To: Undergraduate Curriculum Committee  
Thru: Dr. Mark Archambault, Associate Dean for Academics, College of Engineering and Science  
Thru: Dr. Philip Bernhard, Head, Department of Computer Engineering and Sciences  
From: Dr. T.J. O'Connor, Assistant Professor, Department of Computer Engineering and Sciences  
Date: September 6, 2019  
Re: Adding cybersecurity courses to the undergraduate catalog

The Department of Computer Engineering and Sciences proposes the addition of the following cybersecurity courses as electives in the Computer Science program, to take effect in Fall 2020. These courses, with completion of the appropriate prerequisites, could also be taken by students from other majors.

- CSE 3810 Cyber Defense Fundamentals
- CSE 4820 Wireless and Mobile Security
- CSE 4830 Introduction to Software Reverse Engineering
- CSE 4840 Cyber Offense Fundamentals
- CSE 4850 Introduction to Vulnerability Research

No undergraduate courses on these topics currently exist and no academic program will be impacted by the addition of these courses. Documentation for each course is attached.
**FLORIDA TECH**

**New courses are available beginning with the fall term in which they appear in the University Catalog.**

<table>
<thead>
<tr>
<th>SUBJECT</th>
<th>C S E</th>
<th>COURSE NO.*</th>
<th>3 8 1 0</th>
<th>CREDIT HOURS</th>
<th>3</th>
<th>ACADEMIC YEAR TO BE ADDED TO THE FILE</th>
<th>Fall 2020</th>
</tr>
</thead>
</table>

*Justify level if 1000-level+ and no co- or prerequisites

<table>
<thead>
<tr>
<th>CLASS HOURS</th>
<th>LECTURE HOURS</th>
<th>LAB HOURS</th>
<th>CONTACT HOURS</th>
<th>SCHEDULE TYPE</th>
</tr>
</thead>
<tbody>
<tr>
<td>45/semester</td>
<td>45/semester</td>
<td>0/semester</td>
<td>N/A</td>
<td>Lecture (A)</td>
</tr>
</tbody>
</table>

**DEPARTMENT:** Computer Engineering and Sciences  
(e.g., Biological Sciences)

- [ ] COLLEGE OF AERONAUTICS—23
- [ ] COLLEGE OF PSYCHOLOGY AND LIBERAL ARTS—25
- [ ] NATHAN M. BISK COLLEGE OF BUSINESS—24

**COMPUTER TITLE:** Cyber Defense

This course will be entered into the system as:  
- [ ] Bi-Level
- [ ] Cross-Listed
- [ ] Dual-Numbered
- [ ] Full-Load
- [ ] None of these/Standard Listing

**CATALOG TITLE:** Cyber Defense Fundamentals

**CATALOG DESCRIPTION OF COURSE:** Restricted to 350 characters, including spaces

Examines the defense of information technology from a practical point of view. Introduces security principles, design, methods for reducing complexity and detection of reconnaissance, malicious traffic, and covert channels. Requires students to design and implement a defense architecture by leveraging risk models including NIST SP 800-37/39.

This description has been approved by the catalog office:  
8-27-2019

**GRADES TO BE ISSUED:**  
- [ ] A, B, C, D, F
- [ ] A, B, C, D, F, CEU/Audit
- [ ] CEU
- [ ] S, U
- [ ] P, F
- [ ] Other

**IN ADDITION, PLEASE ATTACH A COURSE SYLLABI AND/OR MORE DETAILED DESCRIPTION.**

**REQUIREMENTS**

- [ ] Prerequisite ONLY
- [ ] Corequisite ONLY
- [ ] BOTH Prerequisite/Corequisite

**ADDITIONAL RESTRICTION**

- [ ] and
- [ ] or

*Course Prefix/Number: C S E 3 8 0 1, C S E 3 2 3 1*

**Please indicate old course information and the date/term the course may be removed from the system:**

- [ ] Yes
- [ ] No

- Will this course be used to measure program-level student learning outcomes?  
  If yes, **review and signature required.**

- Will this course be used to satisfy the scholarly inquiry requirement?  
  If yes, attach "Q" materials for review.

- Will this course impact any existing programs?  
  If yes, attach "Changing Graduation Requirements" form for each program impacted.

- Will this course be used to satisfy the Cross Cultural (CC) requirement?  
  If yes, attach confirmation memo from QEPZ Committee.

**APPROVALS: On completion of description and course number verification, affix appropriate signatures as indicated, and submit to the Office of Graduate Programs, or Undergraduate Curriculum Committee Chair for placement on agenda.**

**Catalog & Curriculum Manager**

**Registrar's Use Only**

<table>
<thead>
<tr>
<th>SCACRSE</th>
<th>SCADETL</th>
<th>SCAPREQ</th>
<th>SCABASE</th>
<th>ACATALOG</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SCAFFIES</th>
<th>CIP Code</th>
<th>Operator Init.</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>11.0701</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Florida Institute of Technology • Office of the Registrar  
150 West University Boulevard, Melbourne, FL 32901-6975 • 321-674-8114 • Fax 321-674-7827

RGR-384-219
CSE 3810 CYBER DEFENSE FUNDAMENTALS

Course Information

Catalog Description
Examines the defense of information technology from a practical point of view. Introduces security principles, design, methods for reducing complexity and detection of reconnaissance, malicious traffic, and covert channels. Students will both design and implement a defense architecture by leveraging risk models including NIST SP 800-37/39.

Textbook
There is no assigned textbook for this course. The instructor will provide materials and digital references including NIST SP 800-37, NIST SP 800-39, NSA CyberSecurity Advisories and Technical Guidance.

Prerequisites
CSE 3801 Introduction to Cyber Operations AND CSE 3231 Computer Networks

Expected Outcomes
By the end of the course, students will have knowledge of and hands-on experience with tools and techniques for cyber defense. More specifically they will be prepared to:

- Employ, analyze, and exploit fundamental security design principles (simplicity, open, design for iteration, fail-safes, least privilege, isolation, abstraction).
- Understand the technologies and methods to secure operating systems (ASLR, stack-prevention, canaries, control flow integrity, host-based intrusion controls, and system event logging).
- Employ signature-based and anomaly-based intrusion detection systems to detect a variety of malicious traffic, covert channels, and data exfiltration.
- Employ security information and event management systems to correlate events to identify complex attacks (Splunk, Security Onion, Cloudshark).

Grading
Your final course grade will be based on the following components ONLY:

- Midterm Exam: 20%
- Course Project: 20%
- Practical Exercises (5 total): 50%
- Student Presentation: 10%
Course Project

Students are required to complete a course project where they will design and secure a system with defense-in-depth to mitigate risk.

Grading Scale

A: 90 to 100, B: 80 to 89, C: 70 to 79, D: 60 to 69, F: below 60

Class Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Type</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lesson</td>
<td>Intro to cyber defense</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>General principles</td>
</tr>
<tr>
<td>2</td>
<td>Lesson</td>
<td>Security design principles</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Methods for reducing complexity</td>
</tr>
<tr>
<td>3</td>
<td>Student Presentation</td>
<td>Security principles presentation</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Networking protocol review</td>
</tr>
<tr>
<td>4</td>
<td>Lesson</td>
<td>Traffic signatures</td>
</tr>
<tr>
<td></td>
<td>Practical Exercise</td>
<td>Signature creation (SNORT/Wireshark)</td>
</tr>
<tr>
<td>5</td>
<td>Lesson</td>
<td>Identity of reconnaissance operations</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Anomaly/intrusion detection</td>
</tr>
<tr>
<td>6</td>
<td>Practical Exercise</td>
<td>Anomaly detection (Scapy / Sklearn)</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Identification of C2 Channels</td>
</tr>
<tr>
<td>7</td>
<td>Lesson</td>
<td>Data exfiltration identification</td>
</tr>
<tr>
<td></td>
<td>Practical Exercise</td>
<td>Data exfil/covert channels (Scapy)</td>
</tr>
<tr>
<td>8</td>
<td>Lesson</td>
<td>Applied cryptography</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Public key infrastructure</td>
</tr>
<tr>
<td>9</td>
<td>Lesson</td>
<td>Review</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Midterm</td>
</tr>
<tr>
<td>10</td>
<td>Lesson</td>
<td>Malicious activity detection via host-based controls</td>
</tr>
<tr>
<td></td>
<td>Practical Exercise</td>
<td>Event logging (systlog / windows event log analysis )</td>
</tr>
<tr>
<td>11</td>
<td>Lesson</td>
<td>Malicious activity detection via network tools</td>
</tr>
<tr>
<td></td>
<td>Practical Exercise</td>
<td>Attack correlation (Splunk)</td>
</tr>
<tr>
<td>12</td>
<td>Lesson</td>
<td>Defense in depth</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Trust relationships</td>
</tr>
<tr>
<td>13</td>
<td>Practical Exercise</td>
<td>Course project overview</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Managing information system risk (NIST SP 800-39)</td>
</tr>
<tr>
<td>14</td>
<td>Lesson</td>
<td>Risk models (NIST SP 800-37)</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Distributed/cloud computing</td>
</tr>
<tr>
<td>15</td>
<td>Lesson</td>
<td>Virtualization (kubernetes/docker)</td>
</tr>
<tr>
<td></td>
<td>Presentation</td>
<td>Course project presentations</td>
</tr>
<tr>
<td>16</td>
<td>Presentation</td>
<td>Course project presentations</td>
</tr>
</tbody>
</table>
Course Policies

Quizzes and Exams

All quizzes and exams are closed book. All lecture slides and other materials that will be included on exams will be posted to the course Canvas page. Electronic devices are not allowed during exams. An electronic device includes, but is not limited to, cell phones, tablets, laptops, calculators, electronic translators, etc. If you are unsure if a specific device is allowed, please ask before the exam begins.

Attendance Policy

Attendance is expected in all lectures. Lectures will contain materials often outside the scope of the assigned reading but will be included in the midterm and final exam. Missing lectures could result in missing key material relevant to the exam. Course exercises will be assigned during the class period. Missing a course exercise will result in the instructor assigning a 0 for the specific assignment.

Academic Honesty

Students are required to comply with the university policy on academic integrity, cheating, and plagiarism found in the Code of Student Conduct at https://policy.fit.edu/policy/9267. The purpose of assignments and exams are to develop your skills and measure your progress in the course. Thus, all assessed coursework must be your own work. Several exercises will include an assigned exercise partner. In the case of assigned partners, you may share the same results as your partner. However, your report must be in your own words. You may discuss assignments with other students. However, you may not partially or completely duplicate the work of others and claim it as your own. In order to deter and detect plagiarism, online tools and other resources may be used in this class. Department and University policies allow severe penalties for plagiarism up to and including an F in the course, and/or expulsion from the University.

Lecture Recording Policy

Students are expressly forbidden from recording lectures using electronic devices with photographic, audio or video recording capability. This includes but is not limited to taking photographs, audio and/or video recordings of any lectures, exercises, exams, or quizzes. Doing so without my permission and/or knowledge is a violation of the policies on Electronic Devices in the Student Handbook at https://policy.fit.edu/policy/9066. If you have been granted this privilege from the Academic Support Center, please gain my permission to do so BEFORE recording lectures.

Accommodations for Disabilities

Reasonable accommodations will be made for students with verifiable disabilities. In order to take advantage of available accommodations, students must register with the Office of Disability Services (ODS), located in the Evans Pavilion Annex. Florida Tech is committed to equal opportunity for persons with disabilities. Therefore, students with documented disabilities are entitled
to reasonable and appropriate educational accommodations. Reasonable accommodations may include adjustments to the classroom or testing setting. Please make the professor aware of any verified disabilities at the beginning of the semester.

What is Title IX

Title IX of the Educational Amendments Act of 1972 is the federal law prohibiting discrimination based on sex under any education program and/or activity operated by an institution receiving and/or benefiting from federal financial assistance. Behaviors that can be considered sexual discrimination include sexual assault, sexual harassment, stalking, relationship abuse (dating violence and domestic violence), sexual misconduct, and gender discrimination. You are encouraged to report these behaviors. Reporting: Florida Tech can better support students in trouble if we know about what is happening. Reporting also helps us to identify patterns that might arise - for example, if more than one complainant reports having been assaulted or harassed by the same individual. Florida Tech is committed to providing a safe and positive learning experience. To report a violation of sexual misconduct or gender discrimination, please contact Linda Jancheson, Title IX Coordinator at 321-674-7277 or ljancheson@fit.edu. * Please note that as your professor, I am required to report any incidences to the Title IX Coordinator. Confidential support for students is available by contacting the Student Counseling Center at 321-674-8050.
**FLORIDA TECH**

## ADDING A NEW COURSE TO THE CURRICULUM

New courses are available beginning with the fall term in which they appear in the University Catalog.

<table>
<thead>
<tr>
<th>SUBJECT</th>
<th>C S E</th>
<th>COURSE NO.*</th>
<th>4 8 2 0</th>
<th>CREDIT HOURS</th>
<th>3</th>
<th>ACADEMIC YEAR TO BE ADDED TO THE FILE</th>
<th>Fall 2020</th>
</tr>
</thead>
</table>
*Justify level if 1000-level+ and no co- or prerequisites (e.g., CSE, 1301)

<table>
<thead>
<tr>
<th>CLASS HOURS</th>
<th>45/semester</th>
<th>LECTURE HOURS</th>
<th>45/semester</th>
<th>LAB HOURS</th>
<th>0/semester</th>
<th>CONTACT HOURS (CEU ONLY)</th>
<th>N/A</th>
</tr>
</thead>
</table>

DEPARTMENT Computer Engineering and Sciences (e.g., Biological Sciences)

- [ ] COLLEGE OF AERONAUTICS—23
- [x] COLLEGE OF ENGINEERING AND SCIENCE—30
- [ ] COLLEGE OF PSYCHOLOGY AND LIBERAL ARTS—25
- [ ] NATHAN M. BISK COLLEGE OF BUSINESS—24

SCHEDULE TYPE Lecture (A) (e.g., Lecture, Lab or Special Topics/Project)

COMPUTER TITLE Wireless/Mobile Security

This course will be entered into the system as: Bi-Level [ ] Cross-Listed [ ] Dual-Numbered [ ] Full-Load [ ] None of these/Standard Listing [x]

CATALOG TITLE Wireless and Mobile Security

CATALOG DESCRIPTION OF COURSE: Restricted to 350 characters, including spaces

Examines the security and privacy of wireless and mobile technologies from a practical point of view. Discusses cryptographic primitives and proper association and authentication of users. Examines the history of design/implementation flaws in various wireless technologies. Discusses recent wireless security-related trends and technologies.

This description has been approved by the catalog office: Emojy

8-27-2019

In addition, please attach a course syllabus and/or more detailed description.

<table>
<thead>
<tr>
<th>RESTRICTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>C S E 3 8 0 1</td>
</tr>
<tr>
<td>C S E 3 2 3 1</td>
</tr>
</tbody>
</table>

Course Prefix/Number

ADDITIONAL RESTRICTION [ ] and [ ] or [ ] and [ ] or [ ]

GRADES TO BE ISSUED

- [x] A, B, C, D, F
- [ ] A, B, C, D, F, CEU/Audit
- [ ] CEU
- [ ] S, U
- [ ] P, F
- [ ] Other [ ]

Please indicate old course information and the date/term the course may be removed from the system:

- [ ] Yes [ ] No Will this course be used to measure program-level student learning outcomes? If yes, review and signature required.**
- [ ] Yes [ ] No Will this course be used to satisfy the scholarly inquiry requirement? If yes, attach "Q" materials for review.
- [ ] Yes [ ] No Will this course impact any existing programs? If yes, attach "Changing Graduation Requirements" form for each program impacted.
- [ ] Yes [ ] No Will this course be used to satisfy the Cross Cultural (CC) requirement? If yes, attach confirmation memo from QEP2 Committee.

**APPROVALS: On completion of description and course number verification, affix appropriate signatures as indicated, and submit to the Office of Graduate Programs, or Undergraduate Curriculum Committee Chair for placement on agenda.

- [ ] Chair, Graduate Council [ ]
- [ ] Date [ ]
- [ ] Chair, Undergraduate Curriculum Committee [ ]
- [ ] Date [ ]

- [ ] Chair, APAC [ ]
- [ ] Date [ ]

**CATALOG & CURRICULUM MANAGER**

These changes/additions have been made for the University Catalog and entered into the BANNER term named above.

<table>
<thead>
<tr>
<th>CATALOG &amp; CURRICULUM MANAGER</th>
<th>REGISTRAR'S USE ONLY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalog &amp; Curriculum Manager</td>
<td>SCACRSE</td>
</tr>
<tr>
<td>[ ] Date</td>
<td>SCARES</td>
</tr>
<tr>
<td>11.0701</td>
<td>[ ]</td>
</tr>
</tbody>
</table>

Florida Institute of Technology • Office of the Registrar

150 West University Boulevard, Melbourne, FL 32901-6975 • 321-674-8114 • Fax 321-674-7827

RGR-384-219
CSE 4820 Wireless and Mobile Security

Course Information

Catalog Description
Examines the security and privacy of wireless and mobile technologies from a practical point of view. Discusses cryptographic primitives and proper association and authentication of users. Examines a lengthy history of design/implementation flaws in various wireless technologies. Discusses recent wireless security-related trends and technologies.

Textbook

Prerequisites
CSE 3801 Introduction to Cyber Operations AND CSE 3231 Computer Networks

Expected Outcomes
By the end of the course, students will have knowledge of and hands-on experience with tools and techniques for securing wireless and mobile devices. More specifically they will be prepared to:

- Cryptographic primitives and enforcement of confidentiality, integrity, and authentication. (Stream and block ciphers, public/private encryption schemes).
- Security of design/implementation flaws in various wireless technologies (A5/1, RC4).
- Understanding of availability attacks and defenses (RACH and carrier-sense flooding/802.11w).
- Recent attack trends including: 5G vulnerabilities, ISMSI catching and smart-phone attacks.

Grading
Your final course grade will be based on the following components ONLY:

- Midterm Exam: 20%
- Final Exam: 20%
- Lab Assignments (6 total): 50%
- Quizzes: 10%

Grading Scale
A: 90 to 100, B: 80 to 89, C: 70 to 79, D: 60 to 69, F: below 60
Class Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Type</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lesson</td>
<td>Overview of wireless technologies</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Enumeration of wireless devices and services</td>
</tr>
<tr>
<td>2</td>
<td>Lab</td>
<td>Scanning and enumeration of wireless technologies</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Wireless denial of service issues</td>
</tr>
<tr>
<td>3</td>
<td>Lab</td>
<td>802.11w enforcement Lab</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Cryptographic primitives for wireless security</td>
</tr>
<tr>
<td>4</td>
<td>Lesson</td>
<td>Stream and block ciphers for wireless</td>
</tr>
<tr>
<td></td>
<td>Lab</td>
<td>WEP/WPA cracking lab (Aircrack-NG)</td>
</tr>
<tr>
<td>5</td>
<td>Lesson</td>
<td>Security issues in hardware and software of wireless</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Case Study: D-link router firmware</td>
</tr>
<tr>
<td>6</td>
<td>Lesson</td>
<td>Smart phones and embedded operating systems</td>
</tr>
<tr>
<td></td>
<td>Lab</td>
<td>Mobile malware de-compilation and source code analysis</td>
</tr>
<tr>
<td>7</td>
<td>Review</td>
<td>Midterm review</td>
</tr>
<tr>
<td></td>
<td>Exam</td>
<td>Midterm exam</td>
</tr>
<tr>
<td>8</td>
<td>Lesson</td>
<td>Intro to digital signal processing</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Software defined radios</td>
</tr>
<tr>
<td>9</td>
<td>Lesson</td>
<td>Telephony Infrastructure</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Introduction to cellular protocols (CDMA, GSM, LTE)</td>
</tr>
<tr>
<td>10</td>
<td>Lesson</td>
<td>Mobile channel separation and access (layer 1)</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Mobile data-link and signaling protocols (layer 2)</td>
</tr>
<tr>
<td>11</td>
<td>Lesson</td>
<td>GSM network model</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>GSM authentication and encryption</td>
</tr>
<tr>
<td>12</td>
<td>Lab</td>
<td>GSM A5/1 key recovery lab (Kraken)</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>LTE network model</td>
</tr>
<tr>
<td>13</td>
<td>Lesson</td>
<td>LTE authentication, and encryption</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Femtocel Attacks and detection</td>
</tr>
<tr>
<td>14</td>
<td>Lesson</td>
<td>Zigbee encryption and authentication</td>
</tr>
<tr>
<td></td>
<td>Lab</td>
<td>Zigbee interception lab ( Killerbee framework)</td>
</tr>
<tr>
<td>15</td>
<td>Lesson</td>
<td>Z-Wave and smart-homes</td>
</tr>
<tr>
<td></td>
<td>Review</td>
<td>Course review</td>
</tr>
<tr>
<td>16</td>
<td>Final</td>
<td>Final exam</td>
</tr>
</tbody>
</table>

Course Policies

Quizzes and Exams

All quizzes and exams are closed book. All lecture slides and other materials that will be included on exams will be posted to the course Canvas page. Electronic devices are not allowed during exams. An electronic device includes, but is not limited to, cell phones, tablets, laptops, calculators, electronic translators, etc. If you are unsure if a specific device is allowed, please ask before the exam begins.
Late Assignments

Lab assignment will be given a specific due date beyond which it will NOT be accepted. Late assignments will not be accepted past the due date and time published on Canvas. Assignments cannot be submitted via email; those that are will be disregarded and will receive a 0. Please note that each lab assignment will include extra credit challenges. These challenges are the only accepted extra credit for the course and must be turned in at the assignment due date published on Canvas.

Attendance Policy

Attendance is expected in all lecture and lab sections. Lectures will contain materials often outside the scope of the assigned reading but will be included in the midterm and final exam. Missing lectures could result in missing key material relevant to the exam. Labs will be assigned during the lab class period. Missing a lab will result in the instructor assigning a 0 for the specific lab assignment.

Missed Work

With very few exceptions, missed quizzes and labs cannot be made up. Exceptions include required ROTC, athletic, or similar university events, significant illness, or family emergencies. Note that in all such cases, an excused absence notice from the office of the Dean of Students will be required. Student should notify Dr. O'Connor in advance if they expect to miss any coursework. Students missing a lab will not be assigned a lab partner and must complete work individually.

Academic Honesty

Students are required to comply with the university policy on academic integrity, cheating, and plagiarism found in the Code of Student Conduct at https://policy.fit.edu/policy/9267. The purpose of assignments and exams are to develop your skills and measure your progress in the course. Thus, all assessed coursework must be your own work. Several labs will include an assigned lab partner. In the case of assigned lab partners, you may share the same results as your lab partner. However, your lab report must be in your own words. You may discuss assignments with other students. However, you may not partially or completely duplicate the work of others and claim it as your own. In order to deter and detect plagiarism, online tools and other resources may be used in this class. Department and University policies allow severe penalties for plagiarism up to and including an F in the course, and/or expulsion from the University.

Lecture Recording Policy

I expressly forbid anyone from recording lectures using electronic devices with photographic, audio or video recording capability. This includes but is not limited to taking photographs, audio and/or video recordings of any lectures, labs, exams, or quizzes. Doing so without my permission and/or knowledge is a violation of the policies on Electronic Devices in the Student Handbook at https://policy.fit.edu/policy/9066. If you have been granted this privilege from the Academic Support Center, please gain my permission to do so BEFORE recording lectures.
Accommodations for Disabilities

Reasonable accommodations will be made for students with verifiable disabilities. In order to take advantage of available accommodations, students must register with the Office of Disability Services (ODS), located in the Evans Pavilion Annex. Florida Tech is committed to equal opportunity for persons with disabilities. Therefore, students with documented disabilities are entitled to reasonable and appropriate educational accommodations. Reasonable accommodations may include adjustments to the classroom or testing setting. Please make Dr. O'Connor aware of any verified disabilities at the beginning of the semester.

What is Title IX

Title IX of the Educational Amendments Act of 1972 is the federal law prohibiting discrimination based on sex under any education program and/or activity operated by an institution receiving and/or benefiting from federal financial assistance. Behaviors that can be considered sexual discrimination include sexual assault, sexual harassment, stalking, relationship abuse (dating violence and domestic violence), sexual misconduct, and gender discrimination. You are encouraged to report these behaviors. Reporting: Florida Tech can better support students in trouble if we know about what is happening. Reporting also helps us to identify patterns that might arise - for example, if more than one complainant reports having been assaulted or harassed by the same individual. Florida Tech is committed to providing a safe and positive learning experience. To report a violation of sexual misconduct or gender discrimination, please contact Linda Jancheson, Title IX Coordinator at 321-674-7277 or ljancheson@fit.edu. * Please note that as your professor, I am required to report any incidences to the Title IX Coordinator. Confidential support for students is available by contacting the Student Counseling Center at 321-674-8050.
New courses are available beginning with the fall term in which they appear in the University Catalog.

SUBJECT CSE
(Course No. 4830) CREDIT HOURS 3 ACADEMIC YEAR TO BE ADDED TO THE FILE Fall 2020

CLASS HOURS 45/semester LECTURE HOURS 45/semester LAB HOURS 0/semester CONTACT HOURS (CEU ONLY) N/A

DEPARTMENT Computer Engineering and Sciences
(e.g., Biological Sciences)

□ COLLEGE OF AERONAUTICS—23
□ COLLEGE OF ENGINEERING AND SCIENCE—25
□ COLLEGE OF PSYCHOLOGY AND LIBERAL ARTS—25
□ NATHAN M. BISK COLLEGE OF BUSINESS—24

COMPUTER TITLE SW Reverse Engineering

SCHEDULE TYPE Lecture (A)
(e.g., Lecture, Lab or Special Topics/Project)

This course will be entered into the system as: □ Bi-Level □ Cross-Listed □ Dual-Numbered □ Full-Load □ None of these/Standard Listing

CATALOG TITLE Software Reverse Engineering

CATALOG DESCRIPTION OF COURSE Restricted to 350 characters, including spaces

Examines different assembly languages and the study of how compilers generate the control flows in each language. Focuses on the constructs of if, if-then-else, Switch, and Loops. Discusses anti-RE techniques, C++ naming, polymorphism and vftables, static/dynamically compiled programs, and embedded/mobile devices.

This description has been approved by the catalog office. 8-27-2019

In addition, please attach a course syllabus and/or a more detailed description.

RESTRICTIONS
CSE 3801
□ Prerequisite ONLY □ Corequisite ONLY □ BOTH Prerequisite/Corequisite □ and □ or

Course Prefix/Number
CS 3120
□ Prerequisite ONLY □ Corequisite ONLY □ BOTH Prerequisite/Corequisite □ and □ or

Course Prefix/Number
CS 3120
□ Prerequisite ONLY □ Corequisite ONLY □ BOTH Prerequisite/Corequisite □ and □ or

Course Prefix/Number
CS 3120
□ Prerequisite ONLY □ Corequisite ONLY □ BOTH Prerequisite/Corequisite □ and □ or

Course Prefix/Number
CS 3120
□ Prerequisite ONLY □ Corequisite ONLY □ BOTH Prerequisite/Corequisite □ and □ or

Course Prefix/Number
CS 3120
□ Prerequisite ONLY □ Corequisite ONLY □ BOTH Prerequisite/Corequisite □ and □ or

Course Prefix/Number
CS 3120
□ Prerequisite ONLY □ Corequisite ONLY □ BOTH Prerequisite/Corequisite □ and □ or

ADDITIONAL RESTRICTION □ and □ or

Please indicate old course information and the date/term the course may be removed from the system:

□ Yes □ No Will this course be used to measure program-level student learning outcomes? If yes, review and signature required.

□ Yes □ No Will this course be used to satisfy the scholarly inquiry requirement? If yes, attach "Q" materials for review.

□ Yes □ No Will this course impact any existing programs? If yes, attach "Changing Graduation Requirements" form for each program impacted.

□ Yes □ No Will this course be used to satisfy the Cross Cultural (CC) requirement? If yes, attach confirmation memo from APEG Committee.

APPROVALS: On completion of description and course number verification, affix appropriate signatures as indicated, and submit to the Office of Graduate Programs, or Undergraduate Curriculum Committee Chair for placement on agenda.

OR

Chair, Graduate Council
Date

Chair, Undergraduate Curriculum Committee
Date

**Chair, APAC
Date

CATALOG & CURRICULUM MANAGER

These changes/additions have been made for the University Catalog and entered into the Banner term named above.

Catalog & Curriculum Manager
Date

REGISTRAR'S USE ONLY

SCACRSE SCADTL SCAPREQ SCABASE ACATALOG

SCARRSES CIP Code 11.0701 Operator Init. Date

Florida Institute of Technology • Office of the Registrar

150 West University Boulevard, Melbourne, FL 32901-6975 • 321-674-8144 • Fax 321-674-7827

RGR-384-219
CSE 4830 SOFTWARE REVERSE ENGINEERING

Course Information

Catalog Description

Examines different assembly languages and the study of how compilers generate the control flows in each language. Focuses on the constructs of if, if-then-else, switch, and loops. Discusses anti-RE techniques, C++ naming, polymorphism and vtables, static/dynamically-compiled programs, and embedded/mobile devices.

Textbook

There is no assigned textbook for this course. However, the following books provide useful reference material.


Prerequisites

CSE 3801 Introduction to Cyber Operations AND CSE3120 Computer Architecture and Assembly

Expected Outcomes

By the end of the course, students will have knowledge of and hands-on experience with tools and techniques for software reverse engineering. More specifically they will be prepared to:

- Apply techniques to reverse engineer x86, ARM, and MIPs assembly code using static and dynamic analysis methods.
- Analyze malware using reverse engineering tools including disassembling, debugging, and virtualizing software in sandbox environments.
- Reverse engineer unknown software to fully understand and document obfuscated functionality and communication protocols.

Grading

Your final course grade will be based on the following components ONLY:

- Homework and Programming Assignments: 45%
- Class and online participation: 5%
- Midterm Exam: 25%
- Project: 25%
Grading Scale
A: 90 to 100, B: 80 to 89, C: 70 to 79, D: 60 to 69, F: below 60

Class Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction to reverse engineering</td>
</tr>
<tr>
<td></td>
<td>Introduction to decompilers and disassemblers</td>
</tr>
<tr>
<td>2</td>
<td>Overview of reverse engineering tools</td>
</tr>
<tr>
<td></td>
<td>Overview of reverse engineering tools</td>
</tr>
<tr>
<td>3</td>
<td>x86 Control Flow</td>
</tr>
<tr>
<td></td>
<td>x86 Control Flow</td>
</tr>
<tr>
<td>4</td>
<td>Arm Control Flow</td>
</tr>
<tr>
<td></td>
<td>Arm Control Flow</td>
</tr>
<tr>
<td>5</td>
<td>Elf Binary Format</td>
</tr>
<tr>
<td></td>
<td>Elf Binary Format</td>
</tr>
<tr>
<td>6</td>
<td>Anti-RE Techniques</td>
</tr>
<tr>
<td></td>
<td>Anti-RE Techniques</td>
</tr>
<tr>
<td>7</td>
<td>C++ Naming Conventions</td>
</tr>
<tr>
<td></td>
<td>Polymorphism, Vtables</td>
</tr>
<tr>
<td>8</td>
<td>Static compilation</td>
</tr>
<tr>
<td></td>
<td>Dynamic compilation</td>
</tr>
<tr>
<td>9</td>
<td>Process Tracing</td>
</tr>
<tr>
<td></td>
<td>Process Tracing</td>
</tr>
<tr>
<td>10</td>
<td>Emulation</td>
</tr>
<tr>
<td></td>
<td>Emulation</td>
</tr>
<tr>
<td>11</td>
<td>Emulation</td>
</tr>
<tr>
<td></td>
<td>Emulation</td>
</tr>
<tr>
<td>12</td>
<td>Embedded Reverse Engineering</td>
</tr>
<tr>
<td></td>
<td>Embedded Reverse Engineering</td>
</tr>
<tr>
<td>13</td>
<td>Embedded Reverse Engineering</td>
</tr>
<tr>
<td></td>
<td>Embedded Reverse Engineering</td>
</tr>
<tr>
<td>14</td>
<td>Dynamic Analysis</td>
</tr>
<tr>
<td></td>
<td>Dynamic Analysis</td>
</tr>
<tr>
<td>15</td>
<td>Binary Analysis Challenges</td>
</tr>
<tr>
<td></td>
<td>Binary Analysis Challenges</td>
</tr>
<tr>
<td>16</td>
<td>Binary Analysis Challenges</td>
</tr>
<tr>
<td></td>
<td>Binary Analysis Challenges</td>
</tr>
</tbody>
</table>

Course Policies

Quizzes and Exams
All quizzes and exams are closed book. All lecture slides and other materials that will be included on exams will be posted to the course Canvas page. Electronic devices are not allowed
during exams. An electronic device includes, but is not limited to, cell phones, tablets, laptops, calculators, electronic translators, etc. If you are unsure if a specific device is allowed, please ask before the exam begins.

Attendance Policy

Attendance is expected in all lectures. Lectures will contain materials often outside the scope of the assigned reading but will be included in the midterm and final exam. Missing lectures could result in missing key material relevant to the exam. Practical exercises will be assigned during the class period. Missing a class will result in the instructor assigning a 0 for the specific practical exercise.

Academic Honesty

Students are required to comply with the university policy on academic integrity, cheating, and plagiarism found in the Code of Student Conduct at https://policy.fit.edu/policy/9267. The purpose of assignments and exams are to develop your skills and measure your progress in the course. Thus, all assessed coursework must be your own work. Several labs will include an assigned lab partner. In the case of assigned lab partners, you may share the same results as your lab partner. However, your lab report must be in your own words. You may discuss assignments with other students. However, you may not partially or completely duplicate the work of others and claim it as your own. In order to deter and detect plagiarism, online tools and other resources may be used in this class. Department and University policies allow severe penalties for plagiarism up to and including an F in the course, and/or expulsion from the University.

Lecture Recording Policy

I expressly forbid anyone from recording lectures using electronic devices with photographic, audio or video recording capability. This includes but is not limited to taking photographs, audio and/or video recordings of any lectures, exercises, exams, or quizzes. Doing so without my permission and/or knowledge is a violation of the policies on Electronic Devices in the Student Handbook at https://policy.fit.edu/policy/9066. If you have been granted this privilege from the Academic Support Center, please gain my permission to do so BEFORE recording lectures.

Accommodations for Disabilities

Reasonable accommodations will be made for students with verifiable disabilities. In order to take advantage of available accommodations, students must register with the Office of Disability Services (ODS), located in the Evans Pavilion Annex. Florida Tech is committed to equal opportunity for persons with disabilities. Therefore, students with documented disabilities are entitled to reasonable and appropriate educational accommodations. Reasonable accommodations may include adjustments to the classroom or testing setting. Please make the instructor aware of any verified disabilities at the beginning of the semester.
What is Title IX

Title IX of the Educational Amendments Act of 1972 is the federal law prohibiting discrimination based on sex under any education program and/or activity operated by an institution receiving and/or benefiting from federal financial assistance. Behaviors that can be considered sexual discrimination include sexual assault, sexual harassment, stalking, relationship abuse (dating violence and domestic violence), sexual misconduct, and gender discrimination. You are encouraged to report these behaviors. Reporting: Florida Tech can better support students in trouble if we know about what is happening. Reporting also helps us to identify patterns that might arise - for example, if more than one complainant reports having been assaulted or harassed by the same individual. Florida Tech is committed to providing a safe and positive learning experience. To report a violation of sexual misconduct or gender discrimination, please contact Linda Jancheson, Title IX Coordinator at 321-674-7277 or ljancheson@fit.edu. * Please note that as your professor, I am required to report any incidences to the Title IX Coordinator. Confidential support for students is available by contacting the Student Counseling Center at 321-674-8050.
New courses are available beginning with the fall term in which they appear in the University Catalog.

SUBJECT: CSE
COURSE NO.: 4840
CREDIT HOURS: 3
ACADEMIC YEAR TO BE ADDED TO THE FILE: Fall 2020

CLASS HOURS: 45/semester
LECTURE HOURS: 45/semester
LAB HOURS: 0/semester
CONTACT HOURS (CEU ONLY): N/A

DEPARTMENT: Computer Engineering and Sciences
(Specialized Sciences)
- COLLEGE OF AERONAUTICS—23
- COLLEGE OF PSYCHOLOGY AND LIBERAL ARTS—25
- NATHAN M. BISK COLLEGE OF BUSINESS—24

SCHEDULE TYPE: Lecture (A)

COMPUTER TITLE: Cyber Offense
This course will be entered into the system as: Bi-Level ☐ Cross-Listed ☐ Dual-Numbered ☐ Full-Load ☐ None of these/Standard Listing ☐

CATALOG TITLE: Cyber Offense Fundamentals
CATALOG DESCRIPTION OF COURSE: Restricted to 350 characters, including spaces

Examines offensive cyber operations scenarios from both a strategic and tactical point of view. Discusses strategic concepts including the planning, execution, and phases of cyber operations. Enumerates attack methods in the cyber kill chain and MITRE Att&ck Framework through practical exercises. Reviews case studies of offensive cyber operations.

This description has been approved by the catalog office. Catalog & Curriculum Manager Date

In addition, please attach a course syllabus and/or more detailed description.

In addition, please attach a course syllabus and/or more detailed description.

Restrictions:
- CSE 3801 ☐ Prerequisite ONLY ☐ Corequisite ONLY ☐ BOTH Prerequisite/Corequisite ☐ and ☐ or
- Course Prefix/Number
  - Prerequisite ONLY ☐ Corequisite ONLY ☐ BOTH Prerequisite/Corequisite ☐ and ☐ or
  - Course Prefix/Number
  - Prerequisite ONLY ☐ Corequisite ONLY ☐ BOTH Prerequisite/Corequisite ☐ and ☐ or
  - Course Prefix/Number
  - Prerequisite ONLY ☐ Corequisite ONLY ☐ BOTH Prerequisite/Corequisite ☐ and ☐ or
  - Course Prefix/Number
  - Prerequisite ONLY ☐ Corequisite ONLY ☐ BOTH Prerequisite/Corequisite ☐ and ☐ or

Please indicate old course information and the date/term the course may be removed from the system:

☐ Yes ☐ No Will this course be used to measure program-level student learning outcomes? If yes, review and signature required.**
☐ Yes ☐ No Will this course be used to satisfy the scholarly inquiry requirement? If yes, attach "Q" materials for review.
☐ Yes ☐ No Will this course impact any existing programs? If yes, attach "Changing Graduation Requirements" form for each program impacted.
☐ Yes ☐ No Will this course be used to satisfy the Cross Cultural (CC) requirement? If yes, attach confirmation memo from QEP2 Committee.

APPROVALS: On completion of description and course number verification, affix appropriate signatures as indicated, and submit to the Office of Graduate Programs, or Undergraduate Curriculum Committee Chair for placement on agenda.

Original Date 6/19

Department Head/Program Chair Date 9/6/2019

Dean of Associate Dean Date 9/6/2019

**Chair, APHC

Florida Institute of Technology · Office of the Registrar
150 West University Boulevard, Melbourne, FL 32901-6975 · 321-674-8114 · Fax 321-674-7827

RGR-384-219
CSE 4840 Cyber Offense Fundamentals

Course Information

Catalog Description
Examines offensive cyber operations scenarios from both a strategic and tactical point of view. Discusses strategic concepts including the planning, execution, and phases of cyber operations. Enumerates attack methods in the cyber kill chain and MITRE Att&ck Framework through practical exercises. Reviews case studies of offensive cyber operations.

Textbook
There is no assigned textbook for this course. Instructor provided materials and digital references including DoD Strategy for Operating in Cyberspace, Joint Publication 3-12, DoD Cyber Table Top Guidebook. Additionally, the following book may prove useful for students during the hands-on exercises.


Prerequisites
CSE 3801 Introduction to Cyber Operations

Expected Outcomes
By the end of the course, students will have knowledge of and hands-on experience with tools and techniques for cyber offense. More specifically they will be prepared to:
• Examine attack frameworks and vulnerability taxonomies (MITRE Att&ck, CVE, OSVDB).
• Discusses the cyber kill chain, and examines the phases of cyber operations (reconnaissance, intrusion, exploitation, privilege escalation, lateral movement, anti-forensics, denial of service, exfiltration).
• Reviews recent high-level attacks (OPM Breach, Operation NewsCaster, NotPeya, Shadow Brokers & MS17-010 EternalBlue).

Grading
Your final course grade will be based on the following components ONLY:
• Midterm Exam: 20%
• Student Project: 30%
• Practical Exercises (4 total): 40%
• Student Presentation: 10%
Grading Scale
A: 90 to 100, B: 80 to 89, C: 70 to 79, D: 60 to 69, F: below 60

Class Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Type</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lesson</td>
<td>Laws and ethics governing offensive operations</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Overview of cyber kill chain</td>
</tr>
<tr>
<td>2</td>
<td>Lesson</td>
<td>Mission planning variables (execution, objectives, phases, effects)</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Network mapping technologies (active and passive)</td>
</tr>
<tr>
<td>3</td>
<td>Practical Exercise</td>
<td>Passive reconnaissance (Shodan &amp; Recon-NG)</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Vulnerability taxonomies and exploit databases (CVE,Exploit-DB)</td>
</tr>
<tr>
<td>4</td>
<td>Lesson</td>
<td>Active reconnaissance (scanning, target enumeration)</td>
</tr>
<tr>
<td></td>
<td>Practical Exercise</td>
<td>Vulnerability scanning (OpenVAS)</td>
</tr>
<tr>
<td>5</td>
<td>Lesson</td>
<td>MITRE Att&amp;ck framework</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>DoD phases of cyber operations</td>
</tr>
<tr>
<td>6</td>
<td>Lesson</td>
<td>Intrusion/initial access/foothold</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Credential access (password spraying, LLMNR/NBT-NS, 2F auth)</td>
</tr>
<tr>
<td>7</td>
<td>Lesson</td>
<td>Exploitation (tailored client side exploits)</td>
</tr>
<tr>
<td></td>
<td>Review</td>
<td>Midterm Review</td>
</tr>
<tr>
<td>8</td>
<td>MidTerm</td>
<td>Exam In-Class</td>
</tr>
<tr>
<td>9</td>
<td>Lesson</td>
<td>Exploitation (Remote code execution exploits)</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Priv escalation (FS permissions, DLL search order, ps injection)</td>
</tr>
<tr>
<td>10</td>
<td>Practical Exercise</td>
<td>(EEP) Exploit, escalate, and pivot</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Pass the hash &amp; windows credential guard defense</td>
</tr>
<tr>
<td>11</td>
<td>Lesson</td>
<td>Denial of Service, data destruction, corruption</td>
</tr>
<tr>
<td></td>
<td>Student Presentations (2)</td>
<td>NotPeya/Wannacry ransomware attacks</td>
</tr>
<tr>
<td>12</td>
<td>Lesson</td>
<td>Exfiltration, C2 Channels, Covert Channels, Bypassing IDS</td>
</tr>
<tr>
<td></td>
<td>Student Presentations (2)</td>
<td>HammerToss/StuxNet</td>
</tr>
<tr>
<td>13</td>
<td>Lesson</td>
<td>Persistence (service/job creation, app shimming, hidden files)</td>
</tr>
<tr>
<td></td>
<td>Practical Exercise</td>
<td>Persistence exercise</td>
</tr>
<tr>
<td>14</td>
<td>Lesson</td>
<td>Defensive Evasion (code signing, compile after delivery, log clear)</td>
</tr>
<tr>
<td></td>
<td>Lesson</td>
<td>Command and Control</td>
</tr>
<tr>
<td>15</td>
<td>Lesson</td>
<td>Emerging Topics: Mainframe vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>Student Project Presentations</td>
<td>C2 Attack Framework Presentations</td>
</tr>
<tr>
<td>16</td>
<td>Student Project Presentations</td>
<td>C2 Attack Framework Presentations</td>
</tr>
<tr>
<td></td>
<td>Course Review</td>
<td>Course Review</td>
</tr>
</tbody>
</table>

Course Policies

Quizzes and Exams
All quizzes and exams are closed book. All lecture slides and other materials that will be included on exams will be posted to the course Canvas page. Electronic devices are not allowed
during exams. An electronic device includes, but is not limited to, cell phones, tablets, laptops, calculators, electronic translators, etc. If you are unsure if a specific device is allowed, please ask before the exam begins.

**Attendance Policy**

Attendance is expected in all lectures. Lectures will contain materials often outside the scope of the assigned reading but will be included in the midterm and final exam. Missing lectures could result in missing key material relevant to the exam. Practical exercises will be assigned during the class period. Missing a lesson will result in the instructor assigning a 0 for the specific practical exercise.

**Academic Honesty**

Students are required to comply with the university policy on academic integrity, cheating, and plagiarism found in the Code of Student Conduct at https://policy.fit.edu/policy/9267. The purpose of assignments and exams are to develop your skills and measure your progress in the course. Thus, all assessed coursework must be your own work. Several practical exercises will include an assigned partner. In the case of assigned partners, you may share the same results as your partner. However, your report must be in your own words. You may discuss assignments with other students. However, you may not partially or completely duplicate the work of others and claim it as your own. In order to deter and detect plagiarism, online tools and other resources may be used in this class. Department and University policies allow severe penalties for plagiarism up to and including an F in the course, and/or expulsion from the University.

**Lecture Recording Policy**

I expressly forbid anyone from recording lectures using electronic devices with photographic, audio or video recording capability. This includes but is not limited to taking photographs, audio and/or video recordings of any lectures, practical exercises, exams, or quizzes. Doing so without my permission and/or knowledge is a violation of the policies on Electronic Devices in the Student Handbook at https://policy.fit.edu/policy/9066. If you have been granted this privilege from the Academic Support Center, please gain my permission to do so BEFORE recording lectures.

**Accommodations for Disabilities**

Reasonable accommodations will be made for students with verifiable disabilities. In order to take advantage of available accommodations, students must register with the Office of Disability Services (ODS), located in the Evans Pavilion Annex. Florida Tech is committed to equal opportunity for persons with disabilities. Therefore, students with documented disabilities are entitled to reasonable and appropriate educational accommodations. Reasonable accommodations may include adjustments to the classroom or testing setting. Please make Dr. OConnor aware of any verified disabilities at the beginning of the semester.
What is Title IX

Title IX of the Educational Amendments Act of 1972 is the federal law prohibiting discrimination based on sex under any education program and/or activity operated by an institution receiving and/or benefiting from federal financial assistance. Behaviors that can be considered *sexual discrimination* include sexual assault, sexual harassment, stalking, relationship abuse (dating violence and domestic violence), sexual misconduct, and gender discrimination. You are encouraged to report these behaviors. Reporting: Florida Tech can better support students in trouble if we know about what is happening. Reporting also helps us to identify patterns that might arise - for example, if more than one complainant reports having been assaulted or harassed by the same individual. Florida Tech is committed to providing a safe and positive learning experience. To report a violation of sexual misconduct or gender discrimination, please contact Linda Jancheson, Title IX Coordinator at 321-674-7277 or ljancheson@fit.edu. *Please note that as your professor, I am required to report any incidences to the Title IX Coordinator. Confidential support for students is available by contacting the Student Counseling Center at 321-674-8050.*
New courses are available beginning with the full term in which they appear in the University Catalog.

Subject: CSE
Course No.: 4850
Credit Hours: 3
Academic Year to be Added to the File: Fall 2020

Class Hours: 45/semester
Lecture Hours: 45/semester
Lab Hours: 0/semester
Contact Hours (CEU Only): N/A

Department: Computer Engineering and Sciences
(e.g., Biological Sciences)
- College of Aeronautics—23
- College of Engineering and Science—30
- College of Psychology and Liberal Arts—25
- Nathan M. Bisk College of Business—24

Catalog Title: Introduction to Vulnerability Research

Restrictions: CSE 3801: Prerequisite Only
CSE 3120: Prerequisite Only

Grades to Be Issued: A, B, C, D, F
A, B, C, D, F, CEU/Audit
CEU
S, U
P, F
Other

In addition, please attach a course syllabus and/or more detailed description.

Approvals: On completion of description and course number verification, affix appropriate signatures as indicated, and submit to the Office of Graduate Programs, or Undergraduate Curriculum Committees Chair for placement on agenda.
CSE 4850 INTRODUCTION TO VULNERABILITY RESEARCH

Course Information

Catalog Description
Introduce exploit development by static and dynamic analysis of vulnerabilities. Provides a taxonomy of vulnerabilities including buffer overflows, use-after-free, format strings, and logic bugs. Examines the concept of overcoming exploit mitigation strategies with return-oriented-programming and memory-leaks.

Textbook

Prerequisites
CSE 3801 Introduction to Cyber Operations AND CSE 3120 Computer Architecture and Assembly Programming

Expected Outcomes
By the end of the course, students will have knowledge of and hands-on experience with tools and techniques for vulnerability research. More specifically they will be prepared to:

- Categorize vulnerabilities according to appropriate taxonomies and discuss the ways in which they can be exploited, their underlying causes, and characteristics.
- Analyze and identify buffer overflows, numeric over/underflows, use-after-free, and race conditions in both user and kernel-space software to construct exploit code.
- Review software to identify input validation issues and discuss mitigation measures in accordance with security design principles.

Grading
Your final course grade will be based on the following components ONLY:

- Homework and Programming Assignments: 45%
- Class and online participation: 5%
- Midterm Exam: 25%
- Project: 25%

Grading Scale
A: 90 to 100, B: 80 to 89, C: 70 to 79, D: 60 to 69, F: below 60
### Class Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
</tr>
</thead>
</table>
| 1    | Introduction to vulnerability research  
      | Introduction to debuggers and disassemblers |
| 2    | x86 control flow  
      | x86 control flow |
| 3    | Reverse engineering to discover vulnerabilities  
      | Reverse engineering to discover vulnerabilities |
| 4    | Static analysis of vulnerabilities  
      | Static analysis of vulnerabilities |
| 5    | Dynamic analysis of vulnerabilities  
      | Dynamic analysis of vulnerabilities |
| 6    | Buffer Overflows  
      | Buffer Overflows |
| 7    | Assembly language for shellcode  
      | Assembly language for shellcode |
| 8    | Review  
      | Mid-Term Exam |
| 9    | Return-to-stack exploit development  
      | Return-to-stack exploit development |
| 10   | Bypassing stack protection mechanisms  
      | Return-oriented-programming |
| 11   | Address Space Layout Randomization  
      | InfoLeaks and Partial Overwrites |
| 12   | Logic Bugs  
      | Logic Bugs |
| 13   | Format String Vulnerabilities  
      | Format String Vulnerabilities |
| 14   | Use-after-free vulnerabilities  
      | Use-after-free vulnerabilities |
| 15   | Binary exploit challenges  
      | Binary exploit challenges |
| 16   | Binary exploit challenges  
      | Binary exploit challenges |

### Course Policies

#### Quizzes and Exams

All quizzes and exams are closed book. All lecture slides and other materials that will be included on exams will be posted to the course Canvas page. Electronic devices are not allowed during exams. An electronic device includes, but is not limited to, cell phones, tablets, laptops, calculators, electronic translators, etc. If you are unsure if a specific device is allowed, please ask before the exam begins.
Attendance Policy

Attendance is expected in all lectures. Lectures will contain materials often outside the scope of the assigned reading but will be included in the midterm and final exam. Missing lectures could result in missing key material relevant to the exam. Practical exercises will be assigned during the class period. Missing a class will result in the instructor assigning a 0 for the specific assignment.

Academic Honesty

Students are required to comply with the university policy on academic integrity, cheating, and plagiarism found in the Code of Student Conduct at https://policy.fit.edu/policy/9267. The purpose of assignments and exams are to develop your skills and measure your progress in the course. Thus, all assessed coursework must be your own work. Several practical exercises will include an assigned partner. In the case of assigned partners, you may share the same results as your partner. However, your report must be in your own words. You may discuss assignments with other students. However, you may not partially or completely duplicate the work of others and claim it as your own. In order to deter and detect plagiarism, online tools and other resources may be used in this class. Department and University policies allow severe penalties for plagiarism up to and including an F in the course, and/or expulsion from the University.

Lecture Recording Policy

I expressly forbid anyone from recording lectures using electronic devices with photographic, audio or video recording capability. This includes but is not limited to taking photographs, audio and/or video recordings of any lectures, exams, or quizzes. Doing so without my permission and/or knowledge is a violation of the policies on Electronic Devices in the Student Handbook at https://policy.fit.edu/policy/9066. If you have been granted this privilege from the Academic Support Center, please gain my permission to do so BEFORE recording lectures.

Accommodations for Disabilities

Reasonable accommodations will be made for students with verifiable disabilities. In order to take advantage of available accommodations, students must register with the Office of Disability Services (ODS), located in the Evans Pavilion Annex. Florida Tech is committed to equal opportunity for persons with disabilities. Therefore, students with documented disabilities are entitled to reasonable and appropriate educational accommodations. Reasonable accommodations may include adjustments to the classroom or testing setting. Please make the instructor aware of any verified disabilities at the beginning of the semester.

What is Title IX

Title IX of the Educational Amendments Act of 1972 is the federal law prohibiting discrimination based on sex under any education program and/or activity operated by an institution receiving and/or benefiting from federal financial assistance. Behaviors that can be considered sexual discrimination include sexual assault, sexual harassment, stalking, relationship abuse (dating violence and domestic violence), sexual misconduct, and gender discrimination. You are encouraged
to report these behaviors. Reporting: Florida Tech can better support students in trouble if we know about what is happening. Reporting also helps us to identify patterns that might arise - for example, if more than one complainant reports having been assaulted or harassed by the same individual. Florida Tech is committed to providing a safe and positive learning experience. To report a violation of sexual misconduct or gender discrimination, please contact Linda Jancheson, Title IX Coordinator at 321-674-7277 or ljancheson@fit.edu. * Please note that as your professor, I am required to report any incidences to the Title IX Coordinator. Confidential support for students is available by contacting the Student Counseling Center at 321-674-8050.