ARES Secure Kernel (ASK) on ZCU102

Nicholas Evancich, Dr. Kyung Kwak
nick@trustedst.com, kj@trustedst.com

January 31, 2022
Trusted Computing Center of Excellence (TCCOE) Summit

TRUSTED
SCIENCE AND TECHNOLOGY

Agenda

- **Overview**
- Trusted ST Intro
- Agile Resilient Embedded Systems (ARES) Secure Kernel (ASK)
- ASK on ZCU 102

Introduction

- seL4: first formally verified microkernel
  - Supported by DARPA High-Assurance Cyber Military Systems (HACMS); keynote on Feb 1 by Dr. Fisher
  - Adopted in AFRL Agile Resilient Embedded Systems (ARES)
- U.S.-based seL4 Center of Excellence, now Trusted Computing Center of Excellence (TCCOE)
  - Envisioned by Nicholas Evancich, Dr. Kyung Kwak and Dr. Jason Li
  - Supported by DARPA and AFRL
  - Executed by Intelligent Automation and Griffiss Institute
- This is the fourth Annual Summit

Challenges and Needs

- Challenges
  - seL4 provides separation capabilities
  - As a microkernel, it doesn't provide needed services and features
- Needs
  - Solution developers need to develop these services and features (e.g., drivers, network stack)
  - Proofs are fragile by nature, and hence need repair or maintenance (Feb 1 keynote and Dr. Martin from DARPA)
  - Identify artifacts based on proofs and executing binaries for building assured systems (Panel discussion on Feb 1 and Feb 2)
  - Establish and sustain an ecosystem and development community (TCCOE and Annual Summits)

Background of the Tutorial

- AFRL Agile Resilient Embedded Systems (ARES)
  - Conducted a thorough analysis of alternatives (AoA) of separation kernels and real-time OS
  - Examples include Integrity, VxWorks, PikeOS, seL4, CertiKOS, DeOS
  - Adopted seL4 (open-source) and DeOS (commercial) as kernels for octocopter flight tests
  - Improved seL4 virtual machine manager (VMM), developed native security services on top of seL4
  - Developed the ARES Secure Kernel (ASK) with security services
  - Integrated with DoD workflow, and demonstrated security and resilience capabilities via lab experimentation and flight tests

Context

- The ARES capabilities and ASK are export controlled
- Therefore, not much details are included in this tutorial
- These capabilities can be leveraged by US government and performers through the TCCOE Private Repository (Session 12 – Patrick Hurley)
- Purpose of this tutorial:
  - Raise the awareness
  - Encourage US government researchers and performers to try-out the ASK package (so that people don't have to "reinvent the wheels")

Agenda

- Overview
- **Trusted ST Intro**
- Agile Resilient Embedded Systems (ARES) Secure Kernel (ASK)
- ASK on ZCU 102

Trusted Science and Technology, Inc

- Small business entity incorporated in Bethesda Maryland
- Expertise in cyber security, embedded system, and network/communication technologies
- Extensive R&D experience from diverse BAA/SBIRs efforts
- Dynamic R&D focus corporate culture
- Member of Maryland Montgomery County Innovation Network/Incubator
  - Office suite with 1500+ sq. ft.

Relevant Experience

- Designed and implemented a secure and resilient system architecture for UAS/UAV with successful flight demonstrations
- Developed a secure, resilient system prototype to transition hardware/software integrated security solution to DoD stakeholder
- Developed and matured the seL4-based AFRL **ARES Secure Kernel** (ASK) for U.S. specific interest

AFRL: Air Force Research Laboratory

ARES: Agile Resilient Embedded Systems

seL4, ASK, and Development

- Provided multiple seL4 training sessions
  - Training AFRL researchers and DoD performers at Griffiss Institute
  - Tutorial during IEEE Secure Development (SecDev) Conference 2021
- Provided multiple ASK short tutorial and support sessions
  - Government researchers
  - FFRDC, UARC and performers
- Led US seL4-based solution development and supported U.S. agencies (e.g., DARPA, AFRL, Army, Navy) and TCCOE governing entities
- Creating roadmaps to fill the gaps and needs (refer to Summit panels)

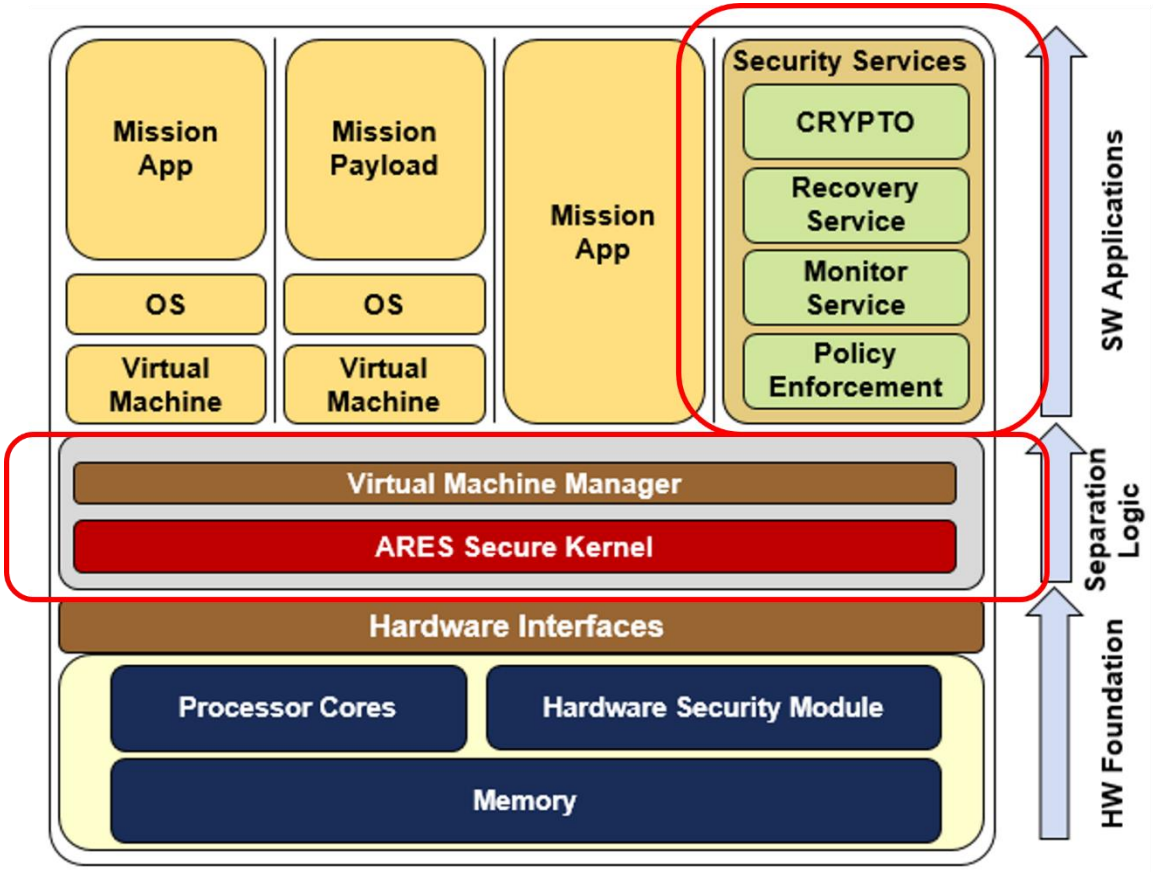
Agenda

- Overview
- Trusted ST Intro
- **Agile Resilient Embedded Systems (ARES) Secure Kernel (ASK)**
- ASK on ZCU 102

ARES Concept

- No “perfect security” in the real world; appropriate security should be built-in
- Build resilience (function through attacks) on top of security
- Holistic design: open architecture, technology selection, safety concerns, attack categories, design trade-offs, risk analysis, etc.
- Architecture must allow for future capability inclusion, as well as supporting legacy mission applications and capabilities
- Sound design must adopt solid security principles (e.g., separation, mediation, least privileges)
- Flexible and versatile cryptography and key management
- Fielding is the ultimate purpose (as opposed to only S&T), hence field (e.g., flight) tests are mandatory

ARES Architecture



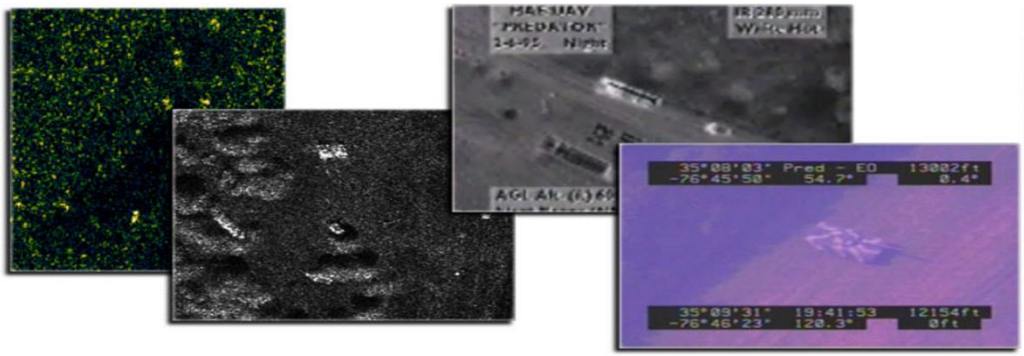
AFRL ARES Secure Kernel with security services

ARES Activities

- Conducted a thorough analysis of alternatives (AoA) of separation kernels and real-time OS
- Adopted seL4 (open-source) and DeOS (commercial) as kernels for octocopter flight tests at AFRL
- Improved seL4 virtual machine manager (VMM), developed native security services on top of seL4
- Supported the DARPA HACMS program as a transition partner
- Integrated with OSD/AFRL end-to-end UAS workflow
- Implemented on real-world mission computer and payload
- Demonstrated security and resilience capabilities via lab experimentation and flight tests under realistic use cases

ARES Successes

AFRL RI Flight Testing and Capstone Demonstration



AFRL RY/RI/RH UAV Testbed Integration and Demonstration

ARES Recent Advances

- Recovery capabilities (kernel and virtual machine)
- Data Distribution Services (DDS) – another tutorial today
- Porting ASK to RISC-V (another talk on Feb 1)
- Enabling swarming of multiple platforms
- Supporting OSD/Army GVSC capability development
- Creating vision and roadmap on proof and assurance
  - Bottom-up verification: design modules amenable for applying bottom-up formal verification
  - Binary-level evidence: finding evidence of assurance properties directly from binaries

ARES Secure Kernel

- Based on seL4
- Becoming a small operating system
  - File system
  - Network Stack: TCP/IP protocol & DDS
  - I/O: Ethernet, CAN, Serial
  - Baked in verification (work in progress)
    - Bottom-up verification
    - Eclipse plug-in for improving source code
  - Security services
    - Monitor, Policy Enforcement, Recovery
  - Platforms
    - ARM (e.g., A53 64-bit, multi-core)
    - Work in progress: RISC-V, PPC, Intel

What We Can Offer

- ARES Secure Kernel on ARM
  - SW package running on ZCU102
  - SW package running on Pi4 (work in progress)
  - Training and support
- ARES Secure Kernel on RISC-V
  - SW package running on a PolarFire board (work in progress)
  - Training and support
- ASK, with VMM and the security services, provide a flexible, **trusted execution environment** needed by many users
- Customized solution for your use cases
  - Design analysis and trade-off options
  - Develop holistic, automatic solutions with support

Agenda

- Overview
- Trusted ST Intro
- Agile Resilient Embedded Systems (ARES) Secure Kernel (ASK)
- **ASK on ZCU 102**

Obtaining the ASK Package

- Contact us
  - Nicholas Evancich, Dr. Kyung Kwak at nick@trustedst.com, kj@trustedst.com
- AFRL POC:
  - Mr. Mike Lynch at michael.lynch.49@us.af.mil
- TCCOE Private Repository (Session 12 of Summit)
  - Patrick Hurley at phurley@griffissinstitute.org

ZCU102

- Quad core A53
- Dual core R5
- Around $3k
- Wide range of I/O
- https://www.xilinx.com/products/boards-and-kits/ek-u1-zcu102-g.html

Q&A