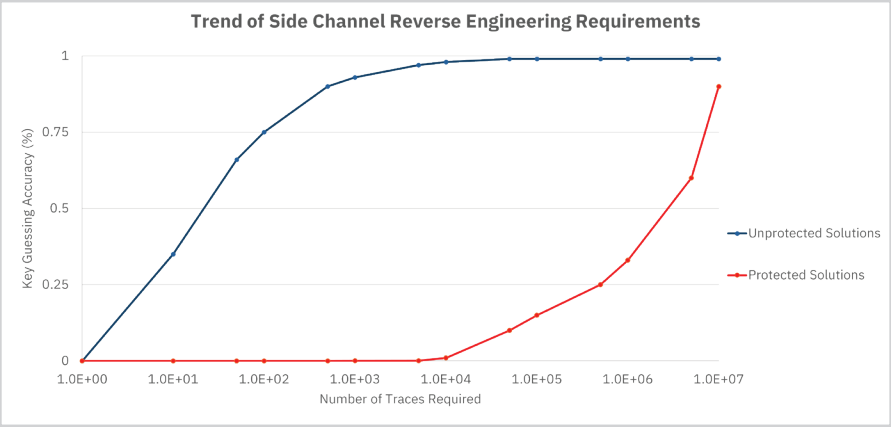
Assurance Research for Embedded Systems (ARES) Lab

Allows for the unclassified performance of reverse engineering (RE) and hardware security analysis of embedded system and microelectronic devices

ARES Lab will provide fully unclassified laboratory capabilities within Riverside Research to perform complete non-invasive and semi-invasive microelectronic RE hardware attacks. This IRAD addresses the DoD need for a laboratory to replicate open-source RE attacks without requiring a classified space—something most GOTS solutions are unable to provide.



As shown above, microelectronic devices featuring counter-RE protections require more collected data captured on better equipment compared to the unprotected solutions often featured in open-source publications. This requirement utilizes TBs+ of storage and immense processing power, combined with skilled users.

For this reason, we are pursuing side channel attacks against existing hardware and simple cryptographic targets. New equipment will allow for improved attacks against protected solutions, which is usually not discussed in the open-source due to the complexity of attacks and required equipment.

Specialized equipment like keysight oscilloscopes, electromagnetic probes, ChipWhisperer devices, spectrum and network analyzers, and thermal chambers have been ordered for ARES Lab.

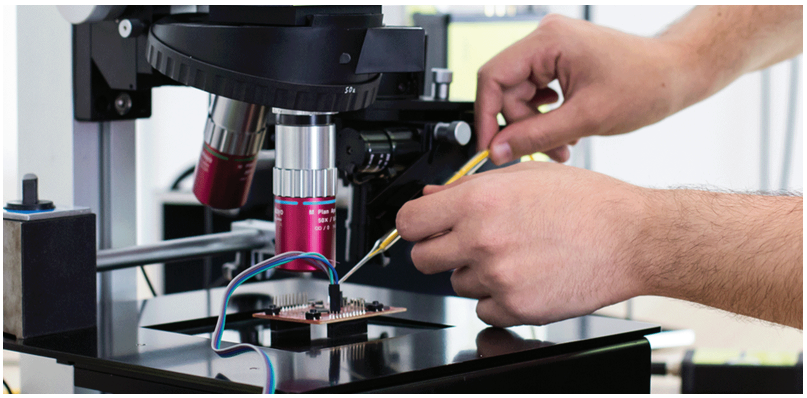
Key Capabilities

- Fully unclassified laboratory to perform microelectronic reverse engineering hardware attacks
- Build a talent pipeline in microelectronic security
- Speed up in-house microelectronic research

Key Equipment

- Keysight Oscilloscopes
- Firewalled development Desktop PCs
- Langer EM fault injection equipment
- Riscure and Langer Electromagnetic (EM) Probes
- Thermal Chamber
- ChipWhisperer devices
- Full solder/de-soldering stations, and microscopes
- Spectrum and Network Analyzers

ARES Lab



State of the Laboratory

Microelectronic RE requires significant high-caliber equipment. As the complexity of device implementations grow, high-end equipment is needed to keep up with higher throughput systems and increasingly complex data.

We are actively installing our ARES laboratory space within the Riverside Research Beavercreek, OH, facility. To date, we have:

- Ordered initial equipment for laboratory and begun to build initial operating capability
- Replicated the software needed to perform open-source attacks against hardware systems, and started Riverside Research IP to advance upon existing open-source attacks
- Planned open-source replication demonstrations with steps to advance attacks to SOTA performance

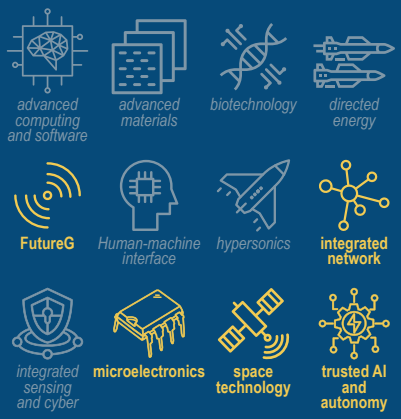
Next Steps

We will finish initial operating capability with ordered equipment:

- Arrange equipment that has been received
- Procurement ordering additional equipment
- Perform final round of equipment procurement to finalize capability
- Combine OIC/SRS lab space with our ARES Lab to best share resources and collaborate
- Expand into more semi-invasive approaches, hardware device fabrication, and fully-invasive device altercation technique

RIVERSIDE RESEARCH

Critical Tech Areas



DoD Priorities

1. Southwest Border Activities
2. Combating Transnational Criminal Organizations in the Western Hemisphere
3. Audit
4. Nuclear Modernization (including NC3)
5. Collaborative Combat Aircraft (CCAs)
6. Virginia-class Submarines
7. Executable Surface Ships
8. Homeland Missile Defense
9. One-Way Attack/Autonomous Systems
10. Counter-small UAS Initiatives
11. Priority Critical Cybersecurity
12. Munitions
13. Core Readiness, including full DRT funding
14. Munitions and Energetics Organic Industrial Bases
15. Executable INDOPACOM MILCON
16. Combatant Command support agency funding for INDOPACOM, NORTHCOM, SPACECOM, STRATCOM, CYBERCOM, and TRANSCOM
17. Medical Private-Sector Care