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

FEB 25 2002
LIBERAL STUDIES

UWUCC USE Only
Number: 01-57C
Submission Date: _____
Action-Date: UWUCC - 3/19/02
Senate 5/7/02

APR - 1 2002

CURRICULUM PROPOSAL COVER SHEET
University-Wide Undergraduate Curriculum Committee

I. CONTACT

Contact Person Dr. Mary Micco Phone 7-2637
Department Computer Science

II. PROPOSAL TYPE (Check All Appropriate Lines)

_____ **COURSE**

Cybersecurity Basics
Suggested 20 character title

__X__ New Course* — COSC 316 Cybersecurity Basics (Course Number and Full Title)

___ Course Revision — Course Number and Full Title

___ Liberal Studies Approval+ for new or existing course — Course Number and Full Title

___ Course Deletion — Course Number and Full Title

___ Number and/or Title Change — Old Number and/or Full Old Title; New Number and/or Full New Title

___ Course or Catalog Description Change — Course Number and Full Title

_____ **PROGRAM:** _____ Major _____ Minor _____ Track

___ New Program* — Program Name

___ Program Revision* — Program Name

___ Program Deletion* — Program Name

___ Title Change — Old Program Name; New Program Name

III. Approvals (signatures and date)

Department Curriculum Committee — Department Chair

College Curriculum Committee 3/19/02 — College Dean

Director of Liberal Studies (where applicable) — *Provost (where applicable)

Format for Requesting New Course Proposals

Part I. **New course proposal for COSC 316 Cybersecurity Basics**

Part II. **Description of Curricular Change**

1. This course is required as part of the new Computer Science/Information Assurance track and the Information Assurance minor. See the detailed course description in Attachment A.

2. Course Analysis Questionnaire. Detailed answers to each of the questions have been included as Attachment B.

Part III. **Letters of Support**

Letters of support from:
1. Dean Eck, supporting need for additional complement if necessary.
2. Louise Burkey, MIS Department Chair, supporting the new track proposal including this course.

NEW Syllabus of Record

COSC 316 Cybersecurity Basics

0 lab hours
3 lectures hours
3 credits
3c-0l-3sh

I. Course Description

COSC 316 Cybersecurity Basics 3c-0l-3sh

Prerequisites: COSC 110 or equivalent programming course, junior standing or permission of instructor.

Provides an introduction to the theory and concepts of computer security in networked systems. The course will look at security issues and policies with regard to hardware, software development, databases, operating systems and networks as well as the use of encryption. The more common attacks on systems will be covered. Vulnerability assessment tools and techniques for defending systems will be explored in various projects.

II. Course Objectives

Upon successful completion of this course, the students will:
1. model the security risks in a network.
2. write a suitable set of security policies for different scenarios.
3. apply various access control techniques.
4. become familiar with the basic tools and techniques used by hackers to attack systems.
5. assess network and system vulnerabilities to these attacks and learn countermeasures.
6. log data on simulated attacks and analyze the logs and other audit controls.
7. gain skill in cyberforensics.
8. be familiar with existing and proposed legislation related to all types of cybercrime.
9. be aware of the importance of ethical conduct.

III. Course Outline

A. Major categories of threats (Attack) 2 weeks
- Wiretapping
- Impersonation/social engineering
- Foot printing
- Packet Sniffing

B. Network attacks/access controls 1 week
- Access controls
- Denial of service
- Email/web hacks
- Other forms of attack
- Risk analysis

C. Security goals/policies. 1 week

D. Security in networks and distributed systems (Defend) 2 weeks
- Network overview: Traffic control
- Firewalls/proxy servers

- Protection schemes.
- Vulnerability assessment tools

E. Audit controls, Logging and log analysis (Convict)	1 week
F. Basic Encryption and Decryption /Protocols and Practices.	2 weeks
G. Program security. • Viruses and other malicious code • Controls against program threats	1 week
H. Protection in General Purpose Operating Systems	1 week
I. Database/web security	1 week
J. Legal Issues in Computer Security	1 week
K. Ethical Issues in Computer Security	1 week
Total=	**14 weeks (including two class tests)**

IV. Evaluation Methods

1. Classroom activities and exercises: 30%. There will be graded assignments involving hands-on exercises or problem solving in the classroom. Outside class readings are required in association with these activities.

2. Assignments: 30%. Students will have 3 research papers to complete outside of class time.

3. Exams and quizzes. 40%. Students will be evaluated on their understanding of the concepts presented using short essay questions on the readings and class material. There will be several quizzes (collectively counting 10%), a mid-term exam (15%) and a final exam (15%).

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

V. Required Textbook:

Garfinkel, Simson CISSP, Gene Spafford (1998), Practical UNIX & Internet Security, O'Reilly & Associates, ISBN: 1565921488
Supplemented by:
Hatch, Brian, James Lee, and George Kurtz (2001), Hacking Linux Exposed: Network Security Secrets and Solutions, Osborne/McGraw Hill, ISBN 0-07-212127-0

VI. Special Resource Requirements

None.

VII. Bibliography

1. Brenton, Chris (1999), Mastering Network Security. Network Press, (SYBEX)
ISBN 0-7821-2343-0

2. Denning, Dorothy E. (1999), Information Warfare and Security. Addison-Wesley, ISBN 0-2014-3303-6

3. Krause, Micki, Harold F. Tipton, Editors (2000), Handbook of Information Security Management. Auerbach, ISBN 0-8493-9829-0

4. Krist, Martin A. (1999), Standard for Auditing Computer Applications. Auerbach, ISBN 0-8493-9983-1

5. McClure, Stuart, Joel Scambray, and George Kurtz (1999), Hacking Exposed: Network Security Secrets and Solutions, Osborne/McGraw Hill, ISBN 0-07-212127-0

6. Nichols, Randall K.,Daniel J. Ryan, and Julie J.C.H. Ryan,(2000), Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves. McGraw Hill, ISBN 0-07-212285-4

7. Schwartau, Winn (1999), Time-Based Security, Practical and Provable Methods to Protect Enterprise and Infrastructure Networks and Nation. Interpact Press, ISBN 0-9628700-4-8

8. Schneier, Bruce (1996), Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley and Sons, ISBN 0-471-11709-9

9. Scott, Charlie, Paul Wolfe, and Mike Erwin (1999), Virtual Private Networks. 2nd Edition O'Reilly and Associates, ISBN 1-56592-529-7

10. Tiwana , Amrit (1999), Web Security. Butterworth-Heinemann, ISBN 1-55558-210-9 2nd Edition

11. Class web site: http://penguin.nsm.iup.edu/security/bibliography.htm

Syllabus of Record: COSC 316. Cybersecurity Basics

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).

This course is designed as one of five courses for an upper level track in information assurance for Computer Science majors. It will be required for all students in the information assurance track and in the information assurance minor.

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

Yes. It is being submitted as part of a new Information Assurance track proposal in the Computer Science Department included with this course proposal. It is also included in the proposal for a Cybersecurity 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.

No. However we ran a NSF funded faculty workshop and invited a professor from James Madison University, a Center for Excellence in Information Assurance Education, to come and teach it the first time in Summer 2001. Several of our students completed this workshop. It is being offered as a Special topics course in Spring 2002.

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

No

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?

This course cannot be taken for variable credit.

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

James Madison University and some 25 other centers for Excellence in Information Assurance Education offer this course.

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.

Universities are being encouraged to develop programs in information assurance by the federal government. Our Information Assurance track and the interdisciplinary minor in cybersecurity are unique approach to this initiative. It is required if we are to be successful in obtaining accreditation as a Center for Excellence in Information Assurance Education from National Colloquium for Information Systems Security Education (NCISSE).

Syllabus of Record: COSC 316. Cybersecurity Basics

NEW Syllabus of Record

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.

This course will 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, which clarify their attitudes toward the proposed change(s).

N/A

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

Yes. Seats will be made available for Continuing Education.

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 or 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:

Space: We have obtained space for a new lab in Stright Room 107A. The lab is now operational.

Equipment: The NSF grant has paid for the new equipment in the lab and lab supplies.

Library Materials: These are being purchased with funding from the grant.

Travel Funds: None required. Students will not be required to travel.

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 initial preparation, start up and lab were funded by the grant. Once the program is under way, the Dean has committed to provide the support that is needed to be self-maintaining as part of our regular curriculum.

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

At least once yearly, but as demand increases we may offer this course once a semester.

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

One.

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.

We plan to accommodate 24 students in each section offered. The number is limited by the seats available in the lab. When more space and machine become available enrolment 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.

Section D: Miscellaneous

Include any additional information valuable to those reviewing this new course proposal.
We expect to be able to obtain additional funding for this program, particularly in the form of scholarships for students, internships and other support for a cybersecurity center.