CGS Agenda Item:16-49
Effective Spring 2017

Eastern Illinois University
New Course Proposal
CIT 4833, Cybersecurity Intrusion Detection and Prevention Systems

Banner/Catalog Information (Coversheet)

1. **_X_ New Course or _____Revision of Existing Course**
2. **Course prefix and number:** CIT 4833
3. **Short title:** _Intrusion Detection__
4. **Long title:** Cybersecurity Intrusion Detection and Prevention Systems
5. **Hours per week:** __2_ Class _2__ Lab _3__ Credit
6. **Terms:** __ Fall ___ Spring ___ Summer __X_ On demand
7. **Initial term**: ___ Fall _X__ Spring ___ Summer Year: _2017
8. **Catalog course description:** A study of principles and applications of Cybersecurity Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS).
9. **Course attributes: N/A**

   General education component: _____N/A_____

   ___ Cultural diversity ___ Honors ___ Writing centered ___ writing intensive ___Writing active
10. **Instructional delivery**
    Type of Course:

    ___ Lecture ___ Lab _X__ Lecture/lab combined ___ Independent study/research

    ___ Internship ___ Performance ___ Practicum/clinical ___ Other, specify: _____

    Mode(s) of Delivery:

    _X_ Face to Face __ online ___ Study Abroad X Hybrid

    Specify approximate amount of on-line and face-to-face instruction: 30% Face-to-face and 70% Online
11. Course(s) to be deleted from the catalog once this course is approved. __NONE
12. **Equivalent course(s):** _____NONE_____

    a. Are students allowed to take equivalent course(s) for credit? ___ Yes _X_ No
13. **Prerequisite(s): ___AET 2523 _____**

    a. Can prerequisite be taken concurrently? ___ Yes X_ No

    b. Minimum grade required for the prerequisite course(s)? _C__

    c. Use Banner coding to enforce prerequisite course(s)? _X_ Yes ___ No

d. Who may waive prerequisite(s)?

___ No one _X__ Chair __ Instructor ___ Advisor ___ Other (specify)

14. Co-requisite(s): __NONE_____

15. Enrollment restrictions

a. Degrees, colleges, majors, levels, classes which <u>may</u> take the course: _Completion of 75 hours in CIT, AET or MIS major or a graduate student.

b. Degrees, colleges, majors, levels, classes which may <u>not</u> take the course: __ALL OTHERS

16. Repeat status: _X_ May not be repeated with credit __ May be repeated once with credit

17. Enter the limit, if any, on hours which may be applied to a major or minor: _3__

18. Grading methods: _X_ Standard ___ CR/NC __ Audit ___ ABC/NC

19. Special grading provisions:

___ Grade for course will not count in a student's grade point average.

___ Grade for course will not count in hours toward graduation.

___ Grade for course will be removed from GPA if student already has credit for or is registered in: _____

___ Credit hours for course will be removed from student's hours toward graduation if student already has credit for or is registered in: _____

20. Additional costs to students:
Supplemental Materials or Software_____

Course Fee _X_ No ___Yes, Explain if yes_____

21. Community college transfer:

___ A community college course may be judged equivalent.

_X__ A community college may not be judged equivalent.

Note: Upper division credit (3000+) will not be granted for a community college course, even if the content is judged to be equivalent.

Rationale, Justifications, and Assurances (Part I)

1. X Course is required for the major(s) of Computer and Information Technology
   ___Course is required for the minor(s) of _____
   ___Course is required for the certificate program(s) of _____
   ___ Course is used as an elective

2. **Rationale for proposal:**

   By examining some of the computer- related crimes that have been committed over the last 20 years, it is a priority for students graduating from the Computer & Information Technology program to understand the threats and security issues that surround computer systems and networks. It is also necessary for them to have the tools and skills to protect computer systems and networks properly. The building blocks of secure and modern network and information systems are founded in the proper combinations of IDS's and IPS's systems.

3. **Justifications for (answer N/A if not applicable)**

   Similarity to other courses: None

   Prerequisites: AET 2523, students need to know the fundamentals of data telecommunications, routing and switching in order to be able to pass this course.

   Co-requisites: N

   Enrollment restrictions: Completion of 75 hours in CIT, AET or MIS majors or a graduate student. Students in these majors have the necessary background to successfully pass this course.

   Writing active, intensive, centered: N/A

4. **General education assurances (answer N/A if not applicable)**

   General education component: N/A

   Curriculum: N/A

   Instruction: N/A

   Assessment: N/A

5. Online/Hybrid delivery justification & assurances (answer N/A if not applicable)

Online or hybrid delivery justification: *The content and structure for this course relies upon independent research, in-depth group discussion, and video based lecture. As compared to many lab courses already offered in technology area, this course requires online delivery of lecture and discussion and face-to-face lab activities for applied projects. For content delivered online, the course employs online video presentations, structured web discussions focused on reading assignments, and linked to articles submitted to the instructor. Students are required to draw on research and review of articles to discuss and develop fundamental procedural knowledge of application. Discussions invite students to explore in more detail the required knowledge and procedures to create various web publishing tools and media. Discussions and examinations will be administered and submitted via the online course management tool. Three years ago this course would have been impossible to be delivered online. Since then, several video tools are now available for editing and manipulation. Many software design companies have made their software tools more readily accessible for students. The Internet connection speed for many users has increased thereby allowing for higher quality rich media instruction to be delivered. Finally, the course management tools that the university now uses allows there to be a richer interaction between students and faculty. To accommodate this situation, many of the given activities may be completed in a hybrid format.*

Instruction: *This course employs instructor led online presentations, student reading assignments, student applied design assignments, peer critique and troubleshooting, student presentations, and examinations. After reviewing the instructor led presentations and completing the student reading assignments, students will be required to draw on what they have read and then to apply it to a context of creating graphics for personal or organizational applications. While working on these projects, students may engage in the activity of troubleshooting or critique while posting their work in an online discussion board for both classmates and the instructor to provide feedback and guidance. Presentations will provide learners a forum to share the results of their work and receive further feedback. Reading assignments, applied projects, and examinations will be administered, collected, and/or submitted via the online course management tool. Presentations may also be delivered in the course tool or face-to-face. All faculty who will deliver this course online are/will be OCDi (or appropriate equivalent) trained.*

Integrity: *Work submitted online, such as discussions and examinations, will be substantiated via learners providing citation in APA format and submitting related articles to quantify work. Further, the length, frequency, quality, and integrity of discussion posts can be monitored via the online course management tool. Examinations will require the same of learners and additionally will use software tools to check work for the integrity and authenticity of submitted assignments. The examinations will be time restricted and of sufficient length to prohibit consultation of unauthorized sources. Work submitted face-to-face in applied lab projects will be checked for authenticity via the individualized nature of project completion. Requirements for projects will require learners to engage in activities that require creation of original content for either themselves or local entity.*

Interaction: *For online content, the course employs email, web-based discussions, exploration of off-site Internet resources, web-based presentations, web chat rooms and lab based applied project work. The instructor will communicate with students through the online discussion board and web-based discussions. Email may also be a tool used for the instructor to communicate with an individual student or to post course announcements. The learners for this course may also communicate with one another for these tools. During digital office hours, the instructor will remain available for discussion during certain times and communicate using a chat room tool in the learning management system. For face-to-face interaction, the instructor may communicate synchronously with the learners during open lab activities and during office hours. The learners are also free to communicate with other learners during lab activities.*

Model Syllabus (Part II)

Please include the following information:

1. Course number and title

CIT 4833 "Cybersecurity Intrusion Detection and Prevention Systems"

2. Catalog description

A study of principles and applications of Cybersecurity Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS)

3. Learning objectives.

Upon completion of this course, students will be able to:

1. Design/describe the appropriate Intrusion detection and Intrusion prevention system's computer security layouts for different security risks situations. (SL 1-3, CT 1-4, WR 1-4, QR 1-5, Grad 1)
2. Apply computer risk assessment and computer vulnerability analysis techniques. (CT 1-4, WR 1-4, QR 1-5, Grad 1, 2, 3, 4)
3. Demonstrate skills and knowledge to set up conventional WANs, LANs, servers, Routers and Firewalls to assure computer and network security. (CT 1-4, WR 1-4, QR 1-5, Grad 1)
4. Analyze issues related with information security, homeland security and their repercussions in today's world. (CT 1-4, WR 1-4, QR 1-5, Grad 1, 2, 3, 4)

GRADUATE LEARNING GOALS

Objective	Depth of Content knowledge	Critical thinking and problem solving	Oral and/or written communication	Advance scholarship through research and creative activity
1	X		X	
2	X	X	X	X
3	X			
4	X	X	X	X

UNDERGRADUATE LEARNING GOALS

Objective	Speaking and Listening	Critical Thinking	Writing and Critical Reading	Quantitative Reasoning	Responsible Citizenship
1	X	X	X	X	
2		X	X	X	
3		X	X	X	
4		X	X	X	X

4. Course materials.

- "Principles of Computer Security, CompTIA Security+ Exam SY0-401": Conklin and White 4th Edition, McGraw Hill, 2016

5. Weekly outline of content. (Face-to-Face Modality)

Meeting day (TH)	TOPICS	ACTIVITIES
Week 1	1. Introduction to security trends 2. General security concepts	- HW 1
Week 2	3. The role of people in security 4. Foundations of cryptography	- LAB 1
Week 3	5. Public Key Infrastructure	- HW 2
Week 4	6. Standards for infrastructure security	- LAB 2

Week 5	7. Wireless security	- MIDTERM 1
Week 6	8. Types of attacks and malicious software	- HW 3
Week 7	9. Web Components/ E-mail Instant messaging	- LAB 3
Week 8	10. Intrusion detections system and network Security I	- HW 4
Week 9	11. Intrusion detections system and network Security II	- LAB 4
Week 10	12. Intrusion Prevention Systems I	- MIDTERM 2
Week 11	13. Intrusion Prevention Systems II	- HW 5
Week 12	14. Intrusion Prevention Systems III	- LAB 5
Week 13	15. Risk management/ Change management	- HW 6
Week 14	16. Privilege management	- LAB 6
Week 15	17. Fundamentals of computer forensics	
Week 16	18.Legal issues and ethics	Final EXAM

Weekly outline of content (Hybrid Modality)

Meeting day (TH)	TOPICS	ACTIVITIES
Week 1	1. Introduction to security trends 2. General security concepts	
Week 2	3. The role of people in security	- HW 1
Week 3 :	4. Foundations of cryptography	- HW 2
Week 4: Face to Face meeting 8 am– 2 p.m.	Q & A/ Review For Weeks 1-3 5. Public Key Infrastructure 6. Standards for infrastructure security	- LAB 1 - LAB 2
Week 5	7. Wireless security	- MIDTERM 1
Week 6	8. Types of attacks and malicious software	
Week 7:	9. Web Components/ E-mail Instant messaging	- HW 3
Week 8: Face to Face meeting 8 am -2 p.m.	Q & A/ Review for weeks 5-7 10. Intrusion detections system and network Security I 11. Intrusion detections system and network Security II	- LAB 3 - LAB 4
Week 9	12. Risk management/ Change management	
Week 10	13. Privilege management	- HW 4
Week 11	14. Fundamentals of computer forensics	- HW 5
Week 12: Face to Face meeting 8 am -2 p.m.	Q & A / Review for weeks 9-11 15. Intrusion Prevention Systems I 16. Intrusion Prevention Systems II	-LAB 5 -LAB 6
Week 13	17. Intrusion Prevention Systems III	-MIDTERM 2
Week 14	18. Risk management	- HW 6
Week 15:	19. Change management	
Week 16: Face to face Meeting 8- noon	Q & A weeks 13-15 20. Legal issues and ethics	FINAL EXAM

6. Assignments and evaluation, including weights for final course grade.

	UNDERGRADUATE	GRADUATE
- 2 "MIDTERMS"	250 points	350 Points
- Laboratories	300 points	250 Points
- HOMEWORK	300 points	350 Points
- Final Project (In lieu of Final Exam)	150 points	200 Points
TOTAL	1000 Points	1150 Points

7. Grading scale.

The final undergraduate grade will be assigned based on the total points "**X**" earned as follows:

X ≥ 901: **A**; 801 ≤ **X** ≤ 900: **B**; 701 ≤ **X** ≤ 800: C 601 ≤ **X** ≤ 700: **D**; **X** ≤ 600: F

The final graduate grade will be assigned based on the total points "X" earned as follows:

X ≥ 1041: A; 920 ≤ **X** ≤ 1040: B; 801 ≤ **X** ≤ 920: C 701 ≤ **X** ≤ 800: D; **X** ≤ 700: F

8. Correlation of learning objectives to assignments and evaluation

Objective	Laboratories	HW Assignments	MIDTERMS	Final Exam
1. Design/describe the appropriate Intrusion detection and Intrusion prevention system's computer security layouts for different security risks situations. (SL 1-3, CT 1-4, WR 1-4, QR 1-5, Grad 1)	Lab 1, Lab2 (10%)	HW1, HW2 (10%)	Midterm 1(12.5%)	X
2. Apply computer risk assessment and computer vulnerability analysis techniques. (CT 1-4, WR 1-4, QR 1-5, Grad 1, 2, 3, 4)	Lab 3, Lab 4(10%)	HW 3, HW 4 (10%)	Midterm 2 (12.5%)	X
3. Demonstrate skills and knowledge to set up conventional WANs, LANs, servers, Routers and Firewalls to assure computer and network security. (CT 1-4, WR 1-4, QR 1-5, Grad 1)	Lab 5, Lab 6(10%)	HW 5, HW 6 (10%)		X
4. Analyze issues related with information security,				X (15%)

homeland security and their repercussions in today's world. (CT 1-4, WR 1-4, QR 1-5, Grad 1, 2, 3, 4)				

Date approved by the department or school: February 16/ 2016
Date approved by the college curriculum committee: 4/25/2016
Date approved by the Honors Council *(if this is an honors course):* Date approved by CAA: 4/28/2016 CGS: 5-3-16