The Heartbleed Bug and Attack

20.1. What is the purpose of the Heartbeat protocol?

20.2. Describe what the mistake is in the Heartbleed vulnerability.

20.3. What lesson do you learn from this vulnerability?

20.4. Figure 1 shows where a malicious Heartbeat request packet is stored in the memory after it is received. The payload length field contains 0x700. Please describe which credit card numbers will be stolen by the attacker.

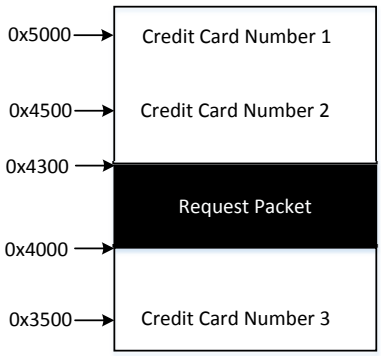

Figure 1: Figure for Problem 20.4.

20.5. Assume that the Heartbeat implementation uses the actual payload length when allocating memory for the response packet (i.e., the memory for the response packet will the same size as that for the request packet). However, during the memory copy, the claimed payload length is used. What kind of security problems does it have?

20.6. Assume that the Heartbeat implementation uses the claimed payload length when allocating memory for the response packet, but during the memory copy, the actual payload length is used. What kind of security problems does it have?