# seL4® Summits and TCCOE – An Overview

Dr. Jason Li, Dr. Ray Richards,
Dr. Renato Levy
October 2022

# Agenda

- Previous seL4® Summits
- TCCOE Summit
- Lessons Learned and Way Forward

# Introduction

Security. Performance. Proof.

- seL4® is the first formally verified microkernel
  - Offers fundamental software separation properties
  - Provides new opportunities to build assured computer systems
- Supported by DARPA and AFRL, US DoD researchers have organized the first three seL4® Summits
  - Organic integration of hardware and software security features
  - Measurable security, resilience and assurance

# Past seL4® Summits

- First seL4® Summit
  - Washington DC Area
  - November 14-15, 2018
- Second seL4® Summit
  - Washington DC Area
  - September 23-25, 2019
- Third seL4® Summit
  - Virtual event due to the COVID pandemic
  - November 15-19, 2020

# Structure

- Training
- A daily inspiring keynote
- Invited papers relevant with the summit focus
  - organized in sessions based on common aspects
  - 3-5 papers in each session to allow enough time for discussion and networking
- A social networking mingle at the end of the first day
- An industry/government panel at the end of the second day

# First seL4® Summit

- Organizers
  - Dr. Jason Li, Dr. Ray Richards
  - Supported by DARPA, AFRL, and Griffiss Institute
- Attendees: government, industry, and academia experts (~135)
- Agenda and presentation:
  - https://trustedcomputingcoe.org/summits/2018-summit/
- Focus: Introduce seL4® for more stakeholders and demonstrate the interest into trusted computing solutions

# Second seL4® Summit

- Organizers:
  - Dr. Jason Li, Dr. Renato Levy, Dr. Ray Richards
  - Supported by DARPA, AFRL, and Griffiss Institute
- Attendees: government, industry, and academia experts (~135)
- Agenda and presentation:
  - https://trustedcomputingcoe.org/summits/2019-summit/
- Focus: Broadening the stakeholder base of seL4®

# Third seL4® Summit

- Organizers
  - Dr. Renato Levy, Dr. Jason Li, Dr. Ray Richards
  - Supported by DARPA, AFRL, and Griffiss Institute
- Attendees: government, industry, and academia experts (~121)
- Agenda, presentation, video, and transcript:
  - https://trustedcomputingcoe.org/summits/2020-summit/
- Focus: Update on trusted computing state-of art, and seL4® updates

# Trusted Computing Center of Excellence

- Officially incorporated as a non-profit in 2022
- Trusted Computing CoE at https://trustedcomputingcoe.org/
- Goals of the Trusted Computing CoE
  - maturation of relevant technology including seL4®
  - stabilization of the software distribution
  - training and expanding the user base
  - developing much needed capabilities required by the U.S. Department of Defense, other government agencies, and commercial applications

TRUSTED COMPUTING
CENTER OF EXCELLENCE

# TCCOE

- Organizing Committee:
  - Dr. Jason Li (Independent Consultant)
  - Dr. Ray Richards (DARPA)
  - Dr. Renato Levy (BlueHalo LLC)
  - Mr. Patrick Hurley (Griffiss Institute)
  - Dr. E. Paul Ratazzi (AFRL)
  - Mr. Todd Carpenter (Adventium Labs)
  - Mr. Robbie VanVossen (Dorner Works)
  - Dr. June Andronick (seL4 Foundation)

# TCCOE Summit – 1

- Virtual event, January 31 - February 3, 2022
- Attendees: government, industry, and academia experts (~85)
- Agenda, presentation, video, and transcript:
  - https://trustedcomputingcoe.org/summits/2022-summit/

- Focus: reducing trusted computing to practice, seL4® updates, industry concerns
- Keynotes
  - Keynote 1: Provable Security: Next Steps to Broader Deployment, Dr. Kathleen Fisher, DARPA
  - Keynote 2: Of Incentives and Insecurity: Driving Adoption of Security Tools for National Security, Ian Crone, OUSD

# TCCOE Summit – 2

- Notable presentations:
  - Reducing Formal Methods to Practice, Dr. Brad Martin, DARPA
  - seL4 – State of the Union, Prof. Gernot Heiser, UNSW and seL4 Foundation
  - How DARPA’s SSITH Program Makes Software More Secure  Keith Rebello, DARPA MTO
  - From CHERI to Morello: Capability Hardware Enhanced RISC Instructions, Dr. Robert Watson, Cambridge University
  - Verified Security Properties and Semantics-Assisted Engineering for the Morello, CHERI-RISC-V, and CHERI-MIPS Capability-Enhanced Architectures, Peter Sewell, Cambridge University
  - Survey and Lessons Learned on Separation Kernels Dr. Ray Richards, Leidos

# TCCOE Panels – 3

- Panel Discussion – Proof, Assurance, and Evidence (Dr. Jason Li)
    - Dr. Ray Richards, Leidos
    - Prof. Kevin Hamlen, University of Texas at Dallas
    - Prof. Gernot Heiser / Dr. June Andronick, UNSW and Data61
    - Dr. Brad Martin, DARPA
- Panel Discussion – Gaps and Needs (Todd Carpenter)
    - Dr. Dariusz Mikulski US Army DEVCOM GVSC
    - Sascha Kegreiß, HENSOLDT Cyber GmbH
    - Nick Evancich, Trusted Science and Technology
    - Dr. Valerio Senni, Collins

# TCCOE 5

- Tutorials
  - Tutorial #1 – Teaser Training seL4, CAmkES and TRENTOS
    Sebastian Eckl, HENSOLDT
  - Tutorial #2 – Model-Based Code Generation for seL4 Prof.
    John Hatcliff & Jason Belt, Kansas State University
  - Tutorial #3 – ARES Secure Kernel on ZCU102
    Nicholas Evancich, Trusted Science and Technology
  - Tutorial #4 – OMG DDS for Simplifying seL4 Development and Use Cases Paul
    Pazandak and Fabrizio Bertocci, RTI

# TCCOE Current Leadership

TRUSTED COMPUTING CENTER OF EXCELLENCE

- Elected Officers:
  - Acting Executive Director: Mr. Patrick Hurley (Griffiss Institute)
  - Vice President: Dr. Jason Li
  - Treasurer: Dr. Stu Card
  - Secretary: Dr. Ray Richards
- Committees:
  - Audit and Finance: Ray Richards, Yong Guan, and Daniel Limbrick
  - Technical Steering: Jason li, Yong Guan, Daniel Limbrick and Gregg Wildes

# Lessons Learned

- Applying tools to problems: from research to practice
- Building synergies: government-industry-academia
- Understanding limitations, gaps, and needs
- Open-source and licensing model
- Improving proof, assurance, and evidence
- Establishing assurance with evidence

# Way Forward

- Nurturing Trusted Computing capabilities
- Organizing TCCOE Summits
  - A sister of seL4 Summits (roughly 6 months apart from each other)
  - Trusted Computing oriented
  - Broader in scope: technique and tools; assured systems; practical lessons
- Fostering community building and collaboration

# BACKUP