175-02...	Sapfewut.Sap...	c:\program files...	SapWorkDir Class
8.30.11	{133AD681-0D...	SAP.OfficeInte...	c:\program files...	SAP Office Integration Default Proxy Class
8.30.11	{133AD683-0D...	SAP.OfficeInte...	c:\program files...	SAP Office Integration Excel97 Proxy Class
8.30.11	{140FD071-E5...	WCRContainer...	c:\program files...	CRDPStream Class
8.30.11	{14833081-050...	SAPGUI.NetPla...	c:\program files...	SapNetzCtrlScripting Class
8.30.11	{148C6F0E-C6...	WINGUI.Draw...	c:\program files...	WINGUI DrawManagerWinTheme
8.30.11	{15D20C6F-DE...		c:\program files...	SAP DP Clipboard Converter Class
8.30.11	{18B62DCD-7A...	SAP.ToolBar.1	c:\program files...	SAPToolBar Class
8.30.11	{1CD0BD81-08...	VisCarrier.VisCo...	c:\program files...	VisCarrier.VisControl
8.30.11	{205D52D9-B0...	SAPGUI.Graphi...	c:\program files...	SapGradpCtrlScripting Class
8.30.11	{20AAC0B7-9A...	WINGUI.Resou...	c:\program files...	WINGUI ResourceManagerDefault
8.30.11	{2F1022B8-E40...	SAP.OfficeInte...	c:\program files...	SAP Office Integration PowerPoint97 Proxy Class
8.30.11	{3308645D-4E...	SAP.FormPaint...	c:\program files...	SAP FormPainter Control
8.30.11	{3399C6C4-AF...	SAP.OLELinkS...	c:\program files...	SAP OLE Link Item Class
8.30.11	{375DA2F6-41...	SAP.BorderPai...	c:\program files...	SAP BorderPainter Control
8.30.11	{3902D36D-61...	SAPQueryTabl...	c:\program files...	SAPQueryTable.QueryTable
8.30.11	{3D6E1044-9D...	Sapgui.Slider	c:\program files...	Sapgui.Slider
8.30.11	{3E91AACC-48...	SAPGUI.LSAPI.1	c:\program files...	LSAPIWrapper Class
8.30.11	{3F24D677-10...	SAP.SapTabCn.1	c:\program files...	
8.30.11	{42AB3E73-17...	SAPGUI.Image...	c:\program files...	SAP Image Control
8.30.11	{468D2820-F85...	SAP.SapTextC...	c:\program files...	
8.30.11	{4CC5F9C2-A5...	SAP.OLELinkS...	c:\program files...	SAP OLE Link Server Class
8.30.11	{4CDD0651-FE...	Sapguiservices...	c:\program files...	SAPGUIAttribute Class



Client-Side Attacks

- SAP GUI provides number of COM libraries with potentially exploitable functions
 - Saved by the fact that the controls are not marked “Safe for Scripting”
- With SAPProxy we can potentially instantiate diverse COM objects



New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic
- Validation
- Replay
- Client-Side attacks
- DoS



Demo: DoS

The screenshot shows the SAP Proxy application window. On the left, a list of connections is displayed, with one entry highlighted: `SRV->GUI: CMP:16807 bytes: DEC:18188 bytes`. The main area is divided into tabs for `SAP Connections & Messages`, `Configuration & Control`, and `Log`. The `Decompressed` tab is active, showing a hex dump of a message. The hex dump is organized into columns for bytes `.0` through `.f`, with a `Length: 18,188 Bytes` indicator. The corresponding ASCII text on the right includes headers like `winxpsap` and `SAPGUI`, and contains IP addresses `92.168.1.10` and `-192.168.1.10`, along with other identifiers like `PLOLEA 0` and `OLE_FLUSH_CALL`.



New (Old) Attacks ?

- Authorisation
- Authentication
- State Management
- Business Logic
- Validation
- Replay
- Client-Side attacks
- DoS
- *



What we're going to talk about

- ~~Why this Talk ?~~
- ~~The history of decompressing SAP DIAG~~
- ~~Understanding the fundamentals~~
- ~~New Attacks~~
- Conclusion



Conclusion

- A couple of factors have been common security knowledge for years...
 - Plain-text communication == #fail
 - Security by obscurity == #fail
- We now have a toolset and programmatic interface into SAP DIAG protocol
 - Game Changer
 - Change the way we look at ABAP
 - Happy Haxoring



Conclusion

- SAP provides encryption for client components in the form of Secure Network Communications
 - Provided by 3rd Parties
 - Provided by SAP
- SAP Clients should ensure the use of SNC is enabled and enforced



Questions ?

- www.sensepost.com/blog

ian@sensepost.com

