A Multimedia-based Virtual Classroom for Cyber-Physical Systems Security Education

Dr. Fei Hu { fei@eng.ua.edu }

Department of Electrical and Computer Engineering
University of Alabama
Tuscaloosa, Alabama

NSF-funded Project

- NSF-CNS # 1315328
- Leading PI: Dr. Fei Hu (UA)
- PI: Dr. Tommy Morris (MSU)
- Project Title: *EDU: Collaborative:* When Cyber Security Meets Physical World: a Multimedia-based Virtual Classroom for Cyber-Physical System Security Education to Serve City / Rural Colleges
- Total: $300K
- Duration: 2013 - 2015

Project Team (city/rural; academy/industry)

- Leading *PI (Hu)* has built medical CPS Security Schemes
- *PI (Morris)* focuses on CPS security especially industrial control security.
- 3 co-PIs from three of the top 20 U.S. rural colleges (selected by WorldWideLearn.com)
- e-learning expert - the director of UA faculty resource center [64], *Dr. Staffo*
- Multimedia design company - Provis Media Group
- Learning evaluator - Dr. McCallum
- Dr. Li (co-PI) is a smart grid expert

Motivation

"Cyber-Physical Systems (CPS) is a critical part of the national cyber infrastructure. Security threats to CPS pose significant risk to the health and safety of human lives, threaten severe damage to the environment, and could impose an adverse impact on the U.S. economy."

- Homeland Security, Dr. Nabil Adam, 2010.

"Rural area education is facing a great challenge: most students in rural colleges have less educational resources than city colleges. They have difficulties to transfer to large city schools. Models of effective urban education practice often do not work well at rural schools."

- Stephen Katsinas, Education Expert, 2010.

Project Goal

- To establish a multimedia-based virtual classroom with a virtual lab teaching assistant for the education of cyber-physical system (CPS) security

Feature 1: Application-driven - 3 types of Cyber-Physical Systems: Medical, Energy, Industry
Feature 2: Enhance rural area colleges' CPS security education via virtual classroom
Feature 3: Virtual Lab TA in open access labs with virtual hardware labs

1: Undergraduate Course	2: Senior Projects	3: Graduate Course
• Emphasize CPS security basics	• Emphasize team & hands-on	• Emphasize research skills
Lectures: (15 weeks of notes) • Basic CPS security concepts; • Teach typical CPS attacks; • Case studies: 3 CPS applica. **Labs**: Total 6 labs on basic attacks in CPS applications.	**Projects:** 5 team-based CPS security senior projects with hardware/software co-design: - Implanted device security; - Smart grid security; - Industrial control security.	**Lectures**: (15 weeks of notes) • Advanced CPS security topics; • Use materials from recent papers; • Train students research ideas. **Labs:** Total 6 class labs with research-oriented questions.

Learning:
Creativity
Multi-disciplinary
Hands-on

Fig.1 Project Overview

Project Novelty

- Novelty 1: Application-oriented Labs
  - select the important, interesting CPS applications including healthcare, renewable energy, and industrial control, for CPS attacks analysis
- Novelty 2: Peer-to-peer On-line Learning - work with a multimedia company to build interesting virtual classroom lectures. We will enhance rural area students' security learning through *peer-to-peer* on-line idea exchange tools
- Novelty 3: Virtual Labs & Virtual Lab TA
  - to meet the open access labs' requirements, we will build interactive virtual lab helper software (called virtual lab TA), to enable remote students to conduct virtual hardware labs and obtain help through multimedia tools.

CPS Security: What?

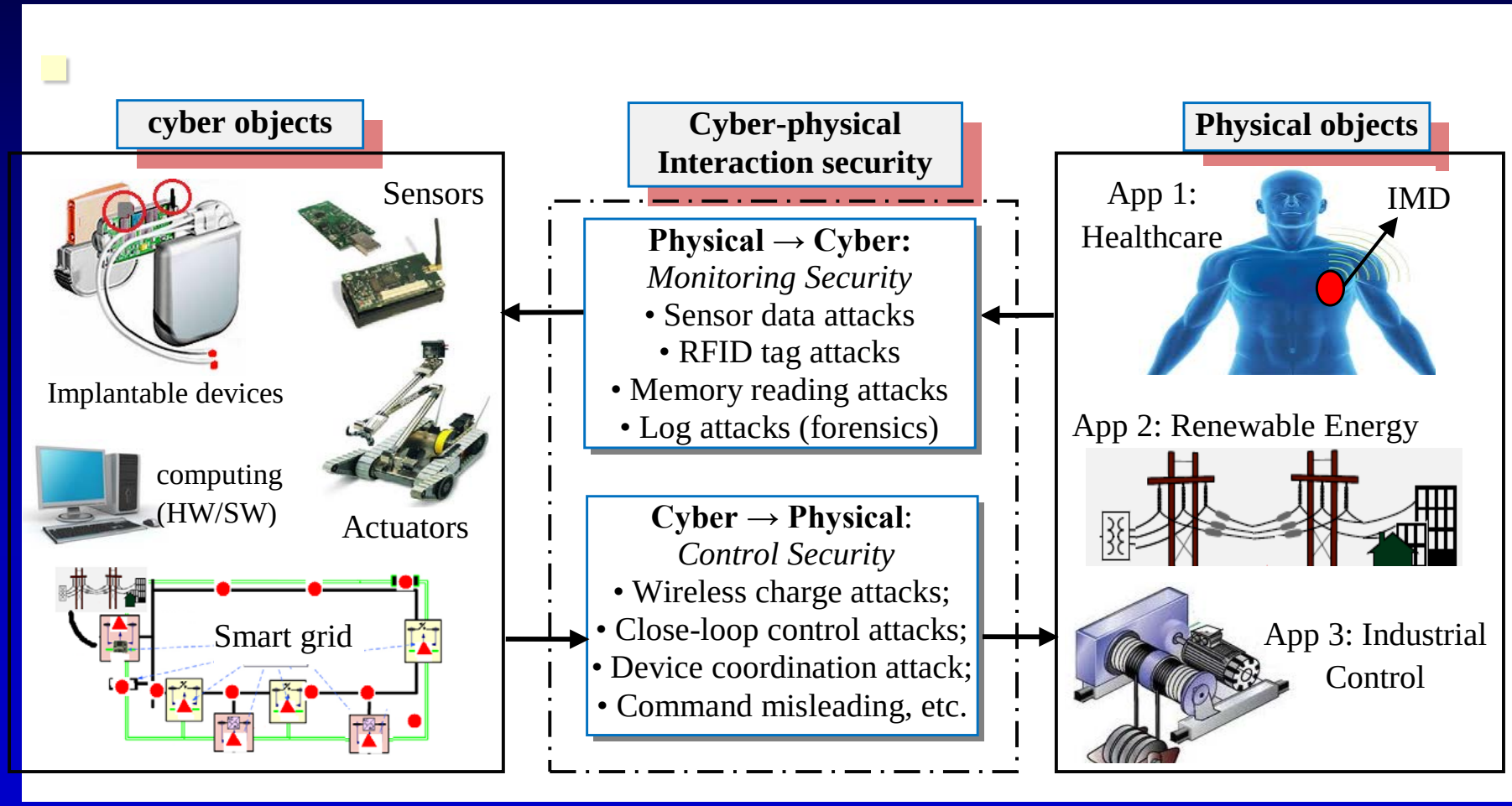


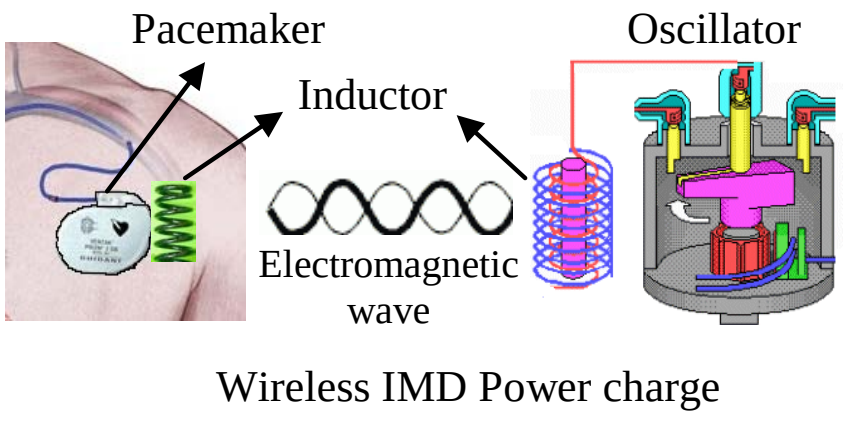
Fig.2 Cyber-Physical Systems (CPS): Security Perspective

CPS Security: Why?

- Cannot teach our students to simply use conventional, general cyber security schemes to achieve all CPS protections.
- This is because most CPS security solutions need to be closely integrated with the underlying physical process control features.

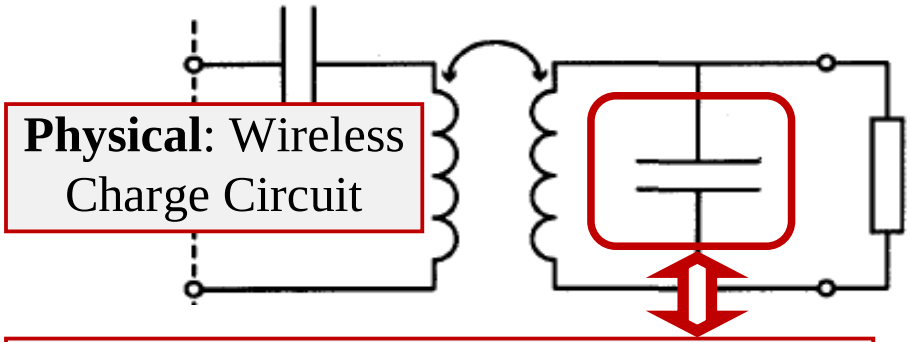
CPS Security: Example

- IMD Wireless Powering security



Wireless IMD Power charge

- It is meaningless to use conventional cryptographies to encrypt the power charge waves
- Energy transfer is entirely different from data transfer



· CPS-oriented security solution

Why help Rural schools?

- In the U.S. 20% colleges located in rural areas.
- 10 times smaller average annual budgets than urban/suburban schools.
- Many dependent upon state funding which has seen deep cuts.
- Faculty paid much less (average ~$46K) than urban/suburban schools (average ~$55K)
- It is difficult for them to attract faculty in *specific* computing fields such as CPS security

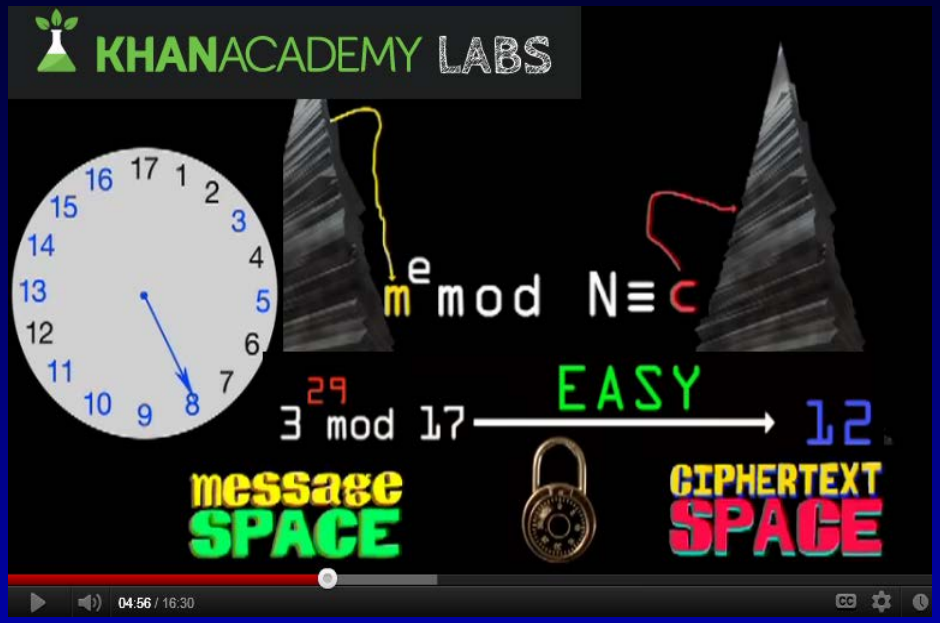
Why Multimedia Virtual Classroom?

- E-classroom enables after-class continuous learning through video, audio, Internet conferencing, chats, or virtual world interaction …
- On-line learning can enable frequent peer-to-peer student interactions.
- Multimedia-oriented materials attract students' attentions better than text-only lectures.

Why Virtual Labs?

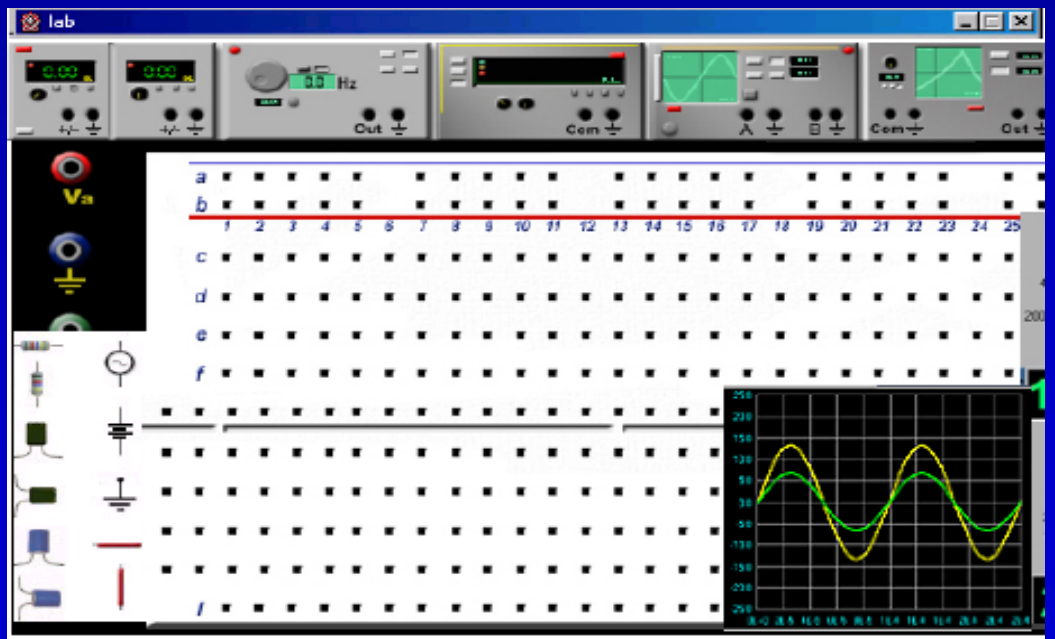
- Rural schools may not have the required lab resources (such as circuit boards, oscillator, etc.)
- Multimedia-oriented virtual lab teaching assistant (V-TA) to answer students' lab questions
- V-TA not only helps remote rural students to complete each security lab, but also adapts to 24/7 open access labs

V-TA Example



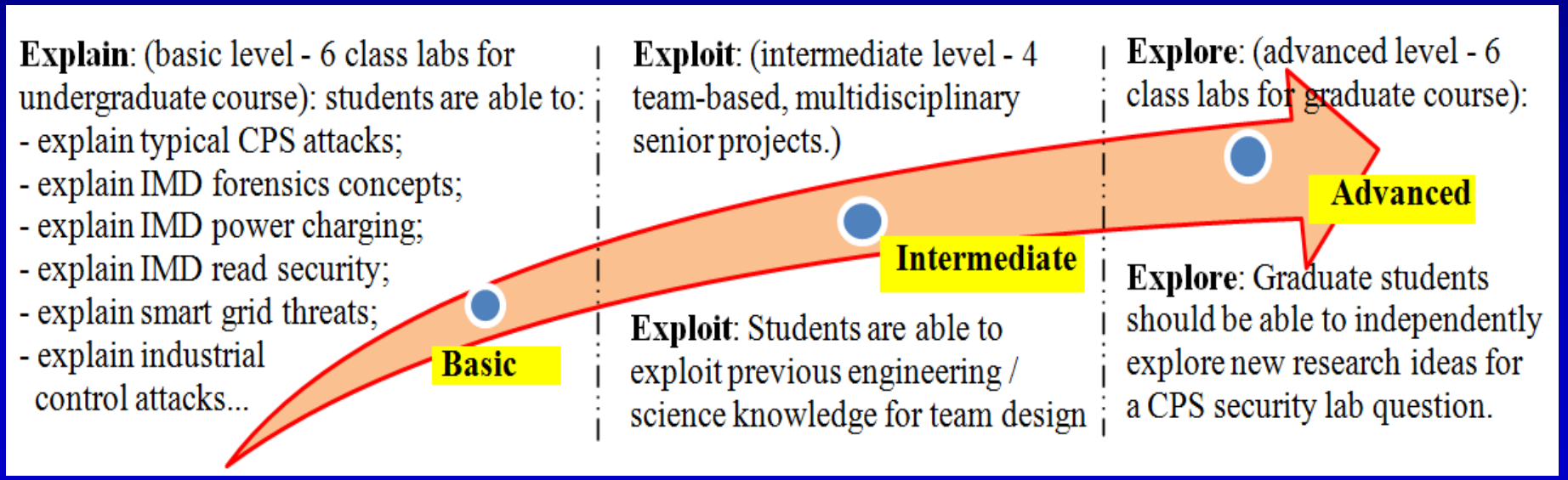
- e-classroom: Multimedia video on RSA

Virtual Hardware Lab via IMITS



Security Labs Development Methodology – 3E-based

- Explain-Exploit-Explore (3E) based Labs/Projects Education



3E-based Lab Development

- *Explanation*-oriented undergraduate class labs (basic level) will be reshaped into senior projects.
- Add some research-oriented questions to the undergraduate labs, and make them suitable to *graduate students.*
- Will design post-lab questions as well as the grading policies

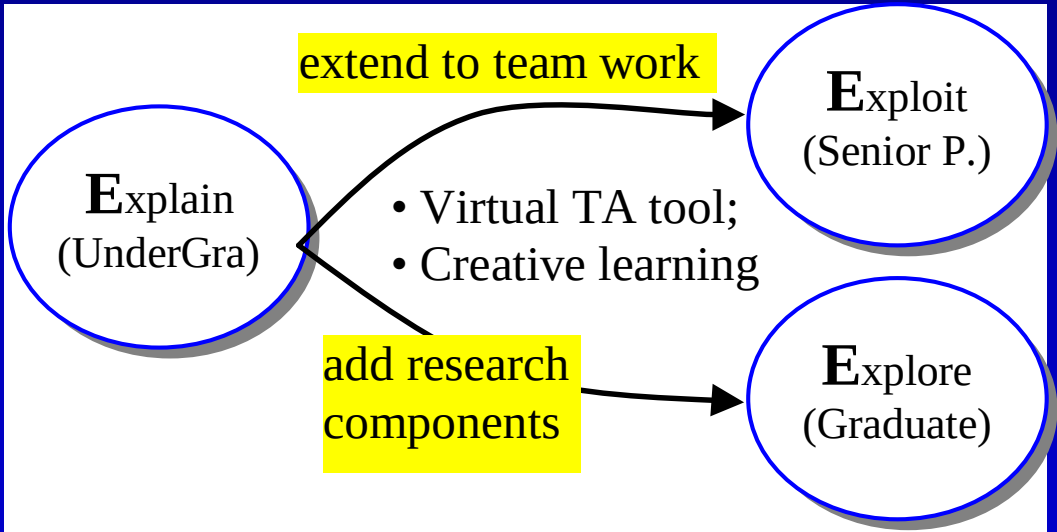


Fig.7 Three types of labs/projects

Lab Example 1 - *Wireless Power Charge Security*

- Traditional cryptography cannot be used here since the signals are not information data
- Capacitance change (physical part) is controlled by a chaotic maps (CM) generation scheme (cyber part).

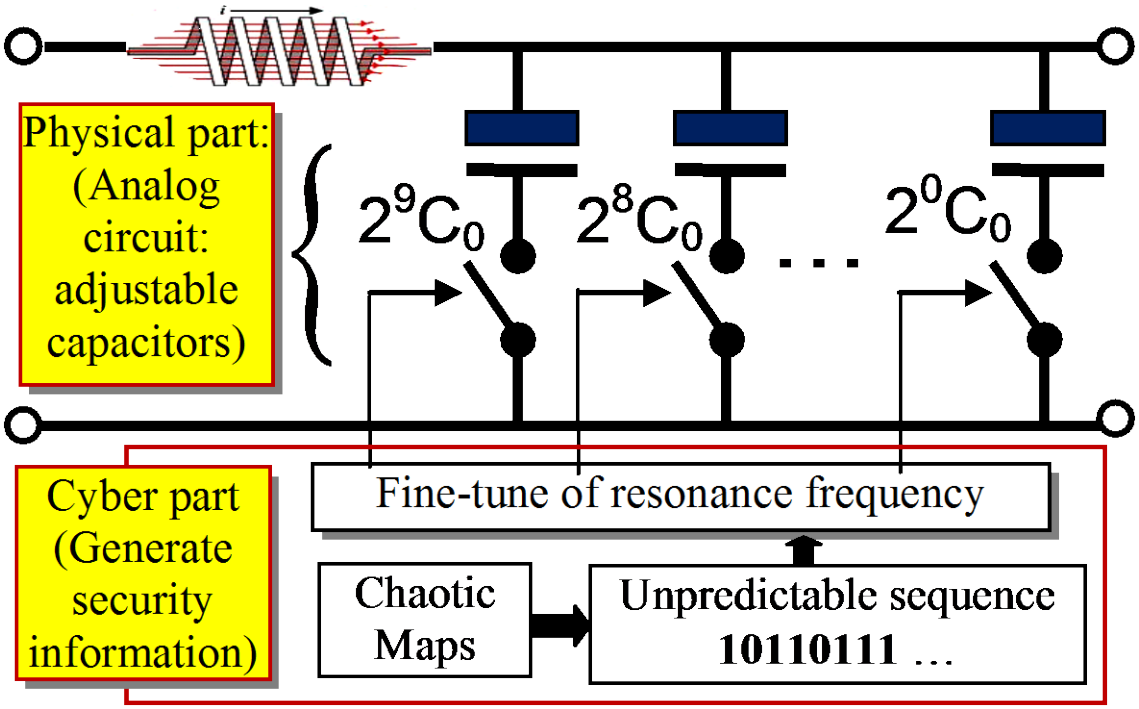
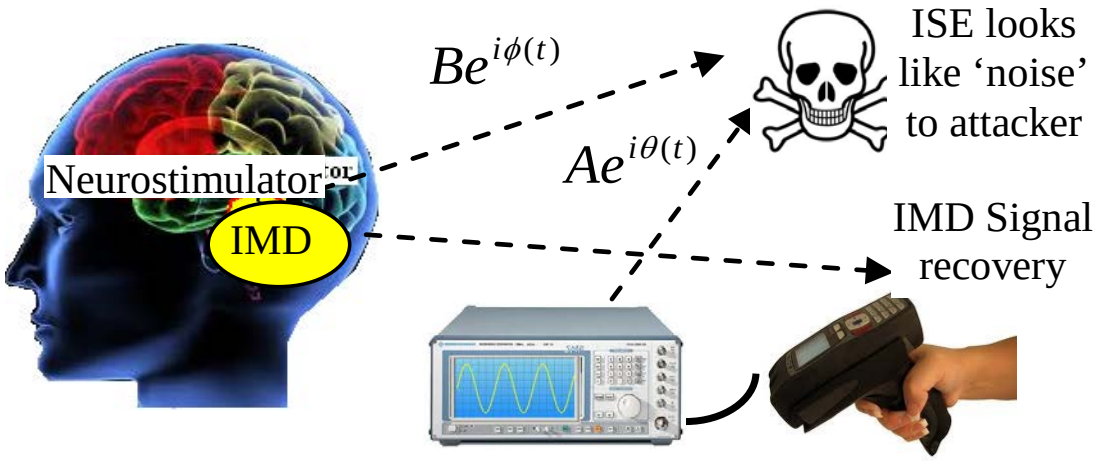


Fig.8 CPS security: wireless power charge lab

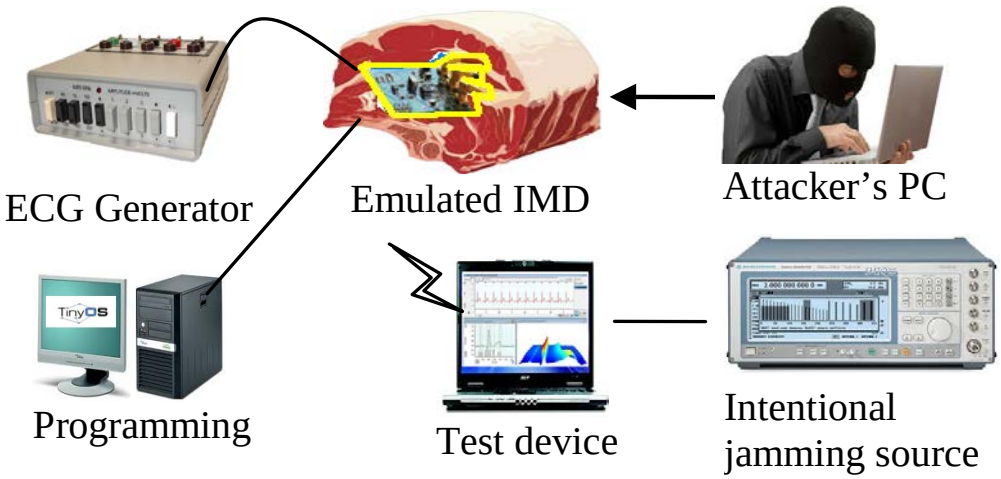
Lab Example 2 – Medical (IMD) Security



IMD is a typical CPS due to the tight coupling between the implanted chip (cyber) and the organ (physical).

Concept of Intentional Signal Jamming (ISJ)

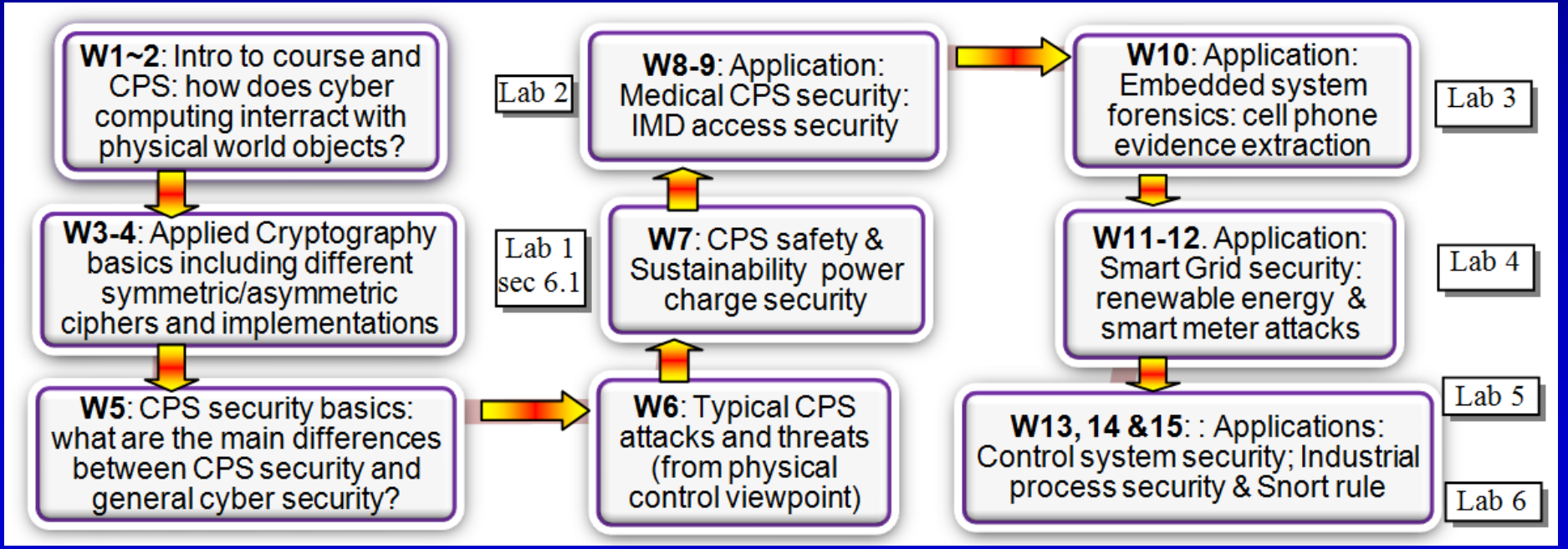
In this lab we will teach students to use an interesting scheme called intentional signal jamming (ISJ) that can hide the legitimate signals from an eavesdropper



Lab settings of IMD access securit

Develop BS Course

- Will develop a complete semester course - *Introduction to CPS security*, for undergraduate students.
- This course emphasizes the basic concepts and models on different CPS attacks and countermeasures.
- To attract students' attentions, we will use some interesting practical CPS applications as security design examples.



Develop Graduate Course

- We will then develop a research-oriented course called *Special Topics on CPS security*, for graduate students education.
- Unlike general cyber security courses, we will emphasize the specific attacks in cyber-physical interactions,
- Education goal is to *improve graduate students' research skills in designing efficient countermeasures to CPS attacks*.

Topic 1 - Attacks on physical state estimation

Topic 2 - Attacks on control loop

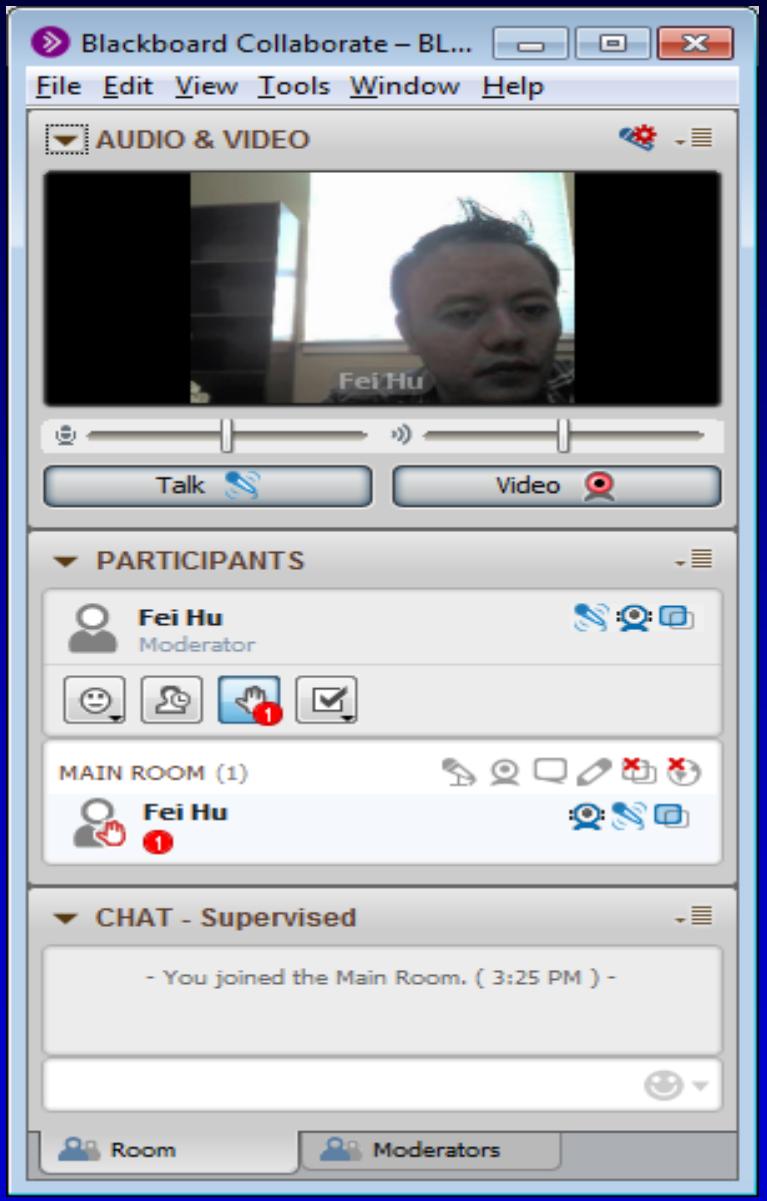
Topic 3 - CPS forensics

Topic 4 - CPS safety and sustainability

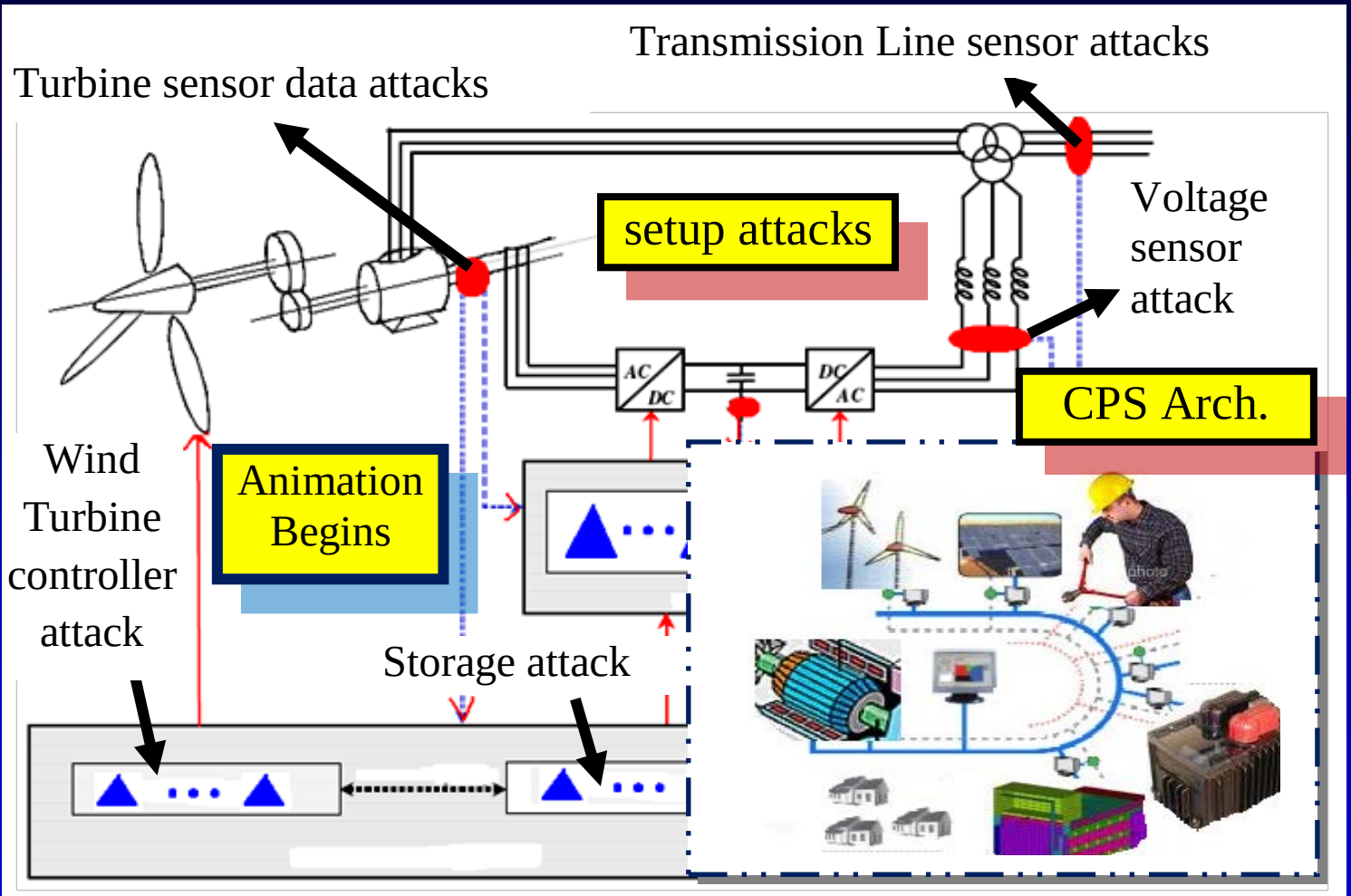
Topic 5 - Future research trend

Virtual Classroom

- Blackboard Collaborate (BC) based e-learning
- virtual office hours to visit instructors for questions
- peer-to-peer on-line learning environment that allows rural students to take online class



Multimedia Design



Interactive multimedia design on power grid attacks

Project Evaluation

"When the cook tastes the soup, that's **formative**; when the guests taste the soup, that's **summative**."

-- Evaluation Theorist Robert Stake

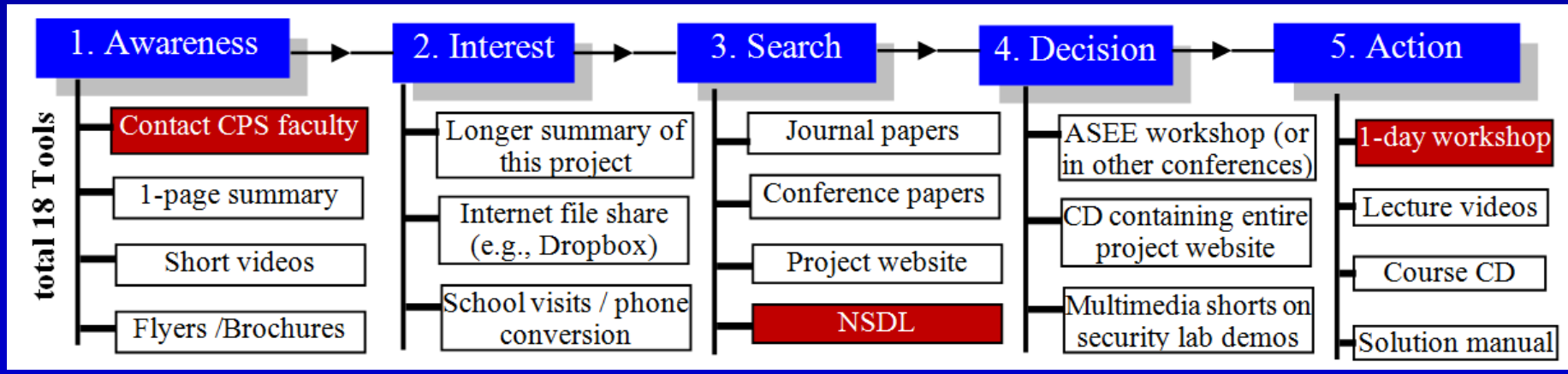
- Project evaluation will be conducted by Dr. McCallum from UA's Institute for Social Science Research (ISSR)

- *formative* evaluation will provide us with on-going information as a means of guiding course improvement.

- *summative* evaluation will be performed in the final phase to assess the entire impact of the CPS security education on rural/city schools

Dissemination: 5-stage model

- Dr. Froyd's famous 5-stage dissemination model
- Highlighted tools will be emphasized since they can help to *more efficiently propagate our virtual classroom modes to other rural/urban schools*
- Once this project is successful, its security teaching methodologies can be easily extended to the other > 500 rural area colleges (20% of U.S. colleges).



Thank you!

- Questions?