

# **CIS 700/002 : Special Topics : Security of Embedded Systems, Cyber-Physical Systems, and Internet-of-Things**

Insup Lee and James Weimer

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science

School of Engineering and Applied Science

University of Pennsylvania

*April 14, 2017*

# Today's Class (last class)

- Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System
  - Yicheng
- Ghost in the PLC: Designing an Undetectable Programmable Logic Controller Rootkit via Pin Control Attack
  - Omkar

# Final Project

- Use tools and insight to assess the security of a commercial device
  - What information is made available?
  - How could this information be exploited?
    - think beyond the obvious – take the extra step!
  - How can these vulnerabilities be patched?
- If you want to meet, email Jim/Insup
  - **out of town: 4/18 – 4/21 (CPS week)**

# Final Project Deliverables

- **Written report**
  - **Email to Jim and Insup by Friday May 05, 2017 at 5 pm**
  - document your assessment/findings for your device
  - assessment should include (minimally) the following:
    - the device / system
    - What was tested (how did you try to get into the device)
    - What you found (Was it secure? Did you get in?)
    - Recommendations for improving security
  - No max page length / minimum
    - use as much space as needed to report your findings
- **Oral presentation (Final project demos):**
  - **Wednesday, May 03, 2017 from 12:00 - 02:00 in TOWN 307**
  - 10 minute presentation (15 minutes for groups) – strictly enforced!
  - present the interesting findings
    - focus on what you were able to successfully achieve
    - should complement the written report