**CEG4430/6430 Homework 1**

(40 Points)

1. One student has designed a new transport-layer protocol, NTLP, that is completely different from the TCP or UDP. He then creates a packet that has a physical-layer header, a data-link-layer header, and an IP header. This packet contains the NTLP header and the application data payload. The packet is sent to the destination IP address as indicated in the IP header. Will this packet be delivered to the destination IP address indicated in the IP header? Please justify your answer. (5 Points)
2. Please determinate the correctness of the following statements and justify your answers (preferably by examples). (5 Points)
   1. HTTP services have to be offered at port 80.
   2. DNS services are usually offered at port 53 through UDP.
   3. An attacker has to use existing transport-layer protocols to make sure the packets are routed through the Internet.
   4. If an attacker uses UDP as the transport-layer protocol, he cannot implement reliable, connection-oriented networking service.
3. Three students, A, B, and C, share an apartment. A, B, and C have been assigned 3 IP addresses, respectively. However, there is only one Ethernet cable outlet in the apartment. Therefore, they decide to buy a device to connect three computers to the outlet. (10 Points)
   1. They have decided to buy a hub. If A wants to eavesdrop packets B sends to C, what should A do?
   2. They have decided to buy a switch. What should A do now if he wants to eavesdrop packets sent from B to C?
4. As we discussed in our lectures, a client can send a DNS request to a recursive DNS server. Then the DNS server will finally issue a DNS request to the authoritative DNS server. An attacker can send fake DNS responses, aiming at poisoning the cache of the target DNS server.
   1. Suppose the source port of the DNS request from the recursive DNS server and the ID field of the request are completely random. What is the probability for the attacker to succeed if the attacker only sends out one fake DNS response whose destination port and ID are randomly selected? (5 Points)
   2. It seems that a client can simultaneously issue many DNS requests (say *M* requests) for the same domain (e.g., cash.foo.com) to the recursive DNS server. Then the recursive DNS server will issue *M* DNS requests to the same authoritative DNS server, despite the fact that these requests look for the same domain. The source port and the ID field of these *M* DNS requests (from the recursive DNS server) will be randomly generated by the DNS server. Does this recursive DNS server facilitate the poisoning attack? Please justify your answer by quantifying the probability of success by an attacker and then comparing your result with the answer to question a. (5 Points)
5. Please read “The Collateral Damage of Internet Censorship by DNS Injection” and answer the following questions.
   1. How do the collateral damages occur? (5 Points)
   2. As a DNS request can traverse a number of routers along a path, and each router along the path can inject fake DNS responses. What are the techniques used by the researchers of the paper to identify the router(s) that actually inject fake DNS responses? (5 Points)