CIS 4930: Secure IoT

Prof. Kaushal Kafle

Lecture 1: Introduction

Lets break it down

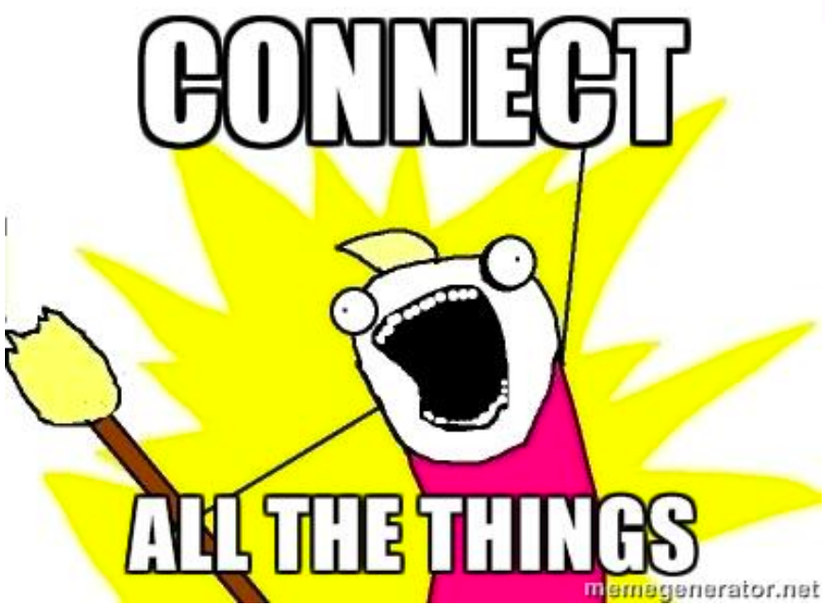
- *Internet* of *Things* (IoT) *Security*

- *How many of you have used “smart” devices in your home?*

The Internet

- Every machine is connected
- Huge, *open*, system
  - No barrier to entry
  - Not just limited to dogs and users
- Built for connectivity, not security (i.e., the "end-to-end" principle)

"On the Internet, nobody knows you're a dog."



The Internet

UnitedHealth says Change Healthcare cyberattack cost it $872 million

MONEY WATCH

By **Khristopher J. Brooks**
Edited By **Anne Marie Lee**
Updated on: April 18, 2024 / 10:30 AM EDT / CBS News

future tense

We Still Haven't Learned the Major Lesson of the 2013 Target Hack

Forty million credit and debit cards, 70 million customers' information, nine years of repeating the same mistakes.

BY WOODROW HARTZOG AND DANIEL J. SOLOVE APRIL 13, 2022 • 5:50 AM

Identity Theft > Data Breaches

Equifax's Massive Data Breach Has Cost the Company $4 Billion So Far

By: Paul J. Lim

Published: Sep 12, 2017 | **4 min read**

PRIVACY / POLICY / TECH

Hackers stole encrypted LastPass password vaults, and we're just now hearing about it

Things are…


nest


nest
AIRWAVE
74


nest


SAMSUNG


wemo


PHILIPS


Yale
1 2 3
4 5 6
CARD
7 8 9
* 0 #

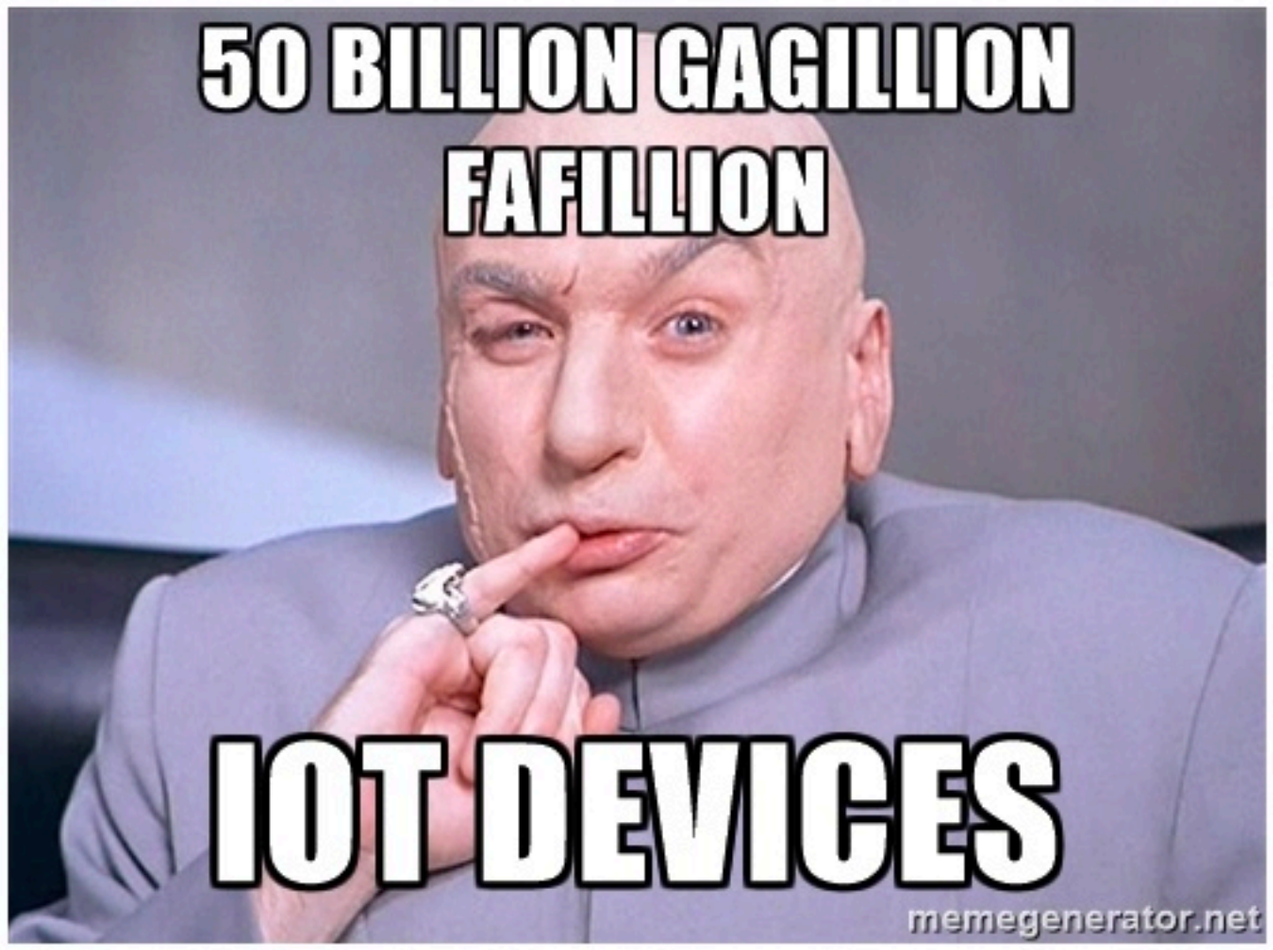

amazon

Things are…

Ubiquitous —

7 Billion[1]

devices in use!



[1] https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/

Things are…

Financially Critical —

$520 Billion[2] by 2021

Expensive —

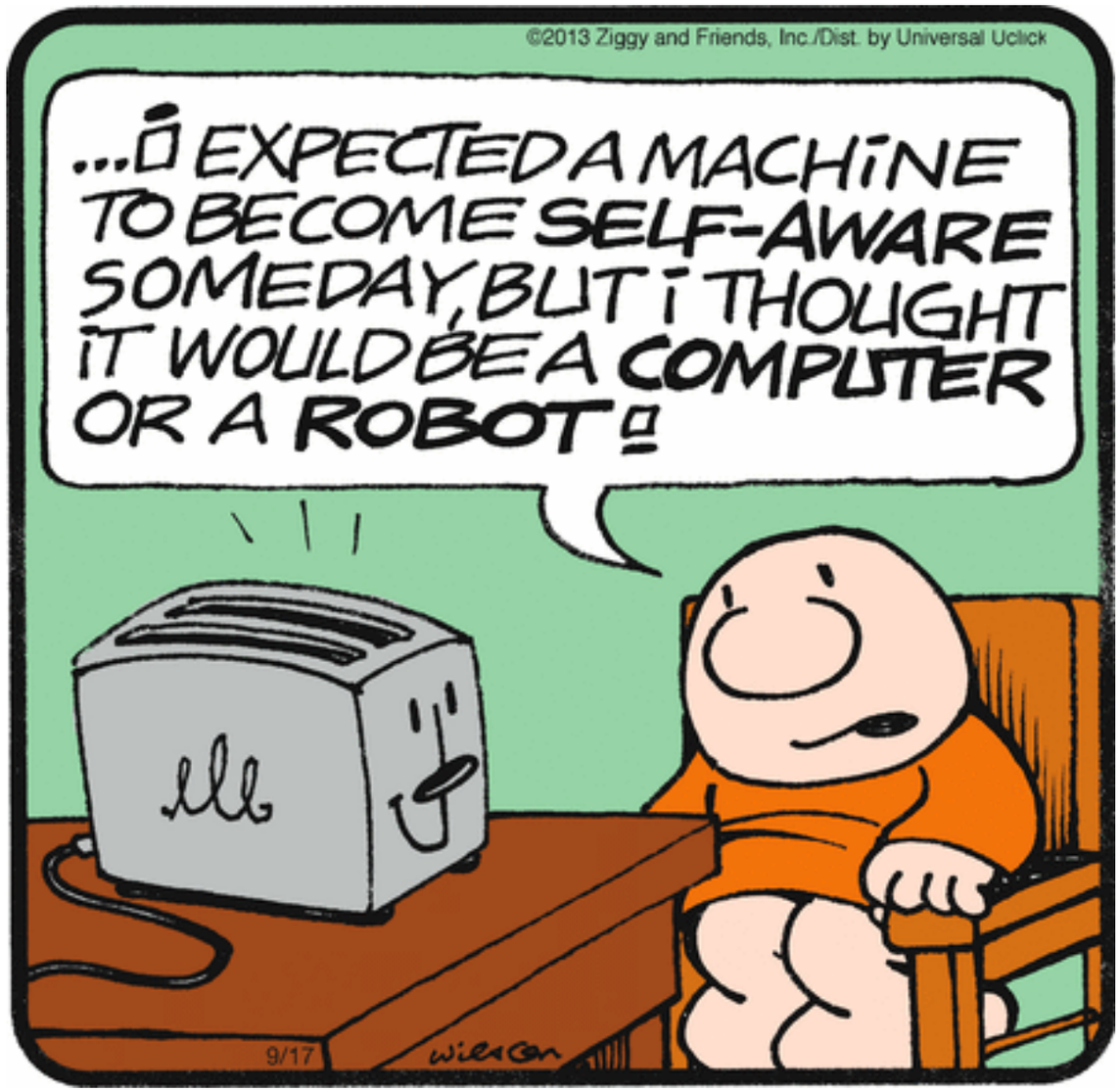
Cameras, door locks cost $$$

[2]https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/

Things are…

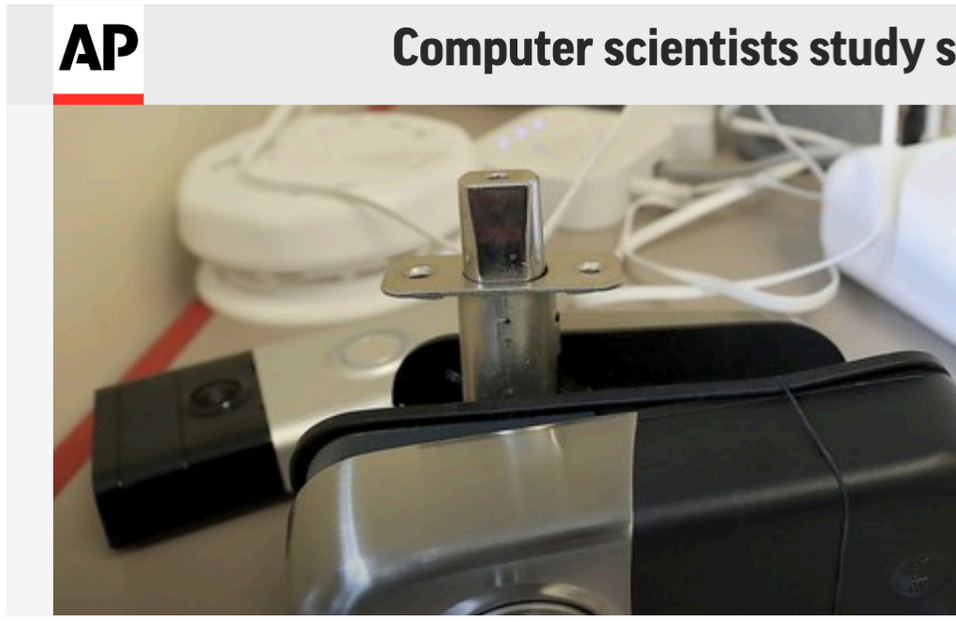
Physical —

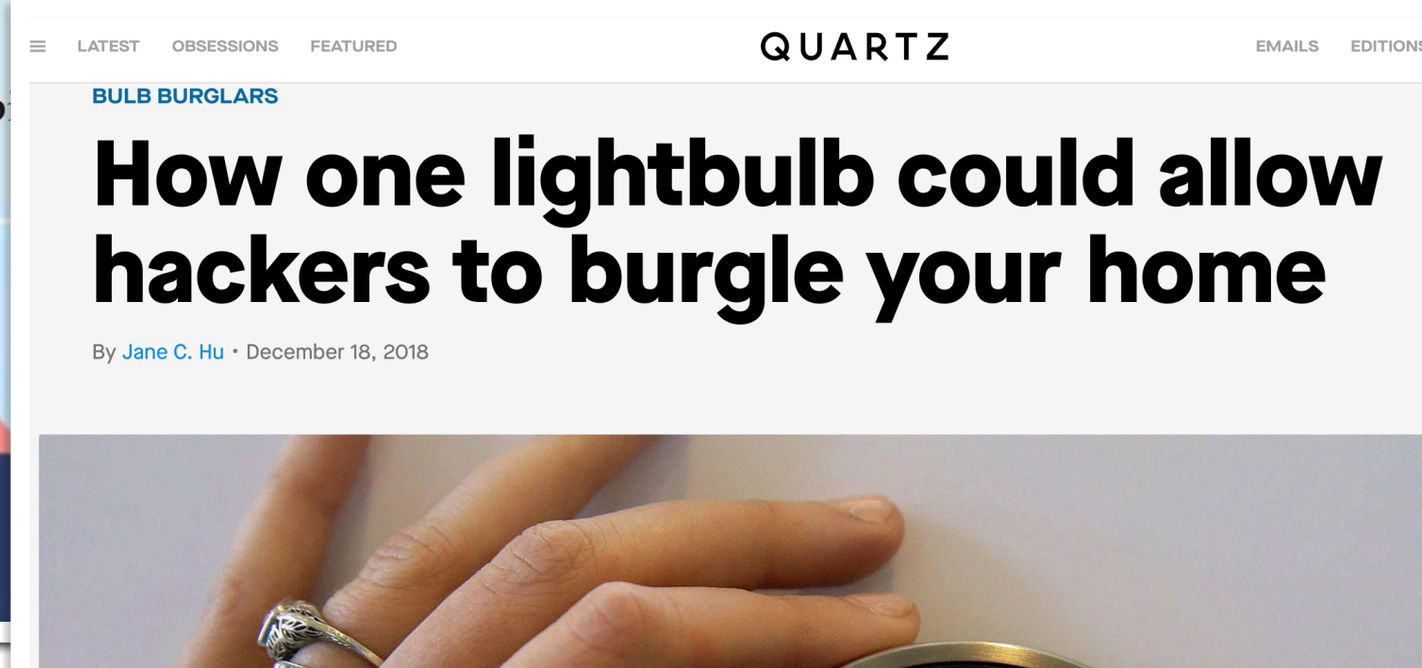
Can view, listen to, and modify our physical spaces.



Some bad news

- We are bad at designing secure systems





Some bad news

- IoT is no different

Tech > Tech Industry

Hacked Nest Cam convinces family that US is being attacked by North Korea

> CYBERSECURITY

Criminals Hacked A Fish Tank To Steal Data From A Casino

Internet Of Things ▶

Massive DDoS Attack On U.S. College Throws IoT Security Into The Spotlight -- Again

Designing secure systems is hard

Fundamental Asymmetry between the attacker and the defender

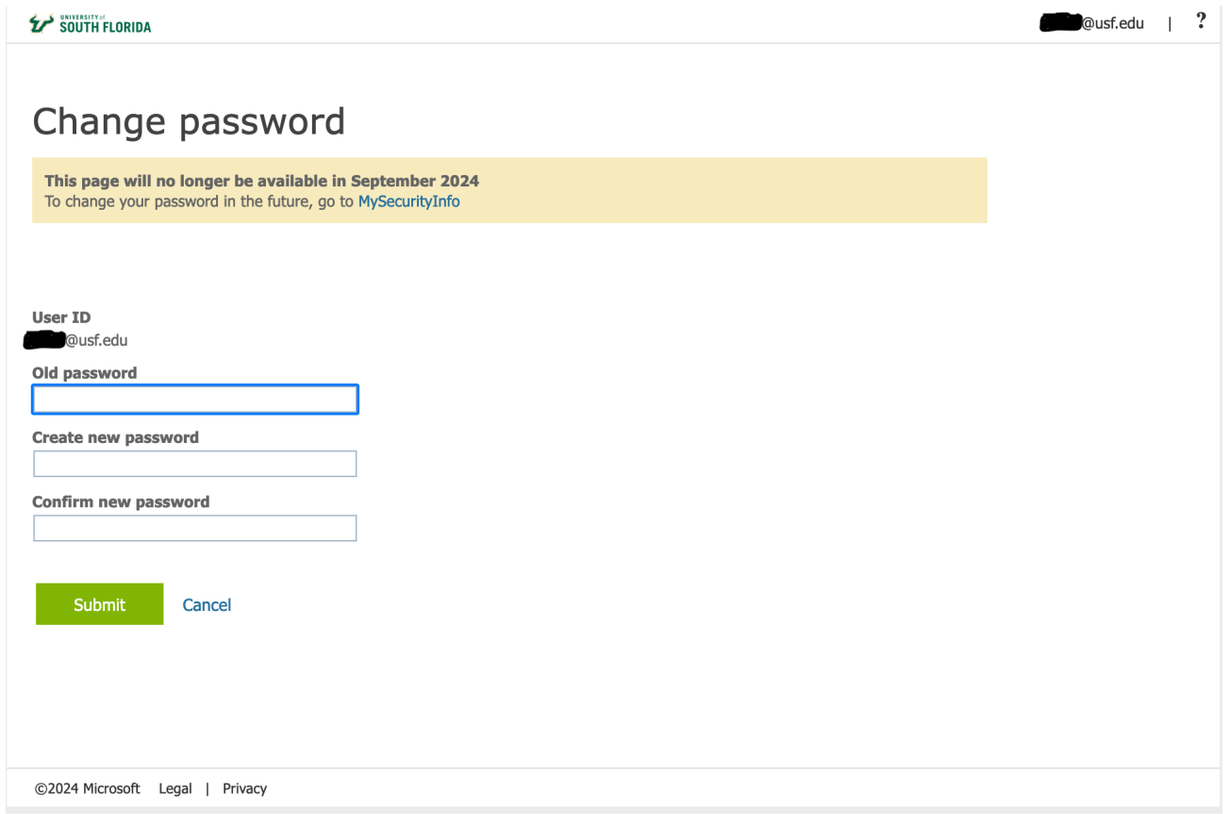
Functionality is *relatively easy* to measure, but…

Airplane works

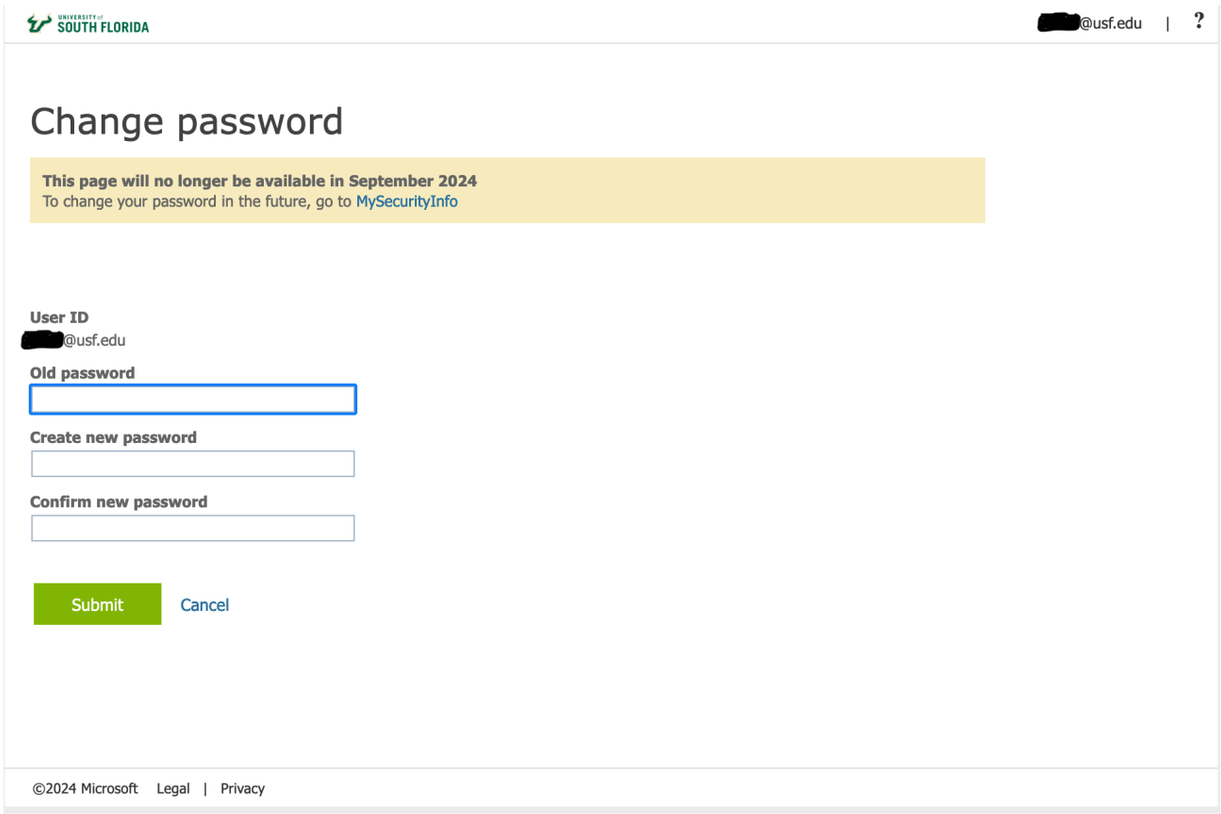
Airplane doesn't work

...*security* *is almost impossible to measure*

Web browser 0wned



Web browser not 0wned



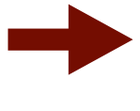
...*in IoT*

Device Vendors - Firmware, cloud infrastructure, data collection and handling

IoT Platforms (Google Home, Alexa, HomeAssistant)

3rd party developers - Android and iPhone apps

...*and automations*



Heating / Off

Recording / Off

nest

HomeKit

hue
PHILIPS

SmartThings

Some good news

Computer security is a growth area.

Awesome

About me

- **Research area:** Security and Privacy
- *Diverse domains and diverse techniques*….
  - IoT security and privacy, Web security and Privacy, Privacy policies and regulations
- ….*but a common theme*:
  - Understand the security and privacy risks in diverse consumer-oriented software systems
    - How does this affect the consumers?
  - Develop *practical* tools to automate the identification and prevention of the security and privacy problems

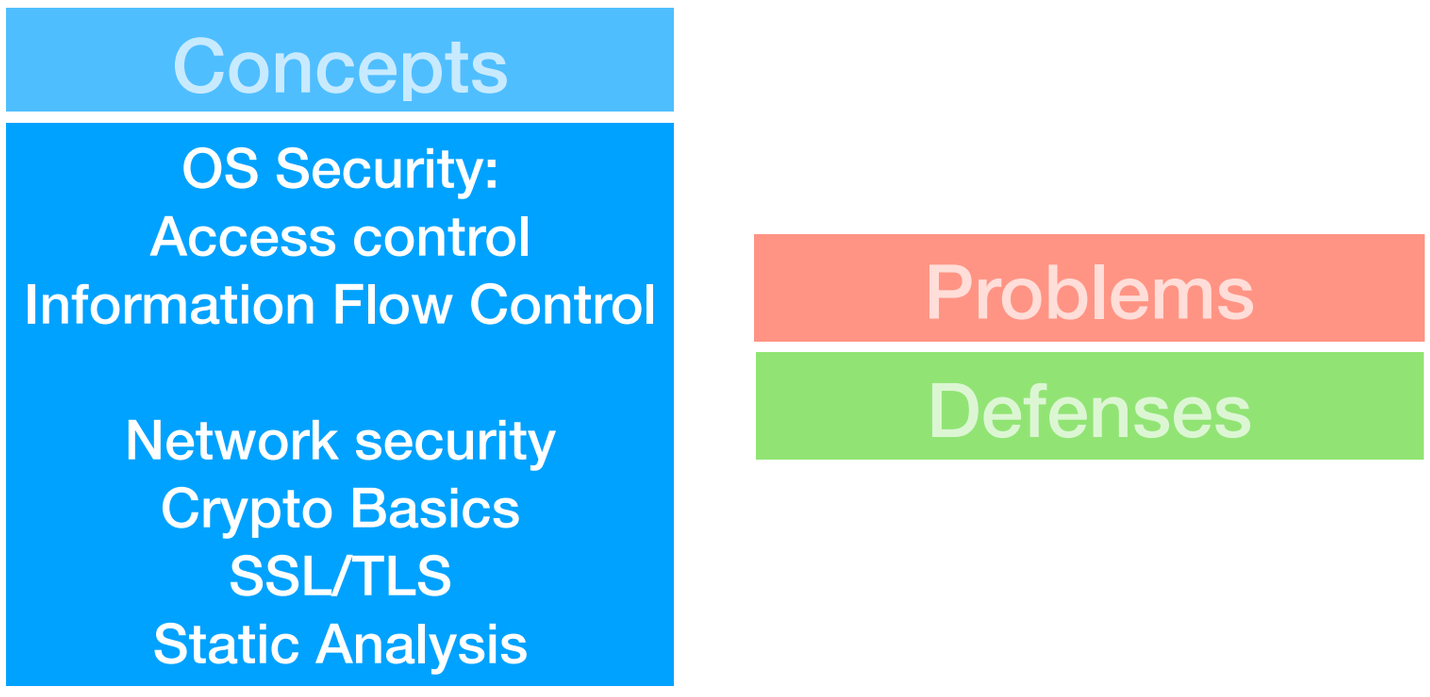
- **Contact:** kafle@usf.edu

- **Research papers and artifacts**: https://kaushalkafle.com

Back to the Course

Learning Goals

- **My Goal:** To provide you with the foundation to (1) *understand*, (2) *evaluate* and (3) *perform* research in IoT Software Security.



- **What to expect in class:**
  - Learn the fundamentals
  - Connect it to IoT security

- **Key Activities to ensure learning:** Readings, Participating in class AND PROJECTS!!

Prerequisites

- No hard prerequisites
- However…
  - Programming background is expected!
    - Scripting (Python, bash) for automating project tasks
    - **Basic knowledge of the following will come handy:** OS Design Principles
  - *Please do not hesitate to clarify even the smallest details*
    - Simple questions are often the most difficult to answer
- Heavy focus on learning fundamentals and real-world application

Course Policies & Expectations

Course Website

https://kaushalkafle.com/teaching/cis4930

- **Discussions:** Canvas
- **Submissions:** Canvas
- **Announcements**: Canvas

Office Hours

- **Time:** Tuesdays and Thursdays *before class* 11:00 am – 12:30 pm,
  - And also *by appointment*

Textbook

- No *required* textbook.
- We will rely on ***paper readings***
- For specific concepts, we will refer to the following (online) textbooks, as needed:
  - Security Engineering, Ross Anderson (Available online: http://www.cl.cam.ac.uk/~rja14/book.html
  - Operating System Security, Trent Jaeger (*Available online via* https://lib.usf.edu/

Course Components and Grading

- This is a *project-and-assignments driven* class (60% grade)

Research Project
40%

Final and Midterm Exams 30%

In-Class Participation 10%

Homework Assignments 20%

Readings “bug bounty” 10*% (bonus!)

***Changed from 5% in syllabus. I will update this in syllabus as well.**

- This will require in-class engagement + semester-long effort and interest!

Course Components

- We will stick to topics outlined in syllabus (except for unforeseen circumstances)
- **Pre-midterm:**
  - Crypto basics
  - Access control and Information Flow control
  - Foundation of IoT security in the smart home context
  - Project on smart home platform wrap-up
- **Post-midterm:**
  - Security analysis fundamentals
  - Research fundamentals
  - Network security topics
  - Project on app analysis wrap-up

Projects

- Projects will be the key aspect of learning in this class.
    - **Goal**: Learn research and collaboration
- It will be divided into 2 main sections:
- **Section 1**: Focus on understanding an IoT Platform (HomeAssistant)
    - Setup, create automations and integrations, interacting with its APIs, learning security primitives used by the platform
    - **End Result**: A functioning platform dashboard, automation scripts and
        - *3-5 page conference-style short paper*
        - Grade: For correct execution of scripts, overall *effort.*
- **Section 2:** Focus on the security analysis of real-world IoT apps
    - Static analysis of Android apps created for IoT platforms or devices
    - **End Result:** *3-5 page conference-style short paper of the security findings*
    - If you are already doing research and want to do something *related to your research?*: **talk to me ASAP**
    - Grade: For quality of *effort* and *research.*

Project Milestones

- 40% of course grade (100 points for project total)
    1. **Project Phase 1 (Idea and Team formation) - Due 09/05!**
        1. Chance for you to pitch in your ideas on what you want to do on HomeAssistant Platform.
            1. HomeAssistant intro in the next class
            2. Finalize your team members.
                1. Each team can have up to 4 members.
    2. **Project Phase 2 assigned (HomeAssistant Integration Design and Implementation)**
    3. **Project Phase 3 (IoT app analysis proposal)**
    4. **Project Phase 4 (Implementation and Evaluation)**
- All submissions (except artifacts) will be in LaTeX.

Readings Bug Bounty!

- Paper readings will provide you supplementary knowledge about the class topic.
  - Especially regarding how IoT research works in practice!
- *However….*
  - Reading research papers is hard work; reading >10 a semester is even harder!
  - You do not have to read all papers, but…..
  - Bonus Points!!
    - Report 2 bugs from the published papers assigned for readings in class
  - With caveats..

Rule 1: You must be the *first to report* the bug, *and report it any time of the semester before 11/28* (thanksgiving break)

Rule 2: It must be *non-trivial* (e.g., impractical assumption, logical flaw that affects the paper's claims)

Rule 3: You must be able to *explain it*

Homework Assignments

- **4 assignments total**
  - 10% + 3 * 30%
- **First homework assigned today!**
  - **Goal:** Learn writing in Latex while giving your introductions!
    - Detailed instructions will be in the assignment pdf
    - Available after the class ends
- *Policies….*
  - Ask questions if you need clarifications!
    - Office hours or Canvas
  - Emphasis on applying course materials

Cheating Policy

- Cheating is not allowed
- We run tools
- If you cheat, you will probably get caught
- If you get caught, you will get a *negative score* on th
ju

This includes the course project!

All text and figures should be your own.

- **I REFER ALL ACADEMIC DISHONESTY INCIDENTS TO THE OFFICE OF STUDENT CONDUCT, WITHOUT EXCEPTION**
- When in doubt, *ask*

Course Credo

Think like an attacker, but behave like a responsible adult

USF's computer usage policies apply to this class.

Security course != permission to disrupt or cause harm

Ethics Statement

- This course considers topics involving personal and public privacy and security. As part of this investigation we will cover technologies whose abuse may infringe on the rights of others. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class and or institution.

- When in doubt, please contact the instructor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from Professor Kafle.

Other Policies

- Please turn off cell phones during class.
- I will do my best to respond to emails within 24 hours. You will receive faster answers if you post to Canvas.
- Students may appeal to the instructor for reconsideration of a grade, but the appeal must be in writing (i.e., email), and must be sent within 3 weeks (or the close of the semester, whichever is sooner) of receiving the graded assignment.
- Behave civilly: **don't be late for class**; don't read newspapers/blogs/etc. during class; don't solve Sudoku puzzles during class; don't struggle with crossword puzzles during class; **respect others' opinions**, *even if they are wrong*.
- Adhere to good scientific principles and practices, and uphold the USF Student Code of Conduct <https://www.usf.edu/student-affairs/dean-of-students/policies/student-conduct-policies.aspx>

Lecture Notes

- **First things first:**
    1. **Student introductions due before next class**
        1. 1-2 sentences will suffice
        2. Help to recruit team members
        2. Homework 1 is assigned after class
        3. Project's first milestone:
            1. Identify teammates, and
            2. Send in project ideas tailored to "smart home platforms and automations"
- Slides will be released on the course schedule after each class.

Good Luck!