

HOMWORK 4 KEY

ENTS 689i Network Immunity
Fall 2008

Questions

1. **(10 points) What are two reasons for using layered protocols? What are two disadvantages to using layered protocols?**

An example of an advantage associated with protocol layering is that it allows protocol designers to focus on each layer independently. Another advantage of protocol layering is that, by defining well understood interfaces between layers, a given protocol layer can be easily replaced with a different implementation.

A example of a disadvantage associated with layered protocols is that often higher layers of the protocol stack are unable to optimize data transfers based on the characteristics of underlying layers. Another disadvantage is that each layer potentially imposes overhead both in terms of processing time and control information stored in protocol headers.

2. **(10 points) Consider a system with an n-layer protocol stack. Applications generate messages of length M bytes. At each of the layers, an h-byte header is added. What fraction of the network bandwidth is filled with headers? Briefly explain how bandwidth would be affected if the packets were fragmented?**

Message length = M bytes

Header length = h bytes

Protocol layers = n

Header bytes per packet = nh

Total bytes per packet = (M+nh)

Fraction of bandwidth filled with headers = $nh/(M+nh)$

If the packets were fragmented, it would result in a larger fraction of the bandwidth being filled with header information since fragments would have to replicate header information. This extra header information would increase message overhead.

3. **(20 points) In slide 17 (“Programming Example (client)”), we made a call to the subroutine htons(). What is the purpose of this function call? Please show, by filling in the boxes (in binary), how the following 32-bit number, 0x11223344, would be stored using both big-endian and little-endian byte orders. Assume big-endian bit order for both cases.**

The subroutine htons() is used to convert an unsigned short integer from host byte order to network byte order. Depending on the hardware architecture, host byte order can be either big-endian or little-endian. Thus, htons() provides a transparent software API for converting unsigned short integers to network byte order (big-endian). In the code sample discussed in

damage would be contained within the DMZ.

7. **(15 points) In class, we described a type of distributed denial of service attack called a “reflector” attack. Describe how I could use each of the following protocols to perform the attack? (Provide details as to the “type” of packet or datagram that would need to be sent to the “reflector” and the response it would generate.)**

a) (5 points) TCP

In order to use TCP to perform a reflection attack, the attackers could send a TCP SYN packet to the reflectors with the source address spoofed to be that of the victim. The reflectors would then respond by sending TCP SYN-ACK packets to the victim.

b) (5 points) UDP

In order to use UDP to perform a reflection attack, the attackers could send a UDP packet to an unused port on the reflector. The reflectors would then respond by sending ICMP port unreachable packets to the victim.

c) (5 points) ICMP

In order to use ICMP to perform a reflection attack, the attackers could send an ICMP echo request packet to the reflectors with the source address spoofed to be that of the victim. The reflectors would then respond by sending ICMP echo reply messages to the victim.

8. **(5 points) Explain what factors make defending a network from distributed denial of service such a challenging problem?**

There are a number of acceptable answers to this question. In class, we discussed two factors in particular. The first relates to the “Slashdot effect”. In general, this relates to the fact that it can be hard to distinguish legitimate traffic from attack traffic. In some instances, a large spike in traffic to your webserver may have similar characteristics and cause the same impact as a distributed denial of service attack. Another factor we discussed in class was that, while it is detected close to the victim, it needs to be stopped close to the sources. This is challenging since the sources may be globally distributed and, in the case of compromised nodes or bots, the owners may not realize they are being used to perform a denial of service attack.

9. **(10 points) One of the biggest challenges we have discussed is IP address spoofing. Does either SSL or IPSec help solve this problem? If so, how?**

10. IPSec was developed to address the security problems associated with the IP protocol, including address spoofing. As an example, the Authentication Header (AH) protocol provides authentication for IP packets by using a Hashed Message Authentication Code (HMAC) that depends on the communicating parties having a shared key. The HMAC is performed over immutable and predictable IP header fields (including the source address), the AH header, and packet payload. A truncated version of the HMAC called the Integrity Check Value is included in the AH header. Since the attacker does not know the shared key, he would be unable to disrupt communication by simply spoofing an IP address.