

2014-2015 LONG SIGNATURE SHEET



UNC CHARLOTTE

Proposal Number: SIS 10-06-14

Proposal Title: Establish a graduate level course: Open Source Security Systems

Originating Department: Software and Information Systems (SIS)

TYPE OF PROPOSAL: UNDERGRADUATE GRADUATE X UNDERGRADUATE & GRADUATE
(Separate proposals sent to UCCC and Grad. Council)

DATE RECEIVED	DATE CONSIDERED	DATE FORWARDED	ACTION	SIGNATURES
9/20/2014	9/27/2014	9/27/2014	Approved	DEPARTMENT CHAIR Mary Lou Maher <i>Mary Lou Maher</i>
9/27/2014	10/6/2014	10/6/2014	Approved	COLLEGE CURRICULUM COMMITTEE CHAIR Yuliang Zheng <i>Yuliang Zheng</i>
10/7/2014	10/17/2014	10/20/2014	Approved	COLLEGE FACULTY CHAIR (if applicable) Srinivas Akella <i>A. Srinivas</i>
10/22/14			Approved	COLLEGE DEAN Yi Deng <i>Yi Deng</i>
			Approved	GENERAL EDUCATION (if applicable; for General Education courses) [print name here:]
			Approved	UNDERGRADUATE COURSE & CURRICULUM COMMITTEE CHAIR (for undergraduate courses only)
10-19-14	11-4-14	11-19-14	Approved	GRADUATE COUNCIL CHAIR (for graduate courses only) <i>Alan R. Freitag</i> ALAN R. FREITAG
				FACULTY GOVERNANCE ASSISTANT (Faculty Council approval on Consent Calendar)
				FACULTY EXECUTIVE COMMITTEE (if decision is appealed)



UNC CHARLOTTE

LONG FORM COURSE AND CURRICULUM PROPOSAL

*To: The Graduate Council

From: College of Computing and Informatics

Date: 10/06/2014

Re: The establishment of a new course: ITIS 6250/8250 Open Source Security Systems

The Long Form is used for major curriculum changes. Examples of major changes can include: creation of a new major, creation of a new minor, creation of a new area of concentration, or significant changes (more than 50%) to an existing program (Note: changing the name of an academic department does not automatically change the name(s) of the degree(s). The requests must be approved separately by the Board of Governors.)

Submission of this Long Form indicates review and assessment of the proposed curriculum changes at the department and collegiate level either separately or as part of ongoing assessment efforts.

*Proposals for undergraduate courses should be sent to the Undergraduate Course and Curriculum Committee Chair. Proposals related to both undergraduate and graduate courses, (e.g., courses co-listed at both levels) must be sent to both the Undergraduate Course and Curriculum Committee and the Graduate Council.

I. HEADING AND PROPOSAL NUMBER.

University of North Carolina at Charlotte

New Graduate

Course and Curriculum Proposal from: Department of Software and Information Systems

Title: Establishment of a new course: ITIS 6250/8250 Open Source Security Systems

II. CONTENT OF PROPOSAL.

A. PROPOSAL SUMMARY.

1. **SUMMARY.** State clearly and concisely the actions proposed (e.g., “the Biology Department proposes to add four new elective courses to the undergraduate curriculum: BIO 2222, BIO 3456, BIO 2345, and BIO 3210).

The Department of Software and Information Systems (SIS) proposes to add a new course, ITIS 6250/8250 Open Source Security Systems, to its graduate curriculum. This course is intended for SIS majors at the masters and PhD levels.

B. JUSTIFICATION.

1. Identify the need addressed by the proposal and explain how the proposed action meets the need.

The past decade has witnessed an accelerated trend towards open source solutions in the field of information technology. This is particularly true with systems that must embody security and privacy for them to function properly. IT vendors such as IBM, Google and Oracle have long been developing and distributing security related open source software tools. More recently, with partial funding from the federal government, major IT vendors have formed the Open Information Security Foundation (OISF) with the aim of developing and promoting the next generation open source internet security software tools. Mirroring the movement towards open source in industries, government agencies are acquiring more open source based products as part of their procurement strategies. This is evidenced by the active participation in the Military Open Source Software (Mil-OSS, mil-oss.org) by the Department of Defense since 2009, and the founding of the Homeland Open Source Technology (HOST) program by the Department of Homeland Security in 2011. Both organizations share a similar mission in investigating open source security methods, models and technologies and identifying viable and sustainable open source approaches that support the nation’s cyber security objectives.

These developments have triggered a rising demand for computing professionals who have mastered knowledge and skills in designing, implementing, evaluating and

maintaining security and privacy systems that are built on open source technologies. This course will prepare students to meet the rising demand.

2. Discuss prerequisites/corequisites for course(s) including class-standing, admission to the major, GPA, or other factors that would affect a student's ability to register.

The pre/co-requisite of this course is "ITIS 6200 Principles of Information Security and Privacy." Knowledge of computing systems and key concepts in cyber security covered in ITIS 6200 help students master open source security technologies to be taught in this course. Students may take this course either after completing ITIS 6200 or concurrently with ITIS 6200.

3. Demonstrate that course numbering is consistent with the level of academic advancement of students for whom it is intended.

The course is intended for graduate students interested in open source security. The numbering (6250/8250) reflects the fact that the course will be typically taken by graduate students either after or concurrently with "ITIS 6200/8200 Principles of Information Security and Privacy."

4. In general, how will this proposal improve the scope, quality and/or efficiency of programs and/or instruction?

This proposal represents the first course to be developed by SIS to prepare its graduate students to master advanced techniques for security application and system development using open source technologies.

5. If course(s) has been offered previously under special topics numbers, give details of experience including number of times taught and enrollment figures.

C. IMPACT. Changes to courses and curricula often have impacts both within the proposing department as well as campus-wide. What effect will this proposal have on existing courses and curricula, students, and other departments/units? Submit an Impact Statement that fully addresses how you have assessed potential impacts and what the impacts of this proposal might be. Consider the following:

1. What group(s) of students will be served by this proposal? (Undergraduate and/or graduate; majors and/or non-majors, others? Explain). Describe how you determine which students will be served.

This course is designed for graduate students who wish to learn techniques for designing security systems using open source technologies. Students with an understanding of software systems and security concepts will be ready to learn how to use open source tools to enhance the security and privacy of applications and systems.

2. What effect will this proposal have on existing courses and curricula?

a. When and how often will added course(s) be taught?

ITIS 6250/8250 will be taught every other semester (Fall or Spring, starting from Fall 2015).

b. How will the content and/or frequency of offering of other courses be affected?

There will be no impact on the content or frequency of offering of other courses.

c. What is the anticipated enrollment in course(s) added (for credit and auditors)?

The anticipated enrollment of ITIS 6250/8250 is approximately 15-20 students per class.

d. How will enrollment in other courses be affected? How did you determine this?

The course is not expected to significantly change the enrollment of other courses. This was determined by the projected growth in the number of students who would enroll in SIS graduate programs in future.

e. Identify other areas of catalog copy that would be affected, including within other departments and colleges (e.g., curriculum outlines, requirements for the degree, prerequisites, articulation agreements, etc.)

This course will be added to lists of available courses for concentrations for Master of Science in Information Technology (MSIT).

III. RESOURCES REQUIRED TO SUPPORT PROPOSAL.

When added resources are not required, indicate “none”. For items which require “none” explain how this determination was made.

A. **PERSONNEL.** Specify requirements for new faculty, part-time teaching, student assistants and/or increased load on present faculty. List by name qualified faculty members interested in teaching the course(s).

No new or part-time faculty is required in order to offer this course; nor will this course introduce an increased teaching load on present faculty.

Faculty qualified to teach this course includes Dr. Yuliang Zheng, Dr. Yongge Wang, and most other faculty members in information security.

B. PHYSICAL FACILITY. Is adequate space available for this course?

The course requires a standard class room and will be usually offered in the evening to cater for part time graduate students. It is not expected to add significant pressure to existing demand for space.

C. EQUIPMENT AND SUPPLIES: Has funding been allocated for any special equipment or supplies needed?

The College of Computing and Informatics (CCI) has the basic hardware and software infrastructure needed to teach this course. No additional equipment or supplies are needed for the proposed course.

D. COMPUTER. Specify any computer usage (beyond Moodle) required by students and/or faculty, and include an assessment of the adequacy of software/computing resources by available for the course(s).

Existing computer laboratories on campus or students' own personal computers will suffice as a computational platform for this course.

E. AUDIO-VISUAL. If there are requirements for audio-visual facilities beyond the standard classroom podiums, please list those here.

Current facilities are adequate to support this course.

F. OTHER RESOURCES. Specify and estimate cost of other new/added resources required, e.g., travel, communication, printing and binding.

None.

G. SOURCE OF FUNDING. Indicate source(s) of funding for new/additional resources required to support this proposal.

None.

IV. CONSULTATION WITH THE LIBRARY AND OTHER DEPARTMENTS OR UNITS**A. LIBRARY CONSULTATION.** Indicate written consultation with the Library Reference Staff at the departmental level to ensure that library holdings are adequate to support the proposal prior to its leaving the department. (Attach copy of [Consultation on Library Holdings](#)).

Consultation was initiated on Feb. 13, 2014 and approved by Library on the same day.

- B. CONSULTATION WITH OTHER DEPARTMENTS OR UNITS.** List departments/units consulted in writing regarding all elements outlined in IIC: Impact Statement, including dates consulted. Summarize results of consultation and attach correspondence. Provide information on voting and dissenting opinions (if applicable).

This course is not expected to overlap with other graduate courses on campus. Consultation with the following Departments has been initiated: Department of Bioinformatics and Genomics and Department of Computer Science on Feb. 13, 2014. Approvals were received on Feb. 13 and Feb. 21, 2014, respectively.

V. INITIATION, ATTACHMENTS AND CONSIDERATION OF THE PROPOSAL

- A. ORIGINATING UNIT.** Briefly summarize action on the proposal in the originating unit including information on voting and dissenting opinions.

Approved by the Department of Software and Information Systems on 9/29/2014. Approved by the College of Computing and Informatics Graduate Committee on 10/6/2014. Approved by faculty of the College of Computing and Informatics on 10/17/2014.

- B. CREDIT HOUR. (Mandatory if new and/or revised course in proposal)**

Review statement and check box once completed:

- The appropriate faculty committee has reviewed the course outline/syllabus and has determined that the assignments are sufficient to meet the University definition of a [credit hour](#).

- C. ATTACHMENTS.**

1. CONSULTATION: Attach relevant documentation of consultations with other units.
2. COURSE OUTLINE/SYLLABUS: For undergraduate courses attach course outline(s) including basic topics to be covered and suggested textbooks and reference materials with dates of publication. For Graduate Courses attach a course syllabus. Please see Boiler Plate for Syllabi for New/Revised Graduate Courses.
3. PROPOSED CATALOG COPY: Copy should be provided for all courses in the proposal. Include current subject prefixes and course numbers, full titles, credit hours, prerequisites and/or corequisites, concise descriptions, and an indication of when the courses are to be offered as to semesters and day/evening/weekend. Copy and paste the [current catalog copy](#) and use the Microsoft Word "track changes" feature (or use red text with "~~strikethrough~~" formatting for text to be deleted, and adding blue text with "underline" formatting for text to be added).

a. For a new course or revisions to an existing course, check all the statements that apply:

- This course will be cross listed with another course.
 There are prerequisites for this course.
 There are corequisites for this course.
 This course is repeatable for credit.
 This course will increase/decrease the number of credits hours currently offered by its program.
 This proposal results in the deletion of an existing course(s) from the degree program and/or catalog.

For all items checked above, applicable statements and content must be reflected in the proposed catalog copy.

b. If overall proposal is for a new degree program that requires approval from General Administration, please contact the facultygovernance@uncc.edu for consultation on catalog copy.

4. ACADEMIC PLAN OF STUDY (UNDERGRADUATE ONLY): Does the proposed change impact an [existing Academic Plan of Study](#)?

- Yes. If yes, please provide updated Academic Plan of Study in template format.
 No.

5. STUDENT LEARNING OUTCOMES (UNDERGRADUATE & GRADUATE): Does this course or curricular change require a change in Student Learning Outcomes (SLOs) or assessment for the degree program?

- Yes. If yes, please provide updated SLOs in template format.
 No.

6. TEXTBOOK COSTS: It is the policy of the Board of Governors to reduce textbook costs for students whenever possible. Have electronic textbooks, textbook rentals, or the buyback program been considered and adopted?

- Yes. Briefly explain below.
 No. Briefly explain below.

IMPORTANT NOTE: A Microsoft Word version of the final course and curriculum proposal should be sent to facultygovernance@uncc.edu upon approval by the Undergraduate Course and Curriculum Committee and/or Graduate Council chair.

Appendix I: Consultation

Supporting memos from the following affected units are attached.

Department of Computer Science:

Subject: RE: New course consultation: pls reply by 2/21 Friday
From: "Ribarsky, William" <ribarsky@uncc.edu>
Date: 02/22/2014 01:06 AM
To: "Zheng, Yuliang" <yzheng@uncc.edu>

Yuliang,
The CS Department and Graduate Committee have reviewed the course proposal. They have no issues with it and support sending it forward.
Bill

Dr. William Ribarsky
Bank of America Endowed Chair in Information Technology
Chair, Computer Science Department
Director, Charlotte Visualization Center
College of Computing and Informatics
University of North Carolina at Charlotte
www.viscenter.uncc.edu

From: Yuliang Zheng [yzheng@uncc.edu]
Sent: Friday, February 21, 2014 9:22 AM
To: Ribarsky, William
Subject: Re: New course consultation: pls reply by 2/21 Friday

Hello Bill,
Please let me know the feedback from your dept.
Thanks,
Yuliang

From: Yuliang Zheng <yzheng@uncc.edu> *To:* Ribarsky, William <ribarsky@uncc.edu>, Mays, Larry <lemays@uncc.edu>
Cc: Maher, Mary <M.Maher@UNCC.EDU> *Subject:* New course consultation: pls reply by 2/21 Friday

Yuliang Zheng wrote, on 2/13/14, 9:00 AM:
Larry and Bill,
Attached is a new course proposal from SIS.
We are seeking support from your departments.
Please provide your feedback by

Friday next week, 2/21/2014.

Thanks,

Department of Bioinformatics and Genomics

Subject: Re: New course consultation: pls reply by 2/21 Friday
From: "Mays, Larry" <lemays@uncc.edu>
Date: 02/13/2014 09:07 AM
To: "Zheng, Yuliang" <yzheng@uncc.edu>, "Ribarsky, William" <ribarsky@uncc.edu>
CC: "Maher, Mary" <M.Maher@uncc.edu>

The Department of Bioinformatics and Genomics enthusiastically endorses your proposal for a new course on open source security systems. It is a very timely topic for your students.
Larry Mays

On 2/13/14, 9:00 AM, "Yuliang Zheng" <yzheng@uncc.edu> wrote:

Larry and Bill,
Attached is a new course proposal from SIS.
We are seeking support from your departments.
Please provide your feedback by

Friday next week, 2/21/2014.

Thanks,

--

Yuliang

Attachment II. Course Outline/Syllabus

1. Course Number and Title: ITIS 6250/8250 Open Source Security Systems

2. Prerequisites

ITIS 6250: “Pre/co-requisites: ITIS 6200 or equivalent, or permission of the department”;

ITIS 8250: “Prerequisites: Ph.D. student standing, or permission of the department”.

3. Syllabus

- Open source ecosystems including software copyrights, software licensing and development models
- common open source software systems and projects
- quality assurance and security implications of open source systems
- open source cryptographic technologies
- designing and implementing security solutions using open source technologies
- hands-on study: Comparison of security features of Linux and BSD, and OS hardening with Bastille
- hands-on study: AxCrypt, OpenSSL, TrueCrypt
- hands-on study: OpenSSH, OpenVPN, NoMachine
- hands-on study: File system encryption
- hands-on study: Comparison of Crypto Libraries: Java Crypto, Crypto++, MIRACL, OpenSSL, NTL, and others
- hands-on study: iptable, pf, snort, suricata
- hands-on study: Nessus, OpenVAS, Metasploit
- hands-on study: Securing websites built on LAMP (Linux, Apache, MySQL and PHP)

4. Course objectives:

- To introduce students to open source environments such as copyright and license issues, open source models and methodologies, common open source software systems and projects, quality and security assurance of open source systems.
- To familiarize students with various cryptographic technologies through the use of open source security source.
- To provide students with hands-on, practical experience by developing security solutions using open source technologies.

5. Instruction Method:

- Lectures / guest lectures
- In-class activities and discussions
- Individual and group projects
- Student demonstrations and presentations

6. Means of student evaluation:

For master’s students taking ITIS6250, evaluation will be based upon the following:

- Course midterm and final examinations account for 40% of the grade.

- Two individual and group hands-on projects account for 30% of the grade.
- One research presentation accounts for 20% of the grade.
- Other assignments and quizzes account for 10% of the grade.

Grading scale for master's students:

90-100 points	A
80-89	B
60-79	C
59 and below	U

For PhD students taking ITIS8250, examinations, projects and presentations will require them to demonstrate a deeper understanding of topical areas as well as greater proficiency at hands-on practices. The students will also be required to complete additional examination questions and hands-on projects. Specifically, the following evaluation method will be employed:

- Course midterm and final examinations account for 40% of the grade. Each examination will have at least one more question than the number of questions for the same examination for master's students.
- Four individual and group hands-on projects account for 35% of the grade.
- One research presentation accounts for 15% of the grade.
- One report surveying a specific topic in the subject area accounts for 5% of the grade.
- Other assignments and quizzes account for 5% of the grade.

Grading scale for PhD students:

90-100 points	A
80-89	B
60-79	C
59 and below	U

7. University Policy:

- The course upholds all university academic integrity policies. Under no circumstances should a student present other people's work as his/her own. The UNC Charlotte Academic Integrity Code can be found at: <https://legal.uncc.edu/policies/up-407>
- Class attendance is mandatory, unless a student obtains written permission from the instructor.
- Students will be assigned grades of A, B, C, or U. Each of these class activities will be graded according to the established criteria and the final grade will be offered based on the accumulation of these grades. Typically, A will be given for a total of 90 and above, B will be given for a total of 80 and above, C will be given for a total of 70 and above, U will be given for a total of below 70.
- No Additional requirements

8. Suggested textbooks and reading materials

1. Raven Alder, Josh Burke, Chad Keefer, Angela Orebaugh, Larry Pesce and Eric S. Seagren, How to Cheat at Configuring Open Source Security Tools, Syngress, 2007 (Free).
2. Amy Brown and Greg Wilson. The Architecture of Open Source Applications. Vols 1 & 2, ISBN-13: 978-1257638017. <http://aosabook.org/en>
3. Ernesto Damiani, Claudio Agostino Ardagna and Nabil El Ioini, Open Source Systems Security Certification, Springer, 2009, e-ISBN-13: 978-0-387-77324-7.
4. Tony Howlett, Open Source Security Tools: A Practical Guide to Security Applications, Prentice Hall PTR, 2004, ISBN 0-321-19443-8.
5. Ewa Huebner and Stefano Zanero, Open Source Software for Digital Forensics, Springer, 2010, e-ISBN 978-1-4419-5803-7.
6. Andrew M. St. Laurent. Understanding Open Source and Free Software Licensing. O'Reilly Media, 2004. ISBN-13: 978-0596005818.
7. Mike D. Schiffman , Building Open Source Network Security Tools: Components and Techniques, John Wiley & Sons, 2003, ISBN:0471205443.
8. Eric Seagren , Secure Your Network for Free, Syngress, 2007 (Free).
9. Sven Vermeulen, SELinux System Administration, Packt Publishing, 2013, ISBN 978-1-78328-317-0.
10. Apache documentation: <http://www.apache.org/>
11. Department of Homeland Security. Open Source Cybersecurity Catalog. <http://www.dhs.gov/csd-host>
12. OpenSSL documentation: <https://www.openssl.org/>
13. David A. Wheeler, Why Open Source Software / Free Software (OSS/FS, FLOSS, or FOSS)? Look at the Numbers!, 2007, http://www.dwheeler.com/oss_fs_why.html

Appendix III: Proposed Catalog Copy

ITIS 6250 Open Source Security Systems (3 credit hours) Pre/co-requisite: ITIS 6200 or equivalent, or permission of the department. An introduction to the design, implementation, evaluation and maintenance of secure software systems and applications using open source technologies, with an emphasis on hands-on experience. Topics include: open source ecosystems, open source security methodologies and models, notable open source software systems and projects, quality and security assurance through open source, open source supply chain security, major open source cryptographic packages; designing, implementing and maintaining security systems using open source technologies; assessment and regulatory compliance using open source tools, and open source hardware. (*On demand*)

ITIS 8250 Open Source Security Systems (3 credit hours) Prerequisite: Ph.D. student standing, or permission of the department. An introduction to the design, implementation, evaluation and maintenance of secure software systems and applications using open source technologies, with an emphasis on hands-on experience. Topics include: open source ecosystems, open source security methodologies and models, notable open source software systems and projects, quality and security assurance through open source, open source supply chain security, major open source cryptographic packages; designing, implementing and maintaining security systems using open source technologies; assessment and regulatory compliance using open source tools, and open source hardware. (*On demand*)

Appendix IV: Library Consultation



J. Murrey Atkins Library

Consultation on Library Holdings

To: Dr. Yuliang Zheng

From: Dr. Melanie Sorrell

Date: 02/13/2014

Subject: ITIS 6250/8250 - Open Source Security Systems

Summary of Librarian’s Evaluation of Holdings:

Evaluator: Dr. Melanie Sorrell Date: 02/13/2014

Check One:

- 1. Holdings are superior _____
- 2. Holdings are adequate __x__
- 3. Holdings are adequate only if Dept. purchases additional items. _____
- 4. Holdings are inadequate _____

Comments:

This is a proposal for a new graduate level course, which includes one research presentation. Library holdings should be adequate to support student research for this course (see list of items held by subject heading below). Students will have access to relevant databases including INSPEC, IEEE Xplore, Compendex, and the ACM Digital Library.

LC Subject Heading	Total items held
Computer networks -- Security measures	534 monographs
Electronic commerce -- Management	171 monographs
Computer software – Development	387 monographs
Information storage and retrieval systems -- United States -- Security measures -- Government policy	24 monographs
Free computer software	6 monographs
IEEE Security & Privacy	Journal title
Information Security	Journal title

Melanie Sorrell

Evaluator’s Signature

02/13/2014
