CySGS: Cyberlearning Environment about Smart Grid Security

Summer Prince
Tennessee Valley Authority
Chattanooga, TN 37402

Ambareen Siraj
Tennessee Tech University
Department of Computer Science
Cookeville, TN 38505

Abstract -The smart grid initiative is working to modernize the North American electric power grid utilizing computing technologies in efforts to increase efficiency, reliability, and security [6, 16]. While the national energy infrastructure's incremental evolution into a smarter grid continues to provide improvements, at the same time it is introducing security problems. The expanding adoption of the smart grid requires current and upcoming smart grid workforce to be aware of and understand specific security issues related to this domain. Educational institutions are frequently challenged to maximize existing resources for teaching the required curriculum, often leaving little to no resources available for teaching specialized courses such as smart grid security. The use of technologies for education provides a cyberlearning environment option for maximizing limited resources. To address the increasing national demand for smart grid security education, Cyberlearning Environment about Smart Grid Security (CySGS) was created to serve as an educational resource for the security community.

Index Terms - Security, Smart Grid, Cyberlearning, Smart Grid Security

INTRODUCTION

The smart grid remains a national priority and one of its main goals: creating a resilient, smarter grid [16]. One substantial source of the smart grid workforce will be the current generation of college students, and educating them in this domain requires dedicated courses and training. Most educational institutions do not have the resources for the establishment of security courses related to the smart grid. For traditional courses, textbooks remain the primary content driver. However only a limited number of textbooks are available in the specific area of smart grid security [13]. One reason is that smart grid security is a relatively new area. Another plausible reason is the rapid evolution of smart grid technologies, compounded by the dynamic nature of security requires authors and publishers of textbooks to update and revise content quickly to keep up with newer developments of problems and solutions in this field. The past decade has seen significant growth in the area of "cloud" web-based software, and so has increased web browser capabilities with users and servers. These changes provide opportunities for exploring alternative methods of education and an avenue of platform delivery to minimize demands on resources. One such solution is Cyberlearning, defined by the NSF as the use of "networked computing and communication technologies to support learning" [17]. Cyberlearning has been an increasing popular method of education and continues to evolve with the introduction of new technologies [7, 8, 9, 17]. Previous evidence that cyberlearning alternatives to learning in traditional courses have been successful [1, 2, 3, 4, 5]. Some benefits of a cyberlearning environment include:

- Integration of technologies and learning
- Anytime/anywhere access
- Interactive course content
- User platform independence
- Personalization of the learning experience

An additional benefit of the cyberlearning environment, in contrast to a traditional course environment, is the ease of dissemination. Traditional courses often require one faculty member to design and set up the

course material. While the course material may be presented online, it is not common for faculty members to have the actual course content available to the public, as courses are intellectual property of educational institutions. There is currently a growing smart grid security knowledge base. There are a few textbooks, some courses being taught in universities in the traditional platform, and conferences [13, 14, 15]. While there are strong efforts to continue research and development of smart grid security, the approach of using cyberlearning to teach smart grid security is currently minimally utilized. In this work, we have designed and developed this novel approach to smart grid security education through a cyberlearning environment to offer as a contribution to the smart grid security knowledge base.

RELATED WORK

Three disciplines of related work include cyberlearning, smart grid, and security. Related work in the area of smart grid education is considerably smaller than the areas of security and cyberlearning, however, each year it continues to grow. There are professional societies which host online smart grid education information such as the IEEE Smart Grid resources offering a range of materials including webinars, "Ask Me Anything" events, videos, interviews, and a newsroom [24]. Another resource for smart grid from an online platform is the U.S. Department of Energy that offers an interactive learning area covering smart grid basics, smart homes, renewable energy, consumer engagement, operations, distribution, and plug-in electric vehicles [25]. Through one of the most popular blogging platforms known as "The Smart Grid Security Blog", current informational post associated with smart grid security is provided [26].

Moving into a more focused area of related work in open online security modules is Security Injections @ Towson [10]. Security Injections offers Educational Modules specific to lower division security courses, like CS0, CS1 and CS2. Unlike CySGS, the Security Injections modules are not focused on the smart grid. Recently there have been adoption of open, online security courses by two established online educational resources providers: Udacity and Coursera [12, 11]. Udacity offers courses in security such as Applied Cryptography and Software Testing. Coursera offers security related courses with their Cryptography I, Cryptography II, Malicious Software and its Underground Economy, Designing and Executing Information Security Strategies, Information Security and Risk Management in Context, Building and Information Risk Management Toolkit, and Computer Security Courses.

While there is considerable work that exists inside of the cyberlearning space, and significant work in both computer science and information security, the combination of cyberlearning, smart grid, and security presents the need and opportunity for development and contribution of the cyberlearning environment about smart grid security education.

DESIGN

A. Educational Modules

CySGS is designed and developed with the primary goal of addressing the problem of educating the smart grid security workforce. The design of CySGS consists of seven Educational Modules each containing three sub-modules hosting a total of 109 exercises. These seven Educational Modules correspond to each of the smart grid domains defined in the NIST Smart Grid Conceptual Model [6]. To complete course, the student participants are required to complete all of the seven Educational Modules. After successfully completing CySGS, student participants receive a certificate of completion. Each Educational Module can be completed in any order and consists of three sub-modules: Learn, Engage, and Assess (Table 1.0).

CySGS is designed to be flexible to provide a platform that can adapt to changing trends in smart grid security. The individual Educational Module design is driven by the current trends in security and the smart grid. For example, there are Educational Modules focusing on mobile security, smart meters, and Supervisory control and data acquisition (SCADA) systems all of which are current high profile smart grid security topics. The Learn sub-modules provide a background and introduction to primary security topics in a corresponding smart grid domain. It contains Learning Objectives, Background, and other relevant information. The learning objectives are precisely focused on core concepts of the smart grid

domain and enable participants to map the domain concept with Confidentiality, Integrity, and Availability (CIA) aspects related to the subject area. This consistent learning theme is followed in CySGS to help exercise critical thinking. After completing CySGS, it is expected that a student participant presented with smart grid technology will be able to analyze how CIA is involved and impacted by the use and abuse of such technology. The following are the Educational Modules and the primary security topics covered in its Learn sub-module:

- Educational Module One (EM1) *Customer Domain*: Smart Meters/AMI
- Educational Module Two (EM2) *Bulk Generation Domain*: SCADA
- Educational Module Three (EM3) *Transmission Domain*: Monitoring Systems
- Educational Module Four (EM4) *Distribution Domain*: Web Service Application
- Educational Module Five (EM5) *Service Provider Domain*: Mobile Applications
- Educational Module Six (EM6) *Operations Domain*: Enterprise Applications
- Educational Module Seven (EM7) *Market Domain:* Retailing Vulnerabilities (Smart Meter Billing)

EM1 Learn sub-module uses smart meters/AMI as the selected topic of discussion because power meters are the most recognized component of the electrical power grid which is crucial and relatable. EM2 Learn sub-module uses SCADA as the primary security topic. While not as commonly known as smart meters, this topic is selected because of its significantly wide use through several smart grid domains. SCADA is a centrally controlled industrial control system driven by computing technology [23] and its presence is ubiquitous in the electrical power grid. Monitoring systems is used in EM3 Learn sub-module because while automating technologies is crucial in improving the smart grid, they require extensive supervision. Web service application is used in EM4 Learn sub-module as a topic due to the shift of application development from stand-alone application to web service/applications which reflects the increase in demand and use of two-way communication inherent in the smarter grid. Mobile application is used in EM5 Learn sub-module due to its high popularity. In EM6 Learn sub-module, Enterprise applications is the primary security topic because a lot of enterprise applications in the electric power industry were not designed with security in mind and are currently at risk when connected to network and exposed to the Internet. EM7 Learn sub-module uses retailing vulnerabilities/spoofing due to the common trend energy theft.

Sub-Module	Description
Learn	Contains learning objectives, background information, and introduction to smart grid security concepts.
Engage	Student research, active learning lessons and exercises with security mechanisms.
Assess	Questions derived from the CIA centered learning objectives and exercise concepts completed in the Engage sub-module to determine student's performance and to provide feedback to student participants.

Table 1.0: Sub-Module Functional Descriptions

Each Learn sub-module requires the student to do research into the suggested references as well as explore other current and trending resources for each of the primary security topics. The measureable outcomes for the learning objectives exist in the following Engage and Assess sub-modules. These sub-modules require the student participants to exercise active learning and to answer challenge questions specific to the smart grid domain under focus. The Engage sub-module provides the student participants with active learning exercises in the context of smart grid security.

The following are the Educational Modules and the active learning exercise topics in the Engage sub-modules

- Educational Module One (EM1) *Customer Domain*: Wireshark and Network monitoring
- Educational Module Two (EM2) *Bulk Generation Domain*: System Security Assessment
- Educational Module Three (EM3) *Transmission Domain*: Buffer overflow – Secure coding practices
- Educational Module Four (EM4) *Distribution Domain*: Application Security
- Educational Module Five (EM5) *Service Provider Domain*: SQLite Database Browser
- Educational Module Six (EM6) *Operations Domain*: DBMS networking vulnerabilities
- Educational Module Seven (EM7) *Market Domain:* Retailing Vulnerabilities: Smart meter billing fraud

EM1 Engage sub-module uses the Wireshark tool to introduce the topic of network monitoring and then applying it to the smart meters. In EM2 Engage sub-module, students work on a balanced approach to smart grid security requiring the student participants to have technical knowledge (secure coding, using technical tools such as Wireshark and SQLite), but also requiring analytical thinking for the security assessment of smart grid components such as SCADA. This exercise teaches students to ask questions involving access, privileges, identifying potential attackers, attack vectors, motivations for attacks, and understanding environments (testing vs. production). EM3 Engage sub-module explores buffer overflows which is one of the most common programming vulnerability. Flaws in software continue to be a primary root cause of modern information security vulnerabilities. Traditional information security curriculum often focuses on defining the flaw. This module provides more than the definition of secure coding but challenges the student participants to look at the fundamental elements of coding. The student participants are challenged to work with code samples in a smart grid context to flex their minds and understanding of a "real world" example. EM4 Engage sub-module uses application security knowledge and critical thinking when designing and developing new web application. This exercise provides highlights into application security for the more connected web service applications. EM5 Engage sub-module introduces the student to SQLite that is used to browse a smart grid mobile application database. EM6 Engage sub-module explores databases and database management systems (DBMS) that are the powerhouses of data storage behind most businesses. This exercise provides students with a high level task of determining the risk/value of smart grid DBMSs. Finally, EM7 Engage sub-module challenges the student to examine smart meter power bills (including information such as power usage and IP addresses) to determine if possible fraud is present.

B. Framework

Selecting appropriate technologies and tools for the framework was a challenge in creating the CySGS environment. The considerations were low cost, high scalability, high flexibility, and low course administration overhead. Most of the tools selected for the framework are cloud-based technologies. The framework cyberlearning technologies included Google Sites, Google Drive, Google Gmail, SubmitBox, Dropbox, SurveyMonkey, and Piazza. The course site is hosted on Google Sites. The course content is hosted on Google Drive. The main method of communication for grading is email. Given Google Drive does not allow uploading of content such as images, a second technology is used for assignment submission called SubmitBox [19] for Dropbox [20]. SubmitBox is a simplified learning management system that serves the primary function of storage and organization of uploaded student submissions. SubmitBox utilizes the Dropbox platform. Dropbox provides file-hosting cloud services with features such as file synchronization. For course evaluation, pre- and post-surveys through SurveyMonkey [21] is used. SurveyMonkey is a cloud based survey development service. Piazza [22] is used for a class forum. Piazza is another cloud-based service offering a Q&A platform through the combination of forums and information sharing. The approach used for the CySGS course is to have a 100% online experience where the students can work through the course material at their own pace for the duration of the course.

EPERIMENTAL DEPLOYMENT

For the purpose of evaluating CySGS as an effective approach to smart grid security education, a pilot course was administered in summer 2013 at Tennessee Tech University. The pilot course was offered as a free of cost learning opportunity primarily for university computer science students. The course was also open to any university students or recent alumni capable of introductory level programming. The amount of time required for course solicitation was minimal with established, effective college and department procedures being used. These procedures included the our university's research review board's approval [18], college and department level emails, targeted emails, course level announcements by instructors, and word-of-mouth. The enrollment interest pre-survey took less than four hours to draft, revise, publish, and distribute. The course post-survey took less than three hours to draft, revise, publish, and distribute. Enrollment of the students into the CySGS framework components took about 20.00 hours. In total about 70.00 hours was spent grading the Educational Modules, with an average of 0.875 hours spent per Educational Module. Approximately 20.00 hours was spent on email communication during the course. 30.00 hours was spent on revisions and adjustments to the pilot course content. The total administration time for the pilot course of CySGS was a little less than 162.00 hours and a breakdown of the CySGS administrative tasks and time spent in hours is represented in Table 2.0

Table 1.0: CySGS Administration Time Overhead Over Course Duration

Administration Task	Time in Hours
IRB process	5.00
Pilot course solicitation	10.00
Pre-survey	4.00
Post-survey	3.00
Pilot course enrollment	20.00
Grading	70.00
Emailing	20.00
Course content revisions	30.00
Total	162.00

RESULTS

A. Educational Module Completion

Of the 32 student participants enrolled in CySGS, there were eight students or 25% that successfully completed the course. From the post-survey results, the primary reason for not completing the course was lack of time. The pilot was offered during the summer semester and the students were enrolled on a voluntary basis with the course grade not being reported on their transcripts. With no commitment to complete this non-credit course offered in summer and other social/family obligations during that time, it is the likely reason why 75% who signed up initially did not complete all of the course material. Following is a detail account of completion statistics. All of the student participants that started the CySGS pilot but did not complete the course stated that although initially self-committed, they failed to make time for this course to complete since it would not have negative any impact on their transcript.

In total 14 student participants completed 62 Educational Modules in 137.26 hours. EM1 had the maximum number of 14 student participants complete the module. EM4 through EM7 being completed by eight student participants had the minimum number of completions. The student attrition rate for the pilot course was 43%. The Educational Module with the highest average amount of time to complete was EM2 at 2.46 hours. The Educational Module with the lowest average amount of time to complete was EM7 at 1.87 hours, which is 0.13 hours less than the design estimate target of 2.00 hours average time to complete one Educational Module. The average time for a student to complete one Educational Module

was 2.17 hours, which is 0.17 hours greater than the design estimate target of 2.00 hours average time for a student to complete one Educational Module. Figure 1.0 shows the average hours spent for all Educational Modules that each student participant completed. The student with the minimum average hours was student participant two with an average of 0.50 hours. The student with the maximum average hours was student participant three with an average of 4.86 hours.

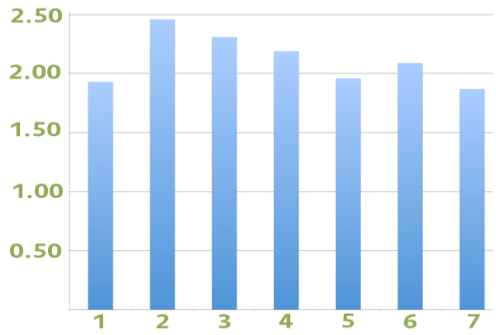


Figure 1.0: Average Learning Hours for All Educational Modules

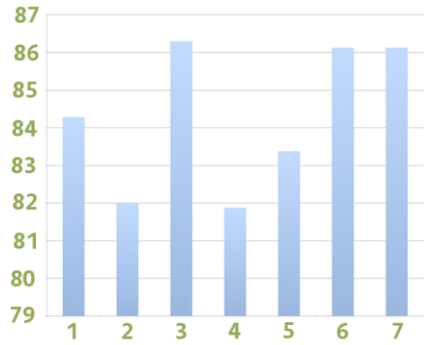


Figure 2.0: Average Student Grades for All Educational Modules

B. Evaluation

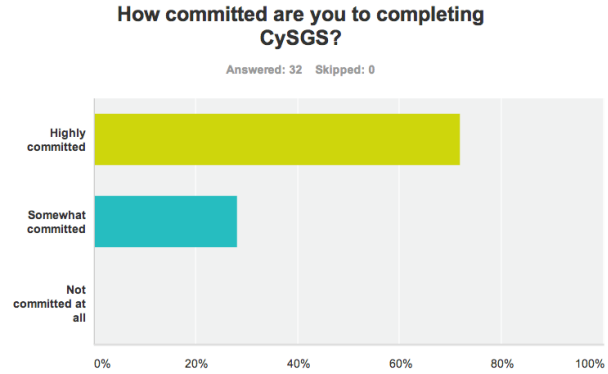
The quality and effectiveness of the course can be measured by engagement, performance and interest of the student participants. In this regard, we used student performance and pre/post survey results for the course.

1. Performance Results

To evaluate student performance, student grades in the in the Educational Module Assess sub-module were analyzed. The grading scale was based out of 100%. A grade above 70% was considered as a passing grade for the course and each Educational module. The course average was 84%. The minimum course grade was for any one Educational Module was 70% (Figure 2). The maximum course grade for any one Educational Module was 99%. The minimum average grade of 81.88% was for EM4. The maximum average grade of 86.30% was for EM3. There appears to be no relationship between the number of student participants that completed each Educational Module and the average grade of the Educational Module and in between the average time to complete the Educational Module and the average grade of the Educational Module. We were not able to correlate students' self-rated knowledge ranking with their actual grades because their individual IDs were not captured in survey design for later correlation. This is something that can be easily incorporated in future deployment of CySGS.

2. Pre-Survey

The pre-survey was completed by 32 student participants with 71.88% indicating they were "highly committed" to completing the pilot course. The levels of commitment results can be viewed in Figure 3.0. In the pre-survey results, the student participants were asked why they were participating in the course with the option to select multiple reasons (Figure 4.0). The top reason for participation in CySGS was personal interest in smart grid security answered by 87.50% of respondents. The next top reason was the course was accessible at no cost selected by 62.50% of respondents.



Answer Choices	Responses	
Highly committed	71.88%	23
Somewhat committed	28.13%	9
Not committed at all	0%	0
Total		32

Figure 3.0: Student Participant Commitment Level

Answer Choices	Responses	
My personal interest in the subject matter	87.50%	28
My advisor's interest	9.38%	3
Accessible at no cost	62.50%	20
Ability to learn at my own pace	46.88%	15
Ability to learn from anywhere	53.13%	17
Time to spare currently	37.50%	12
Total Respondents: 32		

Figure 4.0: Motivation for Student Participant

3. Post-Survey

Of the seven student participants who completed the post-survey (and completed CySGS), six were majoring in Computer Science. One graduate student, three undergraduates in Software & Scientific Application and the remaining two were information technology concentrations. One was a graduate student in electrical engineering. The comparison of pre-survey and post-survey results is shown below in Figure 5.0 through Figure 7.0. The responses for knowledge levels are ranked from lowest to highest knowledge level as follows: 1-Not Knowledgeable, 2-Slightly Knowledgeable, 3-Moderately Knowledgeable, 4-Knowledgeable, 5-Very Knowledgeable.

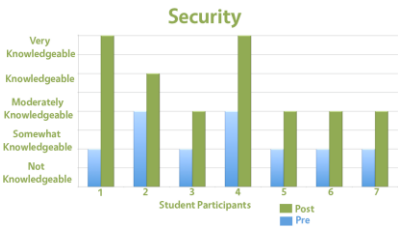


Figure 5.0: Self-Rated Security Knowledge

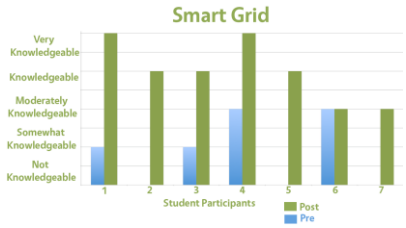


Figure 6.0: Self-Rated Smart Grid Knowledge

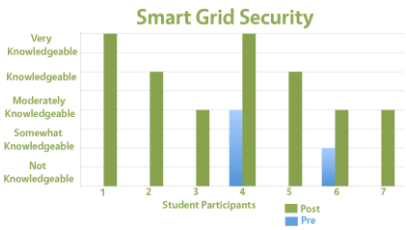


Figure 7.0: Self-Rated Smart Grid Security Knowledge

For the area of security, all student participants reported an increase of knowledge as shown in Figure 5.0. Overall, the minimum increase of security knowledge was observed in student participants two, three, five, six, and seven with all student participants reporting one level of increase in security knowledge. The maximum increase in security knowledge was observed in student participant one with an increase from Somewhat Knowledgeable to Very Knowledgeable. For the area of smart grid, six student participants reported an increase in knowledge as shown in Figure 6.0. Overall, the minimum impact of smart grid education was observed in student participant six with no increase in smart grid knowledge. Student participant six is a graduate student in electrical engineering with research experience in smart grid security. The maximum increase of smart grid knowledge was observed in student participants two and five with an increase from Not Knowledgeable to Knowledgeable.For the area of smart grid security, all student participants reported an increase in knowledge as shown in Figure 7.0. Overall the minimum increase in smart grid security education was observed in student participant six with one level of increase in smart grid security knowledge. Student participant six is a graduate student in electrical

engineering with research experience in smart grid security. The maximum increase in smart grid security knowledge was observed in student participant one with an increase from Not Knowledgeable to Very Knowledgeable. The area of smart grid security was observed to have the highest increase in the level of knowledge after completing CySGS with two student participants reporting having knowledge of smart grid security prior to CySGS. The area of the smart grid was observed to have the second highest increase in the level of knowledge after completing CySGS with four student participants reporting having knowledge of smart grid prior to CySGS. The area of security was observed to have the minimum increase in the level of knowledge after completing CySGS with all student participants reporting knowledge of security prior to CySGS.

CONCLUSION

CySGS provides a cyberlearning environment for smart grid security education with distinct learning objectives, dedicated exercises to engage the students, and assessment for the instructor to provide feedback on student performance. The results of the CySGS pilot course show evidence that a cyberlearning environment can be a useful method of teaching smart grid security. One limitation of the pilot course of CySGS results is the relatively small sample size. Also, the number of students responding to the post-survey for the pilot course was less than the number of students that actually completed CySGS. Nevertheless, the pilot course provided insight into the usefulness of the cyberlearning environment for smart grid security education as well as opportunities for improvements and future work.

FUTURE WORK

The primary area of improvement for CySGS is the platform of the framework. The feedback from students indicated a strong preference for a single platform as opposed to the multiple platform tools used in the pilot course. While the goal during this pilot study was to utilize low-cost and free tools, the number of tools that CySGS used was problematic for most students and increased the time for administration by the instructor. Future work can include development or adoption of automated grading and feedback to possibly reduce the amount of time spent on grading. Additionally, a mobile version of the course could increase the accessibility of the course expanding to smart phones and tablets. Given a procedure, platform, and the fact that core set of Educational Modules has been designed and developed, additional sub-modules can be created and added to CySGS with ease. While CySGS was designed to be taught without an in-person instructor, the Cyberlearning environment is adaptable to traditional course instruction given the instructing departments has available resources. CySGS can be taught 100% online, or a traditional face-to-face course, or blended. Similar to the scalability of the content of CySGS, the Cyberlearning environment can be flexible and adaptable to most educational needs depending on available resources. Since the core content of CySGS has already been developed, it allows educators in the community opportunities for further enhancements instead of creating the course from scratch.

REFERENCES

[1] Bier, N., Lovett, M., Seacord, R. (2011). "An Online Approach to Information Systems Security Education." Proceedings of the 15th Colloquium for Information Systems Security Education (CISSE). June 13 – 15, 2011, Fairborn, Ohio.

[2] Lovett, M., Meyer, O., Thille, C. (2008). "The Open Learning Initiative: Measuring the Effectiveness of the OLI Statistics Course in Accelerating Student Learning." Journal of Interactive Media in Education.

[3] Ryoo, J., Oh, T.H. (2008). "Teaching IP Encryption and Decryption Using the OPNET Modeling and Simulation Tool." Proceedings of the 12th Colloquium for Information Systems Security Education (CISSE). June 2 – 4, 2008, Dallas, Texas.

[4] Steif, P.S., Dollar, A. (2009). "Study of Usage Patterns and Learning Gains in a Web-based Interactive Static Course." Journal of Engineering Education 98, 4 321-333.

[5] Schunn, C.D., Patchan, M. (2009). An Evaluation of Accelerated Learning in the CMU Open Learning Initiative Course "Logic & Proofs." Technical Report by Learning Research and Development Center, University of Pittsburgh.

[6] United States. National Institute of Standards and Technology. Office of the National Coordinator for Smart Grid Interoperability. (2009). NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0.

[7] National Science Foundation. "Cyberlearning: Transforming Education." http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503581

[8] National Education Foundation. "Cyberlearning: A Project of the NONPROFIT NEF." http://www.cyberlearning.org/

[9] Cyberlearning. "Cyberlearning Research Summit". http://cyberlearning.sri.com/

[10] Towson University. Security Injections @Towson. http://cis1.towson.edu/~cssecinj/

[11] University of Pittsburg. Coursera. https://www.coursera.org/

[12] Udacity. https://www.udacity.com/

[13] Flick, T., & Morehouse, J. Securing the Smart Grid. Syngress Press.

[14] Smart Grid Security Summit. Energy & Power Cyber Security Summit.

[15] IEEE. Power and Energy Society. Innovative Smart Grid Technologies Conference.

[16] United States Congress (USC). (2007). Energy Independence and Security Act of 2007 (EISA). Washington, DC: 42 USC 17381.

[17] National Science Foundation Task Force on Cyberlearning. (2008). Fostering Learning in the Networked World: The Cyberlearning Opportunity and Challenge. Washington, DC: NSF.

[18] Omitted for anonymity.

[19] SubmitBox, https://getsubmitbox.com

[20] Dropbox, Http://dropbox.com

[21] Survey Monkey, http://surveymonkey.com

[22] Piazza, https://piazza.com

[23] IEEE. (2012). IEEE Communications Surveys and Tutorials. Introduction to Industrial Control Networks. http://www.rfidblog.org.uk/Preprint-GallowayHancke-IndustrialControlSurvey.pdf.

[24] IEEE Smart Grid, http://smartgrid.ieee.org

[25] United States Department of Energy SmartGrid.gov, http://www.smartgrid.gov

[26] Smart Grid Security Blog, http://smartgridsecurity.blogspot.com