NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER Virtual Seminar

VICEROY PIs
Bernard Van Wie (WSU)
Clement Izurieta (MSU)
James Alves-Foss (UI)
Matthew Boehnke (CBC)
LTC Andrew Van Den Hoek (CWU)
• Project Overview & Goals

• Reports from Each Institution:
  • Central Washington University
  • Columbia Basin College
  • Montana State University
  • University of Idaho
  • Washington State University

• Reports include:
  • Number of undergraduate and graduate students involved
  • Research activities
  • Internship activities
  • Coursework activities
  • Student clubs and cyber competitions
  • Seminars: WSU will list
CySER Website: cyser.wsu.edu
CySER Project Overview & Goals

CySER

Undergraduate Program (BS in CS)

Projects
- Senior Design
- Thesis
- Class

Internships
- Military Inst.
- National Labs
- Industry

Workshop
- Professional skills
- Real-world examples
- Best practices

Cyber-Physical Systems

Socio-Economic Networks

AI and Machine Learning

High School Outreach

Seminars
- Current topics
- Community outreach

ROTC CS & Non-CS Majors
CWU CySER Update

- Three students:
  - Jake Lebovich (AFROTC)
  - Noah Black (non-ROTC)
  - Edward Chavez (AROTC)

Army USAR and National Guard Cyber-Security Slots
- 5 X National Guard CyBER security slots
- May increase slots with density of Cyber professionals in Washington State

Recruitment
- Recruiting in Tri-Cities, Yakima, Vancouver
- Leveraging CySER as an ROTC recruitment tool

Research
- Working with Dr. David Douglas, ITAM Professor

Internships
- Meet to discuss application deadline and website
- DOE Omni Technology Alliance
Columbia Basin College CySER Update
2022-23
Oct 17, 2022

Matt Boehnke
Cyber Security
Assistant Professor, Cyber Security
Email: mboehnke@columbiabasin.edu
Office hours: Zoom online
CBC CySER - Agenda

- Number of undergraduate and graduate students involved
- Research activities
- *Coursework activities
- Internship activities
- Student clubs and cyber competitions
- Questions?
Cyber Security Program

• Started 2014

• Degree Pathways
  • Short Term or 1 year Certifications
  • 2 year AAS;
  • BAS in Cyber Security
  • *Added BAS in Information Technology (2020)
  • Working on: data analytics/ cloud services

• Graduates: 4 - 2015, 28 - 2017 (600% increase)
• Over 85% job placement; average salary: $65,000
Number of undergraduate and graduate students involved

- 4 Undergraduates
- Request: up to 10
- Outreach focus: doubling number of women and minority students
CBC CySER

Research activities

• Threat Modeling
<table>
<thead>
<tr>
<th>Research Activities (mappings + highlights)</th>
<th>security operations</th>
<th>security research</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CSIA 320: Ethical Hacking</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Asset Security</td>
<td>Certified Ethical Hacker (CEH)</td>
<td>Analyze ARP cache poisoning attack.</td>
</tr>
<tr>
<td>• Software Development Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CSIA 330: Wireless Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security and Risk Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security Operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CSIA 420: Cyber Crime and Terrorism</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security and Risk Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Security Operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CSIA 440: Cyber Testing and Penetration</strong></td>
<td>Complete full penetration test on physical production network.</td>
<td>Predict phishing email success based on keyword analysis.</td>
</tr>
<tr>
<td>• Security Assessment and Testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CSIA 450: Cyber Security Capstone</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Identity and Access Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Cyber Security Program

### planned CySER enhancements

<table>
<thead>
<tr>
<th>Course</th>
<th>Timeline</th>
<th>Theory</th>
<th>Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSIA 320: Ethical Hacking</td>
<td>Planned for Spring 2022.</td>
<td>Increase foundational content in cloud security, web application security, and application security.</td>
<td>• Develop projects for each of these three areas.</td>
</tr>
<tr>
<td>CSIA 440: Cyber Testing and Penetration</td>
<td>Planned for Fall 2023.</td>
<td>Increase foundational content in reverse engineering and malware pedigree.</td>
<td>• Enhance malware assessment to include pedigree.</td>
</tr>
<tr>
<td>CSIA 450: Cyber Security Capstone</td>
<td>Planned for Fall 2023.</td>
<td>Increase foundational content in data science and data science theory and ensure mathematical foundations of cryptography.</td>
<td>• Develop new assessment for reverse engineering.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Provide data science and data science theory topics for capstone projects.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Enhance cryptography assessment to include more rigorous mathematical foundations.</td>
</tr>
</tbody>
</table>
CBC Internship Activities

• Internships (PAID)
  • Pacific Northwest National Labs (PNNL)
  • Amazon

• Department of Energy/Ecology
  • Office of River Protection
  • Hanford Laboratory Management & Integration
  • Bechtel National, Inc (BNI)
  • Washington River Protection Solutions LLC (WRPS)
  • DOE Richland Operations Office
  • Hanford Mission Integration Solutions
  • HPM Corporation (HPMC)
  • CH2M Remediation Company
  • Mission Support Alliance (MSA)

• State Agencies
  • Department of Commerce/Port of Benton
  • WA ST Office of Chief Information Officer
  • Energy Northwest (Nuclear/Solar/Wind)

• Regional
  • City of Richland- Solar/ Battery Storage
  • Darklight
  • Marcraft
  • Port of Kennewick (Ransomware 2020)
  • Port of Pasco
  • Port of Benton
Student clubs and cyber competitions

• Questions?
CBC CySER

- Number of undergraduate and graduate students involved
- Research activities
- Internship activities
- Coursework activities
- Student clubs and cyber competitions
- Questions?
NCL - Background

• In 2011, a group of cybersecurity-focused academics from several public agencies

• Important to reduce barriers and excite young people to participate. Students would have easy access, no matter what their age, skill level or location.

• One of the earliest e-Sports

• Simulate real-life cyberthreats in a safe environment

• Growing population - more than 13,000 students of all ages, representing over 650 colleges and high schools across the U.S. - participates each year in the biannual competition.
National Youth Cyber Education Program created by the Air & Space Forces Association to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future.

At the core of the program is the National Youth Cyber Defense Competition, the nation's largest cyber defense competition that puts high school and middle school students in charge of securing virtual networks.

Other programs include AFA CyberCamps, an elementary school cyber education initiative, a children's literature series, CyberGenerations – a senior citizen cyber safety initiative, and a Tech Caregivers program designed to encourage cyber-savvy volunteers to give back to their communities.
In September 2014, the Air & Space Forces Association received a request from the Secretary of the US Air Force to develop a national space design competition, (something similar to CyberPatriot - AFA’s National Youth Cyber Defense Competition and flagship STEM program).

Bill Yucuis, an aerospace engineer with years of experience coordinating an Aerospace Magnet Program, was tasked as the chair of the committee that would go on to build the program from the ground up.

Air Force retired space experts, Tim Brock and Stephen Gourley, along with AFA figurehead David "Buck" Buckwalter, came together to create StellarXplorers

The StellarXplorers Space STEM Program, created by the Air & Space Forces Association (AFA), inspires 6-12 grade students toward careers in aerospace, aviation, and other science, technology, engineering, and mathematics disciplines critical to our nation’s future.
• November 4, 2022 and Saturday, November 5, 2022.

• Hybrid format: both virtual and in-person options.

• Unfilled cybersecurity careers will reach over 1.8 million by 2022. With the ever-increasing amount of technology placed on the internet, security becomes a high priority.

• Department of Energy (DOE), capitalizing on the expertise of current national laboratory staff that previously hosted four successful cyber defense competitions to exercise interactive, scenario-based events, where participants engage in cybersecurity activities includes methods, practices, strategy, policy, and ethics.

• DOE has worked to increase 1) hands-on cyber education to college students and professionals, 2) awareness into the critical infrastructure and cyber security nexus, and 3) basic understanding of cyber security within a real world scenario.
Thank you
CySER Cybersecurity Efforts at Montana State University

October 17, 2022
Dr. Clemente Izurieta
Professor of Computer Science
Software Engineering Laboratory (SEL)
Montana State University
Participants:

Institutional PI: Dr. Clemente Izurieta
ROTC Air Force: Lieutenant Colonel Lance J. Ratterman
ROTC Army: Lieutenant Colonel Christopher L’Heureux
Graduate Research Assistant: Andrew Fallin

2021-2022 Academic year: 4 Air Force cadets
2022-2023 Academic year: 2 Air Force and 2 Army cadets
Hierarchical Software QA Modeling

Theoretical

Characteristics
- Characteristic 1
  - Subcharacteristic 1
    - Quality property 1
- Characteristic 2
- Characteristic 3
- Characteristic n

Operational

Factors
- Portability
- Maintainability
- Security
- Modularity
- Redundancy
- Documentation
- Encryption
- Documentation Smells
- Encryption Smells

Utility Functions
- $f_1(x) = 0.67$ for Coupling
- $f_2(x) = 0.11$ for Duplication
- $f_3(x) = 0.03$ for Documentation Smells
- $f_4(x) = 0.04$ for Encryption Smells

Standards
- ISO/IEC 9126:2001
- ISO/IEC 25010:2011
- NIST 800-53R8
- RMF (Risk Management Framework)
- Quamoco (2012 Wagner et al.)
- Qatch (2017 Miltiades et al.)
- PIQUE (2020 SEL MSU)
CWE-699 View Structure
PIQUE Models

- Pique-Bin (INL, DHS)
- Pique-C# (CERL Army, Air Force)
- Pique-C#-Sec (CERL Army, Air Force, DHS)
- Pique-Azure (DHS)
- Pique-C++ (DHS)
- **Pique-Cloud (DHS)**
- **Pique-ICS (DHS)**
Classification, clustering, and anomaly detection using graph representations of code

Graph data: graph representations (e.g., control flow graphs) of benign and possibly malicious binaries

Extract graph representation using disassembler such as angr

Extract vector representation using graph embedding method such as Graph2Vec

t-SNE visualization of the DBSCAN clustering of the Graph2Vec embedding of the DBC dataset (64 embedding dimensions)
Decomposition of CWE-200

Identify security zones and sensitive sections of source code
Assess the composition, stylometry and origination of software to verify that they are truthful, complete and accurate.
Improving the confidence of machine learning models through improved software testing approaches

Intrusion Detection Systems
Conceptual Frameworks and Theory of Bug Bounty Platforms
Malware detection using obfuscation of Opcodes in FPGAs
• Book Club
• Introductory course in cybersecurity (University of Idaho)
• Independent study credit
• HackerCats club
Research Collaborations

Hoplite is a leading-edge cybersecurity company specializing in the mitigation of cyber risks. Founded in 2013, Hoplite Industries has developed a set of automated cyber defense capabilities and specialized AI solutions driven by cyber research at a global scale.

Cybercore brings together experts in critical infrastructure security assessments, cyber forensic analysis, threat detection and consequence-based targeting to provide real-world technical solutions and innovations that protect operational environments from an ever-evolving threat landscape.
Education

• Associates degree in Cybersecurity (Gallatin College)
• MS in Cybersecurity
  • Board of Regents approved
  • Seeking CAE certification
• NSF REU program – Cybersecurity algorithms
• Griffiss/DoD program to train 4 ROTC cadets on a yearly basis before commissioning
## Software Engineering Laboratory Current Funding

Students: 8 Ph.D., 4 MS, 4 Undergraduates, 1 Postdoc

<table>
<thead>
<tr>
<th>Organization</th>
<th>Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Science Foundation</td>
<td>$400K</td>
</tr>
<tr>
<td>Washington State University/Griﬃss Institute</td>
<td>$162K</td>
</tr>
<tr>
<td>Air Force, Army, CERL</td>
<td>$1.2M</td>
</tr>
<tr>
<td>Raytheon Technologies</td>
<td>$330K</td>
</tr>
<tr>
<td>Idaho National Laboratory and Department of Homeland Security</td>
<td>$3.1M</td>
</tr>
<tr>
<td>Department of Homeland Security</td>
<td>$4.47M</td>
</tr>
<tr>
<td>Resilient Computing</td>
<td>$150K</td>
</tr>
</tbody>
</table>
Washington State University Update

Heading a Five-institution Virtual Institute Consortium

Building an Enhanced Center for Academic Excellence in Cybersecurity Knowledge, Skills & Abilities for a Military & Defense-aligned Civilian Workforce

Washington State University PI: Prof. Bernie Van Wie
bvanwie@wsu.edu; 509-335-4103

WSU Co-PIs: Assefaw Gebremedhin, Noel Schulz

External Evaluator: Olusola Adesope
**Student Status**

- Recruitment - Poster

---

**NORTHWEST VIRTUAL INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH**
cyser.wsu.edu

---

**WHY JOIN CySER?**

- $1000 stipend per semester
- $2000 stipend for attending a 2-week summer workshop in May, here on the WSU campus
- Help finding cybersecurity-related summer internships
- Summer workshop involves presentations and discussions with cybersecurity professors and industry professionals, hands-on activities where participants learn how to use cybersecurity tools and techniques, and field trips to tech and defense sites (the complete agenda from this past summer workshop can be found on the website)
- Bi-weekly seminars from cybersecurity professors and professionals
- Book club with assigned cybersecurity non-fiction reading and bi-weekly discussions
- Participation in mentorship program with graduate student mentors working on cybersecurity-related research, including presentation of that research in a poster session at the summer workshop

---

**INTERESTED IN CYBERSECURITY?**

- Put your computer science skills to the test.
- Develop a deeper understanding of the tech world and how modern infrastructure and data is protected.
- Cybersecurity professionals are in high demand, and have average starting salaries above those in many other fields
- WSU offers two certificates that can be earned alongside your Bachelor's Degree: CySER CAE-CC Fundamentals, and CySER Basics.

---

**ABOUT CySER**

- Funded by DoD through the Griffith Institute
- Member of the VICEROY program
- For more info, visit cyser.wsu.edu

---

**WHO CAN APPLY?**

- Undergraduates in any year (freshman through senior)
- Citizenship or green card required by DoD
- Must be able to participate Fall 2022 and Spring 2023 (one academic year)
- Attendance required for seminars, and participation in mentorship program

---

**APPLY AT cyser.wsu.edu/apply/**
WSU Numbers of Undergraduates & Graduate Students Involved

- 14 New Students for Fall 2022/Spring 2023
  - Majors: CS & CS/Finance, EE, ChE
  - 2-3 Pending
  - 1 ROTC; 1 Pending
- 13 Continuing Students:
  - Majors: CS, CE, SE, MIS/Acctg
  - 1 ROTC
- Stipends: $1K Fall 22; $1K Spring 2023; $2K Summer Workshop
<table>
<thead>
<tr>
<th>NAMES</th>
<th>FACULTY MENTORS</th>
<th>PROJECTS</th>
<th>INTERNSHIPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arjun Anand (WSU)</td>
<td>Prof. Jana Doppa</td>
<td>Finding Cyber Attacks on Networks</td>
<td>None</td>
</tr>
<tr>
<td>Cai Haught (WSU)</td>
<td>Prof. Venera Arnaoudova</td>
<td>Human Factors on software vulnerabilities</td>
<td>GI</td>
</tr>
<tr>
<td>Griffin Gerry (WSU)</td>
<td>Prof. Rob Crossler</td>
<td>Powerless to change - Cyberwarfare</td>
<td>None</td>
</tr>
<tr>
<td>Hillary Zhang (WSU)</td>
<td>Prof. Assefaw Gebremedhin</td>
<td>Microsoft security</td>
<td>None</td>
</tr>
<tr>
<td>James Minteer (WSU)</td>
<td>Prof. Partha Pande</td>
<td>Planned Obsolescence by Aging Manycore Chips</td>
<td>ACE</td>
</tr>
<tr>
<td>Kaitlin White (WSU)</td>
<td>Prof. Assefaw Gebremedhin</td>
<td>Graph neural networks - polymorphic virus detection - reverse engineering</td>
<td>None</td>
</tr>
<tr>
<td>Matthew Kusman (WSU)</td>
<td>Prof. Chris Hundhausen</td>
<td>Tools for cybersecurity education and assessment/ identify vulnerabilities</td>
<td>Radixiot</td>
</tr>
<tr>
<td>Moises Carranza (WSU)</td>
<td>Prof. Chris Hundhausen</td>
<td>Tools for cybersecurity education and assessment/ identify vulnerabilities</td>
<td>None</td>
</tr>
<tr>
<td>Nathan Waltz (WSU)</td>
<td>Prof. Assefaw Gebremedhin</td>
<td>Graph neural networks - polymorphic virus detection - reverse engineering</td>
<td>SEL</td>
</tr>
<tr>
<td>Noah Black (CWU)</td>
<td>Deborah Wells</td>
<td>USB hot-plug attack counter forensics</td>
<td>GI</td>
</tr>
<tr>
<td>Paul Wilmoth (WSU)</td>
<td>Prof. Rob Crossler</td>
<td>Powerless to change – Cyberwarfare</td>
<td>None</td>
</tr>
<tr>
<td>Timothy Cain (WSU)</td>
<td>Prof. John Miller</td>
<td>Clustering software vulnerabilities using self-organizing maps</td>
<td>None</td>
</tr>
<tr>
<td>Timothy Reidy (WSU)</td>
<td>Prof. Larry Holder</td>
<td>CMU ghosts to simulate a user environment and detect novelty</td>
<td>GI</td>
</tr>
<tr>
<td>William Heinecke (WSU)</td>
<td>Prof. Assefaw Gebremedhin</td>
<td>Observability of network security monitoring strategies with TOMATO</td>
<td>None</td>
</tr>
<tr>
<td>Zachary Werle (WSU)</td>
<td>Prof. Assefaw Gebremedhin</td>
<td>Observability of network security monitoring strategies with TOMATO</td>
<td>GI</td>
</tr>
<tr>
<td>INSTITUTIONS</td>
<td>NAMES</td>
<td>STATUS</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>GRADUATE RESEARCH MENTORS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Washington State University</td>
<td>James Halverson (PhD, CS)</td>
<td>Civilian</td>
<td></td>
</tr>
<tr>
<td>Washington State University</td>
<td>Aryan Deshwal (PhD, CS)</td>
<td>Civilian</td>
<td></td>
</tr>
<tr>
<td>Washington State University</td>
<td>Justin Stachofsky (PhD, MIS)</td>
<td>Civilian</td>
<td></td>
</tr>
<tr>
<td>Washington State University</td>
<td>James Crabb (MS, CS)</td>
<td>Civilian</td>
<td></td>
</tr>
<tr>
<td>Washington State University</td>
<td>Brenden Fraser-Hevlin (PhD, ChE)</td>
<td>Civilian</td>
<td></td>
</tr>
<tr>
<td>Washington State University</td>
<td>Vincent Lombardi (MS, CS)</td>
<td>Civilian</td>
<td></td>
</tr>
<tr>
<td>Washington State University</td>
<td>Blessing Adaramola (Ed/Psych)</td>
<td>Civilian</td>
<td></td>
</tr>
</tbody>
</table>
WSU Courses

- Course content and syllabi for 3 new courses developed

<table>
<thead>
<tr>
<th>Course</th>
<th>Offered Fall 2022 &amp; Spring 2022/2023</th>
<th>Offered Spring 2023</th>
<th>Offered Fall 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>KUs: M7, M8, M9, O4, O13, C4</td>
<td></td>
<td></td>
<td>KUs: M4, M9, O2, O3, O4, O13, C4</td>
</tr>
<tr>
<td>KUs: M2, O8, C1, C2, C5, S1, S2, S7</td>
<td></td>
<td></td>
<td>KUs: M2, O8, C1, C2, C5, S1, S2, S7</td>
</tr>
</tbody>
</table>

- CIA & security principles (Saltzer & Schroeder principles)
- Common threat & vulnerability models
- Crypto basics & primitives (randomization)
- Security of authorization mechanisms / frameworks
- Access control mechanisms
- Cloud Infrastr. comp. & interfaces, common service/deployment models
- Network security architectures & protocols
- Web security principles & tools
- Privacy and anonymity principles & tools
- Vulnerability: CVE, CWE, over/underflow, OSVDB, CAPEC, space-based, privilege
- Crypto adv.: symmetric & asymmetric, hashes, key-based, and digital signs
- Wireless security: ciphers, DoS, CIA enforcement, G/WIFI/Bluetooth/RFID
- Application of cryptography to internet, 7 communications security
- Advanced network security: discovery, incident response, resiliency, protocol analysis
- Virtualization: architecture, principles, states, storage, & failover technology
- Cloud Infrastructure: secure deploying/scaling (Pupper/Chef)
- Machine learning
- Operating systems security (architectures, mechanisms, hardening)
- Code analysis (source, static, dynamic, testing, malware, exploits)
- Binary analysis (kernel, firmware, polymorphism, symbolic diff.)
- Vulnerability discovery, fuzzing, crash dumps, side channel, equities, mitig n
- Reverse engineering (embedded systems, SCADA/ICS, malware analysis)
- Distributed fault tolerant systems security: transactions, communication, scalability
- Forensics/anti-forensics (OS, Wireless, Memory, Network, IoT, & Cloud)
WSU Certificate Programs Approved by Faculty Senate

- **CySER CAE-CO Fundamentals Certificate approved** – BS in Computer Science, Computer Engineering, or Software Engineering students interested in specializing in cybersecurity – led by EECS

- Integrates cybersecurity research & education with professional skills in teamwork, communication, leadership, and lifelong learning; Merges theoretical knowledge & experiential learning in cyber operations and defense

- Taking 3 mandatory cybersecurity courses (9 credits)
  - CptS 327 Introduction to Cybersecurity
  - CptS 427 Applied Cybersecurity and
  - CptS 428 Advanced Cybersecurity

- Taking at least 4 elective courses out of the following courses
  - CptS 455 Introduction to Computer Architecture
  - CptS 460 Operating Systems and Computer Architecture
  - CptS 475 Data Science
  - CptS 415 Big Data
  - CptS 443 Human-Computer Interaction
  - CptS 466 Embedded Systems
  - CptS 464 Distributed Systems Concepts and Programming
  - CptS 489 Web Development
  - Univ. of Idaho CYB 447 Computer and Network Forensics
  - CptS 478 Software Process and Management
  - EE 334 Computer Architecture
  - EE 434 ASIC & Digital Systems Design
  - EE 489 Introduction to Control Systems
  - MIS 374 IT Infrastructure & Security

- Taking 1-2 semesters or equivalent of foreign language coursework (Russian, Chinese, Korean, Arabic, or Persian)

- Taking the CptS 421 and 423 Senior Design course sequence with a project focused on cybersecurity

- Engaging in a cybersecurity-related internship experience

- Involvement in CySER research – realized via, e.g., class projects, senior design projects, independent study projects

- Attending the CySER summer workshop

- Attending CySER seminars (at least 60% of the bi-weekly seminars in a semester)
CySER Basic Certificate – Non-computer science majors & ROTC cadets interested in cybersecurity and led by MISE

- Integrates cybersecurity research & education with professional skills in teamwork, communication, leadership, and lifelong learning; Merges theoretical knowledge & experiential learning in cyber operations and defense

The certificate requires taking:
- CPTS 111 Intro to Computer Programming (Python) or CPTS 121 Intro to Programming (C/C+).
- MIS 372 Data Management or CYB 110 Cybersecurity & privacy (a cooperative course offered at the University of Idaho).
- MIS 374 IT Infrastructure and Society or CYB 310 (a collaborative course offered at the University of Idaho)
- CPT S 499 (with a cybersecurity project) or CPT S 421 and CPT S 423 computer science sequence of senior design courses

Additionally, students will:
- Participate in three internship credits (MIS 498; or CPT S 488 and ENGR 489) with a cybersecurity-related experience; or complete at least four foreign language credits or demonstrate equivalent proficiency in Russian, Chinese, Korean, Arabic, or Persian.
- Demonstrate involvement in CySER research (realized via class projects, senior design projects, and independent study).
- Attend the CySER summer workshop.
- Attend CySER seminars (at least 40% of the bi-weekly seminars in a semester).
WSU Cyber Club & Competition Opportunities

• WSU Cyber Security Group
  https://wsu.presence.io/organization/cyber-security-group

• Competition Teams
  
  Cyber Force
  - Competition dates: Nov 4-5, 2022
  - Two teams competing from WSU (Crimson Cougs and Grey Cougs)
  - Most are CySER students, some are outside CySER, all are members of the CSG student club

  NICCD
  - Competition dates: Nov 10-11, 2022
  - One WSU team registered to participate (only one team per institution can participate)
Schedule

• Bi-weekly virtual seminar series
# FALL 2022 SEMINAR SERIES

<table>
<thead>
<tr>
<th>Date</th>
<th>Speaker</th>
<th>Title/Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct. 17</td>
<td>CySER PIs at partner institutions</td>
<td>Fall Seminar Series Kick-off: updates from partner institutions</td>
</tr>
<tr>
<td>Oct. 31</td>
<td>Robert Crossler</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>Dept of Management, Information Systems and Entrepreneurship</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WSU</td>
<td></td>
</tr>
<tr>
<td>Nov. 14</td>
<td>Slater Weinstock</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>Casaba Security</td>
<td></td>
</tr>
<tr>
<td>Nov. 28</td>
<td>James Halvorsen</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>School of EECS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WSU</td>
<td></td>
</tr>
<tr>
<td>Dec. 12</td>
<td>Haipeng Cai</td>
<td>TBD</td>
</tr>
<tr>
<td></td>
<td>School of EECS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WSU</td>
<td></td>
</tr>
</tbody>
</table>
## CySER Seminars Schedule

### FALL 2021 SEMINAR SERIES

<table>
<thead>
<tr>
<th>Date</th>
<th>Speaker</th>
<th>Title/Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov. 29</td>
<td>Dr. Clemente Izurieta</td>
<td>Hierarchical Software Quality Assurance Approach to Leveraging Existing Technologies and Building Quality Gates</td>
</tr>
<tr>
<td></td>
<td>Glanforte School of Computing</td>
<td>Recording</td>
</tr>
<tr>
<td></td>
<td>Montana State University</td>
<td>Slides</td>
</tr>
<tr>
<td>Nov. 8</td>
<td>Matthew Boehnke</td>
<td>Cyberhawks and Beyond</td>
</tr>
<tr>
<td></td>
<td>Department of Computer Science</td>
<td>Recording</td>
</tr>
<tr>
<td></td>
<td>Columbia Basin College</td>
<td>Slides</td>
</tr>
<tr>
<td>Oct. 25</td>
<td>Dr. Jim Alves-Foss</td>
<td>Probabilities, Percentages, and Professions of Performance</td>
</tr>
<tr>
<td></td>
<td>Department of Computer Science</td>
<td>Recording</td>
</tr>
<tr>
<td></td>
<td>University of Idaho</td>
<td>Slides</td>
</tr>
<tr>
<td>Oct. 11</td>
<td>Dr. Assefaw H. Gebremedhin</td>
<td>CySER Overview and Machine Learning</td>
</tr>
<tr>
<td></td>
<td>School of EECS</td>
<td>Recording</td>
</tr>
<tr>
<td></td>
<td>Washington State University</td>
<td>Slides</td>
</tr>
<tr>
<td>Date</td>
<td>Speaker</td>
<td>Title/Media</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| May 2 | Cory Baker  
Cybercore Integration Center  
Idaho National Laboratory | Cybersecurity for the Operational Technology Environment |
| Apr. 18 | Kevin Brennan  
FBI – Special Agent | The Cyber Threat Landscape – The FBI’s Perspective |
| Apr. 4 | Karl Scheuerman  
Crowdstrike – Falcon Complete | Cyber Security Operations on the Front Line  
Recording  
Slides |
| Mar. 21 | Elena Peterson  
Pacific Northwest National Laboratory | Flexible and Adaptive Malware Identification Using Techniques from Biology  
Recording  
Slides |
| Mar. 7 | Charles Carroll  
Schweitzer Engineering Laboratories | Purposeful Design – Defending Critical Infrastructure  
Recording |
| Feb. 7 | Bryson Bort  
Scythe and ICS Village | Can you hack it? Starting your own company  
Recording  
Slides |
| Jan. 10 | Deborah Wells  
Information Technology and Administration  
Central Washington University | Deepfakes and Cybersecurity Concerns  
Recording  
Slides |
Schedule

- Summer workshop: [https://cyser.wsu.edu/summer-workshop/](https://cyser.wsu.edu/summer-workshop/)
- May 23 to June 3, 2022, at WSU in Pullman, WA: presentations, tutorials, and hands-on experiential learning activities
- Field trips: a half-day trip to Schweitzer Engineering Laboratories (SEL, Pullman), full-day Fairchild Air Force Base, 2-day to Keyport Naval Undersea Warfare Center.
- In person, virtual option
- Slides, related material, and recordings of all sessions (excluding the field trips) posted on CySER website
- Topics:
  - Cybersecurity in industrial control systems
  - Digital forensics
  - Cybersecurity and behavioral threats
  - Cyber education
  - Team building and leadership
  - Virtualization
  - Software assurance and trusted software bills
  - Cybersecurity competitions and the National Cyber League
  - Cybersecurity in power systems
  - Adversary emulation, purple teaming, and ICS
  - Applications of machine learning in cybersecurity
  - Human in-the-loop learning for anomaly detection
  - Clustering software vulnerabilities using self-organizing maps
  - On-chip communication in the age of heterogeneity
  - Cybersecurity in biomanufacturing
  - Smartphone technology security
  - Binary analysis
  - US Army Cyber Command
  - Being a Lifelong Learner
- Daily summary emails were sent to workshop participants
CySER Activities

• **Experiential Learning**
  - Mentored cybersecurity research
  - Summer workshop: extensive hands-on components
    - Poster session
  - Leadership – Team Building
    - Major Paul Hyde (WSU)
    - Retired Captain Andrew Van Den Hoek (CWU)
    - LTC Lance Ratterman (MSU)
  - Internships
  - Mentored senior design projects
  - Cybersecurity seminars
  - 3 field trips:
    - Schweitzer Engineering Lab (Pullman, WA)
    - Fairchild Air Force Base (Airway Heights, WA, near Spokane)
    - Keyport Undersea Warfare Center (Keyport, WA)
  - participation on a competitive cybersecurity team (CBC)
**Summary**

**EXTERNAL EVALUATOR SUMMARY – by Dr. Olusola Adesope** (attended biweekly PI meetings to assess goals, infrastructure, examine what was going well / improvements needed). Data from meetings, reports, Qualtrics surveys for faculty, RA faculty, undergraduates.

Significant achievements - year 1:

- Project website developed and launched
- 3 new courses on cybersecurity developed, syllabi passed through university; courses now listed in university catalog.
- 2 CySER certificate programs: CySER CAE-CO Fundamentals & CySER Basic Certificates; approved by the university senate, listed in catalog
- Current CySER students are currently completing program requirements to obtain certificates.
- Biweekly Seminar series in Fall 2021 (5 seminars) and Spring 2022 (7 seminars); Broadly advertised, well-attended (~25 / seminar)
  - Robust intellectual and practical discussions
- 2-week Summer workshop: well-attended, included field trips
- 13 undergraduate students placed in cybersecurity internships
- 32 students are involved in cybersecurity projects at varying levels
- Successful recruitment of ROTC members
- Conducted outreach activities for high school students
- Many graduate student faculty research assistants serve as mentors to undergraduates
- Strong underrepresented minority participation in the project, with Hispanics, African Americans, and females well represented

**Overall, Year 1 achievements of project objectives and outcomes were successful, and plans for year 2 are realistic, aligned with project goals, and well-crafted to reach indicated milestones.**
EXTERNAL EVALUATOR SUMMARY

• PI/Admin team went above and beyond with limited salaries
• Workshop:
  • 90% of student participants indicated they gained a lot from attending the summer workshop
  • 7% gained moderate knowledge
  • 2% gained little experience
• CySER program influenced the students’ learning experience about Cybersecurity
Attendance