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 20, 2017

Course Updates

- Time/location change (obviously)
  - Friday: 9:30 am – noon, Towne 307
  - "break" around 10:50

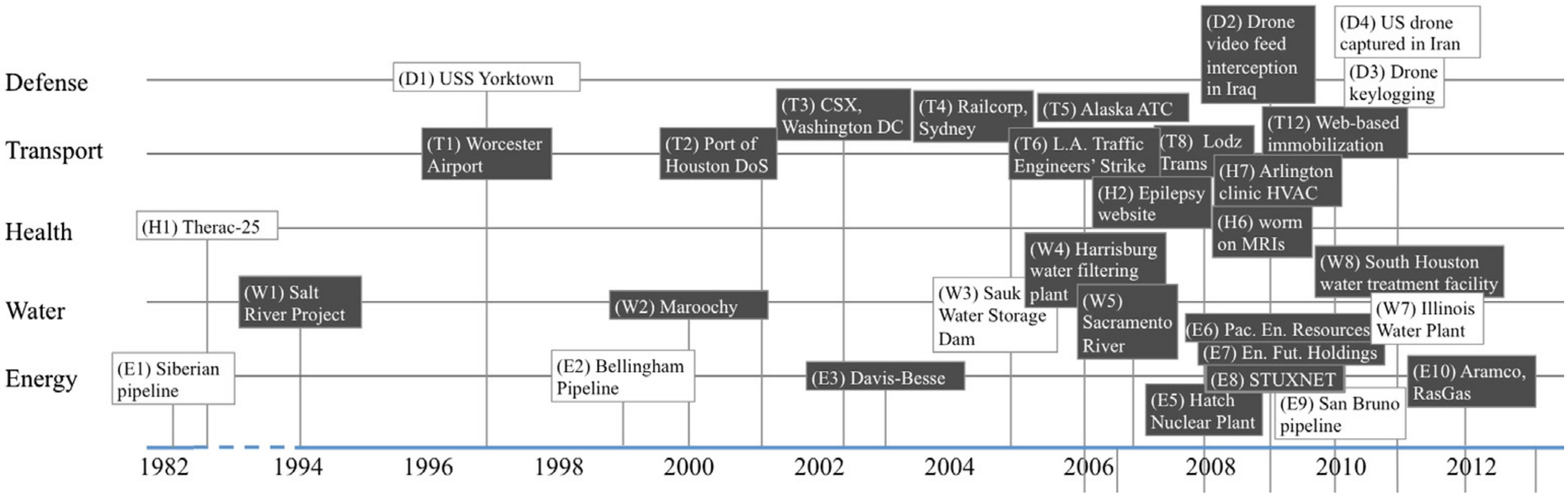
- Policy Update: If you are taking CIS 540, you can leave after the break
  - project/reading assignments will be made at the beginning of the break.
  - students are responsible for what is missed.

Today's Class

- ~~Course Logistics~~
- Review of EMBS/CPS/IoT security incidents
  - Medical security incidents
    - Radoslav Ivanov
  - Automotive security incidents
    - Bipeen Acharya
  - Industrial Control Systems (ICS) incidents
    - Dagaen Golomb
- Overview tools to be studied in course
- Assign next week's reading and presentors

EMBS/CPS/IoT Security Incidents

- last week we overviewed security incidents (at a high level)
  - this week we will go into some details.



- This course will focus on:
  - medical
    - health
  - automotive
    - transportation
  - Industrial Control Systems
    - energy/water/defense

Student Presentations

Course Tools

- Kali Linux
  - Did you setup your box yet?
- Tools (all available in Kali distro):
  - *wireshark*
    - www.wireshark.org
  - *nmap / zenmap*
    - https://nmap.org/
    - https://nmap.org/zenmap/
  - *aircrack-ng / fern*
    - https://www.aircrack-ng.org/
    - https://tuxdiary.com/2015/08/30/fern-wifi-cracker/
  - metasploit / armitage
    - https://www.metasploit.com/
    - http://www.fastandeasyhacking.com/
  - OWSAP Zed
    - https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
  - Nikto
    - http://sectools.org/tool/nikto/
  - Sqlmap
    - http://sqlmap.org/
  - Social Engineer Toolkit
    - https://www.trustedsec.com/social-engineer-toolkit/
  - Maltego
    - https://www.paterva.com/web7/

2 or 3 students for each tool (first come first serve).

- 1) learn the assigned tool
  - read manual, do tutorials, play around.
- 2) present and demo the tool in class
- 3) write 3 to 5 lab/homework problems
  - must require working with tool
  - should illustrate tool capabilities

Sign up on course website under "projects" page

Assignments

- Reading
  - *Cyber-Physical Attacks: A Growing Invisible Threat*. George Loukas, 2015.
    - Chapters 5, 6, 7

- Setup Kali Linux Box
  - review course tools and signup for your preference on course website
  - https://rtg.cis.upenn.edu/cis700-002/projects.html

- Presentations
  - Attack Steps (Chapter 5): Thejas
  - Protections/Secure Design (Chapter 6): Nikheel
  - "Physical-Cyber" Attacks (Chapter 7): Sangdon