Developing a Smart Grid Cybersecurity Education Platform and a Preliminary Assessment of Its First Application

Tim Yardley*, Suleyman Uludag†, Klara Nahrstedt* and Pete Sauer*
*U. of Illinois at Urbana-Champaign, {yardley,klara,psauer}@illinois.edu
†University of Michigan - Flint, Dept. of Computer Science, Eng. and Phy., uludag@umich.edu

***Abstract*—The energy sector worldwide has embarked on a transformational process to modernize the over-a-century-old power grid under an umbrella term of the Smart Grid. This vast infrastructural upgrade and operational change involves integration of a variety of advanced digital computing, communications and industrial control technologies. This brings new capabilities, but also necessitates a re-education of the aging workforce and training of the emerging workforce. While training does exist, the training approach and the accessibility of that training is often at odds with the needs of the utilities.**

To support this education and training need, in this paper we introduce the beginning of a modular, hands-on and open Smart Grid cybersecurity educational training platform and supporting materials together with an assessment of a preliminary version leveraged at the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Summer School held in 2013.

We base pedagogical pillars onto: (1) Active Learning that promotes analysis, synthesis, and evaluation of the content from Bloom's taxonomy, (2) The theory of project-based learning, (3) Piaget's learn-by-doing posture, and (4) Constructivist perspective of education. The main goal of this effort is to develop a complete, phased, and modular learning platform to provide the essential base knowledge and hands-on training exercises for understanding and demonstrating competency in Smart Grid cybersecurity.

I. Introduction

Across the globe, many national institutions have embarked on a transformational process to augment the over-a-century-old power grid under an umbrella term of the Smart Grid. Worldwide Smart Grid investment rose to $15 billion in 2013, according to Bloomberg Energy News Finance. This vast infrastructural upgrade involves integration of a variety of digital computing, communications and industrial control systems and technologies into a modernized and advanced power grid. A key constituent of the Smart Grid effort lies in the incorporation of the bidirectional flow of power (for distributed and renewable energy sources) as well as the two-way communications and control capabilities.

With the enhanced automation, computing, communications and control characteristics of the Smart Grid, a crucial need becomes apparent to address the plethora of security and privacy related challenges. The general term to refer to the aforementioned dimensions of the Smart Grid is *cybersecurity*. In terms of research and education, cybersecurity becomes an indispensable component and key enabler for the successful transformation from the electric power grid of yesterday into the Smart Grid of the future.

Even though there is no universally agreed-upon definition for cybersecurity, the following by ITU-T seems quite broad and comprehensive in its scope [1]:

> *Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.*

The essential nature of Smart Grid cybersecurity spans availability, integrity, and confidentiality of computing, communications, and/or control devices from intentional or accidental harm and damage. The severity of cybersecurity consequences in the Smart Grid is generally exasperated due to the complexity, sheer volume of the devices and stakeholders, and highly time sensitive operational constraints. The by-product of the imperative need to implement and adopt cybersecurity technology, both within the Smart Grid and beyond, has revealed tenuous vulnerabilities of systems, components, and people in both the private and public sectors under a variety of cyber-attacks. Safety in cyberspace continues to be an elusive objective [2], with the primary focus being placed on the infrastructural upgrades.

Education and workforce development have been called out repeatedly, but less effort has been placed to address those needs. The Comprehensive National Cybersecurity Initiative of President Obama identifies cybersecurity as the most serious economic and national security challenge. The National Science and Technology Council with the cooperation of the National Science Foundation recommended a broad, coordinated federal strategic plan for cybersecurity research, training and education to bolster preparedness, to establish a science of cybersecurity, and to transition promising cybersecurity research into practice [3]. Another national initiative: [4] The National Initiative for Cybersecurity Education (NICE) has evolved from the Comprehensive National Cybersecurity Initiative, and extends its scope beyond the federal workplace to include civilians and students in kindergarten through post-graduate school. The goal of NICE is to establish an operational, sustainable and continually improving cybersecurity education program for the nation to use sound cyber practices that will enhance the nation's security. One of the main conclusions of the National Research Council of the National Academies on "Professionalizing the Nation's Cybersecurity Workforce?" report [5] is the need for increased both the capacity and capability of the cybersecurity workforce. As for the workforce demand for cybersecurity graduates, many related professions display significant growth opportunities for the next decade as reported by the US Department of Labor's Bureau of Labor Statistics (BLS) Occupational Outlook Handbook [6]. For example, Information Security Analyst employment is expected to grow by 40% by 2022.

To the best of our knowledge, a coherent path of directed training from entry to expert level topic areas is missing and this is where our educational endeavor will be contributing by means of a modular and adaptable Smart Grid cybersecurity training platform that can be built upon and leveraged world-wide. Through three sessions of evolving TCIPG Summer Schools, we have identified gaps of knowledge, refined base necessities as educational building blocks, and recognized the need for adaptation in a rapidly changing sector. Through these lessons learned, this Smart Grid cybersecurity education platform under development will provide an adaptable basis by which undergrad students are equipped with the necessary knowledge, workforce can be trained, and researchers can be brought up to speed on the relevant topics to allow them to focus on their core research. In this paper, we report our initiative together with a preliminary assessment of first classroom use and discussion of a roadmap for the current work-in-progress expansions.

The rest of this paper is organized as follows: A overview of the Smart Grid, cybersecurity, and the need for its educational requirements are summarized in Section II. Section III presents the underlying theoretical basis of our work with respect to a set of well-known pedagogical frameworks. A summary of related work is given in Section IV. Details of the Smart Grid cybersecurity lab development are provided in Section V. Results and discussion of a preliminary assessment of an initial set of our cybersecurity lab modules are explained in Section VI. Concluding remarks and synopsis of future work are given in Section VII.

II. Background

A. The Smart Grid and Cyber Security

The Smart Grid is not as much a thing as it is an ideal. Starting from the electrical power grid of yesterday, the ideal is to transform it into the smart grid of tomorrow. This transformation is based on the premise that this modernized grid must be more reliable, secure, safer, more efficient, more economically matched, and environmentally friendly. This is to be realized through increased observability and control, bidirectional communication for demand-response, enhanced protection mechanisms for both resiliency and security, more diversification through distributed energy resources, and more adaptive response in the mechanisms by which the power is delivered and consumed.

The electric power grid of the United States has undertaken a monumental modernization and expansion effort, bringing in new technologies and working towards securing existing deployed technology. With this modernization, comes the need for a workforce that both understands the new technology and that can effectively and efficiently use that technology to advance the state of art in the grid. While there are several approaches to training that have been created, there is a lack of easily accessible, comprehensive, and modularly adaptable training in this area.

It is well-accepted that the US lags behind in math and science literacy rates among the 34 member countries in the OECD (Organization for Economic Co-operation and Development) as corroborated by the Science and Engineering Indicators of the National Science Board findings. A report by The 2012 President's Council of Advisors on Science and Technology (PCAST) [7] states that approximately 1 million more Science, Technology, Engineering, and Mathematics (STEM) graduates than expected are needed under the current assumptions.

The situation of the field of cybersecurity within the general STEM education base is no different. Without effectively trained personnel in cybersecurity topics, the electric power grid of the United States could be left vulnerable to attack. Since the act of electrification has been so pivotal in the advances of society, the impact of that resource going away could be catastrophic. Therefore, due to such great importance, the electric power grid is both a high-value target and a critical asset to adequately protect. However, even with some of the most advanced cybersecurity protections in place, humans are still part of the loop and must both understand and effectively operate the cybersecurity mechanisms going forward. Failure to do either of those could result in either attrition of the protection mechanisms or complete failure in the ability to detect, defend, and respond to attacks on that critical infrastructure.

B. Inadequacies in Current Training Approach

Without effective and efficient cybersecurity training in the relevant areas, the existing and emerging workforce will be inadequately prepared to detect and defend attacks against critical infrastructure attacks. While it is nearly impossible to actually quantify the potential incurred losses, those losses could come in the form of financial impact, business reputation, or even widespread loss of life through the failure to protect critical infrastructure. All important stakes to prepare for and defend against.

Current training consists of courses that are run across the span of 2-5 days on average and generally conducted at remote locations. For some training providers, those courses can be brought in-house for extra fees. However, when looking at the coverage of cybersecurity training in comparison to the emerging Smart Power Security Professional (SPSP) [8] designation and the related National Initiative for Cybersecurity Education (NICE) [4] competencies and roles/responsibilities, these courses have yet to cover the full needs of the sector.

Further, these courses suffer from being somewhat monolithic and therefore a cybersecurity professional must take several courses to get the full coverage that they need, and waste time overlapping information across those many courses. This was further complicated by the lack of an easy way to determine what each course covers and how that maps to the needs of the sector.

In this work we evaluate work undertaken to correct some of these issues and make progress towards a maintainable long-term solution for this sector. This is accomplished through developing a modular training platform that aims to address the cybersecurity needs of the sector while allowing for minimized overlap on the body of knowledge. As a stop gap measure, a full crosswalk and gap analysis was done on existing material to determine coverage and mapping to the emerging standards for cybersecurity education in this sector and broadly [9].

Since cybersecurity professionals are in short supply across many sectors, this modular approach to training could be essential to widespread multi-sector addressing of this deficiency. Without such an approach, the many sectors that are relying on having adequately training cybersecurity professionals may suffer due to the lack of available training, resources, or the effectiveness and efficiency of conveying the necessary knowledge to the incoming workforce to adequately prepare them for the jobs they are undertaking. By creating training in this modular way, the sector may leverage the training piece-wise and choose to cover only the topic areas that are necessary for each particular entity.

This effort is a foundational step towards the creation of such a comprehensive coursework and draws from many years of lectures in this domain. By leveraging the prior work, it is anticipated that the effort will be bootstrapped effectively and allow for refinement rather than gross content creation. Further, this existing material has been utilized for a number of years and has been vetted by a number of experts in the field to verify that the information being presented is not just topical, but also correct.

III. Pedagogical Framework

We base pedagogical pillars of our approach onto:

1) Active Learning : As coined by Bonwell and Eison [10], active learning promotes analysis, synthesis, and evaluation of the content from Bloom's taxonomy [11] of the cognitive domain. We aim at shifting the students from the state of passive learners to the level of active learning by engaging them with re-affirming demonstrations of the topic material and through intensive lab exercises.
2) Project-based Learning (PBL): The theory of project-based learning methodology is introduced by Blumenfeld [12]. We believe that fostering student engagement and longer lasting learning are achieved by combining student interest with a variety of challenging, authentic and real-world problem-solving tasks.
3) Piaget's learn-by-doing posture: Piaget's [13] emphasis on learn-by-doing, especially in science, is another pillar of our approach.
4) Constructivism : We are inspired by the Constructivist perspective [14] of education that emphasizes experiential learning. As nicely summarized by Tobin in [15], students need opportunities to internalize the learning by means of experience. Lab exercises naturally fit to the task of letting students learn with understanding and constructing knowledge.

The main goal of our effort, thus, is to develop a complete, phased, and modular learning platform to provide the essential base knowledge and hands-on teaching [16] by means of exercises for understanding Smart Grid cybersecurity. This platform builds upon the vast domain expertise of many years of directed research effort in Smart Grid cybersecurity, leveraging both the knowledge base and the research platforms that TCIPG has built along the way.

IV. Related Work

As we have elaborated in the previous sections, there is a strong need for cybersecurity educational material for use in the classroom. There are some books: Business-oriented, non-technical books [17]–[19]; policy-focused [20]; technical and management-oriented [21]–[24], technical [25], [26], and a collection of academic papers [27]. However, to the best of our knowledge, there is none that is suitable for a textbook or that lends itself to a modular and self-supporting approach, or with any set of lab exercises for the classroom.

There are also some efforts to offer Smart Grid cybersecurity courses in academia. Some only have a small section for cybersecurity within the Smart Grid domain [28]–[30]. The closest to our conception of labs is offered at Washington State University [31] or Iowa State's Short Course [32]. However, based on its syllabus, the course content does not have much in the form of labs nor a strong focus on training towards the needs of the professionals in the sector.

In addition to the books and academic coursework, professional training courses exist that attempt to prepare students and professionals for careers in the emerging Smart Grid cybersecurity domain. This includes the Global Information Assurance Certification (GIAC) newly launched certification program known as the Global Industrial Cyber Security Professional Certification (GICSP) [33] which is designed to assess a specific body of knowledge thought to be representative of the necessary knowledge in this sector. To accomplish training in this sector various approaches exist, including 1) Samurai SCADA security course [34]; 2) Cybati's Critical Infrastructure and Control System Cybersecurity course [35]; 3) SCADAhacker's Industrial Control System Cyber Security Training course [36]; 4) SANS ICS410 ICS/SCADA Security Essentials [37], and 5) Cimation's ICS/SCADA Security courses [38]. An analysis of coverage and mapping to sector needs has been addressed as part of this work and is available online [9] and in graphical form in Figure 3.

There are also other cyber-physical power system testbeds that exist in national labs, academia, and industry. However, while testbeds such as [39] provide a cyber-physical testbed for research utilizing power system hardware and software they are focused on research purposes and do not have the adaptability and reconfigurability to be leveraged for this type of education based training. The TCIPG testbed [40] predates the other academic testbeds by several years, having been formed in 2006 and details published in 2009. While the physical manifestation of the testbed is useful, the technology developed to configure and adapt it at will is essential to the type of flexibility needed for education and training.

V. Smart Grid Cybersecurity Labs

A. Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)

Researchers from the University of Illinois at Urbana-Champaign, Dartmouth College, the University of California at Davis, and Washington State University came together to form TCIPG and address the challenge of how to protect the nation's power grid by significantly improving the way the power grid infrastructure is built, making it more secure, reliable, and safe. This Department of Energy-funded project, with support from the Department of Homeland Security, recognizes that today's quality of life depends on the continuous functioning of the nation's electric power infrastructure, which in turn depends on the health of an underlying computing and communication network infrastructure that is at serious risk from both malicious cyber attacks and accidental failures. These risks may come from cyber hackers who gain access to control networks or create denial of service attacks on the networks themselves, or from accidental causes, such as natural disasters or operator errors.

TCIPG is addressing trust issues in the next-generation power grid cyber infrastructure, and has developed education and training material as well as a large-scale cyber-physical testbed to facilitate that research. This testbed provides a proving ground that validates technologies before commercialization, as well as forming the basis around which much of the research is accomplished. The main purpose of the testbed facility is to serve as a realistic, flexible, configurable, and easily customizable environment that enables innovative research, and subsequently education, in end-to-end trustworthy power system communications and control. The facility uses a mixture of commercial power system equipment and software, hardware and software simulation, and emulation to create a realistic representation of the electric power grid. That representation can be used to experiment with next-generation technologies that span communications from generation through consumption and everywhere in between. In addition to offering a realistic environment, the testbed facility is instrumented with the latest research and commercial tools to explore problems from multiple dimensions, so that researchers can tackle in-depth security analysis, testing, visualization, data mining, leverage federated resources, and develop novel techniques for integrating these systems in a modular way.

B. Cybersecurity Lab for the Smart Grid

The knowledge acquired over the past nine years through operating the TCIPG center and the corresponding testbed has allowed for the creation of training and education material on a wide variety of Smart Grid topics. Having platforms for research is a strong step forward, but enabling those platforms to facilitate education is another complex step. Towards this goal, TCIPG created a hands-on SCADA security module that was taught at their bi-annual TCIPG Summer School in June 2013. This Summer School focuses on providing cutting-edge education in Smart Grid systems ranging from fundamentals through advanced topics. The aim is to provide a comprehensive high-intensity and in-depth survey of the space that leans towards cutting edge topics in Smart Grid cybersecurity enabling researchers, practitioners from both vendors and utilities, as well as government to rapidly acquire the necessary domain knowledge surrounding cybersecurity in the Smart Grid.

This Summer School has been conducted three times with new course material presented at each instance. This material covers a variety of topics that are essential to understanding the Smart Grid and then further to work towards securing and protecting it. The hands-on SCADA assessment lab built a lab-based environment that mimics a general small electric utility (such as a cooperative or municipality) that is attempting to be proactive by securing their infrastructure. That company, *TCIPGco*, is at the center of the scenario. TCIPGco is a fictional utility for which the students in the exercise conducted a three-stage assessment, looking to accomplish specific security related goals. The goals were designed to reinforce the skills that are conveyed in the presented material and designed to help gain a fundamental understanding of the types of techniques and tools that are used in an ethical assessment.

Although TCIPGco is a fictional company and a virtual scenario, the details of which were manipulated and tailored for educational value, the techniques and discoveries that came up as that scenario played out are representative of real issues that could be seen in the field. Emphasizing the impact of information disclosure and lack of fundamental security as a culture that can result in systemic security failures.

The types of topics covered in that course include 1) Ethical approach to assessments, 2) Enumeration techniques, 3) Assessment techniques, and 4) SCADA specific manipulation and assessment. Through these topics, attendees both learned new material and engaged those new skills through discovery and application to accomplish targeted goals. This allows the attendees to explore cyber security provisions and to understand how choices, human behavior, deployment issues, and other real world situations influence the security of the system and ultimately determine the efficacy of the security measures that are protecting it.

In going through this hands-on course, students engage in a phased approach that teaches them particular skills and then allows them to apply those skills as they work through understanding and assessing the target fictitious utility. They learn about cybersecurity topics and tools as well as information about the company, its people, and the reality of deploying security in a utility. In these exercises, everything is representative of real-world scenarios, but at no point is anyone taught actual exploitation of critical infrastructure. They merely leverage the skills and tools to attack a system that is comprised of representative, but not vendor specific, implementations of a control system.

C. Roadmap

Specialized training is traditionally a money-driven and mission-oriented business, focused on bringing a particular audience up to speed with the intended knowledge. This approach, while sometimes quite effective, does not put the material into the hands of the broad general public instead limiting it to those that can afford to pay for the often costly training. This often does not include public entities or academia, as the training tends to be out of reach of most of those participants. Further, it necessitates the direct involvement of subject matter experts to actively teach the topic areas which therefore is limited by instructor availability both in location and timing. In many cases, this material is just a derivation of prior material from another sector that is adapted slightly for the new domain. While adaptation can be effective, it is not an optimal solution for something as specific and critical as the electric power grid.

This project feeds into work that aims to change the training landscape by making self-standing and self-paced training that is openly available and easily modifiable. Further, the focus on a modular approach that encourages use and extension to suit each target audience provides strong flexibility. This also builds on the lessons learned from the existing TCIPG training sessions and the hands-on exercises that were created as part of the TCIPG Summer School.

Since the intent is to leverage this work and its corresponding analysis to create coursework in an open realm, this output will help reduce the cost of training broadly and increase the availability of material that helps convey the appropriate body of knowledge. To realize this, the current curriculum will be expanded, which will focus on the what and how part of the equation. By this, we mean that there is a lot of time spent by various organizations on training people on the skills and tools that are involved in cybersecurity, but little time spent at actually understanding the fundamental premise behind those tools or skills. In academia, there is often a focus on the fundamentals and theories, but not necessarily the application and transition to practice of those theories. This material aims to bridge that gap, explaining the subject areas, the necessary fundamental concepts to address those areas, and what the remaining research or operational problems are in the space that have yet to be fully solved.

These areas are to be explored through both slide material and hands-on exercises that re-affirm the competency in the subject matter while showing the application of that expertise in the particular domain. This will further reaffirm the skill sets while bringing the fundamental concepts to bear in actual application.

VI. Preliminary Assessment

A. TCIPG Summer School

The TCIPG Summer School is a bi-annual event that is organized by the members of TCIPG. It combines academic researchers with members of Industry to teach pertinent topics on Smart Grid cybersecurity in a tightly packed week-long event. This event has been executed three times over the past several years and has been hugely successful. The summer school complements research and other educational activities at TCIPG, which is funded by the U.S. Department of Energy and U.S. Department of Homeland Security.

More specifically, the TCIPG Summer School program is designed to provide an essential background in the basics of security and resiliency for cyber infrastructure in power and smart grids. Participants gain an understanding of the smarter energy systems evolving from the power grid, as well as associated cybersecurity challenges of those systems. Experts from industry, national labs, academia, and government lead sessions that include industrial case studies and examples from current research that highlight the challenges and advanced topic areas of the modernized electric power grid. A Lightning Talk Session is also held that features 5-minute pitches from select summer school participants about bold, new ideas for research activities, products, or outreach. Deep dive sessions are also conducted that partner industry and academic experts to explore critical security topics in depth. In addition to all of that material covered, the hands-on SCADA (supervisory control and data acquisition) security assessment training lab is also offered to a limited number of participants on a first-registered, first-served basis.

B. Lab Session

TCIPG researchers created a portable lab that was brought to the Summer School, providing extended training sessions on ethical security assessment. Training was delivered using a platform designed to provide controlled exposure to SCADA communication mechanisms and systems that are currently the subject of research in the TCIPG testbed. Instructors provide demonstrations and training on assessment tools that are widely used or are in some cases under development in the TCIPG program. The training is built around a hands-on exercise that allows participants to apply what they have learned in a controlled three phase environment.

The hands-on lab ran for 6 hours and covered a variety of topics including 1) Ethical approach to assessments, 2) Enumeration techniques, 3) Assessment techniques, and 4) SCADA specific manipulation and assessment. These topics were covered in three phases of the scenario to allow researchers to build upon their knowledge base and leverage their acquired skills to get further in the specific goals than they could previously without those skills. The goals were varied, including gathering information, leveraging that information to gain control of an asset, reversing encryption schemes, and determining system-wide operation to modify the process or disrupt its operation.

The response to the lab was so great, that the Summer School ended up running three full labs, with some additional spillover rather than the originally planned two courses. Each participant was organized as part of a team, consisting of roughly 8 participants per team. This team based approach was chosen to both facilitate the affirmation of the newly acquired skills as well as building upon the strengths and weaknesses of each participant to form teams that were adequately equipped to solve whatever problems they may need to tackle.

Students were required to bring a laptop, and then leveraged remote desktop connectivity to the portable lab environment that set up a fully contained TCIPGco company instance for each team. A TCIPGco instance consisted of seven virtual machines that were running on a VMWare vSphere server. The TCIPGco instance was broke up into a corporate environment, engineering network, and SCADA network with separation between each of the zones. In the environment, there was a mixture of Windows and Linux systems that allowed the company to carry out its business and the employees the ability to monitor and manage the control system to operate appropriately.

In the SCADA zone, a small environment was created that was representative of a SCADA control system, with monitoring and relay components that were visualized and controlled via a Human Machine Interface (HMI). These components were created from scratch and leveraged their own simple communication protocol for moving data back and forth. The realities of power grid modernization were also in effect here by having TCIPGco in the middle of a security overhaul where the company was adding encryption to the communications protocol and securing other parts of the infrastructure. Just like the real world, these modernizations and transitional phases can result in oversights or misconfigurations. These issues are part of what the class teaches attendees to detect and understand, and then to ultimately leverage to aid in accomplishing goals of the security assessment.

The portable environment cost approximately $15,000 and consisted of a 2U rack-mount server that had 24 effective processors and 512GB of RAM, along with various support resources and network infrastructure. This system virtualized out the TCIPGco environment, setting up a dedicated learning environment for each team, making sure that no individual team would overlap with another. To handle this, the environment setup and manipulation were automated to allow for easy and quick environment setup, reset, and transitioning from phase to phase. The implementation of the SCADA environment was designed to be flexible and allow for easy manipulation of behavior to facilitate future changes. Further, systems in the instance had various patch levels to both allow for machine compromise and to show the reality of patch management affecting security.

All of the participating teams and their supporting virtualized infrastructure were separated out to provide full network isolation from each other. This was done by leveraging at least one VLAN per team along with IP subnetting. The networking was provided from a single core switch which then connected out to unmanaged switches in a hub and spoke model that provided the final connectivity to the participants.

Various back-end systems were in place to both provide the connectivity and to stage the phases of the scenario that were being executed. As mentioned, the environment was scripted out to automate the setup and tear-down, and a set of firewall scripts were created to represent topology variations to the end users as they garner new footholds on the systems. These tools allow for the rapid setup, configuration, variation, and adaptability of the architecture.

C. Assessment

Q1. The amount of material covered was adequate,
Q2. The material was relevant and useful,
Q3. The material was too challenging,
Q4. The instruction team did a good job of presenting the material,
Q5. The instruction team addressed audience questions well,
Q6. The instruction team provided good hands-on assistance,
Q7. Overall Lab Satisfaction.

TABLE I
SURVEY QUESTIONS GIVEN TO THE UIUC TCIPG SUMMER SCHOOL LAB PARTICIPANTS.

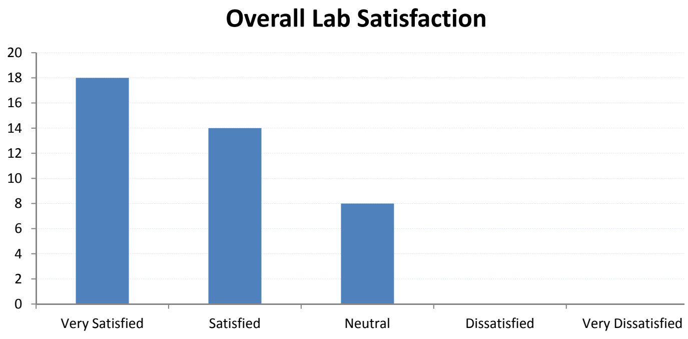

Fig. 2. Overall lab satisfaction, Q7.

D. Discussion

While the evaluation of the hands-on course was not exceptionally deep, the survey provided a basis for understanding the acceptance of the approach and how amenable the attendees were to this format. Future efforts will allow for more detailed observation as the efficacy of this approach and for the creation of competency-based assessment of the knowledge conveyed.

Some of the material that was created as part of the TCIPG Summer School and other TCIPG related activities have also been re-purposed into other forms. For instance, for two years now, pieces of the material have been used to teach a special

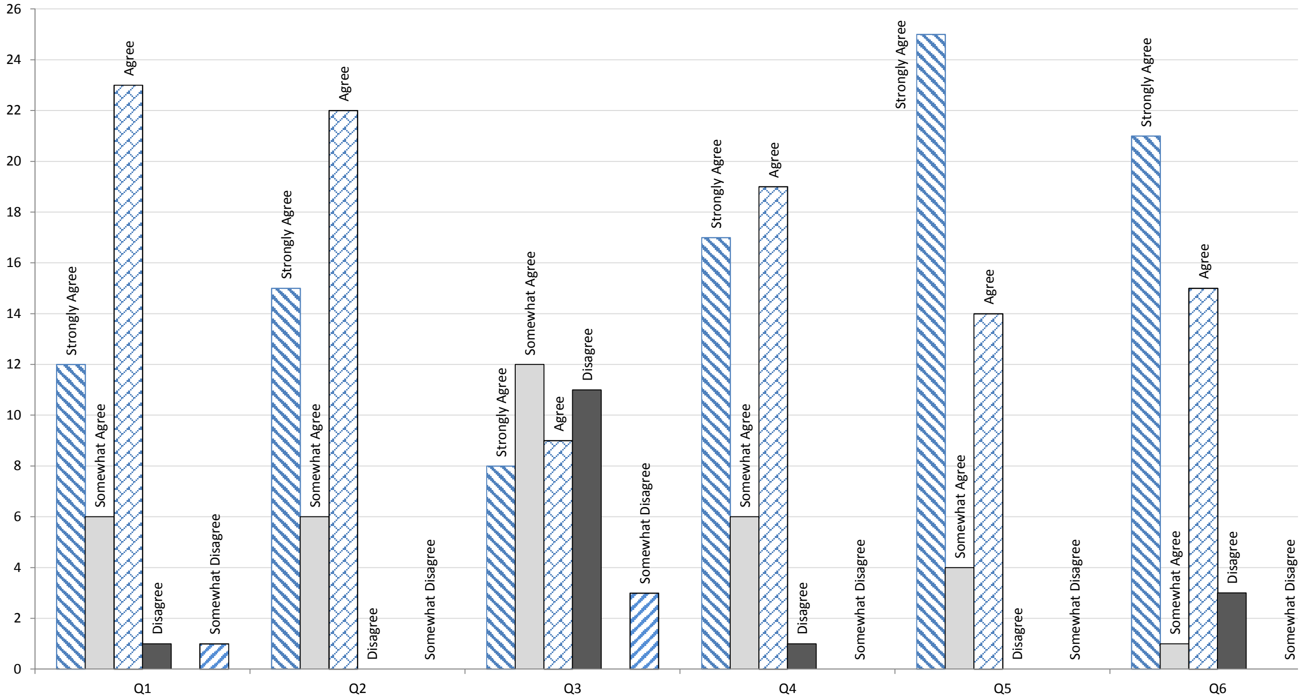

Fig. 1. Questions 1 through 6.

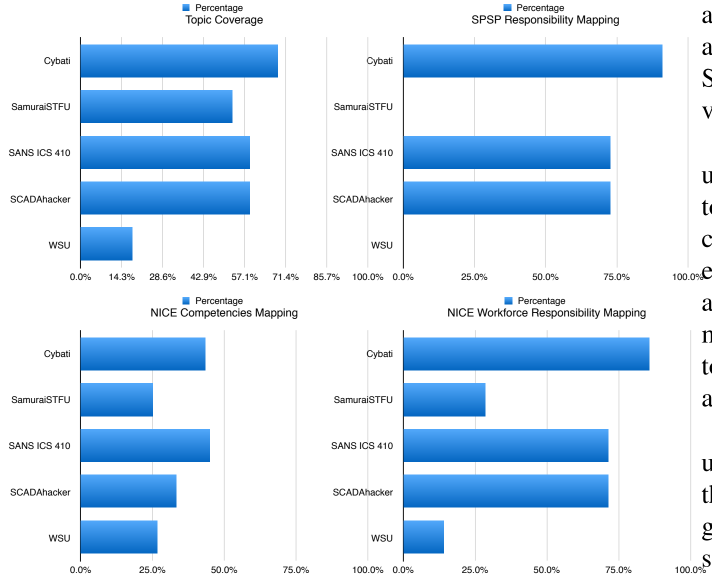

Fig. 3. Mapping of Existing Training

topics section of the University of Illinois Urbana-Champaign CS463 Computer Security II course. This special topics section involves two lectures on Smart Grid cybersecurity topics and has been very well received as a topic area for the course. Analysis of the material usage in that class is ongoing and each year feedback is utilized to determine popular topics and areas of needed improvement. Other pieces of material have also been leveraged for topic areas surrounding privacy in the Smart Grid and its implications to hot-topics in privacy across various industries.

Beyond the academic settings, the material has also been used to give short-courses to IEEE PES members, as well as to DOE and DHS program managers. The aim of these short-courses was to provide some background knowledge and to explore the domain with particular topics of interest to the audience, allowing them to understand those topic areas at a mid-level of detail and determine the mapping between those topic areas, the problems they have, and the solutions that they are overseeing the creation of.

All of the re-use of the material, and the intended primary use of the material have been very well received. The fact that the material has been adapted in so many ways already goes to show that the material is fairly flexible already. This supports the desire to further refine and expand the content and supports the mission of creating an open, modular, and widely available coursework.

VII. Conclusion and Future Work

This preliminary work has been shown to be modular and adaptable in practice. Even more importantly, it has been shown to be very effective at conveying the necessary topic areas and solidifying expertise in those areas that provides a base for further expansion. It is further based on the pillars of pedagogy of active learning, project based learning, Piaget's learn by doing posture, and constructivism approaches.

Our hope is that this core material will continue to grow and provide applicability to a variety of entities. The follow-up work of this effort will aim to provide both a cohesive body of knowledge while also being modular and adaptable to various audiences. The existing material will be further reworked and expanded to form the core of this curriculum when combined with the hands-on exercises that reinforce the material at hand. We are also planning to conduct extensive evaluation of the labs in a variety of settings, to analyze the results and report them in future publications. There is intent to release the initial content, an archive of video lectures, and related activities by the end of this year with a subsequent update pushed out thereafter with the above-mentioned updates.

Finally, all of the coursework and its supporting exercises are planned to be released to the world utilizing an openly available licensing scheme. There is already traction for this work to be utilized as the basis for future courses, training efforts, and education throughout the world.

VIII. Acknowledgment and Disclaimer

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000097.

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

References

[1] International Telecommunication Union (ITU). ITU Telecommunication Standardization Sector (ITU-T), Definition of cybersecurity. *accessed April 25, 2014*. [Online]. Available: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[2] V. G. Cerf, "Safety in cyberspace," *Daedalus*, vol. 140, no. 4, pp. 59–69, Sep 2011.

[3] National Science and Technology Council. (2011, December) Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program. *accessed April 25, 2014*. [Online]. Available: http://j.mp/1rs0dXC

[4] The National Institute of Standards and Technology (NIST) NICE. (2012) The National Initiative for Cybersecurity Education (NICE). *accessed April 25, 2014*. [Online]. Available: http://csrc.nist.gov/nice/framework/

[5] National Research Council, *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making*. The National Academies Press, 2013, Committee on Professionalizing the Nation's Cybersecurity Workforce: Criteria for Future Decision-Making; Computer Science and Telecommunications Board; Division on Engineering and Physical Sciences; National Research Council. [Online]. Available: http://www.nap.edu/openbook.php?record_id=18446

[6] US Department of Labor, Bureau of Labor Statistics (BLS). (2014) The Occupational Outlook Handbook (OOH). *accessed April 25, 2014*. [Online]. Available: http://www.bls.gov/ooh/home.htm

[7] The President's Council of Advisors on Science and Technology (PCAST). (2012, February) Engage to Excel: Producing One Million Additional College Graduates with Degrees in Science, Technology, Engineering, and Mathematics. *accessed April 25, 2014*. [Online]. Available: http://j.mp/1rs3xC6

[8] Pacific Northwest National Laboratory. (2014) Secure Power Systems Professionals (SPSP). *accessed June 25, 2014*. [Online]. Available: http://securepower.vivosuite.com

[9] Tim Yardley. (2014) A Gap Analysis of Cyber Security Training in the Smart Grid. *accessed June 25, 2014*. [Online]. Available: https://github.com/timyardley/training

[10] C. C. Bonwell and J. A. Eison, *Active learning : creating excitement in the classroom*. George Washington University, ERIC Clearinghouse on Higher Education, Washington, DC :, 1991.

[11] B. S. Bloom and D. R. Krathwohl, *Taxonomy of Educational Objectives, Handbook 1: Cognitive Domain*. Addison Wesley Publishing Company, October 1956.

[12] P. C. Blumenfeld, E. Soloway, R. W. Marx, J. S. Krajcik, M. Guzdial, and A. Palincsar, "Motivating project-based learning: Sustaining the doing, supporting the learning," *Educational Psychologist*, vol. 26, pp. 369 – 398, 1991.

[13] J. Piaget, H. Gruber, and J. Vonèche, *The Essential Piaget*, ser. Harper colophon books. Basic Books,Incorporated, 1982. [Online]. Available: http://books.google.com/books?id=yRjeKgAACAAJ

[14] E. Ackermann, "Piaget's constructivism, papert's constructionism: What's the difference?" in *Constructivism: Uses and Perspectives in Education Conference Proceedings*, [September] 2001, pp. 85–94.

[15] K. Tobin, "Research on science laboratory activities: In pursuit of better questions and answers to improve learning," p. 403–418, 1990.

[16] D. Haury and P. Rillero, *Perspectives of Hands-on Science Teaching*. ERIC Clearinghouse for Science, Mathematics and environmental education, 1994. [Online]. Available: http://books.google.com/books?id=x3OAGwAACAAJ

[17] E. Knapp and R. Samani, *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*. Elsevier Science, 2013. [Online]. Available: http://books.google.com/books?id=_9GzAzehLLUC

[18] J. Weiss, *Protecting Industrial Control Systems from Electronic Threats*. Momentum Press, 2010. [Online]. Available: http://books.google.com/books?id=ugOsO17iHB8C

[19] W. Shaw, *Cybersecurity for SCADA Systems*. PennWell Corporation, 2006. [Online]. Available: http://books.google.com/books?id=EyZVJ8KI8C0C

[20] R. Radvanovsky and J. Brodsky, *Handbook of SCADA/Control Systems Security*. Taylor & Francis, 2013. [Online]. Available: http://books.google.com/books?id=FMDTSr63co4C

[21] T. Macaulay and B. Singer, *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*. Taylor & Francis, 2012. [Online]. Available: http://books.google.com/books?id=YBM3cwTNwj0C

[22] T. Flick and J. Morehouse, *Securing the Smart Grid: Next Generation Power Grid Security*. Elsevier Science, 2010. [Online]. Available: http://books.google.com/books?id=8Z9O8lhTSlsC

[23] I. Reid and H. Stevens, *Smart Meters and the Smart Grid: Privacy and Cybersecurity Considerations*, ser. Energy Policies, Politics and Prices: Privacy and Identity Protection. Nova Science Publishers, Incorporated, 2012. [Online]. Available: http://books.google.com/books?id=U2EMuwAACAAJ

[24] P. Barker and R. Price, *Cybersecurity for the Electric Smart Grid: Elements and Considerations*, ser. Energy Science, Engineering and Technology Energy Policies, Politics and Prices Series. Nova Science Publishers, Incorporated, 2012. [Online]. Available: http://books.google.com/books?id=RwfiygAACAAJ

[25] G. Sorebo and M. Echols, *Smart Grid Security: An End-to-End View of Security in the New Electrical Grid*. Taylor & Francis, 2012. [Online]. Available: http://books.google.com/books?id=H6ISH6uTOCwC

[26] H. Li, *Enabling Secure and Privacy Preserving Communications in Smart Grids*, ser. Springer Briefs in Computer Science. Springer, 2014.

[27] Y. Xiao, *Security and Privacy in Smart Grids*. Taylor & Francis, 2013. [Online]. Available: http://books.google.com/books?id=QQ2oY0IrRM8C

[28] V. Namboodiri and V. Aravinthan, "On the design of a graduate-level cross-disciplinary course on smart grids," in *Power and Energy Society General Meeting, 2012 IEEE*, July 2012, pp. 1–2.

[29] M. Shahidehpour, “Smart grid education and workforce training center,” in *Innovative Smart Grid Technologies Asia (ISGT), 2011 IEEE PES*, Nov 2011, pp. 1–3.

[30] J. Momoh, *Smart Grid: Fundamentals of Design and Analysis*, ser. I E E Power Engineering Series. Wiley, 2012, Chapter 9: Research, Education, and Training for the Smart Grid. [Online]. Available: http://books.google.com/books?id=G3prlp3jD4QC

[31] A. Srivastava, C. Hauser, D. Bakken, and M. Kim, “Design and development of a new smart grid course at washington state university,” in *Power and Energy Society General Meeting, 2012 IEEE*, July 2012, pp. 1–2.

[32] Iowa State University. (2014) Short Course on Cyber Security of the Electric Power Grid with Attacks-Defense Training. *accessed June 25, 2014*. [Online]. Available: http://tinyurl.com/iowastshortcourse

[33] Global Information Assurance Certification (GIAC). (2014) Global Industrial Cyber Security Professional Certification (GICSP). *accessed April 25, 2014*. [Online]. Available: http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

[34] Utilisec. (2014) Assessing and Exploiting Control Systems with SamuraiSTFU. *accessed April 25, 2014*. [Online]. Available: http://www.samuraistfu.org/training-syllabus

[35] Cybati. (2014) Critical Infrastructure and Control System Cybersecurity. *accessed April 25, 2014*. [Online]. Available: https://cybati.org/education

[36] SCADAhacker. (2014) Industrial Control System Cyber Security Training. *accessed April 25, 2014*. [Online]. Available: http://www.scadahacker.com/training.html

[37] SANS. (2014) ICS410 ICS/SCADA Security Essentials. *accessed April 25, 2014*. [Online]. Available: http://www.sans.org/course/ics-scada-cyber-security-essentials

[38] Cimation. (2014) ICS/SCADA Security Courses. *accessed April 25, 2014*. [Online]. Available: http://www.cimation.com/training/

[39] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, “Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid,” *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2013.

[40] D. C. Bergman, D. Jin, D. M. Nicol, and T. Yardley, “The virtual power system testbed and inter-testbed integration,” in *Proceedings of the 2Nd Conference on Cyber Security Experimentation and Test*, ser. CSET’09. Berkeley, CA, USA: USENIX Association, 2009, pp. 5–5. [Online]. Available: http://dl.acm.org/citation.cfm?id=1855481.1855486