Course Approval Form

For approval of new courses and deletions or modifications to an existing course.

registrar.gmu.edu/facultystaff/curriculum

Action Requested:

- [x] Create new course
- [ ] Delete existing course
- [ ] Modify existing course (check all that apply)
  - [ ] Title
  - [ ] Credits
  - [ ] Repeat Status
  - [ ] Grade Type
  - [ ] Prereq/coreq
  - [ ] Schedule Type
  - [ ] Restrictions
  - [ ] Other:

Course Level:

- [ ] Undergraduate
- [x] Graduate

College/School: VSE (Volgenau School of Engineering) **Department:** ECE

Submitted by: Robert Osgood **Ext:** 3-5443 **Email:** rosgood@gmu.edu

Subject Code: CFRS **Number:** 773

(Do not list multiple codes or numbers. Each course proposal must have a separate form.)

Effective Term:

- [x] Fall
- [ ] Spring
- [ ] Summer

Year 2014

Title:

Current

Banner (30 characters max including spaces)

New: Mobile Application Forensics and Analysis

Credits: (check one)

- [3] Fixed
- [ ] Variable

X to

Repeat Status: (check one)

- [X] Not Repeatable (NR)
- [ ] Repeatable within degree (RD)
- [ ] Repeatable within term (RT)

Maximum credits allowed:

Grade Mode: (check one)

- [X] Regular (A, B, C, etc.)
- [ ] Satisfactory/No Credit
- [ ] Special (A, B C, etc. +IP)

Schedule Type Code(s): (check all that apply)

- [X] Lecture (LEC)
- [X] Lab (LAB)
- [ ] Recitation (RCT)
- [ ] Internship (INT)
- [ ] Independent Study (IND)
- [ ] Seminar (SEM)
- [ ] Studio (STU)

Prerequisite(s): CFRS 762

Corequisite(s):

Instructional Mode:

- [X] 100% face-to-face
- [ ] Hybrid: ≤ 50% electronically delivered
- [ ] 100% electronically delivered

Special Instructions: (list restrictions for major, college, or degree;hard-coding; etc.)

Are there equivalent course(s)?

- [ ] Yes
- [X] No

If yes, please list

Catalog Copy for NEW Courses Only (Consult University Catalog for models)

Description (No more than 60 words, use verb phrases and present tense)	**Notes** (List additional information for the course)
Presents mobile applications forensics and analysis. Analyze mobile applications on both the android and iPhone platforms in a lab environment in order to understand the weaknesses, pitfalls, and forensic challenges that exist or potentially exist when developing mobile client side software as well as identify forensic artifacts left behind from applications.	.
Indicate number of contact hours: Hours of Lecture or Seminar per week: 3 Hours of Lab or Studio:	
When Offered: (check all that apply) [x] Fall [ ] Summer [x] Spring	

Approval Signatures

Andre Manitius — Department Approval — 10/18/13 — Date

College/School Approval — Date

If this course includes subject matter currently dealt with by any other units, the originating department must circulate this proposal for review by those units and obtain the necessary signatures prior to submission. Failure to do so will delay action on this proposal.

Unit Name	Unit Approval Name	Unit Approver's Signature	Date

For Graduate Courses Only

Graduate Council Member — Provost Office — Graduate Council Approval Date

For Registrar Office's Use Only: Banner_____Catalog_____

revised 2/2/10

SCHOOL PROPOSAL TO THE GRADUATE COUNCIL
BY
THE VOLGENAU SCHOOL OF ENGINEERING

1. CATALOG DESCRIPTION

(a) CFRS 773 Mobile Application Forensics and Analysis
(b) Prerequisite: CFRS 762
(c) Catalog Description: Presents mobile applications forensics and analysis. Analyze mobile applications on both the android and iPhone platforms in a lab environment in order to understand the weaknesses, pitfalls, and forensic challenges that exist or potentially exist when developing mobile client side software as well as identify forensic artifacts left behind from applications.

2. JUSTIFICATION

(a) Course Objectives:
Through this course students will address complex mobile applications forensic and analysis challenges. They will be able to understand the environment in which applications are created and how these applications can be effectively analyzed identifying and interpreting forensic artifacts.

(b) Course Necessity:
Mobile devices are fully functioning computers with an operating system and an almost unlimited number of applications that can be run on these devices. By examining the application side of mobile computing, students will be able to recognize the weaknesses and identify those forensic artifacts required for successful analysis.

(c) Relationship to Existing Courses:
This course builds on the course CFRS 762 Mobile Device Forensics expanding forensics to the applications run on these devices.

3. APPROVAL HISTORY

Department Date: October 18th, 2013

4. SCHEDULING

The course will be offered every fall and spring semester, starting fall 2014 and every regular semester thereafter.

5. PROPOSED INSTRUCTORS

Robert Osgood, Tahir Khan, and other suitably qualified faculty

6. COURSE OUTLINE

(a) **Overview**
Week 1

Introduction, overview and review of web technologies. Topics such as HTTP, HTTPS, SSL, Obfuscation and encryption will be visited. Additionally, review of the various mobile platforms and technologies will be addressed.

Week 2

Understanding of the mobile testing application environment. Installation and configuration of an emulated android environment as well as basic functionality of the emulator

Week 3

Understanding of the mobile testing application environment. Installation and configuration of an iPhone and related testing environment as well as updating tools and software needed to analyze applications on an iPhone

Week 4

The android VM will be used, and students will learn how to navigate the VM as well as use tools to talk to the mobile device via the android debugging bridge. Students will learn how to push and pull files, apks and other items from the android device.

Week 5

The iPhone lab will be used, and students will learn how to connect to the iPhone as well as navigate the file system as well as pushing and pulling files from the device. Students will learn the structure of the file system in more detail and where certain files are located that facilitate in application analysis and forensics

Week 6

Initial analysis on the android platform will occur. Students will install applications from the Play store and learn how to copy the application to their VM for analysis. Students will learn the format of the APK file and what information it contains.

Week 7

Students will disassemble the APK file and perform simple analysis on the files within. This will consist of extracting actionable information such as web addresses, IP addresses, names, etc.. This class will have several in class labs to reinforce the lecture.

Week 8

Students will extract DEX files from the APK and convert them to a JAR file. Students will analyze the jar file in eclipse. This will allow the students to see the program flow and identify and potential weaknesses. The midterm project will be due.

Week 9

Students will learn how to decode the android APK XML encoding format. This will allow students to further understand the structure of the application. If time allows students will disassemble code modify it and reassemble it using tools such as baksmali and smali.

Week 10

iPhone
Students will learn how to analyze IPA files from iPhones. Students will learn how to dump class information and view the basic layout of the application to determine any potential weaknesses. Students will also learn how to obtain copies of the IPA file from other locations to aid in forensics.

Week 11

Students will learn how to identify certificate pinning on the iPhone and bypass it if done poorly. Students will learn how to manipulate methods and calls while running an actual iPhone application.

Week 12

Students will learn how to identify various artifacts left behind from mobile applications. Students will be able to determine if applications were run or not run based on these artifacts.

Week 13

Students will learn how to intercept traffic from mobile devices. Students will learn how to manipulate basic parameters to uncover weaknesses in the mobile applications through network analysis. Students will understand and perform in-class labs to learn how to identify artifacts in network traffic for several mobile applications.

Weeks 14

Final presentations and review

Week 15

Final Exam

(b) Required Reading and Reference Material

Required Text:

Mobile Application Security
By: Himanshu Dwivedi; Chris Clark; David Thiel
Publisher: McGraw-Hill

Pub. Date: January 15, 2010
Print ISBN-10: 0-07-163356-1
Print ISBN-13: 978-0-07-163356-7
Web ISBN-10: 0-07-163357-X
Web ISBN-13: 978-0-07-163357-4
Pages in Print Edition: 430

(c) Student Evaluation Criteria

Project – 40%
Final Exam – 40%
Homework Assignments – 20%