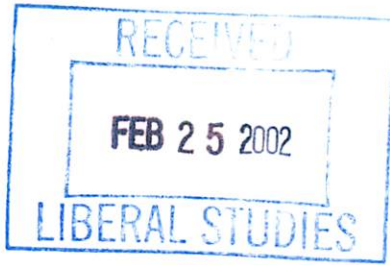LSC Use Only
Number: _____
Submission Date: _____
Action-Date: _____

UWUCC USE Only
Number: _____ 01-57d
Submission Date: _____
Action-Date: _____

UWUCC - App 3/19/02
Senate App. 5/7/02

CURRICULUM PROPOSAL COVER SHEET
University-Wide Undergraduate Curriculum Committee

I. **CONTACT**

Contact Person: **William Oblitey**   Phone: 357-4491

Department: **Computer Science**

II.   PROPOSAL TYPE (Check All Appropriate Lines)

_____ COURSE

    X   New Course*

_____ Course Revision

_____ Liberal Studies Approval +
for new or existing course

_____ Course Deletion

_____ Number and/or Title Change

_____ Course or Catalog Description Change

Network Security
Suggested 20 character title

COSC 356 Network Security
Course Number and Full Title

_____
Course Number and Full Name

_____
Course Number and Full Title

_____
Course Number and Full Title

_____
Old Number and/or Full Old Title

_____
New Number and/or Full New name

_____
Course Number and Full Title

PROGRAM: _____ Major _____ Minor _____ Track

_____ New Program*

_____ Program Revision*

_____ Program Deletion*

_____ Title Change

_____
Program Name

_____
Program Name

_____
Program Name

_____
Old Program Name

_____
New Program Name

III. Approvals (signatures and date)

_____
Department Curriculum Committee

_____ 02/19/02
College Curriculum Committee

_____
Department Chair

_____
College Dean

+ Director of Liberal Studies (where applicable)

*Provost (where applicable)

Part II Description of Curriculum Change

Format for Requesting New Course Proposals

Part I.   **New Course Proposal Cover Sheet for COSC 356. Network security.**

Part II.   **Description of Curricular Change**

        I.   This course is required as part of the new Computer Science/Information Assurance track and is a possible elective for Criminology majors in the new Information assurance minor. (see attached for a detailed description of the new syllabus of record.)

        2.   Course Analysis Questionnaire. Detailed answers to each of the questions have been included in the attachments.

Part III. **Letters of Support**

Letters of support from:
1. Dean Eck, supporting need for additional complement, should the need arise.
2. Louise Burkey, MIS Department Chair, supporting the new information assurance track.

COSC 356 - Network Security

3 lecture hours
0 lab hours
3 credits
(3c-0l-3sh)

I. Catalog Description

COSC 356   Network Security   3c-0l-3sh

Prerequisite: COSC 316 or COSC/IFMG 352

Explores mechanisms for protecting networks against attacks. The course emphasizes network security applications that are used on the Internet and for corporate networks. It investigates various networking security standards and explores methods for enforcing and enhancing those standards.

II.   Course Objectives

Upon successful completion of this course, the student should be able to:

     A.   Utilize network security tools.

     B.   Specify procedures for defending network systems.

     C.   Develop network security policies.

     D.   Recognize threats to network security.

     E.   Deter attacks on network systems.

     F.   Specify procedures for recovery from attacks on networks.

III.   Detailed Course Outline

1.   Network Security Modeling   (6 hours)
A look at possible security violations and the concerns they raise for securing networks. Accessing the security needs of an establishment; evaluating and choosing various security products and policies. An overview of the common security services that is currently available.

2.   Network Systems Communication   (3 hours)
Overview computer network systems communication. An examination of the frames and packets of various protocols that travel the Internet. Analysis of data at the various layers on the Internet using the Open Systems Interconnection (OSI) Reference Model and comparing with the (Institute of Electrical and Electronic Engineers (IEEE) implementation. A study of different routing mechanisms and routing tables. Comparison and contrast of connectionless and connection-oriented communications.

3.   Security Breaches of Interconnected Devices   (6 hours)
A study of the communication properties of network transmissions; digital communications;

electromagnetic interference, etc. A look at the various hardware devices on the network and their contribution to the security of the overall network.

4.   Authentication and Encryption Control   (3 hours)
Study of methods of ensuring that both ends of a communications connection are identifiable and verifiable. Examination of various cryptographic methods. Comparing and contrasting public key and private key cryptographic systems.

5.   Access Control and Detection Systems   (6 hours)
A look at systems for enforcing access control policies: firewalls and proxy servers. Analysis of packet filtering devices and their respective methods of approach to security enhancement. An examination of the strengths and weaknesses of intrusions detection systems.

6.   Virtual Private Networks   (6 hours)
An explanation of how encryption and authentication of a communication channel on a public network constitute a virtual private network. The process of ensuring the security of a virtual private network. Examination of some alternatives to virtual private networks.

7.   Averting Intruders and Viruses   (6 hours)
Establishing the meanings and differences between viruses, Trojans, and worms on the network. A look at various preventive measures used in combating such intrusive elements.

8.   Security Design Issues   (4 hours)
Analysis of the threats that the network system faces. A look at various principles that go into the design on security policies. Design of an authentic security policy.

9. Two class tests	(2 hours)
Total **=**	**42 hours**

IV.   Evaluation Methods

20%   Homework assignments and Research paper.
40%   Examinations. Two in-class exams and a final exam all of which count equally toward the 40%. Examinations consist of short-answer, analysis, and what-if questions.
40%   Project. Selected projects covering various aspects of network security, especially those that cannot be covered exhaustively in class discussions.

Grading Scale: The standard grading scale will be used.
      90%+=A; 80-89%=B; 70-79%=C; 60-69%=D; below 60%=F.

V.   Required Textbook(s), Supplementary Books and Readings

Maiwald, Eric (2000), *Network Security: A Beginner's Guide*, Osborne/McGraw-Hill, Boston, MA. Several handouts will be given to provide students with guidance with the projects. The professor has other related material that will be placed on reserve for students' use during the progress of the course.

VI.   Special Resource Requirements
None

VII.   Bibliography

1. Benton, Chris (1999), *Mastering Network Security*, SYBEX, Inc., San Francisco.
2. Brown, Keith (2000), *Programming Windows Security*, Addison-Wesley, Reading, MA.
3. Frisch, A. and Loukides (1995), *Essential System Administration*, 2nd Ed. O'Reilly & Associates, Inc., Sebastopol, CA.
4. Garfinkel, S., Spafford, G., and Russell D. (1995), *Practical UNIX and Internet Security*, 2nd Ed. O'Reilly & Associates, Inc., Sebastopol, CA.
5. Hatch, B., Lee, J., Kurtz, G. (2001), *Hacking Linux Exposed: Linux Security Secrets & Solutions*, Osborne/McGraw-Hill, Berkeley, CA.
6. Russell, R. and Cunningham S. (2000), *Hack Proofing Your Network: Internet Tradecraft*, Syngress Publishing, Rockland, MA.
7. Scambray, J. and McClure, S. (2000), *Network Security Secrets & Solutions*, McGraw-Hill, Boston, MA.
8. Schneier, B. (2000), *Digital Security in a Networked World*, John Wiley & Sons, Somerset, NJ.
9. Stallings, W. (2000), *Network Security Essentials: Applications and Standards*, Prentice-Hall, Inc., Upper Saddle River, NJ.
10. Wadlow, Thomas A. (2000), *The Process of Network Security: Designing and Managing a Safe Network*, Addison Wesley Longman, Inc., Reading, MA.

Course Analysis Questionnaire

Section A: Details of the Course

A1.   How does this course fit into the programs of the department? For what students is the course designed? (Majors, students in other majors, liberal studies).

Network security addresses the issues of security involved with networked computers. With increasing use of networks due to the Internet and electronic commerce, issues in network security have become essential for both corporations and small businesses.   Many of our interns and graduates go to companies to function as network managers and therefore need to know about network security. The department, at the moment, does not have any course, which explicitly teaches the ideas of network security. The course is designed for the proposed Information Assurance track in Computer Science and for the proposed interdisciplinary minor in Cybersecurity with the Department of Criminology although all students with the necessary background will be accepted.

A2.   Does this course require changes in the content of existing courses or requirements for a program?

The course does not require changes in the contents of any of our existing courses. It will serve as a controlled elective for Computer Science majors and a choice for Criminology majors in the proposed new Information Assurance minor.

A3.   Has this course ever been offered at IUP on a trial basis (e.g. as a special topic)? If so, explain the details of the offering.

The course has not been previously offered at IUP.

A4.   Is this course to be a dual-level course? If so, what is the approval status at the graduate level?

The course is not intended to be listed as dual level.

A5. If this course may be taken for variable credit, what criteria will be used to relate the credits to the learning experience of each student? Who will make this determination and by what procedures?

The course may not be taken for variable credit.

A6. Do other higher education institutions currently offer this course? If so, please list examples.

Quite a number of universities and colleges offer this course in various forms and modifications. For example, Carnegie-Mellon University offers the course as network security.

A7. Is the content, or are the skills, of the proposed course recommended or required by a professional society, accrediting authority, law or other external agency? If so, please provide documentation. Explain why this content or these skills cannot be incorporated into an existing course.

The Association for Computing Machinery (ACM) does not explicitly recommend this course. The National Colloquium for Information Systems Security Education (NCISSE) includes this course in the list of courses that it accepts for granting an institution its designation as Center for Excellence in Information Assurance Education.

Section B: Interdisciplinary Implications

B1. Will this course be taught by one instructor or will there be team-teaching? If the latter, explain the teaching plan and its rationale.

The course is designed to be taught by one instructor.

B2. What is the relationship between the content of this course and the content of courses offered by other departments? Summarize your discussions (with other departments) concerning the proposed changes and indicate how any conflicts have been resolved. Please attach relevant memoranda from these departments that clarify their attitudes toward the proposed change(s).

This course does not overlap with any other course at this University.

B3. Will seat in this course be made available to students in the School of Continuing Education?

Students from the School of Continuing Education who meet the prerequisites are encouraged to take this course.

Section C: Implementation

C1. **Are faculty resources adequate? If you are not requesting or have not been authorized to hire additional faculty, demonstrate how this course will fit into the schedules of current faculty. What will be taught less frequently of in fewer sections to make this possible?**

Faculty resources may not be adequate. We have a letter from Dr. Eck after consultation with the President and Provost supporting the hiring of new faculty should the need arise. (see attachment).

C2. **What other resources will be needed to teach this course and how adequate are the current resources? If not adequate, what plans exist for achieving adequacy? Reply in terms of the following:**

Resources needed for this course are available although they can be improved.
- a. **Space:** Classroom space is adequate.
- b. **Equipment:** The equipment needed for this course has been purchased with funds from the NSF Cybersecurity grant.
- c. **Library Materials:** These are being purchased with funding from the NSF grant.
- d. **Laboratory Supplies and other Consumable Goods:** The Computer Science department has licensed copies of network operating systems and some applications software for projects. However, periodic updates will be required to keep up with the technology.
- e. **Travel Funds:** No travel funds are currently needed.

C3. **Are any of the resources for this course funded by a grant? If so, what provisions have been made to continue support for this course once the grant has expired? (Attach letters of support from Dean, Provost, etc.)**

The NSF cybersecurity grant helped purchase the equipment needed for the hands-on laboratory portion of this course. When the program progresses and the grant is no more, the Dean has committed to support the maintenance of the course (see attachment).

C4. **How frequently do you expect this course to be offered? Is this course particularly designated for or restricted to certain seasonal semesters?**

The course is expected to be offered every other academic year. If demand increases, the frequency of offering will be increased accordingly.

C5. **How many sections of this course do you anticipate offering in any single semester?**

It is anticipated that one section of the course will be offered each time. Again, based on demand, this can be increased.

C6. **How many students do you plan to accommodate in a section of this course? Is this planned number limited by the availability of any resources? Explain.**

Twenty-four students will be accommodated in a section of the course. Available machines and space in the lab dictate this limitation. When more space and equipment become available enrollment can be increased.

C7. **Does any professional society recommend enrollment limits or parameters for a course of this nature? If they do, please quote from the appropriate documents.**

No professional society recommends enrollment limits or parameters for this course or for courses resembling this course. However, past experience with hands-on courses that are taught in computer labs has shown that twenty-four students per section can be accommodated.