Towards a Multimedia-based Virtual Classroom on Cyber-Physical System (CPS) Security Education for Both City and Rural Schools

Fei Hu, Electrical and Computer Engineering, University of Alabama, Tuscaloosa, AL, USA
Thomas H. Morris, Electrical and Computer Engineering, Mississippi State University, USA
Debra M. McCallum, Social Science, University of Alabama, Tuscaloosa, AL, USA
Hongbo Zhou, Computer Science, Slippery Rock University

Abstract – This project [1] aims to establish a multimedia-based virtual classroom with a virtual lab teaching assistant for the education of cyber-physical system (CPS) security. Such a virtual classroom will enable college students in resource-limited rural areas to learn the latest CPS security knowledge through on-line, peer-to-peer learning with other students (such as those in city schools). The novelty of this educational development includes three features. First, all CPS security teaching materials target application-driven learning. We select the important, interesting CPS applications including healthcare, renewable energy, and industrial control, for CPS attacks analysis. Second, we have built interesting virtual classroom lectures. We enhance rural area students' security learning through *peer-to-peer* on-line idea exchange tools. Third, to meet the open access labs' requirements, we have built interactive virtual lab helper software (called virtual lab TA), to enable remote students to conduct labs and obtain help through multimedia tools.

Index Terms – Virtual Classroom, Virtual TA, Cyber-Physical System Security, Rural Schools

1. Introduction

> "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." [1]
>
> - *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." [2]
>
> - *Stephen Katsinas, Education Expert, 2010.*

The ultimate purpose of using cyber infrastructure (including sensing, computing and communication hardware /software) is to intelligently *monitor* (from physical to cyber) and *control* (from cyber to physical) our physical world. A system with a tight coupling of cyber and physical objects is called a cyber-physical system (CPS), which has become one of the most important and popular computer applications today. However, in CPS the physical systems are susceptible to the cyber security vulnerabilities from monitoring and control security perspective (Fig.1). In 2010 people demonstrated a software tool called CarShark [3] which could remotely kill a car engine; some hackers have broken into the U.S. air traffic control systems [4]; in 2010 hackers designed a virus which can successfully attack Siemens plant-control system [5].

We may not 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 [6]. As an example, a typical CPS, called implantable medical device (IMD), may be implanted in the human body for both physical-to-cyber medical sensing and cyber-to-physical organ control. Typical IMDs include pacemakers, neuro-stimulators, insulin pumps, and others. An IMD attack called wireless power charge attack, is a critical issue since an attacker who knows the coil resonance frequency can cause the IMD to

[1] This project is sponsored by NSF DUE-1315328. All ideas presented here do not necessarily represent NSF's opinions.

overheat. It is meaningless to use conventional cryptographies to encrypt the power charge waves since energy transfer is entirely different from data transfer (Fig.2). We may use a CPS-oriented security solution to solve the above issue (Fig.3): using *cyber* scheme (chaotic maps) to control the *physical* object (circuit capacitors) in order to prevent an attacker from guessing the power charge resonance frequency that secretly switches values.

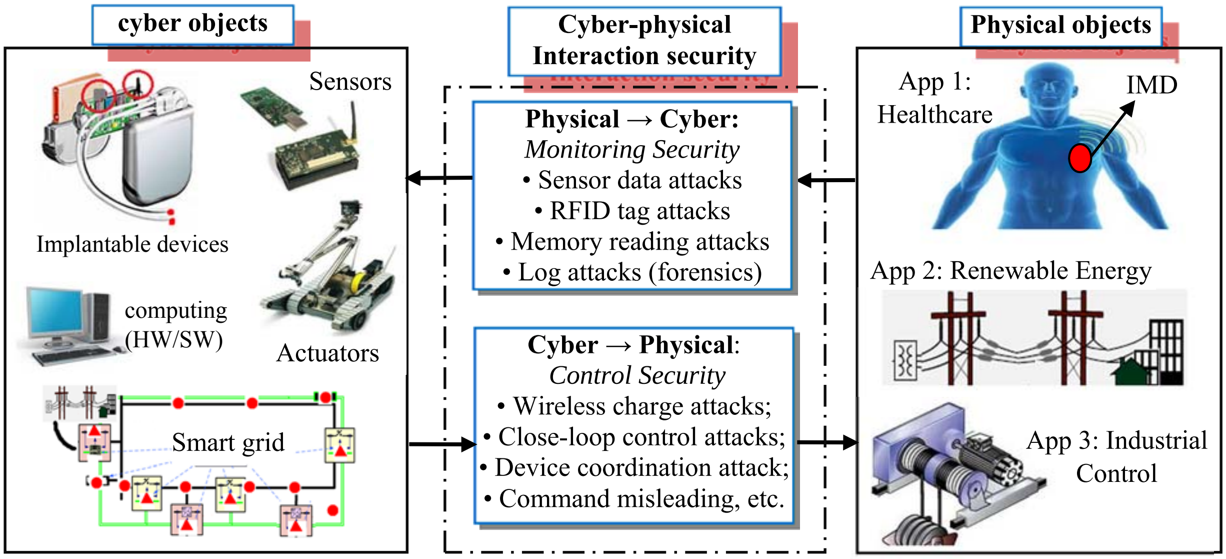


Fig.1 Cyber-Physical Systems (CPS): Security Perspective

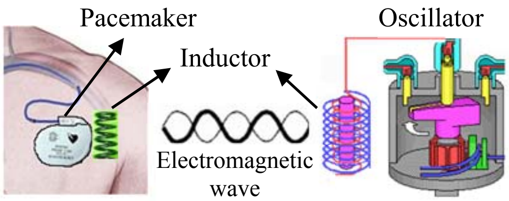


Fig.2 Wireless IMD Power charge

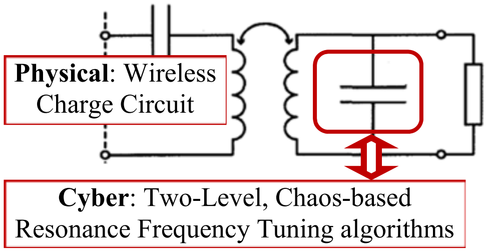

Physical: Wireless Charge Circuit
Cyber: Two-Level, Chaos-based Resonance Frequency Tuning algorithms

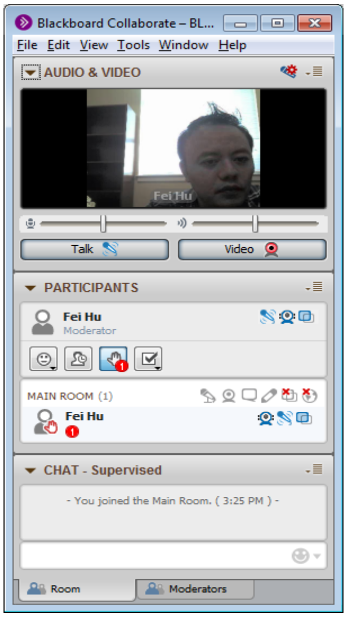
Fig.3 CPS-oriented security solution

Therefore, it is critical to train national CPS security workforce who can handle homeland security issues in the critical CPS applications including healthcare, energy, industrial control, and others. This project aims to develop pioneering CPS security education materials for both undergraduate and graduate students.

Many schools cannot offer CPS security courses for students due to a few reasons. First, this is a relatively new security field, and many research issues are still unsolved. Second, unlike general cyber security, CPS security needs to be tied with concrete, physical-oriented features. This requires an instructor to efficiently convey the security knowledge to students together with the teaching of physical laws and process control models. Third, perhaps the most important reason - many schools lack the corresponding educational resources including cyber security faculty and the corresponding lab conditions. This is especially true for many rural area colleges. Based on the findings from the Education Policy Center at the University of Alabama [2], in the U.S. 20% of colleges are located in rural areas. They have almost 10 times smaller average annual budgets than urban/suburban schools. Many of them are dependent upon state funding which has seen deep cuts in recent years. Moreover, rural college faculty members are paid much less (average ~$46K) than urban/suburban schools (average ~$55K) [2]. Therefore, while rural colleges may have faculty who can teach *general* computing fields, it is difficult for them to attract faculty in *specific* computing fields such as cyber security. The proposed multimedia e-learning of CPS security knowledge via peer-to-peer learning and virtual lab TA tools can efficiently help the rural schools to overcome the constraints of security education resources.

2. Virtual Classroom and Virtual TA

The e-classroom enables after-class continuous learning through various synchronous and asynchronous activities (video, audio, Internet conferencing, chats, or virtual world interaction). While classroom learning has good instructor-student interaction opportunities, on-line learning can enable frequent peer-to-peer student interactions. Modern constructivist theorists stress the value of *peer-to-peer learning* in developing multiple perspectives [7]. Work on collaborative learning illustrates potential gains in cognitive learning tasks, as well as increases in the acquisition of critical social skills in education. This project uses the latest virtual classroom tool called Blackboard Collaborate (BC) [8] (Fig.4) for on-line learning as well as peer-to-peer student interactions among rural/city schools. The director of UA faculty resource center (FLC), Dr. Staffo will help to deliver our materials via BC.



- You joined the Main Room. (3:25 PM) -

Fig.4 Blackboard Collaborate

It has been shown that <u>multimedia-oriented</u> materials attract students' attentions better than text-only lectures [9]. Based on the split-attention principle [10], when giving a multimedia explanation, it is better to present words as auditory narration rather than as visual on-screen text. Hence a multimedia lecture with simultaneous video and audio presentation can generate better learning effects. Fig.5 (a) shows a screenshot of our developed multimedia lecture on RSA encryption/decryption. It follows Khan Academy [11] video design style.

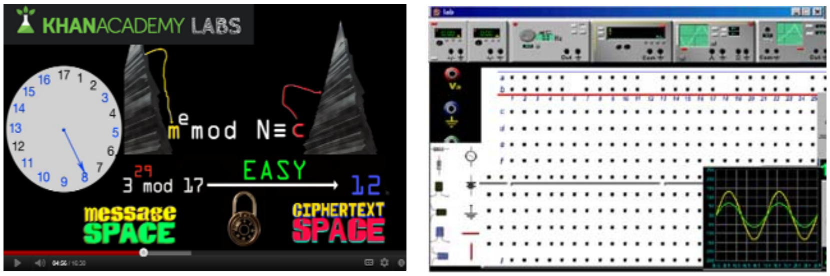


Fig.5 (a) e-classroom: Multimedia video on RSA; (b) Virtual Lab via IMITS

Why build virtual labs with a software-based TA? Besides the above discussed multimedia lectures, this project will also build a series of virtual labs that allow the rural students to try the "virtual hardware". Fig.5 (b) shows such an example. Since the rural schools may not have the required lab resources (such as circuit boards, oscillator, etc.), for *hardware*-based security labs such as IMD power charge security lab, we are investigating the use of the interactive multimedia intelligent tutoring system (IMITS) [12] to guide remote students for hardware settings. For *software*-based security labs (such as the lab on smart grid security), we have built multimedia-oriented virtual lab teaching assistant (V-TA) to answer potential lab questions students may have. The V-TA will have an index of lab questions. When students click any of them, a multimedia clip with video/audio explanations will appear. The V-TA tool includes pre-lab training, topic explanations, instrumentation training, and a post-lab assessment. The V-TA system not only helps remote rural students to complete each security lab, but also adapts to the requirements of 24/7 open access labs: today, more and more schools adopt open labs that allow individual, self-paced learning and fit students' flexible schedules. Open labs save more teaching resources (equipment and space) than traditional fixed-schedule labs [13]. V-TA is especially useful to such open labs since it is not realistic to have 24/7 TAs' help there.

3. Curriculum Development on CPS Security

We have developed a complete semester course - *Introduction to CPS security*, for undergraduate students. All lecture materials can be downloaded from our project website: http://feihu.eng.ua.edu/NSF_CPS/year1/CPS.html.

This course emphasizes the basic concepts and models on different CPS attacks and countermeasures. To attract students' attentions, we have used some interesting practical CPS applications as security design examples. Fig.6 shows our 15-week teaching plan. It consists of the following units:

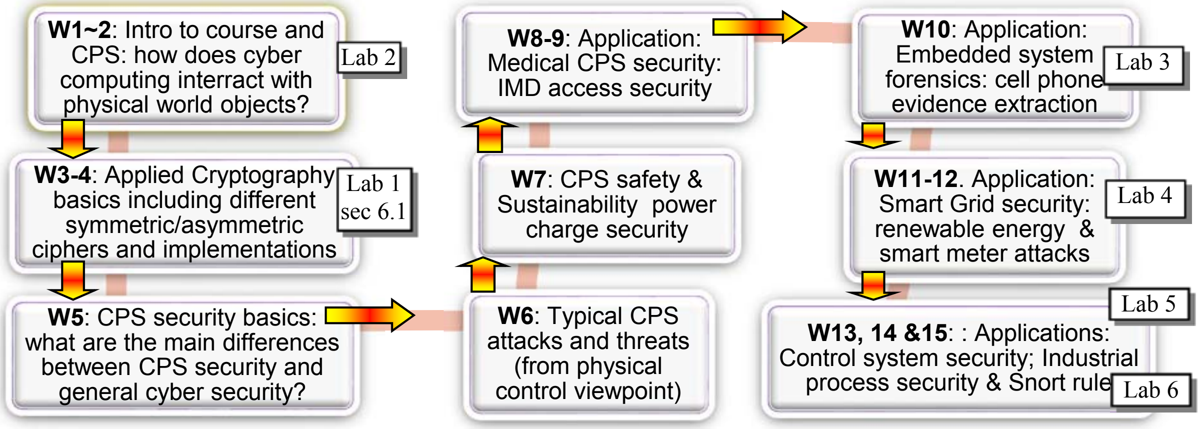

W1~2: Intro to course and CPS: how does cyber computing interract with physical world objects?
Lab 2
W3-4: Applied Cryptography basics including different symmetric/asymmetric ciphers and implementations
Lab 1 sec 6.1
W5: CPS security basics: what are the main differences between CPS security and general cyber security?
W6: Typical CPS attacks and threats (from physical control viewpoint)
W7: CPS safety & Sustainability power charge security
W8-9: Application: Medical CPS security: IMD access security
W10: Application: Embedded system forensics: cell phone evidence extraction
Lab 3
W11-12. Application: Smart Grid security: renewable energy & smart meter attacks
Lab 4
Lab 5
W13, 14 &15: : Applications: Control system security; Industrial process security & Snort rule
Lab 6

Fig.6 Undergraduate course - one semester (15 weeks) teaching plan: lectures + labs

- *Basics on CPS, Applied Cryptography, and CPS security*: First, we need to help undergraduate students understand the basic concepts of CPS security. We have developed 5 weeks of lectures on cyber-physical interaction principles (i.e. what is CPS?), applied cryptography (i.e., what is security?), and CPS security basics (how is it different from conventional cyber security?).
- *Trustworthy CPS*: A trustworthy CPS should have the following **3S** features: (1) **S**ecurity: It can overcome different attacks and threats; (2) **S**afety: It has to avoid the hazards such as operational faults and software failure; and (3) **S**ustainability: It has a long-term, power-efficient, stable operations even under different energy consumption attacks. We will develop lectures on how to support 3S features.
- *Application 1- Medical CPS security*: The PI (Hu) will use his long-term medical CPS security design experiences [43-54] to carefully organize different medical device security concepts into 2 weeks of lectures. We will show students how we can securely coordinate medical devices' operations.
- *Application 2 - embedded system forensics*: Today smart phones have been studied intensively in security field. Students like the topics of embedded system forensics. We will

explain the principles of extracting semantic evidences from binary phone memory via pattern recognition schemes.

• *Application 3 - smart grid security*: Renewable energy systems (such as wind, solar, etc.) have become critical to the nation due to the limited gas/coal resources today. We will develop materials on smart grid attacks such as grid-to-backbone islanding attack, smart meter attack, etc.

• *Application 4 - Industrial process security*: Industrial processes rely on the sensor-controller interaction models for close-loop control. The goal of industrial process security is to ensure that the controller can still make correct decisions even though the sensor data has been polluted. We will use Tennessee-Eastman process control model [83, 84] and Snort rule [76] to explain various control attacks.

4. Developed Labs and VTA

We have built a series of CPS security labs that interest students very much. Those labs reflect the latest progress in this field. They just need low-cost hardware components. Here we list three examples. For each lab, we consider basic, intermediate, and advanced levels.

Lab # 1 *Wireless Power Charge Security:* The *learning goal* of this lab is that the undergraduate students are able to explain the potential CPS attacks in wireless energy transfer to an IMD (or other devices), as well as the effective countermeasures for those attacks. Traditional cryptography cannot be used here since the signals are not information data (they are energy waves). We teach students to use an adjustable capacitor array (Fig.7) to dynamically change the tuning frequency to prevent an attacker's damage. Such a capacitance change (physical part) is controlled by a chaotic maps (CM) generation scheme (cyber part). This is a typical CPS security solution with tight cyber-physical coupling. In this lab, we ask the students to use the breadboard to design such a capacitor array, and then interface the board to a laptop that generates CM sequence.

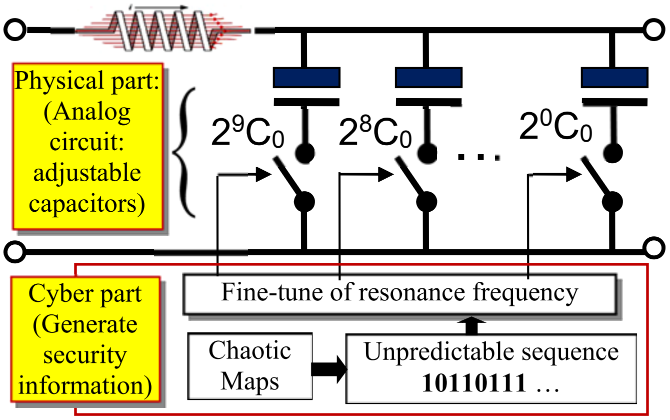

Physical part: (Analog circuit: adjustable capacitors)
2^9C_0
2^8C_0
...
2^0C_0
Cyber part (Generate security information)
Fine-tune of resonance frequency
Chaotic Maps
Unpredictable sequence
10110111 …

Fig.7 CPS security: wireless power charge lab

Extend to Senior Project # 1 (immediate level): We have extended the above undergraduate class lab to a senior project with the following design tasks: (1) hardware design: a few team members are responsible for the analog circuit design through either the breadboard or PCB (printed circuit board). They need to implement the capacitor array. (2) software design: a few students design the CM generation algorithm. (3) CPS security system: all students work closely to integrate all hardware/software components into a CPS security demo platform. Comprehensive security test will be performed.

Extend to graduate course Lab # 1 (advanced level): We have extended the above undergraduate lab to a graduate course lab by adding the following research-oriented lab tasks: (1) How do we extend the 1-D CM to 3-D one to generate a more random bit sequence? (2) How do we fine tune the charging frequency when the capacitor array cannot provide an accurate frequency?

Encourage creative learning: We have given extra credits in senior project #1 if the team can use the programmable breadboard called Prototino from SpikenzieLabs, for a hardware /

software co-design. In the graduate course lab, we encourage students to search for other tuning frequency control algorithms besides the 3-D CM.

Lab # 2. *Mobile-Phone Based Human Behavior Monitoring:* This lab aims to use cell phone sensors to detect human behaviors. Thus we may be able to use phone data to find whether somebody was driving while using phone. We also analyze the phone memory data to recover the calling records. Those records are important to digital forensics. Fig.8 shows the lab principle. After we obtain the phone sensor data, we can use different algorithms to analyze the data and recognize human behavioral patterns. The student will practice the dynamic time warping (DTW) and the support vector machine (SVM) algorithms in our data analysis. Our other main goal involves extracting the data of phone calls and text message and analyzing them on a binary level. This method provides investigators of a way to get data from a crime scene phone despite what brand it is or operating system it runs. After we are able to view this data at binary level, we use an algorithm called the hidden Markov model (HMM) to predict missing data in the phone memory.

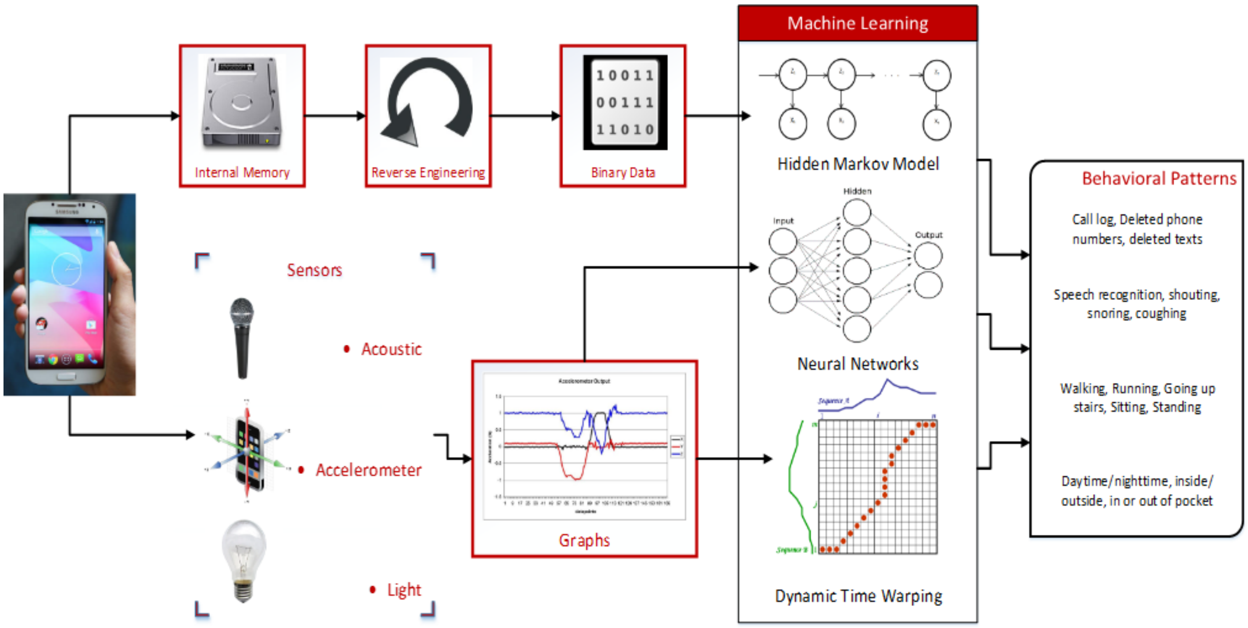
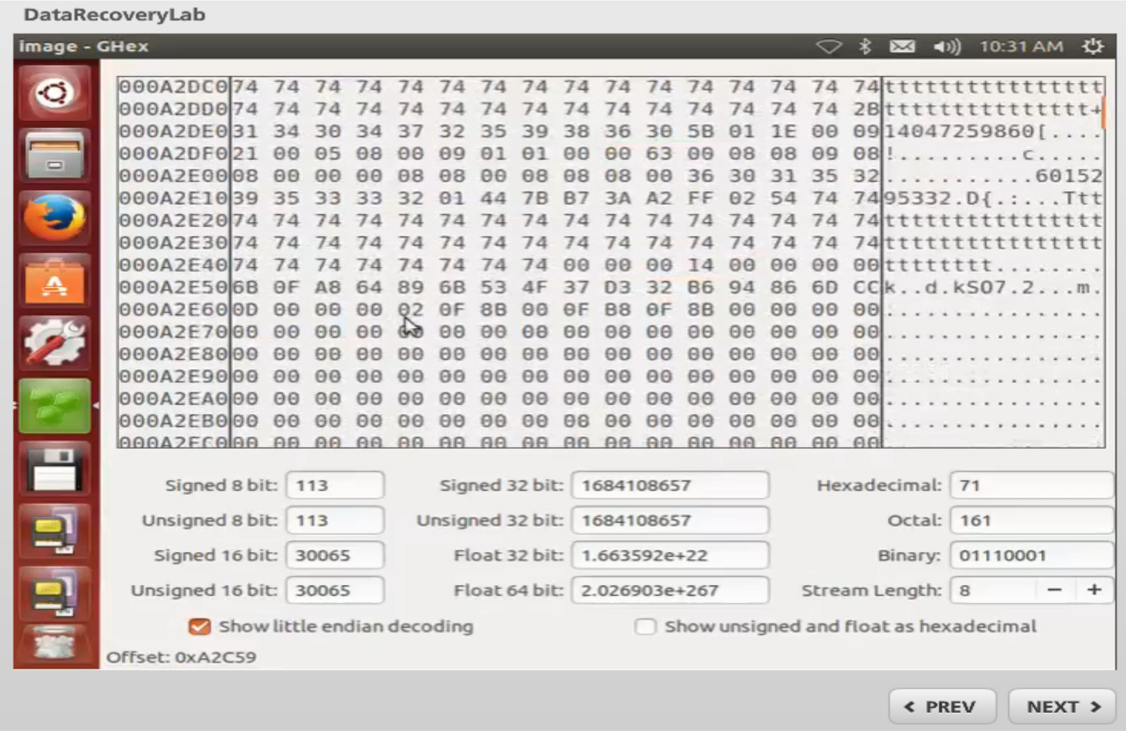


Fig.8 Cell Phone based Human Behavior Analysis

We have also built the virtual TA (VTA) software tool that can help the remote rural students. Fig.9 illustrates such an example screen, which shows how the phone memory looks like.

Lab # 3. *Gas Pipe Security:* This laboratory exercise is meant to serve as a familiarization to the look and security issues of Supervisory Control and Data Acquisition (SCADA) systems. Fig.10 represents a gas pipeline, much like what is present in Mississippi State University's SCADA laboratory. This display consists of a few items: An analog pressure gauge (top left), a digital pressure gauge (shown in the top middle), a solenoid release valve (middle bottom), and the control switches (far right). One of the first steps of an attacker is to gain access to the network that PLC controllers are on. Once the attacker has access to the network, finding out the IP address of devices on the network is important. Once a target IP address is identified, the MODBUS device ID of this machine must be identified. This attack is known as a "Device Scan" attack.

For this lab students will create two attacks: a command injection attack which sends a malicious command to a smart meter, and a response injection attack which uses the Ettercap tool to create a man-in-the-middle exploit and then alter a meter query response to change the instantaneous meter readings to a lower value. The Ettercap tool is downloadable for free. A virtual smart meter which runs in the VMWare Player application (also free) is developed and provided with the lab. The *learning goal* is to emphasize smart meter threats and to emphasize that the lack of cryptographic signature enables command injection and response injection attacks.



```
000A2DC0 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 tttttttttttttttt
000A2DD0 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 2B ttttttttttttttt+
000A2DE0 31 34 30 34 37 32 35 39 38 36 30 5B 01 1E 00 09 14047259860[....
000A2DF0 21 00 05 08 00 09 01 01 00 00 63 00 08 08 09 08 !.........c.....
000A2E00 08 00 00 00 08 08 00 08 08 08 00 36 30 31 35 32 ...........60152
000A2E10 39 35 33 33 32 01 44 7B B7 3A A2 FF 02 54 74 74 95332.D{.:...Ttt
000A2E20 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 tttttttttttttttt
000A2E30 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 74 tttttttttttttttt
000A2E40 74 74 74 74 74 74 74 74 00 00 00 14 00 00 00 00 tttttttt........
000A2E50 6B 0F A8 64 89 6B 53 4F 37 D3 32 B6 94 86 6D CC k..d.kSO7.2...m.
000A2E60 0D 00 00 00 02 0F 8B 00 0F B8 0F 8B 00 00 00 00 ................
000A2E70 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000A2E80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000A2E90 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000A2EA0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000A2EB0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000A2EC0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Signed 8 bit: 113 Signed 32 bit: 1684108657 Hexadecimal: 71

Unsigned 8 bit: 113 Unsigned 32 bit: 1684108657 Octal: 161

Signed 16 bit: 30065 Float 32 bit: 1.663592e+22 Binary: 01110001

Unsigned 16 bit: 30065 Float 64 bit: 2.026903e+267 Stream Length: 8

☑ Show little endian decoding ☐ Show unsigned and float as hexadecimal

Offset: 0xA2C59

Fig.9 VTA Interface (an example screen on phone memory analysis)

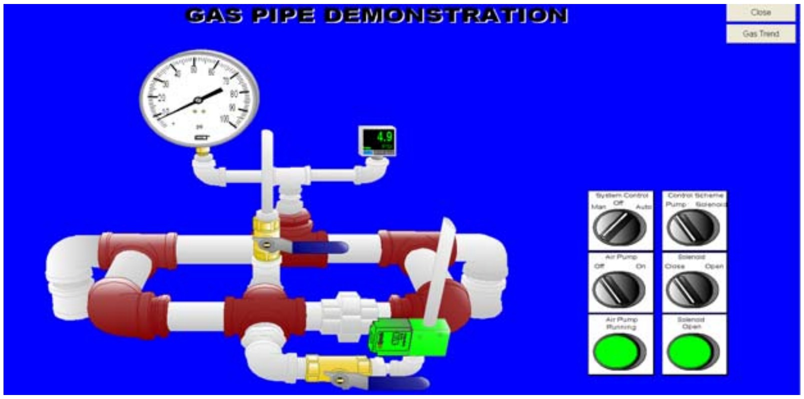


Fig.10 Gas Pipe System

5. Conclusions

It is critical to train national security workforce who can handle homeland security cases in the critical CPS applications. Many schools lack the corresponding educational resources including cyber security faculty and lab conditions. This is especially true for many rural area colleges. To the best of our knowledge, we have not seen any educational developments similar to our proposed one that aims to cover comprehensive principles and hands-on designs of CPS security for both undergraduate and graduate students, together with multimedia-oriented virtual lab TA tools. Our teaching methodologies can be easily extended to other > 500 rural area colleges (20% of U.S. colleges).

References:

[1] U.S. Department of Homeland Security, *Workshop on Future Directions in Cyber-physical Systems Security*, (Final Report), January 2010. Edited by Dr. Nabil Adam, Infrastructure & Geophysical Division, Science and Technology Directorate.

[2] Stephen G. Katsinas, "*America's Rural Community Colleges: Demographics, Challenges, and Opportunities*", (a Briefing on Rural Community Colleges for the U.S. Department of Education), Washington, D.C. (invited talk). February 24, 2010.

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson,H. Shacham, and S. Savage. “Experimental security analysis of a modern automobile”, In Proceedings of the 31st IEEE Symposium on Security and Privacy, May 2010.

[4] Elinor Mills, “Hackers broke into FAA air traffic control system”, The Wall Street Journal, page A6, 2009.

[5] Vanessa Fuhrmans, “Virus Attacks Siemens Plant-Control Systems”, TheWall Street Journal, july 22, 2010.

[6] A. A. C´ardenas, S. Amin, B. Sinopoli, A. Giani, A. A. Perrig, and S. S. Sastry, “Challenges for securing cyber physical systems,” in Workshop on Future Directions in Cyber-physical Systems Security, Newark, NJ, USA, Jul. 2009.

[7] Constructivism (learning theory), see WiKi's explanations on the importance of peer-to-peer learning: (site 1) http://en.wikipedia.org/wiki/Constructivism_%28learning_theory%29 . (site 2): http://en.wikipedia.org/wiki/Peer_learning. All visited in Oct 2012.

[8] Blackboard Collaborate: see http://www.blackboard.com/platforms/collaborate/overview.aspx .

[9] Richard E. Mayer and Roxana Moreno, "A Cognitive Theory of Multimedia Learning: Implications for Design Principles," downloadable from: http://www.unm.edu/~moreno/PDFS/chi.pdf . Visited in Sep of 2012.

[10] Chandler, P. and Sweller, J., "Cognitive load theory and the format of instruction". Cognition and Instruction, 8, 293-332. 1991.

[11] Khan Academy video library and style: see http://www.khanacademy.org/ .

[12] interactive multimedia intelligent tutoring system (IMITS): http://www.temple.edu/imits/imits.htm .

[13] Rahman N. A, Kofli N.T. Takriff M. S, Abdullah S., “Comparative Study between open ended laboratory and traditional laboratory,” IEEE Global Engineering Education Conference, Amman, Jordan, pp. 40-44, April 4-6, 2010.