Heart Bleed

Prof Bill Buchanan, Edinburgh Napier

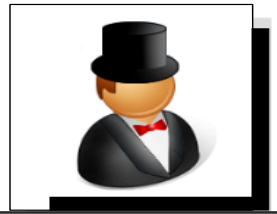
http://asecuritysite.com @billatnapier

HeartBleed

Author: Prof Bill Buchanan

Eve

OpenSSL

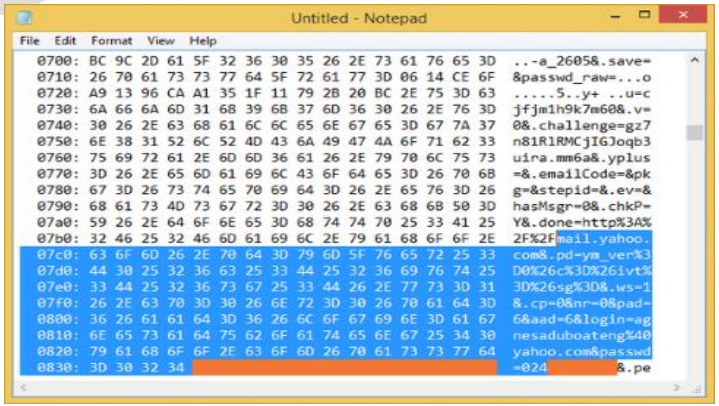


Bob

TLS Heartbeat reveals 64K of memory

SSL/TLS

Alice (Web)



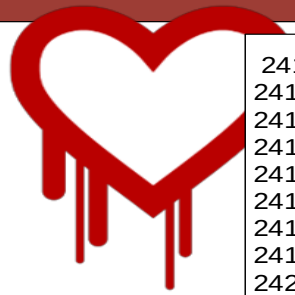
Alice (Cert)

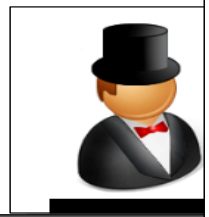
HeartBleed

Encryption

CVE-2014-0160

Author: Prof Bill Buchanan





Bob

```
 2412        /* Read type and payload length first */
2413        hbtype = *p++;
2414        n2s(p, payload);
2415        pl = p;
2416
2417        if (s->msg_callback)
2418                s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
2419                        &s->s3->rrec.data[0], s->s3->rrec.length,
2420                        s, s->msg_callback_arg);
2421
2422        if (hbtype == TLS1_HB_REQUEST)
2423                {
2424                unsigned char *buffer, *bp;
2425                int r;
2426
2427                /* Allocate memory for the response, size is 1 bytes
2428                 * message type, plus 2 bytes payload length, plus
2429                 * payload, plus padding
2430                 */
2431                buffer = OPENSSL_malloc(1 + 2 + payload + padding);
2432                bp = buffer;
2433
2434                /* Enter response type, length and copy payload */
2435                *bp++ = TLS1_HB_RESPONSE;
2436                s2n(payload, bp);
2437                memcpy(bp, pl, payload);
2438
2439                r = ssl3_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload + padding);

+    /* Read type and payload length first */
+    if (1 + 2 + 16 > s->s3->rrec.length)
+        return 0; /* silently discard */
+    hbtype = *p++;
+    n2s(p, payload);
+    if (1 + 2 + payload + 16 > s->s3->rrec.length)
+        return 0; /* silently discard per RFC 6520 sec. 4 */
+    pl = p;
```

Incoming data (Payload is length)

Copy the area of memory defined by the Payload size!!!!!

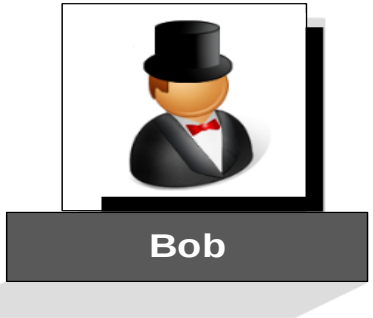
HeartBleed

Encryption

Author: Prof Bill Buchanan

172.16.121.150

OpenSSL



TLS Heartbeat reveals 64K of memory

SSL/TLS

Alice (Web)

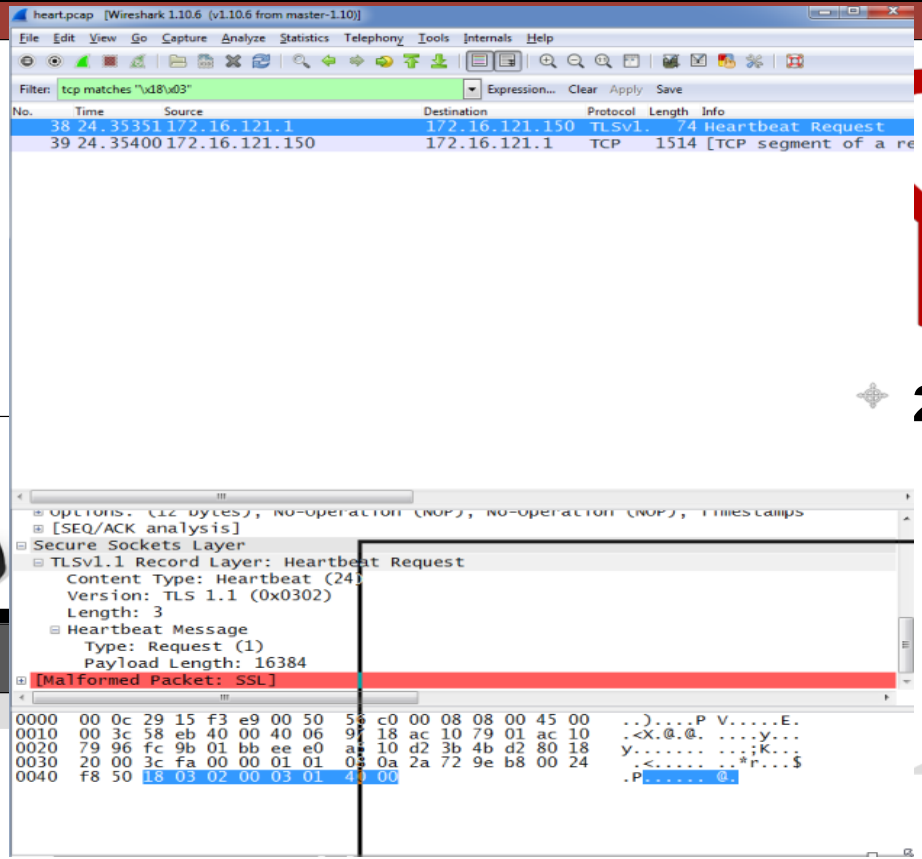
172.16.121.1

HeartBleed

Encryption

CVE-2014-0160

Author: Prof Bill Buchanan



2.16.121.150

Bob

Alice (Web)

HeartBleed

Encryption

18	03 02	00 03	1	40 00
Heartbeat	TLS 1.1	Length	Request	Payload length

Author: Prof Bill Buchanan