

Lecture Notes in Networks and Systems 310

Kim-Kwang Raymond Choo

Tommy Morris

Gilbert Peterson

Eric Imsand *Editors*

National Cyber Summit (NCS) Research Track 2021

 Springer

Lecture Notes in Networks and Systems

Volume 310

Series Editor

Janusz Kacprzyk, Systems Research Institute, Polish Academy of Sciences,
Warsaw, Poland

Advisory Editors

Fernando Gomide, Department of Computer Engineering and Automation—DCA,
School of Electrical and Computer Engineering—FEEC, University of Campinas—
UNICAMP, São Paulo, Brazil

Okyay Kaynak, Department of Electrical and Electronic Engineering,
Bogazici University, Istanbul, Turkey

Derong Liu, Department of Electrical and Computer Engineering, University
of Illinois at Chicago, Chicago, USA; Institute of Automation, Chinese Academy
of Sciences, Beijing, China

Witold Pedrycz, Department of Electrical and Computer Engineering,
University of Alberta, Alberta, Canada; Systems Research Institute,
Polish Academy of Sciences, Warsaw, Poland

Marios M. Polycarpou, Department of Electrical and Computer Engineering,
KIOS Research Center for Intelligent Systems and Networks, University of Cyprus,
Nicosia, Cyprus

Imre J. Rudas, Óbuda University, Budapest, Hungary

Jun Wang, Department of Computer Science, City University of Hong Kong,
Kowloon, Hong Kong

The series “Lecture Notes in Networks and Systems” publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.


More information about this series at <http://www.springer.com/series/15179>


Kim-Kwang Raymond Choo ·
Tommy Morris · Gilbert Peterson ·
Eric Imsand
Editors


National Cyber Summit (NCS) Research Track 2021


 Springer

Editors

Kim-Kwang Raymond Choo 
Department of Information Systems
and Cyber Security
The University of Texas at San Antonio
San Antonio, TX, USA

Tommy Morris 
Department of Electrical
and Computer Engineering
University of Alabama in Huntsville
Huntsville, AL, USA

Gilbert Peterson 
Department of Electrical
and Computer Engineering
Air Force Institute of Technology
Wright-Patterson Air Force Base, OH, USA

Eric Imsand 
Information Technology and Systems
Center (ITSC)
University of Alabama in Huntsville
Huntsville, AL, USA

ISSN 2367-3370

ISSN 2367-3389 (electronic)

Lecture Notes in Networks and Systems

ISBN 978-3-030-84613-8

ISBN 978-3-030-84614-5 (eBook)

<https://doi.org/10.1007/978-3-030-84614-5>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

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, expressed 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

While governments around the world have focused on strengthening their cybersecurity posture in recent years, cybersecurity remains a topic of ongoing importance. For example, in the “Executive Order on Improving the Nation’s Cybersecurity (May 12, 2021)¹”, it was reported that:

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

As we have noted in the past years, there is a continuing need to keep a watchful brief on the cyber threat landscape, and this is the intention of this conference proceedings.

This conference proceedings contains a total of 13 papers consisting of both regular and invited papers from the 2021 National Cyber Summit Research Track. The 2021 National Cyber Summit was originally planned to be held in Huntsville, Alabama, from June 8 to 10, 2021. However, due to the COVID-19 pandemic, all tracks of the 2021 National Cyber Summit were delayed until September of 2021. The 2021 National Cyber Summit Research Track was held in-person from September 28 to 30. Authors from each selected paper presented their work and took questions from the audience.

¹<https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

The papers were selected from submissions from universities, national laboratories, and the private sector from across the USA. All of the papers went through an extensive review process by internationally recognized experts in cyber-security.

The Research Track at the 2021 National Cyber Summit has been made possible by the joint effort of a large number of individuals and organizations worldwide. There is a long list of people who volunteered their time and energy to put together the conference and deserved special thanks. First and foremost, we would like to offer our gratitude to the entire Organizing Committee for guiding the entire process of the conference. We are also deeply grateful to all the Program Committee members for their time and efforts in reading, commenting, debating, and finally selecting the papers. We also thank all the external reviewers for assisting the Program Committee in their particular areas of expertise as well as all the authors, participants, and session chairs for their valuable contributions.

Tommy Morris
Kim-Kwang Raymond Choo
Gilbert Peterson
Eric Imsand

Organization

Organizing Committee

General Chairs

Tommy Morris The University of Alabama in Huntsville, USA
Kim-Kwang Raymond Choo The University of Texas at San Antonio, USA

Program Committee Chairs

Gilbert L. Peterson Air Force Institute of Technology, USA
Eric Imsand The University of Alabama in Huntsville, USA

Program Committee and External Reviewers

Program Committee Members

Cong Pu Marshall University, USA
Jun Dai California State University, USA
Ezhil Kalaimannan University of West Florid, USA
David Dampier Marshall University, USA
Robin Verma University of Texas at San Antonio, USA
Jianyi Zhang Beijing Electronic Science and Technology
 Institute, China
Patrick Jungwirth US Army Research Laboratory, USA
Junggab Son Kennesaw State University, USA
Reza M. Parizi Kennesaw State University, USA
Jaewoo Lee University of Georgia, USA
Vahid Heydari Rowan University, USA
Yifei Wang Alipay, USA
Wei Zhang University of Louisville, USA

David Coe	University of Alabama in Huntsville, USA
Junghee Lee	Korea University, South Korea
Huijun Wu	Arizona State University, USA
Ravi Rao	Fairleigh Dickinson University, USA
Rongxing Lu	University of New Brunswick, Canada

External Reviewers

Einaam Alim
Raphael Barata
Pinyao Guo
Hussam Al Hamadi
David Hayes
Erdal Kose
Yaoqing Liu
Zach Tackett
Chunxu Tang
Benjamin Turnbull
Xiaolu Zhang
Shaohua Wang

Contents

Cyber Security Education

An Integrated System for Connecting Cybersecurity Competency, Student Activities and Career Building	3
Li-Chiou Chen, Andreea Cotoranu, Praviin Mandhare, and Darren Hayes	
Simulating Industrial Control Systems Using Node-RED and Unreal Engine 4	13
Steven Day, William “Kohler” Smallwood, and Joshua Kuhn	
Student Educational Learning Experience Through Cooperative Research	22
Melissa Hannis, Idongesit Mkpogon-Ruffin, and Drew Hamilton	
Digital Forensics Education: Challenges and Future Opportunities	28
Megan Stigall and Kim-Kwang Raymond Choo	
Designing a Cybersecurity Curriculum Library: Best Practices from Digital Library Research	47
Blair Taylor, Sidd Kaza, and Melissa Dark	
Design of a Virtual Cybersecurity Escape Room	60
Tania Williams and Omar El-Gayar	
Cyber Security Technology	
A Novel Method for the Automatic Generation of JOP Chain Exploits	77
Bramwell Brizendine and Austin Babcock	
Increasing Log Availability in Unmanned Vehicle Systems	93
Nickolas Carter, Peter Pommer, Duane T. Davis, and Cynthia E. Irvine	

Testing Detection of K-Ary Code Obfuscated by Metamorphic and Polymorphic Techniques 110
George T. Harter and Neil C. Rowe

Enhancing Secure Coding Assistant System with Design by Contract and Programming Logic. 124
Wenhui Liang, Cui Zhang, and Jun Dai

Social Engineering Attacks in Healthcare Systems: A Survey 141
Christopher Nguyen, Walt Williams, Brandon Didlake, Donte Mitchell, James McGinnis, and Dipankar Dasgupta

Identifying Anomalous Industrial-Control-System Network Flow Activity Using Cloud Honeypots. 151
Neil C. Rowe, Thuy D. Nguyen, Jeffery T. Dougherty, Matthew C. Bieker, and Darry Pilkington

Risks of Electric Vehicle Supply Equipment Integration Within Building Energy Management System Environments: A Look at Remote Attack Surface and Implications 163
Roland Varriale, Ryan Crawford, and Michael Jaynes

Author Index. 175

Cyber Security Education



An Integrated System for Connecting Cybersecurity Competency, Student Activities and Career Building

Li-Chiou Chen^(✉), Andreea Cotoranu, Praviin Mandhare, and Darren Hayes

Pace University, New York, NY 10038, USA

{lchen, acotoranu, pmamdhare, dhayes}@pace.edu

Abstract. For educators, preparing students who are able to solve cybersecurity problems requires not only a curriculum that provides students with interdisciplinary knowledge but also activities that develop their skills and competencies to solve problems that call for an interdisciplinary approach. To facilitate this process, we have developed a system called Cyberpassport, which integrates students' academic and career goals with cybersecurity co-curricular activities. This system is designed for students to search and register for cybersecurity activities, and track their own progress, for advisors to support their mentoring efforts, and for activity hosts such as faculty members or industry professionals to facilitate connection with interested students. Usability testing was conducted to test the application's functionality as well as user experience and interest. Preliminary results indicate that users found the system easy to use and beneficial for a career in cybersecurity. Furthermore, this is the first mobile events app developed that aligns with the skills and competencies defined by the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework.

Keywords: Cybersecurity education · Competency · Workforce · Usability

1 Introduction

Cybersecurity has emerged as an academic discipline because of its importance for organizations in the digital era, in addition to the sophistication of knowledge and skills needed for cybersecurity professionals. The Association for Computing Machinery's (ACM's) Joint Task Force on Cybersecurity Education [1] defined cybersecurity as "a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management." For educators, preparing students to solve cybersecurity problems requires not only a curriculum that provides students with the knowledge and topics that are interdisciplinary in nature but also activities that develop their skills and abilities to solve these interdisciplinary problems. In addition, connecting with cybersecurity professionals and learning from them are important steps in developing a career in cybersecurity.

To facilitate this process, we have developed a system called Cyberpassport, which integrates students' academic and career goals with cybersecurity co-curricular activities. This system is designed to enable students to search and register for cybersecurity activities, track their own progress, support advisors in their mentoring efforts, and facilitate activity/conference hosts (e.g. faculty members or industry professionals) to connect with interested students. In addition, the system will allow students to generate a resume using information captured in the system, including activities that are labeled with skills and competencies defined in the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework [2], which they can ultimately share with potential employers.

Cyberpassport enables students to connect with professional development training or co-curricular activities. The system aims to integrate students' career goals with cybersecurity training sessions, while allowing students to connect to these sessions. Using either the Cyberpassport mobile app or the Cyberpassport website, users of the system can host, search, register and record these training sessions, and detail the skills/competencies that they have learned. Students can then track their progress, review their skill set with faculty mentors or academic advisors, or share the information with potential employers, like a resume on-the-go. The cyber skills utilized in the system aligns with the knowledge/skills outlined in the NICE cybersecurity workforce framework, which is helpful for students when planning for their cyber career development.

Industry professionals can also leverage Cyberpassport to organize cyber activities that can be searched by students. The system allows users to create an event, such as a training session or a workshop. After being reviewed and approved by the administrator of its organization, the event will become available and searchable by all of the registered users. The system also has the potential to be used by employers interested in finding cybersecurity talents via event hosting, if students opt to share their information with employers.

We would like to engage the cybersecurity community in adopting Cyberpassport. The system is scalable and can accommodate a diverse range of cybersecurity activities offered throughout the community. The value of the system will ultimately depend on the number of events that will be entered into the system, and the number of students who will adopt the system. Once the system achieves a critical mass, it will help students to identify and record cybersecurity activities related to the knowledge and skills they aim to strengthen, while assisting advisors seeking to guide students towards meeting their academic and professional goals. This system is unique in the way that it connects students with cybersecurity activities, and can contribute to strengthening the students' knowledge and skills needed for a career in the field.

2 Literature Review

Fostering student competencies in cybersecurity education is critical. The consensus amongst educators is that cybersecurity students should not only obtain theoretical knowledge but should also be trained with the skills and abilities to perform cybersecurity related tasks. NIST's NICE framework [2] defines "competency" as a mechanism for organizations or educators to assess student's overall ability to accomplish a prescribed

project, which can be described as a set of tasks, knowledge, and skills. For instance, an example of a “data analysis” competency could be “The collecting, synthesizing, or analyzing qualitative and quantitative data and information from a variety of sources to reach a decision, make a recommendation, and/or compile reports, briefings, executive summaries, and other correspondence” [2]. The Department of Labor’s Employment and Training Administration (ETA) has also defined a Cybersecurity Competency Model [3], which compliments the NICE framework by adding competencies required by the average worker who uses the Internet or an organization’s computer network. The National Security Agency/Department of Homeland Security’s designation of National Center for Academic Excellence in Cybersecurity (NCAE-C) has also emphasized the importance of competency in cybersecurity education.

Competency has also been defined as a qualification for jobs and assessed by an assessment body to provide industry certifications. Assessment organizations, such as CompTIA, EC-Council, have utilized many techniques to assess the competency of cybersecurity professionals. A previous study [4] analyzed these techniques used for industry certifications and the perception of employers and the efficacy of competency assessment techniques. The study found that multiple choice examinations, used in many certification exams, are perceived as the least effective assessment method, while the qualification bodies use these most frequently. Oral examination, virtual lab examination, employment history and a review of qualifications are perceived as more effective but are used less frequently in the assessment by a qualification body. Another study [5] surveyed cybersecurity professionals and educators and assessed the preparedness of cybersecurity students in terms of competency. The study highlighted the importance of workplace competencies, as perceived by both professionals and educators.

There is a chasm between educators and employers in terms of training students to establish and assess competencies. We designed the Cyberpassport system to bridge the gap so that students can use the tool to explore potential cybersecurity job roles, plan and build competencies needed for these roles, and use the system to document their achievements.

3 The Cyberpassport System

3.1 System Design

As shown in Fig. 1, Cyberpassport is designed as a Web service catering to activity hosts, students, faculty advisors, and employers. CPS is designed specifically for students interested in a career in cybersecurity and allows them to search and sign up for cybersecurity co-curricular activities, such as workshops in a conference, research discussions on campus, or cybersecurity competition training.

Although the approach is conventional in the design and the security features, the innovation of the system is the integration of the design with cybersecurity education, in particular the NICE cybersecurity workforce framework. The hosts of these activities (activity hosts) can use the CPS as a mechanism to promote their cybersecurity activities by adding them to the system and labeling them with the knowledge/skill information defined by the NICE cybersecurity workforce framework.

Moreover, faculty advisors can mentor students based on the types of activities available, activities attended, and the knowledge/skills that the students need in order to achieve their career goals.

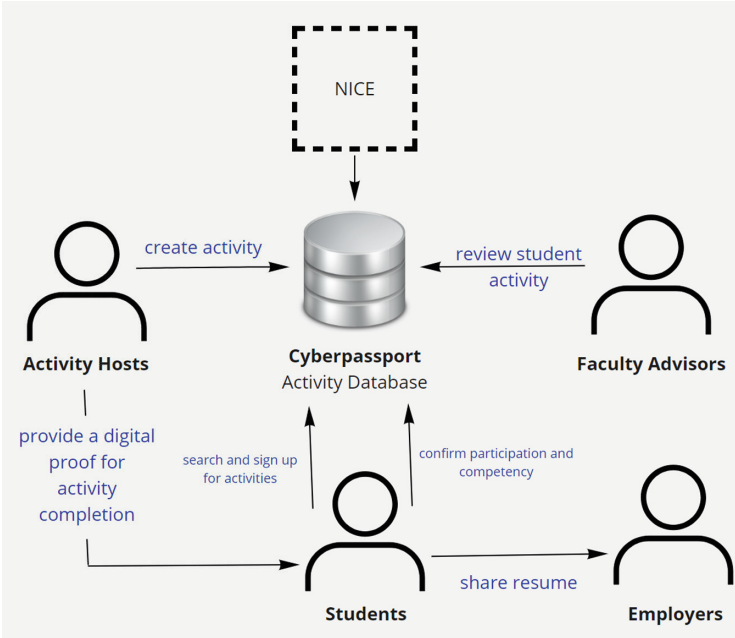


Fig. 1. An illustration of the Cyberpassport system.

Cyberpassport uses a method similar to challenge-response authentication, such as MS-CHAP or PPP-CHAP [6] but incorporates a mobile application to obtain some information required to validate student participation in activities. The system examines a *digital proof* from a student to validate participation. The activity host provides some validation when the activity is satisfactorily completed and the student provides yet another validation.

Activity hosts can register activity information, such as event date, time, duration, name, NICE competency identifier, and an associated URL that contains detailed information about the activity, such as an event website. Each activity is associated with an activity identifier which is stored in the system. A hash of the activity identifier, called an *activity hash*, is used later to confirm completion of the activity.

Students are able to browse and sign up for activities using a client-side mobile application. When the student creates an account in the system, the system generates a student identifier, which is encrypted and stored on the system. A hash of the student identifier, called the *student hash*, is sent to the student and stored on the end-user device, such as within a mobile application. When the student signs up for an activity, the system generates and stores a *digital proof*, which is a hash of the combined value of the activity hash, the student hash, and a password. The digital proof is only used by the system and is concealed from other users at this point.

When a student completes an activity and the activity host is satisfied with their participation, the activity host provides the student with the activity hash, implemented in the form of a QR code generated from the system. The students' client-side interface, either the Web interface or the mobile application, generates a digital proof using the activity hash obtained from the activity host, the student hash stored in their mobile application or Web interface previously, and the password that the student knows. This digital proof is sent to the system and the system validates the participation by comparing this digital proof with the one stored in the system previously. If these two hashes match, the student has a completion record, which shows the student has completed training on a specific NICE competency for a specific duration (e.g. two hours).

Students are also able to use Cyberpassport to generate a resume-like record that reflects the cybersecurity activities completed, and which can be used for employment purposes. Furthermore, advisors could use the system to review student progress and make recommendations for further academic or professional development.

3.2 Implementation

We have implemented Cyberpassport¹ both as a Web application as well as mobile applications for both iOS and Android. The Web application provides access to activity hosts, faculty advisors and students. The mobile applications are developed for students to browse the cybersecurity activities, scan the activity hashes after completing an activity, and send a digital proof to the system.

User Interface. Both a mobile app and a website (Fig. 2) have been developed. The front-end user interfaces, for Web and mobile, are connect to a MySQL database hosted on a Linux server at our university. Users can use either the website or the mobile app to access the system. Both interfaces provide the same functionality.

Cyberpassport QR Code. Once a user creates an account, the user is assigned a unique identifier, called a Cyberpassport number, which can be displayed as a QR code.

¹ Cyberpassport is available as a Web application at cyberpassport.pace.edu, and as a mobile apps at both Apple Store and Google Play.

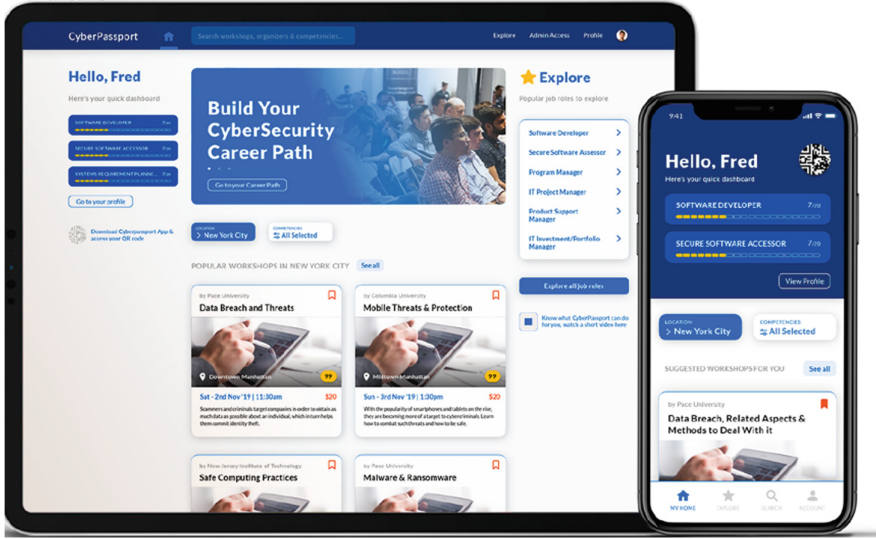


Fig. 2. Cyberpassport Web application and mobile application.

Cybersecurity Event Hosting. A user can create a cybersecurity event, which is defined as a cybersecurity skill training session, for one to three hours (Fig. 3(a)). Each event needs to be a physical or virtual gathering, with an actual date/time and location. Additionally, each event is required to list competencies or skills that are defined in NIST’s NICE Framework. Once an event has been created, it will be reviewed by the Cyberpassport system administrator to ensure that the event is appropriately labeled and that its content is cybersecurity related. Once the event is approved by the administrator, users can then register for the event.

Event Registration. A user can search for cybersecurity events based on NICE skills or other keywords (Fig. 3(b)). Once a desired event is identified, the user can register for it and the host will have access to the list of event attendees.

Event Participation. The event host will scan the user’s Cyberpassport QR code only if the participant attends the entire event.

Cyberpassport Skills. Users can review and demonstrate the skills that they have acquired from various events using their Cyberpassport mobile app. Users can also explore cybersecurity job roles defined in the NICE framework (Fig. 3(c)).

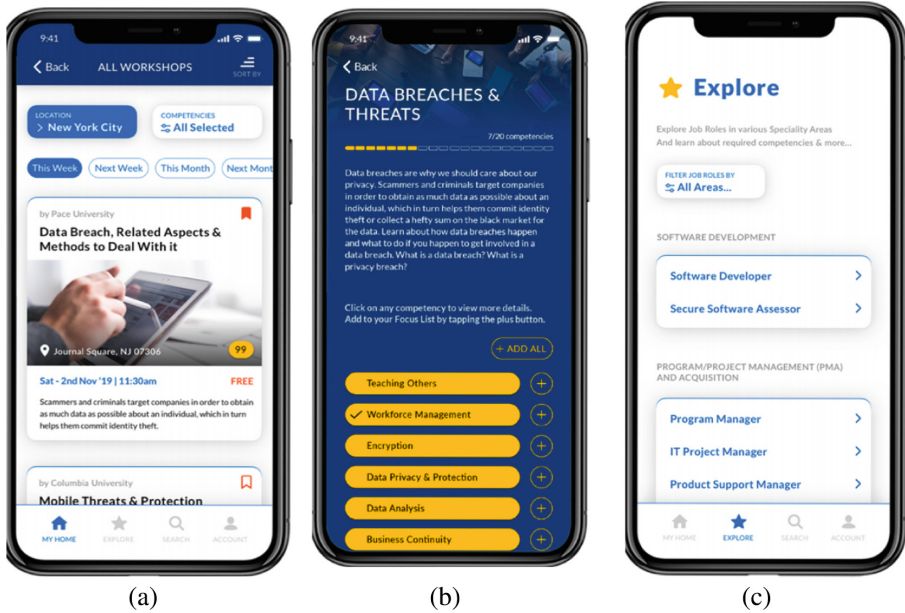


Fig. 3. Cyberpassport mobile applications. 3(a) Cybersecurity event; 3(b) Search events using NICE Competency. 3(c) Explore cybersecurity job roles.

4 Usability Testing

To determine whether Cyberpassport was easy to use, understandable, and satisfied the end user needs, we conducted four rounds of user studies. Of these user studies, three were conducted for the Web application, and one was performed for the mobile application. We reiterated the Cyberpassport interface design based on end user feedback, following each round of testing. In addition, we designed a questionnaire to collect data and to evaluate the end user's perception in using the application based on the Technology Acceptance Model [7]. The questionnaire included a combination of open ended and multiple-choice questions. The questionnaire focused on usability as it pertains to key application functions as well as evaluating the end user's perceived usability and perceived ease of use when using Cyberpassport.

We created and hosted a series of events to provide context to the user studies, and gathered user feedback on the application. These events included three workshops on the topic of “*Cybersecurity Analytics with Python*,” and one presentation on “*Cybersecurity Careers: Knowledge, Skills and Abilities*.” The events were promoted through the school and Cybersecurity Club social media channels, which connect with undergraduate and graduate students at our institution. The Cybersecurity Club students were a relevant end-user population because of their affirmed interest in cybersecurity. The total number of event participants was 68, and we collected a total of 53 complete responses. Of these responses, many were from participants in more than one study.

The event invitations directed students to create an account with Cyberpassport, and to register for each event using the application. All tests were conducted virtually, over