

Tandon School of Engineering of New York University
Department of Electrical & Computer Engineering
CUSP-GX 8011 Special Topics:

“Internet-of-Things Security and Privacy: A Data-Driven Perspective”
Spring, 2021

Lectures (remote - Zoom): Thursdays 2:00 – 4:30 PM (New York Time)

Course Description: Smart home IoT (Internet-of-Things) devices are gaining popularity in average consumer homes. These “smart” devices, such as cameras, plugs, TVs, dishwashers, etc, are also known to pose various security and privacy threats (e.g., your Alexa listening to you), but the opaque nature of these devices makes it difficult to discover security and privacy vulnerabilities.

This course introduces basic and advanced topics on Internet-of-Things (IoT) security and privacy from a data-driven perspective. It starts with preliminaries on networking and Internet security, followed by security research based on a data-driven approach. Every week, students will review and discuss peer-reviewed academic papers from multiple disciplines, ranging from computer science, psychology, and policy/law. Furthermore, students will engage in hands-on projects to independently investigate real-world security and privacy issues of IoT devices and/or propose solutions to fix these issues.

For details, visit the course website: <https://mlab.engineering.nyu.edu/classes/iot-2021-sp>

Prerequisites: Students for this class are expected to have networking knowledge, such as how TCP/IP works, how packets get forwarded, and how to run TcpDump. Otherwise, students are encouraged to take relevant online courses on these topics before the semester begins and to seek the instructor's approval.

Instructor: Professor Danny Y. Huang

- Email: dhuang@nyu.edu
- Homepage: <https://mlab.engineering.nyu.edu/>
- Office hours (remote!) by email appointment.

Textbook: No textbook. Lecture notes and reading materials will be posted on the class website.

Homework, Exam, and grading Policy: Paper presentations (20%). Class participation (10%). Weekly paper reviews (40%). Final project (30%).

Tentative Course Schedule

For details, visit <https://mlab.engineering.nyu.edu/classes/iot-2021-sp>.

Class 1: **Introduction:** Why security and privacy of IoT matters. Provides a high-level overview of different IoT security and privacy issues. Introduces students to reading and reviewing scientific papers. No paper reading.

Class 2: **Intro to network security.** Helps students revisit knowledge learned in their networking classes. Builds connections between networking and security. Discusses final project plans.

Class 3: **Internet scanning and network measurement.** Introduces data-driven methods, such as scanning, to empirically measure security and privacy of real-world devices (including IoT).

Class 4: **Botnets, malware, and denial of service attacks.** Discusses well-known security vulnerabilities of (IoT) devices and their threats to the Internet.

Class 5: **Web and app privacy.** Discusses privacy issues on the web and an Android app, for example, how users can be tracked across websites and/or apps. Briefly introduces their connection to IoT.

Class 6: **Overview of IoT security and privacy.** Provides a high-level overview of IoT security and privacy issues. Discusses challenges specific to IoT that are absent in more traditional security and privacy problems.

Class 7: **Security of connected homes.** Discusses security threats among different types of smart home devices commonly found in the market.

Class 8: **Smart TV security and privacy.** Discusses security and privacy issues on popular smart TV platforms (such as Roku TV and Amazon Fire TV) and ways to protect consumers.

Class 9: **Voice assistant privacy.** Discusses privacy issues on voice assistants (such as Amazon Alexa and Google Home Assistant) and ways to protect consumers.

Class 10: **Human factors of IoT security.** Discusses how humans form the weakness link in security, and how to educate users toward better security.

Class 11: **Children's privacy on IoT devices.** Discusses how IoT devices track children's online behaviors. Introduces COPPA (Children's Online Privacy Protection Act).

Class 12: **Privacy policies.** Discusses different privacy policies (e.g., how data is collected) on various IoT devices.

Class 13: Final project presentation: Part 1

Class 14: Final project presentation: Part 2