UNIVERSITY of SOUTH FLORIDA

CIS 6930

IoT Security

CRN 20335, Section 004, 3 Credit Hours

COURSE SYLLABUS

Semester: Spring 2025
Class Meeting Days: F
Class Meeting Time: 11:00 am – 1:45 pm
Class Meeting Location: BSN 1201
Instructor: Kaushal Kafle
Office Location: BEH 309
Office Hours: Friday 2:30pm – 4:30pm
Email: kafle@usf.edu
Class Website: https://kaushalkafle.com/teaching/cis6930

I. Welcome!

This class will cover diverse topics and challenges in the space of Internet of Things (IoT) security and safety, with a particular focus on smart buildings (i.e., home, office or campus deployments). We will delve into different aspects of IoT security and safety research with an emphasis on understanding the fundamental challenges in IoT security, proposed solutions to these challenges and their tradeoffs. The course will also provide an opportunity for students to execute preliminary research ideas in security.

II. University Course Description

This seminar-style course aims to provide students with the fundamentals in conducting research in the field of IoT security.

III. Course Prerequisites

Required prerequisites: None
Informal prerequisites: An understanding of i) Operating systems (e.g., Linux, Android), ii) Computer networks, iii) File systems, and iv) Analysis of software would be beneficial. Programming background is expected.

IV. Course Purpose

This course is a graduate-level elective for students who want to learn about the current state of IoT security research, learn about the fundamentals of conducting research and learn about working in an individual or a group project in the security domain. As Internet-of-things, especially the devices and frameworks that make up the 'smart' home, get more and more integrated into the daily lives of consumers, it is vital to understand how they work, and analyze critically how secure they are. As such, this course will provide students with the necessary exposure to analyze

the contemporary work in this area, to reason about the research challenges and opportunities in this space, and finally learn to conduct meaningful research by themselves.

V. Course Format

- **Lectures**: Each class typically is structured around a short lecture that discusses the topic of the day.
- **Class Presentation and Discussion**: The lecture is followed by (or sometimes replaced with) a student presentation. This presentation then leads to a class discussion on the topic being presented. This will be an important component of each class, as this will allow students to engage with the research topic. The presentation will typically cover a research paper or a case study on the topic being discussed on that day.
- **Paper Readings and Reviews**: There will be mandatory readings prior to most classes. The reading material will provide the necessary background on the topic(s) being covered in that class so that students will be able to engage with the topic in a meaningful way. *Students will be required to submit a short review of the reading before each class.*
- **Course Project**: The course project requires that students execute research in software security. By completing the project, students will learn to think critically about security problems and solutions. All solutions have limitations, and understanding the ramification of these limitations is critical to understanding the security of an environment.
  The course project milestones mimic the steps required to create a conference-quality paper submission. Be realistic about what can be accomplished in a single semester. However, the work should reflect real thought and effort - projects executed in the closing days of the semester are unlikely to be well received. The grade will be based on the following factors: *novelty, depth, correctness, clarity of presentation, and effort*.
- **Class Interactions, Discussions and Quizzes:**
  This is a discussion-based class, as opposed to one relying solely on lectures. To do well in this course, students must take active and regular roles in discussion and demonstrate comprehension of the reading and lecture themes. This will be closely monitored by the instructor, thereby making a student's ability to demonstrate their comprehension of papers essential to a receiving a passing grade. In addition, the instructor may give quizzes at the beginning/end of *some* classes which will cover topics from the preceding lectures, presentations and readings. Quizzes missed because of absences cannot be made up unless arrangements are made with the instructor prior to the course meeting.

VI. Course Objectives

By the end of this course, students will be able to:

1. Understand and evaluate security research
2. Execute research ideas in security, at least at the preliminary level
3. Explain the fundamental challenges in IoT security, reason about state-of-the-art proposals to address them, and their tradeoffs
4. Develop a fundamental understanding of core concepts in cryptography and security as they apply to commodity computing, e.g., in the domains of mobile security and IoT.

VII. Required Texts and/or Readings and Course Materials

This is a research-based class, and has no formal textbook. The course readings will come from online book chapters, seminal papers, and other informative sources.
Here are some useful online books that provide additional information:

1. Ross Anderson. Security Engineering (http://www.cl.cam.ac.uk/~rja14/book.html), 2nd Edition. Wiley. April 2008.
2. Jaeger, T ., Operating System Security – USF Library Link, Morgan & Claypool, 2008.
3. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography (https://cacr.uwaterloo.ca/hac/). CRC Press. October 1996.

VIII. How to Succeed in this Course

- **Engage in discussion**: Engaging in the class discussion on the weekly topics are critical to success in this course. To that end, students must diligently perform the assigned readings and paper reviews which provide the necessary background for the discussions.
- **Course Project**: Collaborate on the semester-long project as these are encouraged to be done in group. Learning to work in a group environment and communicating in a clear and consistent manner with your group members is a key skill to have as a researcher.
- **Other resources**: If (or when) you run into problems in this course, utilize resources such as office hours or canvas discussion boards. Similarly, feel free to ask questions in class.

IX. Academic Continuity

If the university transitions to remote instruction, the instructor will conduct the course via live, synchronous sessions using Microsoft Teams. As with in-person classes, attendance will be mandatory (except prior approval from the Instructor). The instructor will make the class materials (including slides) available via Canvas or the course website.

X. Communication

Communications will be primarily through Canvas. Assignment submissions should be made through Canvas. Email is preferable for any urgent communication matters.

XI. Grading Scale

Grading Scale (%)			
94 – 100	A	74 – 76	C
90 – 93	A-	70 – 73	C-
87 – 89	B+	67 – 69	D+
84 – 86	B	64 – 66	D
80 – 83	B-	60 – 63	D-
77 – 79	C+	0 – 59	F

XII. Grade Categories and Weights

Graded Items	**Percent of Final Grade**
Course Research Project	45%
Paper Presentation	20%
Paper Reviews	10%
“Bug Bounty” on readings	10%
Class Participation and Discussion	15%

Course Research Project (45 points): The research project is out of 100 points distributed as follows:

- Milestone 1: Project Proposal (5 points)

- Milestone 2: Related work (10 points)
- Milestone 3: Research plan (20 points)
- Milestone 4: Research artifacts (15 points)
- Milestone 5: Final written paper (50 points)

Writing templates (where appropriate) will be provided for the milestones via canvas.

Milestone 1 - Project Proposal: The purpose of this milestone is to settle on 1) a project idea/area, and 2) a project team. While the specific project may change slightly during the course of the semester in response to the related work survey and implementation/experiment findings, it is important to have a strong direction. Projects can be in any area of IoT security, but must be approved by the instructor.
For ideas, students are encouraged to browse the last several years proceedings of USENIX Security, ACM CCS, IEEE Security and Privacy (Oakland), ISOC NDSS, and ACSAC. Each team will upload the project proposal (i.e., 5+ unique project ideas) before the specified deadline, and then meet with the instructor in the following week. Your grade on this milestone will depend on the team's ability to decide on at least one good project idea during this meeting with the instructor. I highly recommend having 5+ unique project ideas (not slight variations) for this meeting.
Milestone 2 - Related work: One of the most critical and overlooked portions of a research project is a sufficient investigation of related work. For this milestone, you will write a related work section. (refer to the course slides for what makes a good related work section). When formatting your related work, use the template provided in class. Include your title and an abstract on the first page. Do not change the font size, margins, or any other formatting.
To receive 5/10 points, the related work must be at least two full columns of text (using the provided template) and contain at least 30 citations. Websites (i.e., not academic work) count as one-half a citation. The remaining 5 points will be based on the overall quality of the document, including the writing, quality of citations, number of missing well known citations, etc. Going well beyond the minimum 30 citations will help achieve the full 10 points for this milestone.
Milestone 3 - Research plan: At this point, you have identified a problem and have at least a vague idea of your solution. A solution idea is of little value if it is not evaluated. For this milestone, you will report on how you plan to evaluate your solution idea. You must describe the following:

- **Problem statement (2 points)**: A short description (one paragraph of less) of the problem you trying to solve. Note that the problem may have been refined from previous milestones. If there are significant changes, please discuss with the instructor.
- **Solution idea (2 points):** A short description (one or two paragraphs) of how you propose to solve the problem. If the goal of your project is an empirical evaluation of some sort, name this section "Study Goal." Note that the solution idea may have been refined from the previous milestones. If there are significant changes, please discuss with the instructor.
- **Threat model (4 points):** A description (at least several paragraphs) describing the security assumptions for your solution idea. A good threat model should describe: (a) who is the adversary, (b) what are the goals of the adversary, (c) what are the capabilities of the adversary, and (d) what is the trusted computing base (TCB). Note,

when describing the adversary capabilities, if is often useful to describe assumptions of what the adversary cannot do (e.g., does not have physical access to a device).

- **Research questions (4 points):** A list of at least three (more desired) research questions that inquire about the problem and/or solution idea. Research questions should be specific, concrete, and unambiguous questions. For example, research questions may inquire about protection against specific threats, performance overhead, scalability, and usability.
- **Methodology (2 points):** A high level description of how you plan to answer the research questions. For example, a project might design and implement a protection and then empirically evaluate the protection in some way.
- **Evaluation plan (6 points):** A description of how you plan to answer the research questions. The evaluation plan may mirror the research questions, or multiple research questions may be answered by a single part of the evaluation. The proposed evaluation may be split into both the design and a more formal evaluation section. In system security research papers, the design section often provides a form of evaluation by describing how the solution defends against potential attacks. If possible, a security evaluation section should summarize the defense against the threat model. Systems security papers also have more formal evaluation sections that consist of several experiments. For each experiment, you should describe: (a) experimental setup (e.g., hardware, software, database used), (b) specific measurements and metrics you plan to use, and (c) what constitutes success.

Milestone 4 – Research artifacts (15 points) – To be submitted with Milestone 5: Security research is often backed by experimental artifacts, such as (1) code for the proposed system/analysis, (2) data collected for/generated from the analysis, and (3) applications/tools analyzed or instrumented. The availability of these artifacts is critical for the reproducibility of the research findings, as well as for helping other build upon them. Top security venues have begun optional artifact evaluations, which may become mandatory in the future. We will conduct a similar artifact evaluation at the conclusion of this class, which will be graded on completeness and correctness; i.e., your artifacts should work exactly as claimed in the paper (i.e., if code), or satisfy the claims made in the paper (if data). Of course, no security system is perfect, and we will consider the limitations that are clearly stated in the paper when evaluating artifacts (e.g., the evaluation will perform the experiments exactly detailed in the paper, without attempting corner cases).

Milestone 5 – Final paper (50 points): The written version of the final project is a conference-quality paper, consisting of 10–12 pages (not including references), 1-inch margins, two column, 10-pt font. Suggested outline is a follows:

- Abstract (around 200 words)
- Introduction (includes references to highly-relevant related work, i.e., state of the art for the problem you are trying to solve)
- Overview of Approach (a nice and accessible “English” description of your approach)
- Protocol/Architecture/Design/…
- Evaluation (don’t forget to interpret your data)
- Discussion (discuss some of the important simplifying assumptions, and suggest possibilities for future work)

- Related Work ("somewhat related" work goes here; directly related work goes into the Introduction)
- Conclusions (don't summarize your work here. That's what the abstract was for. Instead provide some philosophical ruminations of your work and future possibilities, i.e., conclusions that you have arrived at as a result of your work.)
- References

Reading Bug bounty (10 points): The assigned readings are futile unless done *in depth*. As reading 20+ papers in depth in the span of a semester is burdensome, this class pursues an alternative: read few papers, provided you read them in-depth, and think critically about them.Each student can earn 10 bonus points by reporting 2 non-trivial mistakes/bugs/unjustified assumptions made in the papers. Following conditions should be met for the reporting to be valid: (1) you must be the **first in class** to report it (hence, report privately to the instructor), (2) it must be **non-trivial** (i.e., minor spelling/grammar errors, or minor calculation errors that do not affect the claims made in the paper, do not count), and (3) you must be able to **reason about it**, i.e., explain *why* it is a mistake. The instructor reserves the right to adjudicate the validity of a reported bug.

Paper Presentations (20 points): Students will present a select set of recent conference papers on IoT security and safety. Each presentation must be at most 30 mins, and must end with 3 insightful questions to kick-start the class discussion. These presentations will be graded for *content, clarity, and the 3 questions*.

Paper Reviews (10 points): Students will write *conference-style paper reviews* for each paper presented in class. Reviews will be submitted at the beginning of the class, and will ensure that students (1) can evaluate research in IoT security, and that they (2) know enough to participate in class discussions.

Rules for reviews:
1. The student presenting the paper **does not** have to write a review.
2. The review must contain the following (the instructor will provide a review template): i) a list of strengths, ii) a list of weaknesses, and iii) a detailed justification for each strength and weaknesses, i.e., why the reviewer considers a particular aspect of the paper to be a weakness in the context of the claims the paper is making.
3. If *two reviews are assigned* in a week, you **only have to do one** of the two.

XIII. Course Schedule.

[***Some reading links may require you to log in through the institute's SSO (i.e., via USF NetID) to access. If you are still unable to access any material using the provided link, ask for the pdf directly from the instructor.***]

Date	Topics	Readings	Other Activities/Notes
01/17	Course Introduction		1. Project Proposal assigned; due on 02/07 2. Spring drop/add ends
01/24	Smart home platform security (and a visit to the past)	[*READ*] Security Analysis of Emerging Smart Home Applications [link]	

		[*REVIEW*] A Study of Data Store-based Home Automation [link]	
01/31	1. Project Discussions 2. IoT mobile App Security Analysis	[*REVIEW*] Understanding IoT Security from a Market-Scale Perspective [link]	
02/07	Detecting and preventing security and safety issues in IoT Apps	[*REVIEW*] Soteria: Automated IoT Safety and Security Analysis [link] [*READ*] IoTGuard: Dynamic Enforcement of Security and Safety Policy in Commodity IoT [link]	1. **Project Proposal Due**, 2. Related work assigned; due 02/28
02/14	Security Evaluation of IoT Deployments	[*REVIEW*] SoK: Security Evaluation of Home-Based IoT Deployments [link]	
02/21	Data leaks in IoT apps	[*REVIEW*] Sensitive Information Tracking in Commodity IoT [link] [*READ*] A Study of Android Application Security [link]	
02/28	Provenance tracking and contextual integrity in IoT	[*REVIEW*] Fear and Logging in the Internet of Things [link] [*READ*] ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms [link]	1. **Related work due** 2. Research plan assigned; due 03/28
03/07	Access Control Enhancements for Integrity	[*REVIEW*] Practical Integrity Validation in the Smart Home with HomeEndorser [link] [*READ*] Situational Access Control in the Internet of Things [link]	
03/14	Multi-user Smart Home Access Control	[*REVIEW*] Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study [link] [*READ*] Rethinking Access Control and Authentication for the Home Internet of Things (IoT) [link]	
03/21	Spring Break – No Class		
03/28	Beyond IoT Apps – Synthetic Event Generation	[*REVIEW*] Towards a Natural Perspective of Smart Homes for Practical Security and Safety Analyses [link]	1. **Research plan due**

04/04	Security analysis of Trigger-action programs	[*REVIEW*] Some Recipes Can Do More Than Spoil Your Appetite: Analyzing the Security and Privacy Risks of IFTTT Recipes [link] [*READ*] How Risky Are Real Users' IFTTT Applets? [link]	
04/11	Correcting Trigger-action programs	[*REVIEW*] AutoTap: Synthesizing and Repairing Trigger-Action Programs Using LTL Properties [link]	
04/18	Attacking Voice Assistants	[*REVIEW*] Skill Squatting Attacks on Amazon Alexa [link] [*READ*] CommanderSong: A Systematic Approach for Practical Adversarial Voice Recognition [link]	
04/25	Smart Home Privacy Challenges	[*REVIEW*] Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices [link] [*READ*] Smart Home Privacy Policies Demystified: A Study of Availability, Content, and Coverage [link]	
05/02	Final Project Presentations		
05/04			**1. Final paper due**

* Note: The Schedule is subject to revision as the semester progresses.

XIV. USF Core Syllabus Policies

USF has a set of central policies related to student recording class sessions, academic integrity and grievances, student accessibility services, academic disruption, religious observances, academic continuity, food insecurity, pregnancy and related conditions, and sexual harassment that **apply to all courses at USF**. Be sure to review these online: usf.edu/provost/faculty-success/resources-policies-forms/core-syllabus-policy-statements.aspx

XV. Course Policies: Grades

Medical Excuses:

Students should not attend class if they are ill, particularly if they have fever and/or gastrointestinal symptoms and/or respiratory symptoms such as a sneezing, runny nose, sore throat or coughing. Students experiencing any of these symptoms should contact immediately the Student Health Services (813-974-2331) on the Sarasota-Mantatee and Tampa campus or the Wellness Center (727-873-4422) on the St. Petersburg campus for appropriate medical guidance and to obtain a verification of care letter. Students may turn to other health providers as well. **To be approved for missed classes, late assignments or missed**

examinations a verification of care letter must be presented by the student to the faculty member upon return to class.

Campus Free Expression: *It is fundamental to the University of South Florida's mission to support an environment where divergent ideas, theories, and philosophies can be openly exchanged and critically evaluated. Consistent with these principles, this course may involve discussion of ideas that you find uncomfortable, disagreeable, or even offensive. In the instructional setting, ideas are intended to be presented in an objective manner and not as an endorsement of what you should personally believe. "Objective" means that the idea(s) presented can be tested by critical peer review and rigorous debate, and that the idea(s) is supported by credible research. In this course you may be asked to engage with complex ideas and to demonstrate an understanding of the ideas. Understanding and engaging with an idea does not require you to believe it or to agree with it.*

Make-up Exams Policy: If a student cannot be present for an examination for a valid reason (validity to be determined by the instructor), a make-up exam will be given only if the student has notified the instructor in advance that s/he cannot be present for the exam. Make-up exams are given at the convenience of the instructor as the schedule allows.

Group Work Policy: Everyone must take part in a group project and contribute to the success of the project in a proportional manner. Individual scores will be evaluated based on the final project report, submitted artifacts and the final presentations/Q&A with the individual members of the group.

XVI. Course Policies: Student Expectations

Health and Wellness: Your health is a priority at the University of South Florida. We encourage members of our community to look out for each other and to reach out for help if someone is in need. If you or someone you know is in distress, please make a referral at www.usf.edu/sos so that the Student Outreach & Support can contact and provide helpful resources to the student in distress. A 24-hour licensed mental healthcare professional, offered through the counseling center, is available by phone at 813-974-2831, option 3. Please remember that asking for help is a sign of strength. In case of emergency, please dial 9-1-1.

Title IX Policy: Title IX provides federal protections for discrimination based on sex, which includes discrimination based on pregnancy, sexual harassment, and interpersonal violence. In an effort to provide support and equal access, USF has designated all faculty (TA, Adjunct, etc.) as Responsible Employees, who are required to report any disclosures of sexual harassment, sexual violence, relationship violence or stalking. The Title IX Office makes every effort, when safe to do so, to reach out and provide resources and accommodations, and to discuss possible options for resolution. Anyone wishing to make a Title IX report or seeking accommodations may do so online, in person, via phone, or email to the Title IX Office. For information about Title IX or for a full list of resources please visit: https://www.usf.edu/title-ix/gethelp/resources.aspx. If you are unsure what to do, please contact Victim Advocacy – a confidential resource that can review all your options – at 813-974-5756 or va@admin.usf.edu.

Generative AI: With advancements in AI, tools like GPT-4 can generate human-like text and code, raising potential issues related to academic integrity and the authenticity of student

work.
For this class, the following Generative AI rules will apply:

1. You must cite all AI-generated content used in submissions.
2. If used, you must explicitly detail how AI-generated content was used in your submission.
3. The professor can insist that you demonstrate a deep understanding of the subject matter, not solely relying on AI-generated content.
4. You are permitted to use AI tools as a supplemental resource (i.e., as an editor), not as the primary means of completing assignments.
5. Understanding that generative AI tools, while powerful, are not infallible and can produce misinformation or inaccurate results. You will be responsible for the accuracy of your submissions and must cross-verify the information produced by these tools with reliable sources.

Course Hero / Chegg Policy: The USF Policy on Academic Integrity specifies that students may not use websites that enable cheating, such as by uploading or downloading material for this purpose. This does apply specifically to Chegg.com and CourseHero.com – almost any use of these websites (including uploading proprietary materials) constitutes a violation of the academic integrity policy.

Professionalism Policy: Per university policy and classroom etiquette; mobile phones, iPods, etc. **must be silenced** during all classroom and lab lectures. Those not heeding this rule will be asked to leave the classroom/lab immediately so as to not disrupt the learning environment. Please arrive on time for all class meetings. Students who habitually disturb the class by talking, arriving late, etc., and have been warned may suffer a reduction in their final class grade.

Turnitin.com: In this course, turnitin.com will be utilized. Turnitin is an automated system which instructors may use to quickly and easily compare each student's assignment with billions of web sites, as well as an enormous database of student papers that grows with each submission. Accordingly, you will be expected to submit all assignments in both hard copy and electronic format. After the assignment is processed, as instructor I receive a report from turnitin.com that states if and how another author's work was used in the assignment. For a more detailed look at this process visit http://www.turnitin.com. Essays are due at turnitin.com the same day as in class.

Netiquette Guidelines

1. Act professionally in the way you communicate. Treat your instructors and peers with respect, the same way you would do in a face-to-face environment. Respect other people's ideas and be constructive when explaining your views about points you may not agree with.
2. Be sensitive. Be respectful and sensitive when sharing your ideas and opinions. There will be people in your class with different linguistic backgrounds, political and religious beliefs or other general differences.
3. Proofread and check spelling. Doing this before sending an email or posting a thread on a discussion board will allow you to make sure your message is clear and thoughtful. Avoid the use of all capital letters, it can be perceived as if you are shouting, and it is more difficult to read.
4. Keep your communications focused and stay on topic. Complete your ideas before changing the subject. By keeping the message on focus you allow the readers to easily get your idea or answers they are looking for.

5. Be clear with your message. Avoid using humor or sarcasm. Since people can't see your expressions or hear your tone of voice, meaning can be misinterpreted.

End of Semester Student Evaluations: All classes at USF make use of an online system for students to provide feedback to the University regarding the course. These surveys will be made available at the end of the semester, and the University will notify you by email when the response window opens. Your participation is highly encouraged and valued**.**

XVII. Learning Support and Campus Offices

Academic Accommodations

Students with disabilities are responsible for registering with Student Accessibility Services (SAS) in order to receive academic accommodations. For additional information about academic accommodations and resources, you can visit the SAS website.
SAS website for the Tampa and Sarasota-Manatee campuses.
SAS website for the St. Pete campus.

Academic Support Services

The USF Office of Student Success coordinates and promotes university-wide efforts to enhance undergraduate and graduate student success. For a comprehensive list of academic support services available to all USF students, please visit the Office of Student Success website.

Canvas Technical Support

If you have technical difficulties in Canvas, you can find access to the Canvas guides and video resources in the "Canvas Help" page on the homepage of your Canvas course. You can also contact the help desk by calling 813-974-1222 in Tampa or emailing help@usf.edu.
IT website for the Tampa campus.
IT website for the St. Pete campus.
IT website for the Sarasota-Manatee campus.

Center for Victim Advocacy

The Center for Victim Advocacy empowers survivors of crime, violence, or abuse by promoting the restoration of decision making, by advocating for their rights, and by offering support and resources. Contact information is available online.

Counseling Center

The Counseling Center promotes the wellbeing of the campus community by providing culturally sensitive counseling, consultation, prevention, and training that enhances student academic and personal success. Contact information is available online.
Counseling Center website for the Tampa campus.
Counseling Center website for the St. Pete campus.
Counseling Center website for the Sarasota-Manatee campus.

Tutoring

The Tutoring Hub offers free tutoring in several subjects to USF undergraduates. Appointments are recommended, but not required. For more information, email asctampa@usf.edu.
Tutoring website for the Tampa campus.
Tutoring website for the St. Pete campus.

Tutoring website for the Sarasota-Manatee campus.

Writing Studio

The Writing Studio is a free resource for USF undergraduate and graduate students. At the Writing Studio, a trained writing consultant will work individually with you, at any point in the writing process from brainstorming to editing. Appointments are recommended, but not required. For more information or to make an appointment, email: writingstudio@usf.edu.
Writing studio website for the Tampa campus.
Writing studio website for the St. Pete campus.
Writing studio website for the Sarasota-Manatee campus.

XVIII. Important Dates to Remember

All the dates and assignments in the class schedule are tentative and can be changed at the discretion of the professor. For important USF dates, see the Academic Calendar at http://www.usf.edu/registrar/calendars/

XIX. Other Information:

The College of Engineering has worked diligently with Student Counseling Services to appoint our Licensed Mental Health Counselor dedicated to making mental health services more readily accessible to our students. Michelle Morton-Tunstall will continue to provide clinical counseling to our students both here in ENB and at the central counseling center in the Fall semester. Specifically, Michelle will be available to our students at two locations: our College (ENB201) and the central counseling center. This dual-location arrangement is designed to meet the diverse needs of our students, considering factors such as privacy, convenience, and accessibility. Initially, Michelle will be on-site at our College every Wednesday and Thursday from 2-5 p.m., starting from April 1st through May 3rd, while we study the appropriate ratio of demand for meeting here and central unit location. She is currently undergoing training at the central counseling center.