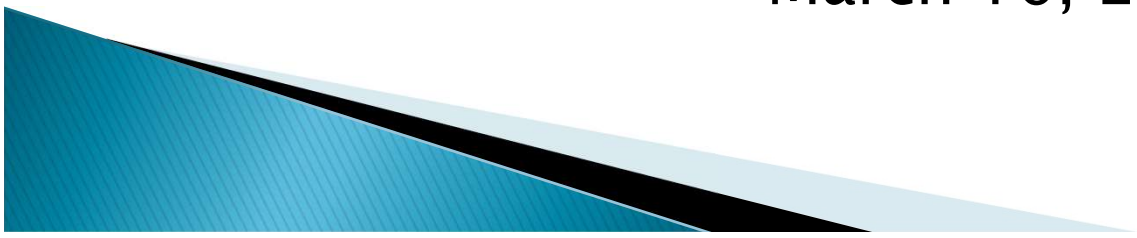
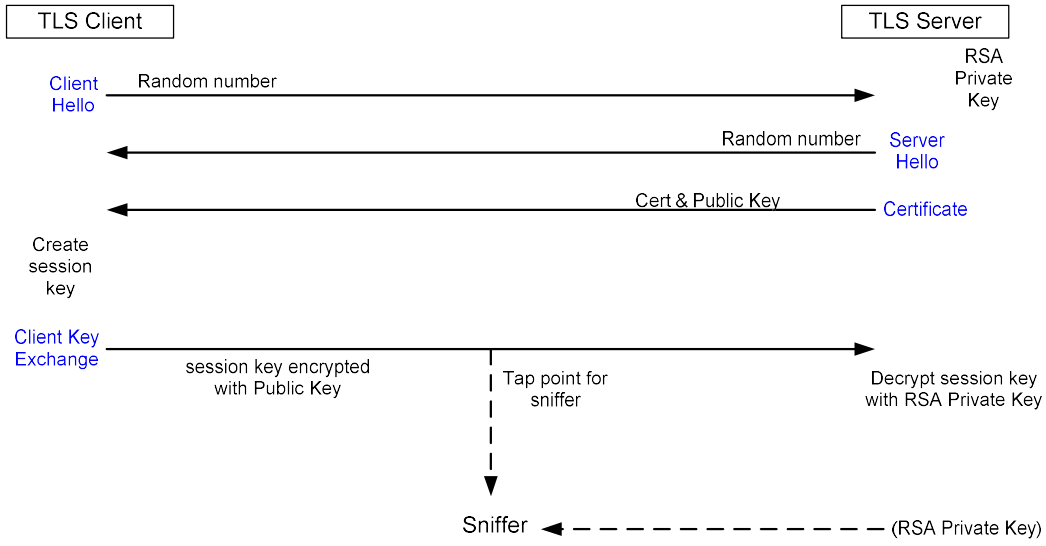
TLS Visibility *Inside* the Data Center

Steve Fenter

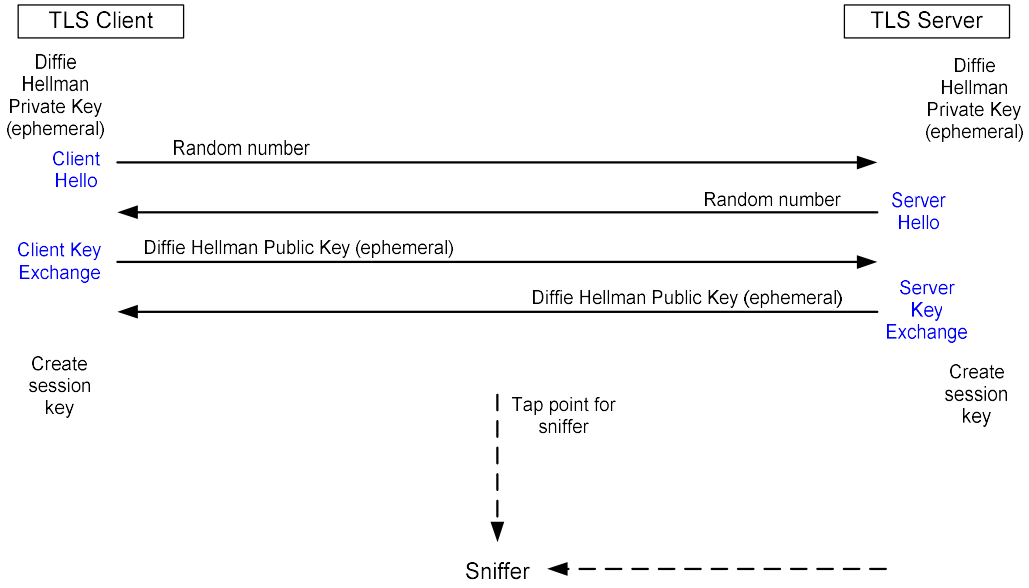
March 16, 2018



RSA Key Exchange



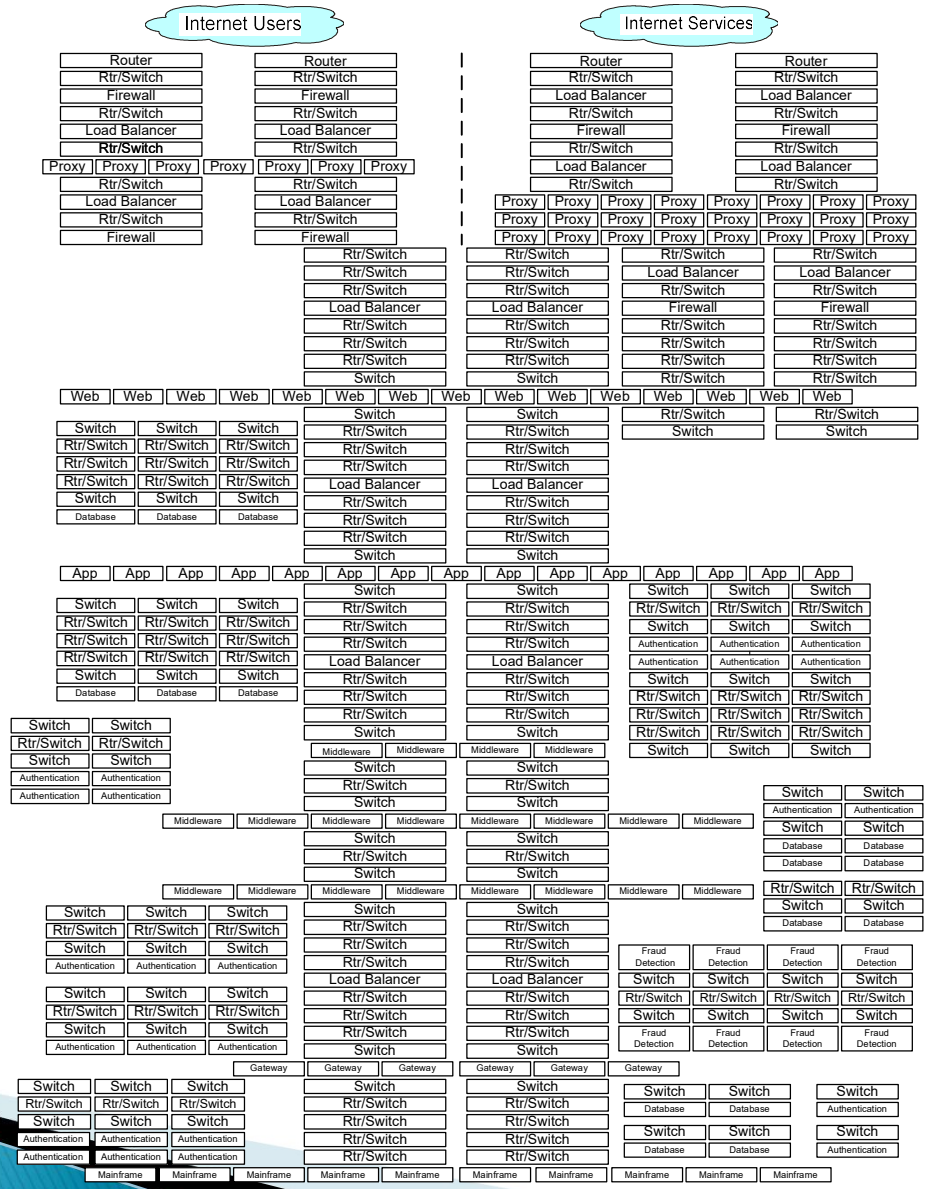
Diffie Hellman Key Exchange



The TLS 1.3 Decryption Problem

- The RSA key exchange option is being removed
- This removes out-of-band TLS decryption capability
- Impact if you're TLS encrypted internally
  - Fraud Monitoring
  - IDS/IPS
  - Malware Detection
  - Layer 7 DDoS Protection
  - Security Incident Response
  - Regulatory Verification
  - Wireshark PCAP decryption
  - NPM/APM

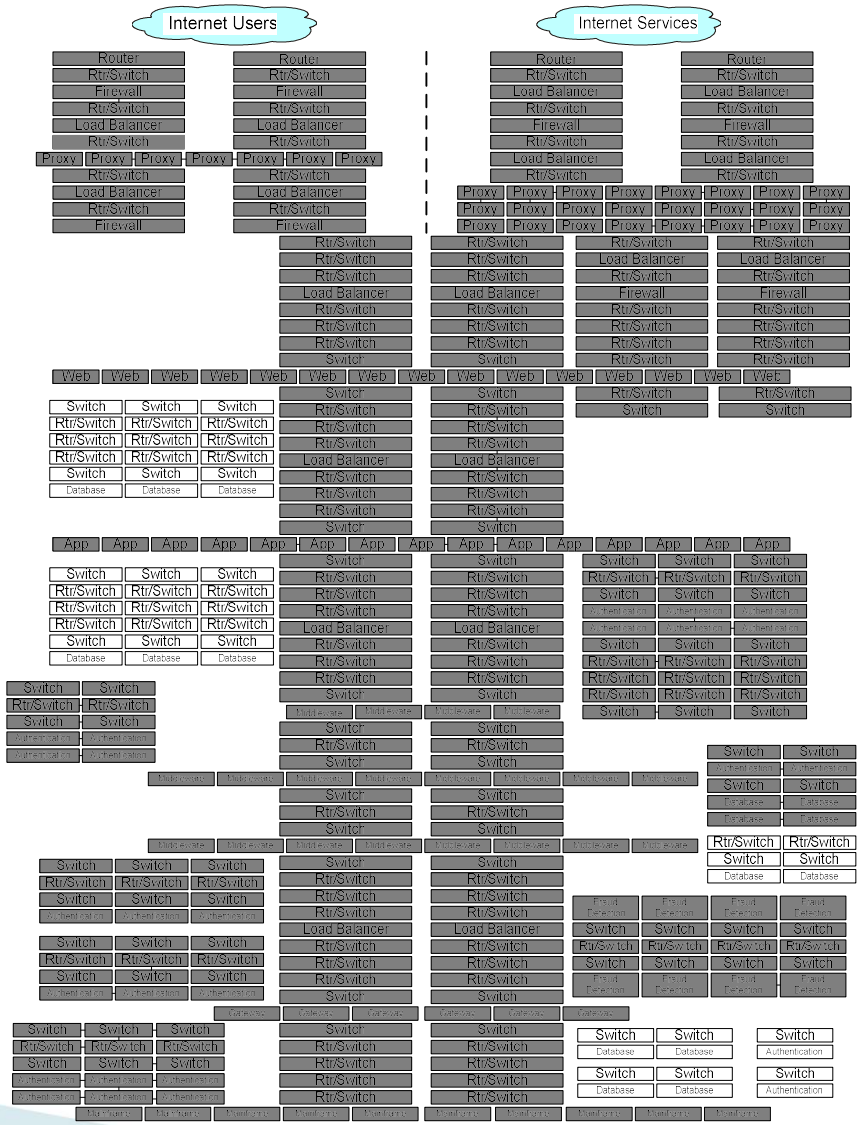
Enterprise Operational Support Environment



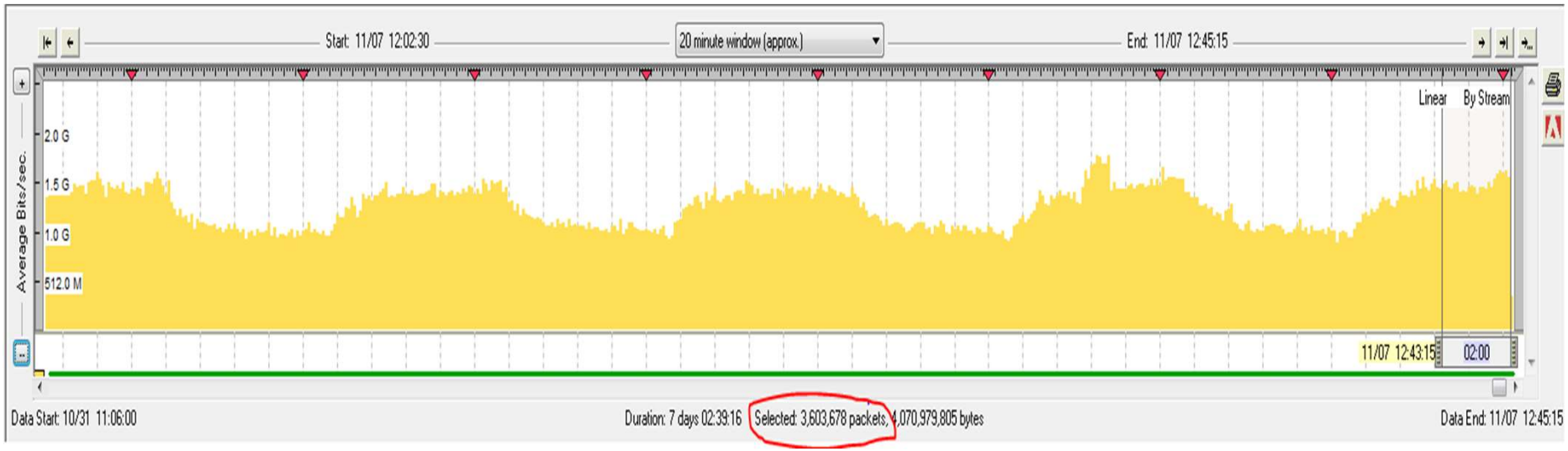
One Internet Facing Application

2000 Total Applications

Enterprise Operational Support Under TLS 1.3



Internet Logon



Internet Logon – Encrypted

No.	Source	Source Port	Destination	Dest Port	tcp.len	Length	Info	Delta Time	Date
48	5.5.5.5	48127	1.1.1.1	443	0	66	48127 → 443 [FIN, ACK] Seq=1024703250 Ack=2976265146 Win=6680 Len=0 TSval=1503040433 TSecr=1000853450	0.000022600	2016-11-06 16:00:03.290964280
49	8.8.8.8	38339	1.1.1.1	443	0	66	38339 → 443 [ACK] Seq=1792253357 Ack=3028574681 Win=4508 Len=0 TSval=1768369599 TSecr=1000801004	0.000004260	2016-11-06 16:00:03.290968540
50	1.1.1.1	443	7.7.7.7	45616	0	66	443 → 45616 [ACK] Seq=2999109147 Ack=2464411239 Win=4757 Len=0 TSval=1000801028 TSecr=1399745673	0.000025850	2016-11-06 16:00:03.290994390
51	1.1.1.1	443	4.4.4.4	39567	1448	1514	[TCP segment of a reassembled PDU]	0.000031430	2016-11-06 16:00:03.291025820
52	1.1.1.1	443	4.4.4.4	39567	877	943	Application Data	0.000002240	2016-11-06 16:00:03.291028060
53	7.7.7.7	45652	1.1.1.1	443	1448	1514	[TCP segment of a reassembled PDU]	0.000048250	2016-11-06 16:00:03.291076310
54	7.7.7.7	45652	1.1.1.1	443	1448	1514	[TCP segment of a reassembled PDU]	0.000010700	2016-11-06 16:00:03.291087010
55	7.7.7.7	45652	1.1.1.1	443	1448	1514	[TCP segment of a reassembled PDU]	0.000011880	2016-11-06 16:00:03.291098890
56	1.1.1.1	443	7.7.7.7	44953	0	66	443 → 44953 [ACK] Seq=2985032055 Ack=341449221 Win=4821 Len=0 TSval=1000853466 TSecr=1399745708	0.000017930	2016-11-06 16:00:03.291116820
57	1.1.1.1	443	7.7.7.7	44953	0	66	443 → 44953 [FIN, ACK] Seq=2985032055 Ack=341449221 Win=4821 Len=0 TSval=1000853466 TSecr=1399745708	0.000002040	2016-11-06 16:00:03.291118860
58	8.8.8.8	38339	1.1.1.1	443	69	135	Encrypted Alert	0.000000260	2016-11-06 16:00:03.291119120
59	1.1.1.1	443	7.7.7.7	44953	0	66	443 → 44953 [ACK] Seq=2985032056 Ack=341449222 Win=4821 Len=0 TSval=1000853466 TSecr=1399745708	0.000000590	2016-11-06 16:00:03.291119710
60	8.8.8.8	38339	1.1.1.1	443	0	66	38339 → 443 [FIN, ACK] Seq=1792253426 Ack=3028574681 Win=4508 Len=0 TSval=1768369599 TSecr=1000801004	0.000014780	2016-11-06 16:00:03.291134490
61	10.10.10.10	34663	1.1.1.1	443	91	157	Change Cipher Spec, Encrypted Handshake Message	0.000130980	2016-11-06 16:00:03.291265470
62	10.10.10.10	34663	1.1.1.1	443	997	1063	Application Data	0.000074890	2016-11-06 16:00:03.291340360
63	10.10.10.10	34662	1.1.1.1	443	91	157	Change Cipher Spec, Encrypted Handshake Message	0.000031590	2016-11-06 16:00:03.291371950
64	1.1.1.1	443	9.9.9.9	35122	0	66	443 → 35122 [ACK] Seq=3046846582 Ack=901284796 Win=2307 Len=0 TSval=1000801029 TSecr=2077406561	0.000103690	2016-11-06 16:00:03.291475640
65	3.3.3.3	53060	1.1.1.1	443	0	66	53060 → 443 [ACK] Seq=3840008680 Ack=2987823235 Win=3922 Len=0 TSval=2110863333 TSecr=1000853431	0.000056930	2016-11-06 16:00:03.291532570
66	10.10.10.10	34662	1.1.1.1	443	1448	1514	[TCP segment of a reassembled PDU]	0.000010410	2016-11-06 16:00:03.291542980
67	10.10.10.10	34662	1.1.1.1	443	1448	1514	[TCP segment of a reassembled PDU]	0.000016080	2016-11-06 16:00:03.291559060
68	10.10.10.10	34662	1.1.1.1	443	1448	1514	[TCP segment of a reassembled PDU]	0.000037220	2016-11-06 16:00:03.291596280
69	1.1.1.1	443	5.5.5.5	48127	0	66	443 → 48127 [ACK] Seq=2976265146 Ack=1024703250 Win=4061 Len=0 TSval=1000853466 TSecr=1503040433	0.000077300	2016-11-06 16:00:03.291673580
70	1.1.1.1	443	5.5.5.5	48127	0	66	443 → 48127 [FIN, ACK] Seq=2976265146 Ack=1024703250 Win=4061 Len=0 TSval=1000853466 TSecr=1503040433	0.000001120	2016-11-06 16:00:03.291674700
71	1.1.1.1	443	5.5.5.5	48127	0	66	443 → 48127 [ACK] Seq=2976265147 Ack=1024703251 Win=4061 Len=0 TSval=1000853466 TSecr=1503040433	0.000000840	2016-11-06 16:00:03.291675540
72	8.8.8.8	38349	1.1.1.1	443	0	66	38349 → 443 [ACK] Seq=1170532302 Ack=2975272445 Win=3784 Len=0 TSval=1768369600 TSecr=1000853440	0.000064540	2016-11-06 16:00:03.291740080
73	1.1.1.1	443	7.7.7.7	45652	0	66	443 → 45652 [ACK] Seq=2990564838 Ack=3576891556 Win=2352 Len=0 TSval=1000801029 TSecr=1399745709	0.000070960	2016-11-06 16:00:03.291811040
74	1.1.1.1	443	7.7.7.7	45652	0	66	443 → 45652 [ACK] Seq=2990564838 Ack=3576894452 Win=3800 Len=0 TSval=1000801029 TSecr=1399745709	0.000001380	2016-11-06 16:00:03.291812420
75	1.1.1.1	443	7.7.7.7	45652	0	66	443 → 45652 [ACK] Seq=2990564838 Ack=3576895900 Win=4524 Len=0 TSval=1000801029 TSecr=1399745709	0.000000920	2016-11-06 16:00:03.291813340
76	1.1.1.1	443	9.9.9.9	35122	177	243	Server Hello, Change Cipher Spec, Encrypted Handshake Message	0.000015430	2016-11-06 16:00:03.291828770
77	8.8.8.8	38349	1.1.1.1	443	91	157	Change Cipher Spec, Encrypted Handshake Message	0.000044250	2016-11-06 16:00:03.291873020
78	1.1.1.1	443	8.8.8.8	38339	0	66	443 → 38339 [ACK] Seq=3028574681 Ack=1792253426 Win=4261 Len=0 TSval=1000801030 TSecr=1768369599	0.000044560	2016-11-06 16:00:03.291917580
79	1.1.1.1	443	8.8.8.8	38339	0	66	443 → 38339 [FIN, ACK] Seq=3028574681 Ack=1792253426 Win=4261 Len=0 TSval=1000801030 TSecr=1768369599	0.000002160	2016-11-06 16:00:03.291919740

```
⊞ Frame 62: 1063 bytes on wire (8504 bits), 1063 bytes captured (8504 bits) on interface 0
⊞ Ethernet II, Src: f[redacted])
⊞ Internet Protocol Version 4, Src: 10.10.10.10, Dst: 1.1.1.1
⊞ Transmission Control Protocol, Src Port: 34663 (34663), Dst Port: 443 (443), Seq: 1779108385, Ack: 3063234623, Len: 997
⊞ Secure Sockets Layer
```

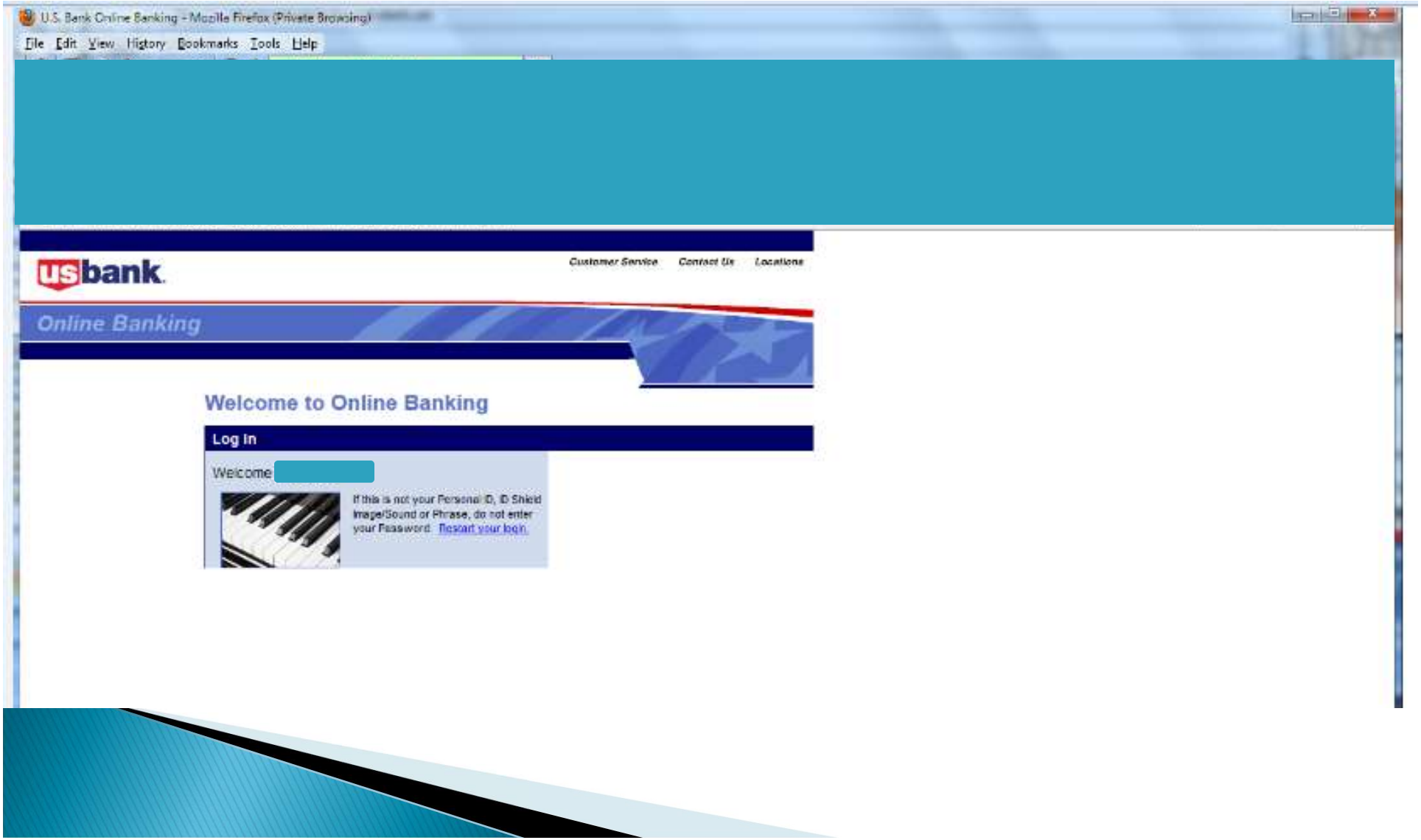
```
0000  f2 bf 6f 2a b6 ce f2 0b  3b 17 f7 5c 08 00 45 00   ..o*.... ;..\..E.
0010  04 19 e4 86 40 00 3b 06  41 43 0a 0a 0a 0a 01 01   ....@.;. AC......
0020  01 01 87 67 01 bb 6a 0b  0a 21 b6 95 40 3f 80 18   ...g..j. .!..@?..
0030  0e c8 ab f3 00 00 01 01  08 0a 84 2f ec 98 3b a7   ........ .../..;.
0040  02 d8 17 03 03 03 e0 9a  5c 03 31 e1 34 84 ef eb   ........ \.1.4...
0050  d6 f9 68 c0 c8 e6 02 f4  7b bc fd 0c c5 d7 8a 5e   ..h..... {......^
0060  2c 88 90 ce c8 9f 81 b0  ea 6b 3a 84 78 bb ee a9   ,....... .k:.x...
0070  2a 72 92 70 1a 52 e7 eb  cc 81 11 20 e1 6e 71 47   *r.p.R.. ... .nqG
0080  db 3e 6e 14 fb 34 9b 53  4a 1a 5b f7 69 4a a3 cb   .>n..4.S J.[.iJ..
0090  d5 c2 c9 c8 63 ce 67 ec  20 29 93 ba ca e7 09 7d   ....c.g. ).....}
00a0  a4 ff ed c7 58 ac 20 4a  7c 09 f7 8d df 1e 9c 07   ....X. J |.......
00b0  ab 99 87 8d 3b 9f 58 81  0f 9a fd cb c3 0d 7e 8a   ....;.X. ......~.
00c0  36 ba b1 07 58 51 cf 0a  aa 06 ba fd 0c 0d e4 44   6...XQ.. .......D.
00d0  21 08 d8 f5 38 77 78 66  32 85 64 32 da b4 ad 79   !...8wxf 2.d2...y
00e0  09 d3 59 b0 ab 10 e3 a6  e2 4e 9c b3 6e 57 49 3b   ..Y..... .N..nWI;
00f0  da 56 fa 4a c2 bb e7 66  19 0e e0 f7 a6 f4 f9 4f   .V.J...f .......O
0100  4e 96 a5 53 6d 51 34 d3  bd 99 61 c5 a6 31 9b 66   N..SmQ4. ..a..1.f
0110  7b 8b b0 37 07 9a 60 d4  e6 43 52 79 36 ae 03 52   {..7..`. .CRy6..R
0120  51 40 9a 91 e6 0b 79 e0  af 0d 05 05 31 26 00 71   Q@....y. ....1&.q
0130  02 0b 00 ae cd b6 71 5e  73 9e 91 61 28 49 61 1e   ......q^ s..a(Ia.
0140  ed 8e dc 63 f5 7d b5 d6  15 91 fc 56 50 7d fc 19   ...c.}.. ...VP}..
0150  e1 57 a1 d5 73 b0 be 80  8b 35 66 13 cb d0 cc 4e   .W..s... .5f....N
0160  69 a7 10 e4 b2 f5 1e 7f  d6 f8 7e 8c f8 2a ba 1e   i....... ..~..*..
0170  fc 6d 2c ef 86 dd 24 e9  e7 e5 12 d7 6b da 17 4a   .m,...$. ....k..J
0180  72 a1 58 1e 5a 6b 12 0c  db 9f 69 02 e9 66 d1 49   r.X.Zk.. ..i..f.I
0190  9c 7d a3 93 d2 e1 ec 09  46 58 0d dd 63 10 40 f6   .}...... FX..c.@.
01a0  8a 86 7a 51 37 75 35 52  52 3f 07 60 d4 6c af c1   ..zQ7u5R R?.`.l..
01b0  00 17 1f 8d 73 6f 87 08  90 95 07 38 b1 ea 15 bb   ....so.. ...8....
01c0  58 bb 1c be bb 8b 4f 6d  9c be 34 d4 5c 14 27 21   X.....Om ..4.\.'!
01d0  d3 5e 21 21 2a 6e 54 b6  d6 55 43 40 bc 0e 43 9e   .^!!*nT. .UC@..C.
01e0  30 8e 85 ed 15 3d 2e 45  a1 f4 40 7b 91 bd 88 ae   0....=.E ..@{....
01f0  29 7d c1 da 9d d4 84 57  a1 7f c3 79 86 a2 34 67   )}.....W ...y..4g
0200  1b bb 14 dd 81 c6 11 7b  05 49 fa bb 58 fc d6 30   .......{ .I..X..0
0210  fc c8 d4 05 64 12 13 74  29 6d 79 e1 16 f2 5c df   ....d..t )my...\.
0220  6f c4 5c 66 94 90 59 9d  3a 4a 95 19 32 68 0e 98   o.\f..Y. :J..2h..
0230  83 62 c6 dc 67 e6 ac 09  0f a9 6e 14 16 65 f1 0c   .b..g... ..n..e..
0240  cb 37 63 fb 1b 84 62 8c  a9 30 8c ea 7a 22 89 20   .7c...b. .0..z"..
0250  40 e2 ab 84 b9 1e 86 8d  ff 64 a2 ee 15 fe 11 a7   @....... .d......
0260  2a 85 5a 60 03 07 cf 9c  20 b8 d0 ff 51 c7 af c6   *.Z`.... ....Q...
0270  c4 c6 aa 44 e0 7c 3f e9  a2 9d e2 04 41 f1 55 3a   ...D.|?. ....A.U:
0280  c4 c2 f3 9e d2 e7 be 0f  59 6c 39 02 7c 26 64 57   ........ Yl9.|&dW
0290  a6 b4 cb 1f 44 c7 ef e0  51 9d 32 d8 1c 47 1e 5f   ....D... Q.2..G._
02a0  f9 f4 e9 98 43 c1 d9 23  7a 35 e9 32 2e a9 14 8c   ....C..# z5.2....
02b0  fd 6b b4 83 40 26 df 5a  1f 47 f6 21 25 6a 08 0b   .k..@&.Z .G.!%j..
02c0  40 d1 05 92 bc c6 e7 1e  72 c0 6a a1 a0 50 9b 73   @....... r.j..P.s
02d0  64 6d fc 14 4b 5a f5 83  53 3a 56 d0 d5 0d b8 59   dm..KZ.. S:V....Y
```

Internet Logon – Decrypted

No.	Source	Source Port	Destination	Dest Port	tcp.len	Length	Info	Delta Time	Date
35	1.1.1.1	443	7.7.7.7	45358	1456	1510	443 → 45358 [PSH, ACK] Seq=3080820754 Ack=3683604260 Win=65535 Len=1456	0.000026340	2016-11-06 16:00:03.288737820
36	1.1.1.1	443	7.7.7.7	45358	1440	1494	443 → 45358 [PSH, ACK] Seq=3080822210 Ack=3683604260 Win=65535 Len=1440	0.000001220	2016-11-06 16:00:03.288739040
37	1.1.1.1	443	7.7.7.7	45358	1456	1510	443 → 45358 [PSH, ACK] Seq=3080823650 Ack=3683604260 Win=65535 Len=1456	0.000025890	2016-11-06 16:00:03.288764930
38	1.1.1.1	443	7.7.7.7	45358	1440	1494	443 → 45358 [PSH, ACK] Seq=3080825106 Ack=3683604260 Win=65535 Len=1440	0.000001220	2016-11-06 16:00:03.288766150
39	1.1.1.1	443	7.7.7.7	45358	1456	1510	443 → 45358 [PSH, ACK] Seq=3080826546 Ack=3683604260 Win=65535 Len=1456	0.000032900	2016-11-06 16:00:03.288799050
40	1.1.1.1	443	7.7.7.7	45358	1440	1494	443 → 45358 [PSH, ACK] Seq=3080828002 Ack=3683604260 Win=65535 Len=1440	0.000002220	2016-11-06 16:00:03.288801270
41	1.1.1.1	443	7.7.7.7	45358	1395	1449	443 → 45358 [PSH, ACK] Seq=3080829442 Ack=3683604260 Win=65535 Len=1395	0.000104990	2016-11-06 16:00:03.288906260
42	1.1.1.1	443	7.7.7.7	45358	1424	1478	443 → 45358 [PSH, ACK] Seq=3080830837 Ack=3683604260 Win=65535 Len=1424	0.000125350	2016-11-06 16:00:03.289031610
43	1.1.1.1	443	7.7.7.7	45358	1440	1494	443 → 45358 [PSH, ACK] Seq=3080832261 Ack=3683604260 Win=65535 Len=1440	0.000031680	2016-11-06 16:00:03.289063290
44	1.1.1.1	443	7.7.7.7	45358	1456	1510	443 → 45358 [PSH, ACK] Seq=3080833701 Ack=3683604260 Win=65535 Len=1456	0.000003670	2016-11-06 16:00:03.289066960
45	1.1.1.1	443	7.7.7.7	45358	1440	1494	443 → 45358 [PSH, ACK] Seq=3080835157 Ack=3683604260 Win=65535 Len=1440	0.000019070	2016-11-06 16:00:03.289086030
46	1.1.1.1	443	7.7.7.7	45358	1456	1510	443 → 45358 [PSH, ACK] Seq=3080836597 Ack=3683604260 Win=65535 Len=1456	0.000003640	2016-11-06 16:00:03.289089670
47	1.1.1.1	443	7.7.7.7	45358	1360	1414	443 → 45358 [PSH, ACK] Seq=3080838053 Ack=3683604260 Win=65535 Len=1360	0.000023160	2016-11-06 16:00:03.289112830
48	1.1.1.1	443	7.7.7.7	45358	247	301	443 → 45358 [PSH, ACK] Seq=3080839413 Ack=3683604260 Win=65535 Len=247	0.000086880	2016-11-06 16:00:03.289199710
49	7.7.7.7	45616	1.1.1.1	443	441	495	45616 → 443 [PSH, ACK] Seq=2464410346 Ack=2999108970 Win=65535 Len=441	0.001227550	2016-11-06 16:00:03.290427260
50	6.6.6.6	42551	1.1.1.1	443	0	64	42551 → 443 [FIN, ACK] Seq=1464719688 Ack=3080330846 Win=65535 Len=0	0.000107910	2016-11-06 16:00:03.290535170
51	1.1.1.1	443	6.6.6.6	42551	0	64	443 → 42551 [FIN, ACK] Seq=3080330846 Ack=1464719689 Win=65535 Len=0	0.000000120	2016-11-06 16:00:03.290535290
52	6.6.6.6	42551	1.1.1.1	443	0	64	42551 → 443 [ACK] Seq=1464719689 Ack=3080330847 Win=65535 Len=0	0.000000020	2016-11-06 16:00:03.290535310
53	7.7.7.7	45652	1.1.1.1	443	1424	1478	[TCP segment of a reassembled PDU]	0.000940650	2016-11-06 16:00:03.291475960
54	7.7.7.7	45652	1.1.1.1	443	1440	1494	[TCP segment of a reassembled PDU]	0.000032240	2016-11-06 16:00:03.291508200
55	7.7.7.7	45652	1.1.1.1	443	1456	1510	[TCP segment of a reassembled PDU]	0.000001780	2016-11-06 16:00:03.291509980
56	1.1.1.1	443	3.3.3.3	53060	0	64	443 → 53060 [FIN, ACK] Seq=2987822994 Ack=3840008167 Win=65535 Len=0	0.000129310	2016-11-06 16:00:03.291639290
57	3.3.3.3	53060	1.1.1.1	443	0	64	53060 → 443 [FIN, ACK] Seq=3840008166 Ack=2987822994 Win=65535 Len=0	0.000000030	2016-11-06 16:00:03.291639320
58	3.3.3.3	53060	1.1.1.1	443	0	64	53060 → 443 [ACK] Seq=3840008167 Ack=2987822995 Win=65535 Len=0	0.000000070	2016-11-06 16:00:03.291639390
59	10.10.10.10	34662	1.1.1.1	443	1424	1478	[TCP segment of a reassembled PDU]	0.000086810	2016-11-06 16:00:03.291726200
60	10.10.10.10	34662	1.1.1.1	443	1440	1494	[TCP segment of a reassembled PDU]	0.000001460	2016-11-06 16:00:03.291727660
61	10.10.10.10	34662	1.1.1.1	443	1456	1510	[TCP segment of a reassembled PDU]	0.000053000	2016-11-06 16:00:03.291780660
62	10.10.10.10	34663	1.1.1.1	443	943	997	GET [redacted]	0.000332720	2016-11-06 16:00:03.292113380
63	8.8.8.8	38349	1.1.1.1	443	1424	1478	[TCP segment of a reassembled PDU]	0.000037880	2016-11-06 16:00:03.292151260
64	8.8.8.8	38349	1.1.1.1	443	1440	1494	[TCP segment of a reassembled PDU]	0.000001330	2016-11-06 16:00:03.292152590
65	3.3.3.3	53123	1.1.1.1	443	0	66	53123 → 443 [ACK] Seq=1973476238 Ack=3000646340 Win=3650 Len=0 TSval=21108633	0.000130270	2016-11-06 16:00:03.292282860
66	8.8.8.8	38349	1.1.1.1	443	408	462	[TCP segment of a reassembled PDU]	0.000052970	2016-11-06 16:00:03.292335830

```
⊞ Frame 62: 997 bytes on wire (7976 bits), 997 bytes captured (7976 bits) on interface 0
⊞ Ethernet II, Src: [redacted]
⊞ Internet Protocol Version 4, Src: 10.10.10.10, Dst: 1.1.1.1
⊞ Transmission Control Protocol, Src Port: 34663 (34663), Dst Port: 443 (443), Seq: 1779108060, Ack: 3063234446, Len: 943
⊟ Hypertext Transfer Protocol
  ⊞ [redacted]
  ⊞ GET [redacted]
  ⊞ [redacted]
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
    User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 10_1 like Mac OS X) AppleWebKit/602.2.14 (KHTML, like Gecko) Version/10.0 Mobile/14B72 Safari/602.1\r\n
    Accept-Language: en-us\r\n
    Referer: https://www.usbank.com/index.html\r\n
    DNT: 1\r\n
    True-Client-IP: 174.219.140.247\r\n
    Pragma: no-cache\r\n
    X-Akamai-CONFIG-LOG-DETAIL: true\r\n
    TE:  chunked;q=1.0\r\n
    Connection: TE\r\n
    Accept-Encoding: gzip\r\n
    Akamai-Origin-Hop: 2\r\n
    Via: 1.1 v1-akamaitech.net(ghost) (AkamaiGHost), 1.1 akamai.net(ghost) (AkamaiGHost)\r\n
    X-Forwarded-For: 174.219.140.247, [redacted]
```

Internet Banking Login Failure



Application Log

15:30:43	Column 12	10.10.10.10	Enter Userid	Challenge Question
15:30:59	Column 12	10.10.10.10	Challenge Answer	Answer OK
15:36:29	Column 12	10.10.10.10	Enter Userid	Challenge Question
15:36:34	Column 12	10.10.10.10	Challenge Answer	Answer OK
15:41:35	Column 11	10.10.10.10	Enter Userid	Challenge Question
15:41:44	Column 11	10.10.10.10	Challenge Answer	Answer OK
15:49:01	Column 6	10.10.10.10	Enter Userid	Challenge Question
15:49:06	Column 6	10.10.10.10	Challenge Answer	Answer OK
15:54:16	Column 9	10.10.10.10	Enter Userid	Challenge Question
15:54:22	Column 9	10.10.10.10	Challenge Answer	Answer OK

Internet Analysis – Encrypted Login Screen

Internet Analysis – Decrypted Login Screen

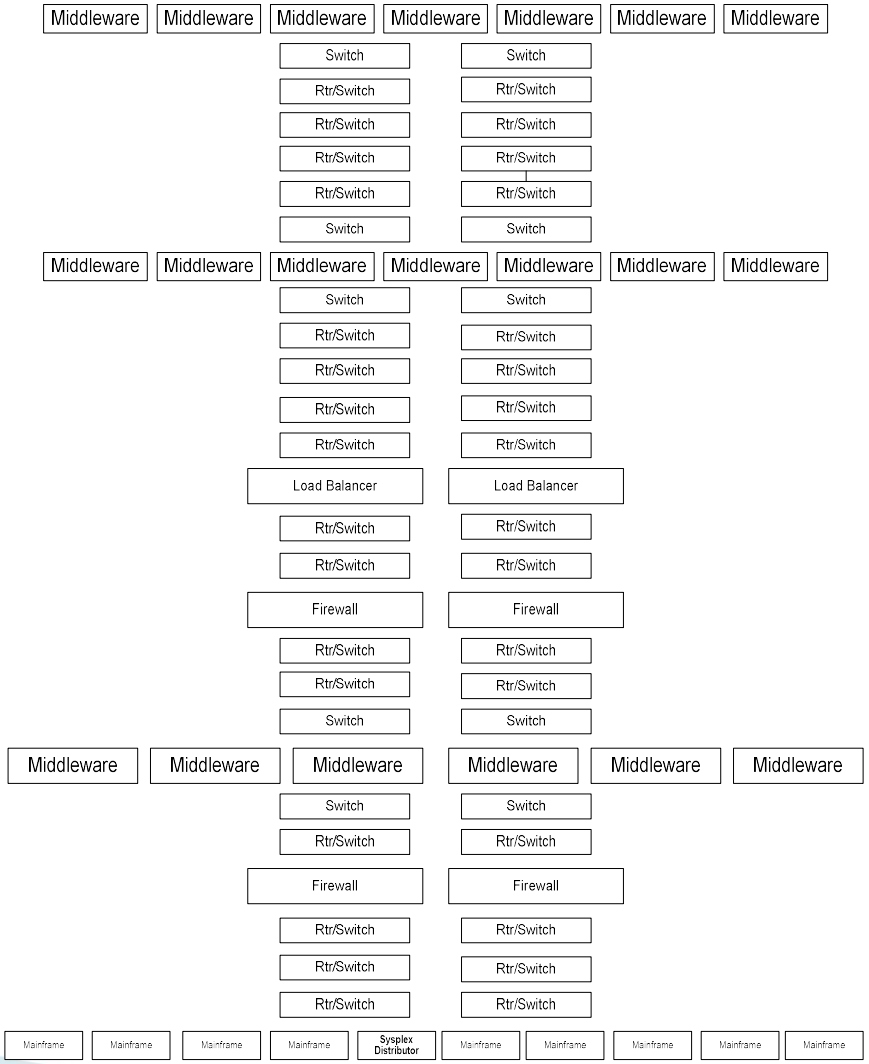
```
TP: 118:       <td class=f32 valign=bottom>Welcome to Online Banking</td>
TP: 119:     </tr>\r\n
TP: 120:     <tr>\r\n
```

```
3d 22 66 33 22 20 68 65 69 67 68 74 3d 22 32 30  ="f3" height="20
22 3e 6d 65 6f 77 3c 2f 74 64 3e 3c 2f 74 72 3e  ">[redacted]/td></tr>
20 0d 0a 09 20 20 09 09 09 09 0d 0a 09 20 20 20  ... ..... .....
09 09 09 09 3c 74 72 3e 0d 0a 09 20 20 20 09 09  ....<tr>... ...
09 09 09 3c 74 64 20 77 69 64 74 68 3d 31 20 68  ...<td width=1 h
65 69 67 68 74 3d 31 30 20 63 6f 6c 73 70 61 6e  eight=10 colspan
3d 34 3e 3c 69 6d 67 20 73 72 63 3d 27 2f 69 6e  =4><img src='/in
74 65 72 6e 65 74 42 61 6e 6b 69 6e 67 53 74 61  ternetBankingSta
74 69 63 2f 69 6d 61 67 65 73 2f 73 70 61 63 65  tic/images/space
72 2e 67 69 66 27 20 77 69 64 74 68 3d 31 20 68  r.gif' width=1 h
65 69 67 68 74 3d 31 30 20 61 6c 74 3d 22 22 3e  eight=10 alt="">
3c 2f 74 64 3e 0d 0a 09 20 20 09 09 09 09 3c 2f  </td>... ....</
74 72 3e 0d 0a 09 20 20 09 09 09 09 3c 74 72 3e  tr>... ....<tr>
0d 0a 09 20 20 20 09 09 09 09 09 3c 74 64 20 77  ... .....<td w
69 64 74 68 3d 38 20 76 61 6c 69 67 6e 3d 74 6f  idth=8 valign=to
70 3e 3c 69 6d 67 20 73 72 63 3d 27 2f 69 6e 74  p><img src='/int
65 72 6e 65 74 42 61 6e 6b 69 6e 67 53 74 61 74  ernetBankingStat
69 63 2f 69 6d 61 67 65 73 2f 61 72 72 6f 77 5f  ic/images/arrow_
72 65 64 32 2e 67 69 66 27 20 76 73 70 61 63 65  red2.gif' vspace
3d 34 20 61 6c 74 3d 22 22 3e 3c 2f 74 64 3e 0d  =4 alt=""></td>.
0a 09 20 20 20 09 09 09 09 09 3c 74 64 20 63 6f  .. .....<td co
6c 73 70 61 6e 3d 33 3e 3c 73 70 61 6e 20 63 6c  lspan=3><span cl
61 73 73 3d 66 36 3e 50 61 73 73 77 6f 72 64 3c  ass=f6>Password<
69 6d 67 20 73 72 63 3d 27 2f 69 6e 74 65 72 6e  img src='/intern
65 74 42 61 6e 6b 69 6e 67 53 74 61 74 69 63 2f  etBankingStatic/
69 6d 61 67 65 73 2f 73 70 61 63 65 72 2e 67 69  images/spacer.gi
66 27 20 77 69 64 74 68 3d 34 32 20 68 65 69 67  f' width=42 heig
68 74 3d 31 20 61 6c 74 3d 22 22 3e 3c 2f 73 70  ht=1 alt=""></sp
61 6e 3e 0d 0a 09 20 20 20 09 09 09 09 09 3c 61  an>... .....<a
20 63 6c 61 73 73 3d 66 33 30 20 68 72 65 66 3d   class=f30 href=
22 2f 69 6e 74 65 72 6e 65 74 42 61 6e 6b 69 6e  "[redacted]
67 2f 52 65 71 75 65 73 74 52 6f 75 74 65 72 3f  
72 65 71 75 65 73 74 43 6d 64 49 64 3d 44 69 73  
70 6c 61 79 4c 6f 67 69 6e 41 73 73 69 73 74 61  
6e 63 65 53 65 6c 65 63 74 69 6f 6e 50 61 67 65  
26 74 79 70 65 3d 70 61 73 73 77 6f 72 64 26 4c  &type=password&L
4f 47 49 4e 41 53 53 49 53 54 41 4e 43 45 46 4c  OGINASSISTANCEFL
41 47 3d 54 52 55 45 22 3e 46 6f 72 67 6f 74 20  AG=TRUE">Forgot 
70 61 73 73 77 6f 72 64 3f 3c 2f 61 3e 3c 2f 74  password?</a></t
```

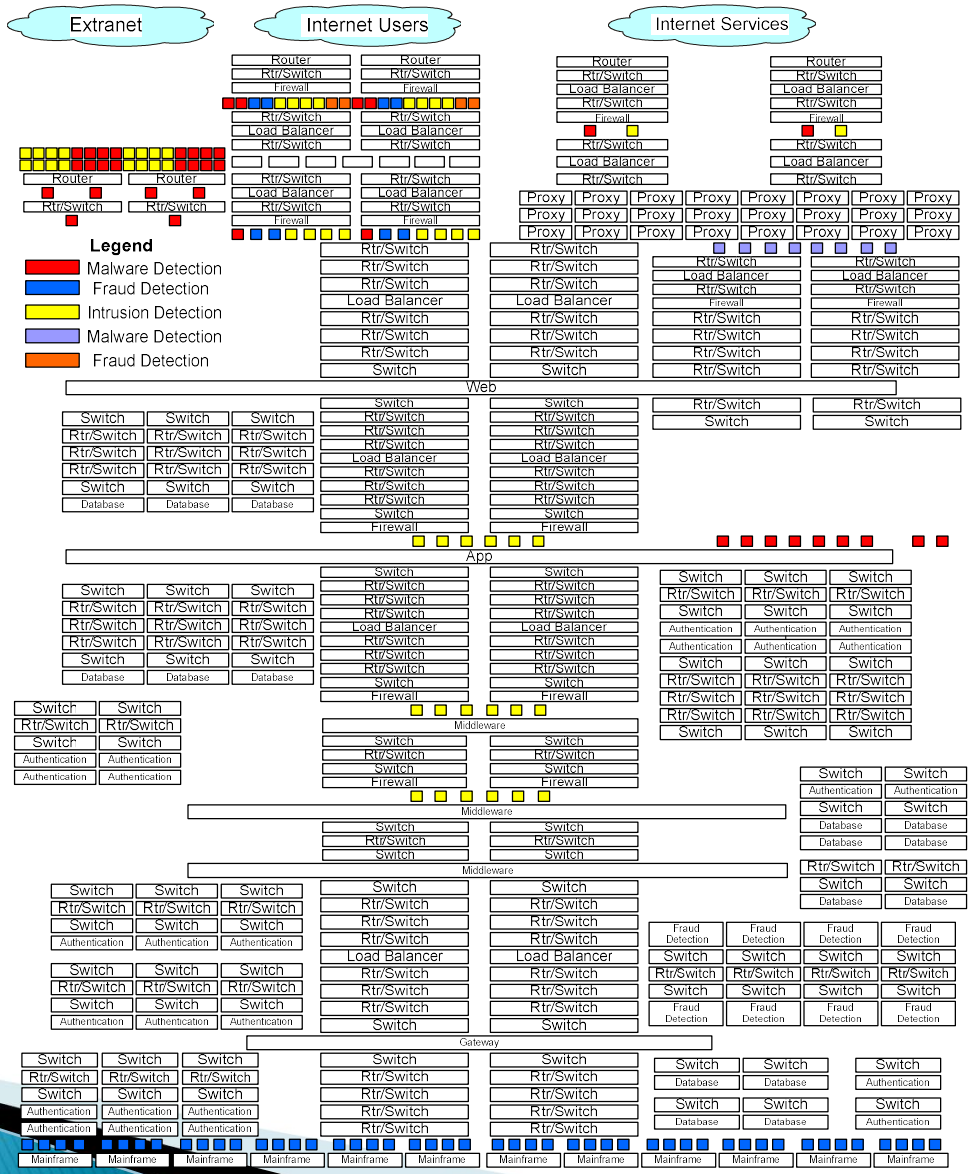
Internet Analysis – Hex Data

```
20 63 6c 61 73 73 3d 22 66 32 22 3e 49 66 20 74   class="f2">If t
68 69 73 20 69 73 20 6e 6f 74 20 79 6f 75 72 20  his is not your
50 65 72 73 6f 6e 61 6c 20 49 44 2c 20 49 44 20  Personal ID, ID
53 68 69 65 6c 64 20 49 6d 61 67 65 2f 53 6f 75  Shield Image/Sou
6e 64 20 6f 72 20 50 68 72 61 73 65 2c 20 64 6f  nd or Phrase, do
20 6e 6f 74 20 65 6e 74 65 72 20 79 6f 75 72 20   not enter your
50 61 73 73 77 6f 72 64 2e 26 23 31 36 30 3b 3c  Password. <
2f 73 70 61 6e 3e 26 23 31 36 30 3b 3c 73 70 61  /span> <spa
6e 20 63 6c 61 73 73 3d 22 66 33 30 22 3e 3c 61  n class="f30"><a
20 68 72 65 66 3d 22 2f 69 6e 74 65 72 6e 65 74  [redacted]
42 61 6e 6b 69 6e 67 2f 52 65 71 75 65 73 74 52
6f 75 74 65 72 3f 72 65 71 75 65 73 74 43 6d 64
49 64 3d 44 69 73 70 6c 61 79 4c 6f 67 69 6e 50
61 67 65 22 20 74 61 72 67 65 74 3d 22 5f 73 65
6c 66 22 3e 52 65 73 74 61 72 74 20 79 6f 75 72  lf">Restart your
20 6c 6f 67 69 6e 2e 3c 2f 61 3e 3c 2f 73 70 61   login.</a></spa
6e 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00  n>..............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Middleware Troubleshooting Example



Enterprise Security Challenges

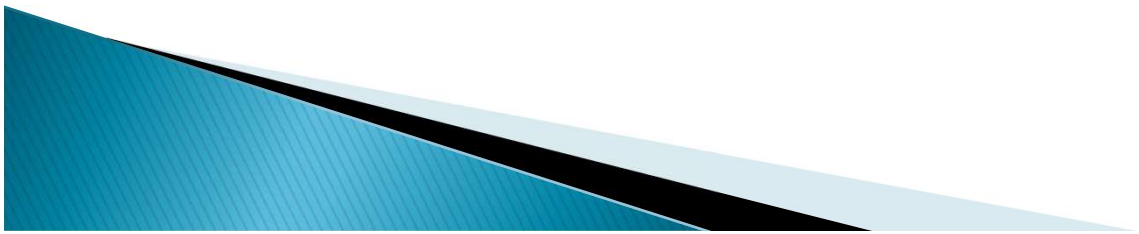


Threat Detection and Incident Response

- IDS Alerts
  - Manual verification – Was it a false positive?
- SQL Injection Attacks
  - Manual verification – Was it successful?
- Manual hunting for known vulnerabilities
- Verify anti-virus alerts and identify root cause
- Heuristics on encrypted packets and/or host-based systems will not accomplish this

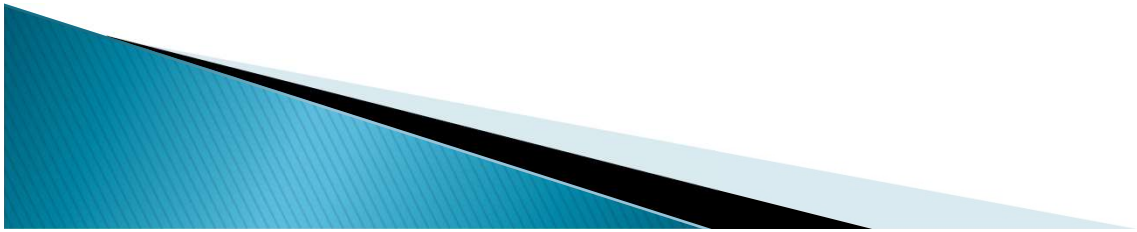
The Cost of Doing Nothing

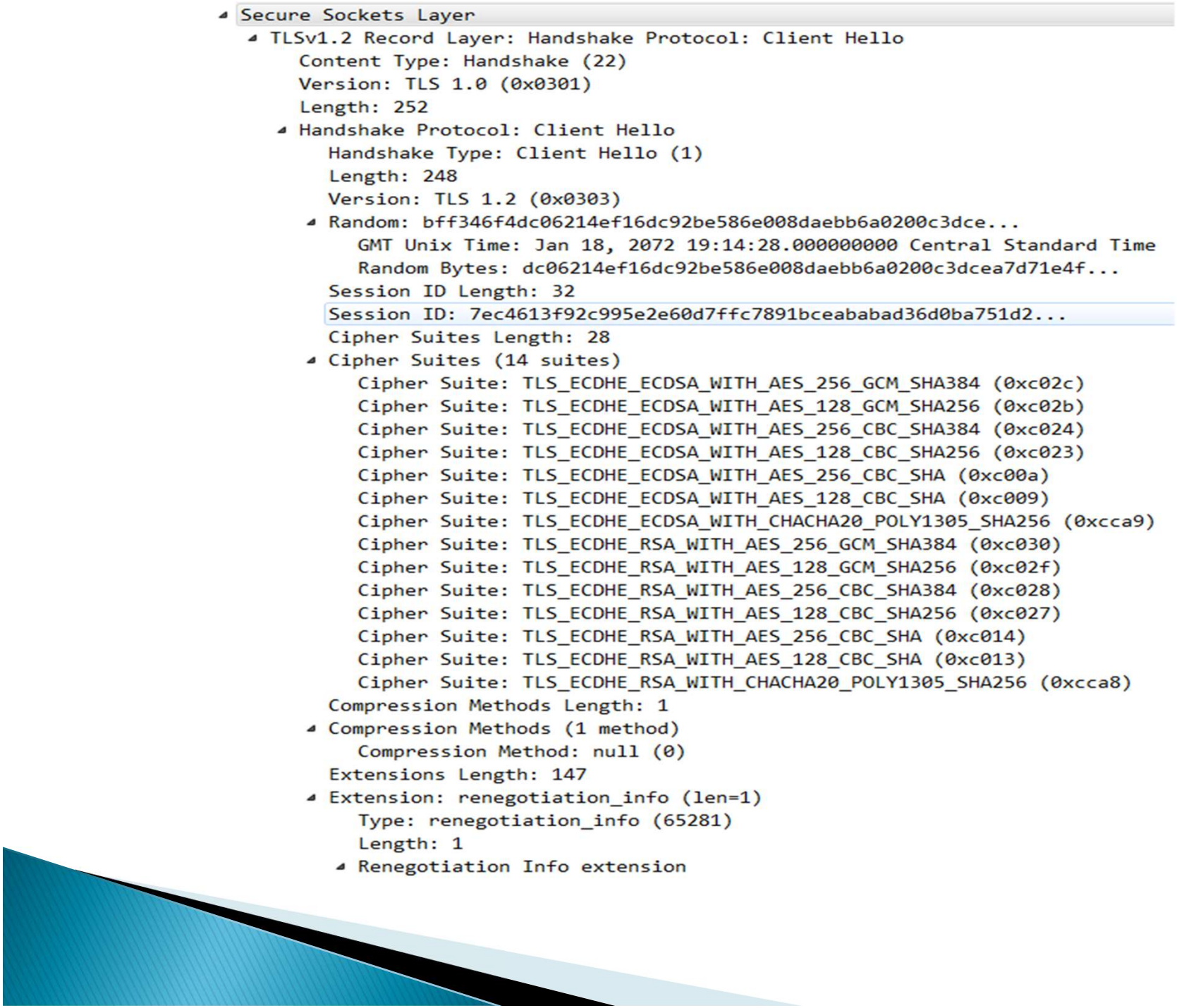
- Severity 1 problems that last more than a week
- Severity two problems that last 2-4 months
  - Citrix environment
  - Outbound SSL environment
- Tens of millions in infrastructure costs
  - Inline/MITM SSL Decryption solution for IDS, Security Analysis, Fraud monitoring, etc…
  - This does not account for the visibility needs of troubleshooting teams.
- Costs of extended outages and malware that is not detected



Urgency – TLS 1.2

- We have a Diffie Hellman problem, not just a TLS 1.3 problem
- Vendors are moving Diffie Hellman ciphers to the top of their TLS 1.2 cipher list
- Vendors are completely removing RSA from their TLS 1.2 cipher list
  - Apple iPhone (App Transport Security)




Secure Sockets Layer
TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 252
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 248
Version: TLS 1.2 (0x0303)
Random: bff346f4dc06214ef16dc92be586e008daebb6a0200c3dce...
GMT Unix Time: Jan 18, 2072 19:14:28.000000000 Central Standard Time
Random Bytes: dc06214ef16dc92be586e008daebb6a0200c3dcea7d71e4f...
Session ID Length: 32
Session ID: 7ec4613f92c995e2e60d7ffc7891bceababad36d0ba751d2...
Cipher Suites Length: 28
Cipher Suites (14 suites)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
Compression Methods Length: 1
Compression Methods (1 method)
Compression Method: null (0)
Extensions Length: 147
Extension: renegotiation_info (len=1)
Type: renegotiation_info (65281)
Length: 1
Renegotiation Info extension

Urgency – New RSA Vulnerabilities

- New RSA vulnerabilities may accelerate its demise in TLS 1.2

Transport Layer Security (TLS) Vulnerability
12/13/2017 10:46 AM EST

Original release date: December 13, 2017

CERT Coordination Center (CERT/CC) has released information on a Transport Layer Security (TLS) vulnerability. Exploitation of this vulnerability could allow an attacker to access sensitive information.

The TLS vulnerability is also known as Return of Bleichenbacher's Oracle Threat (ROBOT). ROBOT allows an attacker to obtain the RSA key necessary to decrypt TLS traffic under certain conditions. Mitigations include installing updates to affected products as they become available. US-CERT encourages users and administrators to review CERT/CC Vulnerability Note VU #144389.

TLS Email List Comments
[EXTERNAL] Re: [TLS] A closer look at ROBOT, BB Attacks, timing attacks in general, and what we can do in TLS

"Let's not forget defense 0: migrating away from broken algorithms (which means turning them off)...."
Sincerely,
Watson Ladd

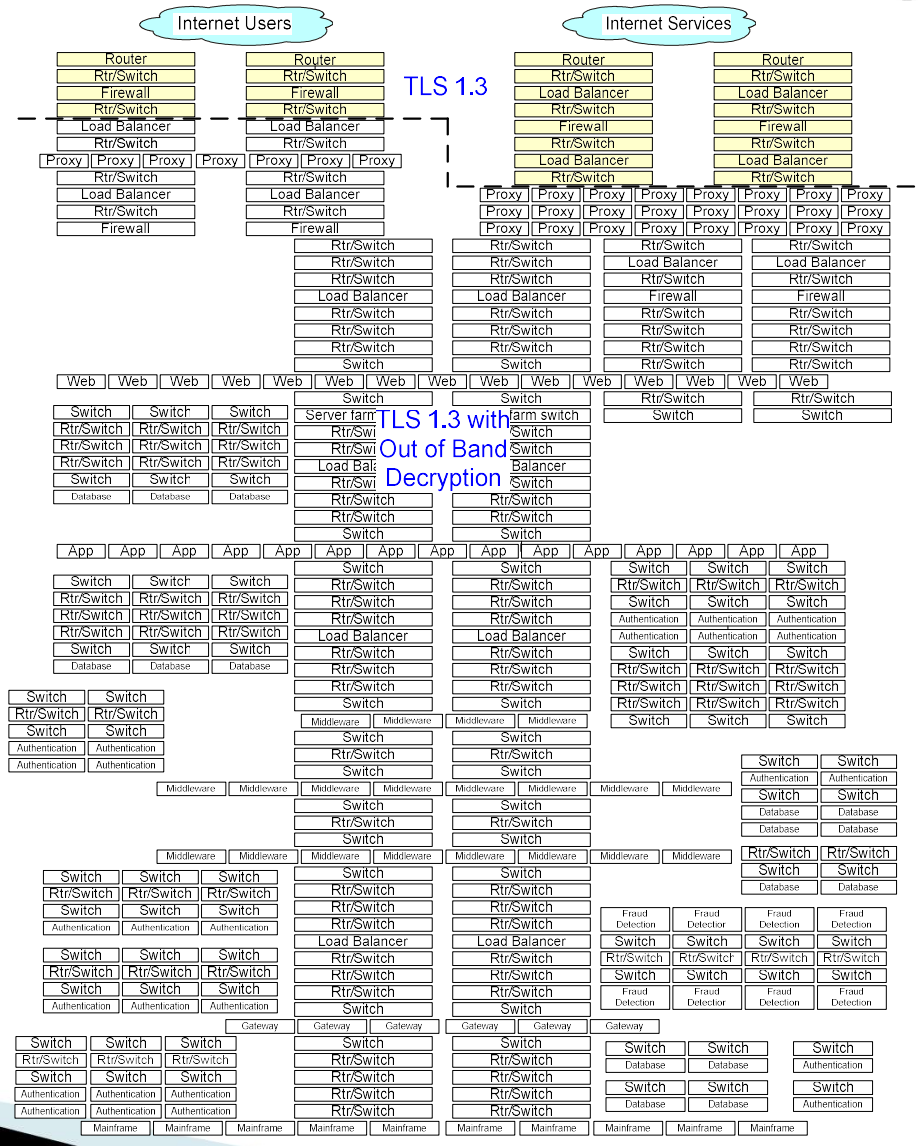
"I think there should be a draft which formally deprecates RSA, recommends the support to be removed (at least from server side) and updates TLS 1.2 to change the MTI ciphersuite. Of course, certain ("visibility") folks would scream about that."

-Ilari

Summary

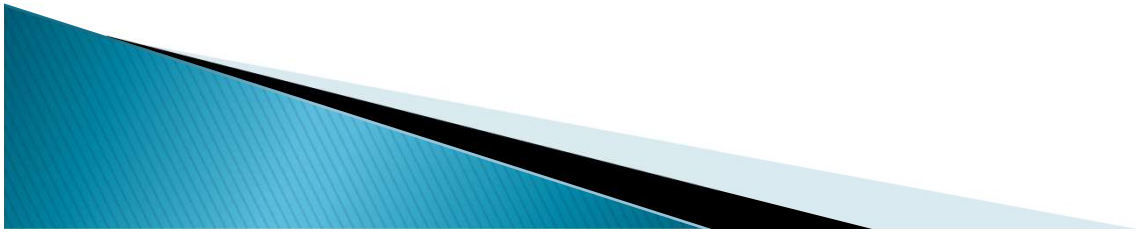
- This is an industry-wide concern
  - Financial, Health Care, Retail, Government and others are affected
- We need a Diffie Hellman decryption solution
- TLS 1.2 is not a long term solution

Proposed Data Center Visibility Solution



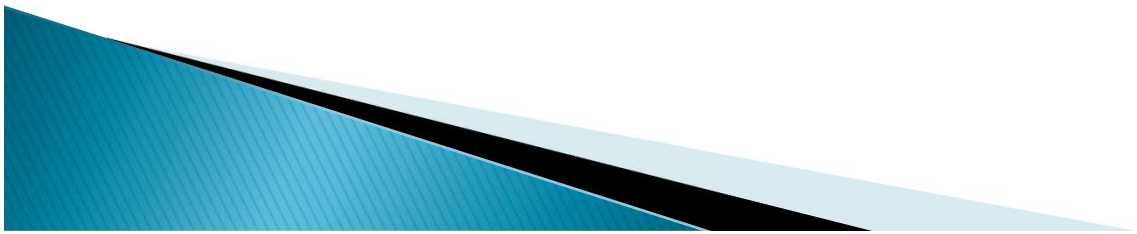
Additional IETF Encryption Efforts to Watch

- QUIC
- HTTP2
- DPRIVE
- TCPINC
- IPSec



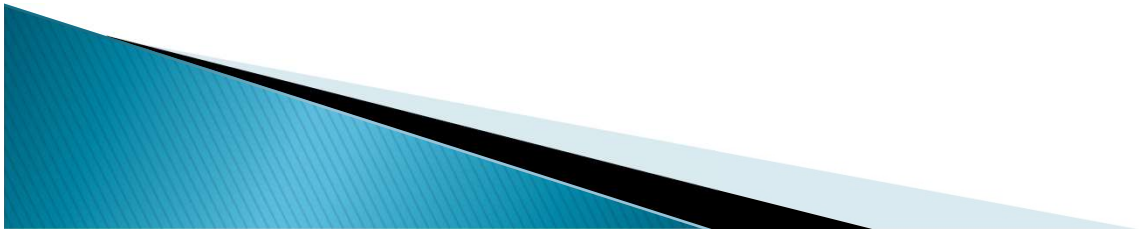
Lessons Learned

- Involvement with the TLS working group would have been way easier four years ago
- There is a lack of enterprise involvement in the IETF
- Culture change takes time
  - IETF involvement needs to be for the long term



IETF 101 London March 19

- Presentation of draft-rhrd-tls-tls13-visibility-01
  - Export of Diffie Hellman ephemeral keys
  - Client Opt In
  - Out of Band TLS decryption
  - Inline TLS decryption when TLS is not terminated
  - Decryption of reused TLS sessions
- Requests
  - We need participants in the room
  - We need speakers at the mic
  - We need remote participants (March 19, 12:40 – 1:40 PM)



Additional 2018 TLS 1.3 Standards Activities

- 3 IETF Meetings
  - London – March
  - Montreal – July
  - Asia – November
- ETSI (European Telecommunications Standards Institute)
- NIST NCCoE (National Cybersecurity Center of Excellence) Lab testing
- Vendor Visits