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

March 3, 2017

Penn Engineering

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

Today's Class

- Second week of tool demos (begin the hands on portion).

- Aircrack-ng / fern / reaver
  - Dagaen

- Metasploit / armitage
  - presenter: Junkil

- **Break**

- OWSAP Zed
  - presenter: Hitali

- Nikito2
  - presenter: Swathi

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?
  - How can these vulnerabilities be patched.

- Potential devices:
  - Owlet baby monitor
  - Constant glucometer
  - Smart home automation devices
  - "dealer's choice": (almost) any EMBS/CPS/IoT device

- In 2 weeks devices will be assigned (March 17th)
  - Description on course website (under projects)
  - April 7th: Mid-term
  - April 28th : Final Demo

In 2 Weeks

- Next week is spring break – NO CLASS
- More tool demos:

- SQLmap
  - Hung

- Social engineer toolkit
  - Thejas
  - Nikheel

- Maltego
  - Sangdon