Information & Security: An International Journal

Skarga-Bandurova, Ryazantsev, and Kiryushatova, vol.35, no. 2, 2016, 123-132

https://doi.org/10.11610/isij.3506

AN EXPERIENCE REPORT ON EDUCATION AND TRAINING PROGRAMME IN CYBERSECURITY OF CRITICAL INFRASTRUCTURES

Inna SKARGA-BANDUROVA, Alexandr RYAZANTSEV, and Katerina KIRYUSHATOVA

Abstract: The paper presents the results of designing and implementing an educational programme in risk analysis of security and resilience of critical infrastructures. The main goal of the programme is to create a knowledge base for multidisciplinary research on critical infrastructure risk management and develop a security curriculum for suitable and recognized industry and academic experts. It is expected that this programme will allow training of highly-qualified specialists and arm them with up-to-date tools and techniques enabling security risk assessment, risk management, and response to new challenges of cyber society.

Keywords: cybersecurity, critical infrastructure, enterprise, industrial control system, risk analysis, resilience, curriculum.

1 Introduction

A problem of cyber security of critical infrastructures is not a novel but recent years it increases dramatically. Now, the world has entered a new era of crisis when political ambitions prevail over economic benefits and common sense. As a response to this challenges the cyberspace has not generated the new threats, instead it has raised the new threat properties. Previously, we thought that the security protection is effective if it results in a situation where the benefit of the cyber criminal from the attack was less than the cost of the attack. With the increasing politicized context, that era is over. People hack into computer systems at any price, not even wanting to extract something real from them. They are quite satisfied with the result if the service is unavailable. Thus, threats stay the same but their weights have changed. At the same time, cyber crimes are getting more sophisticated more organized and more frequent. All this leads to the fact that the critical infrastructure remains vulnerable to such malicious activity and organizations at all levels face with the severe shortage of well-

trained personnel who are able to strike asides and organize an effective defence. In the concerned circumstances, TEMPUS SEREIN [1] is a unique for Ukrainian society, ambitious and innovative project oriented on education and training highly qualified specialists in cyber security assessment and management. SEREIN project covers a wide range of issues in training a new generation of engineering and research staff capable of performing constructive development in cyber security assessment and ensuring. In this paper, we report on the design and execution only a small part of this project dedicated to educational and training program in risk analysis of security and resilience which we called CSCI (Cyber Security of Critical Infrastructures).

2. Program Objectives and Motivation

The main aim of CSCI program is to create a knowledge base for multidisciplinary research on critical infrastructure risk management and develop a security curriculum of suitable and recognized industry and academic experts as well. In view of the economic characteristics of our region, as a main object for the study we have chosen industrial enterprise. There are at least three reasons for it. First, approach to the protection of industrial systems is much like those used 15 years ago to ensure the security of IT systems and, therefore, requires significant changes in view of the new calls. Secondly, industrial IT architectures differ from traditional IT systems due to wide usage SCADA and/or industrial control systems (ICS). Until recently they were relatively safe from cyber intrusions and operated as they were designed. However, ICS became more and more integrated to enterprise infrastructure and, as a result, to the Internet that leads to great cyber threats. And third, specificity of ICS (priority of access) does not allow the use of information security solutions with great intellectual component. For security ICS, cryptographic solutions were rarely used because they tend to generation redundant computation and can slow down or even stop the sending and receiving a control signal. If the suspension of the process is a normal measure for standard IT systems (in the case of suspected malicious activity, for example), in industrial applications it can cause a man-made disaster.

Given how many industrial enterprises have difficulty finding qualified workers, it became clear that the traditional training courses in information security do not meet the modern need for cyber security staff and still there is a wide space for innovative programs in this area. Therefore, we created our program to combine research, training, and outreach efforts in risk analysis of security and resilience. It has been customized to the developing needs of industry and extended to address cyber threats specific for ICS.

3 Program overview and educational outcomes

Before moving to the program structure, it is necessary to point out that we taught a CSCI course for the first time and it was a pilot project limited to one semester. It raised a large quantity of pedagogical and management issues that we discuss below. Initially, to developing our CSCI program we turned to the well-proven postgraduate programs of our TEMPUS SEREIN partners from City University London: Management of Information Security and Risk,[2] and Cyber Security.[3] Both of them include the average eight taught modules, six core and two elective modules with a full-time individual project completed over the summer. With an eye toward our goals and to fit into time constraints we decided to dwell on the four modules:

1. Foundation of critical infrastructure security and resilience;
2. Security risk analysis techniques and standards;
3. Enterprise cyber security and risk management;
4. Industrial control system security and resilience.

The CSCI course itself is a combination of lectures, seminars and laboratory exercises directed to gaining experience in both industrial security concepts and advanced use of particular tools. Training support package includes a course outline, ad hoc teaching materials, borrowed open-source software and native software. To CSCI course implementation, we have developed lecture materials in a shape of slides, a set of training material in the form of student manual for laboratory class, and a program for the seminars. We also drew up a list of recommended reading and provided the students with e-copies of four books in the targeted area: Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS,[4] The security risk assessment handbook,[5] Information security risk analysis,[6] and The IAONA Handbook for Network Security.[7] The major topics covered in the seminars are shown in Table 1.

The benefits of a laboratory experiments for a computer security courses have been noted in many papers.[8, 9, 10] Within the scope of the lab course, we focused primarily on work with virtual machines. It allows students to simulate and study characteristics in the heterogeneous environment similar to industrial systems, to obtain the different issues that can arise with various OS, and to gain experience with some of the tools across multiple platforms. The labs we proposed for CSCI were on the following topics, with particular tools written in parentheses (Figure1).

Table 1: Seminar topics.

No.	*Topic*	*Details*
1	Cyber crimes & Ethics	Cyber crimes (CC) in industry; CC in governance; CC against property, against person; financial CC, Intellectual property crimes, Cyber criminals (kinds, organized hacktivists, disgruntled employees, professional hackers), corporate espionage. Ethics in information security police.
2	IT security risk analysis methods	Quantitative vs. qualitative risk analysis. Qualitative risk analysis basics. Improving quantitative risk analysis with security ontologies. Quality risk analysis and QRM tools. Case studies.
3	Security risk management methodologies	OCTAVE, CORAS, CRAMM, FRAP, COBRA, ISRAM, CORA, IS Risk Analysis Based on a Business Model, RiskWatch, Australian Risk Management Standard AS/NZS 4360:2004, Dutch A&K Analysis, Ebios, ISO/IEC IS 13335-2, ISO/IEC IS 17799, IT-Ground-schutz, Mehari. Integrating HAZOP and SIL/LOPA Analysis
4	ICS security	Security risk metrics in industry. ICS Characteristics, Threats and Vulnerabilities. Major ICS Security Objectives. Comparing ICS and IT Systems. Cyber Attack Modeling and Security risk management methodologies for ICS.
5	A cyber security risk assessment for the design of ICS	Assessments during the system design phase. System Identification and Cyber Security Modeling during design. Asset and Impact Analysis. Threat Analysis. Vulnerability Analysis. Security Control Design. Penetration testing.

1. Analysis of security auditing tools (nmap, Nessus, Nexpose, etc.);
2. Network security analysis using attack graphs approach (MulVAL [11] and as alternative freeware tool to study attack graph approach TVA, Attack Graph Toolkit, NetSPA, etc. can be used);
3. Cyber threats risks modeling with Bayesian networks (AgenaRisk [12] and as alternative tool to study risks modeling techniques with Bayesian networks variety tools such GeNIe && SMILE, SamIam, etc. are also available);

4. Assessing risks and opportunities in enterprise architecture (EAAT Object Modeler[13] & CySeMoL class model.[14] Systems Aris, ETIS, QualiWare, System Architect, etc. can be used alternatively).
5. Risk-based and functional security testing the program source code (native software AutoTestDFB).

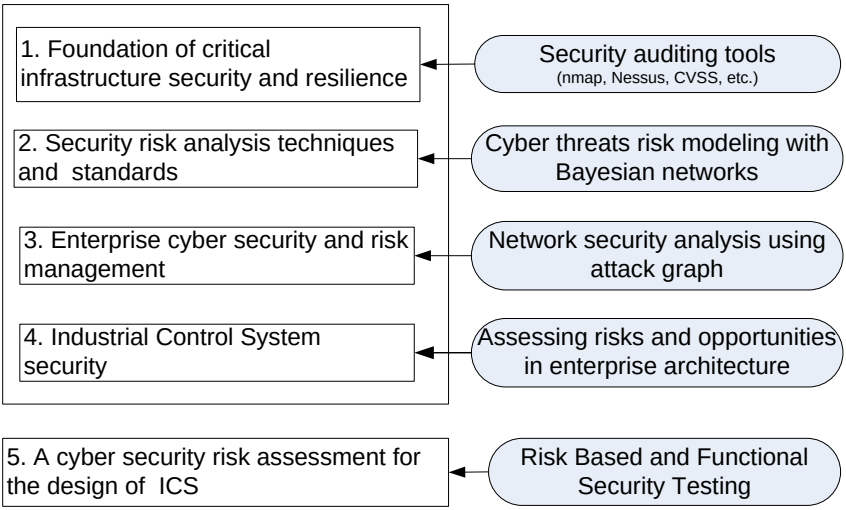

Figure 1: Consistency of theoretical (left) and practical (right) parts of CSCI program.

The structure of the CSCI program contains three complementary educational aspects. First, the core educational component combines an intensive training with the small groups on labs. Second, CSCI provides the students with the opportunity to enhance their skills by wide involvement industrial practice and case study. Case study enables students to develop realistic solutions to the industrial security problems and to understand crucial nature of complex analysis both specifically and generally. Finally, we try to encourage the students to use their knowledge and ambitions to draw information security concepts into their research activity. By the end of semester, the successful student should be able to:

- employ the functional representation of industrial system interconnections for structural and resilience analysis in the framework of resilience and risk assessment;
- select appropriate risk analysis method for different tasks of cyber security;

- prepare test scenarios designed to validate the performance of security systems and protective force in detecting, interdicting and countering threats;
- utilize different software tools to compile and analyse data to identify trends regarding security assurance activities and create reports to support customer requirements and/or compliance related requirements;
- perform risk analyses and process analyses related to security data manipulation and management;
- analyse ICS risks and opportunities to ensure their security and resilience.

As acquired professional competencies we expect an) effective analytical and problem-solving skills to contribute to creative solutions to complex cyber security problems, b) gaining experience in working under limited direction within scope of the assignment and using independent judgment in choosing methods, techniques, software, and evaluation criteria and c) ability to interact effectively with peers and customers.

4 Results

Developing and running the pilot version of CSCI has required the significant efforts from our instructional staff. Nevertheless, we got added evidence that this program is worth that effort, especially since we received many suggestions from our industrial partners. Thus, at the request of our colleagues from research and production enterprise in the middle of the semester we have introduced the additional fifth module devoted to studies of cyber security risk assessment during designing and producing ICS (see Figure 1).

It is worth also noting that this is a first course at our faculty that was taught in English. There is no doubt that it was an additional difficulty for all of us, but both personnel and students have opened the new advantages and opportunities in it. By the end of the semester, we became a real occupational community with the common interest, singular language, and some new ideas and projects.

Regarding problems with the pilot version CSCI we would like to accent on two aspects. First is obsolete equipment in our computer classes. There was a big problem to install virtual machines on slow computers and as a result students found a nearly diplomatic decision, they brought their own computer components and laptops to perform labs. Second, are known issues with freeware soft. For example, in the open source package MulVal v1.1, we could not run a function for automatically generating attack graphs directly from Nessus' reports probably due to a malfunction of the adder. It took the time to fix this bug and configure software for proper

operation. Overcoming these small complexities, have led us to the conclusion that cyber security area is a breeding ground to young brilliant minds. It means that students from less advanced and wealthy countries can enter to cyber security world as a citizen of the world, at a much higher level than in the traditional physical offense and defence world.

As researchers and educators, we have derived two major benefits from designing and running the pilot version of CSCI. We have been able to create and adjust a curriculum structure and the accompanying content that achieved the educational goals of the program and meet expectations of our partners. The combination of training, internship, and mentoring components has offered students a holistic educational experience. We have set security education in motion by providing a premise for current research on critical infrastructures security and resilience by combining system approach and holistic risk management in the context of the discipline. As essential part, we gave our students the ethical foundation for the application of the knowledge they gained so that they were able to maintain proper conduct during the exercise and in their future work as computer professionals.

5 Future work

We have extensive plans concerning the further expansion of CSCI course. In future offerings of the course, we will add other laboratories on topics such as modelling critical infrastructures resilience within the cyber security framework, analysing cyber threats specific for ICS, and red team – blue team training for ICS cyber security [9, 10, 15, 16] to give our students further experience with the major issues, strategies and tools involved in computer security.

For our industrial partners we are going to design and implement two summer training programs: a) a special laboratory training in “cyberwars” to give students practical skills in the protecting enterprise system networks, identifying vulnerabilities, learning how vulnerabilities can be exploited, and learning defensive and mitigation strategies for ICS and b) training in cyber risks and threats intelligence to give them key to understanding which data must be secured, and how, what to look for, what current threats are, and how to best respond. With present-day needs these short courses will be prepared and taught in the native language.

Continuing to engage with industry partners and our TEMPUS SEREIN partners from Ukrainian and EU academic institutions, we hope to foster improvements in cyber security education and provide undergraduates with valuable experience developing and maintaining secure information infrastructure.

Acknowledgment

Educational and training program in risk analysis of security and resilience which we called here CSCI was designed as a pilot version of Master Program "Risk Analysis of SoS Security and Resilience" within the framework TEMPUS Project "Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains" co-founded by the Tempus Programme of the Europe Union. Project Number: 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR.

References

1. National Aerospace University "KhAI." TEMPUS SEREIN project web site. Accessed October 28, 2015, http://serein.net.ua/.

2. City University London. "Management of Information Security and Risk. Programme Specification." Accessed October 17, 2015, www.city.ac.uk/__data/assets/pdf_file/0005/178691/PSMISR-MSc-Management-of-Information-Security-and-Risk.pdf.

3. City University London. "Cyber Security. Content and Structure." Accessed October 17, 2015, http://www.city.ac.uk/courses/postgraduate/cyber-security#course-detail=1.

4. Tyson Macaulay, *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS* (Boston, MA: Auerbach Publications, 2011).

5. Douglas Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, 2nd edition (Boca Raton, FL: CRC Press, Taylor & Francis Group LLC, 2011).

6. Thomas R. Peltier, *Information Security Risk Analysis*, 3rd edition (Boca Raton, FL: CRC Press, Taylor & Francis Group, 2010).

7. *The IAONA Handbook for Network Security. Industrial Automation Open Networking Alliance*, Version 1.5 (Magdeburg, Germany, 2006). Accessed August 12, 2015, http://www.vpi-initiative.com/download/IAONA-Security-Guide-15-draft.pdf.

8. Michael E. Locasto and Sara Sinclair, "An Experience Report on Undergraduate Cyber-Security Education and Outreach," (2009). Accessed October 14, 2015, http://www.ists.dartmouth.edu/docs/Experience%20Report.pdf.

9. Daniel Noyes, "Cyber Security Testing and Training Programs for Industrial Control Systems." The 18th Pacific Basin Nuclear Conference (PBNC 2012),

BEXCO, Busan, Korea, March 18-23, 2012. Accessed: September 12, 2016. https://www.osti.gov/servlets/purl/1044208/.

10. Paul J. Wagner and Jason M. Wudi, "Designing and Implementing a Cyberwar Laboratory Exercise for a Computer Security Course." *ACM SIGCSE Bulletin* 36, 1 (2004): 402–406. https://doi.org/10.1145/1028174.971438.

11. Argus Cybersecurity Lab at Kansas State University. "MulVAL: A Logic-based, Data-driven Enterprise Security Analyzer." Accessed October 28, 2015, http://people.cis.ksu.edu/~xou/argus/software/mulval/readme.html.

12. Agena. "Bayesian network and simulation software for risk analysis and decision support AgenaRisk". Accessed October 17, 2015, http://www.agenarisk.com.

13. KTH Royal Institute of Technology, "About Enterprise Architecture Analysis Tool." Accessed October 28, 2015, https://www.kth.se/en/ees/omskolan/organisation/avdelningar/ics/research/sa/p/eaat/about-eaat-1.387294.

14. KTH Royal Institute of Technology, "The Cyber Security Modeling Language." Accessed October 28, 2015, https://www.kth.se/en/ees/omskolan/organisation/avdelningar/ics/research/cc/cysemol/downloads-1.432383.

15. Jose Carlos Brustoloni, "Laboratory Experiments for Network Security Instruction," *Journal on Educational Resources in Computing* 6, no. 4 (2006). https://doi.org/10.1145/1248453.1248458.

16. European Network for Cyber Security, "The ENCS Red Team Blue Team Training for Industrial Control Systems and Smart Grid Cyber Security" Accessed October 12, 2015. https://www.encs.eu/wp-content/uploads/2015/08/2015_ENCS_Factsheet_RedBlue_Training_v1.pdf.

About the authors

INNA SKARGA-BANDUROVA is professor at the Computer Engineering Department of Volodymyr Dahl East Ukrainian National University, Severodonetsk, Ukraine. She graduated from the East Ukrainian State University in 1996 and received a PhD degree in Computerized Control Systems and Progressive Information Technology from Donetsk National University, Ministry of Education and Science of Ukraine, in 2006. In 2015 she took a degree Doctor of Science in Information Technology from Kherson National Technical University, the Ministry of Education and Science of Ukraine. Research interests: Decision Theory; Formal Methods for Data Analysis; Critical Infrastructures Safety; Health Informatics; Environmental Informatics. She is an author and co-author of two books and 84 papers published in Ukrainian and international refereed journals. Her current researches devoted to formal methods in information technologies for industry and medicine, functional safety of I&C systems for critical infrastructures. E-mail: skarga-bandurova@ukr.net.

ALEXANDR RYAZANTSEV is Head of the Computer Engineering Department of Volodymyr Dahl East Ukrainian National University, Severodonetsk, Ukraine. He graduated from the Kharkiv Institute of Radio Electronics in 1988 and received a PhD degree in Systems of designing automatization from Institute of Radio Electronics, Ministry of Education and science of Ukraine, Kharkiv, in 1993. He received a Sc.D. degree in Information Technology from Kherson National Technical University, Ministry of Education and Science of Ukraine in 2012. He has authored and co-authored of seven books and more than 60 papers published in Ukrainian refereed journals. His current research focused on developing of methodologies and information technologies for environmental and technologic safety of industrial regions. E-mail: a_ryazancev@mail.ru.

KATERINA KIRYUSHATOVA is assistant lecturer at the Information Technology Department of Kherson National Technical University, Faculty of Cybernetics and Systems Engineering, Kherson, Ukraine. She graduated from the Kherson National Technical University in 2009 and received MSc degree. Research interests: systems analysis, information technology. Her current researches devoted to education technologies and the practice of institutional collaboration. E-mail: katyakir@mail.ru.