Trusted Computing Center of Excellence
2022 Summit Speaker Bios

1. **Kathleen Fisher** – Feb 1 Keynote

Bio: Dr. Kathleen Fisher assumed the role of deputy office director for DARPA's Information Innovation Office (I2O) in October 2021. Fisher joins DARPA from Tufts University, where she is an adjunct professor in the Department of Computer Science, and served as department chair. Fisher previously served as a program manager in I2O where she created High-Assurance Cyber Military Systems (HACMS) and Probabilistic Programming for Advancing Machine Learning (PPAML). Earlier in her career, she was a principal member of the technical staff at AT&T Labs Research. Dr. Fisher is an ACM fellow and received her PhD in computer science from Stanford University.

2. **Gabriela Ciocarlie / Matthew Jablonski / Duminda Wijesekera** – CADA: CyManII Attack-Defense Annex

Bio: Duminda Wijesekera is the acting chair of the newly formed Cyber Security Engineering Department and a professor in the Department of Computer Science at George Mason University, Fairfax, Virginia and a visiting research scientist at the National Institute of Standards and Technology (NIST). He leads the Laboratory of Radio and RADAR Engineering (RARE) at Mason and currently supports the CCI Nova node director with the CCI Innovation Laboratory at Arlington and Secure Manufacturing Automation (SMA) in the DoE funded CyManII project. His research area includes safety and security of networked control systems in general (and Intelligent Transportation Systems (ITS) and Industrial Automation Systems in particular), Next G based Edge services.

Bio: Mr. Matthew Jablonski is a Ph.D. candidate in Information Technology. He is a graduate research assistant with the CCI Innovation Laboratory at George Mason University, and a security researcher at the Cybersecurity Manufacturing Innovation Institute (CyManII). His research interests include safety and security risk management within cyber physical systems. He received an M.S. in Information Security and Assurance.

Bio: Gabriela F. Ciocarlie is an associate professor in the Department of Electrical and Computer Engineering at The University of Texas at San Antonio and Vice President for Securing Automation and Secure Manufacturing Architecture for CyManII. Her expertise is in anomaly detection, distributed alert correlation, network and application-level security, cyber physical systems security and distributed system security. Before UTSA, Gabriela was the Chief Product Officer at Elpha Secure and a senior technical manager of SRI's New York City research hub focused on cyberanalytics, which she established

in 2016. Gabriela holds a Ph.D. and an M.S. in computer science from Columbia University, and a B.Eng. in computer engineering from Polytechnic University of Bucharest.

Abstract: In this talk, we present how formalized models and methods developed by CyManII are intended to evaluate the progress of both safety and security aspects of a manufacturing system, and the system's resiliency to withstand threats arising of exploiting both. We use Architectural Analysis and Design Language (AADL) to specify requirements from established safety and security standards, along with timing requirements and other security properties, and verify them within an AADL model. To enable adoption and transferability, we build these concepts into a CyManII Attack-Defense Annex (CADA), intended to show attacker and defender behaviors within a manufacturing system.

3. **Thomas Barnett** - Secure Architecture for Army Mission Critical Systems

Bio: Tom Barnett is a member of the Combat Capabilities Development Command (DEVCOM) Aviation and Missile Center (AvMC) Cyber Technologies Division and currently serves as the Cyber Engineering and Integration Lead for PEO Aviation. Mr. Barnett served as the first Cyber Technology Area Lead (TAL) where he established the Cyber Technology Area within the overall Missile Science and Technology (S&T) portfolio. Mr. Barnett has 34 years of systems engineering experience in the areas of cyber resiliency, system of systems hardware in the loop (HWIL) and all-digital constructive simulations, radar and infrared sensors, integrated air and missile defense and short-range air defense.

Abstract: The U.S. Army DEVCOM Aviation and Missile Center (AvMC) a leader in developing technologies to increase weapon system survivability through cyber resilience. The AvMC utilizes RDT&E funds from program offices, the Army Science & Technology (S&T) portfolio and the Army SBIR program to drive development and integration of these technologies. While we utilize cyber security techniques to address common vulnerabilities, we must rethink the fundamental computational architectures and business models used to build our mission critical systems. There is a need for an agile, secure and highly assured mission computer with adaptive defense techniques to minimize the system’s exposure to battlefield cyber threats and accomplish mission objectives.

To that end, the AvMC has sponsored an SBIR program under which Trusted Science and Technology Inc. (Trusted ST) has ported the DoD seL4-based secure kernel into a RISC-V instruction set architecture (ISA) and COTS platform. The Trusted ST team successfully completed an initial secure kernel porting on a PolarFire SoC Icicle Kit for a feasibility and proof-of-concept demonstration in SBIR Phase I. This presentation will provide porting approaches and plan to fully port the secure kernel and release the code base to DoD agencies and performers.

4. **Dariusz Mikulski** – Feb 2 Panel Expert

Bio: Dariusz Mikulski, Ph.D. is a Lead Research Scientist for Ground Vehicle Robotics (GVR) in the US Army DEVCOM Ground Vehicle Systems Center (GVSC), where he is dedicated to improving cybersecurity, artificial intelligence (AI), and cooperative teaming in autonomous self-driving vehicles and robotics systems. He leads GVR’s Hybrid Autonomy & Cybersecurity Research (HACR) Laboratory to study and solve issues at the intersection of vehicle autonomy and cybersecurity; and is currently serving as both the Technical Manager for the Cybersecurity for Robotic & Autonomous Systems Hardening (CRASH) Joint Capability Technology Demonstrator (JCTD) and a Thrust-Area Lead for the DARPA Assured Autonomy program. Dr. Mikulski is known in his research circles for pioneering the

novel concept of trust-based vehicle control, based on his PhD research and invention of the RoboTrust algorithm. In 2021, he was awarded the Civilian Service Commendation Medal from the Secretary of the Army for exemplary service and excellence for his work in cybersecurity for the Army. Dr. Mikulski earned his Ph.D. in Electrical and Computer Engineering (2013) at Oakland University in Michigan. He also earned his BSE in Computer Science (2003) from the University of Michigan (Ann Arbor) and Masters in Computer Science and Engineering (2006) from Oakland University.

5. **Peter Sewell** - Verified Security Properties and Semantics-Assisted Engineering

Bio: Peter Sewell is a Professor of Computer Science at the University of Cambridge. His research builds mathematically rigorous foundations for the engineering of real-world computer systems, to make them better-understood, more robust, and more secure - focusing especially on semantics and reasoning for relaxed-memory concurrency, architecture specifications, C, and CHERI.

Abstract: Memory safety bugs continue to be a major source of security vulnerabilities in our critical infrastructure. The CHERI project has proposed extending conventional architectures with hardware-supported _capabilities_ to enable fine-grained memory protection and scalable compartmentalisation, allowing historically memory-unsafe C and C++ to be adapted to deterministically mitigate large classes of vulnerabilities, while requiring only minor changes to existing system software sources. ARM is currently designing and building Morello, a CHERI-enabled prototype architecture, processor, SoC, and board, extending the high-performance Neoverse N1, to enable industrial evaluation of CHERI and pave the way for potential mass-market adoption. However, for such a major new security-oriented architecture feature, it is important to establish high confidence that it does provide the intended protections, and that cannot be done with conventional engineering techniques.

This talk will describe work to put the Morello architecture on a solid mathematical footing from the outset. We define the fundamental security property that Morello aims to provide, reachable capability monotonicity, and prove that the architecture definition satisfies it. This proof is mechanised in Isabelle/HOL, and applies to a translation of the official Arm Morello specification into Isabelle. The main challenge is handling the complexity and scale of a production architecture: 62,000 lines of specification, translated to 210,000 lines of Isabelle. We do so by factoring the proof via a narrow abstraction capturing essential properties of arbitrary CHERI ISAs, expressed above a monadic intra-instruction semantics. We also develop a model-based test generator, which generates instruction-sequence tests that give good specification coverage, used in early testing of the Morello implementation and in Morello QEMU development. We also use ARM's internal test suite to validate our model. This gives us machine-checked mathematical proofs of whole-ISA security properties of a full-scale industry architecture, at design-time. To the best of our knowledge, this is the first demonstration that that is feasible, and it significantly increases confidence in Morello.

6. **Sean Peisert, Venkatesh Akella** - Edge-to-Center Data Enclaves for Scientific Computing

Bio: Dr. Venkatesh Akella is a Professor of Electrical & Computer Engineering at University of California, Davis and a Faculty Affiliate in the Computational Research Division at Lawrence Berkeley National Laboratory. He received his Ph.D. in Computer Science from University of Utah and a MS from Indian Institute of Science. His current research interests are computer architecture, systems for machine learning, and cyber-physical systems with emphasis on memory, data privacy, and security. He received an NSF CAREER Award and is a Senior Member of the ACM.

Bio: Dr. Sean Peisert leads computer security research and development at Lawrence Berkeley National Laboratory and is a full adjunct professor of Computer Science at the University of California, Davis and of Health Informatics at the University of California, Davis School of Medicine. He is also editor-in-chief of IEEE Security & Privacy; a member of the Distinguished Expert Review Panel for the NSA Annual Best Scientific Cybersecurity Paper Competition; and a member of the DARPA Information Science and Technology (ISAT) Study Group. He received his Ph.D., Masters, and Bachelor's degrees in Computer Science from UC San Diego.

Abstract: Trusted Execution Environments (TEEs) or secure enclaves are gaining traction as a hardware enforced mechanism for protecting data while in use or during computation in the cloud computing environment. Our prior work has shown that TEEs -- especially AMD's SEV -- are a promising avenue for meeting the unique security requirements for secure HPC as well, though there are some significant challenges in terms of extending the boundaries of enclaves to multiple (heterogeneous) nodes, including accelerators such as GPUs and FPGAs, reducing the performance overheads of crossing security domains and key management/attestation protocols, and mapping user workflows, such as those in high-performance computing, to computing platforms with TEEs. Existing approaches have numerous drawbacks: they are proprietary, have significant performance penalties, burden the programmer with partitioning an application into secure/unsecure parts, have extremely large trusted computing bases, and do not support low-latency, secure multi-node computing or heterogeneous architectures. We are developing new architectures that overcome these limitations for data-centric workflows to address the specific power, performance, and usability, and needs from the edge to the HPC center.

7. **Nicholas Evancich** - ARES Secure Kernel on ZCU102

Bio: Mr. Nicholas Evancich is currently a Chief Engineer at Trusted Science and Technology. Before he established the Trusted ST, Mr. Evancich was a Program Manager and served as PI and technical lead on numerous R&D projects including AFRL ARES BAA, OSD RAUSO BAA, DARPA seL4 Center of Excellence, and ONR/DHS cyber security programs. Mr. Evancich worked as a principal engineer designing exploits at Fort Meade, where he developed technical exploits via reverse engineering and data-based exploits. He built a correlation engine for the Navy TSw Enterprise Network Management System (ENMS), which included an Ozone Widget Framework visualizer. Mr. Evancich was a Systems Engineering and Technical Assistance (SETA) at DARPA supporting Tactical Ground Reporting System (TIGR) and Transformative Applications (TA). While working at DARPA, he helped design search optimization improvements to TIGR and aided in the deployment of a major upgrade to TIGR. He wrote several of the canonical example apps for the TAs project and worked on the design and implementation of the security version of 'droid. Prior to his DARPA work, Mr. Evancich was the chief engineer for the Biometrics Automated Toolset (BAT) program (the Army's large scale biometric collection project).

Abstract: The ARES Secure Kernel (ASK) on a ZCU102 tutorial focuses on showing how to deploy ASK on a Xilinx ZCU102 development board. This includes an overview of ASK features, compiling and building ASK, getting the ASK image on an SD card, required alteration to u-boot, overview of the needed hardware changes, and finally botting the image on the ZCU102.

8. **John Shackleton** (Adventium Labs) - Temporal Isolation with MCS

Bio: Mr. Shackleton is a Senior Principal Research Scientist with over 25 years of engineering experience, specializing in real-time embedded systems, model-based engineering, and cybersecurity. He is currently leading the Adventium effort on the DARPA Cyber Assured System Engineering (CASE) program, subcontracted to Collins Aerospace, to develop an automated AADL-based software build environment that targets seL4. He is lead developer for several AADL-based analysis tools, including temporal analysis, separation analysis, and change analysis. He developed prototype demonstrations to investigate Authoritative Single Source of Truth requirements and tool capabilities. Other technical areas of interest include time-critical systems, dynamic resource management, safety-critical systems, and cyber forensics.

Abstract: The prototype Temporal Isolation CASE Scheduler (TICS) runs on seL4 mixed-criticality systems (MCS). TICS provides strong temporal isolation for an MCS execution environment, with several advantages over the stock seL4 domain scheduler. For example, TICS supports multiple schedules, such as an initialization schedule and a run-time schedule. This allows TICS to provide strong temporal isolation, meet hard real-time guarantees, and also accommodate the significant overhead of starting up Linux Virtual Machines during initialization, then switching to an efficient run-time schedule. Since TICS runs in userland, it does not negatively impact existing seL4 proofs.

TICS currently enforces a static cyclic schedule upon the other application components, analogous to the behavior of the domain scheduler provided by stock seL4. In the future, TICS could be expanded to implement dynamic scheduling models. TICS integrates with, although does not require, CAmkES. CAmkES provides a flexible component-based abstraction for specifying seL4-based systems.

9. **Renato Levy** - I see the ECO, But Where is the System?

Abstract: So much has been talked about the seL4 eco-system, but after all these years the level of support for multiple required devices at seL4 is still very low. Most embedded systems are forced to run Linux on top of seL4 to have device access. In this presentation, we will talk about an architecture to provide native support for sought of devices direct at seL4, as well as, allow Java and C# programs to run on native environment

10. **Noah Evans** - Trusted Systems Research at Sandia

Bio: Noah Evans is the technical lead for Hardware Verification for the Digital Foundations and Math at Sandia. He comes from a system and HPC background.

Abstract: As the nation's stockpile modernizes, trust and assurance must be guaranteed in ever shorter schedules. This presentation describes ongoing verification work at Sandia in the Digital Foundations and Math department, in particular, our work verifying mission software and hardware and integrating formal approaches into Sandia's Systems and Digital engineering workflows.

11. **Fabrizio Bertocci** – Jan 31 Tutorial

Bio: Fabrizio leads the development of seL4-based research at RTI. Real-Time Innovations (RTI) is the largest software framework provider for smart machines and real-world systems. Our software is running in over 1,000 critical systems world-wide spanning defense, autonomous & electric vehicles, health, robotics, and energy systems.

Abstract: In this presentation we will dig into the technical design of a modular, resilient and secure prototype built on RTI Connext DDS and seL4. The architecture incorporates both the use of virtual machines and userland execution to provide execution isolation and high assurance. We utilize two variants of RTI Connext - our full pro version (in the VMs) and our DO178C DAL-A (in userland). We will discuss the design and performance in detail. We offer free research licenses to RTI Connext Micro which can be run in seL4 v12, and CAmkES/TrentOS.

12. **Eric Smith** - Correct-By-Construction Generation of C code for seL4 Networking

Bio: Dr. Eric W. Smith is the CEO of Kestrel Institute and works as a formal methods researcher at Kestrel Technology. He is the developer of the Axe toolkit for software verification, and he co-leads Kestrel's APT (Automated Program Transformations) project, which is developing proof-emitting program transformations in the ACL2 theorem prover. APT has been used in several Kestrel projects, and Dr. Smith is currently using it to synthesize verified networking code for seL4. Before joining Kestrel, Dr. Smith completed his Ph.D. in Computer Science at Stanford University under Professor David Dill.

Abstract: Kestrel Institute is currently extending its APT toolkit (kestrel.edu/apt) with a correct-by-construction C generator (kestrel.edu/atc). The talk will discuss this tool, created by Alessandro Coglio, and show examples of verified C code that it generates, including proofs checked by the ACL2 theorem prover. In parallel, Kestrel personnel have been creating APT transformations that help put ACL2 functions into a form suitable for input to the C generator. These also produce proofs. I will discuss this work in the context of our project to generate a correct-by-construction TCP/IP network stack for seL4.

13. **Hui Lu** - Achieving Both Security of VMs and Speed of Containers in Cloud Native?

Bio: Hui Lu is an assistant professor from State University of New York at Binghamton. His research focuses on developing key virtualization techniques to empower state-of-the-art cloud infrastructure. Particularly motivated by his current research observations that critical challenges commonly exist in virtualization techniques in light of container-enabled technologies and the emerging cloud-native paradigm, Hui Lu seeks to enable secured, lightweight virtualization techniques for elastic cloud-native applications.

Abstract: Existing virtualized cloud systems have been long built upon software/hardware stacks with rigid boundaries. While being able to support traditional, monolithic applications running smoothly in cloud, it unfortunately creates barriers to meeting the stringent needs of emerging cloud-native applications, each requiring running in an extremely lightweight yet strongly isolated virtualized environment, while maintaining high elasticity. Recent effort seeks to answer this question with various sandboxing approaches, e.g., micro-VMs, unikernels, and kernel-extended containers. A common goal of these approaches is to retain a guest kernel (thus reusing its functionality), but to make it small, fast, and easy to administer at large scale. However, they share some common drawbacks: It remains inefficient to have one guest kernel (though minimized) to host each tiny, short-lived component. Further, different hosting components may access distinct portions of the guest kernel; hence, a “one-size-fit-all” optimized guest kernel might not apply. Third and most importantly, since guest kernels have been greatly minimized and/or deteriorated to only provide the needed subroutines for hosting applications to function (i.e., unikernels), existing approaches purely rely on hypervisors for isolation. But, even with all the precautions, hypervisors do have their share of vulnerabilities and/or bugs those attackers can exploit. This presentation will scrutinize these boundaries with a particular focus on

isolation, performance, and elasticity, identify key gaps, and develop new fitting virtualization techniques and system abstractions to bridge these gaps.

14. **Jason Sebranek** - Building a Commercial Virtualized Mobile Device with seL4

Bio: Mr. Sebranek started his cybersecurity career in 2002 with Northrop Grumman as a Software Engineer. Over his career he grew into many roles, including Section Manager, Lead Software Engineer, R&D Principal Investigator, Cyber Architect, and Technical Fellow. In his R&D role, Mr. Sebranek led the Trusted Mobility team exploring cybersecurity for mobile platforms.

Mr. Sebranek began his career at Cog Systems, Inc. as the Director of Technical Marketing, reporting directly to the Chief Marketing Office and CEO. In 2019 Mr. Sebranek became the Chief Technology Officer, with responsibilities including product and technology planning/roadmap, cybersecurity architecture, and industry partnerships.

Abstract: Cog Systems, Inc. specializes in developing secure solutions leveraging virtualization on connected mobile devices. Cog Systems has developed a Virtualized Mobile Device (VMD) architecture and has placed the seL4 microkernel and VMM the heart.

In 2017 Cog Systems developed a single domain virtualized device on an HTC One A9 smartphone, and successfully validated it against the relevant National Information Assurance Partnership (NIAP) Protection Profiles, allowing for its use in Commercial Solutions for Classified (CSfC) solutions. Cog Systems has leveraged our VMD to develop a next-gen commercial virtualized smartphone - again bound for NIAP/CSfC, and availability commercially to the US government by January 2022.

Our presentation serves as a case study of a lengthy and challenging project to apply seL4 to a product commercialization effort. Cog Systems will share some of the technical challenges we encountered while working with chipset and mobile device vendors and will address tradeoffs made with regards to formal verification.

Cog Systems believes that this presentation is of interest to the TCCOE as well as to the seL4 community at large. It describes our work to expand the seL4 user base and spurs a conversation around commercial application of the technology in a government-grade security context.

15. **Olivier Engelkes** - From Slideware to Hardware

Bio: Olivier Engelkes is HENSOLDT Cybers Head of Engineering. With a background in Computer Science, he carried out engineering projects for the road, the air, for tracks and for space. He is focused on safety and security critical embedded systems with hard real time constraints - from the initial design ideas up to the fully certified commissioning.

His objective at HENSOLDT Cyber is to employ seL4 and RISC-V based technologies to answer the challenge of ever more stringent industrial requirements on safety and security for cutting edge applications.

Abstract: Today's approach on security in most industrial fields is to airgap everything from hostile environments such as the internet. While the isolation of embedded equipment might provide some form of security, it degrades capabilities in normal operations, and becomes problematic as soon as

maintenance is needed – then, whatever reduces downtime becomes acceptable and leaves the door wide open for attacks.

HENSOLDT Cyber takes a different approach: using guarantees from formally validated technologies such as seL4 based TRENTOS and the RISC-V based MiG-V Microprocessor, HENSOLDT Cyber provides secured pathways to access safety and security critical embedded equipment in the field – all over the world.

From Slideware to Hardware tells what it takes to bring seL4 based technologies to real world applications and shows their impact and advantages for the people using them.

16. **Sebastian Eckl, Axel Heider** - Porting seL4 to Secure (RISC-V) Hardware

Bio: Sebastian Eckl joined HENSOLDT Cyber's TRENTOS development team as a Senior Software Engineer in 2020. Prior to that, he worked as a Research Associate at the Technical University of Munich (TUM), where he focused on teaching L4 microkernel based operating systems for several years. At the Chair of Operating Systems of the Technical University of Munich (led by Prof. Baumgarten) he is currently working on his doctoral thesis dealing with migration-supported dynamic reconfiguration in distributed embedded real-time systems.

Bio: Axel Heider is an seL4 enthusiast who joined HENSOLDT Cyber to grow the ecosystem and build a high secure system based on a RISC-V SoC. Before that he was building a proprietary L4 based operating system that is deployed as TEE in Arm TrustZone on various commercial systems. He has a degree in computer science from Technical University of Munich (TUM).

Abstract: Providing extensive platform support marks a critical requirement for any operating system environment in order to be widely adopted. Nevertheless, porting even a manageable amount of code to a new platform can be quite a complex and challenging task. We therefore present the experiences made during porting the seL4 microkernel, its dedicated platform support libraries as well as HENSOLDT Cyber's TRENTOS operating system environment on top and provide a guide that helps in identifying the relevant areas for adaptation. Hereby, both a modern ARM-based environment (Raspberry Pi 4) as well as HENSOLDT Cyber's MiG-V (a RISC-V based SoC) are used. We will present the seL4 kernel changes we have made to boot and run seL4 from ROM. We will also present the bootloader design that allows building, loading and running a custom system on the ROM kernel.

17. **Sascha Kegrei** – Feb 2 Panel Expert

Bio: Sascha Kegrei joined HENSOLDT Cyber in 2018 as CTO. He is also a member of the governing board of the seL4 Foundation. His experience is in safety, security and mission critical systems for military aircrafts. During his career he was able to work in areas of technical sales, development, management and operation/support.

18. **Michael Doran** - Accelerating seL4 VMM Development with VM-Composer

Bio: Mr. Doran has been working within the embedded devices space for eight years and specifically within embedded virtualization for the last 3 years. He received my undergraduate degree in computer/electrical engineering, and he is currently working towards my graduate degree in computer/electrical engineering.

Abstract: seL4 VMM development currently proposes a challenge when it comes to configuration management and rapidly prototyping a design in an efficient manner. VM-Composer mitigates setup time by providing a GUI driven environment to setup, configure, and build seL4 VMM projects for target hardware. VM-Composer is a desktop application that allows for a developer to utilize a drag and drop interface in order to configure and build an seL4 VMM project for a specific platform. This is achieved by providing a complete back-end development environment which includes the seL4 source code and tool-chain. The application is an abstraction from the seL4 development tools that is separated into two components. The front end: which is developed using Electron, and JavaScript. The second component is the VM-Composer back-end tool which is developed with Python. Both components are responsible for specifying and building a component architecture, using CAmkES.

19. **Robert N. M. Watson** - From CHERI to Morello: Capability Hardware Enhanced RISC Instructions