seL4 Center of Excellence – Plans and Progress

Intelligent Automation, Inc.

Nick Evancich

Distribution Statement A. Approved for public release. Distribution is unlimited.

seL4 Center of Excellence (CoE) - Goals

- Mature the technology
- Stabilize software distribution
- Expand user adoption in the U.S.
- Foster collaboration among contributors in the U.S.
- Transition into various applications

Special thanks to: DARPA, Data 61, AFRL



seL4 CoE Philosophy

Community

- Software is complex and shouldn't be created by a single entity
- Combine the experience of more people

Quality

- Increase the number of eyes on the source code
- Community driven
- Features driven by the community's need

Permissive Licensing

- Not for profit
- Promotes the use of open source software
- Maximize the benefit and impact



CoE Components



Training

- Online training
- On-site training
- seL4 developer certification

Development Center

- Gaps in seL4 and new capabilities
- U.S. Repository
- "Controlled" Repository

Innovation Center

- Bringing new ideas
- Landing pad for other DoD programs
- Incubator for new ideas

Outreach Program

- Hosting interns
- Moderating forums
- Sponsoring various academic papers
- Holding workshops



CoE Workflow

Generate new interest / developers

Outreach Program

Training Program



From members of the COE / student interns / developers

Developed by closing gaps funded by other commercial partners or government

New seL4 based pervasive technology from the Innovation Center



CoE Research Team

- Intelligent Automation Inc. (IAI)
 - Leading the overall CoE effort
 - Coordinating the outreach program
 - Current administrator of the development center
- DornerWorks
 - Major developer of the training materials
 - Major contributor to the development center
- Griffiss Institute / Cyber Research Institute
 - Transition partner; strong support from AFRL/RI
 - Manage the private repository and exercise access control
 - Lead the process to establish the official seL4 CoE
- Special team member Data 61



Accomplishments



Current Progress - 1

Training

- Collaboration with other contributors
- Tutorials and training materials on wiki page
- Course materials & try-out at AFRL / GI / CRI
- Matured training materials during Summit 2018
- Transition plan (SAE, GI)

Outreach

- Website https://sel4-us.org/
- Engagement of most seL4 performers in the U.S.
- seL4 internship
- 2018 Annual seL4 Summit
- Academic projects
- MILCOM panel on secure embedded system design



Current Progress - 2

Development

- Stabilized seL4 with bug fixes and thread safety
- New libraries with API for process and threads
- seL4 hardware lab
- Public release of source code from DARPA
- Version 1.0 available on 08/30/2018 at GitHub https://github.com/sel4-us/

Innovation

- Conversations with most U.S. seL4 performers
- New ideas and opportunities identified
- An example workflow
 - seL4 libraries put in the incubator stage
 - Included in the opensource DARPA release
 - Part of Version 1.0
 - Expect good usage



Stable seL4 Version 1.0

- POSIX-like process and thread creation
- Simplified capability generation/passing
- Simplified messaging configuration
- Simplified memory allocation and configuration
- Memory map verification for AARCH32 and AARCH64
- Corrected RW- and R-X memory on AARCH32 and AARCH64
- Thread-safe malloc()
- Thread-safe vka() and vspace()
- Round-Robin scheduling
- Sleep() and GetTicker() functions
- Posix-like mutexes, conditions, and reentrant locks
- Multi-core AARCH64



CoE Teaming Agreement

- CoE members agree to work towards achieving the overall COE goals stated earlier
- 2. CoE members **agree to share their intermediate progress and source code** of core seL4 components (i.e., no application-specific code needs to be shared) with other CoE members to the extent that their contracts allow
- 3. CoE members **agree to work towards open-sourcing** their additions to seL4 to the extent that their contracts allow
- 4. CoE members agree to put all of their additions to seL4 in the CoE Repositories
- 5. CoE members **agree to follow the CoE's bylaws** when using USA Public or Private Repositories



Public versus Private Repositories

- Public distribution of seL4 components will be performed via the public GitHub organization account at https://github.com/seL4-USA
- Private distribution of seL4 components that have been developed by US-based contributors with proper distribution statement or government approval will be uploaded to a CoE private server
 - ITAR controlled
 - Distribution will be performed either according to Government Distribution Statements B, C, or D, or according to special requirements defined by the U.S. Government
- 3. Public and Private Repositories differ in terms of A) content, B) who has access, C) what level of access is granted, and D) requirements for submitting new content



Requirements for Public Repositories

- 1. Public Repositories are on www.github.com
- 2. IAI holds the **USA seL4 www.github.com account**. Others submit their code changes to IAI for review before it is incorporated into the greater codebase
- 3. Regarding **repository content**, CoE members agree to:
 - 1. Only submit code for incorporation that has been approved for opensource
 - Follow the CoE's Test Procedure before submitting their code for incorporation
 - 3. Use <u>www.github.com</u> Pull-Requests to submit their finalized code changes for approval before those changes are incorporated into the repositories
 - 4. Include release notes explaining their changes
 - 5. Perform code reviews
 - 6. Get permission from IAI before making major architecture changes
 - 7. Allow the CoE to remove their content if it introduces errors



Way Forward



CoE Transition Plan

Training

- Transition to SAE for course development
- Broader audience
- Customized training

Development

- seL4 stable version
- Public repository
- Technical support
- Data 61 keeps the seL4 brand (e.g., Penguin logo for Linux)
- CoE distributes stable versions (e.g., RedHat Linux)

Outreach and Innovations

- Mature website (forums, job postings, on-line ads, training)
- Internship programs
- seL4 certificates
- Roadmaps and new projects

From 'Pilot' to operations

- CRI at Griffiss Institute
- AFRL/RI
- Private repository
- Legal entity
- Governance



Some Thoughts to Share

- Participation → success
- Do what is best for the community
- Keep the source code clean
- Follow the process
- Maintain relevant documentation
- Technical roadmap & visions
- New projects and applications

- Agree on purpose
- Establish the governance
- Manage legal issues

- CoE operations
- Technical support
- Community facing teams
- Engage more users with various events



Moving Forward

- Stable Version 2.0
 - Add automated unit and regression test system (e.g., Jenkins)
 - Add and maintain copious documentation
 - Need community input
 - Version 2.0 features
 - Down selection of high-level functional language
- Enhance technical development and support
- Expand user base
- Hold more summits
- Extend to more application domains
- Create governance council

