GUEST SPEAKER TITLES AND ABSTRACTS

Title: The Convergence of Cyber, Information Warfare, and AI

Presenter: Bryant Wysocki

Abstract: The convergence of cyber, information warfare, and artificial intelligence (AI), is reshaping global power competition by integrating AI-driven capabilities into cyber operations and information campaigns. This fusion enables activities like automated threat response, adaptive cyber maneuvers, and AI-powered misinformation, that significantly enhance the impact of hybrid warfare strategies.

As these technologies blur the lines between competition and conflict, they present societal challenges and raise critical ethical and legal questions. This talk will explore the implications of this convergence, highlighting the need for new defense approaches and international norms to address the evolving landscape of AI-enhanced activities.

Title: The Software Reverse Engineering Skillset

Presenter: Damon Smith

Abstract: Seasoned software reverse engineers at the National Security Agency draw from a wide and esoteric set of skills to support the NSA's cybersecurity and foreign intelligence missions. Bringing new reverse engineers up to speed can take months or years.

This talk considers the skills and competencies an aspiring reverse engineer might focus on to improve their readiness for a career in cybersecurity and the intelligence community.

Title: The Evolution of Social Engineering in Cybersecurity

Presenter: Jon Roumfort

Abstract: This presentation examines the dynamic evolution of social engineering. With traditional security vulnerabilities becoming more short-lived and less effective to exploit, attackers have found leveraging vulnerabilities in human behavior through social engineering to be an easier and more profitable alternative to more complicated and short-lived attacks on technology itself. Social engineering has become the most prevalent and damaging cyber attack today and it will only increase with the help of artificial intelligence.

This presentation will examine several types of past and current social engineering techniques, explore emerging trends, and go over ways to help prevent the attacks.

Title: Growing the Next Generation of Cyber Talent

Presenter: Matt Isnor

Abstract: The increasing prevalence of cyber threats highlights the critical need for the Department of Defense to have a capable and ready cyber workforce. Developing such a workforce involves a multi-disciplinary approach across policy, program development, strategy, data analytics, and data science that will drive innovation and development across the cyber workforce.

This presentation will provide information on the DoD CIO's by Cyber Workforce Strategy Implementation Plan, DoD Cyber Workforce Framework, DoD 8140 Cyberspace Workforce Management and Qualification Program, Academic Outreach, and Cyber Excepted Service.

Through targeted initiatives, investment in personnel, and a commitment to continuous development activities, we can build and sustain an agile, capable, and ready cyber workforce.

Title: Navy Cyber Science and Technology

Presenter: Joey Mathews

Abstract: In 1915, American inventor Thomas Edison opined, "The Government should maintain a great research laboratory to develop guns, new explosives, and all the technique of military and naval progression without any vast expense." This statement led to the creation of the Naval Research Laboratory in 1923. One hundred years later, NRL has changed the way the military fights and tilted the world's balance of power on at least three occasions with the first US radar, the world's first intelligence satellite, and the first operational satellite of the Global Positioning System.

NRL's Information Technology Division carries out research and development in the collection, transmission, assurance, and processing of information to provide Naval and joint warfighting forces with the means to achieve and maintain information dominance.

In this talk, I will discuss factors which motivate Naval science and technology investments, cybersecurity considerations for Navy platforms, and opportunities for students to engage with and contribute to the Navy's innovation ecosystem.

Title: From Campus to Career: Making Moves, Not Mistakes

Presenters: Jon David and Lohan Zellem

Abstract: Undergraduate students are generally motivated, self-educating, and technical, but may need assistance in securing and maintaining industry employment after graduation.

This presentation will provide students with résumé and interview tips, do's and don'ts for their first year of employment, and personal anecdotes on mistakes recent graduates tend to make. In addition, incident response stories will be shared for students to gain first-hand knowledge of real-world situations.

ABOUT CYBERSECURITY DAT AT IUP

Each year since 2008, the IUP Institute for Cybersecurity in conjunction with IT Support, has hosted Cybersecurity Day during the month of October to celebrate National Cybersecurity Awareness Month.

Nationally recognized security experts from government, academia, and industry are invited to present technical, or employment-focused topics to students, faculty, staff, and the community. Topics in previous years include incident response, cyber crime, cyber forensics, machine learning, privacy, current cybersecurity challenges, and many more.

Cybersecurity Day at IUP is always free and open to the public, and all are invited to attend.

For complete details on previous Cybersecurity Day activities, visit bit.ly/IUP-CSDAY

Please contact Dr. Waleed Farag, Director, Institute for Cybersecurity, at farag@iup.edu with questions.

PC4A PA Community College Consortium Cooperative Agreement

IUP

M MILLENNIAL SOFTWARE

THE 17TH ANNUAL

CYBERSECURITY DAY AT IUP

OCTOBER 29, 2024

OHIO HUB
IUP MAIN CAMPUS

CYBERSECURITY DAY AT IUP

TIME SLOT	SESSION TITLE AND PRESENTER
9:00 AM to 9:05 AM	***Introduction to the 17th Annual Cybersecurity Day at IUP*** Waleed Farag, Director, IUP Institute for Cybersecurity, Professor of Computer Science
9:05 AM to 9:10 AM	***Opening Remarks*** Lara Luetkehans, IUP Provost and VP for Academic Affairs
9:10 AM to 9:20 AM	***Event History, ICS Work, Recent Achievements, and Logistics*** Waleed Farag, Director, Institute for Cybersecurity, Professor of Computer Science
9:20 AM to 10:05 AM	***The Convergence of Cyber, Information Warfare, and AI*** Bryant Wysocki, Technical Advisor for C5ISRT, US Air Force and Space Force
10:15 AM to 11:00 AM	***The Software Reverse Engineering Skillset*** Damon Smith, Technical Director for Computer Network Operations, National Security Agency
11:10 AM to 11:55 AM	***The Evolution of Social Engineering in Cybersecurity*** Jon Roumfort, CISSP, IUP Senior Security Analyst
11:55 AM to 1:00 PM	**Lunch Break**
1:00 PM to 1:05 PM	***Welcome Back and Afternoon Logistics*** Waleed Farag, Director, IUP Institute for Cybersecurity, Professor of Computer Science
1:05 PM to 1:10 PM	***President's Remarks*** Michael Driscoll, President, Indiana University of PA
1:10 PM to 1:55 PM	***Growing the Next Generation of Cyber Talent*** Matt Isnor, Program Lead, DOD Cyber Workforce Development Branch, US Department of Defense
2:05 PM to 2:50 PM	***Navy Cyber Science & Technology*** Joey Mathews, Superintendent of the Information Technology Division, US Naval Research Laboratory
2:50 PM to 3:05 PM	**Afternoon Break**
3:05 PM to 3:50 PM	***From Campus to Career: Making Moves, Not Mistakes*** Jon David, Managing Director/Co-Founder, NR Labs, and Logan Zellem, Security Director, NR Labs
3:50 PM to 4:00 PM	***Event Conclusion*** Waleed Farag, Director, IUP Institute for Cybersecurity, Professor of Computer Science

BIOGRAPHICAL INFORMATION ON GUEST SPEAKERS

Bryant Wysocki, Technical Advisor for C5ISRT, US Air Force and Space Force

Bryant Wysocki, a senior-level executive, is the technical advisor for C5ISRT for the US Air Force and Space Force. Bryant provides technical oversight of these areas for the department and advises senior leadership. He holds a PhD in electrical engineering from Cornell University.

Damon Smith, Technical Director for Computer Network Operations, National Security Agency

Damon Smith has been programming and reverse engineering software for NSA since 2005. He has a master's in information security from Carnegie Mellon University and a bachelor's in computer science from Dartmouth College. Damon has worked for NSA in Maryland, overseas, and, since 2017, in Colorado.

Jon Roumfort, CISSP, IUP Senior Security Analyst

Jonathan Roumfort is a senior security analyst in IT Services at Indiana University of Pennsylvania and serves as a lead in the ITS Cybersecurity Leadership Team. Jonathan has been employed at IUP for over 25 years, where he has managed IT security, enterprise systems, and networking. He has served IUP as a senior security analyst for almost 22 years and is on IUP's Institute for Cyber Security steering committee. Jonathan is a member of various security groups and has been an ISC2 Certified Information Systems Security Professional since 2010.

Matt Isnor, Program Lead, DoD Cyber Workforce Development Branch, US Departnment of Defense

Matt Isnor an expert in the federal cyber workforce with DoD/CIO and is the former Cyber Mission Force program lead for training for US Cyber Command. He currently is the program lead for the development and refinement of standardizing the cyberspace workforce through work roles included in the DoD Cyberspace Workforce Framework. He is also responsible for leading the effort in DoD CIO to create the 8140 Policy Series, which sets the qualification program for all of DoD. Another area is that he is one of the cochairs with NSA and USCYBERCOM to lead the development of Cyber Institutes at each of the senior military colleges. Isnor holds a master of business administration with a concentration in information systems from Hawaii Pacific University and a master's of cybersecurity from Webster University.

Joey Mathew, Superintendent of the Information Technology Division, US Naval Research Laboratory

Joey Mathews is the superintendent of the Information Technology Division at the US Naval Research Laboratory. He leads a broad-based program of research and development spanning artificial intelligence and autonomy, networking and communications, information operations, high-assurance systems and cyber warfare, knowledge management and decision support, and computational science.

Jon David, Managing Director & Co-Founder, NR Labs

Jon David, a former director at Mandiant, boasts over 15 years of extensive experience in both private and DoD cybersecurity sectors. His expertise lies in enabling organizations to comprehend their threat landscape, strategically prioritize defenses, and effectively mitigate exposure to malicious threats. Throughout his career, David has played a pivotal role in aiding numerous enterprises across diverse industries in identifying and addressing vulnerabilities within complex environments. Drawing from this wealth of experience, he intimately understands the unique challenges each industry encounters when safeguarding its digital ecosystems.

Logan Zellem, Security Director, NR Labs

Logan Zellem is a security director with over eight years of experience. He has provided guidance and expertise to hundreds of federal clients, nonprofit organizations, and Fortune 500 companies. He specializes in privileged access management, designing and architecting secure systems that ensure compliance, streamline automation, and bolster overall security efficiency with a focus on mitigating risk.

2024 CYBERSECURITY DAY SPONSORS

The 17th Annual Cybersecurity Day is proudly sponsored by IUP, PC4A and Millennial Software.

PC4A
PA Community College
Consortium Cooperative Agreement

IUP

MILLENNIAL
SOFTWARE