VICEROY™

NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER

CySER Virtual Seminar

GRIFFISS INSTITUTE

VICEROY PIs

Bernard Van Wie (WSU)

Clement Izurieta (MSU)

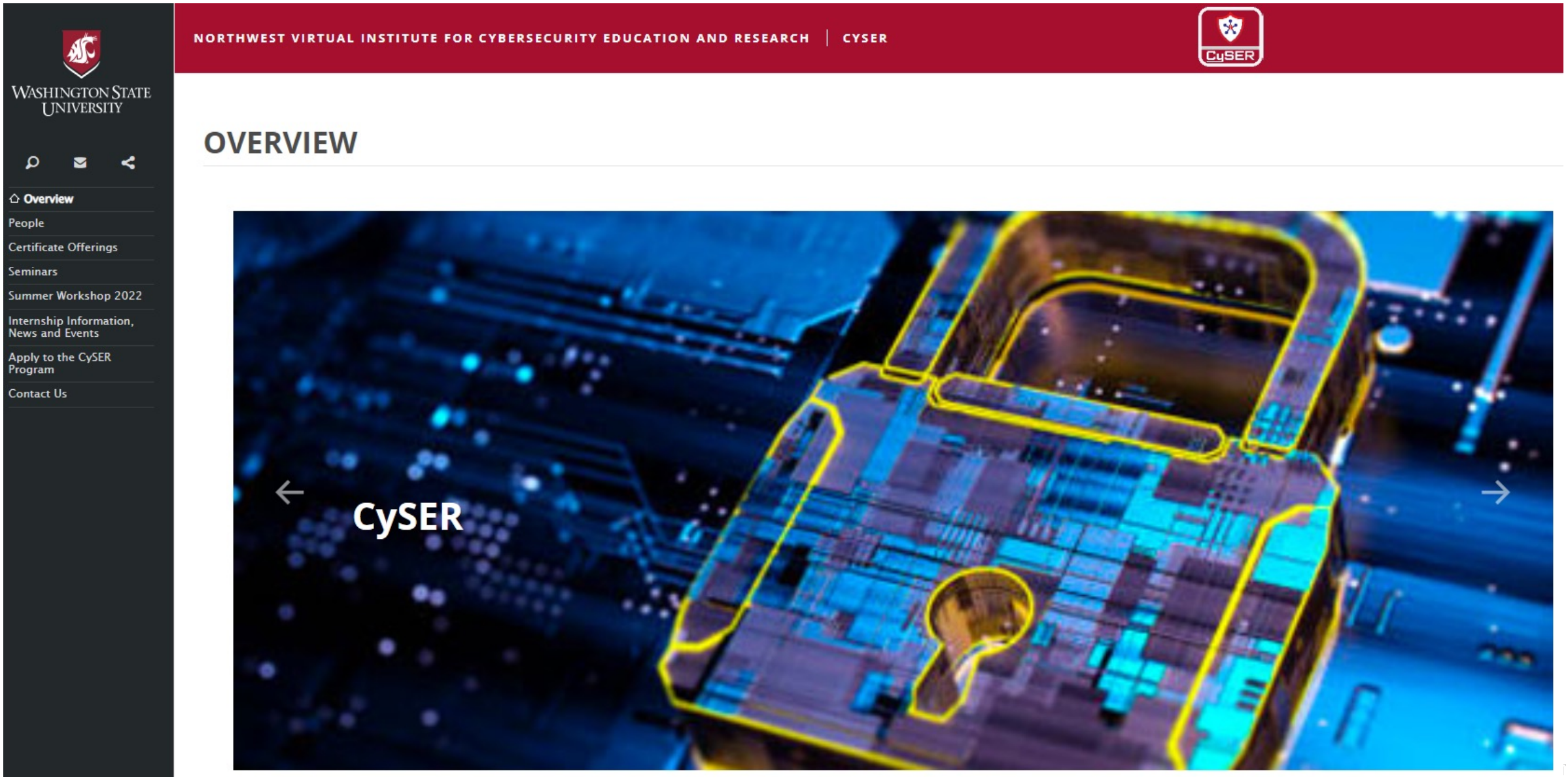
James Alves-Foss (UI)

Matthew Boehnke (CBC)

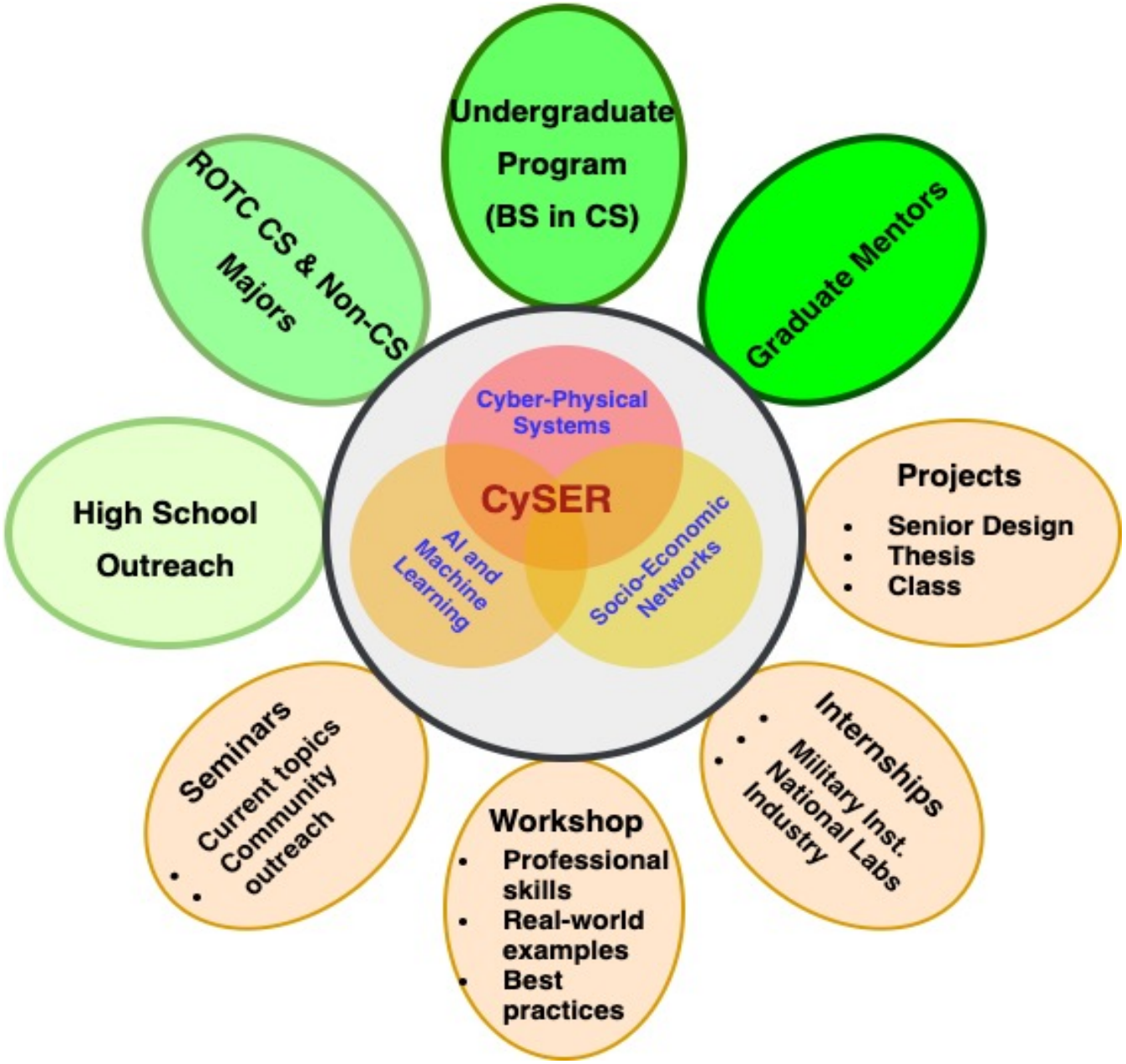
LTC Andrew Van Den Hoek (CWU)

- 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



GRIFFISS INSTITUTE

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

DOE Omni Technology Alliance
INTERNSHIP PROGRAM
de omnibus dubitandum
Be suspicious of everything

We All Soar Together

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 Columbia Basin College

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

CERTIFIED AS A NATIONAL CENTER OF ACADEMIC EXCELLENCE (CAE2Y)

Designation is certified by the National Security Agency (NSA) and the U.S. Department of Homeland Security due to the college's proof of commitment to excellence in the field of Information Assurance and Cyber Defense Education.

CBC CySER

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

CBC CySER

Research Activities (mappings + highlights)

			security operations	security research
CSIA 320: Ethical Hacking	• Asset Security • Software Development Security	Certified Ethical Hacker (CEH)	Analyze ARP cache poisoning attack.	**Use algorithmic approach to predict malware infection rates.**
CSIA 330: Wireless Security	• Communication and Network Security	Certified Wireless Security Professional (CWSP)	Assess and strengthen wireless security assets.	Remediate smart meter firmware vulnerability.
CSIA 420: Cyber Crime and Terrorism	• Security and Risk Management • Security Operations		Quantify cybersecurity risk using Monte Carlo methods.	**Optimize control selection to minimize cybersecurity risk.**
CSIA 440: Cyber Testing and Penetration	• Security Assessment and Testing		Complete full penetration test on physical production network.	Predict phishing email success based on keyword analysis.
CSIA 450: Cyber Security Capstone	• Security Architecture and Engineering • Identity and Access Management		Assess mobile device security models and vulnerabilities.	Predict social engineering success based on human risk indices.

Cyber Security Program

planned CySER enhancements

		theory	practice
CSIA 320: Ethical Hacking	Planned for Spring 2022.	Increase foundational content in cloud security, web application security, and application security.	• Develop projects for each of these three areas.
CSIA 330: Wireless Security	Complete for Winter 2022.	Increase foundational knowledge in the electromagnetic spectrum.	• Review and summarize a relevant cybersecurity research paper in this area.
CSIA 440: Cyber Testing and Penetration	Planned for Fall 2023.	Increase foundational content in reverse engineering and malware pedigree.	• Enhance malware assessment to include pedigree. • Develop new assessment for reverse engineering.
CSIA 450: Cyber Security Capstone	Planned for Fall 2023.	Increase foundational content in data science and data science theory and ensure mathematical foundations of cryptography.	• Provide data science and data science theory topics for capstone projects. • Enhance cryptography assessment to include more rigorous mathematical foundations.

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

CBC CySER

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?

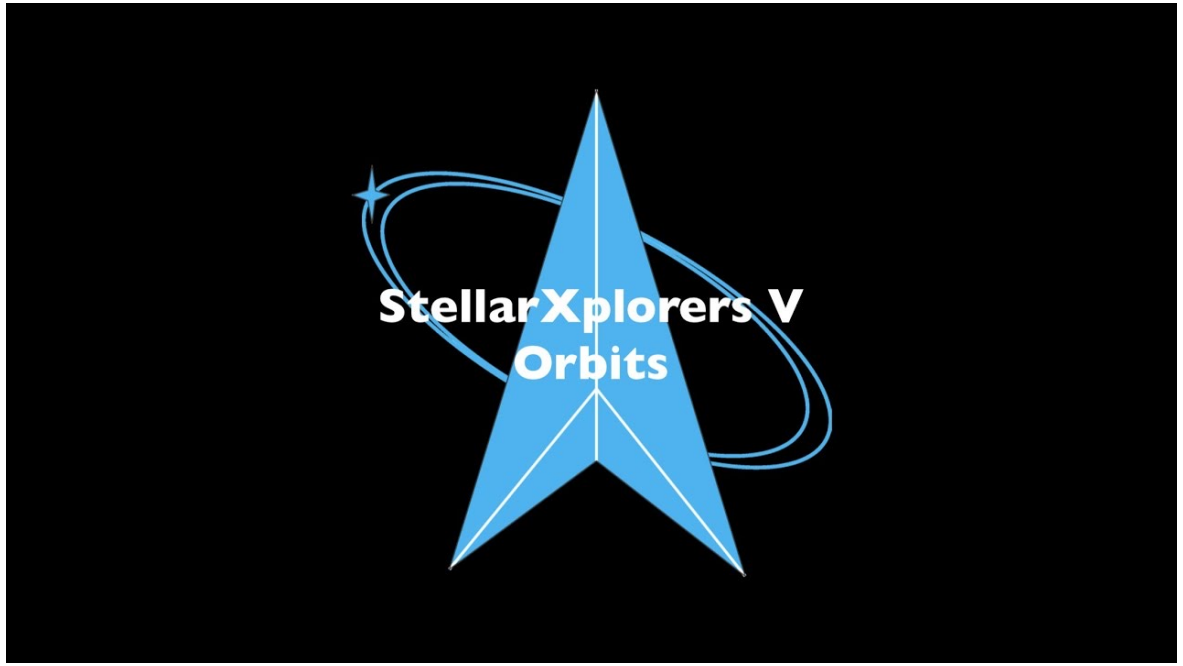
NCL - Background

- 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.

CyberPatriot

- 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.

StellarXplorers



- 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.

CyberForce

- 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

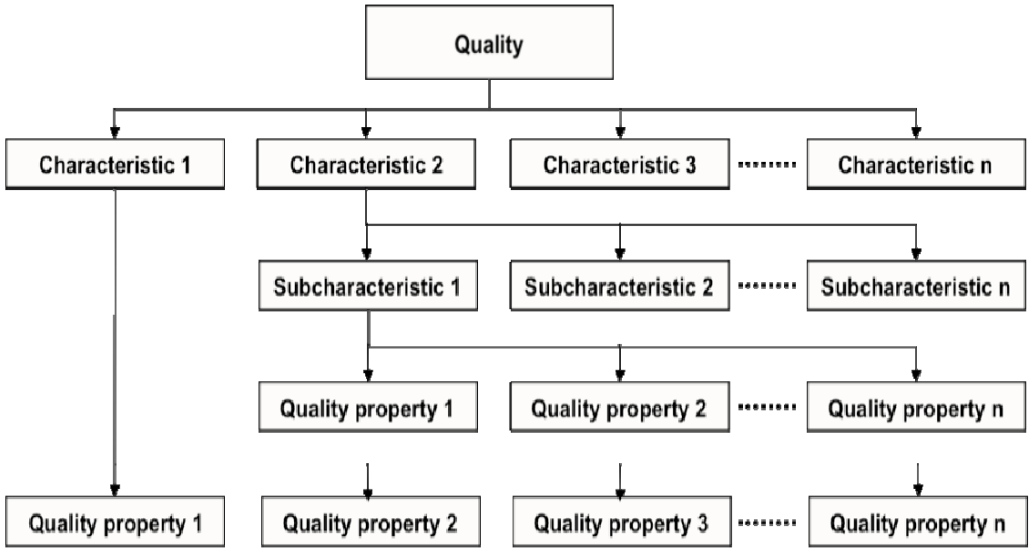
Participants:

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

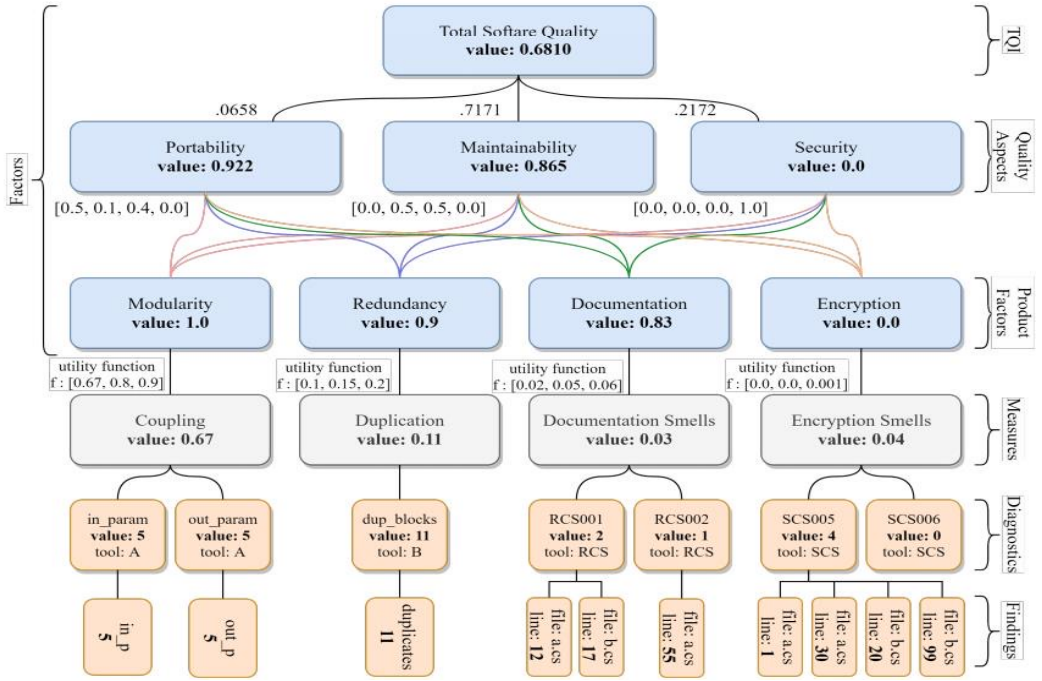
2021-2022 Academic year: 4 Air Force cadets
2022-2023 Academic year: 2 Air Force and 2 Army cadets

Hierarchical Software QA Modeling

Theoretical



Operational



Standards
ISO/IEC 9126:2001
ISO/IEC 25010:2011
NIST 800-53/82
RMF (Risk Management Framework)

Quamoco (2012 Wagner et al.)
Qatch (2017 Miltiades et al.)
PIQUE (2020 SEL MSU)

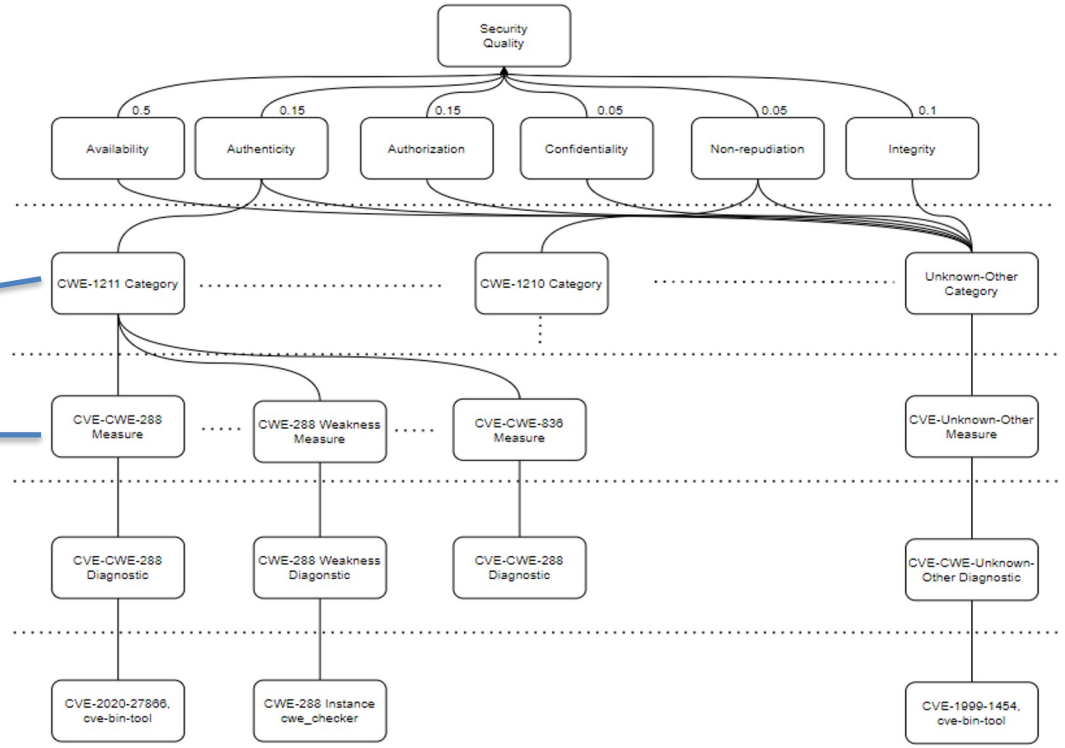
CWE-699 View Structure

699 - Software Development

- C API / Function Errors - *(1228)*
  - B Use of Inherently Dangerous Function - *(242)*
  - B Use of Function with Inconsistent Implementations - *(474)*
  - B Undefined Behavior for Input to API - *(475)*
  - B Use of Obsolete Function - *(477)*
  - B Use of Potentially Dangerous Function - *(676)*
  - B Use of Low-Level Functionality - *(695)*
  - B Exposed Dangerous Method or Function - *(749)*
- C Audit / Logging Errors - *(1210)*
  - B Improper Output Neutralization for Logs - *(117)*
  - B Truncation of Security-relevant Information - *(222)*
  - B Omission of Security-relevant Information - *(223)*
  - B Obscured Security-relevant Information by Alternate Name - *(224)*
  - B Insertion of Sensitive Information into Log File - *(532)*
  - B Insufficient Logging - *(778)*
  - B Logging of Excessive Data - *(779)*
- C Authentication Errors - *(1211)*
  - B Authentication Bypass Using an Alternate Path or Channel - *(288)*
  - B Authentication Bypass by Spoofing - *(290)*
  - B Authentication Bypass by Capture-replay - *(294)*
  - B Improper Certificate Validation - *(295)*
  - B Improper Following of a Certificate's Chain of Trust - *(296)*
  - B Improper Check for Certificate Revocation - *(299)*
  - B Incorrect Implementation of Authentication Algorithm - *(303)*
  - B Missing Critical Step in Authentication - *(304)*
  - B Authentication Bypass by Primary Weakness - *(305)*
  - B Missing Authentication for Critical Function - *(306)*
  - B Improper Restriction of Excessive Authentication Attempts - *(307)*
  - B Use of Single-factor Authentication - *(308)*
  - B Use of Password System for Primary Authentication - *(309)*
  - B Key Exchange without Entity Authentication - *(322)*
  - B Use of Client-Side Authentication - *(603)*
  - B Overly Restrictive Account Lockout Mechanism - *(645)*
  - B Guessable CAPTCHA - *(804)*
  - B Use of Password Hash Instead of Password for Authentication - *(836)*

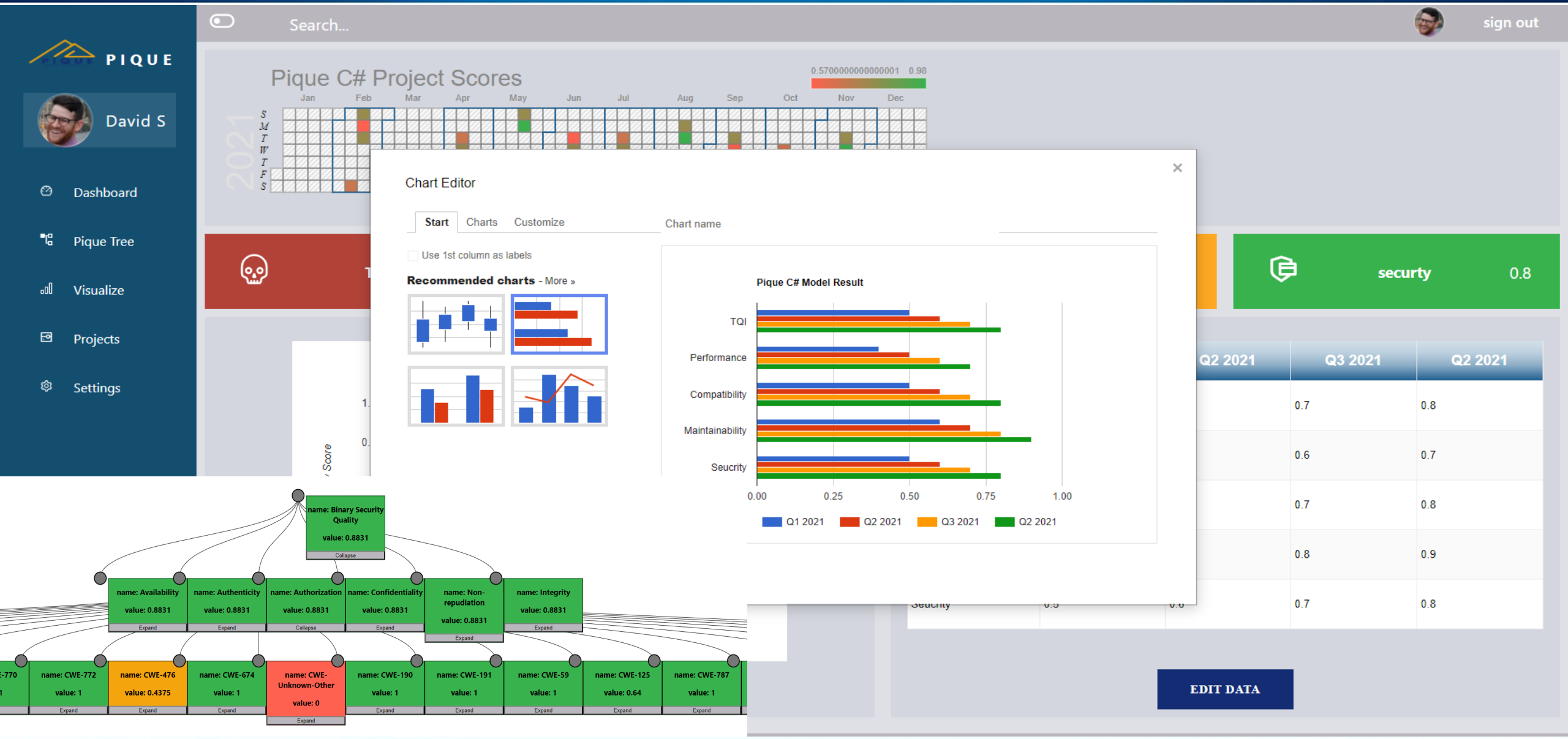
Microsoft STRIDE

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

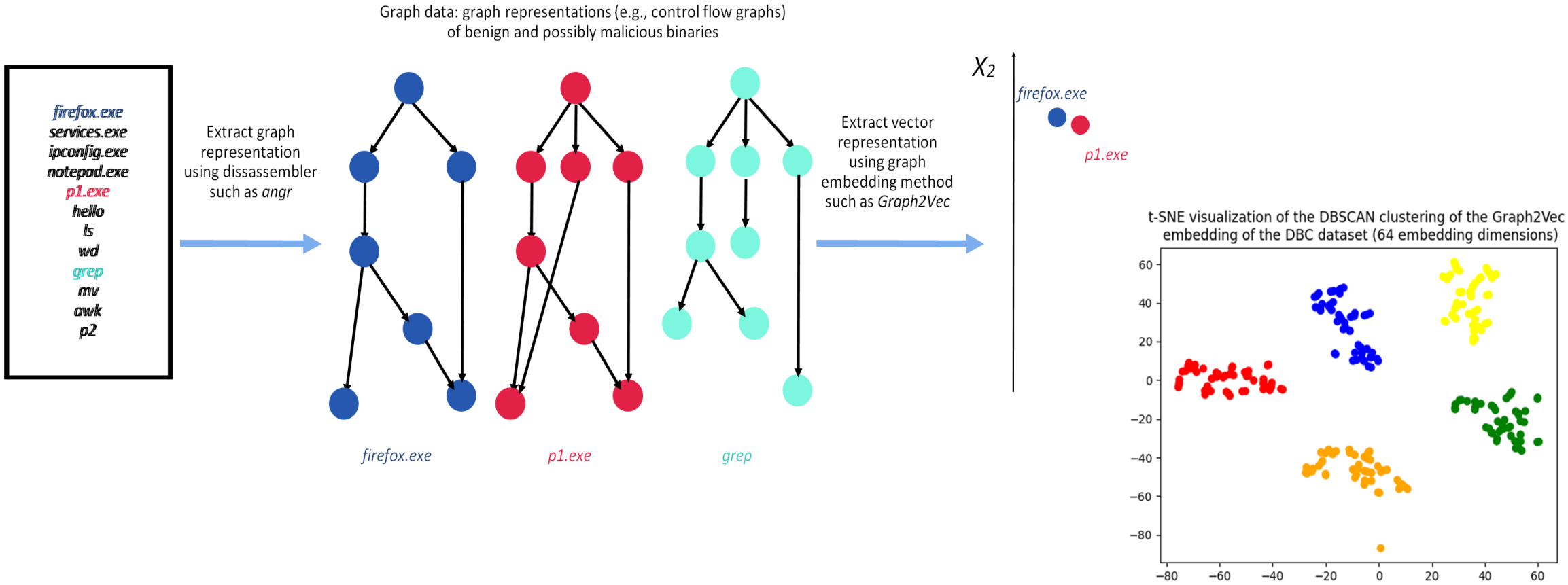


PIQUE Models

- 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)***

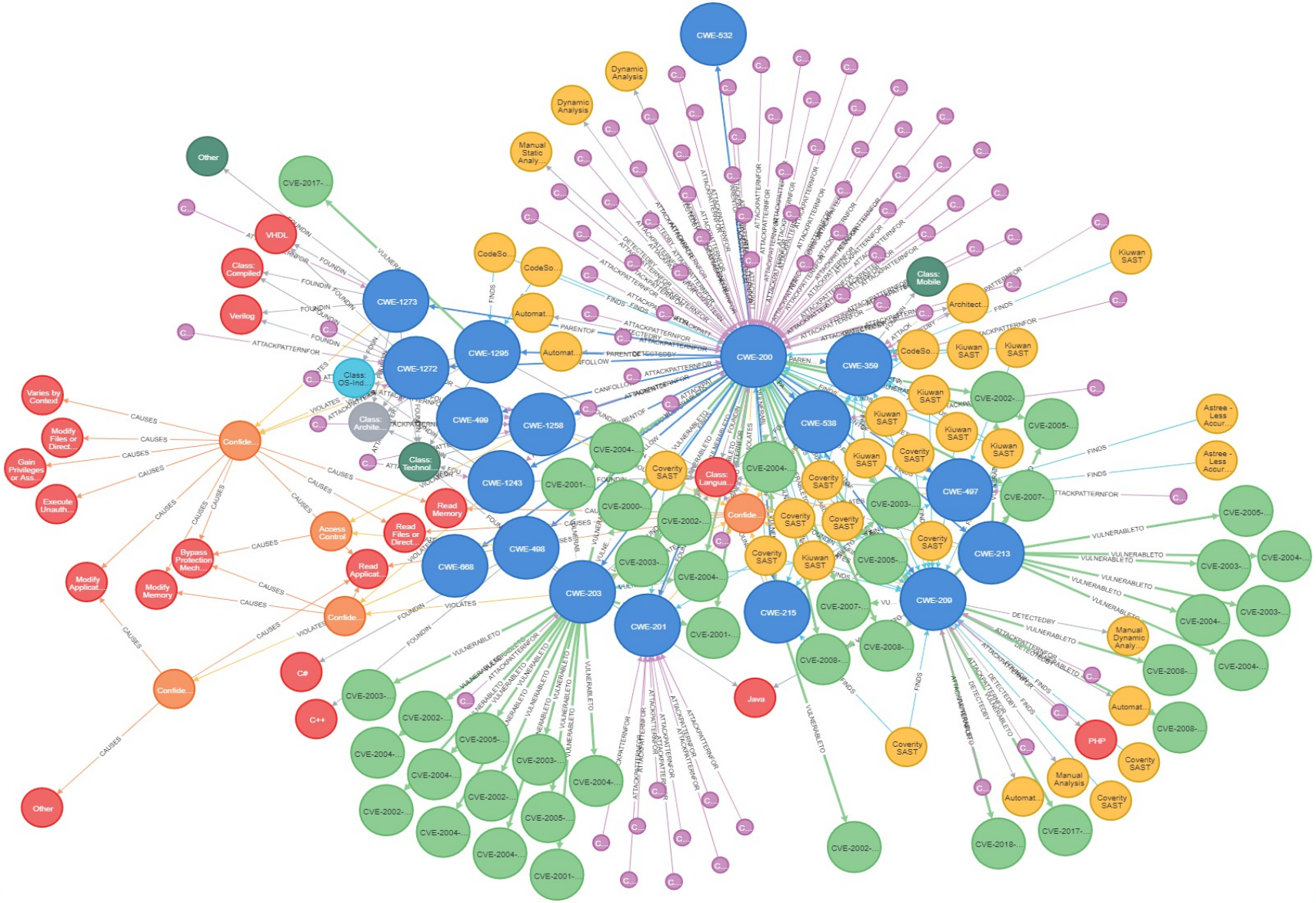

PIQUE
David S
Dashboard
Pique Tree
Visualize
Projects
Settings
Search...
sign out
Pique C# Project Scores
0.5700000000000001
0.98
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
2021
Chart Editor
Start
Charts
Customize
Chart name
Use 1st column as labels
Recommended charts - More »
Pique C# Model Result
TQI
Performance
Compatibility
Maintainability
Seucrity
0.00
0.25
0.50
0.75
1.00
Q1 2021
Q2 2021
Q3 2021
Q2 2021
securty
0.8
Q2 2021
Q3 2021
Q2 2021
0.7
0.8
0.6
0.7
0.7
0.8
0.8
0.9
0.7
0.8
EDIT DATA
name: Binary Security Quality
value: 0.8831
Collapse
name: Availability
value: 0.8831
name: Authenticity
value: 0.8831
name: Authorization
value: 0.8831
name: Confidentiality
value: 0.8831
name: Non-repudiation
value: 0.8831
name: Integrity
value: 0.8831
Expand
Collapse
name: CWE-772
value: 1
name: CWE-476
value: 0.4375
name: CWE-674
value: 1
name: CWE-Unknown-Other
value: 0
name: CWE-190
value: 1
name: CWE-191
value: 1
name: CWE-59
value: 1
name: CWE-125
value: 0.64
name: CWE-787
value: 1

Classification, clustering, and anomaly detection using graph representations of code

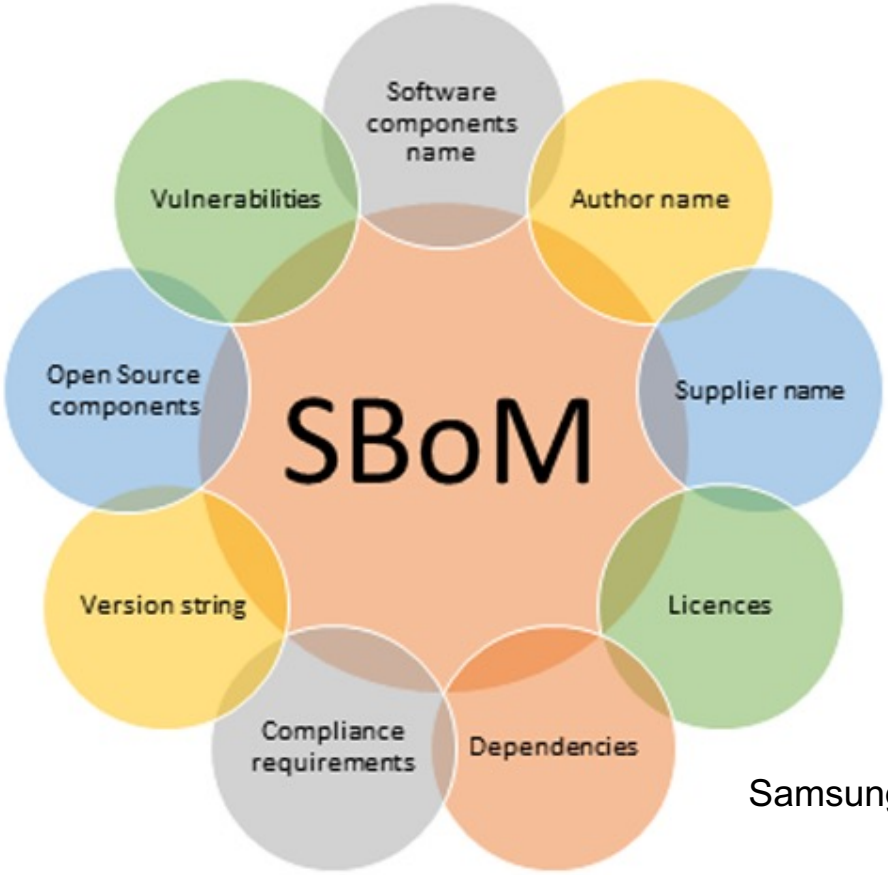


Decomposition of CWE-200

Identify security zones and sensitive sections of source code



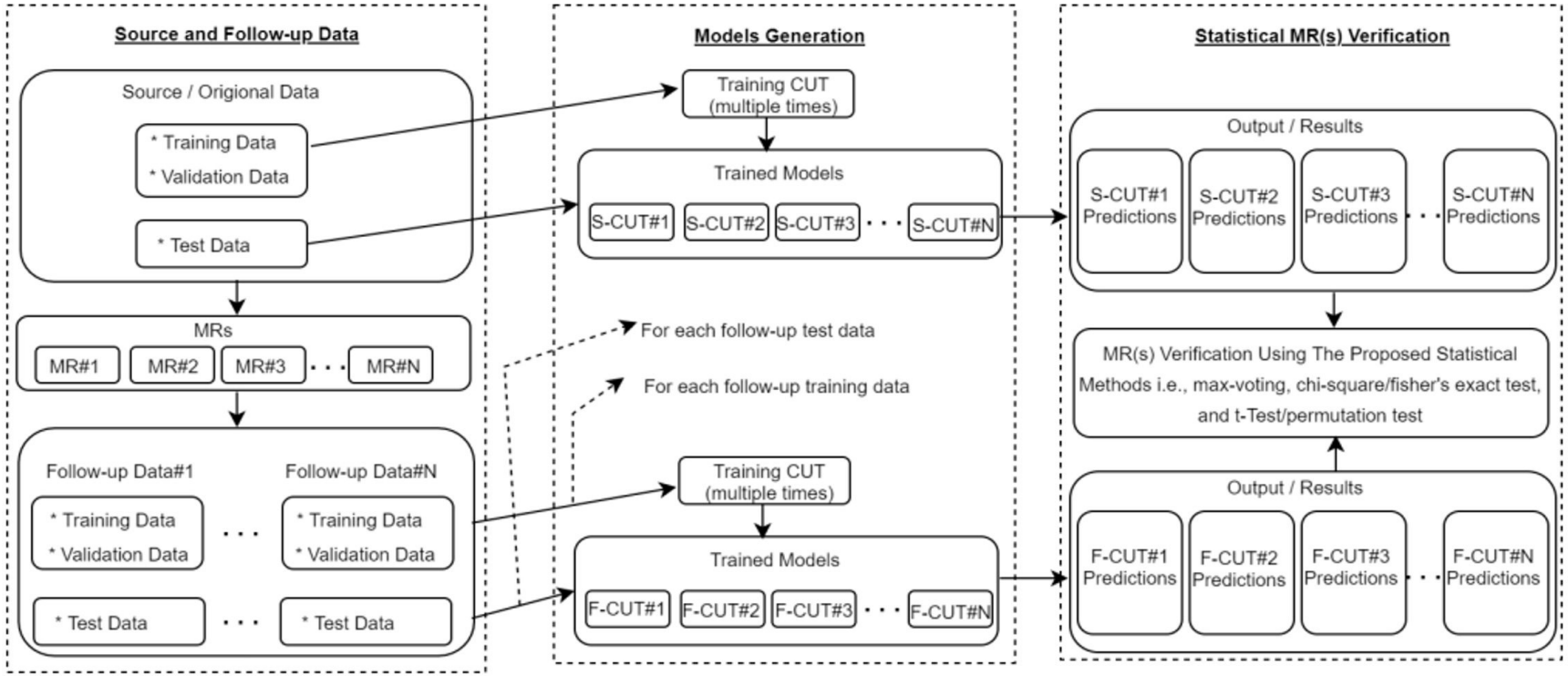
Assess the composition, stylometry and origination of software to verify that they are truthful, complete and accurate



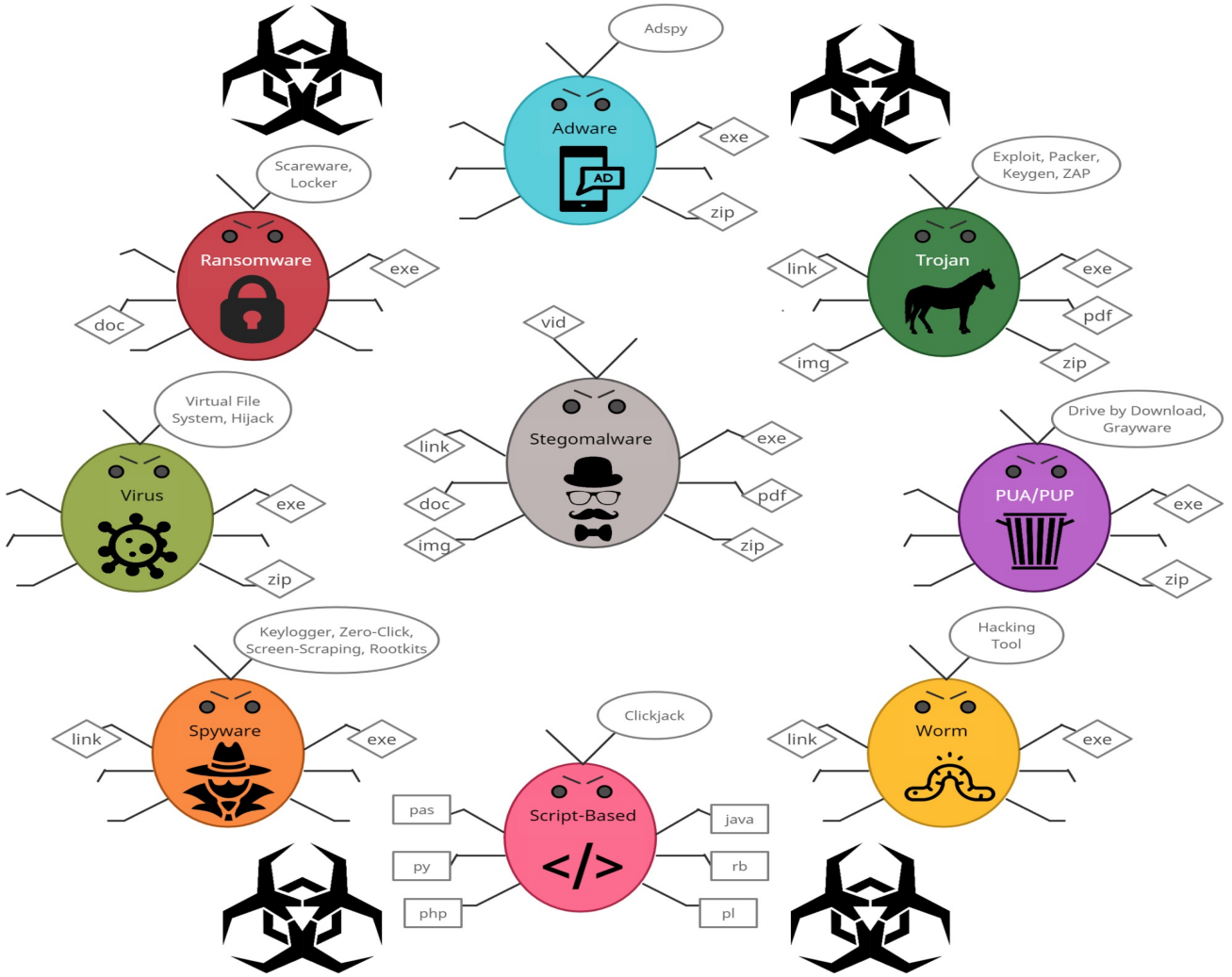
Samsung Research

Improving the confidence of machine learning models through improved software testing approaches

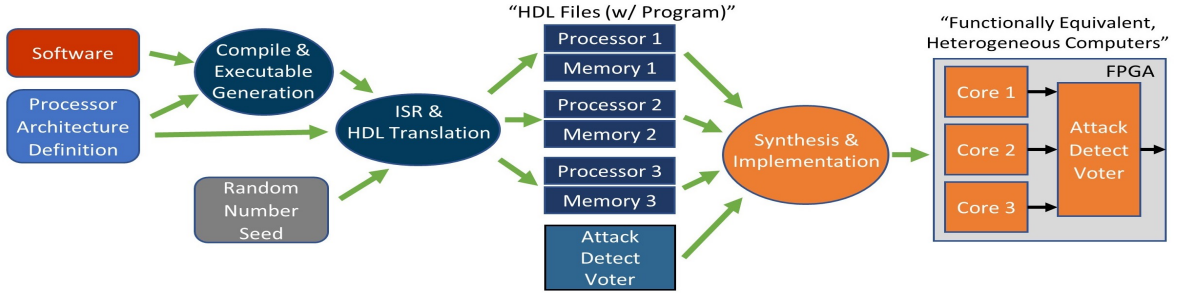
Intrusion Detection Systems

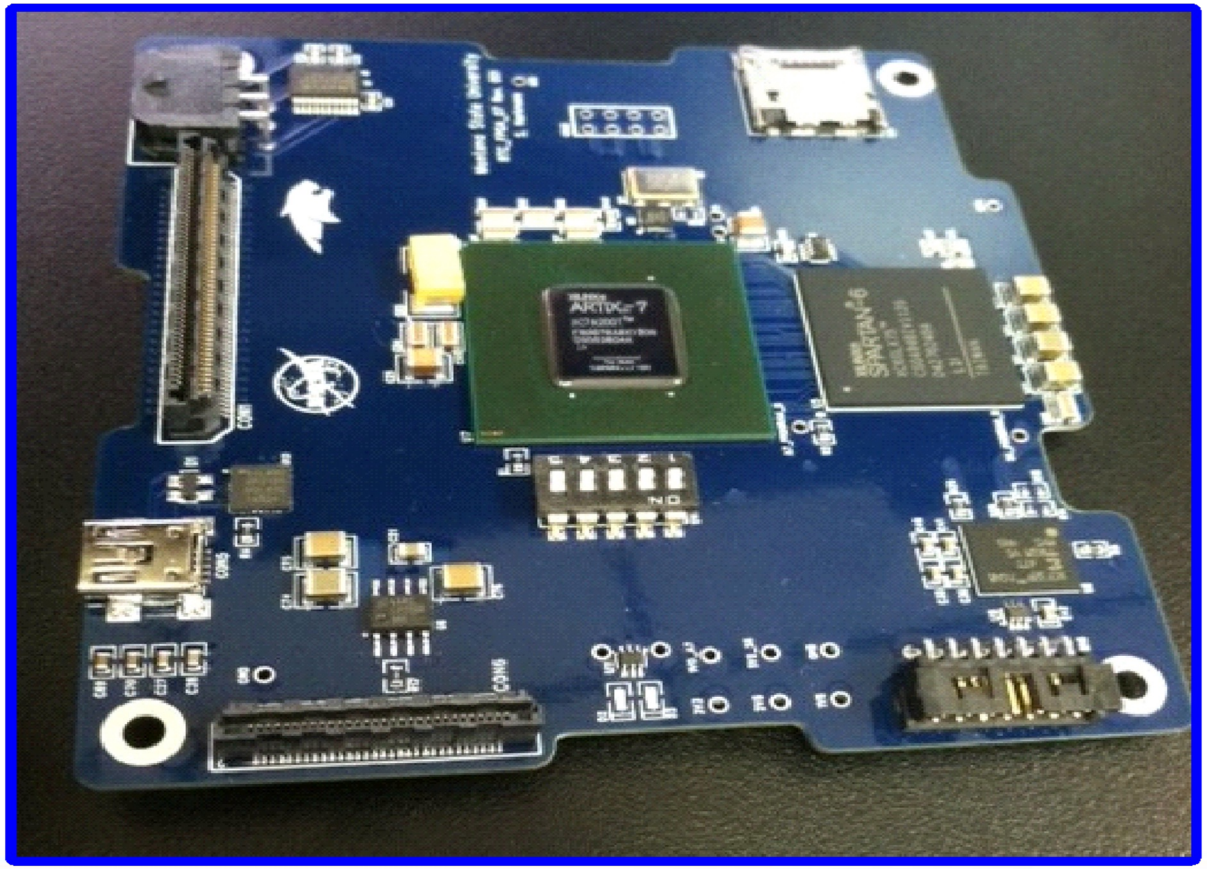


Conceptual Frameworks and Theory of Bug Bounty Platforms

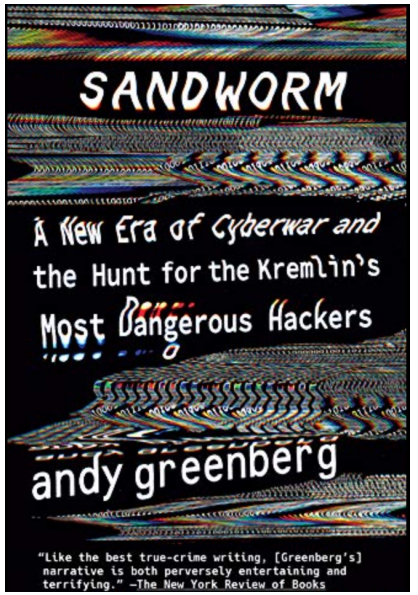


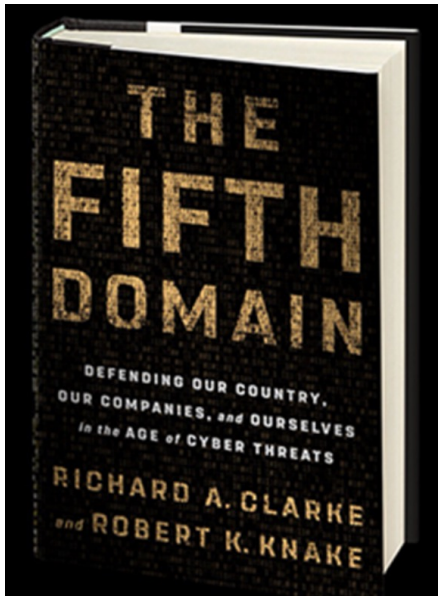
Malware detection using obfuscation of Opcodes in FPGAs





- *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

National Science Foundation	$400K
Washington State University/Griffiss Institute	$162K
Air Force, Army, CERL	$1.2M
Raytheon Technologies	$330K
Idaho National Laboratory and Department of Homeland Security	$3.1M
Department of Homeland Security	$4.47M
Resilient Computing	$150K

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

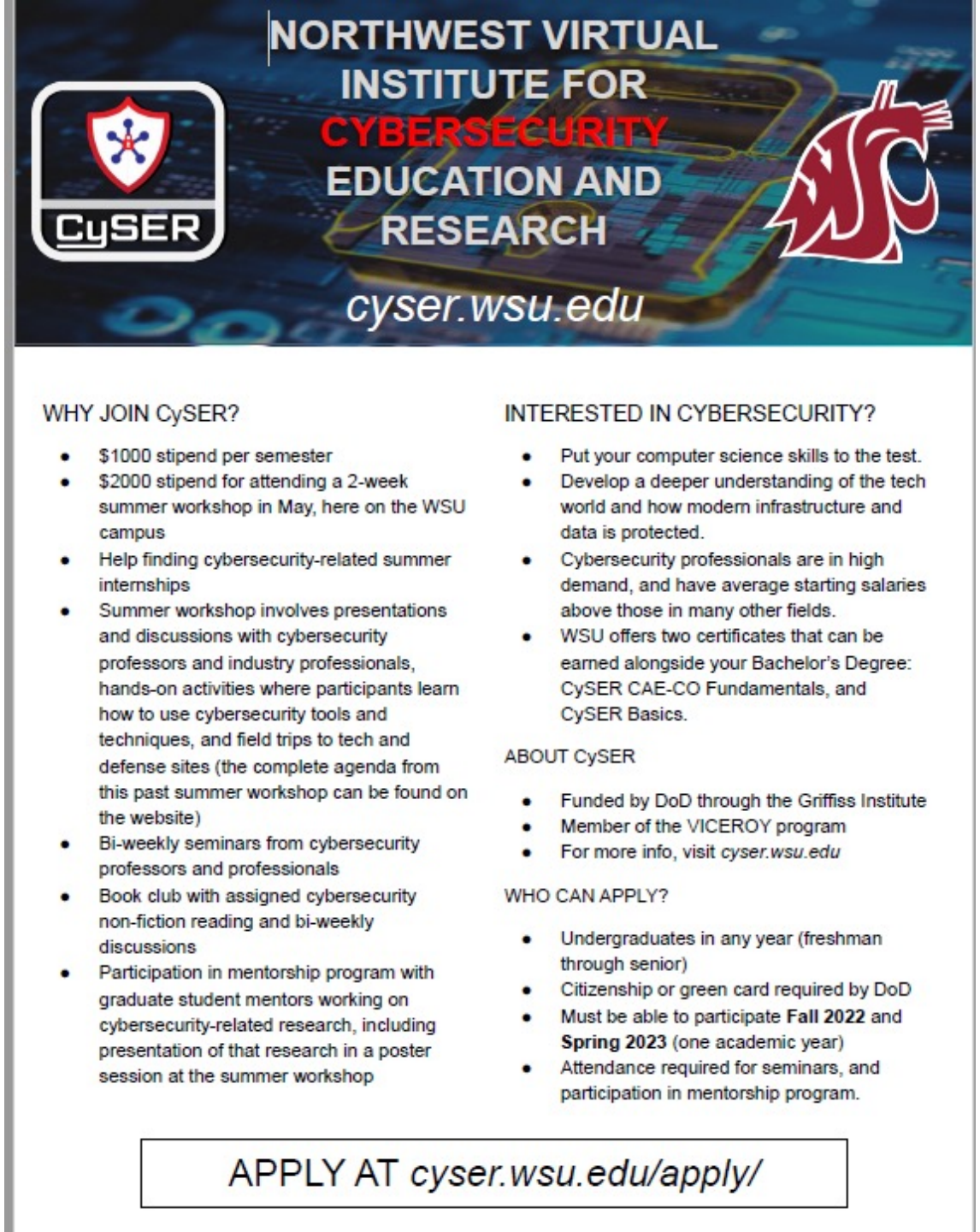
bvanwie@wsu.edu; 509-335-4103

WSU Co-PIs: Assefaw Gebremedhin, Noel Schulz

External Evaluator: Olusola Adesope

WASHINGTON STATE UNIVERSITY

- Recruitment - Poster



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

GRIFFISS INSTITUTE

Research Projects & Internships

Griffiss Institute Internship Application Deadline, Dec. 31, 2022!

NAMES	FACULTY MENTORS	PROJECTS	INTERNSHIPS
UNDERGRADUATE PROJECTS AND INTERNSHIP SUMMARY			
Arjun Anand (WSU)	Prof. Jana Doppa	Finding Cyber Attacks on Networks	None
Cai Haught (WSU)	Prof. Venera Arnaoudova	Human Factors on software vulnerabilities	GI
Griffin Gerry (WSU)	Prof. Rob Crossler	Powerless to change - Cyberwarfare	None
Hillary Zhang (WSU)	Prof. Assefaw Gebremedhin	Microsoft security	None
James Minteer (WSU)	Prof. Partha Pande	Planned Obsolescence by Aging Manycore Chips	ACE
Kaitlin White (WSU)	Prof. Assefaw Gebremedhin	Graph neural networks - polymorphic virus detection - reverse engineering	None
Matthew Kusman (WSU)	Prof. Chris Hundhausen	Tools for cybersecurity education and assessment/ identify vulnerabilities	RadixIot
Moises Carranza (WSU)	Prof. Chris Hundhausen	Tools for cybersecurity education and assessment/ identify vulnerabilities	None
Nathan Waltz (WSU)	Prof. Assefaw Gebremedhin	Graph neural networks - polymorphic virus detection - reverse engineering	SEL
Noah Black (CWU)	Deborah Wells	USB hot-plug attack counter forensics	GI
Paul Wilmoth (WSU)	Prof. Rob Crossler	Powerless to change – Cyberwarfare	None
Timothy Cain (WSU)	Prof. John Miller	Clustering software vulnerabilities using self-organizing maps	None
Timothy Reidy (WSU)	Prof. Larry Holder	CMU ghosts to simulate a user environment and detect novelty	GI
William Heinecke (WSU)	Prof. Assefaw Gebremedhin	Observability of network security monitoring strategies with TOMATO	None
Zachary Werle (WSU)	Prof. Assefaw Gebremedhin	Observability of network security monitoring strategies with TOMATO	GI

Student Status

INSTITUTIONS	NAMES	STATUS
GRADUATE RESEARCH MENTORS		
Washington State University	James Halverson (PhD, CS)	Civilian
Washington State University	Aryan Deshwal (PhD, CS)	Civilian
Washington State University	Justin Stachofsky (PhD, MIS)	Civilian
Washington State University	James Crabb (MS, CS)	Civilian
Washington State University	Brenden Fraser-Hevlin (PhD, ChE)	Civilian
Washington State University	Vincent Lombardi (MS, CS)	Civilian
Washington State University	Blessing Adaramola (Ed/Psych)	Civilian

WSU Courses

- Course content and syllabi for 3 new courses developed

CptS 327: Intro. to Cyber Security || Computer, Web & Applications Sec.	CptS 427 New: Applied Cyber Security || Software, Network & Cloud Security	CptS 428/528: Advanced Cyber Security || Reverse Engineering & Forensics
Offered Fall 2022 & Spring 2022/2023	**Offered Spring 2023**	**Offered Fall 2022**
KUs: M7, M8, M9, O4, O13, C4	KUs: M4, M9, O2, O3, O4, O13, C4	KUs: M2, O8, C1, C2, C5, S1, S2, S7
• 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 dif.) • 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)

GRIFFISS INSTITUTE

WSU Certificate Programs Approved by Faculty Senate

- **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 121Intro 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

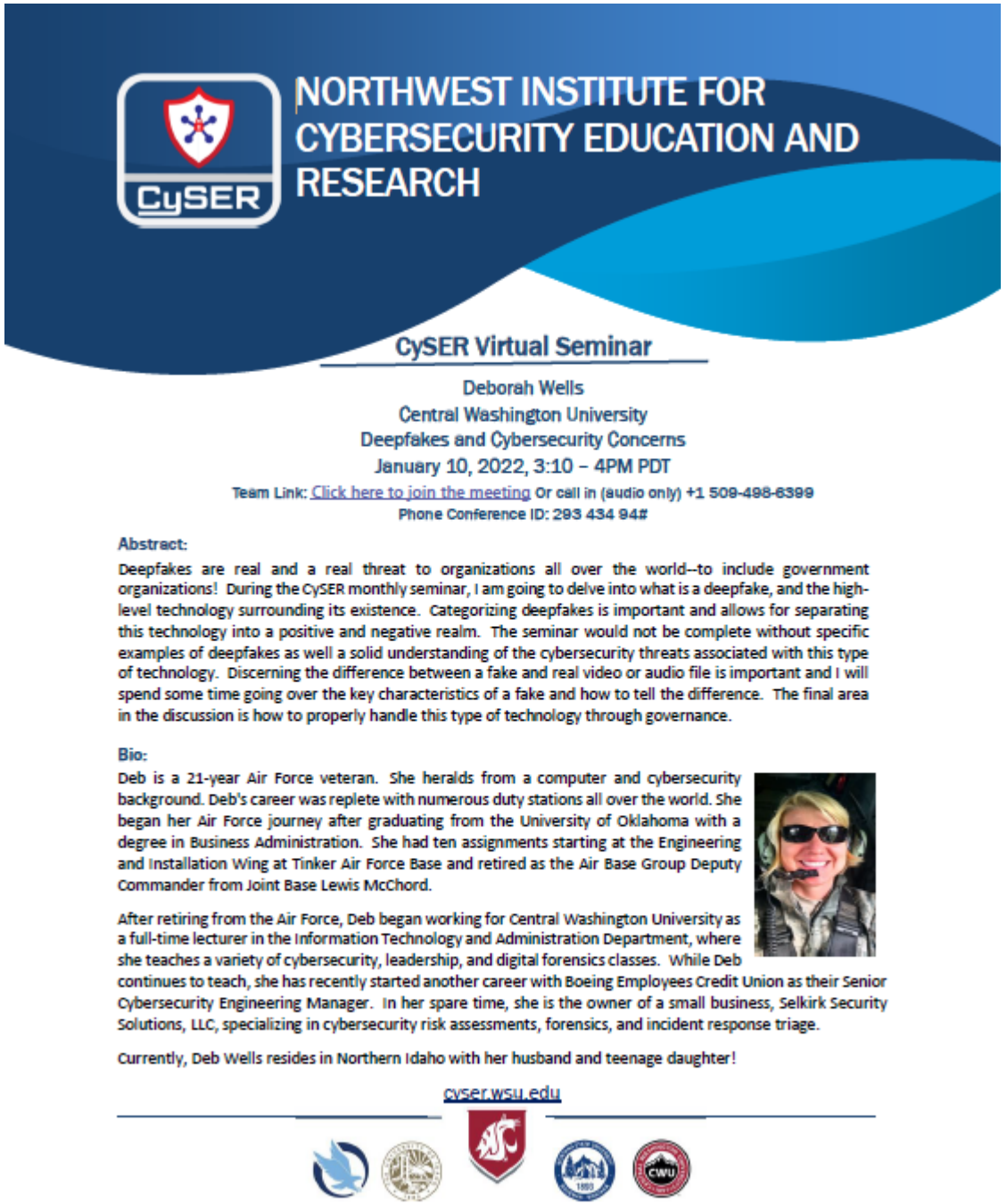
- Competition dates: Nov 4-5, 2022
- Two teams competing from WSU (Crimson Cougs and Grey Cougs)
- Most are CySER students, some are outside CySER, all are members of the CSG student club

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



NORTHWEST INSTITUTE FOR CYBERSECURITY EDUCATION AND RESEARCH

CySER

CySER Virtual Seminar

Deborah Wells
Central Washington University
Deepfakes and Cybersecurity Concerns
January 10, 2022, 3:10 – 4PM PDT

Team Link: Click here to join the meeting Or call in (audio only) +1 509-498-6399
Phone Conference ID: 293 434 94#

Abstract:

Deepfakes are real and a real threat to organizations all over the world--to include government organizations! During the CySER monthly seminar, I am going to delve into what is a deepfake, and the high-level technology surrounding its existence. Categorizing deepfakes is important and allows for separating this technology into a positive and negative realm. The seminar would not be complete without specific examples of deepfakes as well a solid understanding of the cybersecurity threats associated with this type of technology. Discerning the difference between a fake and real video or audio file is important and I will spend some time going over the key characteristics of a fake and how to tell the difference. The final area in the discussion is how to properly handle this type of technology through governance.

Bio:

Deb is a 21-year Air Force veteran. She heralds from a computer and cybersecurity background. Deb's career was replete with numerous duty stations all over the world. She began her Air Force journey after graduating from the University of Oklahoma with a degree in Business Administration. She had ten assignments starting at the Engineering and Installation Wing at Tinker Air Force Base and retired as the Air Base Group Deputy Commander from Joint Base Lewis McChord.

After retiring from the Air Force, Deb began working for Central Washington University as a full-time lecturer in the Information Technology and Administration Department, where she teaches a variety of cybersecurity, leadership, and digital forensics classes. While Deb continues to teach, she has recently started another career with Boeing Employees Credit Union as their Senior Cybersecurity Engineering Manager. In her spare time, she is the owner of a small business, Selkirk Security Solutions, LLC, specializing in cybersecurity risk assessments, forensics, and incident response triage.

Currently, Deb Wells resides in Northern Idaho with her husband and teenage daughter!

cyser.wsu.edu

CWU

GRIFFISS INSTITUTE

FALL 2022 SEMINAR SERIES

Date	Speaker	Title/Media
Oct. 17	CySER PIs at partner institutions	Fall Seminar Series Kick-off: updates from partner institutions Meeting link
Oct. 31	Robert Crossler Dept of Management, Information Systems and Entrepreneurship WSU	TBD
Nov. 14	Slater Weinstock Casaba Security	TBD
Nov. 28	James Halvorsen School of EECS WSU	TBD
Dec. 12	Haipeng Cai School of EECS WSU	TBD

CySER Seminars Schedule

FALL 2021 SEMINAR SERIES

Date	Speaker	Title/Media
Nov. 29	 Dr. Clemente Izurieta Gianforte School of Computing Montana State University	Hierarchical Software Quality Assurance Approach to Leveraging Existing Technologies and Building Quality Gates Recording Slides
Nov. 8	 Matthew Boehnke Department of Computer Science Columbia Basin College	Cyberhawks and Beyond Recording Slides
Oct. 25	 Dr. Jim Alves-Foss Department of Computer Science University of Idaho	Probabilities, Percentages, and Professions of Performance Recording Slides
Oct. 11	 Dr. Assefaw H. Gebremedhin School of EECS Washington State University	CySER Overview and Machine Learning Recording Slides

GRIFFISS INSTITUTE

Schedule

SPRING 2022 SEMINAR SERIES

Date	Speaker	Title/Media
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/

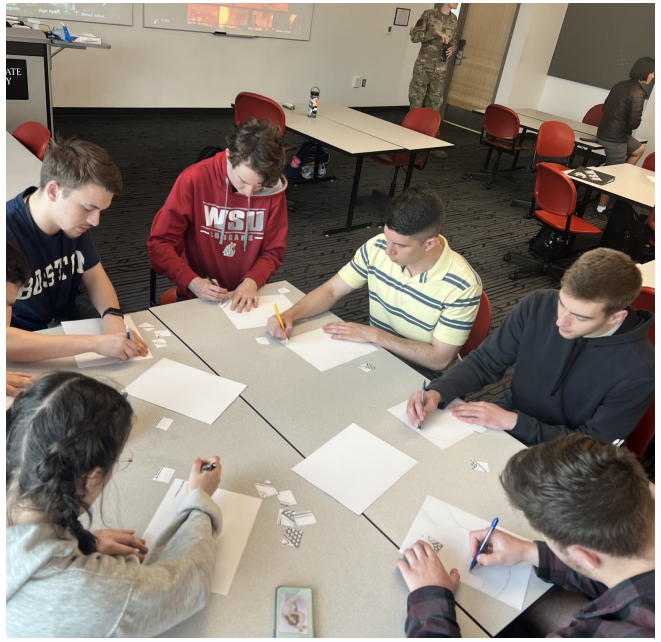
- May 23 to June 3, 2022, at WSU in Pullman, WA: presentations, tutorials, and hands-on experiential learning activities
- Field trips: a half-day trip to Schweitzer Engineering Laboratories (SEL, Pullman), full-day Fairchild Air Force Base, 2-day to Keyport Naval Undersea Warfare Center.
- In person, 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

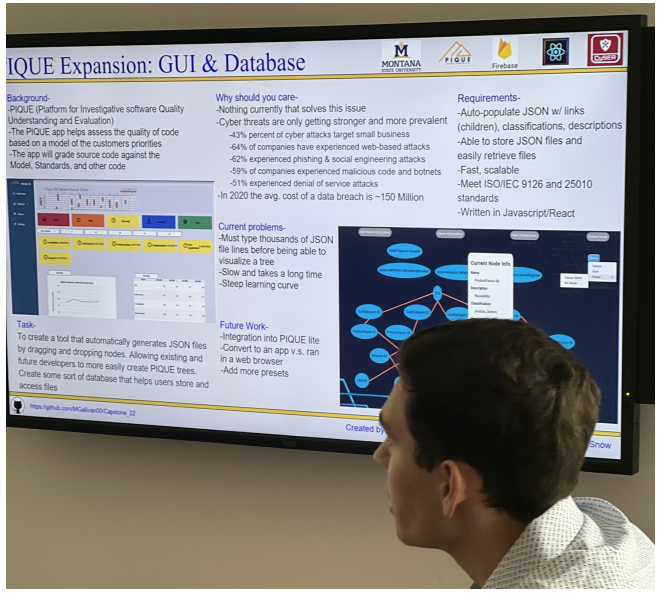
CySER Activities

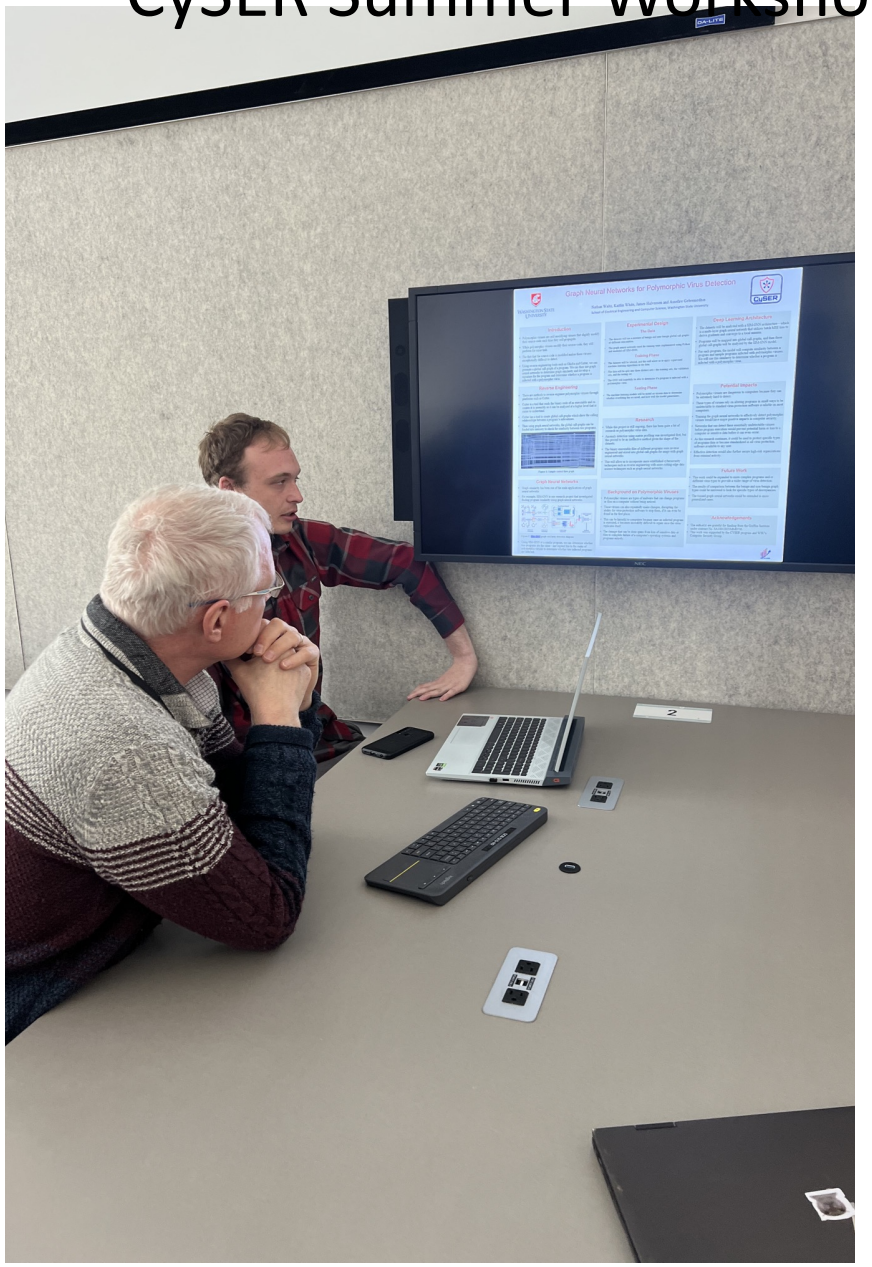
- Experiential Learning
  - Mentored cybersecurity research
  - Summer workshop: extensive hands-on components
    - Poster session
  - Leadership – Team Building
    - Major Paul Hyde (WSU)
    - Retired Captain Andrew Van Den Hoek (CWU)
    - LTC Lance Ratterman (MSU)
  - Internships
  - Mentored senior 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)

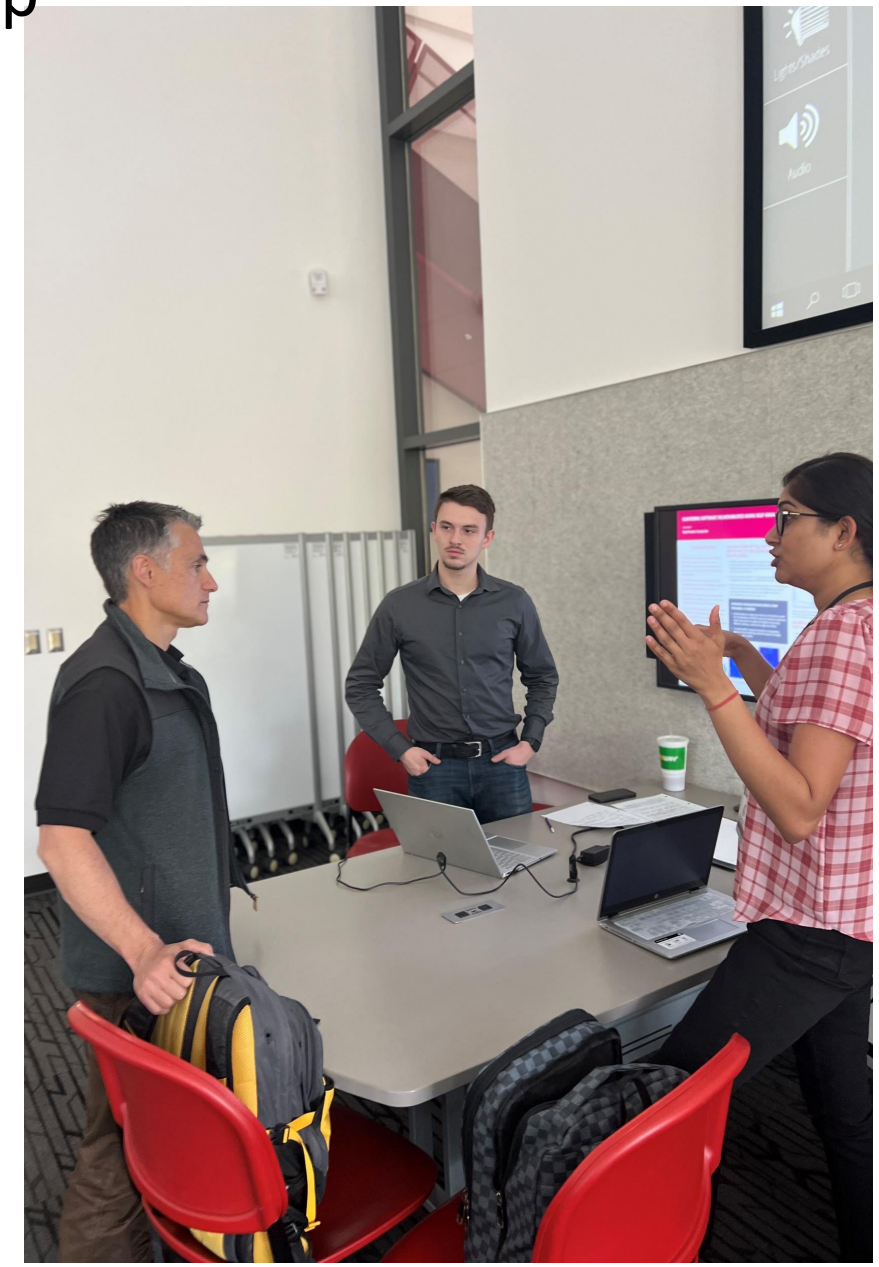
GRIFFISS INSTITUTE

CySER Summer Workshop









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

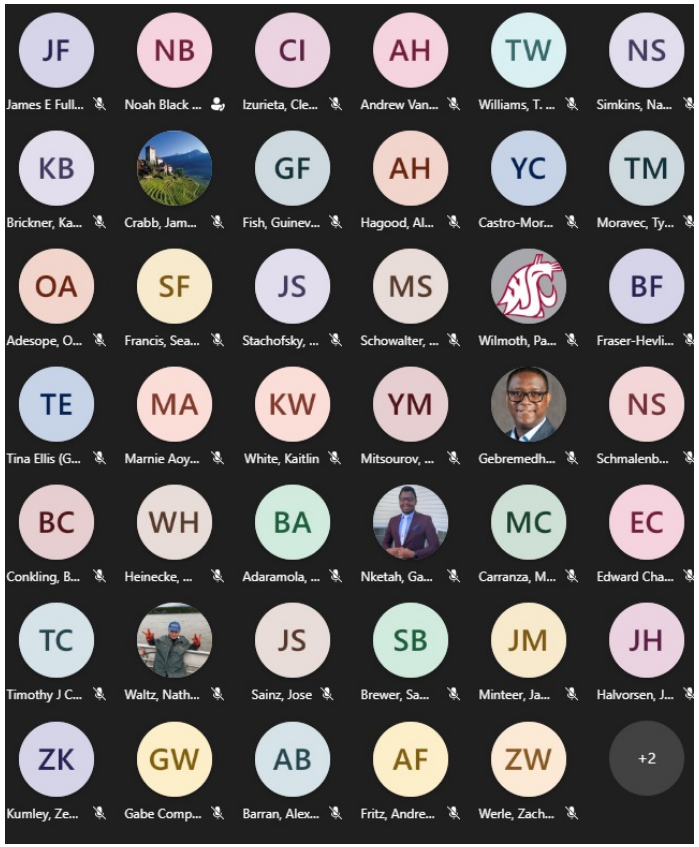
Overall, Year 1 achievements of project objectives and outcomes were successful, and plans for year 2 are realistic, aligned with project goals, and well-crafted to reach indicated milestones.

Summary

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



GRIFFISS INSTITUTE