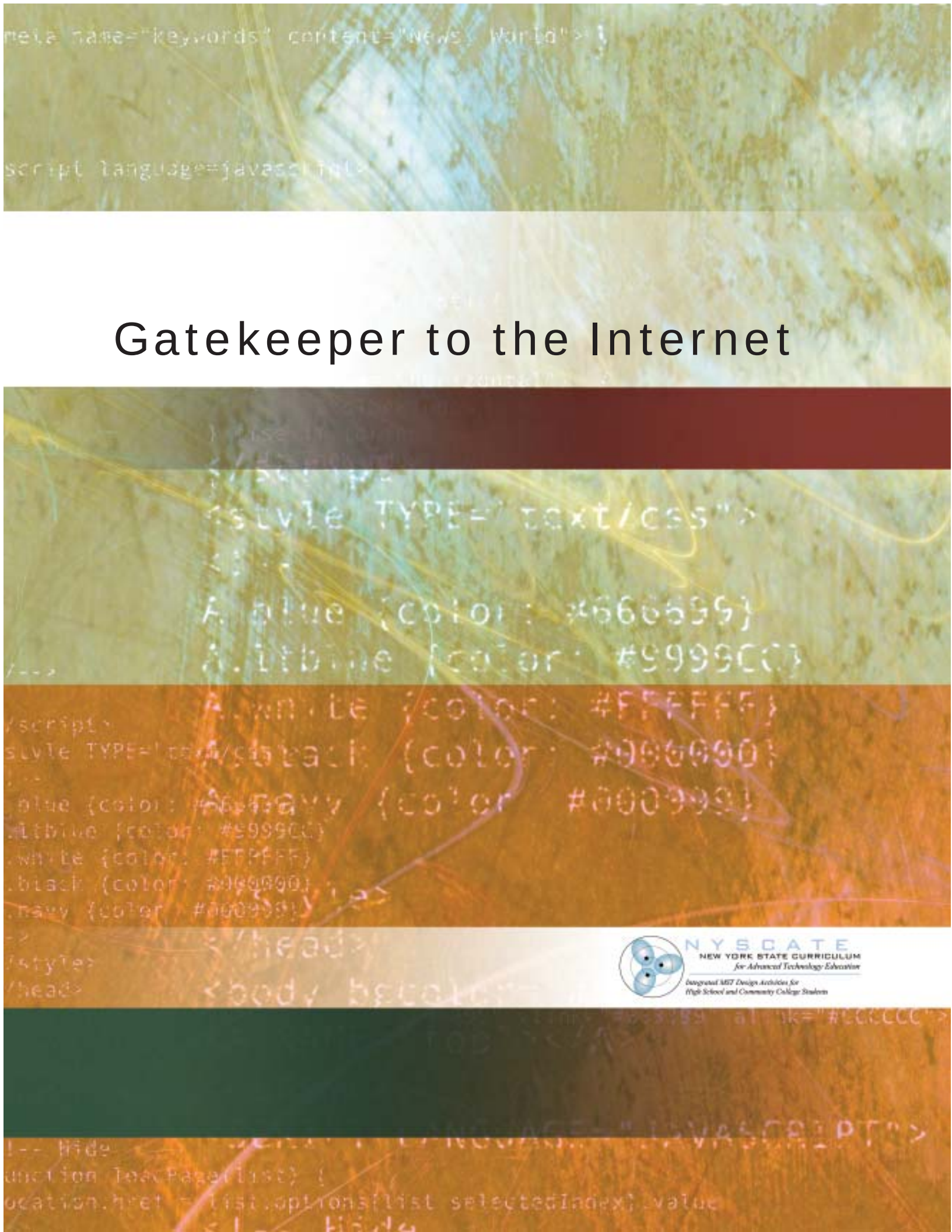
Gatekeeper to the Internet



NYSCATE
NEW YORK STATE CURRICULUM
for Advanced Technology Education
Integrated MST Design Activities for
High School and Community College Students

Partners in New York State Curriculum for Advanced Technology Education
Hofstra University
New York State Education Department

Project Co-Principal Investigators
Linda Hobart
Finger Lakes Community College

John E. Jablonski, Vice President and Dean of the College
Fulton-Montgomery Community College

Margarita Mayo, Director of Education, Training and Quality
New York State Business Council

Godfrey I. Nwoke, Ph.D.
New York City College of Technology

Jean Stevens, Assistant Commissioner, Office of Workforce Preparation and Continuing Education
New York State Education Department

Management Team

Project Co-Directors
M. David Burghardt, Ph.D.
Michael Hacker
Hofstra University

Project Coordinator
William Peruzzi, Ph.D.
Hofstra University

Project Administrative Assistant
Lois Miceli
Hofstra University

Project Advisory Council
Stuart Field (Chair), Manager, Saratoga Division
Slack Chemical Company

Dr. James C. Dawson, Member
N.Y.S. Board of Regents

Nancy Bryan, Past President
New York State Technology Education Association

James Cimino, Executive Director
Association of Career and Technical Education Administrators

Dr. Lorraine Hohenforst, Coordinator of Instructional Services
Hamilton-Fulton Montgomery BOCES

Dr. Elaine, A. Johnson, Director
Bio-Link (ATE) Center, City College of San Francisco

Dr. James V. Masi, Retired Executive Director, Northeast (ATE) Center for Telecommunications Technology
Professor Emeritus, Western New England College

Mr. Bernard McInerney, Statewide Tech Prep Coordinator
New York State Education Department

Mr. Gordon Snyder, Executive Director
National Center for Telecommunications Technology

Project Evaluation Team
Bert Flugman, Ph.D. Director
Deborah Hecht, Ph.D.
Center for Advanced Study in Education
City University of New York

Principal Writer: Badreddine Oudjehane
Contributing Author: Josephine Braneky
Consultant/Writer: Barry Borakove

Copy Editor: Barbara L. Kelly
Publications Designer: Lesa Clark, Liz Scott

NYSCATE modules and ancillary materials such as the NYSCATE Pedagogical Framework may be downloaded from http://www.nyscate.net or www.hofstra.edu/nyscate

This material is based upon work supported by the National Science Foundation under Grant 0053269. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

The University of the State of New York
The State Education Department

NYSCATE MODULE GUIDE

GATEKEEPER TO THE INTERNET

TABLE OF CONTENTS

I. INTRODUCTION AND OVERVIEW

ABSTRACT
In this NYSCATE module second-year community college students explore various methods used to implement security on the Internet. The Design Challenge requires students to design a solution that will secure an e-commerce company from unauthorized access, but at the same time will permit full remote access to the company's traveling salespeople.

Students develop a security proposal for the company and then test their designed security system to ensure that it fulfills the intent of the proposal.

GRADE LEVEL
This module is designed for students in the third or fourth semester of community college. Students will need prerequisite course work and a working knowledge of computer networks, including IP addressing schemes, and some administrative computer maintenance.

TIME ALLOCATION
Eight to 9 class/lab sessions should be allocated for this module; each class/lab session consists of two 50-minute periods. Total approximate time is 16 to 18 class/lab periods in a setting where computers are available for student use.

EXISTING COURSES ENHANCED BY THE MODULE
For example, these courses are offered by New York City Technical College:

Computer Systems Technology Department
Microcomputer Business Systems program:
- MS 307 Local Area Networks
- MS 405 Microcomputer Operating Systems
- CS 507 Advanced Single LAN Concepts
- CS 607 Interconnectivity
- CS 707 LAN-Internet Connection

Electromechanical Technology Department
Computer Engineering Technology program:
- EM 360 Data Communications
- EM 973 Microcomputer Interfacing

Electrical Engineering Technology Department
Telecommunications Technology program:
- TC 570 Computer Systems
- TC 620 Data Networks and Traffic Control

II. DESIGN CHALLENGE OVERVIEW

SETTING THE CONTEXT FOR STUDENTS

Introduction
Security has always been an important issue. Recorded history has shown that humans were designing and constructing technological solutions regarding their security long before the Internet came into being.

In medieval times, security involved feudal lords' protecting their castles from attack by armored warriors on horseback. Larger castles, with higher and thicker stone walls, were built to withstand such attacks. As invaders acquired new skills, feudal lords responded with additional security measures, such as moats, bridges, gates, and guard towers. Finding it increasingly difficult to storm a castle, invaders developed technological tools of their own—namely the *trebuchet* (catapult), which hurled 200-pound stone "missiles" at castle walls, and the cannon, which had enormous capacity to destroy. As security increased, *authorized* access to the castle became more difficult. In fact, authorized access while the castle was under siege was impossible.

The Internet has similar security issues and some differences. It must be secure from attack, but at the same time it must have the capacity to permit complete access when an authorized user requests it. In medieval times castle walls were built to withstand the attack of armored warriors on horseback and archers traveling by foot. Today, we use *firewalls* to secure our networks and servers, and the attackers are typically *hackers* using such modern weapons as *viruses* (hostile programs) that can cripple our systems if they gain access to our resources.

Design Challenge
A website of a well-known company involved in e-commerce has been hacked. Passwords have been accessed and confidential information has been compromised. You and the members of your team will design a solution to secure both the website and the company resources (data).

Specifications
- The website and the network must be secured to prevent all unauthorized access.
- The website and the network must permit full remote access to three traveling salespeople who need access to all network resources and internal data.

Constraints
- Dial-up solutions cannot be used since large-scale direct-dial access is unavailable.
- Internal data must be accessed through the Internet (an ISP account) using VPN.

III. GOALS AND LEARNING OUTCOMES

Tech Prep Information Technology Skill Standards

Network Technologies: Technical Learning Component

Learner Program Outcomes

- Demonstrate an understanding of the overall design and components of LAN and WAN systems.
- Demonstrate the ability to perform basic setup and configuration of network hardware and software.

Key Competencies

- Present and explain the design features of LAN and WAN systems.
- Install and configure a network server.
- Set up and configure a basic workstation connected to the network.
- Determine the type of network topology needed, such as peer-to-peer server based.
- Set up and configure TCP/IP services on workstation and server level.

Organization/Delivery of Presentations: Foundation Learning Component

Learner Program Outcomes

- Demonstrate the ability to select presentation technology, methods, and material appropriate to the audience and purpose of the presentation.
- Demonstrate the ability to organize and deliver the presentation material.

Key Competencies

- Select a technology delivery system and method appropriate to the size and nature of the audience and purpose of the presentation.
- Identify the requirements relating to the presentation space and environment.
- Organize the material so that it is complete and logically sequenced, and make sure it addresses the presentation timelines.
- Deliver the presentation, using good speaking skills and appropriate technology to enhance the delivery of the content.

Teamwork: Foundation Learning Component

Learner Program Outcomes

- Demonstrate the ability to organize and work in a team setting.
- Demonstrate the ability to recognize expertise and to learn from others, and demonstrate collaborative decision making.
- Demonstrate the ability to work and communicate effectively with persons of different backgrounds.

Key Competencies

- Use effective communication skills when interacting in a team environment.
- Work collaboratively to set team goals, showing flexibility in accepting others' leadership.
- Manage conflicts that arise, and maintain and build on the team process.

IV. TIMELINE CHART

This module is designed to be completed within 16–18 class/lab periods (assuming a class/lab period of 50 minutes). Each instructional session consists of two class/lab periods.

Session	FOCUS MODEL COMPONENT (for teachers)	INFORMED DESIGN LOOP COMPONENT (for students)	ACTIVITY
1	**Focus** discussion on Problem Context **Organize** for Informed Design	Clarify Design Specifications and Constraints	Begin discussion of Introductory Packet (Module Overview). Discuss informed design cycle; finish packet.
2–5	**Coordinate** Student Progress	Research and Investigation	Conduct KSB 1: Network and Security Overview. Conduct KSB 2: Methods of Unauthorized Access. Conduct KSB 3: Security Tools. Conduct KSB 4: Desktop Versus Network Security. Conduct KSB 5: Extending Your Network over the Internet - VPN.
6–7	**Coordinate** Student Progress	Generate Alternative Designs Choose and Justify Optimal Design Construct and Test the Network Design	Create diagrams of alternative solutions. Select and defend the choice of preferred alternative. Develop network diagram. Develop plans for testing the design solution
8	**Unite** Class Thinking about Accomplishments **Sum** Up Progress on Learning Goals	Test and Evaluate Network Design	Hold class presentations of methods and results. Assess student progress, the mod, and instruction.

V. MATERIALS AND RESOURCES

Materials Needed

Each group of students should have at least three computer networks (each network should use a different network IP address).

- ***Each network can be represented by a PC:***
  - one PC to act as the ***provider*** of web services (web server, and/or e-mail server)
  - one PC to act as the ***client*** to access web services
  - one PC to act as the ***"gatekeeper,"*** or firewall.

Depending on the type of network connections available, using only the TCP/IP protocol is recommended. By attempting to access the ***provider***, the ***client*** will test the access. In addition, a group of students can attempt to access another group's ***provider***. This will serve as a test to determine if an outside client can gain access to a private network (VPN).

SOURCES

- Cisco Systems: OSI Model, ConfigMaker, *http://www.cisco.com*
- Securing Your Business Network: Cisco Secure Solutions
  http:/www.cisco.com/warp/public/cc/so/neso/sqso/bznet_pl.htm
- Cisco Network Security Primer
  http://www.cisco.com/warp/public/cc/so/neso/sqso/netsp_pl.htm
- Internet Week, *http://www.internetweek.com/VPN/default.html*
- Network Magazine, *http://www.networkmagazine.com/article/NMG20010226S0002*
- Network ICE, *http://advice.networkice.com/Advice/default.htm*
- Gibson Research, *http://grc.com*
- Insecure Org., *http://www.insecure.com*

VI. PROCEDURAL SUGGESTIONS

SUGGESTIONS

The following suggested strategies are presented to the teacher within the context of the NYSCATE FOCUS on Informed Design, a pedagogical model for teachers. The FOCUS components are: **Focus** discussion on the problem context, **Organize** for informed design, **Coordinate** student progress, **Unite** the class in thinking about what has been accomplished, and **Sum up** progress on the learning goals (see NYSCATE *Pedagogical Framework*, www.nyscate.net, for more on this model).

Session 1: *Focusing discussion on the problem context*

The problem. In order to focus and engage your students, discuss the Design Challenge with the class.

Many companies are now involved in e-commerce. Customers can order merchandise, take care of banking needs, and even take a course over the Internet. Much sensitive information passes through the Internet. It is extremely important to protect all sensitive and personal information. As a client, you want to make sure that the password to your bank account is not accessed by anyone other than yourself. Nor do you want your credit card number to be distributed to anyone other than the authorized person(s).

Hackers are constantly trying to prove their skills by breaking into company websites and compromising sensitive data.

Inform the class that they will be focusing on designing a solution to secure both the website for a particular company and sensitive data that the company keeps. In addition, tell the class that they will design a policy to prevent any kind of break-in to the website or

INTRODUCTORY PACKET: Overview of the Module and Design Challenge

HERE IS WHAT YOU WILL DO

In the NYSCATE module ***Gatekeeper to the Internet***, you will work in a group to:

- design a solution for an e-commerce company whose website has been hacked and whose resources have been compromised;
- investigate the characteristics of network security;
- review common methods that are used to gain unauthorized access to a network;
- explore the many firewall and security tools that are available;
- investigate the differences when designing desktop and network security schemes; and
- gain remote access to a network using the virtual private network (VPN) protocol.

PROBLEM CONTEXT

Introduction

Security has always been an important issue. Recorded history has shown that humans were developing technological solutions regarding their security long before the Internet came into being.

In medieval times, security involved feudal lords' need to protect their castles from attack by armored warriors on horseback. Larger castles, with higher and thicker stone walls, were built to withstand such attacks. As invaders acquired new skills, feudal lords responded with additional security measures, such as moats, bridges, gates, and guard towers. Finding it increasingly difficult to storm a castle, invaders developed technological tools of their own—namely the *trebuchet* (catapult), which hurled 200-pound stone "missiles" at the castle walls, and the cannon, which had enormous capacity to destroy. As security increased, *authorized* access to the castle became more difficult. In fact, any authorized access while the castle was under siege was impossible.

The Internet has many similar security issues and some differences. It must be secure from attack, but at the same time it must have the capacity to permit complete access when an authorized user requests it. In medieval times castle walls were built to withstand the attack of armored warriors on horseback and archers traveling by foot. Today, we use *firewalls* to secure our networks and servers, and the attackers are typically *hackers* using such modern weapons as *viruses* (hostile programs) that can cripple our systems if they gain access to our resources.

Design Challenge

A website of a well-known company involved in e-commerce has been hacked. Passwords have been accessed and confidential information has been compromised. You and the members of your team will design a solution to secure both the website and the company resources (data).

data. Distribute the Introductory Packet, but have students put it aside until the following meeting. Introduce the informed design loop. Ask "KWL" questions to find out what the students do **know**, what they **want to know**, and what they need to **learn**. Examples of such questions are: Why do we need to make a website secure? Why is it important for personal/sensitive data not to be compromised? How would you devise an encryption scheme? This kind of questioning will help you discover and work on the naïve conceptions individual students hold about securing a website and data that is transferred through a network.

The challenge. The website of a company involved in e-commerce has been hacked. Passwords have been accessed and confidential information has been compromised. You will design a solution to secure both the website and the company's data.

Redirect students to the Introductory Packet. As you go through the packet's contents together, try to motivate students as you present the challenge. For example, start by describing the latest virus that affected the Internet, and follow with a discussion about hacking and converting "pirated" software to MP3 files (use the example of Napster). Discuss the need for storage sites on the Internet where materials to be shared are stored and retrieved under strict guidelines enforced by the site administrator. There are many examples that can be used in a discussion of data security. One is identity theft, which does not necessarily occur over the Internet; instead, identity thieves may simply obtain information by raiding a mailbox or going through trash. The Internet, however, has provided a new avenue for accessing, distributing, sharing, and using illegally obtained information. A discussion of data security should also include recent news about network intrusions and the subsequent loss of data. End the discussion following a brief look at the Here's What You Will Do, Problem Context, and Materials Needed sections.

Period 1: *Organizing for Informed Design*

Informed design. (See the NYSCATE *Pedagogical Framework* for a more detailed discussion on focusing students on the process of informed design.) Elicit from students what they know about good design and who engages in design. Ask for examples of good design and poor design.

Tell the class that completing a series of KSBs will help prepare them for addressing the Design Challenge they face. Then distribute the student handout describing the informed design cycle, and provide time to read it.

The information sheet on the informed design cycle should be referred to often as groups work on the Design Challenge. The informed design loop can be particularly useful to the students as they chart their progress using a Design Journal. Like professional engineers, they will find themselves using the loop in an iterative rather than a linear way.

Discuss the informed design cycle and stress that although design is normally informed by the designer's current knowledge, completion typically requires access to new knowledge. Discuss the need to research what solutions exist to solve this Design Challenge, and make sure the class understands that reaching an optimal design solution requires meeting specifications, working within constraints, and making trade-offs.

Student requirements. Discuss the student requirements (see Introductory Packet); students will be expected to maintain a Design Journal. (This document is discussed in the NYSCATE *Pedagogical Framework,* p. 15, along with guidelines for the Design Report, p. 27, and the group presentation, p. 27.) Help students see that the Design Journal allows them to document progress as they complete literature searches, factor investigations, and Knowledge and Skill Builders (KSBs). Describe the requirement that each student submit a Design Report and each group make a class presentation at the conclusion of the module. Explain that the report and the presentation will be based on information recorded in the Design Journal. Alert students that the presentations should be multimedia and should detail their design process and results. Help them see that such a presentation summarizes work completed in researching, collecting, and analyzing data; developing models; improving designs; and making refinements. Describe the multiple forms of media (e.g., presentation software, color overheads, videos, computer animation) that they might use to enhance their presentations. Assure them that when classmates ask probing questions and challenge group findings at the end of presentations, they are mirroring proceedings that are common at science conferences.

Assigning groups. Talk with some of the students ahead of time to see how experienced they are at working in cooperative groups. Organize small working groups; assigning three students per group is often ideal (see "Forming and Facilitating Design Teams" in the *Pedagogical Framework,* p. 12). Monitor groups throughout the module.

Sessions 2–7: *Coordinating student progress*

Coordinate work by individuals. Plan opportunities within this module for students to revisit their initial understandings by providing experiences with new phenomena that contradict their stated perceptions. Unless students have the opportunity to actively process such contradictions, they may fail to grasp the new concepts and then may revert to their preconceptions.

Help individual students make the connection between carefully documenting information as they proceed and well-written reports and presentations at the end.

Note that a student displaying unacceptable behavior may be doing so because other members of the group do not value that student's contribution to the project. Get to know the strengths of such a student and try assigning roles for all members of his or her group. Give the student a role that features a personal strength and inform the group ahead of time that this person is known to do that task well.

As the work becomes more technical and cerebral, some students will begin to complain that they are doing all the work while others loaf. Citing examples from your own experience, explain to such individuals that the best way to learn something is to teach it to others. Remind the group that it is essential that *all* members of a cooperative group understand all ideas and steps along the way. Conduct frequent oral checks to see that each student has adequate understanding before the group moves on in its work.

Group research and investigation through KSBs. Have students complete the following KSBs sequentially:

KSB 1: Network and Securities Overview – Students will develop an understanding of different facets of security.
KSB 2: Methods of Unauthorized Access – Students will learn the many ways of accessing a network and effects on security issues.
KSB 3: Security Tools – Students will investigate the different methods a site/server can be secured using firewalls.
KSB 4: Desktop Versus Network Security – Students will explore different security methods.
KSB 5: Extending Your Network over the Internet – VPN. Students will learn VPN protocols and security solutions.

Knowledge and Skill Builders

KSB 1: Network and Security Overview

Security has always been an important consideration in the field of information technology. When mainframes "ruled the world," access was provided through terminals that were hardwired to the mainframe. It was also relatively easy to control the resources that could be accessed by a terminal by using a system of accounts. Having secure accounts was the major line of defense; remote access was rare and reserved to a few. With the explosion of distributed computing, computers have become networked together, and this development has opened a virtual floodgate of security issues that we are still grappling with today. Remote access has been increasing to the extent that today's computer users expect to have complete remote access to all resources. Since most account information has to be sent out across telephone lines, password/log-in names can be hacked and used later to collect sensitive data on the Internet. Both servers and networks need to be properly secured. Additionally, the envelope is pushed even further with the management of the workstation/servers.

In this KSB you will be introduced to the many facets of network security. You will survey the types of attacks, viruses, definitions, and theories/methods behind them. You will create accounts on a server and then attempt remote access while recording the network packets. You will record these network packets, using a network analyzer.

The essential services available on today's networks will be presented and you will set up some of those services. You will then attempt to read from recorded network packets the log-in data to an FTP server. You will also investigate methods that can be used to manage a client remotely.

Knowledge and Skill Builders

KSB 2: Methods of Unauthorized Access

Security issues are keeping pace with the rapid changes that are occurring in information technology. Securing a desktop is a much simpler task than securing a network; networks can have multiple methods of access. Identifying the risks for a network and providing a suitable response must be part of a carefully designed plan. Any organization that relies on a network must develop policies and emergency procedures. It is much easier to follow a well-thought-out procedure than to think of one as you are attempting to resolve the problem. In mission-critical systems such as e-commerce companies that are required to be online and operational at all times, any down time reduces profits. More security can result in greater inconvenience for users as well. Since a network has many resources that users need or want to access, policies that are too harsh may not be followed. In fact, a major concern of companies deploying security policies is policies that are either ignored, or circumvented, by employees.

In this KSB you will explore your current security situation and learn about the many ramifications of having a presence on the Internet. Specifically, you will gain an understanding of the implications of *your* presence on the Internet. You will learn methods used to recognize ports, and you will learn how these ports can be scanned to detect potential unauthorized access. Since ports can be blocked, they can be used as a tool to control access.

Develop your understanding

1. Review the resources made available by your teacher and describe two recent security problems that have affected some companies.
2. Research two types of attacks as well as countermeasures and present them to the class.
3. Design a security policy that addresses the prevention of

Knowledge and Skill Builders

KSB 3: Security Tools

Many tools have been designed to protect desktops and networks from potential security problems. None of these tools can compensate for carelessness on the part of the user. In addition, if an administrator does not follow elementary rules of security (e.g., using an appropriate password selection scheme, not sharing information), then no tools can ensure network security. Networks must be monitored so that security breaches can be discovered early enough to mount a response and minimize their consequences. Constant testing is also needed as the ingenuity of the attackers increases to match that of the security engineers. Although most issues concern the Internet and remote access, networks can be at risk from users with questionable intentions locally, or anywhere in the world.

Authentication proves to be an extremely important issue, since a weak procedure can diminish the robustness of any defense. Although there is no one best scheme, authentication methods should require users to prove their identity either through answers to personal or secret questions (such as mother's maiden name), answers to a challenge (using some agreed-upon scheme), keys (smartcard or checksum with virus detection), or physical characteristics of the user (such as retina, fingerprints, or voice recognition).

You will explore the different methods through which a site/server can be secured with firewalls. There are several types of firewalls; you will study packet filtering, application proxy firewalls, and NAT routers and personal firewalls. You will discuss and study how and where to place the firewall on the network.

Knowledge and Skill Builders
KSB 4: Desktop Versus Network Security

As you have seen in your work so far, there are many possible ways to design a secure environment. A network that is secured from outside access is not necessarily secured from internal access. Securing a desktop/server is a different issue as well.

Since cost is always an important factor when designing security solutions, cost consideration must be weighed when implementing any security solution. It is also important to know the characteristics of security products and understand how these products can be implemented into a security policy. While some network services are geared to provide services to users (e-mail, web server), others are geared to support network services (DSN). This leads to consideration of network design features such as using a single filter for screening: an Internet host, a server, subnets, or IP architecture.

In this KSB you will implement several network services and security schemes. You will also install and test some personal firewall products and evaluate their limitations or constraints. Some of the commonly available network-supported services are FTP, Telnet, http, ICMP, SMTP, NETBIOS ports, and SNMP. You will select two of these services and use them in the development of a security scheme.

Develop your understanding

1. Research and report available network protocols that support security communications.
2. Use the following Cisco white papers to discuss the differences between securing a business network and a personal network: • Securing Your Business Network: Cisco Secure Solutions • Cisco Network Security Primer.
3. List and describe five [illegible] methods that

Knowledge and Skill Builders

KSB 5: Extending Your Network over the Internet - VPN

You have secured your network but remote access is needed; what do you do? Do you simply "poke a hole" in your firewall? Do you use dial-up? A much more secure alternative is to use the Internet as a means of connecting while securing the link using special network protocols (establishing a virtual private network, or VPN) over the Internet. You can now achieve remote access by using a local ISP and connecting to your network. Full access to the internal network and data is achieved without compromising security.

In this KSB you will set up one computer as a client and another as a VPN server. You will test access while both machines are connected to different networks. You will also set up another VPN to two clients from the other groups in your class and test the access of both the VPN nodes and the other computers in your classroom.

Develop your understanding

1. Search the Internet for a VPN hardware solution. Summarize your findings and determine how this hardware solution compares to possible software solutions.
2. Summarize and describe the following VPN protocols:
    a. L2TP
    b. IPSEC
3. Create a secure network and attempt to access it. Record the network traffic and highlight the frames that transport your attempts.
4. Set up a VPN and repeat step 3.

Seeking additional factors and affecting the design of network security

Sharing. Convene the large group one or more times to share results of individual and group investigations. Invite students to listen critically to one another, and facilitate a discussion of how this knowledge can be used to inform their efforts in the design of a network. Continue to work as a facilitator as students work in their groups to create alternative designs. Check to see that each group understands that its solution must address the specifications and constraints and the conditions needed to design the network. Remind each group to make decisions and select design components on the basis of their investigations. You may want to develop a rating system to determine which alternative design is preferred.

Planning and constructing. Continue to work as a facilitator as groups select their preferred alternative and develop plans for design. Facilitate a discussion of trade-offs that are made in the search for optimal design solutions. Encourage groups to identify and model functional design elements and construct their working prototype.

Testing. Bring students together as a large group and discuss ways in which groups might test their design solutions. Facilitate small group development for testing and evaluation procedures.

Bring the entire group together to compare results. Encourage student groups to carefully review the work of other groups to glean ideas that might inform a redesign. When redesign is discussed, continue to direct students' attention to how the understanding can guide improvement.

Session 8: ***Summing up progress on the learning goals***

Design Report. The reports are one of the major opportunities for you to determine whether individuals have attained the goals for this module. Continue to work as a facilitator as groups document their progress and share results. Explain that each student must submit a Design Report. Assist individuals in structuring and writing their Design Reports. The Design Report should include a discussion of redesign with justifications for the redesign decisions. Provide students with the Design Report guidelines from the NYSCATE *Pedagogical Framework*. When you introduced this module, you told students that careful documentation in the Design Journal leads to a well-written final report later on. For individuals who have trouble writing, check their documentation frequently along the way to ensure that they will have a source of information adequate to generate a report. It is advisable to set aside some class time for students to work on their reports. Looking over their reports at this time will provide you with feedback as to how the students are progressing and will enable you to assist students during regular class time.

Group presentations. Discuss with the class what is considered proper and expected behavior during group presentations. Address the need to use a variety of media to support the presentation. Review and distribute the presentation guidelines from the NYSCATE *Pedagogical Framework*.

During the group presentations to the class, encourage students (through example) to ask appropriate questions and provide constructive feedback to the presenters.

VII. ADDITIONAL SUPPORT FOR TEACHERS

ASSESSMENT STRATEGIES
Assessment scoring sheets follow which assess student performance in the following five categories:

- A. Design Solution: This should include a security policy proposal that assesses the current security environment of the client and outlines a new (and improved) security policy. Operation of the solution is tested to verify that it meets design criteria.
- B. Oral Presentation to Class: Preparation and presentation of material to the class should be evaluated. Was the design solution justified?
- C. Student Class Work and Group Work: Consider the participation of each student, including individual effort and contribution to the group effort.
- D. Design Journal: Student documentation of all investigations is necessary. Accuracy is essential, and complete records of investigations and the Design Challenge must be included.
- E. Final Report: Does the final design solution reflect work on the KSBs? Has the design process been used correctly? Was good written English used?

Gatekeeper to the Internet

Assessment Student Scoring Sheets

A. Design Challenge Solution

Security Policy Proposal

1. Proposal provides a complete assessment of the current network environment.	(0–20 pts.)	_____
2. Proposal accurately describes the current security policy.	(0–20 pts.)	_____
3. Deficiencies in the current security policy are identified.	(0–20 pts.)	_____
4. Proposed security policy adequately addresses the deficiencies observed in the client's original security policy.	(0–20 pts.)	_____
5. Proposed security policy is firmly grounded in current network security practices.	(0–20 pts.)	_____
6. Strategies are provided for the management of a security breach or crisis.	(0–20 pts.)	_____
7. Proposal reflects good written English with all sources properly cited.	(0–20 pts.)	_____

Security Policy Operational Performance

8.	Client is provided with an operational network with 3 VPNs.	(0–18 pts.)	_____
9.	Each VPN has full access to all network resources and data.	(0–18 pts.)	_____
10.	Testing confirms that the security policy performs as stated in the security policy proposal.	(0–24 pts.)	_____
		Total (200 pts.)	_____

B. Oral Presentation to Class

1.	Presentation followed a logical sequence.	(0–5 pts.)	_____
2.	All team members actively participated.	(0–5 pts.)	_____
3.	Presenters were clear and audible.	(0–5 pts.)	_____
4.	Presenters were appropriately dressed.	(0–5 pts.)	_____
5.	Presentation held the attention of the audience.	(0–5 pts.)	_____
6.	Audience participation was encouraged.	(0–5 pts.)	_____
7.	Questions were answered in a professional manner.	(0–5 pts.)	_____
8.	Presenters were well prepared (all materials were ready).	(0–5 pts.)	_____
9.	Technical terms were correct and were used appropriately.	(0–5 pts.)	_____
10.	The design solution was justified to the class.	(0–5 pts.)	_____
		Total (50 pts.)	_____

C. Student Class Work and Group Work

1.	Assigned tasks were completed in a timely fashion.	(0–10 pts.)	_____
2.	Student managed time well.	(0–10 pts.)	_____
3.	Student worked collaboratively with teammates.	(0–10 pts.)	_____
4.	Student followed teacher's instructions well.	(0–10 pts.)	_____
5.	Student contributed her/his share of the group effort.	(0–10 pts.)	_____
6.	Student conducted herself/himself in a businesslike manner.	(0–10 pts.)	_____
		Total (60 pts.)	_____

D. Design Journal

1. Journal documents all work on both the KSBs and the Design Challenge.	(0–6 pts.)	_____
2. Journal contains observations and data that were collected during the KSBs and the Design Challenge.	(0–8 pts.)	_____
3. All entries are legible and complete with correct grammar and punctuation.	(0–8 pts.)	_____
4. Entries are chronologically correct.	(0–6 pts.)	_____
5. Entries were made on a daily basis.	(0–6 pts.)	_____
6. Illustrations are used to enhance the journal entries.	(0–6 pts.)	_____

Total (40 pts.) _____

E. Final Report

1. An introduction explains the context of the problem and notes the specifications and constraints.	(0–7 pts.)	_____
2. Research and investigations are documented as are existing solutions that helped solve the problem.	(0–7 pts.)	_____
3. Multiple solutions are generated and the selection of alternative solutions is justified.	(0–7 pts.)	_____
4. An optimal solution is chosen and it is based upon engineering, mathematical, and scientific data and principles.	(0–8 pts.)	_____
5. The construction of a working model is described and any modifications and refinements are discussed.	(0–7 pts.)	_____
6. Methods used to test the design solution are described; data that were collected and the evaluation of the design solution are described.	(0–7 pts.)	_____
7. Recommendations are made for redesign to enhance the performance of the design solution.	(0–7 pts.)	_____

Total (50 pts.) _____

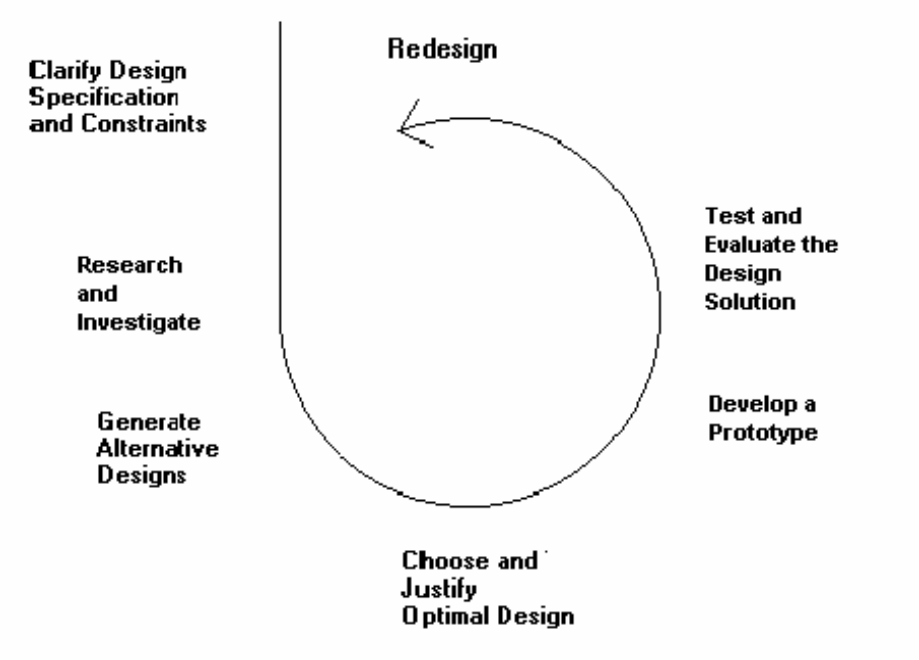
Grand Total: Sections A-E (400 pts.) _____

NYSCATE DESIGN CYCLE

- The Design Cycle

Characteristic of the design process is its iterative nature. It is iterative in that decisions are made without complete knowledge and therefore they must be revisited. Each solution element can be refined in a multistep process involving monitoring performance against desired results and making appropriate modifications. Typically, trade-offs are required to address design criteria optimally.

A method is shown (see informed design loop below) to illustrate informed technological design for students.



The loop includes several phases. In this model, the phases together are referred to as the design cycle. The model involves repeatable phases that engage the student in the design process. The student hereby works in a manner similar to that of adult professionals who do engineering design for a living. Engineers and other designers rarely follow these phases in order. Instead, they move back and forth from one phase to another as needed. You also should not expect students to go through these phases in the same order each time that they design something. The designer arrives at solutions while monitoring performance against desired results and making appropriate changes as needed. Almost always, following design criteria leads to trade-offs taking place. The phases of the informed design cycle are described here:

1. *Clarify design specifications and constraints.* Describe the problem clearly and fully, noting constraints and specifications. Constraints are limits imposed upon the solution. Specifications are the performance requirements the solution must meet.

2. *Research and investigate the problem.* Search for and discuss solutions that presently exist to solve this or similar problems. Identify problems, issues, and questions that relate to addressing this Design Challenge.

3. *Generate alternative designs*. Don't stop when you have one solution that might work. Continue by approaching the challenge in new ways. Describe the alternative solutions you develop.

4. *Choose and justify optimal design.* Defend your selection of an alternative solution: Why is it the optimal choice? Use engineering, mathematical, and scientific data, and employ analysis techniques, to justify why the proposed solution is the best one for addressing the design specifications. This chosen alternative will guide your preliminary design.

5. *Develop a prototype.* Make a model of the solution. Identify possible modifications that would lead to refinement of the design, and make these modifications.

6. *Test and evaluate the design solution.* Develop a test to assess the performance of the design solution. Test the design solution, collect performance data, and analyze the data to show how well the design satisfies the problem constraints and specifications.

7. *Redesign the solution with modifications.* In the redesign phase, critically examine your design and note how other students' designs perform to see where improvements can be made. Identify the variables that affect performance and determine which science concepts underlie these variables. Indicate how you will use science concepts and mathematical modeling to further enhance the performance of your design.

Note: Phase 4 involves (a) hypothesizing that the design solution will meet specifications and constraints; and (b) showing that the design should work by conducting M/S/E/T analyses. When choosing the optimal design from among alternatives, two things are in play: The first is that the optimal design is chosen by rating it against design specifications and constraints. After doing so, the designer is not yet really sure that the design will work as intended. A hypothesis is made on the basis of the rating. It is not until mathematical or engineering analysis has been done that the designer is reasonably certain that the design will meet specifications. For example, if the design is a table, it is analyzed under the intended load (a stress analysis is done). This is an interesting deviation from the current design models because it calls out specifically for two kinds of analyses to be done: one qualitative, one quantitative. It draws the student a step closer to informed design.

VIII. STUDENT HANDOUT SECTION

Student Handout section begins on the following page:

HERE IS WHAT YOU WILL DO

In the NYSCATE module *Gatekeeper to the Internet*, you will work in a group to:

- design a solution for an e-commerce company whose website has been hacked and whose resources have been compromised;
- investigate the characteristics of network security;
- review common methods that are used to gain unauthorized access to a network;
- explore the many firewall and security tools that are available;
- investigate the differences when designing desktop and network security schemes; and
- gain remote access to a network using the virtual private network (VPN) protocol.

PROBLEM CONTEXT

Introduction

Security has always been an important issue. Recorded history has shown that humans were developing technological solutions regarding their security long before the Internet came into being.

In medieval times, security involved feudal lords' need to protect their castles from attack by armored warriors on horseback. Larger castles, with higher and thicker stone walls, were built to withstand such attacks. As invaders acquired new skills, feudal lords responded with additional security measures, such as moats, bridges, gates, and guard towers. Finding it increasingly difficult to storm a castle, invaders developed technological tools of their own—namely the *trebuchet* (catapult), which hurled 200-pound stone "missiles" at castle walls, and the cannon, which had enormous capacity to destroy. As security increased, *authorized* access to the castle became more difficult. In fact, any authorized access while the castle was under siege was impossible.

The Internet has similar security issues and some differences. It must be secure from attack, but at the same time it must have the capacity to permit complete access when an authorized user requests it. In medieval times castle walls were built to withstand the attack of armored warriors on horseback and archers traveling by foot. Today, we use *firewalls* to secure our networks and servers, and the attackers are typically *hackers* using such modern weapons as *viruses* (hostile programs) that can cripple our systems if they gain access to our resources.

Design Challenge

A website of a well-known company involved in e-commerce has been hacked. Passwords have been accessed and confidential information has been compromised. You and the members of your team will design a solution to secure both the website and the company resources (data).

Specifications

• The website and network need to be secured to prevent all unauthorized access.

• The website and network must permit full remote access to three traveling salespeople who need access to all network resources and internal data.

Constraints

• Dial-up solutions cannot be used since large-scale direct-dial access is unavailable.
• Internal data must be accessed through the Internet (an ISP account) using VPN.

Materials Needed

• Each group of students should have at least three computer networks (each network should use a different network IP address). Each network ***can be represented by a PC***:
    • one PC to act as the ***provider*** of web services (web server, and/or e-mail server)
    • one PC to act as the ***client*** to access web services
    • one PC to act as the ***"gatekeeper,"*** or firewall.

Depending on the type of network connections available, using only the TCP/IP protocol is recommended. By attempting to access the ***provider***, the ***client*** will test the access. In addition, a group of students can attempt to access another group's ***provider***. This will serve as a test to determine if an outside client can gain access to a private network (VPN).

STUDENT REQUIREMENTS

Each team will be responsible for a *security policy proposal* that elaborates the following components:

• assessment of the current network environment
• current security policy used by the client
• proposed security policy designed for the client
• strategies to manage a security breach or crisis.

Demonstrate full access to data for each of the three required VPNs.

You will maintain an individual **Design Journal**, which will contain all of your observations and collected data. Entries will be made on a daily basis and will document your efforts on the KSBs and the Design Challenge.

You will submit a final **Design Report**, which will contain information gathered from your Design Journal:

• literature searches
• hands-on research (factor studies)
• completed Knowledge and Skill Builders (KSBs)
• work on the Design Challenge
• methods used to generate the final design solution.

Each team's oral presentation to the members of the class should:

- Justify your design solution.
- Use a variety of media.
- Be prepared and delivered in a professional manner.
- Demonstrate that the solution meets design criteria.

Knowledge and Skill Builders

KSB 1: Network and Security Overview

Security has always been an important consideration in the field of information technology. When mainframes "ruled the world," access was provided through terminals that were hardwired to the mainframe. It was also relatively easy to control the resources that could be accessed by a terminal by using a system of accounts. Having secure accounts was the major line of defense; remote access was rare and reserved to a few. With the explosion of distributed computing, computers have become networked together, and this development has opened a virtual floodgate of security issues that we are still grappling with today. Remote access has been increasing to the extent that today's computer users expect to have complete remote access to all resources. Since most account information has to be sent out across telephone lines, password/log-in names can be hacked and used later to collect sensitive data on the Internet. Both servers and networks need to be properly secured. Additionally, the envelope is pushed even further with the management of the workstation/servers.

In this KSB you will be introduced to the many facets of network security. You will survey the types of attacks, viruses, definitions, and theories/methods behind them. You will create accounts on a server and then attempt remote access while recording the network packets. You will record these network packets, using a network analyzer.

The essential services available on today's networks will be presented and you will set up some of those services. You will then attempt to read from recorded network packets the log-in data to an FTP server. You will also investigate methods that can be used to manage a client remotely.

Develop your understanding

1. Research any two different types of computer viruses; your findings should summarize their effects. Include methods that can be used to detect and remove these viruses.
2. Investigate the organization whose name is **CERT**. What is the origin of this organization? What is the functional purpose of CERT as it relates to network security?
3. Survey and describe the latest and most common types of attacks (including viruses). You can use www.insecure.org and/or www.grc.com to research the postmortem.
4. Design a simple encryption scheme.
5. Briefly describe two essential services provided for Internet customers.
6. What are the potential problems of having Internet access through a DSL?

Knowledge and Skill Builders

KSB 2: Methods of Unauthorized Access

Security issues are keeping pace with the rapid changes that are occurring in information technology. Securing a desktop is a much simpler task than securing a network; networks can have multiple methods of access. Identifying the risks for a network and providing a suitable response must be part of a carefully designed plan. Any organization that relies on a network must develop policies and emergency procedures. It is much easier to follow a well-thought-out procedure than to think of one as you are attempting to resolve the problem. In mission-critical systems such as e-commerce companies that are required to be online and operational at all times, any downtime reduces profits. More security can result in greater inconvenience for users as well. Since a network has many resources that users need or want to access, policies that are too harsh may not be followed. In fact, a major concern of companies deploying security policies is policies that are either ignored, or circumvented, by employees.

In this KSB you will explore your current security situation and learn about the many ramifications of having a presence on the Internet. Specifically, you will gain an understanding of the implications of *your* presence on the Internet. You will learn methods used to recognize ports, and you will learn how these ports can be scanned to detect potential unauthorized access. Since ports can be blocked, they can be used as a tool to control access.

Develop your understanding

1. Review the resources made available by your teacher and describe two recent security problems that have affected some companies.
2. Research two types of attacks as well as countermeasures and present them to the class.
3. Design a security scheme that addresses the prevention of unauthorized access to a building.
4. List personal information about yourself that you would want to secure. Also list information about a node on the Internet that you would want to secure.
5. Research NAT and discuss its pros and cons.
6. List tools and software that can be used to scan networks, test ports, and record and analyze network traffic.
7. Scan a network using the IP addresses provided by your instructor. Present your findings to the class.

Knowledge and Skill Builders

KSB 3: Security Tools

Many tools have been designed to protect desktops and networks from potential security problems. None of these tools can compensate for carelessness on the part of the user. In addition, if an administrator does not follow elementary rules of security (e.g., using an appropriate password selection scheme, not sharing information), then no tools can ensure network security. Networks must be monitored so that security breaches can be discovered early enough to mount a response and minimize their consequences. Constant testing is also needed as the ingenuity of the attackers increases to match that of the security engineers. Although most issues concern the Internet and remote access, networks can be at risk from users with questionable intentions locally, or anywhere in the world.

Authentication proves to be an extremely important issue, since a weak procedure can diminish the robustness of any defense. Although there is no one best scheme, authentication methods should require users to prove their identity either through answers to personal or secret questions (such as mother's maiden name), answers to a challenge (using some agreed-upon scheme), keys (smartcard or checksum with virus detection), or physical characteristics of the user (such as retina, fingerprints, or voice recognition).

You will explore the different methods through which a site/server can be secured with firewalls. There are several types of firewalls; you will study packet filtering, application proxy firewalls, and NAT routers and personal firewalls. You will discuss and study how and where to place the firewall on the network.

Develop your understanding

1. Select two firewall products and summarize their specifications including cost for the network implementation.
2. Select and use a password testing utility. Summarize your results.
3. Using the information from step 2 above, design a password policy that provides effective security, test its effectiveness, and discuss it with your classmates.
4. Use a password policy on a node (system) that is not using a firewall. Attempt to break that password. Record the network traffic and highlight the frames containing the break attempt.
5. Repeat step 5, but this time you should have a firewall protecting that node.
6. Research the network services installed in your system and compare a tool installed as an application versus a tool that uses a service.
7. Install a remote access tool and use it to control a remote node.
8. Outline how a password/key authentication would be implemented.
9. Research an open source authentication process.

Knowledge and Skill Builders

KSB 4: Desktop Versus Network Security

As you have seen in your work so far, there are many possible ways to design a secure environment. A network that is secured from outside access is not necessarily secured from internal access. Securing a desktop/server is a different issue as well.

Since cost is always an important factor when designing security solutions, cost consideration must be weighed when implementing any security solution. It is also important to know the characteristics of security products and understand how these products can be implemented into a security policy. While some network services are geared to provide services to users (e-mail, web server), others are geared to support network services (DSN). This leads to consideration of network design features such as using a single filter for screening: an Internet host, a server, subnets, or IP architecture.

In this KSB you will implement several network services and security schemes. You will also install and test some personal firewall products and evaluate their limitations or constraints. Some of the commonly available network-supported services are FTP, Telnet, http, ICMP, SMTP, NETBIOS ports, and SNMP. You will select two of these services and use them in the development of a security scheme.

Develop your understanding

1. Research and report available network protocols that support security communications.
2. Use the following Cisco white papers to discuss the differences between securing a business network and a personal network: • Securing Your Business Network: Cisco Secure Solutions • Cisco Network Security Primer.
3. List and describe four basic security methods that are described in the Cisco materials named above.
4. Select one of the security tips (with the aid of your instructor) from the Cisco materials and prepare a five-minute presentation to deliver to the class.
5. In your own words, summarize the approach used by Cisco to address the problem of security.
6. Select one type of threat and present a case study.
7. For the threat selected in step 6, research countermeasures.
8. Use the IP information and setup by your instructor and apply them to your network. Record also the IP data given to the other groups. Implement the mission given to you and gather the tools needed to perform your task. Set up the proper measures to protect and monitor your network. In this exercise one group will be the hacker while the other will be the target network. Execute your mission and report any detection/intrusion.

Knowledge and Skill Builders

KSB 5: Extending Your Network over the Internet - VPN

You have secured your network but remote access is needed; what do you do? Do you simply "poke a hole" in your firewall? Do you use dial-up? A much more secure alternative is to use the Internet as a means of connecting while securing the link using special network protocols (establishing a virtual private network, or VPN) over the Internet. You can now achieve remote access by using a local ISP and connecting to your network. Full access to the internal network and data is achieved without compromising security.

In this KSB you will set up one computer as a client and another as a VPN server. You will test access while both machines are connected to different networks. You will also set up another VPN to two clients from the other groups in your class and test the access of both the VPN nodes and the other computers in your classroom.

Develop your understanding

1. Search the Internet for a VPN hardware solution. Summarize your findings and determine how this hardware solution compares to possible software solutions.
2. Summarize and describe the following VPN protocols:
    a. L2TP
    b. IPSEC
3. Create a secure network and attempt to access it. Record the network traffic and highlight the frames that transport your attempts.
4. Set up a VPN and repeat step 3.