UNIVERSITY OF LOUISIANA AT LAFAYETTE

STEP Committee

Technology Fee Application

Upgrading Cyber-Physical System Security
Teaching and Research Lab

Title

Dr. Xiali Hei

Name of Submitter
(Faculty or Staff Only)

CMIX/RPA College of Sciences

Organization

Title: Upgrading Cyber-Physical System Security Teaching and Research Lab
Date: 1/13/2020

Name (Contact Person): Dr. Xiali Hei
Address: 315 E Lewis Street
Phone Number: 482-1037 Email: xiali.hei@louisiana.edu
Department/College/Org: School of Computing and Informatics

ABSTRACT (250 words or less):

Recent decades have witnessed an extraordinary level of investment in cyber-physical systems (CPS) such as self-driving vehicles, robotic devices, drones, and medical devices. All the decision-making systems of CPSs are often built upon environmental perception based on various sensor measurements. Adversaries can manipulate the sensor circuitry and deliver malicious control to sensors embedded in automatic control systems. The malicious control and the unpredictable consequences of it pose risks to the rapidly developed autonomous systems. It is critical to investigate the CPS security issues and propose better design solutions for them.

The purpose of the proposal is to upgrade the teaching and research lab of CPS Security with more contemporary equipment so that students can learn state-of-the-art CPS Security techniques in a professional setting because the upgraded teaching and research lab will have the necessary equipment to conduct the research and lab demonstration. The undergraduate students who enroll INFX 455- Cyber-Physical System Security, the graduate students who enroll CSCE 598 Special Topic: Advanced Cyber-Physical System Security and CSCE 512 Computer Network Security, the undergraduate and graduate students and post-doc/visiting scholars under PI Hei's advising will benefit from the upgrading. The new request equipment will benefit student research and education in CMIX for the next 10 years because they will come with a service plan that will allow for necessary upkeep and inspections. Students graduating from this lab will be familiar with modern laboratory equipment. More importantly, for this one-time investment, hundreds of students will be positively impacted for the foreseeable future.

PROPOSAL DESCRIPTION:

a. Purpose of grant and impact to student body as a whole

The purpose of the grant is to upgrade the teaching and research lab of Cyber-Physical System Security with more contemporary equipment (see Table 1) so that the upgrade can last at least next 10 years and students can learn cutting-edge Cyber-Physical System Security techniques in a professional setting because the upgraded teaching and research lab will have the necessary equipment to conduct the research and lab demonstration. It is important due to two reasons:

- PI Hei will teach INFX 455 - Cyber-Physical System Security for undergraduates and CSCE 598 – Special topic: Advanced Cyber-Physical System Security every fall semester. In this class, we have six to eight lab planned sessions. To conduct the lab session, the students need to access the PI's CPS security lab. Besides, PI Hei will teach CSCE 512- Computer Network Security every spring semester; the students in her class will use the lab for two or three labs.

- Recent decades have witnessed an extraordinary level of investment in cyber-physical systems (CPS) such as self-driving vehicles, robotic devices, drones, and medical devices. All the decision-making systems of such CPSs are often built upon environmental perception based on various sensor measurements. However, advances in fields such as material science and microfabrication techniques are continuously reducing the size of the sensors, which make them exhibit susceptibility to the influence of physical stimuli, including out-of-band signals that can be unintendedly captured by analog sensor components. Consequently, adversarial methodologies can be further developed to craft targeted malicious signals in the sensor circuitry and deliver malicious control to sensors embedded in automatic control systems. The malicious control and the unpredictable consequences of it pose risks to the rapidly developed autonomous systems. It is critical to investigate the cyber-physical system security issues and propose better design solutions for them. PI Hei’s CPS security research lab has generated 12 papers. Three of them have been featured by international media like The Register [1, 2] and RECLAIM the Net[3] and other media like the University of Michigan Engineering News [4]. Two of them published at top security conferences like USENIX SECURITY 2018 [5] and ACM CCS 2019 [6].

Currently, our oscilloscope and multi-channel power supply were borrowed from Dr. Zhongqi Pan’s lab. The amplifier cannot normally work now. A lot of key hardware components are missing. Without these appliances, the research and the teaching could not be processed as expected. The new request equipment will benefit student research in CMIX for the next 10 years because they will come with a service plan that will allow for necessary upkeep and inspections that we don’t have. Students graduating from this lab will be familiar with modern laboratory equipment, not outdated/homemade ones. More importantly, for this one-time investment, hundreds of students will be positively impacted for the foreseeable future. There are at least 16 students (six graduate and ten undergraduate students) per year whose research is dependent on the techniques. Within ten years, about 160 students will be positively affected.

b. Projected lifetime of enhancement

The upgrade will provide needed laboratory teaching enhancement for at least next 10 years. After this upgrade, the lab will be maintained through lab fees so that its equipment setup is not behind the state-of-the-art.

c. Person(s) responsible for Implementation, Installation, Maintenance, Operation, Training

The proposers will be responsible for implementing, installing, maintaining, operating and training of the equipment. The proposers have experience and skills to perform these tasks.

[1] https://www.theregister.co.uk/2018/08/28/hacking_motion_control/

[2] https://www.theregister.co.uk/2019/09/04/recaptcha_robot_hack/

[3] https://reclaimthenet.org/google-recaptcha-easily-broken/

[4] https://news.engin.umich.edu/2019/09/remote-attack-on-temperature-sensors-threatens-safety-of-incubators-industry/

[5] Y. Tu, Z. Lin, I. Lee, and X. Hei, “Injected and Delivered: Fabricating Implicit Control over Actuation Systems by Spoofing Inertial Sensors,” In Proc. of **USENIX Security 2018**, pp. 1545-1562, 2018.

[6] Trick or Heat? Manipulating Critical Temperature-Based Control Systems Using Rectification Attacks. Published at **ACM CCS (2019).**

Name	**Price($)**	**Purpose**	**Justification**
Tektronix AFG31101 Signal Generator	4,270.00$	Signal generation in experiments and tutorials.	The signal generator in the lab has a limited frequency range and a button on it is misfunctioning. The Tektronix AFG31101 generator is capable of generating signals in a wide frequency range to demonstrate the security issues in cyber-physical systems.
Keysight MSOX3104T Mixed Signal Oscilloscope	16,980.00 $	Signal analysis in experiments and tutorials.	The oscilloscope is essential for experiments related to embedded systems and signals. However, our lab does not own an oscilloscope that can be used in experiments. We have to borrow an oscilloscope from other labs if we want to do experiments or tutorials.
Instek GPS-3303 195W, 3-Channel, Linear D.C. Power Supply	396.90 $	Power supply for experiments.	We do not have a multi-channel DC power supply for experiments related to sensors, actuators, and circuits of cyber-physical components.
Avisoft Portable Ultrasonic Power Amplifier	950 EUR (1,058.06 USD)	Ultrasonic signals amplification for cyber-physical security and privacy analysis.	The device will be used to amplify ultrasound in different kinds labs of CPS security analysis. For example, the students will be able to repeat experiments in recent top academic cyber-security conferences under instructions of the PI.
LDC205C - Benchtop LD Current Controller	1091.86$	Current controller	This equipment will be used in tutorials of

			cyber-physical analysis, such as laser-based command injection on voice controlled assistants (e.g., Amazon Echo).

Budget Proposal

1.	**Equipment**	**$ 23,796.82**
2.	**Software**	**$**
3.	**Supplies**	**$**
4.	**Maintenance**	**$**
5.	**Personnel**	**$**
6.	**Other**	**$**
TOTAL:		**$ 23,796.82**