ISBN: 979-8-3503-3286-5

2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC)

8th -11th March 2023

Virtual Conference

SPONSORS

Editors
Prof. Rajashree Paul

About the Conference

IEEE CCWC 2023

We are proud to present **IEEE CCWC 2023** that will provide an opportunity for researchers, educators and students to discuss and exchange ideas on issues, trends, and developments in Information Technology, Electronics and Mobile Communication. The conference aims to bring together scholars from different disciplinary backgrounds to emphasize dissemination of ongoing research in the fields of computing and Mobile Communication. Contributed papers are solicited describing original works in the above-mentioned fields and related technologies. The conference will include a peer-reviewed program of technical sessions, special sessions, business application sessions, and demonstration sessions.

All accepted papers will be presented during the parallel sessions of the Conference and the accepted and presented papers will be submitted for publication at IEEE Xplore® digital library (Scopus, Science Direct, Google Scholar).

This conference will also promote an intense dialogue between academia and industry to bridge the gap between academic research, industry initiatives, and governmental policies. This is fostered through panel discussions, keynotes, invited talks and industry talks where academia is exposed to state-of-practice and results from trials and interoperability experiments. The industry in turn benefits by exposure to leading-edge research in networking as well as the opportunity to communicate with academic researchers regarding practical problems that require further research.

Copyright

2023 IEEE 13th Annual Computing and Communication

Workshop and Conference (CCWC).

IEEE Catalog Number: CFP23CWA-ART

ISBN: 979-8-3503-3286-5

Our Reviewers

IEEE CCWC 2023 followed a rigorous single-blind review process in order to identify suitable papers for both presentation and publication. This process helped the organizers to shortlist good quality papers from diverse regional areas and across various domains. This edited book also incorporates four invited papers from experts across the globe. The congress received more than three hundred full papers for review and approximately forty percent were selected for full paper submission. In the end, one seventy three papers, including invited papers were found acceptable for presentation and congress proceedings.

Such a detailed review process was possible due to the excellent and enthusiastic support extended by the strong technical review team of IEEE CCWC 2023. For every stage of submission, CCWC had a specific template review procedure to analyze the submissions and provide suitable comments for the authors to incorporate.

Organizing Committee

General Co-Chairs

- Son Vuong (University of British Columbia)

Technical Co-Chairs

- Phillip Bradford (University of Connecticut, USA)
- Rajashree Paul (University of Engineering & Management)

Financial chair

- Rajashree Paul (University of Engineering & Management)

Technical Program Committee

- Heba Affify (Cairo University)
- Mohd Ashraf Ahmad (Universiti Malaysia Pahang)
- Cajetan Akujuobi (Prairie View A&M University)
- Hussain Al-Asaad (University of California, Davis)
- Md. Golam Rabiul Alam (BRAC University)
- Md L Ali (Rider University)
- Ali Abdullah S. AlQahtani (North Carolina A&T State University)
- Wolfgang Bein (University of Nevada, Las Vegas)
- Noureddine Chabini (Royal Military College of Canada)
- Satyajit Chakrabarti (Insitute of Engineering and Management)
- Deepak Chandramouli (Apple)
- Sudarshan S Chawathe (University of Maine)
- Udhaya Kumar Dayalan (Trane Technologies)
- Cleonilson Protasio de Souza (Federal University of Paraiba)
- Dharati Dholariya (Rashtriya Raksha University)
- Sven Dominka (Robert Bosch AG)
- Pallav Dutta (Aliah University)
- Heba Elgazzar (Morehead State University)
- Francisco de Asis Lopez Fuentes (UAM-Cuajimalpa)
- Mohammad Reza Ghavidel Aghdam (Özyeğin University)
- Khan Md Hasib (Bangladesh University of Business and Technology)

- William C Headley (Virginia Tech)
- Krutthika Hirebasur Krishnappa (Dayananda Sagar College of Engineering)
- Md Hossain (Southern Connecticut State University)
- Shrikant S Jadhav (San Jose State University)
- Sandip Jana (IIT Hyderabad)
- James Jones (George Mason University)
- Bhargavi K (Viveswaraya Technological University)
- Eman Abdelfattah (Sacred Heart University)
- S Kannadhasan (Study World College of Engineering)
- Mohammed Zafar Ali Khan (Indian Institute of Technology Hyderabad)
- Basar Koc (Stetson University)
- Rajasekhar Konda (Apple)
- Karthik Krishnamoorthy (Micron Technology)
- Krutthika Krishnappa (Dayananda Sagar College of Engineering)
- Renato R. Maaliw (Southern Luzon State University)
- Ryan P Michaels (St Edward's University)
- Muath Obaidat (City University of New York)
- Ammar J Odeh (Princess Sumaya University for Technology)
- Marcelo Okano (CEETEPS)
- George A Papakostas (International Hellenic University)
- Rajvardhan Patil (Grand Valley State University)
- Stefan Pickl (UBw Munich)
- Arisoa S. Randrianasolo (Abilene Christian University)
- Hayssam El- Razouk (California State University, Fresno)
- Jiajia Shi (The Chinese University of Hong Kong)
- Yong Shi (Kennesaw State University)
- Raghubir Singh (University of Bath)
- Kanika Sood (California State University, Fullerton)
- Xiaoyuan Suo (Webster University)
- Christian Trefftz (Grand Valley State University)
- Nur Uddin (Universitas Pembangunan Jaya)
- Washington Velasquez (Escuela Superior Politecnica del Litoral)
- Zhaohong Wang (California State University, Chico)
- Yuan Xing (University of Wisconsin-Stout)
- Sotirios Ziavras (New Jersey Institute of Technology)
- Lidong Wang (Mississippi State University)
- Vipul Bansal (CME Group, Chicago)

Keynote Speakers

CORPORATE KEYNOTE SERIES

Sami Abu-El-Haija (Senior Research Scientist, Google Research)

Bio: Sami is a Senior Research Scientist at Google Research, working at the Algorithms & Optimizations research group. He has published several papers in top-tier venues. He studied at top-tier institutions. Most recently, at the University of Southern California for his PhD.

Talk Title: Initializing deep Fully-connected Neural Networks with closed-form solutions.

Abstract : Feed-forward neural networks -- such as, Graph Neural Networks (GNNs) achieve outstanding empirical performance on several prediction tasks -- such as link prediction and node classification, on graphs, e.g., on social or biological graphs. However, state-of-the-art (SOTA) models require long training time (hours-to-days, even on expensive GPUs). On the other hand, shallow (1-layer) neural networks pose convex objective functions. In some cases, their optimal parameters can be estimated in closed-form, without calculating gradients. Sami will describe his journey in explaining a new kind of deep neural networks, that are specially hand-crafted, such that, on one hyperplane in their parameter space, the networks will be equivalent to standard MLP network with ReLu activation. On another hyperplane, the network becomes linear in its parameters. Such networks can be initialized, in closed-form, by restricting projecting their parameters onto the linear hyperplane. Afterwards, these networks can be fine-tuned in the usual regime. In his experiments, such a training paradigm can speed-up training hundreds or thousands of times.

Pin-Yu Chen (Principal Research Scientist, IBM)

Bio: Dr. Pin-Yu Chen is a principal research scientist at IBM Thomas J. Watson Research Center, Yorktown Heights, NY, USA. He is also the chief scientist of RPI-IBM AI Research Collaboration and PI of ongoing MIT-IBM Watson AI Lab projects. Dr. Chen received his Ph.D. in electrical engineering and computer science from the University of Michigan, Ann Arbor, USA, in 2016. Dr. Chen's recent research focuses on adversarial machine learning and robustness of neural networks. His long-term research vision is to build trustworthy machine learning systems. At IBM Research, he received several research accomplishment awards, including an IBM Master Inventor and IBM Corporate Technical Award in 2021. His research contributes to IBM open-source libraries including Adversarial Robustness Toolbox (ART 360) and AI Explainability 360 (AIX 360). He has published more than 50 papers related to trustworthy machine learning at major AI and machine learning conferences, given tutorials at NeurIPS'22, AAAI'22, IJCAI'21, CVPR('20,'21), ECCV'20, ICASSP'20, KDD'19, and Big Data'18, and organized several workshops for adversarial machine learning. He received the IEEE GLOBECOM 2010 GOLD Best Paper Award and UAI 2022 Best Paper Runner-Up Award.

Talk Title: AI Model Inspector: Towards Holistic Adversarial Robustness for Deep Learning

Abstract: In this talk, I will share my research journey toward building an AI model inspector for evaluating, improving, and exploiting adversarial robustness for deep learning. I will start by providing an overview of research topics concerning adversarial robustness and machine learning, including attacks, defenses, verification, and novel applications. For each topic, I will summarize my key research findings, such as (i) practical optimization-based attacks and their applications to explainability and scientific discovery, (ii) Plug-and-play defenses for model repairing and patching, and (iii) attack-agnostic robustness assessment. Finally, I will conclude my talk with my vision of preparing deep learning for the real world and the research methodology of learning with an adversary.

Ben Adlam
(Research Scientist ,Google Brain)

Bio: Dr Ben is a Research Scientist at Google Brain working to understand deep learning and apply it to basic-science problems. He joined Google in 2018 as an AI Resident, and before that he was a PhD student in applied math at Harvard, where he used techniques from probability theory and stochastic processes to study evolutionary dynamics and random matrices.

Talk Title: Kernel Regression with Infinite-Width Neural Networks on Millions of Examples

Abstract: While kernel regression remains an important practical method, its connection to neural networks as their width becomes large has initiated fresh research. These neural kernels have drastically increased performance on diverse and nonstandard data modalities but require significantly more compute, which previously limited their application to smaller datasets. In this work, we address this by massively parallelizing their computation across many GPUs. We combine this with a distributed, preconditioned conjugate gradients algorithm to enable kernel regression at a large scale (i.e. up to five million examples). Using this approach, we study scaling laws of several neural kernels across many orders of magnitude for the CIFAR-5m dataset. Using data augmentation to expand the original CIFAR-10 training dataset by a factor of 20, we obtain a test accuracy of 91.2% (SotA for a pure kernel method). Moreover, we explore neural kernels on other data modalities, obtaining results on protein and small molecule prediction tasks that are competitive with SotA methods.

RESEARCH KEYNOTE SERIES

Michael Bronstein

(Professor, University of Oxford, UK)

BIO: Michael Bronstein is the DeepMind Professor of AI at the University of Oxford and Head of Graph Learning Research at Twitter. He was previously a professor at Imperial College London and held visiting appointments at Stanford, MIT, and Harvard, and has also been affiliated with three Institutes for Advanced Study (at TUM as a Rudolf Diesel Fellow (2017-2019), at Harvard as a Radcliffe fellow (2017-2018), and at Princeton as a short-time scholar (2020)). Michael received his PhD from the Technion in 2007. He is the recipient of the Royal Society Wolfson Research Merit Award, Royal Academy of Engineering Silver Medal, five ERC grants, two Google Faculty Research Awards, and two Amazon AWS ML Research Awards. He is a Member of the Academia Europaea, Fellow of IEEE, IAPR, BCS, and ELLIS, ACM Distinguished Speaker, and World Economic Forum Young Scientist. In addition to his academic career, Michael is a serial entrepreneur and founder of multiple startup companies, including Novafora, Invision (acquired by Intel in 2012), Videocites, and Fabula AI (acquired by Twitter in 2019).

Talk Title: Physics-inspired learning on graphs

Abstract: The message-passing paradigm has been the “battle horse” of deep learning on graphs for several years, making graph neural networks a big success in a wide range of applications, from particle physics to protein design. From a theoretical viewpoint, it established the link to the Weisfeiler-Lehman hierarchy, allowing to analyse the expressive power of GNNs. We argue that the very “node-and-edge”-centric mindset of current graph deep learning schemes may hinder future progress in the field. As an alternative, we propose physics-inspired “continuous” learning models that open up a new trove of tools from the fields of differential geometry, algebraic topology, and differential equations so far largely unexplored in graph ML.

Aldo Faisal

(Professor, Imperial College London, UK)

Professor Aldo Faisal (@FaisalLab) is the Professor of AI & Neuroscience at the Dept. of Computing and the Dept. of Bioengineering at Imperial College London (UK) and Chair of Digital Health at the University of Bayreuth (Germany). In 2021 he was awarded a prestigious 5-year UKRI Turing AI Fellowship. Since 2019, Aldo is the founding director of the £20Mio UKRI Centre for Doctoral Training in AI for Healthcare, and leads the Behaviour Analytics Lab at the Data Science Institute, London. Aldo works at the interface of Machine Learning, Medicine and translational Biomedical Rngineering to help people in diseases and health. He currently is one of the few engineers world-wide that lead their own clinical trials to validate their technology. In this space his works focusses on Digital Biomarkers and AI for medical intervention (Makin et al,Nat Biomed Eng; Komorowski et al, NatMed, 2018; Gottessmann et al NatMed, 2019). His work received a number of prizes and awards, including the $50,000 Research Discovery Prize by the Toyota Foundation.

Talk Title: Ethomics - the AI-enabled way to understand human behaviour

Abstract : Here we present a novel AI-driven approach to human behaviour analytics called Ethomics (Kadirvelu et Faisal, 2023, Nature Medicine, Ricotti et Faisal, 2023, Nature Medicine) that allows unprecedented resolution in diagnosing and measuring disease progression. We apply the same AI framework to two very different degenerative diseases affecting adults (Friedreichs) and children (Duchenne). Crucially the AI method detects imperceptible changes to human behaviour that allows us to measure gene transcription rates from movement changes alone and can predict each individual patient's disease trajectory up to a year into the future. Our ethomics technology allows us therefore to dramatically de-risk and accelerate drug development for rare diseases, as it allows us to cut the duration of clinical trials in half and requires only a fraction of patients to determine if a treatment is working compared to current „gold"-standard methods.

Faramarz Fekri

(Professor, Georgia Tech University, USA)

Bio: Dr. Fekri is a Professor of ECE and a GTRI Fellow at Georgia Tech. He is one of the leading researchers in Statistical Signal Processing, information theory, graphical models, inductive logic reasoning and machine learning with applications to communications, biology, robotics and artificial intelligence. He is an IEEE Fellow and a faculty member of the Georgia Tech Center in Machine Learning. Dr. Fekri received the Faculty Research Innovation Award by Sony Inc, Samsung GRO Award, National Science Foundation CAREER Award, Southern Center for Electrical Engineering Education Young Faculty Development Award, and Outstanding Young faculty Award of the School of ECE. He serves on the Technical Program Committees of several IEEE/ACM conferences. He is currently an Associate Editor in IEEE Transactions on Molecular, Biological, and Multi-Scale Communications. In the past, he served on the editorial board of the IEEE Transactions on Communications, and the Elsevier Journal on PHYCOM.

Talk Title: A Machine Learning Framework for Distributed Functional Compression over

Abstract : Deep Learning has revolutionized machine learning and has expanded its reach into many diverse fields, from autonomous driving to augmented reality and distributed IoT devices. Not unexpectedly, this has also led to deep- learning based design of communication systems. In particular, in all these applications, we often need to compute specific target functions that do not have any simple forms, e.g., obstacle detection, object recognition, etc. However, traditional cloud-based methods that focus on transferring data to a central location either for training or inference place enormous strain on wireless network resources. To address this, we develop a machine learning framework for distributed functional compression over wireless channels. We advocate that our machine learning framework can, by design, compute any arbitrary function for the desired functional compression task in IoT. In particular, the raw sensory data are never transferred to a central node for training or inference, thus reducing communication overhead. For these algorithms, we provide theoretical convergence guarantees and upper bounds on communication. Our simulations show that the learned encoders and decoders for functional compression perform significantly better than traditional approaches, are robust to channel condition changes and sensor outages. Compared to the cloud-based scenario, our algorithms reduce channel use by two orders of magnitude. Finally, we turn our attention to the problem of privacy in the distributed functional compression, where the node(s) are looking to hide private attributes correlated with the function value. We first study the single node and receiver problem. We then return to the distributed functional compression problem and devise a framework that demonstrates a state-of-the-art privacy-utility trade-off in the distributed scenario.

Yuejie Chi
(Professor, Carnegie Mellon University)

Bio: Dr. Yuejie Chi is a Professor in the department of Electrical and Computer Engineering, and a faculty affiliate with the Machine Learning department and CyLab at Carnegie Mellon University. She received her Ph.D. and M.A. from Princeton University, and B. Eng. (Hon.) from Tsinghua University, all in Electrical Engineering. Her research interests lie in the theoretical and algorithmic foundations of data science, signal processing, machine learning and inverse problems, with applications in sensing, imaging, decision making, and societal systems, broadly defined. Among others, Dr. Chi received the Presidential Early Career Award for Scientists and Engineers (PECASE) and the inaugural IEEE Signal Processing Society Early Career Technical Achievement Award for contributions to high-dimensional structured signal processing. She is an IEEE Fellow (Class of 2023) for contributions to statistical signal processing with low-dimensional structures.

Talk Title: Accelerating Ill-conditioned Low-rank Estimation via Scaled Gradient Descent

Abstract: Many problems encountered in science and engineering can be formulated as estimating a low-rank object from incomplete, and possibly corrupted, linear measurements; prominent examples include matrix completion and tensor completion. Through the lens of matrix and tensor factorization, one of the most popular approaches is to employ simple iterative algorithms such as gradient descent to recover the low-rank factors directly, which allow for small memory and computation footprints. However, the convergence rate of gradient descent depends linearly, and sometimes even quadratically, on the condition number of the low-rank object, and therefore, slows down painstakingly when the problem is ill-conditioned. This talk introduces a new algorithmic approach, dubbed scaled gradient descent (ScaledGD), that provably converges linearly at a constant rate independent of the condition number of the low-rank object, while maintaining the low per-iteration cost of gradient descent. A nonsmooth variant of ScaledGD provides further robustness to corruptions by optimizing the least absolute deviation loss. In addition, ScaledGD continues to admit fast global convergence, again almost independent of the condition number, from a small random initialization when the rank is over-specified. In total, ScaledGD highlights the power of appropriate preconditioning in accelerating nonconvex statistical estimation, where the iteration-varying preconditioners promote desirable invariance properties of the trajectory with respect to the symmetry in low-rank factorization.

Ehsan Afshari

(Professor, University of Michigan)

Bio: Prof. Afshari received his Ph.D. EE from Caltech in 2006 and joined the ECE department of Cornell University. Ten years later, he joined the EECS department of the university of Michigan, Ann Arbor. His team is engaged in the theoretical foundations, design and experimental validation of analog, RF, mm-wave, and THz integrated devices, circuits and systems for a variety of applications including communications, imaging, and sensing. His work is funded by federal agencies such NSF, DARPA, ONR, and ARL as well as industry such as Intel, TI, Raytheon, and Qualcomm. He has been the recipient of several awards and honors, including a 2008 DARPA Young Faculty Award, a 2010 NSF CAREER Award, a first place at Stanford-Berkeley-Caltech Innovation Challenge in 2005, and several best paper awards at the leading conferences in his field. He has also served as a Distinguished Lecturer for the IEEE Solid-State Circuits Society. He is selected as one of 50 most distinguished alumni of Sharif University. His doctoral students have also received several prestigious awards and fellowships, including the 2018, 2017, 2012, 2011, and 2010 Solid-State Circuit Society Predoctoral Achievement Award, 2011, 2013, and 2017 IEEE MTT-S Microwave Engineering Graduate Fellowships, Cornell Best Ph.D. Thesis Award in 2011 and 2014, as well as many best paper awards. The Ph.D. graduates of his group are the leaders of the field including faculty members at MIT, UC Davis, UC Irvine, Penn State University, and University of Minnesota, and companies such as IBM, Bell Labs, Qualcomm and Broadcom.

Talk Title: Superman Vision: Fully Integrated Terahertz Imaging Radar in CMOS

Abstract: The increasing demands for compact, low-cost, and high-resolution imaging radar systems have pushed the operation frequency to the terahertz range due to the shorter wavelength and larger available bandwidth. These radars can be used in security screening, industrial quality control and biological hydration sensing applications. In this talk, we review basics of imaging radar systems as well as recent advances in this area.

Alexandre Bayen (Professor, UC Berkeley)

Bio: Alexandre Bayen is the Associate Provost for Moffett Field Program Development at UC Berkeley, and the Liao-Cho Professor of Engineering at UC Berkeley. He is a Professor of Electrical Engineering and Computer Science(link is external), and Civil and Environmental Engineering(link is external). From 2014 - 2021, he served as the Director of the Institute of Transportation Studies(link is external) at UC Berkeley (ITS). He is also a Faculty Scientist in Mechanical Engineering, at the Lawrence Berkeley National Laboratory(link is external) (LBNL). He received the Engineering Degree in applied mathematics from the Ecole Polytechnique, France, in 1998, the M.S. and Ph.D. in aeronautics and astronautics from Stanford University in 1999 and 2004, respectively. He was a Visiting Researcher at NASA Ames Research Center from 2000 to 2003. Between January 2004 and December 2004, he worked as the Research Director of the Autonomous Navigation Laboratory at the Laboratoire de Recherches Balistiques et Aerodynamiques, (Ministere de la Defense, Vernon, France), where he holds the rank of Major. He has been on the faculty at UC Berkeley since 2005. Bayen has authored two books and over 200 articles in peer reviewed journals and conferences. He is the recipient of the Ballhaus Award from Stanford University, 2004, of the CAREER award from the National Science Foundation, 2009 and he is a NASA Top 10 Innovators on Water Sustainability, 2010. His projects Mobile Century and Mobile Millennium received the 2008 Best of ITS Award for 'Best Innovative Practice', at the ITS World Congress and a TRANNY Award from the California Transportation Foundation, 2009. Mobile Millennium has been featured more than 200 times in the media, including TV channels and radio stations (CBS, NBC, ABC, CNET, NPR, KGO, the BBC), and in the popular press (Wall Street Journal, Washington Post, LA Times). Bayen is the recipient of the Presidential Early Career Award for Scientists and Engineers (PECASE) award from the White House, 2010. He is also the recipient of the Okawa Research Grant Award, the Ruberti Prize from the IEEE, and the Huber Prize from the ASCE.

Talk Title: The MegaVanderTest.

Abstract: This lecture will present the story of the MegaVanderTest, a test involving 103 self-driving vehicles, which ran on Nov. 18, 2022 on I24 in Nashville, TN. The MegaVanderTest is

to our knowledge the test which achieved the largest concentration of self-driving vehicles collaboratively controlling traffic on a single stretch of freeway in the history of self-driving vehicles. The lecture will explain the objectives of CIRCLES, a consortium led by UC Berkeley, which conducted the MegaVanderTest. It will explain the algorithms and policies that ran in during the test. It will finally show some preliminary results, on the way to our quest: leveraging 1% to 2% of the total flow of vehicles to to improve the fuel economy of every car on that freeway on that day (not just ours), by up to 10%.

Torsten Hoefler (Professor , ETH Zurich)

Bio : Torsten Hoefler is a Professor of Computer Science at ETH Zurich, a member of Academia Europaea, and a Fellow of the ACM and IEEE. Following a “Performance as a Science” vision, he combines mathematical models of architectures and applications to design optimized computing systems. Before joining ETH Zurich, he led the performance modeling and simulation efforts for the first sustained Petascale supercomputer, Blue Waters, at the University of Illinois at Urbana-Champaign. He is also a key contributor to the Message Passing Interface (MPI) standard where he chaired the "Collective Operations and Topologies" working group. Torsten won best paper awards at ACM/IEEE Supercomputing in 2010, 2013, 2014, 2019, 2022, and at other international conferences. He has published numerous peer-reviewed scientific articles and authored chapters of the MPI-2.2 and MPI-3.0 standards. For his work, Torsten received the IEEE CS Sidney Fernbach Memorial Award in 2022, the ACM Gordon Bell Prize in 2019, the IEEE TCSC Award of Excellence (MCR), ETH Zurich's Latsis Prize, the SIAM SIAG/Supercomputing Junior Scientist Prize, the IEEE TCSC Young Achievers in Scalable Computing Award, and the BenchCouncil Rising Star Award. Following his Ph.D., he received the 2014 Young Alumni Award and the 2022 Distinguished Alumni Award of his alma mater, Indiana University. Torsten was elected to the first steering committee of ACM's SIGHPC in 2013 and he was re-elected for every term since then. He was the first European to receive many of those honors; he also received both an ERC Starting and Consolidator grant. His research interests revolve around the central topic of performance-centric system design and include scalable networks, parallel programming techniques, and performance modeling for large-scale simulations and artificial intelligence systems. Additional information about Torsten can be found on his homepage at htor.inf.ethz.ch.

Red Team Ethical Physical Penetration Testing Simulations using Open Source Intelligence

C. DeCusatis, C. Danyluk, D. MacCarthy, J. Shapiro, and N. Regan
Marist College
Poughkeepsie, NY USA
casimer.decusatis@marist.edu

Abstract—**Recent studies have shown the importance of ethical physical penetration testing as part of an overall cybersecurity defense. However, these techniques are often neglected in a traditional undergraduate curriculum. We have developed a physical pen testing training program using a combination of free, open source intelligence (OSINT) tools and low-cost hardware (such as the Arduino). We present a series of education modules covering tools and concepts such as covert entry (lock and key bypass, including elevators and wall safes), social engineering (pretexting), and cloning RFID credentials. The framework is developed and assessed using the proven Octalysis gamification framework. Before/after testing on a sample student population is conducted to demonstrate short-term learning.**

Keywords—Cybersecurity, physical, penetration, test, gamification, Octalysis

I. INTRODUCTION

Ethical physical penetration testing is an often-neglected aspect of cybersecurity, although it is an important part of red team performance (emulating the enemy). Red team physical pen tests offer several benefits, including risk enumeration and exposure of physical security vulnerabilities [1]. According to the National Center for Education Statistics [2], without strong physical security it's impossible to provide true information security or effective security controls. Physical pen testing includes features such as door bypass and lock picking, on-site reconnaissance, covert infiltration, social engineering, situational awareness, and credential cloning [3]. Training programs which teach covert entry and other aspects of this trade craft are available from several sources, including the SANS institute [4], the Core Group [5], and The Red Team Alliance [6]. These courses can cost thousands of dollars or more for about a week of intensive training. There is a need for low cost, easily accessible education resources in this area, which could integrate with a typical undergraduate 12 to 15-week cybersecurity course. Since it is very difficult and cost prohibitive to get permission for physical pen testing of an actual data center, we consider online virtual environments to simulate some aspects of this experience.

There are several free online instructional videos covering different aspects of physical pen testing and open source intelligence gathering (OSINT) for beginners [7-9]. Inspired by this prior work, in this paper we present a virtual red team education and training program using online resources, OSINT techniques, and low-cost hardware such as the Arduino development platform. The program is suitable for undergraduate and graduate students or beginning adult learners. This approach is suitable for individual students or small teams of 2-4 students. No prior experience with pen testing is required or assumed, although a basic understanding of cybersecurity principles may be helpful (such as defense in depth and least privileges).

This project has several goals. We plan to educate students on physical pen testing in the context of an undergraduate cybersecurity curriculum, without requiring specialized environments or equipment. We also intend to combine technical training with a firm grounding in professional ethics. We hope to make this material accessible to a wider body of students, in an effort to address the ongoing shortage of cybersecurity professionals (according to recent studies [10], there is a global shortage of 4 million cybersecurity professionals, which is expected to grow in the near future). By making this training more easily accessible and cost effective, we have a secondary goal of diversity and outreach to encourage traditionally under-represented groups in the cybersecurity field. As part of a balanced cybersecurity training program, this project encourages students to "think like a hacker" while exercising their ethical training. To accomplish these goals, we have designed a series of physical pen testing challenges which can be completed online using a web browser (we also reuse some contributions from online videos and blogs [7-9]). We create a scenario in which the student is contracted to perform an ethical pen test which includes 12 separate modules. To simulate the environment of a physical test, students are not allowed to progress to the next module until they satisfactorily complete the current module. We implement this scenario using the Octalysis gamification framework, which has been proven to provide an effective learning environment that improves information retention [11]. Students are evaluated before and after the training to assess short-term learning.

The remainder of this paper is organized as follows. After the introduction, we describe the structure of our physical pen testing modules, noting examples from previously published work which illustrates the learning objectives involved. Results of student assessments before and after training are

979-8-3503-3286-5/23/$31.00 ©2023 IEEE

then presented to assess the effectiveness of this approach. We then evaluate the program based on the eight Octalysis metrics, evaluate short-term learning on a sample student population, and suggest directions for future development.

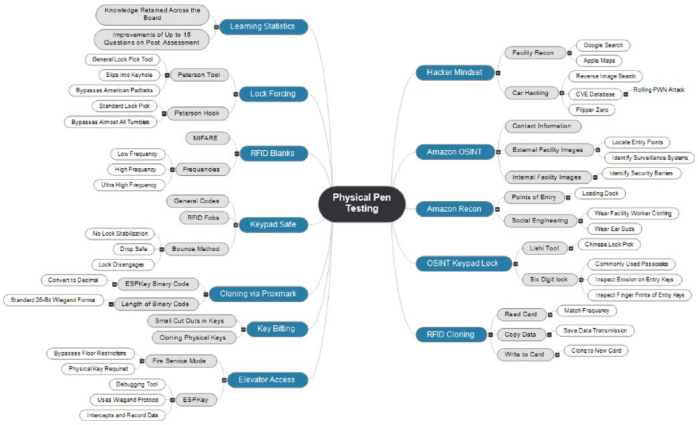
II. Framework and Experimental Results

The project is divided into 12 modules, each with a specific set of objectives as shown in Table 1, which cover a mind map [12] of related topics as shown in Table 2. Based on our experience, each module can take between several hours and several days to complete; a typical undergraduate cybersecurity curriculum could offer one module per week, allowing time for supplemental lectures and course evaluations during a 15-week semester.

Table 1: Module structure for ethical physical pen testing

	Student Assessment before training
1	Thinking like a hacker: ethical principles; OSINT reconnaissance on the supply chain and vehicle hacking
2	Detailed target reconnaissance and video surveillance
3	Access to the target facility via secondary entrance
4	OSINT bypassing keypad lock
5	Arduino RFID cloning and bypass
6	Elevator access: harvesting Bluetooth credentials; playback attack; MITM attack
7	Decoding key bitting, locksmith fundamentals
8	Cloning access cards, least privileges, defense in depth
9	Accessing keypad safe
10	RFID blanks, Weigand protocol,
11	Lock forcing and bypass techniques
12	After-action report and mind map
	Student Assessment after training

Table 2: Mind map of topics for physical pen testing training



The scenario for this project involves a team of students who have been hired to conduct an ethical pen test for a large organization, specifically to determine if they can gain physical access to the client's main server room using physical, social, and digital techniques. Students must document all their steps in sufficient detail for others to reproduce the test (another student team or the course instructor may be used to test this documentation). Students are provided with an introduction to ethics, including Kantian and Utilitarian principles, based on the ethical frameworks published by leading professional societies [13, 14]. We will discuss examples of the techniques used in this course, without giving away details that would reduce the replay value of the training modules. Similar test images, websites, and other data may be substituted to modify or customize the course as long as the basic training principles for each module are maintained.

To begin the course, students are provided with some limited background information on their target, including a list of companies who use their services or are part of their supply chain. While this information is incomplete, the files include a photo from Instagram of a company who is part of the client's supply chain. Students are asked to use OSINT techniques to identify the building and its location based on this image. Reverse image search is not permitted for this portion of the engagement, and all metadata has been removed from the image. This approach is based on previously published examples, such as the building shown in Figure 1 [8]. In this case, the street sign, city logo, and partial image of another business sign yield information which can be used in an online search to determine the name of the business using this building, its address, and website.

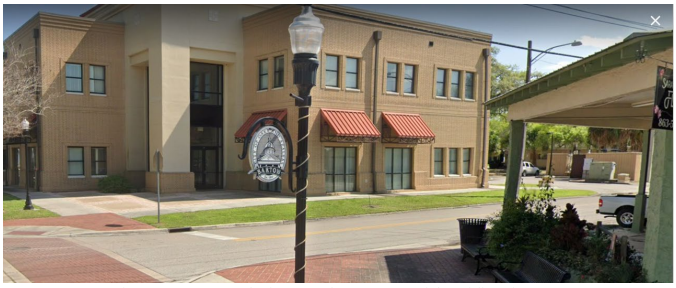


Figure 1 – sample image for OSINT identification [8]

Once the supply chain building is identified, students will note a publicly accessible parking lot without any obvious video surveillance, containing cars that bear the corporate logo. After verifying that the ethical pen test agreement includes authorization to pen test company-issued cars used for deliveries and other business purposes, students are asked to identify the make, model, and year of a car located in a reserved executive parking spot (Figure 2). Reverse image search is allowed for this exercise. Based on this information, students can determine that the vehicle in question is likely vulnerable to keyless entry attacks [15], such as the rolling PWN attack described in CVE-2021-46145 and CVE-2022-27254 [16]. Students must describe how to perform this attack using a Flipper Zero tool [17]; there are several videos illustrating this for different vehicles, some of which are accessible on reputable InfoSec twitter sites [18].

978-1-6654-8303-2/22/$31.00 ©2023 IEEE

Figure 2 – Sample image for vehicle identification

After accessing the vehicle, students find some business correspondence with the address of a data center facility which will be their next target. For example, this is similar to a previously published challenge [7] which gives the address of an Amazon distribution facility outside Virginia. Students are required to perform reconnaissance using Google Street View to determine entry points for this building (Figure 3).

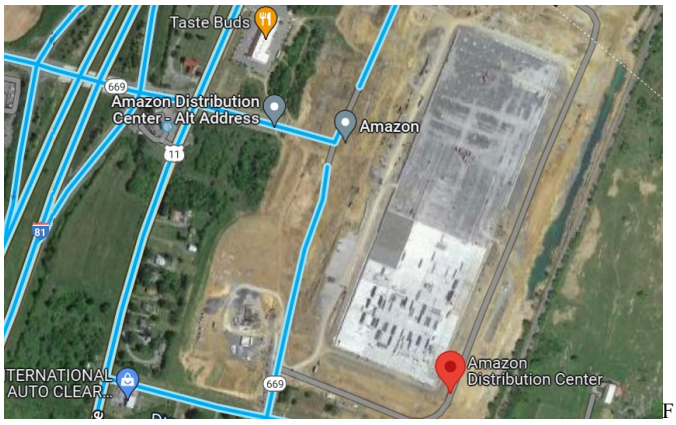


Figure 3 – Google Maps image of Amazon warehouse [7]

Due to information leakage, this reconnaissance can also yield images of the building interior, people who work there, and other potentially useful information. Students will note several security features protecting the main entrance, including turnstile access points and metal detectors/man traps with security attendants. Balustrades (large potted plants) are deployed strategically to block forced entry. Not only will this make tailgating or social engineering entry difficult, but the metal detector may stop visitors from bringing laptops or other pen testing tools into the facility. Video surveillance/recording is evident throughout the main lobby, and seems to cover all the approaches to the main entrance. Students observe cameras such as the example shown in Figure 4, and are asked to research this manufacturer and any known security vulnerabilities (the company is notable for being listed on the Specially Designated Nationals and Blocked Persons (SDN) list) [19]. Further research using Shodan [20] can determine how many cameras from this manufacturer are deployed worldwide, along with their approximate locations.

Figure 4 – Sample image, video surveillance camera

However, due to the high level of security at the main entrance, it's possible the target has developed a false sense of security and become overconfident. Other access routes may not be well protected, and anyone who's inside the building is assumed to have a right to be there. Students learn about pretexting, social engineering, and how to play into established narratives [21]. For example, additional Google reconnaissance reveals images of a loading dock and security office (Figure 5), including employees with yellow vests that may be used during pretexting incursions. Students take this opportunity to study pretexting and its relationship to Occam's Razor [22] (most people will assume the simplest explanation is the most likely, so a person inside the facility wearing a reasonable facsimile of a security vest is assumed to be part of the security team, rather than a potential threat actor impersonating security staff). This image also requires students to explain the function of security features such as the strike plate next to the door latch, location of the door hinges which affects which way the door opens, and other factors which may affect the approach to this building.

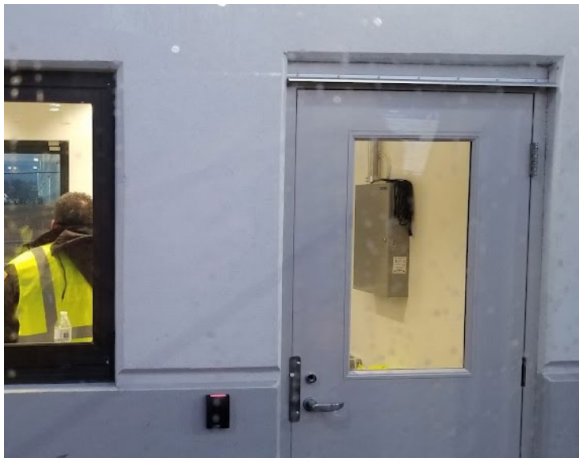


Figure 5 – Warehouse access door, Google Streetview [7]

Further reconnaissance reveals a postal access box, as shown in figure 6 [7]. Searching for the brand name and model of this box yields a user manual with the default factory access code (some users don't bother to change the default code). The manual also includes a description of the default access key required to open this box (A126 key, also known as a 222343 key), and instructions on executing a postal lock bypass by rewiring the interior circuits once the panel is open.

978-1-6654-8303-2/22/$31.00 ©2023 IEEE

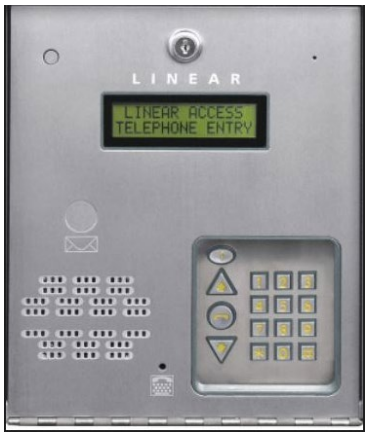


Figure 6 – Sample image, Linear postal lock box [7]

Students who successfully describe these techniques are allowed to proceed further into the virtual facility, where they encounter an electronic keypad dead bolt lock (such as Figure 7 [23]). Students must use OSINT techniques to identify the type of lock, whether it has anti-tampering features, and the manufacturer's default access code. Close examination of the image reveals that several buttons are shiny and free of dirt and corrosion; these are likely the commonly used access keys. Students also take this opportunity to review the mathematics of permutations and combinations to analyze the number of potential combinations and the feasibility of a brute force attack. If such an attack is not feasible, students describe how a Lishi tool [24] may be used to defeat the keyhole and gain access [25].

Figure 7 – Sample image, key pad lock [23]

The interior of the building is protected by badge readers using RFID and/or Bluetooth. Students must build, program, and test an RFID tag cloning system using an Arduino equipped with an RFID adapter card (similar approaches using a Raspberry Pi or other platforms may be substituted). There are several open source Arduino projects available which can clone RFID cards [26]. Students are given several RFID key fobs and cards to clone and rewrite, which are available at very low cost from several sources, including the popular MiFare cards [27]. Students take this opportunity to learn about other credential cloning equipment, which may not be available to them, such as the Proxmark [28]. There are many additional sources to learn about badge access systems, including the IBM Trusted Identity project [29]. Further inside the building, there are additional badge readers segmenting the building floor into different security zones. Students research the Weigand protocol [30] used by these devices, and work out the HIDProx ID values required to clone access cards, allowing pen testers to roam freely around the building. This demonstrates access control best practices.

After virtually bypassing these security features, students are able to gain further access to the building interior, including the main lobby. It is reasonable to assume that near the end of the scheduled business day or after business hours, students would be able to mingle with other people entering and exiting the facility using pretexting. Checking the posted corporate directory and visitor map, they determine the location of the data center. There's also a visitor center on the ground floor with open cubicles, which may come in handy later; such areas usually have open Wi-Fi, and visitors waiting in this area won't arouse as much suspicion. There is an elevator available to access the upper floors; the stairwell is locked with a mechanism that would be difficult and time consuming to defeat. Fortunately, the client didn't take the security precaution of not putting buttons inside the elevator. Students must research elevator hacking [31] including security features such as Independent Service Mode, Sabbath Mode, Security Mode, Riot Mode, Code Blue, and Fire Service. Students should be able to identify the access key required to operate an Otis elevator in fire service mode, and use of the infamous 2642 key in New York State to override elevators.

However, if you don't happen to have the correct fire service key, it may still be possible to defeat the RFID card reader connected to the elevator controls. While all the electronics that manage this lock are located in the secure area behind the door, communication between the card reader and its electronic back end are not always encrypted. Students learn how to install an ESPkey on the card reader using self-stripping installation displacement connectors (Figure 8 [7, 32]). This is an example of a classic man-in-the-middle attack.

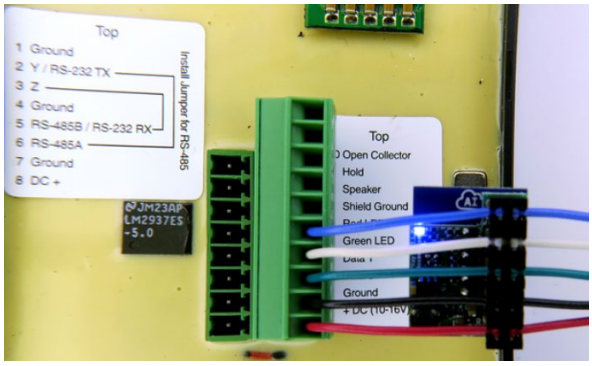


Figure 8 – ESPkey installation [7, 32]

After installing the ESPkey, students need to wait for someone to use the elevator so their credentials can be duplicated. The open visitor cubicles located earlier are ideal for this purpose. Awhile later, when most people have gone home, the cleaning

978-1-6654-8303-2/22/$31.00 ©2023 IEEE

staff shows up and starts work. Their keys are visible, and a quick photo (Figure 9 [33]) should allow students to identify the type of key and work out the biting code. The code can either be estimated manually or measured using free online tools [34]. Note the key brand name is not visible, but may be inferred from the key head shape using OSINT. With this information, a blank key and file can be used to make a copy sufficient to bypass most locks. This provides experience with lateral movement within a physical pen test site.

Figure 9 – Key image with bitting code template [33]

Returning to the elevator and connecting to the ESPkey local Wi-Fi using a smart phone reveals several sets of credentials have been captures (Figure 10 [7]). Students must convert the binary string ID which was captured to a decimal code, which can be used to electronically clone the credentials. A replay attack may then be used to access the elevator reader.

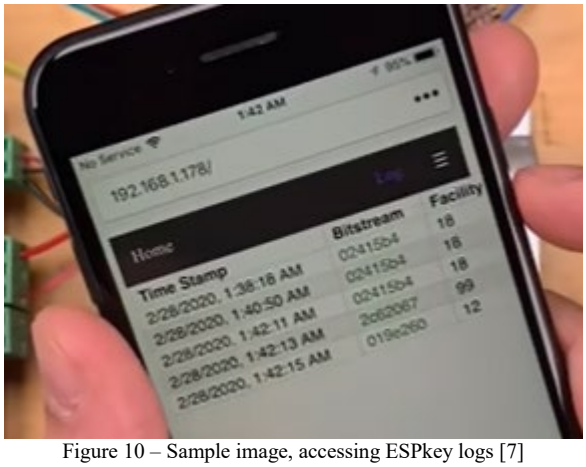


Figure 10 – Sample image, accessing ESPkey logs [7]

Taking the elevator to the appropriate floor yields an access door which seems to lead into the data center raised floor, but the card reader on the door doesn't work with the credentials cloned so far (apparently the person whose credentials were copied didn't have server room access privileges). This requires students to pivot their approach and use lateral thinking to reach their next objective. Backtracking to an administrative office nearby, and using the key copied from the janitor to go inside, yields access to an executive office. This person has good security hygiene; they didn't leave anything on top of the desk when they left for the day. However, there is a wall safe mounted nearby (Figure 11 [35]), and students can work out the default combinations and access bypass instructions for this particular model. Students also take this opportunity to learn about mechanical safe lock ratings, such as TL-15, TRTL, and TXTL.

Figure 11 – Sample image, wall safe [35]

Inside the safe is a pack of blank RFID cards, including one that has been separated from the pack. Students need to identify these from the code printed on the side of the box [27], including the compatible manufacturer, memory size, and operating frequency. Students take this opportunity to research the different types/frequency ranges for RFID cards (such as LF, HF, and UHF).

Further inside the virtual facility, students must describe the use of different types of under the door tools (UDTs) to slip the latch on a door leading to the server room. Peering through the glass server room cage reveals an older inner padlock, part of the American 1100 series. Students learn about bypassing this lock without a key using available bypass tools [37]. After successfully entering the server room, students take a photo, leave a small sticker behind to prove the room was breached, and exit before a guard can follow up on the proximity alarm (if this had been a real attack, there would have been plenty of time to slip a USB drive full of malware into a couple of servers, bypassing all the network defenses). Students complete an after-action report with prioritized recommendations for improving facility security, including a discussion of basic security hygiene. Students complete a 20-question evaluation before and after the pen testing project, which assesses their understanding of tools and concepts such as ProxMark, Flipper Zero, MiFare RFID cards, Weigand protocols, ESPkeys, Lishi keys, UDTs, key bitting, and pretexting. Results from a sample of four undergraduate students are shown in Figure 12.

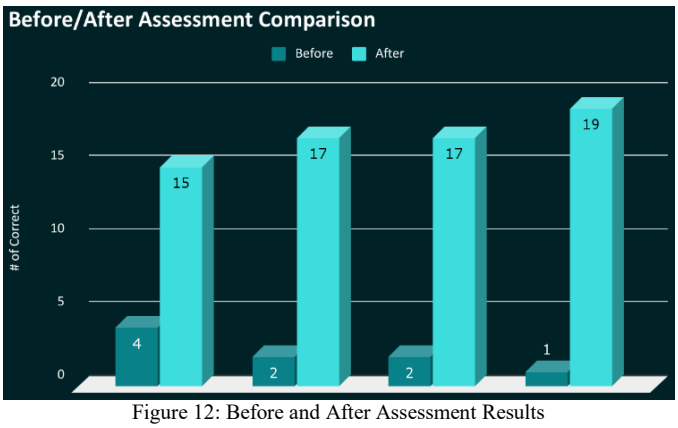


Figure 12: Before and After Assessment Results

978-1-6654-8303-2/22/$31.00 ©2023 IEEE

The students began with little to no understanding of physical pen testing fundamentals, and demonstrated a significant improvement (up to 94%) after completing the 15-week course. Additional studies are planned to further assess effectiveness of this training and to explore long-term information retention.

This approach was designed and further assessed using the Octalysis gamification framework. This approach to human-centric design and incorporation of gaming elements into non-gaming contexts was introduced in 2012, and its pedagogical benefits have been well documented [11]. For this paper, we provide only a brief overview of this framework. Octalysis organizes a series of eight gamification elements or cognitive drivers into a quantitative scale which can be used to measure an application's level of user engagement and motivation. Gamification elements are broadly organized into both positive motivators, such as providing the user with a sense of skill mastery, creativity, and higher purpose, and negative motivators, such as fear, uncertainty, greed, or punishment. Further, these elements are organized by extrinsic motivations (logic, calculations, and ownership) or intrinsic motivations (creativity, self-expression, and social context). A balanced game attempts to exploit as many of these motivators as possible, and strives to excel at several of them, in order to produce desired levels of engagement, motivation, and retention among users. We used the Octalysis metrics to analyze the ethical physical pen test project; results are shown in figure 13.

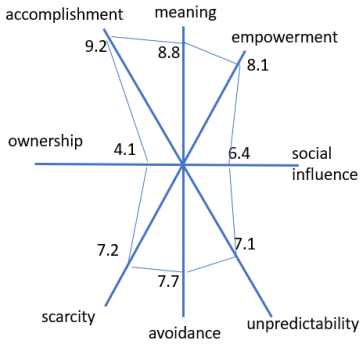


Figure 13: Octalysis analysis of physical pen testing

Each attribute is scored out of a possible 10 points. These results indicate our approach has particularly strong senses of accomplishment, empowerment, and meaning for the student. The areas with lower scores include unpredictability (7.1), which reflects that the program currently has limited replay value, since many challenges are re-used. To address this, we could introduce the challenges in a random order, and select from a pool of similar challenges with different details. The second area with a lower score was social influence (6.4), which reflects that students are currently allowed to compete against the challenges themselves, rather than against other students. A leaderboard scoring system with digital badges or connections to social media platforms would help improve this score. The third area with a lower score was ownership (4.1), which reflects the lack of a badge/achievement system as well as other factors such as limited customizability.

III. Summary and Conclusions

As evidenced by recent studies, there is a need for improved cybersecurity awareness training, including red team ethical physical penetration testing. We have developed and tested a virtual environment for physical pen testing, inspired by the free resources and OSINT tools currently available as well as low-cost Arduino hardware. To improve learning and retention, we employed the Octalysis gamification framework. The resulting 12 module education approach was tested on a group of undergraduate cybersecurity students. We found an increase in short-term learning of up to 94%, indicating this approach is successful in our goal of training students in both technical and ethical aspects of red team pen testing. Additional studies to assess long-term retention are planned. We quantified application effectiveness using the proven Octalysis framework with eight metrics. Results indicate the strengths of this approach are its sense of empowerment, accomplishment, and meaning; three areas (unpredictability, social influence, and ownership) were identified as focal points for future development. We plan to further enhance this approach and gather additional data on a larger, more diverse body of students in the future to assess the impact of the virtual physical pen testing approach.

Acknowledgments

We gratefully acknowledge Chris DeRobertis and Laurie Ward of IBM for their support of this project and contributions to our classroom environment. We also gratefully acknowledge the inspiration and contributions from references [7-9].

References

[1] RedTeam Security physical penetration testing services, https://www.redteamsecure.com/penetration-testing/physical-penetration-testing (last accessed October 29, 2022)

[2] National Center for Education Statistics report, "Safeguarding your technology", chapter 5, "Protecting your system: physical security", https://nces.ed.gov/pubs98/safetech/chapter5.asp (2022) (last accessed October 29, 2022)

[3] S. Oriyano, *Hacking Technques, Tools, and Incident Handling*, Jones and Bartlett, New York, NY (third edition, 2021)

[4] SANS Institute, course SEC487: Open Source Intelligence (OSINT) Gathering and Analysis, https://www.sans.org/cyber-security-courses/open-source-intelligence-gathering/ (last accessed October 29, 2022)

[5] The Core Group, Physical Penetration Testing Services, https://enterthecore.net/ (last accessed December 8, 2021)

[6] RedTeam Alliance course, Covert Methods of Entry, https://shop.redteamalliance.com/products/covert-methods-of-entry-lockpicking-red-team-training-for-pentest-penetration-testing-boot-camp (last accessed October 29, 2022)

[7] Virtual Physical Penetration Test (8 video series), TheNotSoCivilEngineer https://www.youtube.com/watch?v=KozaBTo-6To&list=PLwxkGxLTPJTnBbIYCTPNg6DBfZdXqf5Zs&index=1 (last accessed October 29, 2022)

978-1-6654-8303-2/22/$31.00 ©2023 IEEE

[8] Intro to OSINT (2 video series), TheNotSoCivilEngineer https://www.youtube.com/watch?v=Uud6xapckXk&t=17s (last accessed October 29, 2022)

[9] LockPickingLawyer video series, https://www.youtube.com/c/lockpickinglawyer/videos (last accessed October 29, 2022)

[10] HDI Worldwide Report, "The cybersecurity skills gap: 4 million professionals needed worldwide" (December 2020) https://www.hdi.global/infocenter/insights/2020/cyber-skills-gap/ (last accessed December 8, 2021)

[11] D. Economou, I. Doumanis, F. Pedersen, P. Kathrani, M. Mentzelopoulous, and V. Bouki, "Evaluation of a dynamic role playing platform for simulations based on Octalysis gamification framework", Proc. Workshop of the 11th International Conference on Intelligent Environments, D. Preuveneers, editor (2015); see also https://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/ (last accessed October 29, 2022)

[12] A.Kraus, "The CISO mind map: what is it and how can you use it to improve your imfosec posture":, November 13, 2019 https://zeguro.com/blog/the-ciso-mind-map-what-is-it-how-can-you-use-it-to-improve-your-infosec-posture (last accessed October 29, 2022)

[13] S. Vallor, "An introduction to cybersecurity ethics", February 2018 https://www.scu.edu/ethics/focus-areas/technology-ethics/resources/an-introduction-to-cybersecurity-ethics/ (last accessed October 29, 2022)

[14] IEEE Code of Ethics, https://www.ieee.org/about/corporate/governance/p7-8.html (last accessed December 8, 2021)

[15] A.Voronova, "Unlock any Honda car", July 8, 2022 https://hackaday.com/2022/07/08/turns-out-you-can-just-unlock-any-honda-car/ (last accessed October 29, 2022)

[16] A.Sharma, "Honda bug lets a hacker unlock and start your car via replay attack", March 25, 2022, https://www.bleepingcomputer.com/news/security/honda-bug-lets-a-hacker-unlock-and-start-your-car-via-replay-attack/ (last accessed October 29, 2022)

[17] Flipper Zero multi-tool, https://flipperzero.one/ (last accessed October 29, 2022)

[18] IstroSec video, "Honda civic using Flipper Zero", https://www.youtube.com/watch?v=2bb45r2Cbh4). (last accessed October 29, 2022)

[19] U.S. Department of the Treasury, "Specially designated nationals and blocked persons list (SDN list)", last update October 28, 2022 https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists (last accessed October 28, 2022)

[20] Shodan search engine, https://www.shodan.io/ (last accessed October 28, 2022)

[21] White Paper, "What is Pretexting?", https://www.malwarebytes.com/cybersecurity/business/what-is-pretexting (last accessed October 28, 2022)

[22] The power of pretexting, TheNotSoCivilEngineer, https://www.youtube.com/watch?v=ZcFy4_cxSU0&list=PLwxkGxLTPJTmmbd3Bv0-1VsbeCTWx_L1x&index=3) (last accessed October 28, 2022)

[23] Physical pen test challenge, TinkerSec, https://twitter.com/TinkerSec/status/1518583239090319363?t=RYraKg_H5nNZU8nFuibKXA&s=03 (last accessed October 28, 2022)

[24] Covert Instruments, Lishi Tools, https://covertinstruments.com/collections/lishi-tools (last accessed October 28, 2022)

[25] Using a Lishi with VFX x-ray vision, TheNotSoCivilEngineerr, https://www.youtube.com/watch?v=Xk4KvV60AwM (last accessed October 28, 2022)

[26] S. Sarraj, "RFID cards hacking and cloning using Arduino", Sept. 20, 2021 https://zsecurity.org/rfid-cards-hacking-cloning-using-arduino/ (last accessed October 28, 2022)

[27] MiFare classic 1K (MF1/CS50) white PVC card, https://www.usmartcards.com/mifarer-classic-1k-mf1ics50-white-pvc-card.html?___store=us (last accessed October 28, 2022)

[28] Proxmark RFID cloning, http://proxmark.org (last accessed October 28, 2022)

[29] C.Y. Byrnes and T. Rimaldi, "Implementing a mobile identity application in a ubiquitous computing environment", https://www.marist.edu/documents/20182/564159/Mobile_Identity_Final.pdf/c39c8762-da75-4782-9362-17ed1bb74009 (last accessed October 28, 2022)

[30] Weigand calculator, 26 bit format, http://ccdesignworks.com/wiegand_calc.htm (last accessed October 28, 2022)

[31] D. Ollum and H. Payne, "Elevator hacking from the pit to the penthouse", DefCon 2022, https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/DEF%20CON%2022%20-%20Deviant-Ollam-and-Howard-Payne-Elevator%20Hacking-From-the-Pit-to-the-Penthouse.pdf (last accessed October 28, 2022)

[32] Real World ESPkey attacks, TheNotSoCivilEngineer, https://www.youtube.com/watch?v=uSNLBh-4jRo (last accessed October 28, 2022)

[33] Decode keys with Microsoft Word, TheNotSoCivilEngineer, https://www.youtube.com/watch?v=vxJ3Kovz-bo&list=PLwxkGxLTPJTmWMI8EqsZ5V2WWbi4LQBoc&index=9 (last accessed October 28, 2022)

[34] D. Ollam, Key and Pin Decoding Template, https://github.com/deviantollam/Key-and-Pin-Decoding (last accessed October 28, 2022)

[35] Saflok hotel safe override, LockPickingLawyer, https://www.youtube.com/watch?v=De0D7otNxME (last accessed October 28, 2022)

[36] American Padlock Bypass Tool, https://lockpicktools.com/american-padlock-by-pass-tool/ (last accessed October 28, 2022)

978-1-6654-8303-2/22/$31.00 ©2023 IEEE