Heartbleed 漏洞与攻击

N13.1. TLS Heartbeat 协议的目的是什么？

N13.2. Heartbleed 漏洞中的具体编程错误是什么？

N13.3. 从 Heartbleed 漏洞中可以吸取哪些教训？

N13.4. 图 1 显示恶意 Heartbeat Request 收到后在内存中的位置。其 Payload Length 字段为 `0x700`。攻击者会读到哪些信用卡号？

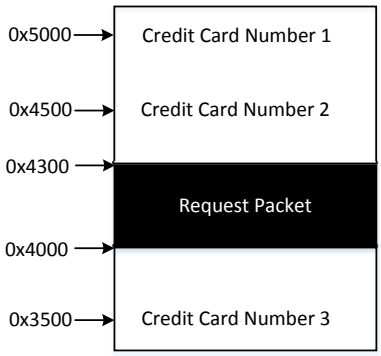

图 1: 问题图 N13.4.

N13.5. 假设 Heartbeat 实现按实际收到的载荷长度为响应分配内存，却在复制时使用报文中声明的 Payload Length。会产生什么安全问题？

N13.6. 假设实现按声明的 Payload Length 分配响应缓冲区，却按实际收到的载荷长度复制。会产生什么安全问题？