Computer Security Capstone

Term Project: Exploring Vulnerabilities in IoT Devices

Chi-Yu Li (2021 Spring)
Computer Science Department
National Yang Ming Chiao Tung University

Goal

- To practically explore vulnerabilities in IoT devices

- You will learn how to
  - examine vulnerabilities of an IoT device from scratch
  - check insecurity of IoT communication
  - apply ARP spoofing and MITM attacks to real IoT devices
  - exploit vulnerabilities to launch an attack

How to Proceed?

- You are allowed to team up. Each team has at most 2 students
- You need to choose an IoT device from a given list in Google sheet
  - Mark it with your student ID(s): first come, first served
  - The link of the Google sheet will be sent out by this Friday (5/14)
  - Pick up the IoT device in the given time slots (5/20 – 5/26)
- You can use any tools or methods to explore vulnerabilities and launch attacks on your chosen IoT device
- Total bonus on your Final Score: 5 points

IoT Device List

- Voice Assistant
  - Amazon Echo, Google Nest Mini, etc.
- Smart Camera
  - D-Link DCS-8526LH, TP-Link Tapo C210, Beseye Pure, SpotCam Pano, etc.
- Smart Video Doorbell
  - 360 Video Doorbell, KINGNET Doorbell, etc.
- Smart Socket
  - TP-Link HS105, SecuFirst CHC-OA1S, D-Link DSP-W118, etc.

Two Cases for IoT Communication Security

- Consider IoT communication between IoT device and server
  - Case I: Unprotected: packets sent in plaintext
  - Case II: Protected: e.g., with TLS connection

- Attack model (assumptions)
  - You are not able to control the Wi-Fi AP to which the target IoT device connects
  - One of your devices is allowed to connect the same Wi-Fi AP

Case I: Unprotected IoT Communication (3 points)

- Please do the following tasks for IoT devices in this case
  - Task 1: Show that IoT communication is not protected
  - Task 2: Launch an MITM attack to control the IoT device
    - Control the IoT device: any small action can be performed on it
    - e.g., smart socket: power on/off, smart video doorbell: false ring
- Please explain how you get it done and show your experimental evidence for the results

Case II: Protected IoT Communication (2.5 points)

- Please do the following tasks for IoT devices in this case
  - Task 1: Show how IoT communication is protected
  - Task 2: Launch an MITM attack and examine whether it can work for the IoT device. Why yes or why no?
- Please explain how you get it done and show your experimental evidence for the results

More Vulnerabilities (2.5 points)

- Please feel free to discover more vulnerabilities from your IoT device
  - e.g., backdoor and weak default authentication
- The grade points will be given based on what you have found

Project Submission

- Due date: 6/21 11:55pm

- Submission rules
  - The report must be written in English with font size 11 or 12 in Times New Roman. It must be submitted in one PDF file with a name “report.pdf.”

- Note: for each result you claim to have, please provide its experimental evidence; otherwise, it may not be considered

Questions?