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 13, 2017

Course Info

- Instructor: Insup Lee
- Co-Instructor: James Weimer

- Friday at 10:30am – 1:30pm, Town 321
  - No Class: 3/10, 4/21, 4/28

- Course website:
  - https://rtg.cis.upenn.edu/cis700-002

What can you expect?

- Course that extends the CPS security reading group
  - http://cis.upenn.edu/~sangdonp/cps-security-reading-group/
- “More than a reading group”
  - potential quizzes on readings (~ 3 papers a week)
  - hands on demos and tutorials (~ 1 a week)
  - assess the security of commercially available devices (final project)
- You will learn (and use) common security tools/techniques
  - tools will be listed on course website
- A typical class (3 hours):
  - 20 minute intro / overview (led Insup / Jim)
  - 3 x 45 minutes student presentations (plus a 5 minutes break)
  - 20 minute discussion (led by Insup/Jim)
- Lunch! (maybe).

What do we assume?

- No security experience / exposure.

- Prerequisites:
  - CIS 541 or working knowledge of embedded software and hardware systems.

- Computer running Kali Linux with (multiple) USB ports
  - https://www.kali.org/
  - industry standard
  - All additional hardware will be provided / loaned

Some security terminology

- **Vulnerability:** A flaw or weakness in a system's design, implementation, operation, or management that could be exploited to violate the system's confidentiality, integrity, or availability

- **Threat:** Any circumstance or event with the potential to exploit a vulnerability and adversely affect a system through unauthorized access, destruction, disclosure, or modification of data, denial-of-service, etc.

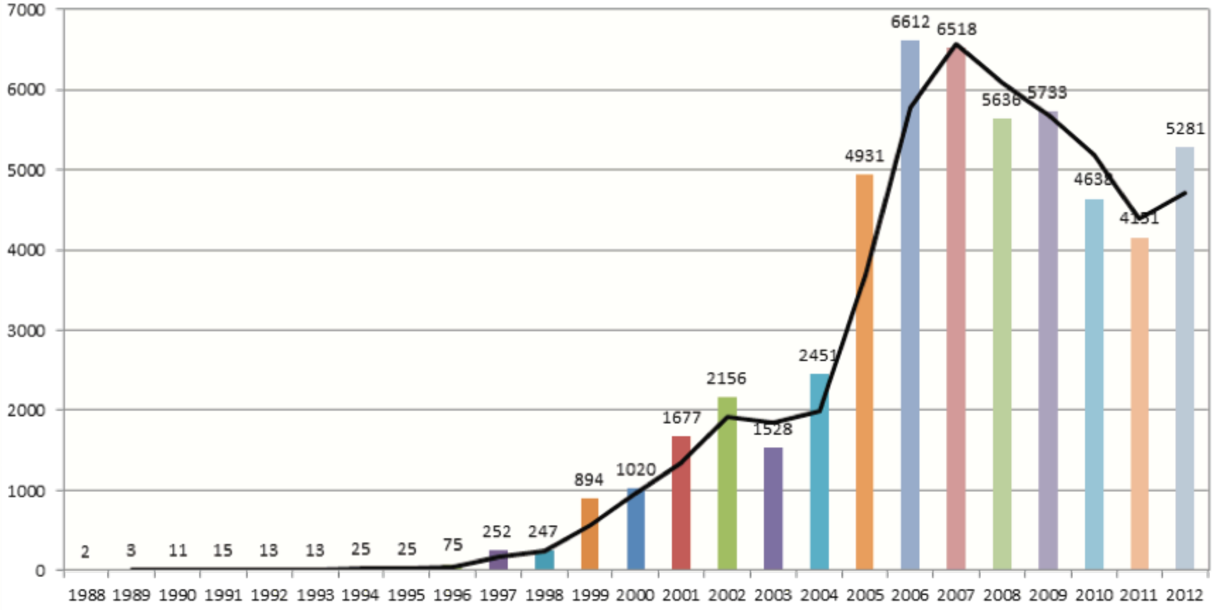
- **Attack:** An intentional assault on system security that derives from an intelligent threat.
  - **Active attacks** attempt to alter system resources or affect their operation
  - **Passive attacks** attempt to learn or make use of information from a system but does not affect that system.

- **Adversary**: An entity that attacks a system or is a threat to a system.
  - synonyms: intruder, attacker, cyber attacker, cracker, hacker, etc.

- **Countermeasure:** An action, device, procedure, or technique that meets or opposes (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

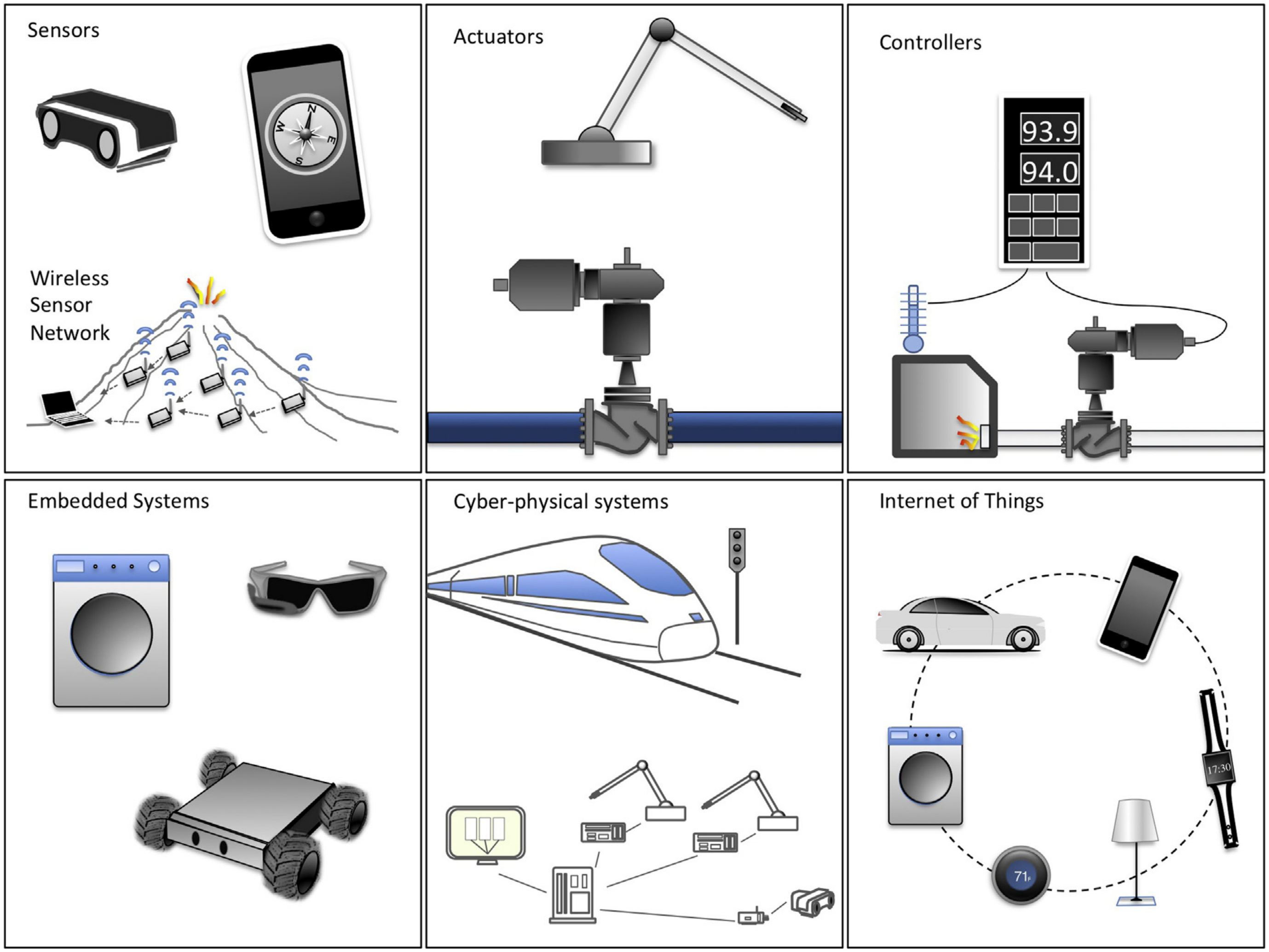
How big is the “security” problem

- $350 Billion annually (2012)
  - http://www.securitymagazine.com/articles/84623-security-industry-market-worth-350-billion-study
- Common Vulnerabilities and Exposures
  - https://cve.mitre.org/about/faqs.html
  - e.g., Heartbleed, Shellshock, Stuxnet



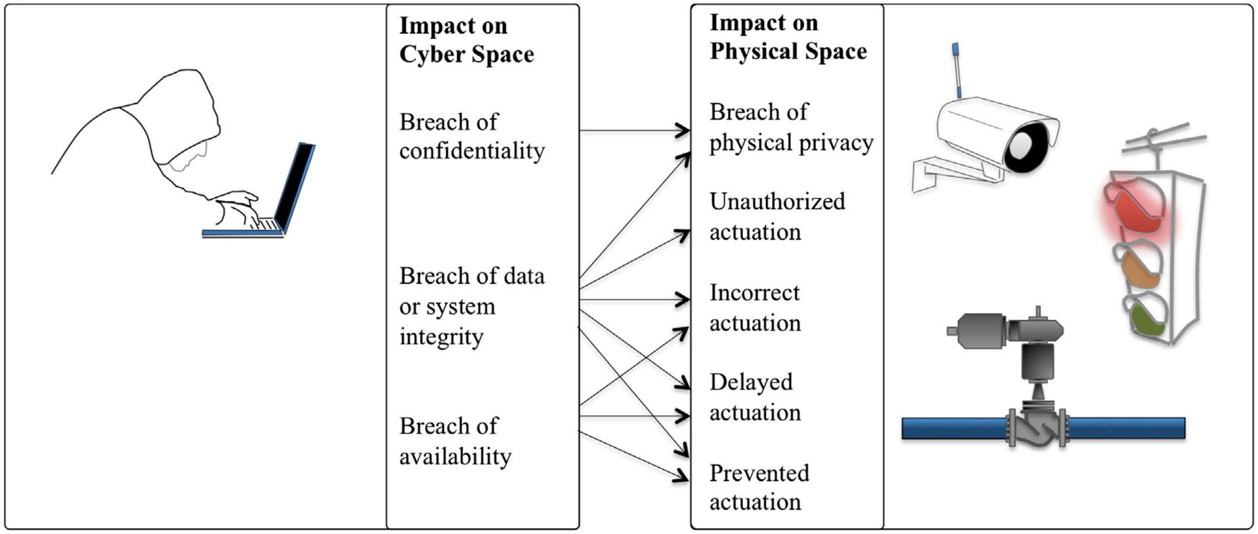
25-years of vulnerabilities, 1988-2012. Yves Younan.

Why EMBS/CPS/IoT security?



cyber-physical attacks: a growing invisible threat: George Loukas, 2015.

Impact on EMBS/CPS/IoT performance



Impact on Cyber Space

Breach of confidentiality

Breach of data or system integrity

Breach of availability

Impact on Physical Space

Breach of physical privacy

Unauthorized actuation

Incorrect actuation

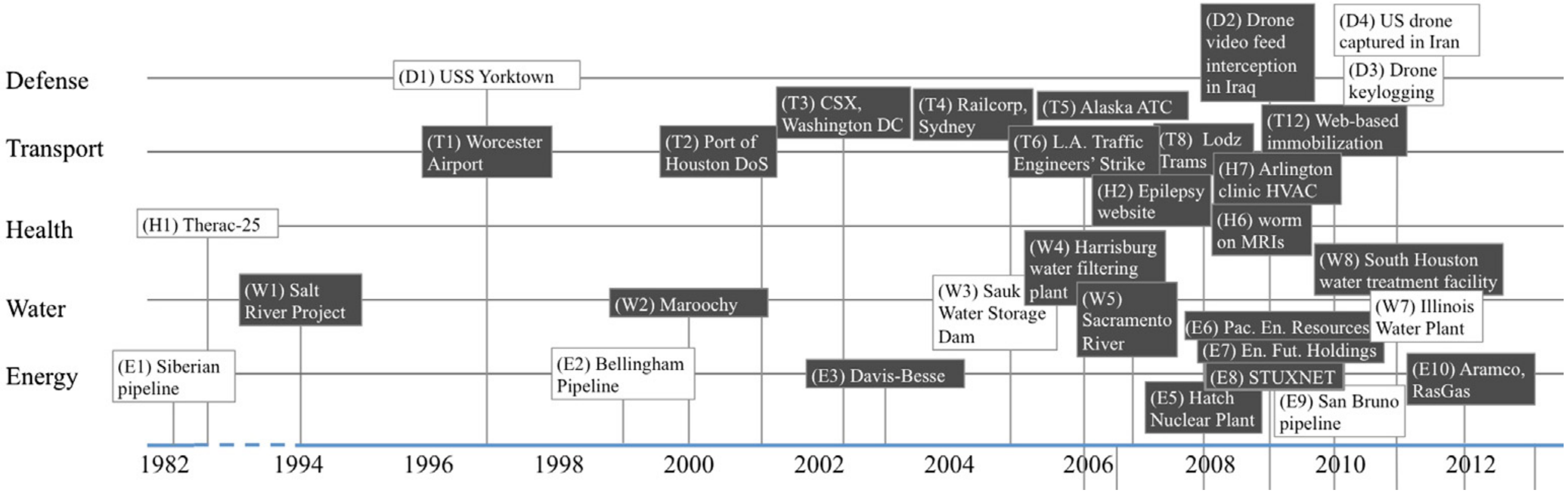
Delayed actuation

Prevented actuation

- Taxonomy of system impact
  - Unauthorized actuation
  - Incorrect actuation
  - Delayed actuation
  - Prevented actuation

cyber-physical attacks: a growing invisible threat: George Loukas, 2015.

EMBS/CPS/IoT security incidents



Defense

Transport

Health

Water

Energy

(D1) USS Yorktown

(D2) Drone video feed interception in Iraq

(D3) Drone keylogging

(D4) US drone captured in Iran

(T1) Worcester Airport

(T2) Port of Houston DoS

(T3) CSX, Washington DC

(T4) Railcorp, Sydney

(T5) Alaska ATC

(T6) L.A. Traffic Engineers' Strike

(T8) Lodz Trams

(T12) Web-based immobilization

(H1) Therac-25

(H2) Epilepsy website

(H6) worm on MRIs

(H7) Arlington clinic HVAC

(W1) Salt River Project

(W2) Maroochy

(W3) Sauk Water Storage Dam

(W4) Harrisburg water filtering plant

(W5) Sacramento River

(W7) Illinois Water Plant

(W8) South Houston water treatment facility

(E1) Siberian pipeline

(E2) Bellingham Pipeline

(E3) Davis-Besse

(E5) Hatch Nuclear Plant

(E6) Pac. En. Resources

(E7) En. Fut. Holdings

(E8) STUXNET

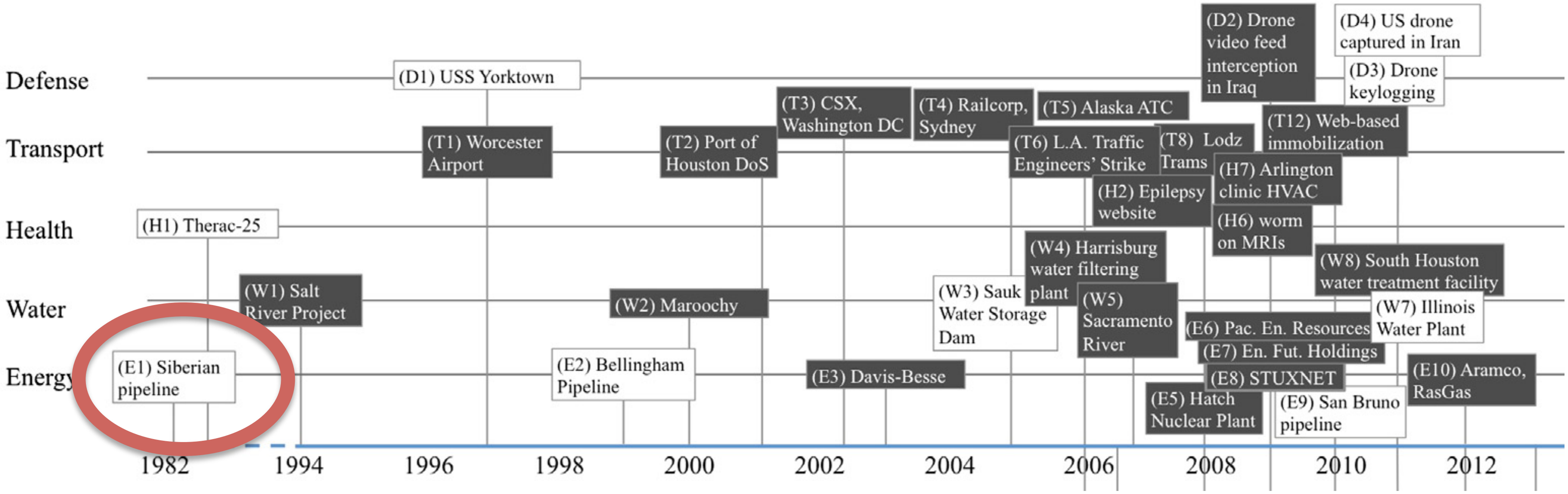
(E9) San Bruno pipeline

(E10) Aramco, RasGas

1982 1994 1996 1998 2000 2002 2004 2006 2008 2010 2012

cyber-physical attacks: a growing invisible threat: George Loukas, 2015.

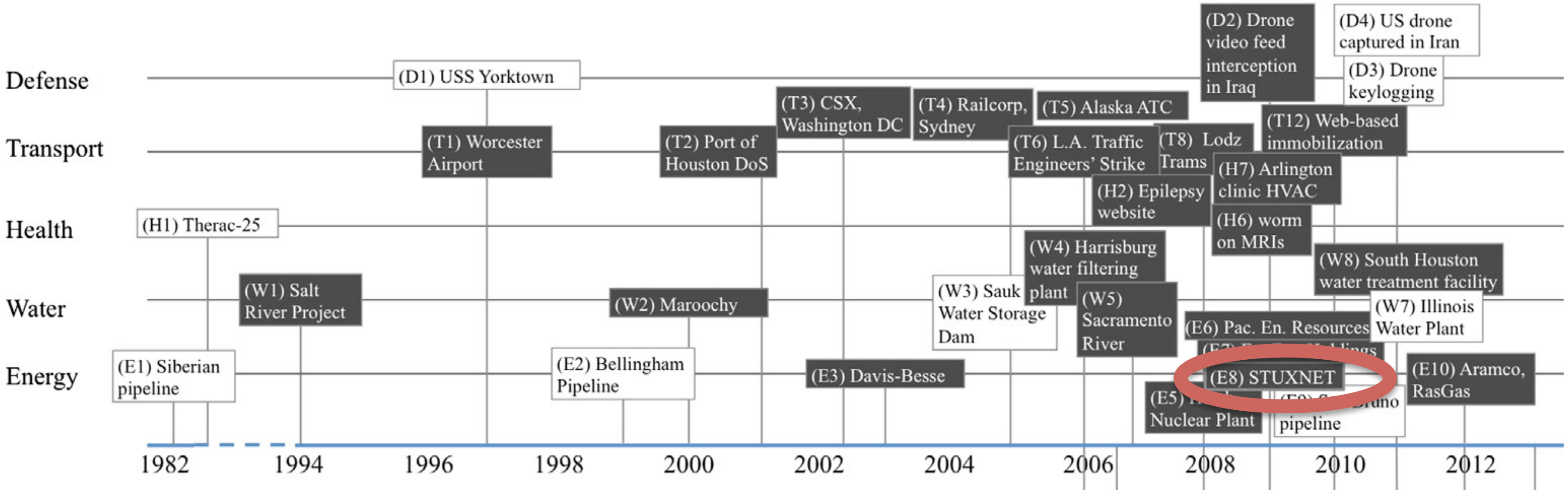
EMBS/CPS/IoT security incidents



- Siberian pipeline: June 1982: (controversial)
  - *Allegedly* Soviets stole control software from a Canadian company.
  - *Allegedly* US influenced Canadian company to alter code such that pipeline pressures would build up.
  - explosion could be seen from space.

cyber-physical attacks: a growing invisible threat: George Loukas, 2015.

EMBS/CPS/IoT security incidents

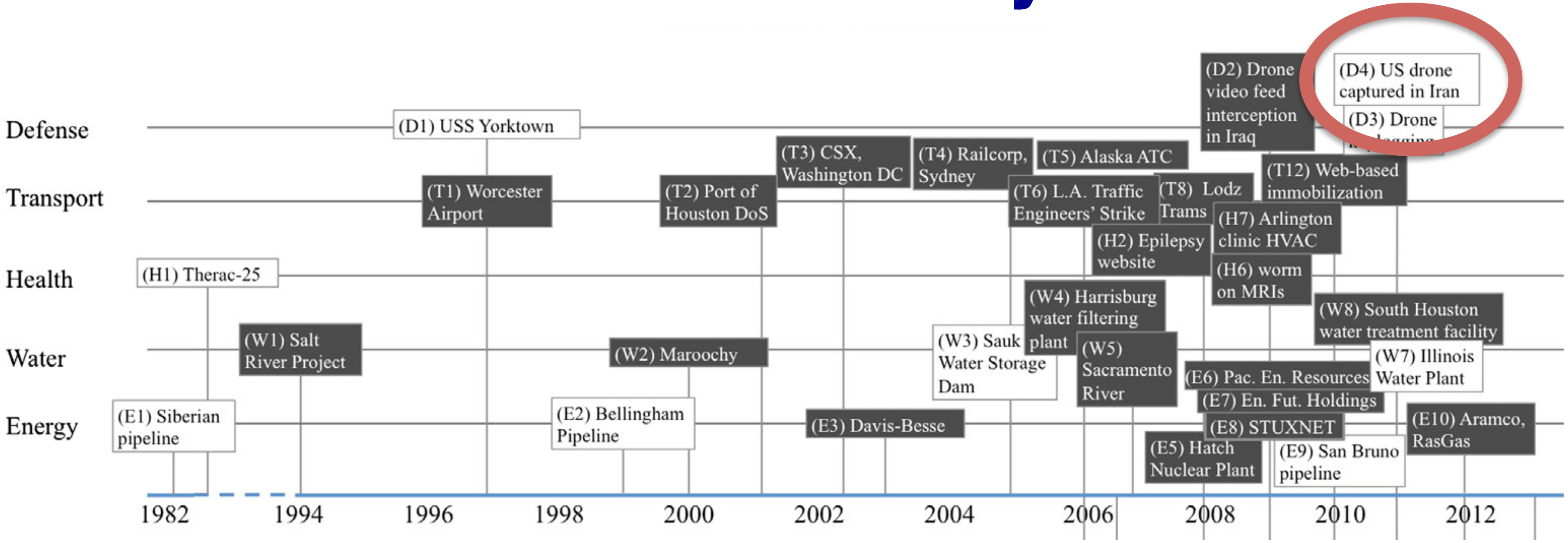


– Stuxnet: 2009:

- Attack on Iranian nuclear facility
- Used 4 undiscovered exploits targeting control

cyber-physical attacks: a growing invisible threat: George Loukas, 2015.

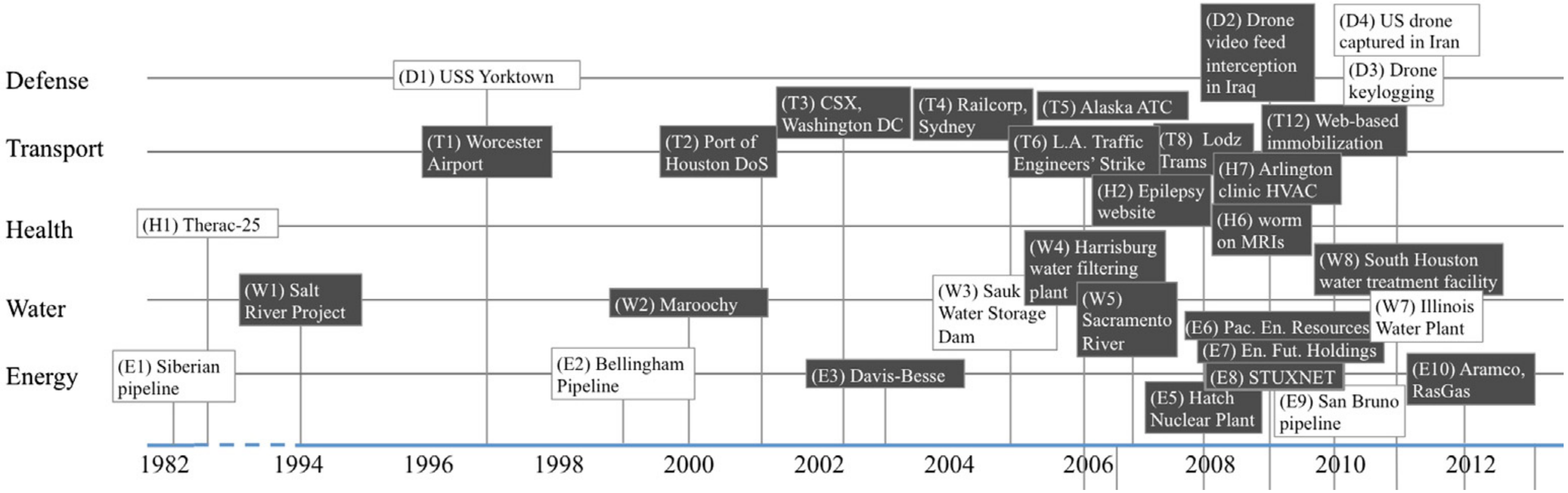
EMBS/CPS/IoT security incidents



- US Drone captured: 2011:
  - Iran captured predator drone that landed in the wrong area.
  - GPS spoofing
  - “System” worked perfectly
    - sensor measurements where wrong

cyber-physical attacks: a growing invisible threat: George Loukas, 2015.

EMBS/CPS/IoT security incidents



- IoT DDoS : October 21, 2016
  - thousands of devices overtaken using default passwords
  - organized into botnet to flood DNS provider
  - took down many major websites
    - $17 Billion cost to economy (0.1% of GDP)

cyber-physical attacks: a growing invisible threat: George Loukas, 2015.

Summary

- EMBS/CPS/IoT security is an emerging area with significant challenges.

- This course will provide exposure to tools and techniques for assessing and improving EMBS/CPS/IoT security
  - practice makes (almost) perfect

Assignments

- Reading
  - *Cyber-Physical Attacks: A Growing Invisible Threat*. George Loukas, 2015.
    - Chapters 1, 2 (this week)
    - Chapters 3, 4 (next week)
- Setup Kali Linux Box
- Presentations
  - Implants: Radoslav Ivanov
  - Vehicles: Bipeen Acharya
  - Industrial Control Systems (IDS): Dagaen Golomb