Cybersecurity Workshop
Technical Abstract Descriptions

Wednesday, August 30, 2023, 3:00 – 5:00 p.m.

Session 1 **Cyberspace Test Technology**
Chair Dr. Mike Shields, Chief Scientist for the TRMC T&E/S&T Cyberspace Test Technology (CTT)

3:00 p.m. **"Activity and Content Enhancement – Next Gen Traffic Generation Toolkit"**
Steve Durst, R&D Engineer, Skaion Corporation

On-host and network traffic generation are essential aspects to conducting effective cyber operations testing and training.

Activity and Content Enhancement (ACE) provides AI-based realism on-host and network activity that is convincingly human and representative of the target environment.

We present the Advanced Cyber Environment, a next-generation traffic generation toolkit for implementing and controlling highly realistic on-host user behavior, network traffic, modern social interactions between users, and live network services, all suitable for use in a closed or "clean room" environment.

3:30 p.m. **"Vader Modular Fuzzer (VMF) – USG Fuzzing Capability"**
Arch Owen, Program Manager for Weapon Security, Draper Laboratory

TRMC T&E/S&T CTT (Cyberspace Test Technology) has initiated an effort to expand USG (United States Government)-wide awareness and experience in fuzzing, and to provide tools suited to DoD needs - specifically tools that are affordable, usable in closed spaces, suited to unique testing needs (e.g. real time embedded systems), easily adapted, incorporate the latest fuzzing techniques, and can be quickly learned by non-fuzzing experts. In order to support this initiative, the CTT is developing Vader Modular Fuzzer (VMF), a suite of fuzzers and modules that allow users to tailor fuzzers to specific needs. In addition, USG Fuzzing Working Group is stood up to promote adoption of VMF and share knowledge on fuzzing. This presentation is to update the T&E community on the VMF development status, the features included in current phase (Phase 2 of 4-year project) and how to get started with VMF.

4:00 p.m. **"Measure and Share: TRMC T&E/S&T Cyberspace Test Technology's Project to Improve Cyber T&E Impacts Across DoD"**
Dr. Donald Pellegrino, CEO, DeciSym, LLC

The Measure and Share Initiative is to Measure the Efficacy of Cyber Test and Evaluation, and Share the results at an appropriate classification level by providing a relevant perspective to the DoD stakeholders.

The Goals of this initiative are:

- ♦ *Improve T&E Results*
- ♦ *Improve JTF and Service Commanders Cyber Knowledge*
- ♦ *Enable Better Acquisition Outcomes*
- ♦ *Improve Intelligence Community Reporting Impacts*

The initial focus has been a development of a distributed, secured data storage system designed to enable organizations to store the data (for example, system models, test plans, test results, etc.) at appropriate classification levels.

This presentation will describe the Measure and Share Initiative in depth including the Concepts of Operations, current status and a way forward.

4:30 p.m. **"Extensible QEMU for Broader Emulation Functionality and Application"**
Arch Owen, Program Manager for Weapon Security, Draper Laboratory

TRMC is funding development of a more extensible version of QEMU (QuickEMUlator) to support a broader range of applications relevant to DoD needs than is feasible with the standard QEMU. QEMU is a very popular, open-source emulator used in a wide range of applications, both within the DoD and in broader industry. Being open-source, it is a very attractive alternate to fee-based emulators such as SIMICS. Furthermore, QEMU allows for plug-ins so that users can add their functionality to the base QEMU. However, despite the plug-in functionality, the base QEMU is not as adaptable and extensible as many users need. As such, users often create their own, isolated, QEMU branch with one-off application-specific modification that are not easily integrated with other user-specific branches of QEMU. To overcome this plethora of unsupported, isolated, one-off QEMU instances, and to enable a broader range of QEMU application, TRMC is funding the development of a QEMU enhancement that (1) provides a more robust extensibility than the current QEMU plug-in interface, and (2) includes new functionality that can be applied to a range of DoD emulation needs. This presentation will describe some of the current QEMU limitations, the design of this new QEMU extensibility, and some new capabilities that will be enabled with this new QEMU extensibility.

Wednesday, August 30, 2023, 3:00 – 5:00 p.m.

Session 2 **Cyber Resilience Requirements**
Chair Jean Petty, Cyber Resilience T&E Manager, Department of Homeland Security

3:00 p.m. **"Lessons Learned from Conducting Operational Cyber Testing for Mission Resilience"**
Mr. Timothy Fitzgerald, Cybersecurity Assessments Flight Director, 346th Test Squadron

The 346th Test Squadron Cybersecurity Assessments flight conducts advanced penetration testing and technical analysis to validate offensive cyber operations, defensive cyber operations, airframe, satellite, radar, seaborne, and special mission system capabilities supporting Air Force, Joint, combatant command, and Department of Defense objectives. Our presentation includes a discussion of lessons learned from our penetration testing, vulnerability assessments, and compliance assessments for testing for mission resilience. This includes assessing for cyber operational effectiveness and suitability of systems with trained operators and defenders, in operationally representative contested environments. It also helps determine susceptibility of the system to cyberspace attacks, effectiveness of controls to identify and mitigate of mission critical vulnerabilities, and recoverability from cyberspace attacks both during the operational mission and after it. The output of our assessments illuminate cybersecurity weaknesses in the systems and missions we evaluate, and provide answers to whether these weaknesses allow threat actors, intentionally or unintentionally, the opportunity to disrupt, degrade, or deny the accomplishment of its Critical Operational Issues and Mission Essential Functions. To help counter these cybersecurity threats, we provide remediation recommendations to reduce risk to the system and mission.

We support various acquisition programs and project types, to include operational testing (e.g., Cooperative Vulnerability and Penetration Assessments, congressional oversight systems), acquisition milestones decisions, system certifications (e.g., Risk Management Framework), Defense Assessments, ICS/SCADA, DevSecOps, Cyber Effects and Enabling Capabilities, and code reviews. Our assessment experience includes airframe, satellite, radar, cyber, and seaborne weapons systems. Assessments are conducted from several threat vantage points such as the malicious insider and unauthorized intruder - nearsider and outsider.

Our penetration testing, vulnerability assessment, and compliance assessment tools and tactics, techniques, and procedures are tailored to meet system cybersecurity assessment requirements. These capabilities are "packaged" into service offerings designed to identify and provide remediation recommendations to cyber security risks on the system under test as well as, on developmental and operational points across its acquisition spectrum. These type of missions we execute include: Cyber Vulnerability Assessment - a hybrid, holistic evaluation of a system, network, and/or application(s) to determine the security posture of the targeted assets; code reviews and DevSecOps support - looking at the software *code during the development process/timeline for cybersecurity flaws and identifying issues that may persist into operations; Defense Assessments - threat emulation to identify system and operator readiness to respond to cybersecurity threats.*

3:30 p.m. **"Automated Risk Assessment Process for DoD, DHS, & Other Agencies"**
Djenana Compara, President, KDM Analytics

As Federal ever-changing requirements for cybersecurity protection increase so has the importance and need to demonstrate their compliance and effectiveness within implemented/deployed IT/OT systems'. These requirements have placed a heavy burden on cybersecurity risk assessment tools, such as the need to support the Risk Management Framework (RMF), CSF (Cyber Security Framework), CSA (Cyber Survivability), and MRAP-C (Mission-based Risk Assessment Process for Cyber). Since time is of essence, these tools need to produce systematic and comprehensive assessment results in near real-time, support T&E teams in their evaluation, and propose a course of action to harden protection of systems to ensure a secure supply chain, protection of sensitive information, and readiness to mitigate cyber attacks. Acquired Data Solutions will cover preparing your IT/OT to comply with today's government requirements and the necessary artifacts through automation of risk assessment process.

4:00 p.m. **"Australian Update on Cybersecurity of Critical Infrastructure: Governance Challenges and Approaches"**
Dr. Keith F. Joiner, Senior Lecturer Test, Evaluation and Aircraft Design

The ongoing advanced persistent cyber-threat is continuing to present major challenges in Australia. Public trust in the last year has focused mainly on two large digital health data leaks where cybersecurity vulnerabilities were forecast by Offner et al. (2020). Another public event was the costly removal from Government buildings of 900 products, mainly security cameras, made by Hikvision and Dahua, where public service acquisitions were found not to be following early intelligence advice. Within a Defence context, instances of cybersecurity concerns have not been public since 2021 when the Battle Management System (BMS) made by the Israeli company Elbit came into question. This instance, and a major project to introduce an integrated air and missile defence system for Australia, saw several large companies showcase new battle-management systems at the recent Australian airshow. The Government last year legislated to provide cybersecurity oversight to 120 critical infrastructures under the Home Affairs Department with the first major audit reports submitted in September 2022. Defence is also working on new cybersecurity assessment and test processes for its weapon systems, estate and ICT infrastructure (Joiner et al. 2022).

This paper and presentation will outline several governance initiatives proposed and being trialled in Australia to help achieve more systematic cybersecurity governance. First, is the use of model-based systems engineering assessments to assess the cyber-attack surfaces and identify the kill chains (Fowler et al., 2023:

submitted): these offer superior quick risk analysis of controls, engaged cyber table-topping and a more evergreen and resilient decision-making posture. Second, is a cybersecurity governance survey based upon the complex systems governance modelling and pathology structure by Keating and Katina (2019): this offers quick diagnosis generic to any organization of the management meta-functions at greatest risk of not evolving adequately to any cybersecurity (Vanzomeren et al. 2023: preparation). Third, is a framework for cybersecurity specific to the development of space-based systems (Shazdad et al., 2022). Finally, differences will be noted in how a middle-power like Australia approaches cybersecurity uplift, particularly in areas where commercial leverage is low.

4:30 p.m. **"Test and Evaluation of Cyber Resilience using the Framework for Operational Resilience in Engineering and Systems Test"**
Dr. Peter A. Beling, Director, Intelligent Systems Division, Virginia Tech National Security Institute

This talk will describe the Framework for Operational Resilience in Engineering and System Test (FOREST) as a best practice in the context of cyber resilience of critical systems. The framework provides an end-to-end methodology for addressing cyber resilience as a development and test philosophy. Although focused on cybersecurity, the methodology applies to any resilience concerns and features of a system. FOREST can be applied at every stage of the systems engineering process and throughout the lifecycle. The framework is meant to be a reusable, repeatable, and practical framework that calls for system designers to describe a system's operational resilience design in a designated, partitioned manner that aligns with resilience requirements and directly relates to the development of associated test concepts and performance metrics.

While FOREST provides a decomposition of resilience and structure for setting requirements and test activities, it does not include tools or methods to fully support the architecting, design, or engineering aspects of operational resilience. We describe the integration of FOREST with a meta-model called Mission Aware (MA) which is intended to describe resilience features and decisions in a Model-Based Systems Engineering (MBSE) framework. MA provides a reference architecture for operational resilience of cyber-physical systems in response to security and other potential disruptions. FOREST, the MA meta-model, and the Cyber Resilience Requirement Methodology (CRRM), a companion methodology for loss-driven resilience design, provide an end-to-end framework for addressing security as a functional requirement in the systems engineering process.

Our talk will describe the application of FOREST and its companion methodologies to a case study of an Oil & Gas Pipeline System. This use case was designed to represent the characteristics and complexities of critical systems in terms of cyber resilience. The use case experiences support the hypothesis that FOREST and its companion methodologies can be used for setting requirements for operational resilience, can provide a useful aid in the design of sensing and reconfiguration options, and can serve as the basis for the derivation of measures and metrics in support of test plans.

Wednesday, August 30, 2023, 3:00 – 5:00 p.m.

Session 3 **Cyber & Spectrum Warfare Considerations in 5G/6G**
Chair Patrick Lardieri, Technical Director, National Cyber Range (NCR) Program,
Lockheed Martin

3:00 p.m. **“5G / FutureG Technology to Meet DoD Challenges”**
LTCol Ben Pimentel, PhD, USMC

The future battlefield environment envisioned in emerging warfighting concepts is characterized by the proliferation of unmanned, autonomous, and intelligent systems across all warfighting functions and echelons of command. Just as the explosion of intelligent devices designed to automate various aspects of civilian life has given rise to the commercial Internet of Things (IoT), the complex ecosystem of sensors and actuators that will accomplish tasks ranging from intelligence collection to kinetic operations represents the evolution towards the Internet of Battlefield Things (IoBT). Fifth generation (5G) and future generation (FutureG) mobile wireless networks provide the capability necessary to support the IoBT across the Joint Force. In addition to the high throughput, low latency, and high device density, 5G/FutureG networks offer spectral agility, interoperability, improved security, integrated intelligence, and the flexibility of containerized deployment through innovative approaches such as Open Radio Access Networks (ORAN). This presentation will explore the ways in which 5G/FutureG capabilities support emerging warfighting concepts and enable the Joint Force to sense, make sense, and act.

3:30 p.m. **“Cyber Threats and/or Technology Robustness”**
Jorge Laurel, NSA Cybersecurity Collaboration Center

Taking on a behemoth challenge of securing 5G can often bring about little tangible progress because the problem seems “too big.” Through public private partnerships, the Enduring Security Framework (ESF) maximized its unique position as a cross-sector working group to explore the threats to 5G and subsequently take incremental steps to securing it. ESF has released eight publicly available 5G threat reports over the past two years that outline industry and government risks associated with U.S. adoption of 5G infrastructure.

This talk will introduce the Enduring Security Framework, guide the audience through the products released by ESF over the past two years, and detail how 5G will impact industrial control systems and the secure foundation required through best practices associated with 5G infrastructure.

- ♦ *Introduce the Enduring Security Framework- a public-private partnership comprised of representatives from the Information Technology, Communications, and Defense Industrial Base critical infrastructure sectors*
- ♦ *Explore the ESF released 5G security products*

- ♦ *Walk through methodology of attacking a strategic challenge by implementing tactical, scoped plans.*

4:00 p.m. **“T&E Methods and Tools that Enable Assessment of the Operational Resilience of 5G Enabled Systems to Cyber and Spectrum Threats”**
Connor Bruso, Lockheed Martin Cyber & Intelligence

New 5G Technologies and architectures introduce significant cyber-attack surface and potential pitfalls to operational resiliency. In this talk we will cover how our team developed attacks and playbooks to support penetration testing in order to evaluate the resiliency of 5G enabled systems. We will discuss some example findings our testing has identified, the challenges faced as our processes and methodologies matured, tools and techniques that have proven helpful along the way, and opportunities for future development.

4:30 p.m. **“5G Security Assurance Specifications”**
Yong Zhou, Keysight Technologies

In this talk, we will go over the 5G security challenges, principles to follow in general, followed by current coverage of 5G/O-RAN security assurance specifications, and what is needed beyond current scope. In conclusion, we will discuss what the industry/user really needs for the security testing solution.

Wednesday, August 30, 2023, 3:00 – 5:00 p.m.

Session 4 **Cyber T&E of Generative AI Systems**
Chair Dan Rieken, American Systems Corporation & Dr. Natalie Kautz, MITRE

3:00 p.m. **“Securing the Attack Surface of AI Enabled Systems”**
Josh Harguess, PhD, Department Manager, AI Security and Perception, MITRE
and Chris Ward, Principal AI Researcher, MITRE

With the acceleration of Artificial Intelligence (AI) innovation in recent years, organizations across the public sector have been racing to adopt AI into their products and processes. With respect to National Security, AI adoption offers the potential to automate the operation of valuable assets and provide critical warfighter support across the observe–orient–decide–act (OODA) cycle. As we progress towards integration of AI-enabled mission critical systems, the robustness of these systems must be verified, especially against adversarial exploitation. We present a process for red-teaming AI systems used in real-world decision-making. We consider attacks on target AI systems in the context of the larger concept of operations (CONOPS) and use threat modeling to narrow down likely attack vectors. Next, we share our approach to formulating, implementing, and testing attacks. Finally, we assess the impact of the attack on the mission. Our aim is to codify best practices and capture lessons learned from red teaming exercises as applicable to organizations that want to build an AI Red Team, AI Red Teams that want to methodically examine a target system, and AI practitioners looking for best practices and lessons learned through AI Red Teaming.

3:30 p.m. **“Supercharging Security with Generative AI”**
Spencer Andrus, Customer Engineer, Google Public Sector

Generative AI will empower cyber security defenders as much as attackers. How can specialized, security Large Language Model (LLM), like Sec-PaLM help? Using the latest technology cyber defenders can address threat overload, repetitive tasks and empower their talented workforce.

Google has leveraged its deep history with generative AI and continues to advance the application of this key technology. Generative AI increases efficiency and improves human cognitive ability. These tools are not intended to replace expertise and experience. This presentation will focus on how to use generative AI to effectively integrate this key capability in the Cyber T&E community of practice.

4:00 p.m. **“Auditing ML Collection Hardware”**
Ryan Ashley, Senior Software Engineer, IQT Labs

Increasingly organizations are looking to AI and machine learning to allow them to scale their processes. However, creating these ML systems requires huge quantities of curated, well labelled data. For simple use cases procuring such data can be straightforward, but when the type of data required can only be collected *or labelled with specialized equipment or expertise the challenge of creating a training dataset can demand prohibitive amounts of time and money. One frequently proferred solution to the problem of labelling training data is to use an automated system to collect and algorithmically label data. While this method can reduce the difficulty of creating a dataset, it is not without its own unique risk profile. Recently, IQT Labs, in conjunction with a government partner, conducted an audit of such a system, complicated by the fact that the collection system under audit was a specialized hardware platform. This talk will explain how the audit was performed and significant findings that came out of it. It will begin with an overview of our approach to auditing systems utilizing machine learning. It will also discuss the tools and procedures used in the audit. Finally it will cover the framework used to understand, categorize, and communicate the risks uncovered and how that framework was used to prioritize a remediation plan.*

4:30 p.m. **"Opening the Door to the Mind's Eye: Cognitive Science, Cybersecurity, and Interfaces in ML Testing"**
Timothy Kelley, Scientist, Naval Surface Warfare Center Crane Division

Brain Body Environment Systems Theory in Cognitive Science pulls together ideas of situatedness, embodiment, and dynamical systems to hypothesize a theoretical framework for studying and testing cognitive agents. That underlying structure states that, in order to study a given agent, one must consider the environment that in which it exists, the features and components of its body and how the body interacts with the environment, and how its nervous system, or interpretive engine, interacts with capabilities and weaknesses its body provides. These interfaces are evaluated as a time-dependent feedback loops.

This conceptual framework ends up looking like different aspects of a formal testing program and allows reasoning about Machine Learning testing at different scales. For example, one may wish to develop a test for the entire system, or perhaps just of the underlying interpretive engine. Perhaps one needs to test how an individual component integrates with the whole system (e.g., the effects of sensor changes). Smaller models may be amenable to individual parameter manipulation, while larger models require macro-level evaluations and descriptions.

The brain-body-environment-systems framework meshes well with a cybersecurity mindset for the development of threat models, as they both consider system decomposition as well as the underlying operational environment of a system and potential feasibility and ramifications of manipulations. Looking at the whole system, but also at the various system subdivisions, offers ways to begin to consider testing boundaries interfaces, which is where a Cybersecurity approach and mindset are useful. The interpretive engine interacts with its world and receives its information through its body. It exists on hardware, is implemented in software, and receives data from different sources. The body represents the simplest application of Cybersecurity testing, but also represents a critical aspect of system vulnerability. Failures in database or network security can lead to leaking *the model; hardware and software vulnerabilities can cause behavior to deviate from expectations.*

Just as compromising aspects of the system's body creates vulnerabilities, manipulation of the environment also creates potential risks. Adversarial signals represent a form of this type of attack. Adversarial testing looks at weaknesses between the sensors (body) as they take information from the environment and deliver them to the interpretation engine. Data poisoning is another attack on the interaction between data collected by sensors and the interpretive engine with a goal to predispose the engine to misbehave in the presence of certain cases/classes of cases.

Thursday, August 31, 2023, 1:00 – 3:30

Session 5 **New Cyber DoD Manual and DoD 5000.89 Cyber Policy Brief and Cyber in DEVSECOPS**

Chair Tom Walrond, Office of the Director, Operational Test and Evaluation, Office of the Secretary of Defense

1:00 p.m. **"U.S. Department of Defense (DoD) Joint Cyber T&E Policy and Guidance—What's New?**"

Nilo Thomas, Software & Cyber Advisor to Deputy Director for Strategic Initiatives, Policy and Emerging Technologies, Office of the Director, Operational Test and Evaluation, Office of the Secretary of Defense

Cyber T&E policy and guidance are being modernized to keep pace with the U.S. DoD acquisition objectives stated in DoDI 5000.01:

1. *Simplify Acquisition Policy*
2. *Tailor Acquisition Approaches*
3. *Empower Program Managers*
4. *Conduct Data-Driven Analysis*
5. *Actively Manage Risk*
6. *Emphasize Sustainment*

This presentation will provide a brief introduction to the DoD's iterative cyber T&E approach superseding the six phases. We will cover the following topics:

- *Iterative Cyber T&E Methodology*
- *Cyber T&E Strategy and the Integrated Decision Support Key (IDSK)*
- *Activities for Scoping Iterative Cyber T&E:*
  - *Cyber Requirements, Mission-Based Cyber Risk Assessments, Threat Characterization, Attack Surface Characterization, and Using Cyber T&E Security Verification, Cooperative, and Adversarial Testing*

2:00 p.m. **"Cybersecurity in DevSecOps—How to Test for Security in a Fast-Paced Development Environment"**

Tim Chase & Pat Quilter, STAT COE/ALPI

The Scientific Test and Analysis Techniques Center of Excellence (STAT COE), sponsored by the Office of the Director, Operational Test and Evaluation (DOT&E), has developed a whitepaper on implementing Cybersecurity in DevSecOps and ensuring alignment with best practices. While DevSecOps offers numerous advantages, it also introduces new complexities related to integrating Cybersecurity into software-development processes which further necessitate the understanding of how to test for security in a fast-paced development environment.

This paper describes security testing inside DevSecOps and demonstrates the different types of testing performed, who should perform them, and metrics used to demonstrate success. As DevOps has continued to increase in usage, security *testing needed to adapt to the new development model. To accommodate that, a process called DevSecOps was introduced. When integrating security testing into DevSecOps, there are many types of testing included. Each type of testing integrates into DevSecOps differently and the responsibilities of testing change depending on the goals.*

A software factory typically powers the DevSecOps process. The factory contains the systems and software necessary to deploy and manage the system under test. The security of the software factory needs to be tested as well. By testing the software factory, it helps ensure the integrity of the system under test.

Thursday, August 31, 2023, 1:00 – 3:30

Session 6 **Test Automation and AI**
Chair Mickey Rhodes, Cyber Test Engineer, Booz Allen Hamilton

1:00 p.m. **“Incorporating Chaos Experiments into Automated Pipelines”**
Jenn Bergstrom, CTO, Mission Solutions Sector, Parsons

Chaos Engineering was designed to be run in production environments. However, sometimes customers or clients cannot risk operational disruption caused by a chaos experiment gone wrong in production. Does that mean chaos engineering cannot be incorporated in those systems? No! This session presents guidelines and strategies for implementing chaos experiments into automated dev and test/staging pipelines to build confidence in the production system’s ability to withstand unplanned events in operations.

1:30 p.m. **“Using Graph-Based Machine Learning Algorithms for Software Analysis”**
Michael D. Brown, Principal Security Researcher, Trail of Bits, Inc.

Software analysis is a well-established research area focused on automatically determining facts about a program’s properties and behaviors and using them to improve the program. Software analysis techniques are used in many domains, most notably to achieve performance and security enhancements (compilers), identify bugs and security vulnerabilities (code scanners), simplify programming through abstraction (DSL interpreters), and reverse engineer software. The limitations of software analysis for these purposes are well understood – in general it is impossible to collect a complete set of program facts about a particular piece of software, especially for complex software used in the DoD. As a result, many software analysis tools employ heuristics or rely on humans in the loop to make meaningful advances in the space.

The recent technological leaps forward in Machine Learning (ML) have created a unique opportunity to make advances in software analysis that were previously not possible because ML-based solutions are not bounded by the same computational constraints as traditional software analysis techniques. Further, these techniques excel at approximating and replicating human problem solving. As a result, there has been a dearth of new research on ML-based software analysis, however recently proposed techniques have fallen flat because they failed to exploit the natural shape and form of software: directed graphs.

Over the last three years, my team and I have researched and developed techniques to address several key challenges that researchers face when creating effective, graph-based ML software analysis tools. Specifically, we have developed techniques to aid researchers in generating realistic training data sets, converting software to a representation that graph-based ML algorithms can consume, and formulating real-world software analysis problems as graph recognition problems. Using these techniques, we have created two tools that outperform state of the art traditional software analysis tools: VulChecker and CORBIN. Vulchecker is a *static application security testing (SAST) tool that excels at identifying fuzzy security vulnerabilities in source code. CORBIN is a system for lifting advanced mathematical constructs (formulas, lookup tables, PID controllers, etc.) from legacy binary software that powers cyber-physical systems like power generation and onboard vehicular control systems.*

In this technical track session, I will first discuss the inherent challenges in using ML to create software analysis tools and how exploiting the graph-based nature of software can bring about success. Second, I will present two successful graph-based ML software analysis tools created under the DARPA AIMEE and ReMath programs: VulChecker and CORBIN. Finally, I will present a set of guiding principles and guardrails for applying ML to software based on the lessons learned from building these tools.

2:00 p.m. **"Humans vs. Robots: Structuring Mission Based Cyber Risk Assessment (MBCRA) Inputs"**
William D. Bryant, Technical Fellow, MTSI

Part of the ongoing debate on the best way to do Mission Based Cyber Risk Assessment (MBCRA) is whether human subject matter experts, or an automated process such as a risk algorithm should be used to generate the inputs into the risk assessment process.

There are strong reasons to distrust the accuracy and precision of human experts in assessing probabilities given the evidence of decades of research. However, typical automated methodologies may not apply well to platform cybersecurity and may have human assessment hidden within the apparently impartial algorithm. While the research is clear that even improper linear models typically outperform human experts, the necessary pre-requisites of quantifiable inputs, unambiguous results, feedback, and repetition do not exist in the platform cybersecurity arena. Humans are inconsistent, adaptable, biased, and slow, but can think and integrate multiple complex and changing data streams. Thus, humans are preferred as the integration point, although they should incorporate as much risk algorithm data as they can as risk algorithms will find things humans will miss.

Uncertainty comes from two sources, epistemic, based on a lack of knowledge, and aleatory, due to random variation. Both sources are present in our typical formulation of risk but are often conflated. Despite the difficulty in determining an accurate likelihood for risk scenarios, likelihood should still be considered or we will likely mis-prioritize our resources.

Accuracy refers to how close a subject is able to get to a desired mark with precision referring to the variation between shots. Human accuracy in risk scoring can be improved with better analysis, improved knowledge, and reducing biases. Human precision can be improved with better calibration, categorization, and utilizing methods that capture uncertainty.

A structured elicitation process can help minimize the known issues with human subject matter experts and different levels of structure, complexity, and difficulty can be utilized depending on how accurate an assessment is the goal.

While humans have many issues, they remain the best option to integrate the complex data flows to provide a reasonably accurate and precise indication of platform cybersecurity risk.

2:30 p.m. **"Proactive Threat Hunting - Getting Left of Boom"**
Matt Lembright - Director of Federal Applications, Censys

This past year, Censys uncovered a Russian ransomware group within its data by identifying suspicious hosts and leveraging historical analysis and technical pivots. The journey began with open source hacking tools and ended with ransomware packages, a removed IOC, and two Bitcoin hosts for payment. Matt Lembright will demonstrate how investigators don't have to wait for the enemy to be knocking on the door to find them in the wild.

For reference, this is a version of the talk presented to Forrester. https://www.youtube.com/watch?v=M3FENy9zi34

Thursday, August 31, 2023, 1:00 – 3:30

Session 7 **Tomorrow's Cyber Solutions…. Today**
Chair Dr. Peter A. Beling, Director, Intelligent Systems Division, Virginia Tech National Security Institute

1:00 p.m. **“Cyber Table Top Toolset (CT3) Demonstration” [CUI: Distribution C]**
Nisha Patel, Software Engineer, Trideum Corporation

Abstract not releasable.

1:30 p.m. **“Risks and Opportunities for AI in Managing Disruptions to Hardware Supply Chains”**
Zach Collier, Assistant Professor, Department of Management, Radford University

The global supply chain for electronics has been subjected to numerous stressors over recent years, including the pandemic, droughts, and global instability. Chip shortages hampered production of many consumer goods such as vehicles and household appliances and caused schedule delays and lost revenue for many organizations. Building a resilient supply chain, where the flow of components within it are trustworthy and secure, is imperative to the global economy. Recent advances in AI technology are poised to augment risk management for the supply chain but may also introduce unique challenges to it. This presentation describes research efforts related to modeling the risks of disruption and proposes avenues for future AI-enabled research that can aid in the testing and evaluation of components and strengthening of the supply chain.

2:00 p.m. **“Physically Unclonable Functions (PUFs) Using Protein-Self-Assembly and Deep Neural Networks”**
Stephen Adams, Assistant Director, Intelligent Systems Division, Virginia Tech National Security Institute

Counterfeiting is an increasingly pervasive problem that impacts both the private and public sector. Physically unclonable functions (PUFs) are physical devices with unique and random features that can be used to validate the authenticity of a product. PUFs have been created using a wide range of techniques but many of the established methods require sophisticated methods and specialized tools. This talk will outline our work utilizing protein-self-assembly as the randomness generator for a PUF image that can be easily printed on a biodegradable and flexible silk-fibroin label and affixed to an object. This work also explores the feasibility of using deep neural networks as a component of the cryptographic key generation process. The randomness of the cryptographic keys has been evaluated using the NIST SP 800-22 Statistical Test Suite. This talk will conclude with a brief summary of our current and future work focused on developing an application for scanning and verifying the PUF image using a mobile device.

2:30 p.m. **“Cyber Risk Scoring and Mitigation for Resilient Cyber Infrastructure”**
Dr. Sachin Shetty, ODU

Security metrics play a key role in supporting cyber risk management and mitigation decisions for critical infrastructures. The availability of quantitative insights ensures operational resilience and assists in the development of cost-effective mitigation plan. The resilient operation of critical infrastructures will depend on tools that can aid in continuous cyber resilience assessment. In this talk, he will present theoretical techniques and tools for security risk scoring and prioritized cyber defense remediation plan for effective cyber risk management. He will present cyber risk scoring techniques based on attack and vulnerability graph modeling and cyber defense remediation technique based on optimal resource allocation modeling. He will also present the Cyber Risk Scoring and Mitigation (CRISM) tool that provides cyber risk scores and a prioritized mitigation plan based on vulnerability detection, attack graph modeling, and risk assessment. A demonstration of the CRISM tool will conclude the talk.

Thursday, August 31, 2023, 1:00 – 3:30

Session 8 **Cyber Automated Tools & Test**
Chair Eugene Costello, Cybersecurity Director, OPTEVFOR

1:00 p.m. **“AFRL ITEC Pen Test Capability Brief”** **[CUI: Distribution C]**
Josh Young, AFRL ITEC Pen Test Lead, Booz Allen Hamilton

Penetration testing, or pen testing, is a crucial practice for government and military clients seeking to strengthen their cybersecurity defenses. One of the main benefits for performing pen test assessments is to meet regulatory compliance requirements, covered by NIST, AFI, and DoDI regulations.

NIST SP 800-115 provides a comprehensive framework for pen testing, enabling government and military clients to identify vulnerabilities and assess risks in their systems, networks, and applications. AFI 17-130 recognizes the importance of pen testing in safeguarding military infrastructure, while DoDI 8501.01 establishes requirements for cybersecurity risk management. Pen testing, aligned with these guidelines, enhances clients' cyber resilience, ensures compliance, and supports mission-critical operations.

Penetration testing offers significant benefits for government and military clients in enhancing their cybersecurity defenses. Firstly, pen testing provides an objective and independent assessment of their systems, networks, and applications, helping to identify vulnerabilities that adversaries could exploit. By uncovering these weaknesses through simulated attacks, pen testing enables clients to take proactive measures to address them before real-world incidents occur. Secondly, pen testing allows for targeted remediation efforts by assessing risks based on the impact and likelihood of exploitation. This approach helps clients allocate their limited resources effectively, focusing on critical vulnerabilities that pose significant threats to national security and sensitive information. Additionally, regular pen testing fosters a proactive cybersecurity culture within organizations, promoting awareness and best practices among personnel. This, in turn, strengthens the overall cybersecurity resilience and readiness of government and military clients to combat evolving cyber threats.

1:30 p.m. **“## Wave Function Collapse Algorithm for Automatic Design of Secure Networks”**
Grant Willey, Information Systems Security Officer, Geeks and Nerds (GaN) Corporation

The Wave Function Collapse (WFC) algorithm takes inspiration from the quantum mechanics where different potential outcomes are defined by a probability function. In any physical system, the outcome depends on various independent factors that define the system, and only when all the states are known/collapse, the outcome can be determined. The Wave Function Collapse algorithm has been used in the realms of image generative art and game design to create complex *maps and textures based on a small sample. The concept is to allow each cell to have many possibilities. Starting with all possible elements/undefined state, by imposing rules/constraints, the cells can collapse into a single assembled form. The collapsing algorithm is based on the rule set, but it is possible to generate contradictory states, and number of iterations may be required to generate a final form that meets all the rules/constraints. The collapsing rule set for image generation is dependent on the neighboring cells, but can be adapted to more abstract structures. This paper examines the potential of adapting this algorithm to build out a novel secure network topology. This network could be software defined or dynamically stood up in a virtual environment such as Graphical Network Simulator-3 (GNS3) to run penetration tests and other validations before being deployed. The rulesets can be as simple or complex to allow for topology flexibility, and can be expanded to affect physical positioning, such as separation requirements for TEMPEST. With flexibility of rule sets and wave function collapsing algorithms, tracking an aggregate risk score is possible along with other metrics. This approach presents a potential for greatly improving time, effort and effectiveness of designing a new LAN or enterprise network.*

2:00 p.m. **"Cybersecurity and the Rise of AI: Risks and Opportunities"**
Jason Schalow, Chief, Special Missions Flight, 412th, Communications Squadron, Edwards AFB

Over just the last year, the state-of-the-art for Artificial Intelligence has developed exponentially, with capabilities such as ChatGPT and Stable Diffusion capturing the media spotlight and open-source communities such as Huggingface and Kaggle making these technologies more accessible than ever. This presentation will discuss the cybersecurity risks and opportunities of these technologies as they apply to Test and Evaluation, with the goal of posturing both cyber defense and T&E professionals to operate securely in an AI-enabled environment. Discussion will include applications of AI as a defense tool, as well examining security relevant aspects of these technologies and the open-source ecosystem that is quickly growing around them.

2:30 p.m. **"Building Automation System (BAS) An Industrial Control System Focused Security"**
Dan Turner, Booz Allen Hamilton

The importance of securing Industrial Control Systems (ICS) and Defense Critical Infrastructure (DCI) is increasing with more systems being connected to the internet in our hyper connected world. Typically for Supervisory Control and Data Acquisition (SCADA) and remote programming/control, the threat of malicious actors or software penetrating and disrupting these systems is at an all-time high. To better understand our ICS/DCI challenges, Booz Allen has designed and built several ICS/DCI demo systems. The Building Automation System (BAS) is a demo that represents the automated systems typically found in commercial buildings; Physical Security, Fire Detection/Suppression System, and Heating Ventilation and Air Conditioning (HVAC) System.

To accurately model these systems as they are used in the real-world, the BAS only includes commercially available hardware and software components. For Physical Security, the BAS has a Human Machine Interface (HMI), RFID card reader, magnetic door lock, push-to-exit button, and access control software. The fire system includes a smoke detector, alert strobe/horn, and a fire-pull station. Lastly, the HVAC system is comprised of HMI vent fans, damper actuator (for opening/closing vents), a simulated boiler, and a simulated chiller. All these systems are connected to and controlled by a Programmable Logic Controller (PLC), which is connected via ethernet to a network.

With the pervasiveness of networked ICS/DCI systems controlling critical processes such as power generation, water distribution and wastewater treatment, the lack of built-in cybersecurity presents a challenge for those who are responsible for securing these systems. The BAS acts as a mobile lab and provides the ability to demonstrate security vulnerabilities and to showcase security tools that can help protect these systems, all while allowing users to physically interact with the equipment and see first-hand the impact attacks have on control systems.