The Cybersecurity education in smart grids Body of Knowledge development and implementation roadmap (Executive Report)

Authors:

Rūta Pirta-Dreimane, Jana Bikovska, Andrejs Romānovs, Maria Valliou, Bahaa Eltahawy, Jānis Pekša

Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)

Erasmus+ Strategic Partnership Project

Intellectual Output 4

Riga Technical University, University of Vaasa, National Technical University of Athens, University of Oldenburg

This project has received funding from the European Union's Erasmus+ Programme under Grant Agreement № 2020-1-FI01-KA203-066624.

Contents

Abbreviations

ACM	Association for Computing Machinery
NICE	National Initiative for Cybersecurity Education
CC-RSG	Cybersecurity Curricula Recommendations for Smart Grids
CPES	Center for Power Electronics Systems
ENISA	European Network and Information Security Agency
EU	European Union
JTF	Joint Task Force
IT	Information Technology
IO	Intellectual output
MOOC	Massive online open courses
NIST	National Institute of Standards and Technology
PMU	Phasor Measurement Unit
OT	Operational Technology
SCADA	Supervisory control and data acquisition
SMEs	Small and medium-sized enterprises
VET	Vocational education and training
WP	Work Package

1. Introduction

Cybersecurity is defined as one of European strategic capabilities and it has been acknowledged that the EU must significantly improve its digital capacities in the cybersecurity field [1]. This includes the deployment of digital technologies, as well as the necessary digital skills for all EU workforces. Cybersecurity is an interdisciplinary subject [2]- [3], to ensure all critical competences, several dimensions and disciplines must be integrated in education programs, such as computer science, engineering, psychology, sociology, and law. Cybersecurity specialists must have deep technical knowledge, meantime, also general skills are essential, especially in crisis situations.

The environment of smart grids involves additional complexity in terms of cybersecurity. Smart grid integrates variety of sensors, control systems and communication networks what increases the cyberattack surface. Cybersecurity specialists working in the smart grid environment must have a wide range of competences to protect the infrastructure, balancing cybersecurity and electrical engineering competences, along with the soft skills.

This document represents the project “Cybersecurity Curricula Recommendations for Smart Grids (CC-RSG)” WP4 outcome. This work activity aims to conceptualize knowledge gained in the project and provide recommendations for cybersecurity curricula development for smart grids.

The main objective of the document is to provide recommendations for educators and other relevant parties for educational programs development, considering, industry needs, workforce requirements, student-centric educational methods and emerging support tools.

2. Model for Education Curricula

The aim of the model is to provide guidance for competence-driven cybersecurity education programs for smart grids design, execution and evaluation. The model explains how a body of knowledge (e.g., this document) should be used to enable workforce and education dimensions integration.

The model is based on the methodology proposed in [4] and it consists of three key building blocks (Figure 1):

1. **Education curricula content** defines roles and tasks-specific competences and associated knowledge areas, knowledge units, learning topics and learning outcomes.
2. **Education program design methodology** suggests study programs and courses design, execution and evaluation principles and process.
3. **Tools and methods bank** includes methods and tools list and their usage guidance (patterns), that can be used in cybersecurity education programs for smart grids design, execution and evaluation.

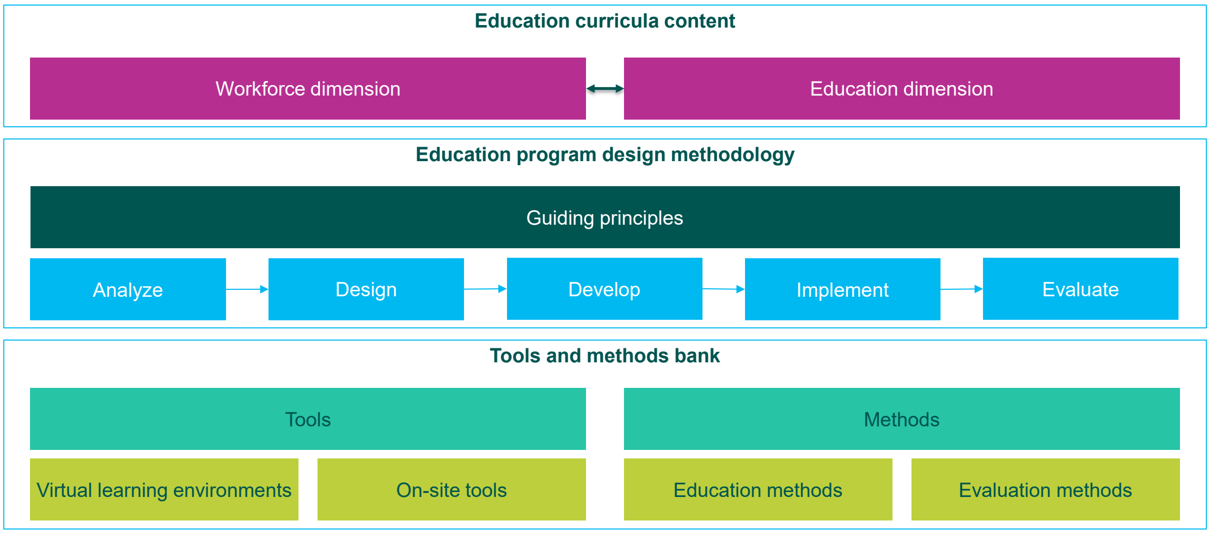

Figure 1 Model for Education Curricula Overview

2.1 Education Curricula Content Model

Education curricula must be designed based on workforce requirements to ensure that cybersecurity specialists' competences meet industry demand, including skills that need to be taught and areas of expertise that need to be covered [2].

The proposed model for education curricula incorporates two dimensions – workforce dimension and education dimension (Figure 2).

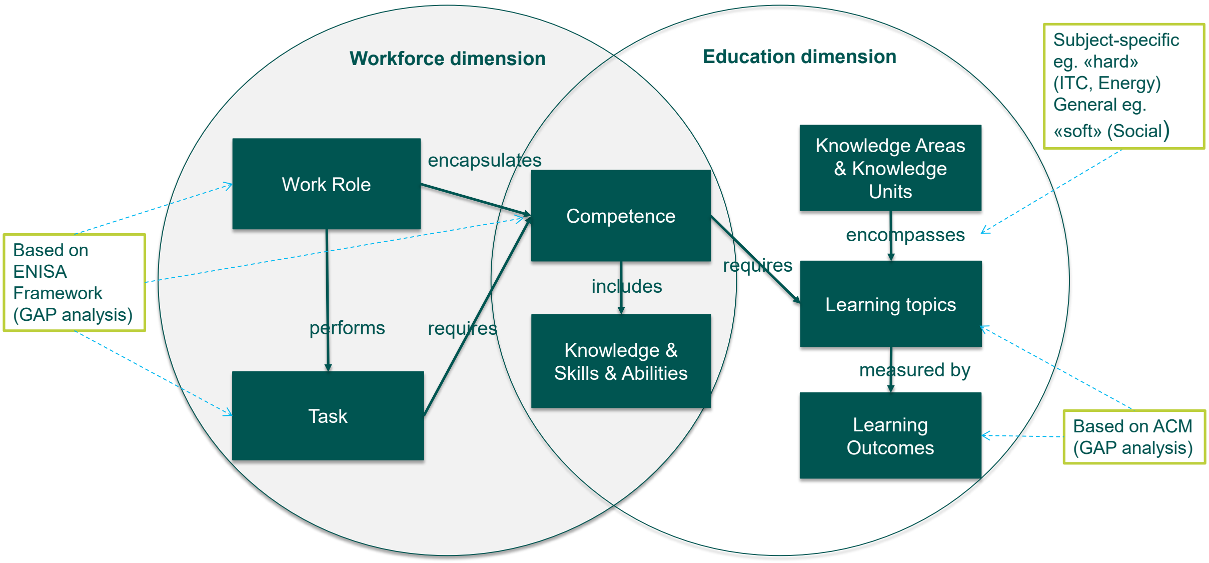
Workforce dimension
Education dimension
Subject-specific eg. «hard» (ITC, Energy) General eg. «soft» (Social)
Work Role
encapsulates
Competence
Knowledge Areas & Knowledge Units
encompasses
Based on ENISA Framework (GAP analysis)
requires
includes
Learning topics
performs
requires
Knowledge & Skills & Abilities
measured by
Task
Learning Outcomes
Based on ACM (GAP analysis)

Figure 2 Model for Education Curricula Overview

The workforce dimension includes the following key concepts [5]:

- **Work roles** are the most detailed groupings of cybersecurity-related work, including a list of attributes, i.e., knowledge, skills, and abilities required to perform tasks associated with the role.
- **Tasks** represent specific defined pieces of work that, combined with other identified tasks, compose the work scope in a specialty area or work role.

- **Competencies** describe capabilities of applying or using knowledge, skills, abilities, behaviors, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position. It is important to distinguish the capabilities between subject-specific (e.g., “hard skills”) and general (e.g., “soft-skills”). Hard skills include technical or administrative competence. Soft skills are a cluster of productive personality traits that characterize one's relationships in a social environment. These skills can include social graces, communication abilities, language skills, personal habits, cognitive or emotional empathy, time management, teamwork and leadership traits.

Several frameworks define cybersecurity related roles, associated tasks and required competences, for example, National Initiative for Cybersecurity Education (NICE) Workforce Framework (NIST NICE framework) [5] and the European Union Agency for Cybersecurity (ENISA) skill framework (ENISA framework) [6].

For cybersecurity education in smart grids, it is suggested to use ENISA competence model as basis for education programs design, as it has simpler work role's structure compared to NIST. NIST roles are mainly designed for large enterprises, therefore they represent siloed cybersecurity capabilities split across organizations. Empirical observations show that enterprises typically combine similar roles and enable “T-shaped” competences and multi-functional teams.

Existing cybersecurity competence models focus on cybersecurity governance and IT-specific cybersecurity aspects, but they don’t address smart-grids cybersecurity roles, tasks and competences. Therefore smart-grids cybersecurity specific tasks are incorporated into ENISA model (Section 3.2.). Tasks and competences are suggested by the project expert team (Section 3). Therefore, this document defines reference model for smart-grid cybersecurity roles and tasks that is basis for relevant education programs design.

The workforce dimension interferes with education dimension via competences, that includes skills, abilities and knowledge. The education dimension includes following key concepts [7]:

- **Knowledge areas** and **knowledge units** are thematic groupings that encompass multiple, related **learning topics**.
- **Learning outcomes** represent more detailed outcomes than the competencies and may be seen as course or lesson learning outcomes. Learning outcomes emphasize what students can do over merely what students know.

Several cybersecurity curriculum recommendations suggest main knowledge areas, knowledge units, learning topics and learning outcomes. For example, Cybersecurity Curricular Guidance for Associate-Degree Programs (Cyber2yr2020) prepared by Association for Computing Machinery Committee for Computing Education in Community Colleges [7] and CSEC2017 Joint Task Force on Cybersecurity Education (JTF) global cybersecurity curricular recommendations [3].

For cybersecurity education in smart grid, it is suggested applying Cyber2yr2020 guidelines for IT specific cybersecurity knowledge units, knowledge areas, topics and learning outcomes definition. Smart grids specific cybersecurity education is addressed limited in existing frameworks, therefore smart-grids cybersecurity specific competences, learning topics and learning outcomes are incorporated into Cyber2yr2020 model. Smart-grid specific cybersecurity competences, learning topics and learning outcomes are suggested by project experts' team (Section 3.3.).

In this document, the competences are divided in four groups:

- IT-specific competences define knowledge, abilities and skills required to perform IT-specific cybersecurity tasks. These competences are based on Cyber2yr2020 guidelines (only essential competences). These competences define ‘‘what is to be done’ aspects [7].
- Smart-Grids -specific competences define knowledge, abilities and skills required to perform smart grids-specific cybersecurity tasks. These competences are prepared by project experts' team and validated with industry experts. These competences define ‘‘what is to be done’ aspects [7].
- Operational competences compile managerial and operational competences what defines ‘‘how activities should be done’ in both – IT specific and smart-grids specific areas.
- General competences define expected “soft skills”.

2.2 Education Program Design Methodology

Education program design methodology defines general principles what need to be followed and main steps in how education program should be defined (Figure 2). In program definition, execution and evaluation educators can use smart grid cybersecurity competence model and curricular content recommendations described in this document. However, precise content must be aligned to program learner profiles and their needs (target roles etc.).

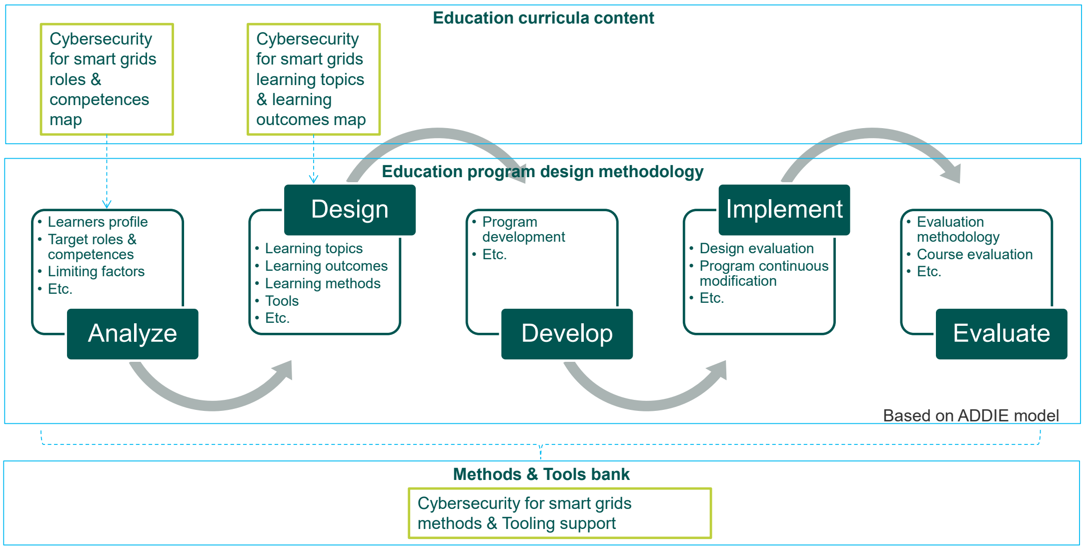
Education curricula content
Cybersecurity for smart grids roles & competences map
Cybersecurity for smart grids learning topics & learning outcomes map
Education program design methodology
• Learners profile
• Target roles & competences
• Limiting factors
• Etc.
Analyze
Design
• Learning topics
• Learning outcomes
• Learning methods
• Tools
• Etc.
• Program development
• Etc.
Develop
Implement
• Design evaluation
• Program continuous modification
• Etc.
• Evaluation methodology
• Course evaluation
• Etc.
Evaluate
Based on ADDIE model
Methods & Tools bank
Cybersecurity for smart grids methods & Tooling support

Figure 3 Education Program Design Methodology

Education programs should be prepared following several guiding principles. According to the design thinking approach regarding the usage in educational design [8], [9] design principles are frequently used to state the main direction that must be followed in programs design and execution [10]. The design principles are defined as [9]: ‘‘...an intermediate step between scientific findings, which must be generalized and replicable, and local experiences or examples that come up in practice. Because of the need to interpret design principles, they are not as readily falsifiable as scientific laws. The principles are generated inductively from prior examples of success and are subject to refinement over time as others try to adapt them to their own experiences". Design principles elicit design knowledge from successful learning environments [10] and summarize reusable best practices.

For cybersecurity education in smart grids, it is suggested to follow such key principles:

1) **Target roles and tasks driven competence design** - competences must be defined based on learners' target roles to enable workforce and education dimensions integration.
2) **Learner centricity and personalization** – study programs must focus on students' needs and provide profile specific competence development.
3) **Subject-specific and general competences synergy** – general competences must be integrated in every learning topic along with subject-specific competences.
4) **Real-world experiences integration** – study programs and courses content must reflect real-world challenges and must adapt over time.
5) **Vertical integration** – cybersecurity is a multi–disciplinary subject; programs must integrate social sciences (as psychology) to enable general competences development.
6) **Feedback based continuous improvement** – continuous improvement must be planned based on learners and workforce feedback.

The suggested education program design process is based on ADDIE model [11]. The ADDIE model is the generic process traditionally used by instructional designers and training developers. The model includes five phases:

1. **Analysis** - learners profiles analysis (including their characteristics, existing competence, expected target roles and training needs), instructional goals and objectives definition. The program must be designed to incorporate competences that are required for learners' target roles. This document includes typical cybersecurity roles that are enriched with smart-grid specific cybersecurity tasks and competences (Section 3.2.). This document can be used as reference model for learner's target roles mapping. The roles are designed based on identified typical smart grid cybersecurity learners' profiles (Section 3.1.) that are defined based on project experts' experience.
2. **Design –** study program objectives, learning topics, learning outcomes and teaching methods definition. This document defines the set of learning topics and learning outcomes that defined roles must have (Section 3.3.). The topics are encapsulated in knowledge areas and units. Work roles, tasks, competences and learning topics map is added in Appendix 1. The topics must be selected based on identified learners target roles. Learners can have individual plans, based on their existing competences (e.g., if learner has previous education in IT specific cybersecurity and he aims to became Security architect in energy sector institution, he/she must obtain smart grid specific cybersecurity competences). The document includes methods bank (Section 4) and tools bank (Section 5) that can be used for education program design support.
3. **Development** – study program materials development and loading in e-learning systems (if applicable).
4. **Implementation – actual program and courses delivery.**

5. **Evaluation –** feedback and data collection for improvement areas identification. The document includes methods bank (Section 4) and tools bank (Section 5) that can be used for education program evaluation support.

2.3 Methods and Tools Bank

The methods bank and the tools bank (Section 4) suggest methods and toolbox that study program designers and educators can use in all education development process phases (analysis, design, development, implementation and evaluation). Methods and tools are defined in the form of reusable patterns forming a knowledge base for courses design and execution support. Methods and tools linkage to education design and execution process phases are described on each method /tool card.

3. Education Curricula Recommendations

Education curricula recommendations forms reference model for workforce and education integration. It includes such main concepts:

- **Learners' profiles** – typical smart grid cybersecurity learners' profiles provide grounds for target work roles definition;
- **Work roles and tasks** represent learners target roles, tasks and required competences (including, IT-specific cybersecurity competences, smart grid specific cybersecurity competences, operational and general competences);
- **Knowledge units and knowledge areas** define **learning topics and learning outcomes** required to obtain competence.

3.1 Learners Profiles

The purpose of the student profile is to highlight student groups to which the curriculum model can be applied.

Here two groups of graduates who can be interested in continuing their education in the area of cybersecurity for smart grids can be highlighted: graduates in computing area and graduates in power systems. The other two groups are professionals either IT&OT or management of smart grids. They have work experience in power systems and smart grids however they need more advanced knowledge in cybersecurity for smart grids.

The following attributes are considered for the profile:

- background refers to educational attainment or professional skills of a learner;
- educational needs are the gap between the learner's current level of knowledge, skills, and attitudes and the desired one, in order to adapt to a new situation which can be acquired through education,
- Expectations describe the knowledge and skills that students are expected to demonstrate by the end the studies.

The energy industry needs a cybersecurity-literate workforce, and higher education could play a valuable role in filling the gap.

3.2. Work Roles and Tasks

The smart-grid cybersecurity work roles have been built on ENISA suggested roles: Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Legal, Policy & Compliance Officer, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Implementer, and Cybersecurity Risk Manager. The roles, tasks and competences have been supplemented according to the specifics of the smart grid.

The ENISA roles were supplemented by new roles considering the specifics of the smart-grids – Energy Citizen, Grid Assets Manager and Grid Communication Engineer. The common business objectives for smart-grid specific roles are [12]: maintain safety, maintain power system reliability, maintain power system resilience and support grid modernization.

3.3. Knowledge Areas and Knowledge Units

Knowledge areas and units are based on "ACM Cybersecurity Curricular Guidance for Associate-Degree Programs 2020 Cyber2yr2020" association for Computing Machinery (ACM) Committee for Computing Education in Community Colleges (CCECC): Data security, Software security, Component security, Connection security, System security, Human security, Organizational security, Societal security. They are enriched with smart grid specific competences required for defined work roles (3.2. section). New knowledge area "Smart-Grid Security" supplements the ACM framework.

3.4. Methods & Tools Bank

The methods and tools bank specifies suggested methods and tools to be used in cybersecurity education in smart grid: Simulation tools, CPES laboratories and testbeds, Gamification, Problem and Project based learning and Flipped learning. A quick way for the teachers/trainers that want to formulate a curriculum, to see the basic elements of the method and its usual use cases on the topic of cybersecurity and/or smart grids. Along with the educational methods the tool of simulation testbeds is also described with use-cases provided.

Testbeds are used to simulate in varying degrees real-life systems. Some testbeds use software simulation for parts of the system and others use only hardware components. Additionally, there are testbeds that only simulate a component of the system and others that simulate the whole system. Using a real-time simulator combined with real hardware (like inverters and PMUs) to simulate an entire microgrid is the most realistic and complete way to study the behavior of an electrical grid under a cyber-attack.

Gamification is a teaching method in which elements and mechanisms from game designing are used to increase student engagement [13]. Those elements and mechanisms can be for example a narrative story, limited time to accomplish a task, points, badges and level-beating.

In Problem-based learning (PBL) a group of students investigates an open-ended real-world problem and tries to come up with the most suitable solution which then the group presents to other peers. Project Based Learning is based on the same idea but in general it has a longer duration and a concrete outcome rather than a theoretical solution provided.

The main characteristic of Flipped learning is that the students study the material that is usually studied during class hours at their home. In that way when they are at class, they have the opportunity to reflect on the studied material and have time for experimentation.

References

[1] European Commission, “The EU’s Cybersecurity Strategy for the Digital Decade,” 2020. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, and R. De Nicola, “Framework, Tools and Good Practices for Cybersecurity Curricula,” *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3093952.

[3] Joint Task Force on Cybersecurity Education, *Curricula 2017 Cybersecurity Curriculum - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*, vol. Version 1., no. December. 2017.

[4] R. Pirta-Dreimane, A. Brilingaite, E. Roponena, and K. Parish, “Multi-dimensional Cybersecurity Education Design: A Case Study,” in *2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)*, IEEE, Sep. 2022, pp. 1–8. doi: 10.1109/DASC/PiCom/CBDCom/Cy55231.2022.9927931.

[5] D. S. M. C. S. K. A. W. and G. W. R. Petersen, “Workforce Framework for Cybersecurity (NICE Framework),” 2020.

[6] E. European Union Agency for Cybersecurity, “European cybersecurity skills framework,” *https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles*, 2022.

[7] Cyber2yr2020 Task Group, *Cybersecurity Curricular Guidance for Associate-Degree Programs*. 2020. doi: 10.1145/3381686.

[8] I. Wrogemann, L. Sarp, N. Susser, and J. Falk, “D-Learning – Design Thinking as a means to innovative product development in adult learning,” *https://cesie.org/media/ d-learning-manual-en.pdf,* 2021.

[9] S. Panke, “Design Thinking in Education: Perspectives, Opportunities and Challenges,” *Open Education Studies*, vol. 1, no. 1. 2019. doi: 10.1515/edu-2019-0022.

[10] Y. Kali, R. Levin-Peled, and Y. Dori, “The role of design-principles in designing courses that promote collaborative learning in higher-education. Computers in Human Behavior,” *Comput Human Behav*, vol. 25, 2009.

[11] G. Morrison and S. Ross, *Designing Effective Instruction, 7th Edition*. 2013.

[12] J. Marron, A. Gopstein, N. Bartol, and V. Feldman, “Cybersecurity framework smart grid profile,” Gaithersburg, MD, Jul. 2019. doi: 10.6028/NIST.TN.2051.

[13] S. Deterding, K. O’Hara, M. Sicart, D. Dixon, and L. Nacke, “Gamification: Using game design elements in non-gaming contexts,” in *Conference on Human Factors in Computing Systems - Proceedings*, 2011. doi: 10.1145/1979742.1979575.