George Jone

913177426

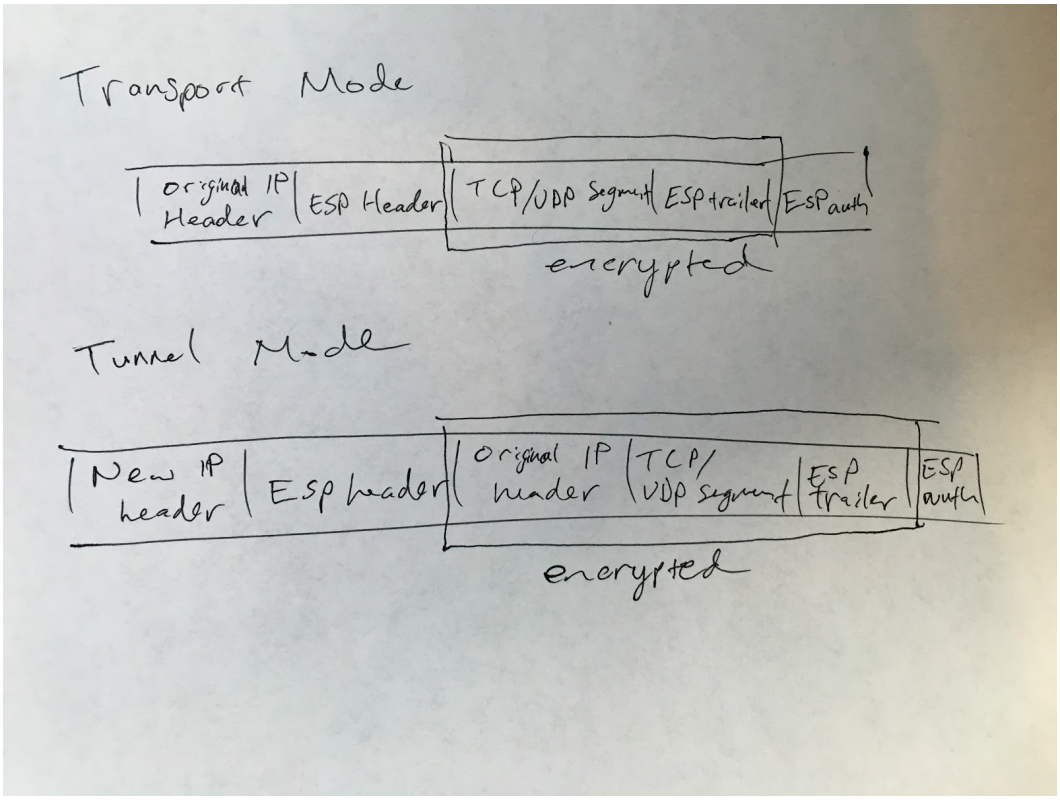
Due: 7:00PM, Wednesday, 04/20/2016

CSC650 Secured Network Systems

Homework 3

1. Phishing is falsely claiming to be from authority in hopes of extracting private information. The attacker makes you think you are in one place you trust, when in fact you are not. An example is fraudulent Instant messages. Baiting is creating a “lure” object and letting the victim come to you. An example is a link to porn movie (.mov), which is actually an executable on the website
2. The Application layer is for supporting network applications. The Transport layer is for process-process data transfer. The Network layer is for routing of datagrams from source to destination. The Link layer is for data transfer between neighboring network elements. The Physical layer is the actual bits “on the wire”.
3. The Transport layer is the layer in the Internet protocol stack where the TCP sequence prediction attack occurs. The Network layer is the layer where the routing manipulation attack occurs
4. The TCP sequence prediction attack is where an attacker guesses QS to get S to accept whatever data it wants. It can use the TCP three way handshake to establish a connection. To prevent it you stop making the sequence numbers predictable by randomizing them.
5. The three components in IPsec are IKE, AH, and ESP. Internet Key Exchange (IKE) establishes security association containing keys and cryptographic algorithms for AH and ESP. Authentication Header (AH) provides origin authentication and data integrity. Encapsulating Security Payload (ESP) provides origin authentication, data confidentiality and integrity.

6. Draw the structure of the datagram transmitted in Transport Mode and in Tunnel Mode, respectively, when AH is used. (10 Points)

a. 

7. The DDoS attack is a Distributed Denial of Service attack. DDoS is a Network oriented attack that aims at preventing access to host, network, or service. It saturates the target's network with traffic, consumes all network resources, overloads a service with requests, uses "expensive" requests. The IP address is often spoofed. ICMP Traceback is when forwarding packets, routers generate a Traceback message that is sent along to the destination. You include the information on previous hop and next hop of the packet. It generates with low probability, and the target can determine the source and reconstruct the path.