1. First of all, Jill should never be given responsibility ever again. Jill runs a lot of risk allowing her WiFi to be open. A person can use a packet analyzer to see the traffic of Jill and her neighbors. Changing her router settings could run a DNS spoofing attack by changing her DNS and add or remove data Jill sends and receives.
2. 20 bytes for the header and 16 bytes for the footer. For UDP, there is no need for the checksum so only 12 bytes for the footer.
3. I can XOR my private key with the private key of the server, and then encrypt that whole with my key. I should decrypt with my key and then use the public key of the server. If the message decrypts correctly, everything is okay. If the message is messed up, then mitm has occurred.
4. SYN Cookies use more CPU time now that memory, so an attack could throttle enough CPU by continuing the connection and then immediately closing it. Introducing latency like this would slow down the server.
5.
6. 32768 fake responses.
7. An IDS can see a signature from the same source IP trying different destination ports and notify a manager outside the network.
8. Ack = 883790340, Seq = 156955004
9. A third party could forge a tcp packet from one of the computers, set the RST flag to 1, and terminate the connection. If a packet sniffer is available, then the IPs and ports are easy to grab and forge. If a packet sniffer is not available, then the third party could try sending a malicious packet that could violate one of the computer’s firewall and close the connection.
10. If the source IP of the packet doesn’t match any of the IPs in the internal network, the packet should be filtered out.
11. The DNS cache might’ve been supplanted in other parts of the network, for example an ISP DNS cache. In which case, even if the local DNS TTL expires, the ISP DNS will still give the incorrect address.
12. A router should not forward any ICMP packet to its targeted to broadcast addresses.