Collection of questions with answers from paper submission, mostly unedited except for few additions.

Note that questions in the final will appear in different formats within the content and concepts covered by the following questions.

**GROUP 1** - multiple Choice Type (corrected answers are in bold face)

1. What VPN technologies are most prevalent today?
   a. **SSL, IPSec**
   b. IPSec, PPTP
   c. L2TP, SSL
   d. MLPS, IPSec

2. T/F SSL VPN provide good site to site connectivity where UDP traffic is involved.

3. VPN stands for:
   a. Varied Packet Network
   b. Virtual Page Negotiation
   c. **Virtual Private Network**
   d. Virtual Paged Network

4. T/F SSL VPN are marketed as a clientless VPN technology.
   (Which VPN marketed as clientless VPN technology?)

5. IPSec and **SSL** are the two dominate VPN technologies today.

6. What is E-Government?
   a. **E-Government establishes common standards across government, delivering services more effectively, and providing ways for agencies to work together using technology**
   b. A website to learn about education facilities
   c. A place to find information about politicians
   d. A place in Washington

7. All of the following are general services that E-Government provides except
   a. **File taxes**
   b. Renew driver's license
   c. **Renew vehicle registration**
   d. Check your grades

8. What is Authentication?
   a. **security feature that makes sure people are who they say they are so that the right people are given access to the right information or service**
   b. a type of website program
   c. A type of computer language
   d. All of the above

9. What is the purpose of GovNet?
   a. **protect government data and infrastructure**
   b. evaluate government websites
   c. raise money for government websites
   d. none of the above

10. After 911 the public holds E-Government accountable for
    a. **favor of a mechanism to aid in protecting the U.S. from further terrorist attacks.**
    a. Punishing hackers
    b. All problems online
    c. All of the above
11. How do you identify a secure site? Circle all that are correct.
   A. http
   B. https
   C. the open pad-a-lock
   D. the locked pad-a-lock

12. Security includes all of the following topics except:
   A. non-repudiation
   B. integrity
   C. privacy
   D. RSA
   E. authentication

13. SET stands for
   A. Secure Electronic Transfer
   B. Secure Electronic Tunneling
   C. Someone Else Thinking
   D. Super Electronic Tunneling

14. Secure Sockets Layer
   A. uses handshaking to create a secure connection
   B. uses polling to create a secure connection
   C. sits on top of the application layer
   D. opens a connection that is only closed by the user when they choose to do so

15. Which of the following is not true of Certificate Authorities?
   A. they are unbiased
   B. there are many of them
   C. they provide authentication
   D. they provide certificates

16. Which of these uses Public Key Infrastructure (PKI) and digital certificates to provide privacy and authentication?
   A. DES
   B. TLS
   C. SET
   D. SSL

17. What characteristics make passwords more secure?
   a. Length
   b. Doesn't contain dictionary words
   c. Contains special characters (%, &, #, etc)
   d. All of the above

18. An unsophisticated user that downloads malicious software from websites and follows posted instructions to carry out attacks on the internet is called a(n):
   a. Hacker
   b. Script Kiddy
   c. Neo
   d. Agent

19. What does 'DOS' stand for when referring to an internet attack?
   a. Denial Of Service
   b. Disk Operation System
   c. Department Of State
   d. Distributed Overhead System
20. What was the first security measure implemented in very early computer systems?
   a. Biometrics
   b. Encryption
   c. Physical
   d. Emotional

21. What is NOT an internet protocol used for security?
   a. SSL
   b. SHTML
   c. SHTTP
   d. SSH

22. Which of these will make you safer from Trojans?
   a. Using an alternative OS
   b. Always using the onscreen keyboard to enter credit card data
   c. Use an Anti-Virus Software
   d. All of the Above

23. What is one thing a Trojan does?
   a. Protects your computer from advertisements
   b. Logs your keystrokes
   c. Improves virtual memory efficiency
   d. Causes your power supply to overheat

24. Who can make money off of spyware?
   a. The spyware company
   b. The person who bundles the spyware with their software
   c. The person whose computer is infected with spyware
   d. Both A and B

25. What is one commercial product that could be considered spyware?
   a. PCanywhere
   b. Trojacom
   c. Dataconnector
   d. Net Stagger

26. Roughly what percentage of companies monitor their workers computer usage?
   a. 25%
   b. 50%
   c. 75%
   d. 95%

Group 2 - Short answer type

1. Name four different types of attacks.
   - Denial-of-service attacks, including SYN floods and surfing
   - Disclosure of information, such as theft of credit card numbers
   - Destruction of data, which can be an act of economic terrorism
   - Alteration of data, such as grade fixing

2. What are the two layers of the Transport Layer Security (TLS) and what does each do?
   **TLS Record Protocol** - Provides connection security with an encryption method such as the Data Encryption Standard (DES).
   **TLS Handshake Protocol** - Allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged.
3. What are the four secure electronic transaction essentials and what does each mean?

   - Privacy - sender and receiver expect all interactions to be confidential
   - Authentication - receiver is assured of the sender’s identity
   - Integrity - data arrived at the receiver site exactly the way it was sent
   - Non-repudiation - receiver is able to prove the message came from a specific sender

4. What is the purpose of a digital signature?
   Verifies a user sending a message is who he or she claims to be and provides the receiver with means to encode a reply

5. Explain affect of cyber terrorism with examples.
   Cyber-terrorism is an organized attack on a computer network which is designed to cause loss of life and/or widespread social disorder by disrupting vital infrastructure and economic activity. Recent attempts at cyber-terrorism include the October 2002 Denial of Service attack on the internet and the January 2003 SQL Slammer attack, which crippled northwestern metropolitan emergency 911 networks. These can be considered warning signs of how cyber terrorism might be deployed to increase the damage caused by conventional terrorism.

6. Explain the term SSL.
   Secure Socket Layer (SSL) is the industry standard protocol for secure, web-based communications and transactions. SSL provides message security by encrypting all information exchanged between the web server and the consumer's browser. SSL is typically used for transactions involving a credit card but can be used for any transaction requiring a heightened level of privacy. SSL also provides message integrity by checking the data received and alerting the recipient that the message is not legitimate if it fails the check.

7. How the use of HTML frames can deceive users for checking if a site is secure or not?
   An important thing to remember when checking out whether or not a site is secure is that the use of frames on the webpage can deceive users. HTML Frames allow the webpage designer to separate the page into separate files so header and navigation information can remain in one file that is reused from page to page and page specific information can be separated into its own file. The problem is that the header file might seem secure, but the page specific file where all of the valuable information is might not really be secure.

8. When and why was SET created?
   Secure Electronic Transfer, SET, was developed by Visa and Mastercard to provide a secure way to make electronic payments with a credit card over the Internet. It is not a good idea to send credit card information over the internet without taking adequate security measures. SET, created in 1996, not only encrypts credit card information, but also uses digital signatures to ensure that the credit card transaction was authorized.

9. Explain how is SET secure for online transactions?
   Secure Electronic Transfer, SET, provide a secure way to make electronic payments with a credit card over the Internet. It not only encrypts credit card information, but also uses digital signatures to ensure that the credit card transaction was authorized.

   There are four parties involved in a secure electronic transfer. They are the customer, the merchant, an Acquirer Gateway, and a Certificate Authority. The customer and the merchant are obvious; the Acquirer Gateway takes care of transferring the money between the customer and the merchant. The Acquirer Gateway is responsible for ensuring that the customer authorizes the transaction. The Certificate Authority is unbiased to the three other parties. The job of the Certificate Authority is to distribute digital certificates that authenticate the different parties.

   There are several steps involved in a secure electronic transfer that makes it safe. First, the customer initiates an order with the merchant. Secondly, the merchant verifies electronic funds with the Acquirer Gateway. The third step involves the Acquirer Gateway replying to the merchant with an authorization of the purchase and verifies the merchant's certificate. Then the merchant confirms the order to the customer in the fourth step. Step five is where the merchant gets to request the funds
from the Acquirer Gateway. This whole process safeguards the customer’s credit card information. In the Secure Electronic Transfer, the digital certificate is almost impossible to fake. It would take 100 computers, trying 10 million certificates per second, $2.8 \times 10^{12}$ years to break the system. And even that would only break one message; the whole process would have to start over for the next message.

10. Explain briefly the term phishing scam.
   In computing, phishing is the luring of sensitive information, such as passwords and other personal information, from a victim by masquerading as someone trustworthy with a real need for such information. It is a form of social engineering attack.
   Typically, a phishing email will appear to come from a trustworthy company and contain a subject and message intended to alarm the recipient into taking action. A common approach is to tell the recipient that their account has been de-activated due to a problem and inform them that they must take action to re-activate their account. The user is provided with a convenient link in the same email that takes the email recipient to a fake webpage appearing to be that of a trustworthy company. Once at that page, the user enters her personal information which is then captured by the fraudster.

11. How do you protect from phishing scam on the Internet?
   The best way to protect yourself from a phishing scam is to make sure that you always know what website you are at. Checking the URL in the address bar of the browser may not be sufficient, as, in some browsers, that can be faked as well. However, the file properties feature of several popular browsers may disclose the real URL of the fake webpage. If you are contacted about an account needing to be "verified," you should contact the company directly, or always go to your browser and type the address in instead of clicking on suspicious links.

12. Name at least four packet filtering criteria used by firewalls.
   - Source IP address
   - Destination IP address
   - TCP/UDP Source port
   - TCP/UDP Destination port
   - Packet type

13. What is application layer proxy?
   An application proxy is a program running on a firewall that emulates both ends of a network connection. It acts as a sort of "translator" in-between two computers communicating. Each computer communicates with the other by passing all network traffic through the proxy program. The proxy program evaluates data sent from the client and decides which to pass on and which to drop. Communications between the client and server occur as though the proxy wasn't there, with the proxy mimicking the client when talking with the server, and the server when talking with the client.

14. What is the function of HTTP proxy?
   Each different application has its own proxy program that emulates the application's protocol. An HTTP proxy program emulates the hypertext transfer protocol.

15. Explain what is SHTTP?
   Secure Hyper Text Transport Protocol (SHTTP) is a secure message-oriented communications protocol designed for use in conjunction with HTTP. Since SHTTP was designed to be used in conjunction with HTTP, it uses the same transaction model (uses port 80) and implementation characteristics of HTTP, this makes SHTTP easy to implement. SHTTP simply changes the protocol designator to tell the system that this is in fact a SHTTP packet.