CIS 6930:
IoT Security

Prof. Kaushal Kafle

Lecture 1: Introduction

Lets break it down

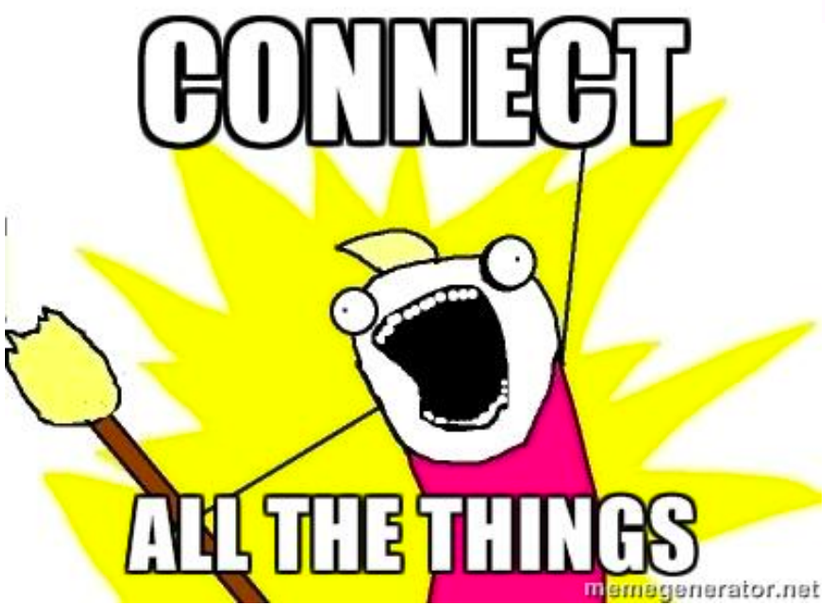
- *Internet* of *Things* (IoT) *Security*

- *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…

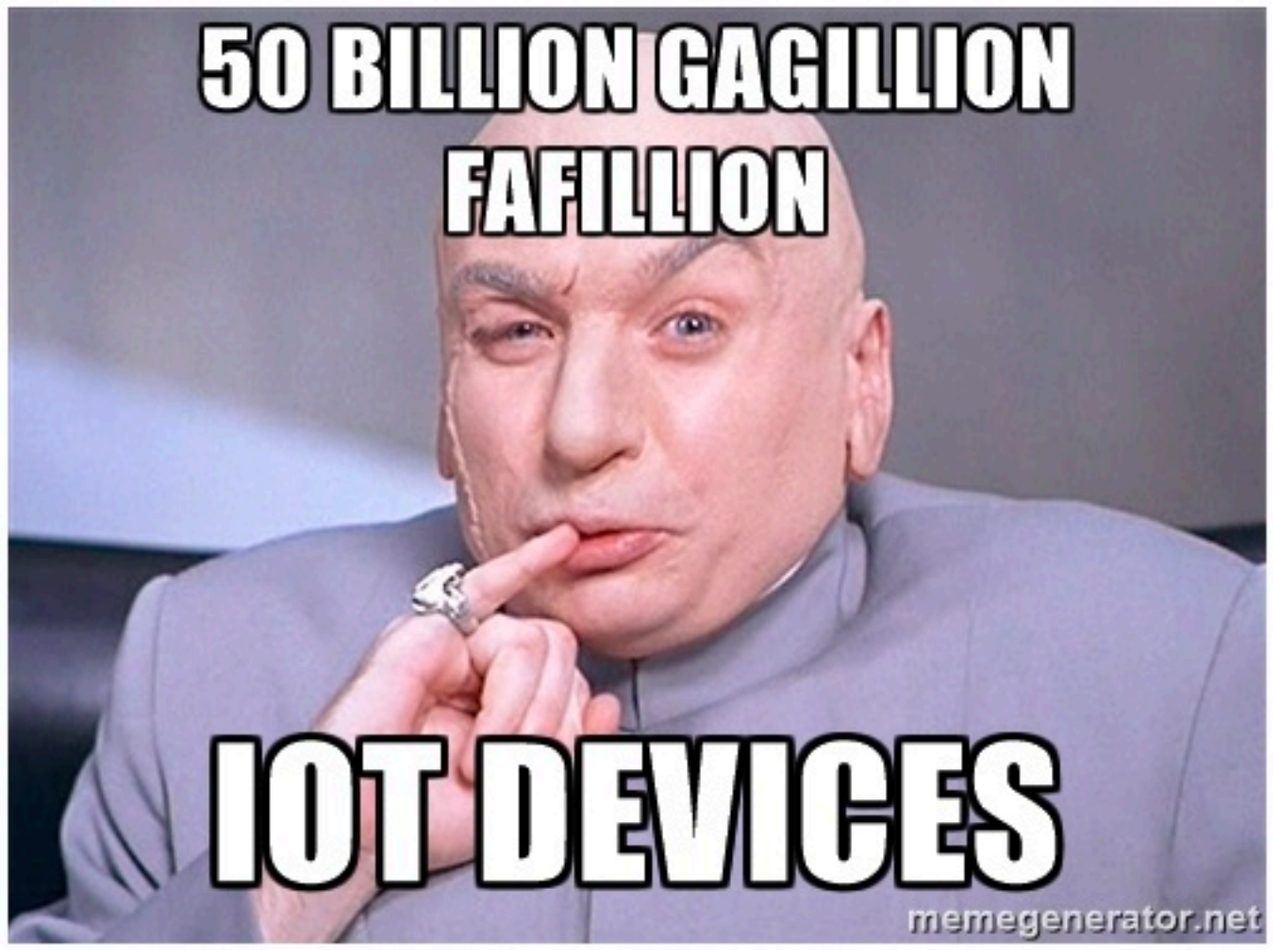
Have you used any of these ‘smart’ things?

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 —

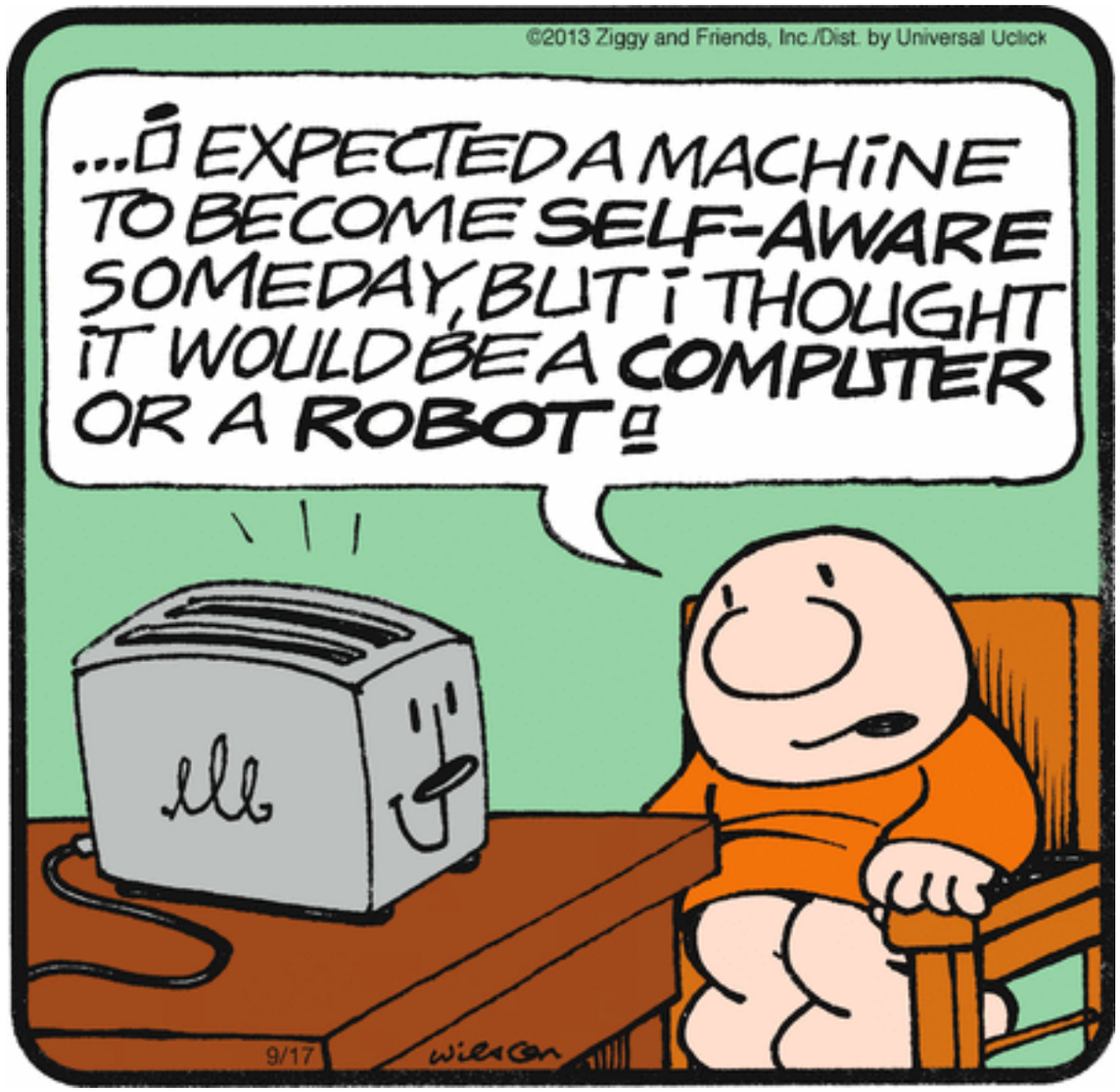
Cameras, door locks cost $$$

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

Things are…

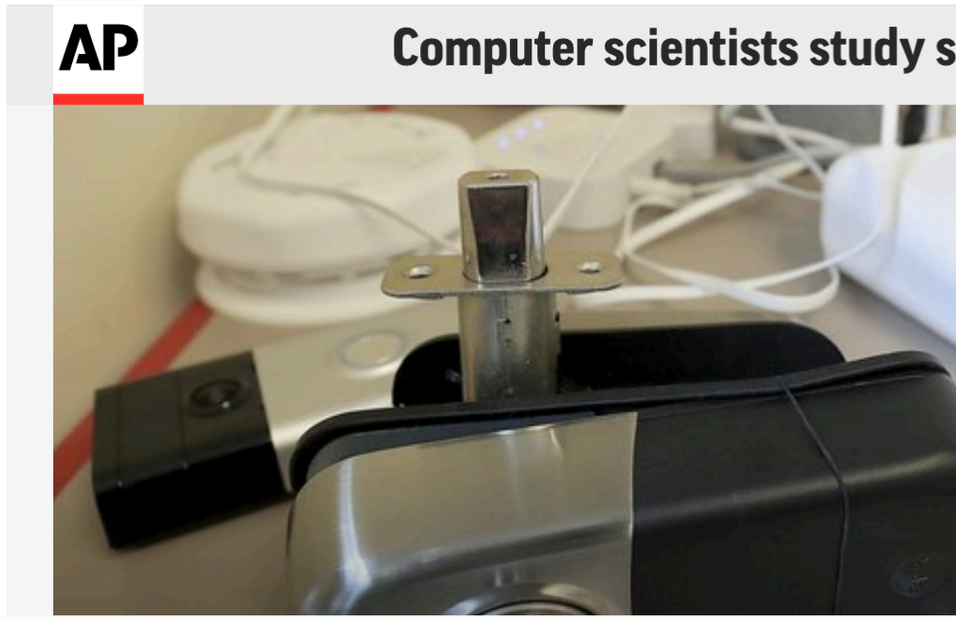
Physical —

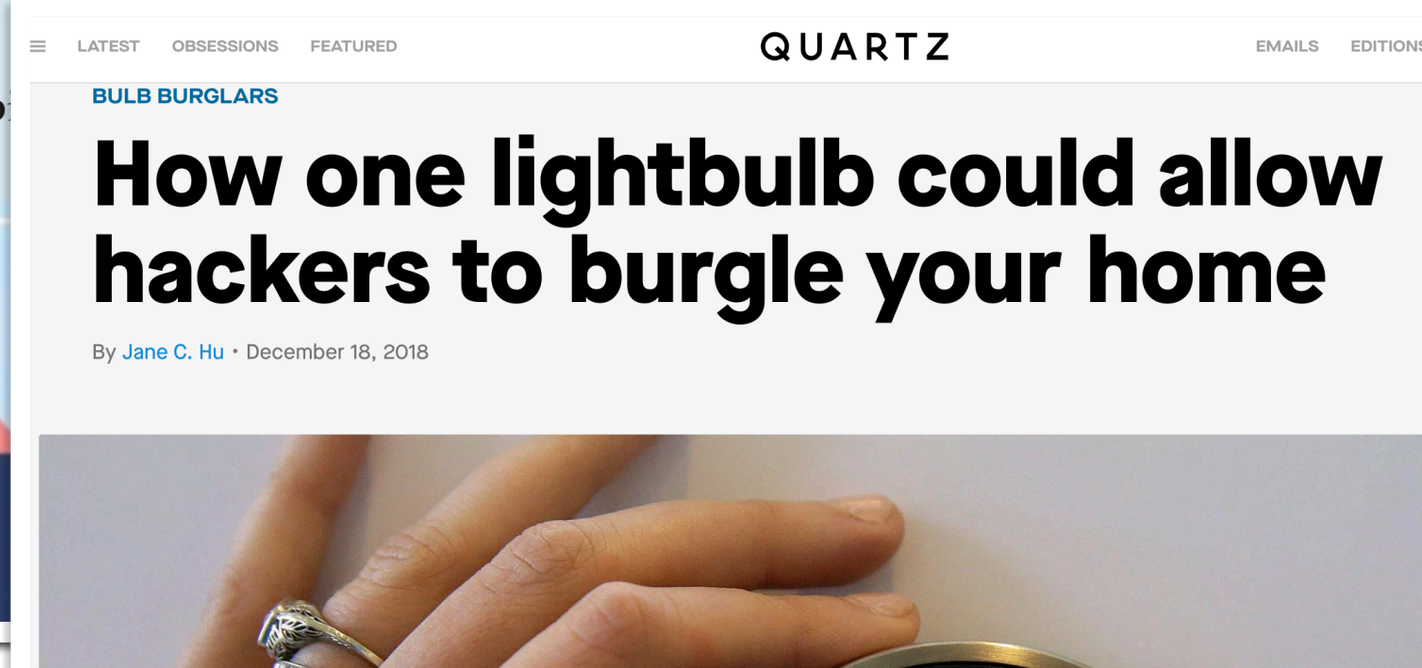
Can view, listen to, and modify our physical spaces.



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

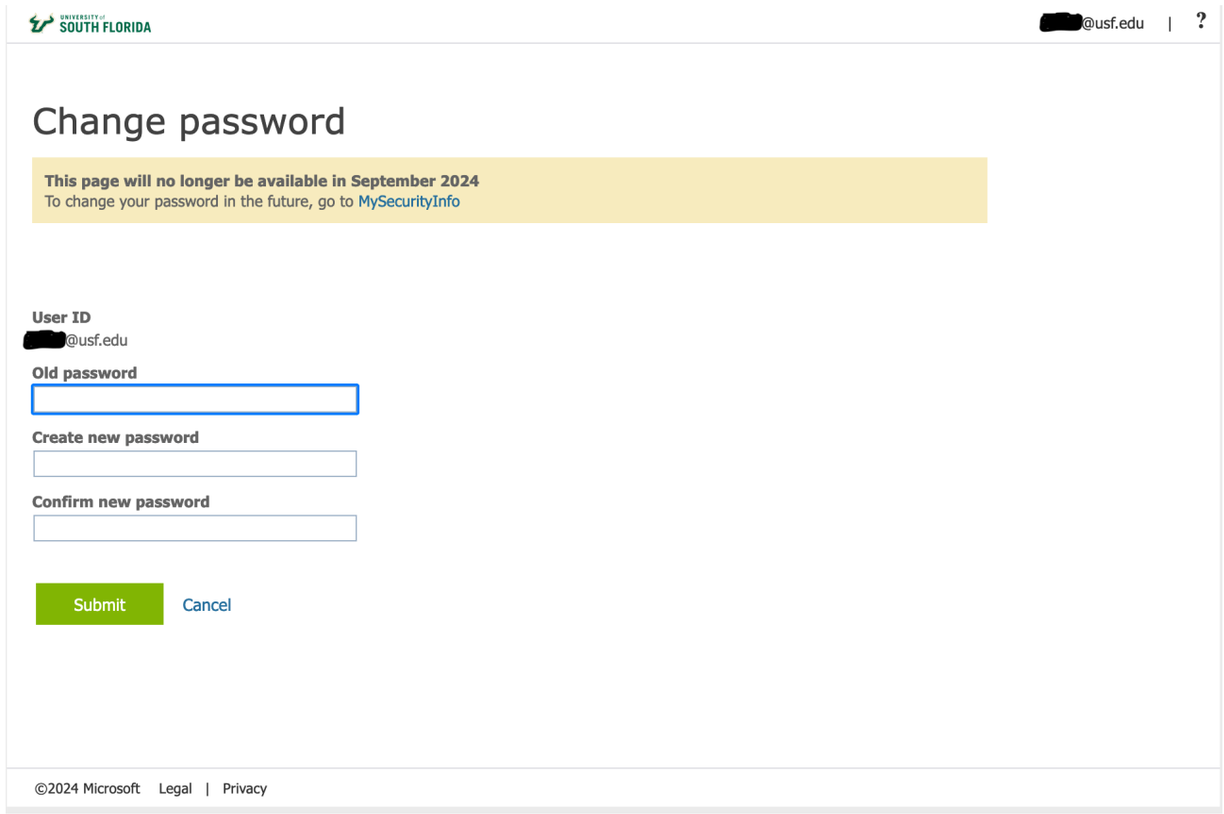
Functionality is *relatively easy* to measure, but…

TV works..

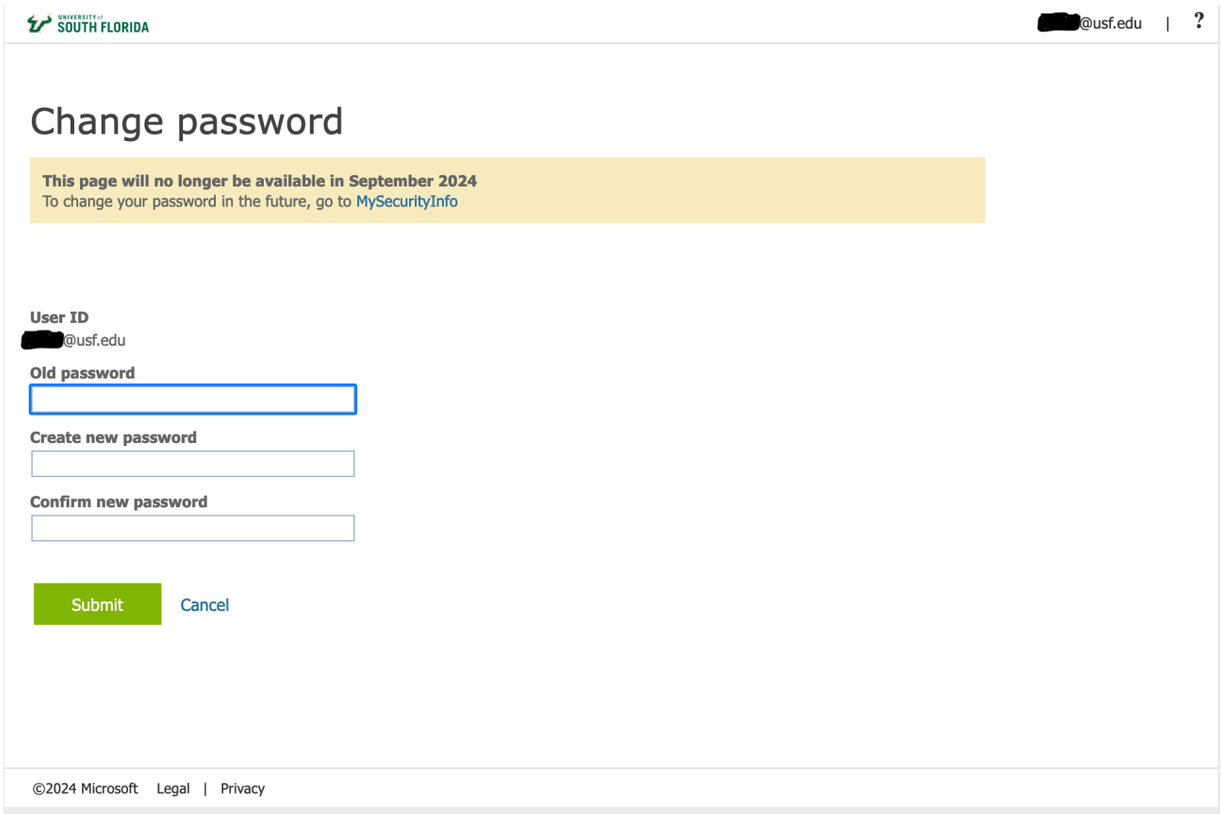
TV doesn’t work..

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

Web browser 0wned



Web browser not 0wned



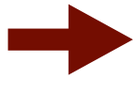
...*in IoT*

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

About you..

- Introduce yourself!
  - **Post your introduction in canvas -> this is your attendance for today!**

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.

Concepts

OS Security:
Access control
Information Flow Control

Network security
Crypto Basics
SSL/TLS
Static Analysis

Problems

Defenses

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 existing literature in IoT security.
        - **Paper readings and reviews**
    - Paper Presentations
    - Participate in class discussions
        - Research area,
        - Efficacy of the methodology,
        - Limitations of the approach
- **Key Activities to ensure learning:** Readings, class discussions AND PROJECTS!!

Prerequisites

- No hard prerequisites
- However…
  - Programming background is expected!
  - **Good knowledge of the following will come handy:**
    - OS Design Principles
    - Network fundamentals
- *Please do not hesitate to ask questions!*
  - Clarify even the smallest details; *better to ask than having to redo*!
  - Simple questions are often the most difficult to answer.

Course Policies & Expectations

Course Website

https://kaushalkafle.com/teaching/cis6930

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

Office Hours

<Time changed due to a conflict. Will be updated in the syllabus.>

- Thursdays 10:30 am – 12:30 pm, 2 pm - 3 pm
- Also *by appointment*

Textbook

- No *required* textbook.
- We will rely on ***paper readings***
- For specific concepts, you can 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-readings driven* class.
  - Paper readings are vital for success in this class.

Research Project
45%

Paper Presentation
20%

Paper reviews
10%

Class Participation and Discussion 15%

Readings “bug bounty”
10%

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

Course Components

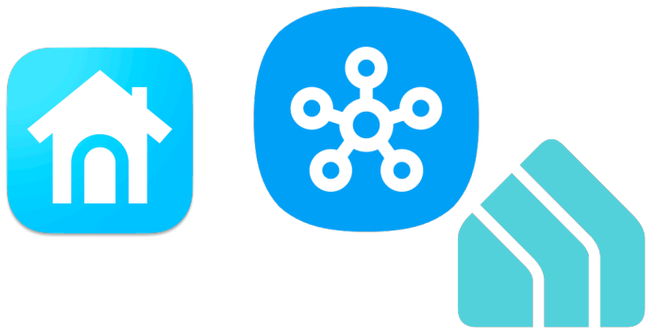
- We will stick to topics outlined in syllabus (except for unforeseen circumstances)

- **1st half:**

  - IoT platform analysis

  - IoT apps security analysis

    - Focus on access control, api misuses, data leaks



- **2nd half:**

  - Trigger-action specific security issues

  - Voice assistants

  - Privacy challenges

Paper Presentation

Research Project
45%

Paper Presentation
20%

Paper reviews
10%

Class Participation and Discussion 15%

Readings “bug bounty”
10%

Research Project

- Projects will be the key aspect of learning in this class.
  - **Goal**: Learn research and collaboration
- **Details are in the syllabus (section XII)**
  - Divided into 5 milestones
  - 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)

- If you are already doing research and want to do something *related to your research?* > **talk to me ASAP**

Project Milestones

- **Milestone 1: Project Proposal** (due 02/07)
  - Create a project team -> 1-3 members per team
  - Settle on a project idea.
    - Choose from any area of IoT security
      - For ideas: Browse last several years of Usenix, IEEE S&P, ACM CCS, NDSS, ACSAC proceedings
      - Focus on novelty, scope and practicality of the idea.
    - The grade for this milestone will depend on the team's ability to decide on at least one *good* project idea.
    - Each team will meet with me to finalize the project idea they will work on.

We will discuss other milestones in detail when they are assigned.

Paper Presentation

Research Project
45%

Paper Presentation
20%

Paper reviews
10%

Class Participation and Discussion 15%

Readings “bug bounty”
10%

Paper Presentation

- **Each week's class will have 1-2 student presentation(s)!**
  - This is a key skill you will learn as a graduate student.
  - Focus will be on explaining the main idea of the paper being discussed.
    - Problem Motivation and Challenges
    - Overview and system components
    - Methodology
    - Results and interesting findings
    - Discussion/pros-cons/Limitations

- The student presenting will finish with (at least) 3 questions for the class-at-large to discuss about the paper/area.

Presentations will be done in alphabetical order.

Class Participation/Discussion

Research Project
45%

Paper Presentation
20%

Paper reviews
10%

Class Participation and Discussion 15%

Readings “bug bounty”
10%

Class Participation/Discussion

- **The presentation finishes with a list of questions to discuss.**
  - To do well in this course, you must take active and regular part in the discussion.
    - The ability to debate about the research ideas being presented is very important.
      - This also demonstrates your comprehension of the course topics and readings.
- **You are required to do your readings for the class.** Your readings will help you gain the necessary background to participate in the class discussion.
- I will help steer the conversation + monitor the discussion.

Paper Reviews

Research Project
45%

Paper Presentation
20%

Paper reviews
10%

Class Participation and Discussion 15%

Readings “bug bounty”
10%

Paper Reviews

- **Before each week's class: submit 1 paper review in canvas.**
  - Student(s) presenting will not have to submit the review.
  - If 2 reviews are assigned in any week, you only need to do 1 of them.
- This will be a conference-style review.
  - You will be provided a review template.
  - Some key things to include in the review are:
    - A short summary of what the paper is about.
    - List of strengths and weaknesses
    - Detailed justification of why you think a particular point is a strength or a weakness.
      - That is, why do you think a particular aspect of the paper is a weakness in the context of the claims the paper is making?

Readings Bug Bounty

Research Project
45%

Paper Presentation
20%

Paper reviews
10%

Class Participation and Discussion 15%

Readings “bug bounty”
10%

Readings Bug Bounty

- Paper readings will provide you the necessary background about every class topic.
- *However….*
  - Reading research papers is hard work; reading >10 a semester is even harder!
  - So, on top of review points, reading of papers more critically will be rewarded via bug bounty!
    - **Report 2 bugs from the papers assigned for readings in class**
- Following rules will be applied to assess the validity of bugs..

  Rule 1: You must be the *first to report* the bug, *and report it any time of the semester before 04/26* (before final presentations)

  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*

Class Policies

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

- Read the syllabus carefully for additional information about this course.
- 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>

Good Luck!