SECURITY SYSTEM ANALYSIS AND PLANNING

1. Objectives

- To practice the formal procedure of system/network security analysis and planning.
- To examine the vulnerability and security need of a university campus network.
- To devise strategies to overcome system vulnerability.

2. Target Network

Consider a simple Internet deployed on a campus of a small university. Figure 1 on the next page depicts the overall topology of such a network. The Internet is divided into four *sub-networks*, each of which has its own internet address range:

- *Administrators' and Officers' Subnets* — These networks are used by the officers (principal, provoke and faculty members) as well as the administrators (technicians and secretaries) of the university; this part of the Internet is subdivided into two layer-two subnets, *Officers' Subnet,* which is used by the officers to conduct high-level management of the university and *Administrators' Subnet,* which is used by the administrators to handle daily operation of the school; note that these two subnets are separated merely by a layer-two switch and thus share a contiguous range of IP addresses.
- *Student Subnets* — It is the biggest sub-network on campus, and is designated to be used by all the students to meet their computational and communicational needs. This subnet consists of two hardware sub-structures, the *Dial-In Subnet* uses a bank of high-speed telephone modems to provide off-campus students with remote-access services and the *On-campus Subnet* is made up of personal computers scattered over the campus. Although the hardware structures of these two component networks are different from one another, they nonetheless share a contiguous IP address range. Certain segments of this address space is used by the Dial-In Subnet and administrated by the Dynamic Host Connectivity Protocol (DHCP).
- *Teaching Subnet* — This sub-network consists of computers and other networking equipment used in various teaching laboratories. The subnet is made up of multiple layer-two networks, each may have its own hosts, servers and switches, but they share a contiguous IP address range.
- *Research Subnet* — This sub-network contains all the computing and communication devices scattered across all the research laboratories and offices. Again, this subnet is made up of multiple layer-two networks, each has its own hosts, servers and switches, but they share a contiguous IP address range.

These subnets are all connected to the external public Internet through a gateway router.

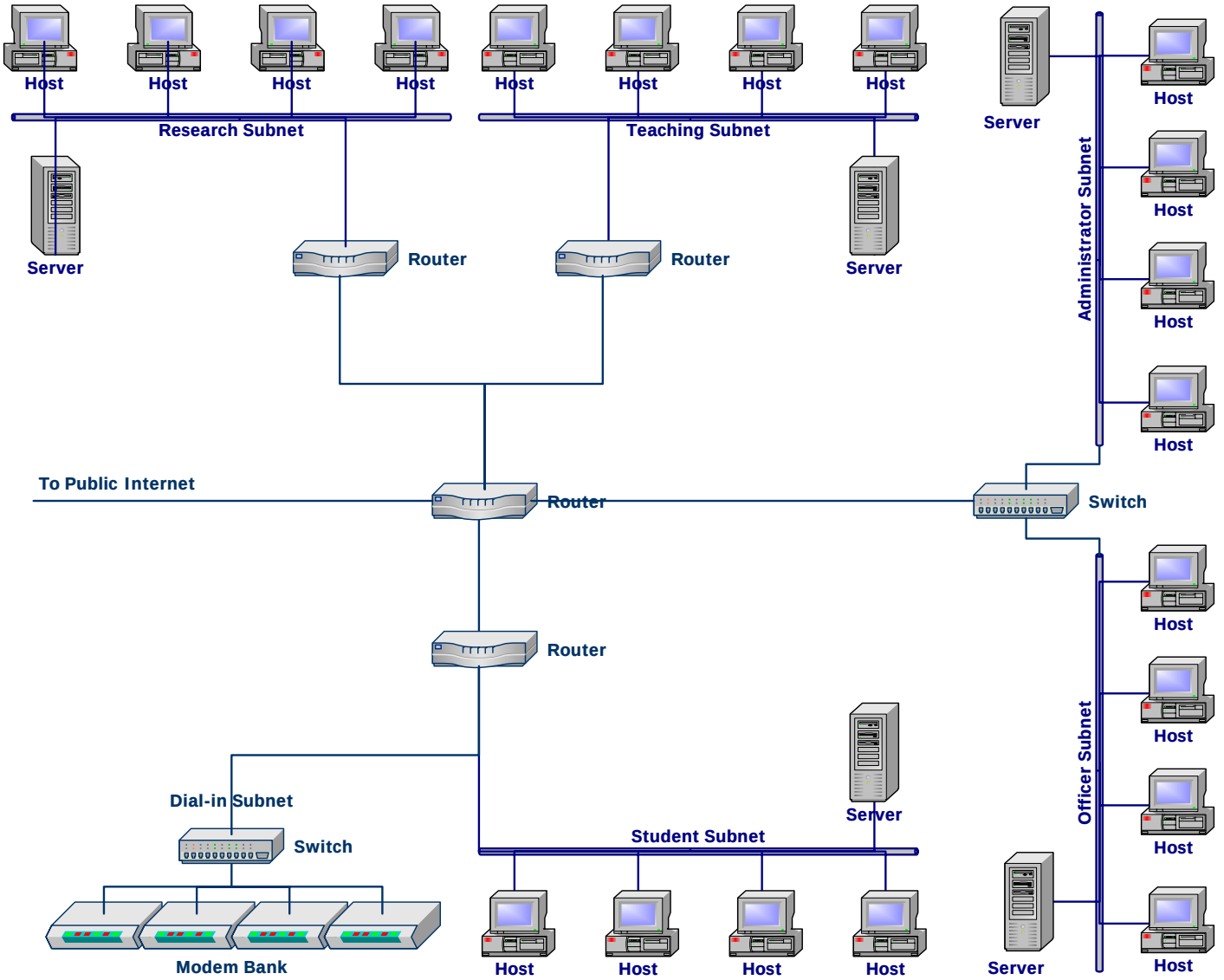

Figure 1: Topology of University Campus Internet

3. Assignment Detail

This homework assignment contains the following three consecutive parts:

1. *Vulnerability Assessment* — In this part, you are asked to identify potential weakness (vulnerability) of this campus Internet, and of its individual sub-networks.
2. *Security Service Selection* — In this part, you are asked to propose prioritized set of services to amend the vulnerability of individual sub-networks and hence the overall campus Internet. Note that the proposed services must be prioritized so that they can be implemented in proper order under existing financial constraints.
3. *Network Architecture Recommendation* — In the process of vulnerability analysis and security service selection, you may discover weak points in the current network architecture. They may also discover the need to implement selected security services at some crucial sites in the network. Students are encouraged to report their finding of network architecture weakness and security deployment sites.

3.1 Vulnerability Assessment [Grading: 50%]

The aim of *vulnerability analysis/assessment* is to identify a prioritized set of threats that are relevant to a particular system for a specific set of users and applications under a specific set of conditions. The practice often yields one or more *threat matrix(ces)*, each of which tabulates both general (top-level) and application/user specific (lower-level) threats.

In order to limit the workload of this homework, you are asked to complete the following *threat matrix* for two (2) subnets of the campus Internet: *Officers' Subnet* and *Students' Subnet*. Note that the threats posted by different users and applications used on these subnets might be quite different. Only two applications, Electronic Mail (Email) and Web Browsing, are to be considered in the vulnerability analysis of each subnet. Depending on the subnet, the network users may include students, faculty members, university visitors, officers and administrators. For the sake of simplicity, we assume that only the faculty members will use the Officer Subnet, and only the students will use the Student Subnet.

General Threats	Confidentiality	Integrity	Availability	Resource Abuse	...
Application Specific Threats					
Email					
Web Browsing					

3.2 Service Selection [Grading: 50%]

After performing the vulnerability analysis, you are asked to determine the security services that should be employed in order to protect the entire campus Internet and its sub-networks. The service selection process should be conducted by identifying the security services that are necessary to countermand individual threats mentioned in the threat matrices, and then collate these services according to their types and deployment sites. The results of this process shall be a short list of basic security services

(confidentiality, integrity, authentication, access control, non-repudiation and audit) to be employed on each subnet with respect to different user groups and applications.

Again, to limit the workload, you are asked to select security services necessary to protect only *two (2)* subnets: *Officers' Subnet* and *Students' Subnet*. Two lists of security services that shall be deployed at the hosts, the servers and the gateway router of the two subnets should be provided. Each service should be qualified by the place it shall be deployed and the application(s) it tries to protect.

3.3 Architecture Recommendation [Grading: 20%, Optional]

As an option, you are encouraged to discover security weak points in current network architecture. The existence or more often non-existence of certain partitions among the subnets and/or interconnections between clients and servers may lead to major security breaches. Conversely, clever deployment of well-chosen security services can yield very effective protection. Additional points will be given to students who give relevant comments on security weakness of current network architecture and effective remedies.