Vocabulary

Asset Authentication- A security method of guaranteeing that a message is genuine, that it has arrived unaltered, and that it comes from the source indicated.
Availability-Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts.
Confidentiality-Confidentiality is roughly equivalent to privacy. Measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong people, while making sure that the right people can in fact get it: Access must be restricted to those authorized to view the data in question.
Integrity-Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). These measures include file permissions and user access controls.
Risk-The level or amount of exposure to an item when compared with other items. It is a hazard or chance of loss. Risk is the degree of difference, as in, "What level of risk does one threat have when compared to the other threats?"
Biometric System- A biometric system is a technological system that uses information about a person (or other biological organism) to identify that person. Biometric systems rely on specific data about unique biological traits in order to work effectively
Brute Force Attack - A way of breaking an encrypted message by trying all possible values of the key.
Denial of Service Attack (DoS Attack)- A DoS attempts to disrupt the network by flooding the network with messages so that the network cannot process messages from normal users
IP Spoofing- IP Spoofing is a technique used to gain unauthorized access to machines, whereby an attacker illicitly impersonate another machine by manipulating IP packets. IP Spoofing involves modifying the packet header with a forged (spoofed) source IP address, a checksum, and the order value.
Business Continuity - is the ability of an organization to maintain essential functions during, as well as after, a disaster has occurred
Disaster Recovery - (DR) involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster
Packet Level Firewall - A Packet Level Firewall protects an internal network against unauthorized access and attack from a public or external network by blocking some

packets. Packets may be blocked based on source IP address, destination IP address, source or destination TCP port number, other packet header fields, time of day or user authentication.

Cryptography - Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Symmetric - One Key Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys.

Key - a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

Key Management -Key management is the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

Asymmetric Encryption - is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt. Frequently (but not necessarily), the keys are interchangeable, in the sense that if key A encrypts a message, then B can decrypt it, and if key B encrypts a message, then key A can decrypt it.

RSA - is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

Public and private key - symmetric Keys. Asymmetric keys, also known as public/private key pairs, are used for asymmetric encryption. ... The public key of a key pair is often distributed by means of a digital certificate. When one key of a key pair is used to encrypt a message, the other key from that pair is required to decrypt the message.

Public Key Infrastructure (PKI) - A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Certificate Authority (CA) -In cryptography, a certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
Data Encryption Standard (DES) - is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit.
Triple DES (3DES) - Triple DES (3DES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.
Advanced Encryption Standard (AES) - is a symmetric block cipher used by the U.S. government to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.
Kerberos - is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology. Kerberos is available in many commercial products as well.
Secure Socket Layer (SSL) - is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
IP Security Protocol (IPSEC)- is a protocol suite for secure Internet Protocol (IP) communications that works by authenticating and encrypting each IP packet of a communication session.
IPSec Tunnel Mode - When IPSec tunnel mode is used, IPSec encrypts the IP header and the payload, whereas transport mode only encrypts the IP payload. Tunnel mode provides the protection of an entire IP packet by treating it as an AH or ESP payload.

Networking:

1. What factors have brought increased emphasis on network security?
   - Securing info from hackers & recovering any datas that has been lost.

3. Main impact areas:
   - financial - revenue & expenses
   - Productivity: business operations
   - Reputation - customer perceptions
   - Safety - health of customers & employees
   - Legal - potential fines & litigation.

5. common threats:
   viruses, theft of equipment, theft of information, device failure, natural disaster, sabotage, denial of service.

7) Q: What is the purpose of the risk score & how it is calculated

- Risk scores are used to compare the risk scores among all the different threat scenarios to help us identify the most important risks we face! It is calculated by multiplying the impact score by the likelihood (using 1 for low likelihood, 2 for medium likelihood, & 3 for high likelihood)

8 documenting existing controls is the fourth step in the process.

9. Four Risk Control Strategies: D.A.M.S
1. Accept the risk, mitigate it, share it, defer it.

10. Q: Why IS it important to identify improvements that are needed to mitigate risks?
A. Because risks are always changing; responses (including technologies) are changing as well.

11. The most important element of the disaster recovery plan are:
back up
recovery control

12. Computer virus:
Computer program that multiplies itself to create some unwanted events.

Macro virus:
Virus contained in documents or spreadsheets

Worm:
Virus without human intervention.
It spreads on its own.

13. DOS (Denial of Service):
- attacker sending massive message (flooding) to interrupt the network.

14. DOS - single computer
DDOS - can involve hundreds of computers.

19. Disaster Recovery firm: provide second level support for major disasters.

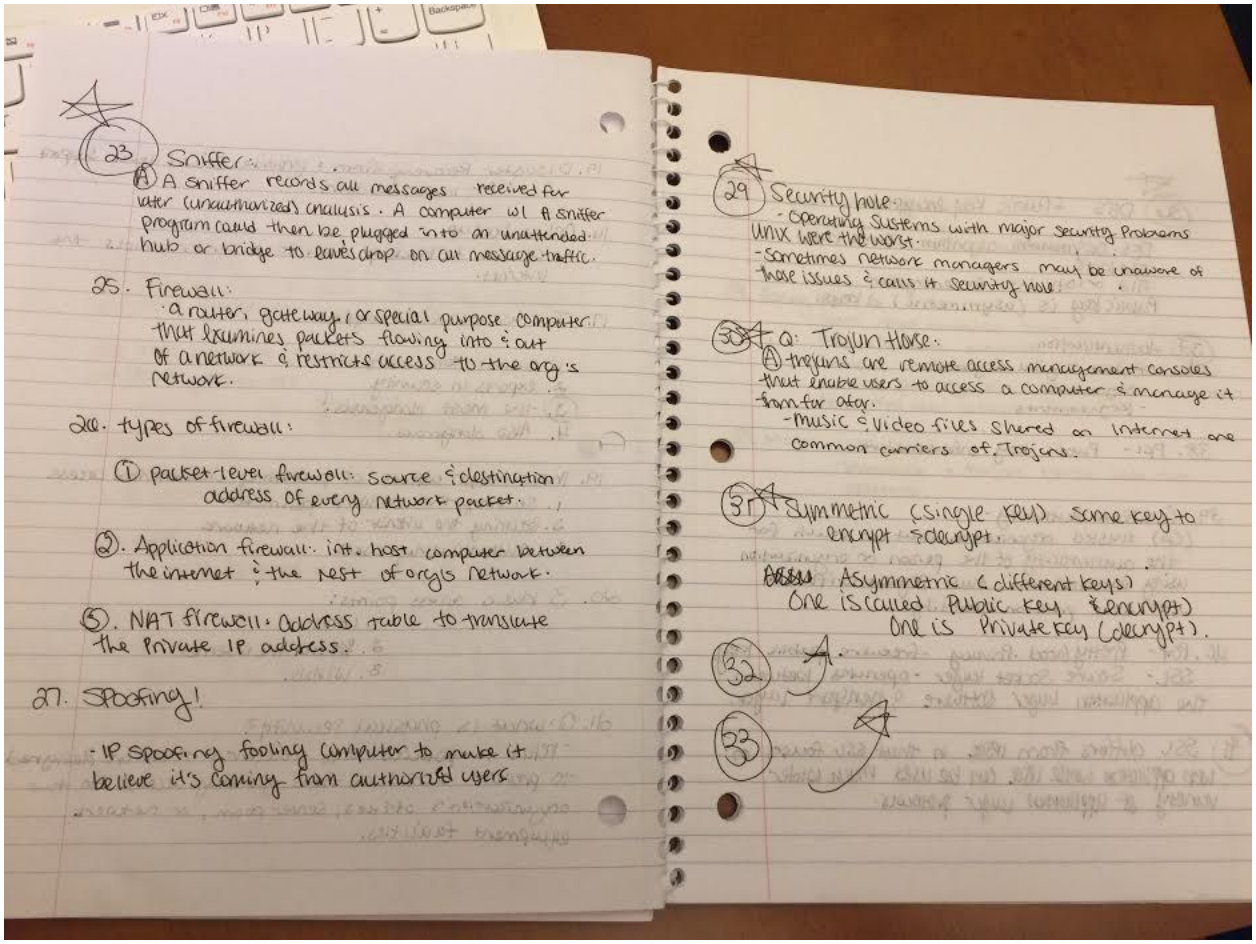
16. Online backup:
allows to backup data to a server across the internet.

17. Intrusions (four type)
1. casual computers
2. experts in security
3. the most dangerous!
4. Also dangerous.

19. Three major aspects of preventing unauthorized access
1. Securing the network perimeter
2. Securing the interior of the network
3. authenticating users.

20. 3 basic access points:
1. LANs
2. ~~from~~ the internet
3. WLANS.

21. Q: What is physical security?
- refers to policies and procedures that are design to prevent outsiders from gaining access to the organization's offices, server room, or network equipment facilities.



23 Sniffer:
A sniffer records all messages received for other (unauthorized) analysis. A computer w/ a sniffer program could then be plugged into an unattended hub or bridge to eavesdrop on all message traffic.

25. Firewall:
a router, gateway, or special purpose computer that examines packets flowing into & out of a network & restricts access to the org's network.

26. types of firewall:

① packet-level firewall: source & destination address of every network packet.

② Application firewall: int. host computer between the internet & the rest of org's network.

③ NAT firewall: address table to translate the private IP address.

27. Spoofing!

- IP spoofing fooling computer to make it believe it's coming from authorized users

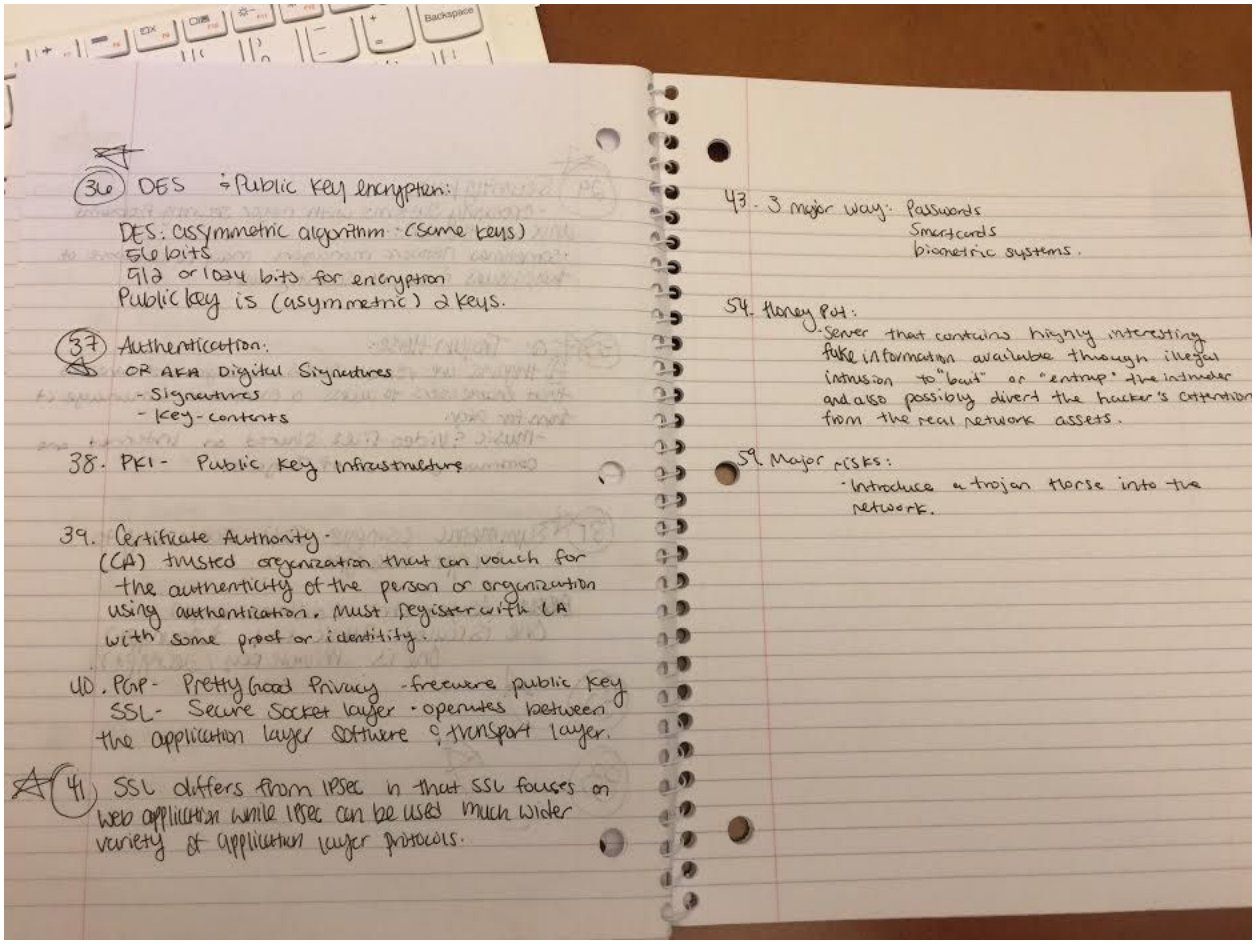
29 Security hole:
- Operating systems with major security problems Unix were the worst.
- Sometimes network managers may be unaware of those issues & calls it security hole.

30 Q: Trojan Horse:
A trojans are remote access management consoles that enable users to access a computer & manage it from far ofer.
- music & video files shared on internet are common carriers of Trojans.

31 Symmetric (single key) same key to encrypt & decrypt.
Asymmetric (different keys)
One is called Public key (encrypt)
One is Private key (decrypt).

32

33



36) DES & Public key encryption:

DES: assymmetric algorithm (same keys)
56 bits
Old or today bits for encryption
Public key is (asymmetric) 2 keys.

37) Authentication:
OR AKA Digital Signatures
- Signatures
- key-contents

38. PKI - Public key infrastructure

39. Certificate Authority:
(CA) trusted organization that can vouch for the authenticity of the person or organization using authentication. Must register with CA with some proof or identity.

40. PGP - Pretty Good Privacy - freeware public key
SSL - Secure Socket layer - operates between the application layer & transport layer.

41) SSL differs from IPSec in that SSL focuses on web application while IPSec can be used much wider variety of application layer protocols.

43. - 3 major way: Passwords
Smartcards
biometric systems.

54. Honey Pot:
- Server that contains highly interesting fake information available through illegal intrusion to "bait" or "entrap" the intruder and also possibly divert the hacker's attention from the real network assets.

59. Major risks:
- Introduce a trojan horse into the network.