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

January 27, 2017

Today's Class

- Assign next week's homework/reading
- Industrial Control Systems (ICS) incidents (finish)
  - Dagaen Golomb
- Attack Steps (Chapter 5): Thejas
- **Break**
- Protections/Secure Design (Chapter 6): Nikheel
- "Physical-Cyber" Attacks (Chapter 7): Sangdon

Course Tools Demos

- *wireshark*
  - Swathi, Omkar, Bipeen
- *nmap / zenmap*
  - Teng
- *aircrack-ng / fern*
  - Dagaen, Hitali
- metasploit / armitage
  - Sangdon
- OWSAP Zed
  - Kamenee
- Nikto
  - ???
- Sqlmap
  - ???
- Social Engineer Toolkit
  - ???
- Maltego
  - ???

Who hasn't signed up?
Demo assignments will be posted this week

Assignments

- Reading / Presentations
  - *A survey on wireless Security: Technical Challenges, Recent Advances, and Future Trends. Zou et al., Proceedings of IEEE, May 2016.*
    - *presenter: Konstantinos Gatis*
  - Practical attacks against WEP and WPA. M. Beck and E. Tews, Aircrack-ng, 2008.
    - presenter: Dagaen Golumb
  - Bluetooth: With Low Energy comes Low Security. M. Ryan, Workshop on Offensive Technologies, 2013.
    - presenter: Kamenee Arumugam
- Setup Kali Linux Box
  - See course webpage for links to different dual-boot configurations
    - Ensure you have WIFI monitoring capabilities
  - Any questions?