### [**3413ICT Network Security**](file:///D:\Profiles\user\My%20Documents\Teaching\Courses_2003\6216INT_03\6216inthome.html)

### **Workshop – 7A**

|  |
| --- |
| **Review Questions:**   1. Explain the DAD triad and CIA triad for information (systems/ networks) security, and the relation between DAD triad and CIA triad.  * DAD   + **Disclosure:** unauthorized individuals gain access to confidential information   + **Alteration**: data is modified through some unauthorized mechanism   + **Denial (or Destruction):** authorized users cannot gain access to a system for legitimate purposes * CIA   + **Confidentiality:** confidential information should not be accessible to unauthorized users   + **Integrity:** data may only be modified through an authorized mechanism   + **Availability:** authorized users should be able to access data for legitimate purposes as necessary   Essential they both stand for the same thing using different words.   1. List and explain some of the challenges of implementing security mechanisms to a computer network.  * Not simple * Must consider potential attacks * Involve algorithms and secret information * Must decide where to deploy mechanisms * Battle of wits between attacker / admin * Not perceived on benefit until fails * Requires regular monitoring * Regarded as impediment to using system  1. Describe the model for network security. What are required for using this model?    1. have a suitable algorithm for the security transformation      * 1. generate secret information (keys) used by the algorithm      * 1. develop methods to distribute and share the secret information   2. specify a protocol enabling the principals to use the transformation and secret information for a security service      1. Describe the model for network access security. What are required for using this model?    1. select appropriate gatekeeper functions to identify users    2. implement security controls to ensure only authorised users access designated information or resources          1. Name and explain six characteristics of a computer network.  * Topology * Availability * Speed or Bandwidth * Reliability * Security * Scalability  1. Explain the benefits of modelling a computer network by using a layered structure.  * Reduced complexity * Easier to develop * Simple to learn * Standard interfaces * Multi-vendor interoperability * Facilitates modular engineering * Accelerate evolution  1. Explain the seven layers of the OSI reference model for computer networks. 2. Briefly explain the procedure of internet packet encapsulation in TCP/IP.   Each layer warps around the other layer. For example the Application layer is wrapped with the presentation header. The presentation header is wrapped with the session header, etc. Transport layer is added on top of the Network later so the packet would look like this: [ IP HEADER | TCP / UDP HEADER | UPPER LAYER HEADER | APPLICATION LAYER DATA]   1. What is a protocol for data communications? Explain the following two types of protocols: connectionless protocol and connection-oriented protocol. Give an example for each type.   Protocols are broadly classified as connectionless and connection oriented   * **Connectionless protocol** * Sends data out as soon as there is enough data to be transmitted * E.g., user datagram protocol (UDP) * **Connection-oriented protocol** * Provides a reliable connection stream between two nodes * Consists of set up, transmission, and tear down phases * Creates virtual circuit-switched network * E.g., transmission control protocol (TCP)  1. List and explain the two versions of the Internet Protocol (IP), which are both used currently. Explain the security mechanisms in IP.   IPV4: IPv4 is a connectionless protocol for use on packet-switched networks. It operates on a best effort delivery model, in that it does not guarantee delivery, nor does it assure proper sequencing or avoidance of duplicate delivery. These aspects, including data integrity, are addressed by an upper layer transport protocol, such as the Transmission Control Protocol (TCP).  IPV6: is the latest version of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.  Both may implement IPSec. Some of the features that IPSec implements are: Confidentiality, Authentication, and Data Integrity. Confidentiality is achieved by encrypting the payload by using ESP architecture.   1. What is ICMP?  * One of the core protocols of TCP/IP * It is used by devices   + to send error messages indicating, for example, that a requested service is not available   + or that a host or router could not be reached   + It is also used to relay query messages * ICMPv6 is for IPv6 (while ICMPv4 was for IPv4)  1. List and explain two security attacks that use ICMP.   ***Network discovery*** (e.g., sending ICMP echo request to a host and waiting for response)  ***Smurf DoS attack*** (using the address of the victim, a malicious host can broadcast a ping request to many computers; then the responses can cause the victim to crash   1. Explain the differences between UDP and TCP.   UDP:  Connectionless protocol  Provides limited error-checking  Provides best effort delivery  Has no data recovery features  TCP:  Connection-oriented protocol  Error checking  Sequencing of data packets, acknowledgement of receipt  Data-recovery functions   1. Explain what SNMP is.   Simple network management protocol: Supported by most network equipment manufacturers   * Operates at the application layer * Allows administrators to remotely monitor, manage, and configure network devices * It functions by exchanging management information between network devices * Each SNMP-managed device has an agent or service   + Listens for and executes commands  1. Compare the two protocols for email services: POP and IMAP.     POP: -Allows you to download message from the server without a copy left behind  -After downloading with one computer, you cannot access the message from another computer  -Better use of the storage space of the server  IMAP:  -IMAP stores messages directly on the mail server, even after you've accessed your e-mail from your home computer  -IMAP e-mail takes up more of your available storage on the server  You can have access to your e-mail from multiple locations |

**Hands-on Exercises:**

In the second half of the semester, the hand-on exercises consist of several networking projects to be done by using OPNET IT Guru Academic Edition, with a particular interest in network security issues. You may spend up to two days (using the workshop times) to complete the project.

Please see the first project (Lab 1) on the course website.