Topic 21 Networks – Summary

Vocabulary

network security (n): activities designed to protect a network and its data from threats such as viruses, hacker attacks, denial of service attacks, data interception and theft, and equipment failure.

confidentiality (n): ensuring that information is accessible only to those authorized to view it. Confidentiality prevents unauthorized disclosure.

data integrity (n): data is accurate and consistent.

accessible (n): information and systems are accessible when needed

denial of service (**DoS**) (adj): an attack on a network that attempts to prevent the legitimate users from accessing its services. More details in the *Concepts* section.

network service (n): an application running on a server which provides facilities or operations such as data storage, printing, or communications.

hacking (v): exploiting technical vulnerabilities to gain unauthorized access or achieve a specific outcome

social engineering (n): the psychological manipulation of people into performing actions or divulging confidential information.

Concepts

The CIA Triad: Confidentiality, Integrity, and Availability

The CIA Triad – *confidentiality*, *integrity*, and *availability* – is the cornerstone model of information security, representing the three fundamental objectives that guide protection measures for data and systems. Think of it as the three-legged stool of security: if any leg is weak or broken, the entire structure collapses.

Confidentiality – secrets are kept secret

Ensuring that information is accessible only to those authorized to view it. Confidentiality prevents unauthorized disclosure.

This is accomplished by: encryption, passwords and access controls, implementing need-to-know principles, preventing data leaks or eavesdropping.

Attacks include: interception (packet sniffing, man-in-the-middle attacks, session hijacking), unauthorized access (password cracking, SQL injection, key logging, remote access viruses, spyware) physical theft (stolen computer, shoulder surfing), or social engineering (phising, pretexting, intimidation).

Integrity – information is accurate and unaltered

Maintaining the accuracy, consistency, and trustworthiness of data throughout its lifecycle. Integrity prevents unauthorized modification.

This is accomplished by: using cryptographic hash functions to detect file tampering, database constraints and validation rules, digital signatures for emails and software, and version control and audit logs.

Attacks include: data tampering, malware injection, man-in-the-middle attacks, unauthorized edits.

Accessibility - information and systems are accessible when needed

Guaranteeing that authorized users have reliable and timely access to information and resources.

This is accomplished by: redundant servers and load balancing, DDoS protection services, regular system maintenance and backups, disaster recovery plans.

Attacks include: denial-of-service (DoS/DDoS) attacks, ransomware that locks data, hardware failures, network outages.

Denial of Service (Dos) Attack

A *denial of service* (DoS) attack is a malicious attempt to make a network resource, server, or website unavailable to its intended users. A DoS attack is accomplished by overwhelming the target with more requests or traffic than it can handle, exhausting its resources (like bandwidth, CPU, memory, or connection states).

If a denial of service attack comes from one, or a small number of machines, one method of defense is to block the originating IP address(es). A ***distributed denial of service*** (**DDoS**) attack originates from a ***botnet*** – a vast network of often thousands or millions of compromised machines distributed worldwide. It is very difficult to defend against, as distinguishing whether a request is coming from a legitimate client or a machine in the malicious network is nearly impossible.

The Pearson IG CSc textbook almost makes it sound like DoS can delete data, eavesdrop, etc. This is incorrect. The DoS only affects data *availability*, not *confidentiality* or *integrity.*