UNIVERSITY of SOUTH FLORIDA

CIS 4930

Secure IoT

CRN 96661, Section 006, 3 Credit Hours

COURSE SYLLABUS

Semester: Fall 2024
Class Meeting Days: T, R
Class Meeting Time: 2:00 – 3:15 pm
Class Meeting Location: CHE 101
Instructor: Kaushal Kafle
Office Location: BEH 309
Office Hours: Tuesdays and Thursdays 11:00 am – 12:30 pm
Email: kafle@usf.edu
Class website: https://kaushalkafle.com/teaching/cis4930
TA office hours: Mondays 1-2pm Teams link

I. Welcome!

This class will cover diverse topics and challenges in the space of Internet of Things (IoT) security, with a particular focus on smart buildings (i.e., home, office or campus deployments). We will explore these challenges in relation to existing security concepts including (but not limited to) access control, authentication, network security, program analysis and operating systems security.

II. University Course Description

Special topics in computer science and computer engineering

III. Course Prerequisites

COP 4530 and CDA 3201

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

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. This course will provide the necessary background in network security (e.g., SSL/TLS) and concepts of operating system security (e.g., access control) to understand and analyze the modern smart home platforms. It also covers topics directly related to the security of the modern smart home platforms and their architectures, including the paradigm of trigger-action programming that is enabled in every major smart home

platform. The course also provides students with the opportunity to directly work on a commercial smart home platform (e.g., HomeAssistant) to create automations or perform network tests by utilizing its programming interfaces.

V. Course Format

- **Lectures**: Each class typically is structured around a lecture that discusses the topic of the day.
- **Homework assignments**: The instructor will assign periodic homework assignments. The assignments may involve basic programming, writing or performing basic research. Consult the schedule to refer to when they will be assigned and when they are due. They make up 20% of the course grade.
- **Readings**: There will be recommended readings prior to most classes. The reading material will provide supplementary background to the topics being covered in that class. Paper readings will be few, but the emphasis will be on reading them in-depth and thinking *critically* about them. To this end, 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.
- **Course Project**: The course project is divided into two phases.
  The **first phase** will focus heavily on building automated testing scripts on simulated devices in the HomeAssistant smart home platform. The focus will be on learning the architecture of and real-world programming on top of a commercial smart home platform.
  The **second phase** will focus on mobile IoT app vulnerabilities. As such, students will perform analysis on sample IoT apps to find potentially exploitable vulnerabilities in them.
  Each phase will amount to 20% in the course grade.
- **Class Interactions and Quizzes:** The course relies on interactive lectures, so students are expected to interact with the Instructor on the course materials being discussed. Quizzes may given at the beginning/end of class and will cover topics from the preceding lecture and readings. Quizzes missed because of absences cannot be made up unless arrangements are made with the instructor prior to the course meeting. Combined, they make up 10% of the course grade.

VI. Course Objectives

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

- Explain the architecture of general IoT platforms, and the underlying security challenges.
- Outline the security problems and potential solutions in various concepts associated with IoT platforms, such as trigger-action programming, multi-user homes, lateral privilege escalation.
- Perform manual and semi-automated analysis of mobile IoT apps.
- Write automated scripts to interact with the HomeAssistant platform
- Explain concepts related to network security and access control in operating systems (e.g., the principle of least privilege), and their security implications.

VII. Required Texts and/or Readings and Course Materials

- There are no required textbooks for the class.
- Recommended readings will be provided in the course schedule, and may be updated up to 1 week prior to the scheduled class. They may consist of book chapters or security papers related to the topic of the day. Students can earn bonus points through the class readings associated with security papers (details above).

VIII. 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.

IX. Communication

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

X. Grading Scale

Grading Scale (%):

>=95	A	65 - 69	C
90 - 94	A-	60 - 64	C-
85 - 89	B+	55 - 59	D+
80 - 84	B	50 - 54	D
75 - 79	B-	45 - 49	D-
70 - 74	C+	0 - 44	F

XI. Grade Categories and Weights

Graded Items	Percent of Final Grade
Course Project (2 Phases, 20% each phase)	40%
Final Exam	20%
Midterm	10%
Homework Assignments	20%
In-Class Participation/Quizzes	10%
Readings (Finding 2 non-trivial mistakes, *details above*)	10% (bonus)

XII. Course Schedule.

Note: Recommended Readings that are TBA will be added a week before the scheduled class.

Date	Topics	Recommended Readings	Other Activities/Notes
08/27	Course Introductions	Reflections on Trusting Trust (Turing Award Lecture 1983) [link]	1. Homework 1 assigned; due 09/03 11:59 pm 2. Project Phase 1 (Idea and Team formation) assigned; due 09/05 11:59 pm
08/29	1. IoT Security fundamentals 2. Intro to HomeAssistant	1. Security Engineering, Chapter 1 [link]	**08/30 Last day to add/drop classes**

		2. HomeAssistant Architecture [link1, link2] and Integrations [link1, link2]	
09/03	Crypto 1: Secret Key Crypto	Security Engineering, Chapter 5.1-5.5 [link]	Homework 1 due
09/05	Crypto 2: Hashes and Message Authentication	1. Security Engineering, Chapter 5.6 [link] 2. Ross Anderson, Why CryptoSystems fail [link]	1. Homework 2 assigned; due 09/19 11:59 pm 2. Project Phase 1 due
09/10	Crypto 3: Public Key Cryptography	Security Engineering, Chapter 5.7 [link]	Project Phase 2 assigned (HomeAssistant Integration Design and Implementation); due 10/22 11:59 pm
09/12	SSL/TLS	SSL and TLS: A Beginner's Guide [link]	
09/17	Access Control Basics	1. Operating System Security, Chapters 1,2 and 5 [link] 2. [*Only Section I-A*] J. Saltzer and M. Schroeder, The Protection of Information in Computer Systems. Proceedings of the IEEE 63(9) (1975) pp. 1278-1308 [link]	Project Plan (title, design, timeline, etc.) of the chosen project due
09/19	Information Flow Control	1. [BB] How risky are real users' IFTTT applets? [link]	Homework 2 due
09/24	Trigger-Action Programs	1. [BB] Soteria: Automated IoT Safety and Security Analysis [link] 2. [BB] Towards a natural perspective of Smart Homes for Practical Security and Safety Analyses [link]	Homework 3 assigned; due 10/08
09/26	~~Smart Home Platforms: Architecture and Security~~ **Cancelled due to Helene**	1. [BB] Security Analysis of Emerging Smart Home Applications [link]	
10/01	Smart Home Platforms: Lateral Privilege escalation	1. [BB] A Study of Data Store-based Home Automation [link]	
10/03	Smart Home Security: Situational Access Control and Integrity Validation	1. [BB] Situational Access Control in IoT [link] 2. [BB] Practical Integrity Validation in the Smart Home [link]	

10/08	~~Permission models: Smart Home vs Android apps~~ **Cancelled due to Milton**	~~1. [BB] Android Permissions Demystified [link]~~	~~Homework 3 due~~
10/10	~~1. Smart Home: Challenges of Multiuser Access Control~~ 2. ~~Midterm exam review~~ **Cancelled due to Milton**	~~1. [BB] Rethinking Access Control and Authentication for the Home IoT [link]~~	
10/15	~~**Midterm exam**~~ Asynchronous Class 1: 'Multi-User based Smart Home Access Control'	1. [BB] Rethinking Access Control and Authentication for the Home IoT [link]	
10/17	Asynchronous Class 2: 'Crypto-API Misuses in IoT Apps'	1. [BB] Jin et. al., Understanding IoT Security from a Market-Scale Perspective, CCS 2022 [link]	
10/22	1. Integrity Validation (contd..) 2. Class updates, Midterm notice		
10/24	**Midterm Exam**		Homework 3 due
10/29	1. Async classes recap 2. Permission Models and Platform Defenses	[BB] Android Permissions Demystified [link]	
10/31	Smart Home Wrap-Up: Privacy Issues	1. [BB] Smart Home Privacy Policies Demystified [link]	1. Project Phase 2 report due 2. Project Phase 3 (IoT app analysis proposal) assigned; due 11/07
11/05	Network Security: TCP	A look back at "Security problems in the TCP/IP protocol suite" [link]	
11/07	Network Security: Worms and Botnets	S. Staniford and V. Paxson and N. Weaver. How to 0wn the Internet in Your Spare Time. In Proceedings of the 11th USENIX Security Symposium, August 2002. [link]	1. Project Phase 3 due 2. Homework 4 assigned; due 11/26
11/12	Network Security: Routing	Why is it Taking so Long to Secure Internet Routing? [link]	Project Phase 4 (Implementation and Evaluation) assigned; due 12/12
11/14	Network Security: Wireless	Brenza et al. A Practical Investigation of Identity Theft Vulnerabilities in Eduroam. In Proceedings of the ACM Conference on Security and Privacy in Wireless	

		and Mobile Networks (WiSec). 2015 [link]	
11/19	Network Security: Intrusion Detection and Firewalls	S. Axelsson, The Base-Rate Fallacy and Its Implications for the Difficulty of Intrusion Detection. In Proceedings of the ACM Conference on Computer and Communication Security. November, 1999. [link]	
11/21	Network Security: User Authentication 1	The science of password selection, Troy Hunt [link]	
11/26	Network Security: User Authentication 2	P. G. Kelley et al., Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. IEEE Symposium on Security and Privacy, 2012. [link]	Homework 4 due
11/28	**No Class** Happy Thanksgiving!		
12/03	Course Summary: Finals review and Project updates 1		
12/05	Course Summary: Finals review and Project updates 2		
12/10	**Final exam**		
12/12 Thursday	**Final report due**		Project Phase 4 report due

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

XIII. 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

XIV. Course Policies:

Late Work Policy:

There are no make-ups for in-class writing, quizzes, the midterm, or the final exam. Assignments turned in up to 24 hours late will count for 50% of its associated weight, and 0% after that. Project milestones submitted up to 24 hours late will count for 50% of its associated weight, and 0% after that.

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.**

Extra Credit Policy:

- Extra credit can be earned through the course readings of security papers. Each student can earn 5 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.

Grades of "Incomplete":

The current university policy concerning incomplete grades will be followed in this course. For undergraduate courses: An "I" grade may be awarded to a student only when a small portion of the student's work is incomplete and only when the student is otherwise earning a passing grade. The time limit for removing the "I" is to be set by the instructor of the course. For undergraduate students, this time limit may not exceed two academic semesters, whether or not the student is in residence, and/or graduation, whichever comes first. For graduate students, this time limit may not exceed one academic semester. "I" grades not removed by the end of the time limit will be changed to "IF" or "IU," whichever is appropriate.

Attendance Policy:

Students are expected to attend classes. The instructor will inform students of attendance requirements on the syllabus, and will accommodate excused absences by making arrangements with students ahead of time (when possible) or by providing a reasonable amount of time to make up missed work.

First Day Attendance Policy

This course will use the "first day attendance" system in Canvas to record your first day of attendance. The associated USF policy and details can be found here: How to keep your courses.

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 (scheduled on a case-by-case basis).

Group Work Policy:

Everyone must take part in group projects. All members of a group will receive the same score; that is, the project is assessed and everyone receives this score. Once formed, groups cannot be altered or switched, except for reasons of extended hospitalization.

Final Examinations Policy: The final exam will be scheduled in accordance with the University's final examination policy.

XV. 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.*

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, the instructor may utilize turnitin.com. Turnitin is an automated system which instructors may use to compare each student's assignment quickly and easily 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 the electronic format and the hard copy (if needed). 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.

XVI. 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.

XVII. Important Dates to Remember

All the dates and assignments are tentative and can be changed at the discretion of the professor.
Follow the course schedule closely for course work related deadlines.
For important USF dates, see the Academic Calendar at http://www.usf.edu/registrar/calendars/

Drop/Add Deadline:	*Fri, Aug 30, 2024*
Labor Day Holiday:	*Mon, Sept 2, 2024*
Mid-term Grading Opens:	*Mon, Oct 7, 2024*
Mid-term Grading Closes:	*Tues, Oct 22, 2024*
Withdrawal Deadline:	*Sat, Nov 2, 2024*
Veteran's Day Holiday:	*Mon, Nov 11, 2024*
Thanksgiving Holiday:	*Thurs, Nov 28, & Fri, Nov 29, 2024*
Final Examination Week:	*Sat, Dec 7 - Thurs, Dec 12, 2024*