IFIP Advances in Information and Communication Technology 531

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the first World Computer Congress held in Paris the previous year. A federation for societies working in information processing, IFIP's aim is two-fold: to support information processing in the countries of its members and to encourage technology transfer to developing nations. As its mission statement clearly states:

> *IFIP is the global non-profit federation of societies of ICT professionals that aims at achieving a worldwide professional and socially responsible development and application of information and communication technologies.*

IFIP is a non-profit-making organization, run almost solely by 2500 volunteers. It operates through a number of technical committees and working groups, which organize events and publications. IFIP's events range from large international open conferences to working conferences and local seminars.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is generally smaller and occasionally by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is also rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

IFIP distinguishes three types of institutional membership: Country Representative Members, Members at Large, and Associate Members. The type of organization that can apply for membership is a wide variety and includes national or international societies of individual computer scientists/ICT professionals, associations or federations of such societies, government institutions/government related organizations, national or international research institutes or consortia, universities, academies of sciences, companies, national or international associations or federations of companies.

More information about this series at http://www.springer.com/series/6102

Lynette Drevin · Marianthi Theocharidou (Eds.)

Information Security Education – Towards a Cybersecure Society

11th IFIP WG 11.8 World Conference, WISE 11
Held at the 24th IFIP World Computer Congress, WCC 2018
Poznan, Poland, September 18–20, 2018
Proceedings

Springer

Editors
Lynette Drevin
North-West University
Potchefstroom
South Africa

Marianthi Theocharidou
European Commission Joint
Research Centre
Ispra
Italy

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-319-99733-9 ISBN 978-3-319-99734-6 (eBook)
https://doi.org/10.1007/978-3-319-99734-6

Library of Congress Control Number: 2018952563

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers presented at the 11th World Conference on Information Security Education (WISE 11) held during September 18–20, 2018, in Poznan, Poland, in conjunction with the 24th IFIP World Computer Congress. WISE 11 was organized by the IFIP Working Group 11.8, which is an international group of people from academia, government, and private organizations who volunteer their time and effort to increase knowledge in the very broad field of information security through education. WG11.8 has worked to increase information security education and awareness for almost two decades.

This year, WG11.8 organized the 11th conference of a successful series under the theme "Towards a Cybersecure Society." We received 25 submissions from around the world. Each submission was blind reviewed by at least three international Program Committee members. The committee decided to accept 11 full papers. The acceptance rate for the papers is thus 44%.

In line with this year's theme, several additional events on cybersecurity took place during the three days of the conference. On the second day of the conference, the "SecTech Cybersecurity Curriculum Workshop" was organized by the SecTech Project Partnership. The following day, a new "TC11.8 Work Group on Cyber Ranges and Cyber Challenges" was discussed based on a proposal by the Norwegian University of Science and Technology and the Norwegian Defence University College. Both events are described in detail in the following section of this preface. S. E. Goodman (chair), S. Furnell, R. von Solms, and M. Bishop formed a panel discussing the topic of "Building National Cybersecurity Workforces." The panel highlighted challenges, such as how to estimate the size and make-up of national cyber security workforces based on needs, how to characterize such workforces, and how to achieve balance between employing organizations' priorities and national needs. The panel also addressed how such challenges may differ across a range of nations as well as the role of educational institutions to stimulate supply and demand. We would like to thank all the panelists and workshop organizers for their contribution to the conference.

This conference took place thanks to the support and commitment of many individuals. First, we would like to thank all TC-11 members for continually giving us the opportunity to serve the working group and organize the WISE conferences. Our sincere appreciation also goes to the members of the Program Committee, to the external reviewers, and to the authors who trusted us with their intellectual work.

We are grateful for the support of WISE11.8 Officers L. Futcher, M. Bishop, N. Miloslavskaya, and E. Moore. Finally, we would like to thank the local organizers for the support and especially the IFIP WCC 2018 General Congress co-chairs

The original version of the frontmatter was revised: By mistake two short workshop descriptions were omitted. They are now included in the revised version.

R. Slowinski and L. Strous for the collaboration. For the preparation of this volume, we sincerely thank E. Siebert-Cole and our publisher Springer for their assistance.

July 2018

Lynette Drevin
Marianthi Theocharidou

Organization

WISE11 Conference Chair

Lynn Futcher	Nelson Mandela University, South Africa

WISE11 Program Chair

Lynette Drevin	North-West University, South Africa

WISE11 Conference Secretariat

Matt Bishop	University of California, Davis, USA

WISE11 Publications Chair

Marianthi Theocharidou	European Commission, Joint Research Centre, Italy

WISE11 Local and Logistics Chair

Natalia Miloslavskaya	National Research Nuclear University MEPhI, Russia

WISE11 Web Chair

Erik Moore	Regis University, Colorado, USA

Program Committee

Maria Bada	University of Oxford, UK
Matt Bishop	University of California, Davis, USA
William Caelli	IISEC Pty Ltd, Australia
Nathan Clarke	University of Plymouth, UK
Jun Dai	California State University, Sacramento, USA
Melissa Dark	Purdue University, USA
Tamara Denning	University of Utah, USA
Lynette Drevin	North-West University, South Africa
Steven Furnell	Plymouth University, UK
Lynn Futcher	Nelson Mandela University, South Africa
Roberto Gallo	University of Campinas, Brazil
Seymour Goodman	Georgia Institute of Technology, USA
Ram Herkanaido	Plymouth University, UK
Lech Janczewski	The University of Auckland, New Zealand
Borka Jerman-Blazic	University of Ljubljana, Slovenia

Audun Josang	University of Oslo, Norway
Suresh Kalathur	Boston University, USA
Christos Kalloniatis	University of the Aegean, Greece
Vasilios Katos	Bournemouth University, UK
Sokratis Katsikas	Center for Cyber and Information Security, NTNU, Norway
Siddharth Kaza	Towson University, USA
Andrea Kolberger	University of Applied Sciences Upper Austria, Austria
Elmarie Kritzinger	UNISA, South Africa
Hennie Kruger	North-West University, South Africa
Costas Lambrinoudakis	University of Piraeus, Greece
Javier Lopez	University of Malaga, Spain
Herbert Mattord	Kennesaw State University, USA
Vashek Matyas	Masaryk University, Czech Republic
Natalia Miloslavskaya	National Research Nuclear University MEPhI, Russia
Stig Mjolsnes	Norwegian University of Science and Technology, Norway
Erik Moore	Regis University, Colorado, USA
Kara Nance	University of Alaska Fairbanks, USA
Jason Nurse	University of Kent, UK
Ruxandra Olimid	Norwegian University of Science, Norway Technology and University of Bucharest, Romania
Jacques Ophoff	University of Cape Town, South Africa
Allen Parrish	United States Naval Academy, USA
Günther Pernul	Universität Regensburg, Germany
Carlos Rieder	isec ag, Switzerland
Chien-Chung Shen	University of Delaware, USA
Marianthi Theocharidou	European Commission Joint Research Centre, Italy
Kerry-Lynn Thomson	Nelson Mandela University, South Africa
Alexander Tolstoy	National Research Nuclear University MEPhI, Russia
Ismini Vasileiou	Plymouth University, UK
Rossouw Von Solms	Nelson Mandela University, South Africa
Edgar Weippl	SBA Research, Austria
Susanne Wetzel	Stevens Institute of Technology, USA
Stephen D. Wolthusen	Royal Holloway, University of London, UKNorwegian University of Science and Technology, Norway
Louise Yngstrom	Stockholm University and Royal Institute of Technology, Sweden
Sergey Zapechnikov	National Research Nuclear University MEPhI, Russia

Additional Reviewers

Böhm, Fabian

Short Workshop Descriptions

SecTech Cybersecurity Curriculum Workshop

Elena Andreeva, Steven Furnell, Danilo Gligoroski,
Sokratis Katsikas, Djamel Khadraoui, Stewart Kowalski,
Maria Papadaki, Guenther Pernul, Bart Preneel, Gerald Quirchmayr,
Juha Röning, Thomas Schaberreiter, Qiang Tang, and Teemu Tokola

SecTech Project Partnership
qiang.tang@list.lu

1 Background

Given the mounting level of cyber threats facing Europe, a coordinated cyber security education effort becomes more urgent than ever. The malware waves hitting Europe in 2017 give a clear warning of the dangers lying ahead, ranging from criminal activities to often state sponsored theft of intellectual property and a rising possibility of cyber sabotage. Those developments have also increased the demand for cyber security experts in an already virtually empty market. It is obvious that an increased supply of talent becomes an absolute necessity if Europe as a whole shall improve cybersecurity for society and economy, and meet the high aims set in recently passed legislation such as the network and information security (NIS) directive [1] or the general data protection regulation (GDPR) [2]. However, a joint and well-coordinated European approach to education in this field is still missing. Given the variety and diversity of topics that need to be covered, comprising such diverse areas as information and communications technology, management and organization, law, economics, sociology, criminology and psychological issues, it becomes painstakingly clear that a wide range of expertise needs to be accessed.

2 SecTech Project

In line with those developments the Erasmus+ strategic partnership project SecTech was formed by seven European higher education institutions (KU Leuven, Luxembourg Institute of Science and Technology, Norwegian University of Science and Technology, University of Oulu, University of Plymouth, University of Regensburg, and University of Vienna) to collaboratively develop a European cybersecurity curriculum. The core motivation of SecTech is to provide a seed curriculum, including ready to use online teaching materials, to give European academic institutions a much better starting point for implementing and delivering a cyber-security education program, either on their own or in cooperation with other institutions. The primary contributions the project are aimed at supporting are the integration of knowledge that is currently available across Europe, the introduction of a curriculum template, the provision of online course materials that can serve as a core, and finally the establishment of an online repository and cooperation platform that can provide basis for a Europe wide joint educational effort. As the free sharing of the developed course materials is expected to have an essential impact, established open standards and systems such as Moodle and SCORM will form the technological basis.

3 Workshop Content

This workshop will cover the main results of the SecTech project, including:

- The collaborative SecTech cybersecurity curriculum, and its mapping as a practical implementation of the CSEC 2017 cybersecurity curricular guidelines [3]
- The content and module structure proposed in SecTech
- The content creation and delivery strategy

The session will include a demonstration of the SecTech solution and will be followed by panel discussion involving members of the project and the CSEC 2017 coordinators.

Acknowledgments. The SecTech project is funded by the European Union's Erasmus+ programme as a strategic partnership in higher education with the grant number 2016-1-LU01-KA203-013834.

References

1. The European Parliament and The Council of the European Union. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Official Journal of the European Union L 194/1 (2016)
2. The European Parliament and The Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1 (2016)
3. CSEC2017: Cybersecurity Curricula 2017 - Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, Version 1.0 Report, 31 December 2017. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

Cyber Ranges and Cyber Challenges: Proposal to Form a New TC11.8 Work Group

Stewart Kowalski[1], Basel Katt[1], Espen Torseth[1], Kirsi Helkala[2], Inge Øystein Moen[1], and Geir Olav Dyrkolbotn[1]

[1]Norwegian University of Science and Technology, Gjøvik, Norway
[2]Norwegian Defence University College, Lillehammer, Norway

1 Proposal

1.1 What Are Cyber Ranges

A cyber range is a technological platform that allows students to practice both attack and defense techniques and technologies in enclosed and monitored IT environments. The configuration of this environment can vary from a simple monolithic client server network of similar machines to complex social models with different operating systems and devices connected via complex digital eco-systems.

Given that the platform operates on an enclosed and monitored environment, a range allows a teacher to structure a student's experience in terms of difficulty and depth, and makes it possible to create game situations where students can compete against each other. Today many universities have or are creating cyber ranges alone or in cooperation as federation of cyber ranges can to both cut cost and share experiences [1].

1.2 What Are Cyber Challenges

Cyber challenges are events where participants (students and/or professionals) come together for a specified period of time and compete against each other in regard to their skills to defend and attack systems [2]. Events can stretch over days and nights and cover both technical skills and policy skills [3, 4]. Cyber challenge competitions are held both in nationally and internationally arena's with different complexity levels involving participants from a high school, college, university or expert level.

2 Relevance to TC11.8

Cyber ranges are aligned with the main aim of TC11.8 since they are helping to promote information and cyber security education at university by providing a focus facility on campus to coordinate and promote security education [1]. They also allow a technological platform to exchange experience and education modules between universities.

2.1 Goal to be Achieved During WISE

At the WISE conference, we hope to collect information about the current state of the TC11.8 members in regards to establishing, operating, and maintaining cyber range facilities. We also hope to collect experience in participating in the different types of challenges. A discussion about the pedagogical strengths and weaknesses with teaching information and cyber security on a cyber range will held and include discussions about when to use capture the flag style competitions, when to use attack/defense type exercises, and when to add policy exercises on the top of the technical exercises. Finally, we hope to discuss the possibilities to establish a federation of cyber ranges and challenges among TC.11 members.

2.2 Plans for Continued Collaboration

If sufficient interest is shown we plan to establish a network of TC.11 cyber ranges and coordinate not only the exchange of experiences and software but also hold joint competitions and challenges, remotely and onsite.

References

1. Curtis, F.: 7 University-Connected Cyber Range to Know Now, Darkread. https://www.darkreading.com/cloud/7-university-connected-cyber-ranges-to-knownow/d/d-id/1331224. Accessed 07 May 2018
2. Bashir, M., et al.: Cybersecurity competitions: the human angle. IEEE Secur. Priv. **13**, 74–79 (2015)
3. Cyber 9/12 Challenge Homepage. http://www.atlanticcouncil.org/programs/brentscowcroft-center/cyber-statecraft/cyber-9-12. Accessed 07 May 2018
4. European Cyber Challenge Homepage. https://www.europeancybersecuritychallenge.eu/. Accessed 07 May 2018

Contents

Information Security Learning Techniques

Information Security Training and Awareness

Information Security Courses and Curricula