Securing the Future of O-RAN: Insights from the Public Wireless Supply Chain Innovation Fund

U.S. Department of Commerce
National Telecommunications and Information Administration

Brian Gomez
Federal Program Officer

Session Outline

Public Wireless Supply Chain Innovation Fund

PWSCIF Notice of Funding Opportunities

PWSCIF Current State: NOFO 1 & 2

Award Highlights: ORAN Security

Q&A

Public Wireless Supply Chain Innovation Fund (PWSCIF)

The Public Supply Chain Wireless Fund (Innovation Fund) is a $1.5 billion competitive grant program authorized by Section 9202(a)(1) of the FY21 NDAA and appropriated by Div. A, Section 106 of the CHIPS and Science Act of 2022 over a 10-year period.

Vision

Develop a competitive global ecosystem of trusted telecommunications vendors that are fielding open and interoperable network equipment domestically and overseas.

Mission

Develop and implement a grant program that accelerates the adoption and deployment of open radio access networks through investments in interoperability, hardware maturity, security, and supply chain diversity.

PWSCIF Notice of Funding Opportunities (NOFO)

NOFO 1

Objective: Accelerate the Development, Deployment, and Adoption of Open and Interoperable Radio Access Networks (RAN)

This effort is supported through a competitive grant program focused on driving innovation in the wireless industry.

Projects aim to:

- **Expand industry-accepted testing and evaluation** to effectively facilitate and assess the interoperability, performance, and/or security of open and interoperable, standards-based 5G radio access networks.
- **Develop new and/or materially improve existing testing methodologies** to test, evaluate, and validate the interoperability, performance, and/or security of these networks, including their component parts, to address needs not currently met by industry-accepted tests and best practices.

NOFO 2

Objective: Advance Open RU Commercialization and Innovation

This NOFO aims to build upon previous efforts by investing in the technological development and commercial deployment of open radio units (RUs)—a critical component of RAN that represents the largest portion of carrier network capital expenditures (CAPEX).

Specific Research Focus Areas:

- **Open Radio Unit (RU) Commercialization:** Projects funded under SRFA 1 will focus on accelerating the development of open RU products to the point where they meet carrier needs and are ready for commercial trials.
- **Open RU Innovation:** Projects funded under SRFA will focus on improving the overall performance and capabilities of open RUs through targeted research and development.

Current State: Notice of Funding Opportunities 1 & 2

NOFO 1

(NTIA) has awarded over $140 million to 17 projects under the first round of the Public Wireless Supply Chain Innovation Fund. These projects focus on:

(3) Testing and Evaluation (T&E) Facilities: Establishing centers for rigorous testing of network performance, interoperability, and security.

(14) Research and Development Projects: Advancing the transition to more open, resilient 5G networks through innovative testing methods, cybersecurity enhancements, and energy efficiency improvements.

These initiatives are foundational to the success of open and interoperable wireless networks, building confidence in the viability of Open RAN solutions and breaking down barriers to adoption.

NOFO 2

NOFO 2 Award Selection Process:

The NTIA received an overwhelming response of 269 applications for funding under NOFO 2. These applications are currently undergoing a rigorous selection process, including Initial Review, Merit Review, and Programmatic Review. This comprehensive evaluation ensures that only the most innovative and impactful projects are selected, aligned with the overarching goals of advancing open and interoperable network technologies.

The exact dates for the award announcements are yet to be determined, reflecting the careful and thorough review process.

Award Highlights: ORAN Security

Mississippi State University:

- **Focus:** Soft Tester UE (Soft T-UE) for RAN Security
- **Overview:** Pioneering an open-source, software-based solution designed to rigorously test and enhance RAN security. The project addresses the need for adaptable, transparent testing frameworks crucial for future-proofing telecom networks.

Booz Allen Hamilton:

- **Focus:** Enhancing O-RAN Systems Against Sophisticated Attacks
- **Overview:** Developing cutting-edge security mechanisms to fortify O-RAN environments against evolving threats. Emphasis on real-time threat detection and resilient network defense strategies.

EchoStar/DISH:

- **Focus:** Open RAN Center for Integration & Deployment (ORCID)
- **Overview:** Establishing a state-of-the-art, vendor-agnostic testing facility. The lab specializes in assessing and mitigating real-world security challenges in O-RAN deployments, ensuring robust, telecom-grade network security.

Software-Tester UE (Soft T-UE)

NOFO1 R&D Project

Mississippi State University—Wireless@MSU
Vuk Marojevic, vm602@msstate.edu

Mississippi State University

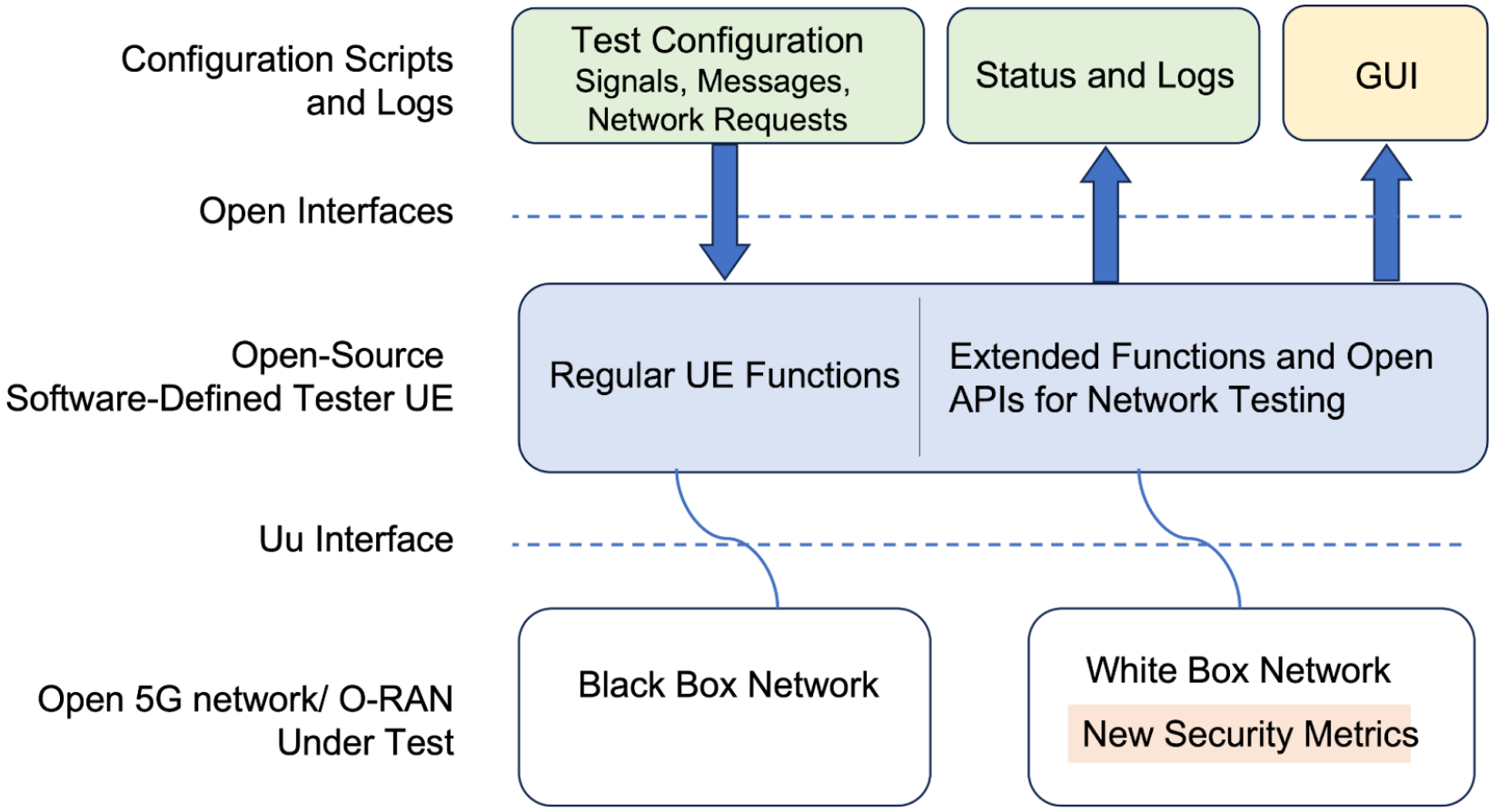
Motivation

- Testing is expensive, requires specialized equipment
- Test procedures evolve with the standard, requiring frequent upgrades
- Traditional hardware test equipment is becoming software-centric, introducing software licenses with high maintenance/ support fees
- Industry focus is on performance and conformation tests for quick product rollout
- Limited security test procedures, which are gaining importance

Proposed Approach

- RAN security testing where attacks come from end devices over the Uu interface
- Evaluate existing and introduce new security metrics
- White box and black box RAN testing
- Testing methodology and tool: software-based tester user equipment (soft-T UE), for rapid prototyping, configuration, and adaptation of test procedures
- Free and open-source software using COTS software radio hardware
- Full transparency of what tests are implemented and how they are implemented with the ability to improve or extend the suit of tests

Proposed Approach



Mississippi State University

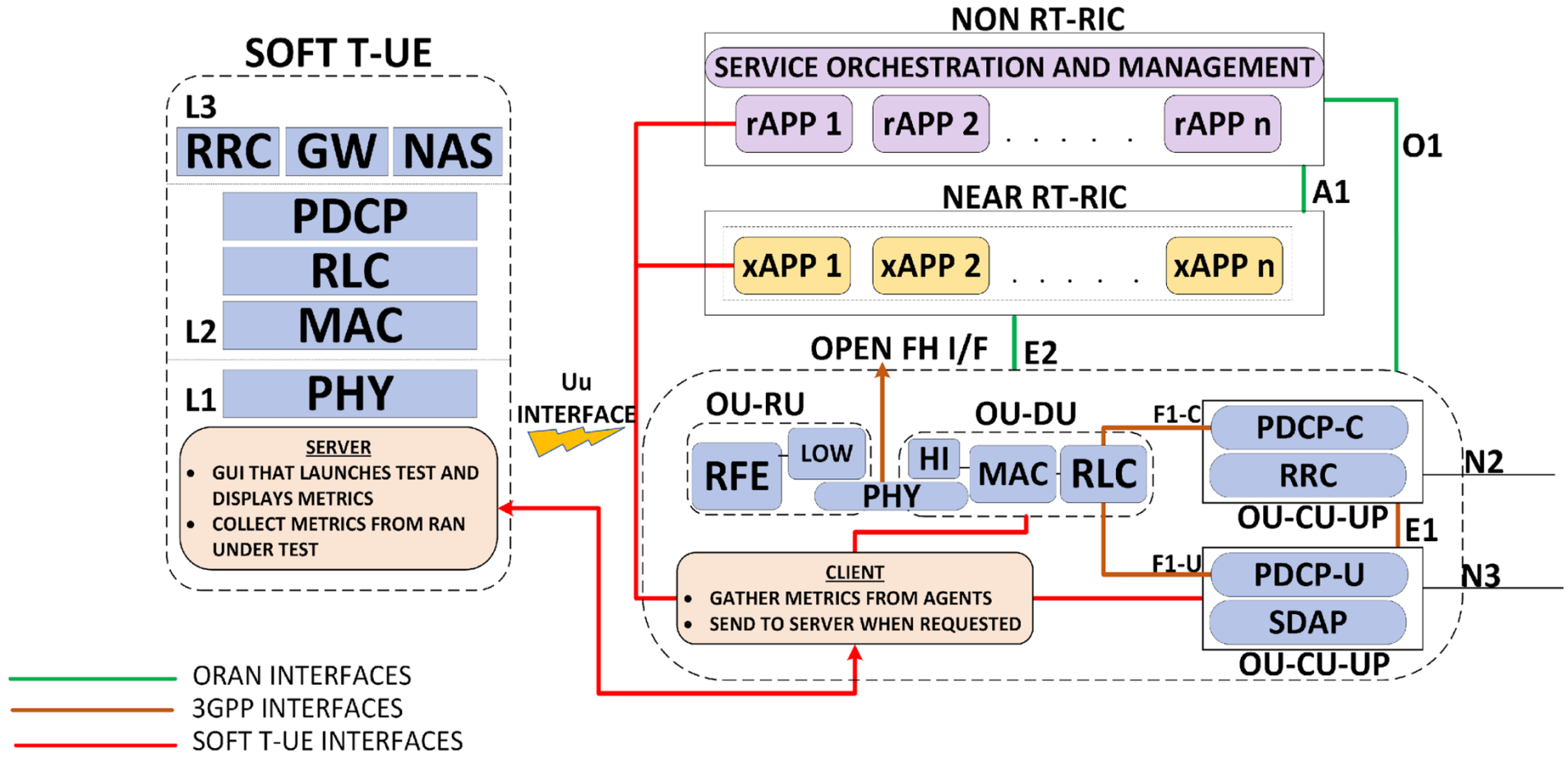
Benefits

- Free open-source software testing for spurring domestic and multi-vendor RAN development and standard evolution:
- Low cost and low entry barrier for self-testing of open 5G networks
- Instant testing and test results, enabling phased development and integration
- Customizable tests for in-house testing before sending RAN equipment for certification
- Introduction of custom RAN products to provide competitive advantages backed up by demonstrable and reproducible test results
- Consistent assessment approach for evaluating the security posture of network components, regardless of their origin

Context

- 3GPP Interface Tests: Ensures security and reliability of 3GPP-defined interfaces like N1, N2, N3 through integrity, confidentiality, and availability checks
- O-RAN Alliance Security Test Specifications: Comprehensive security testing, including vulnerability assessments and compliance with security requirements
- **Customizable Security Tester: Configurable attack scenarios and security KPI/data collection**

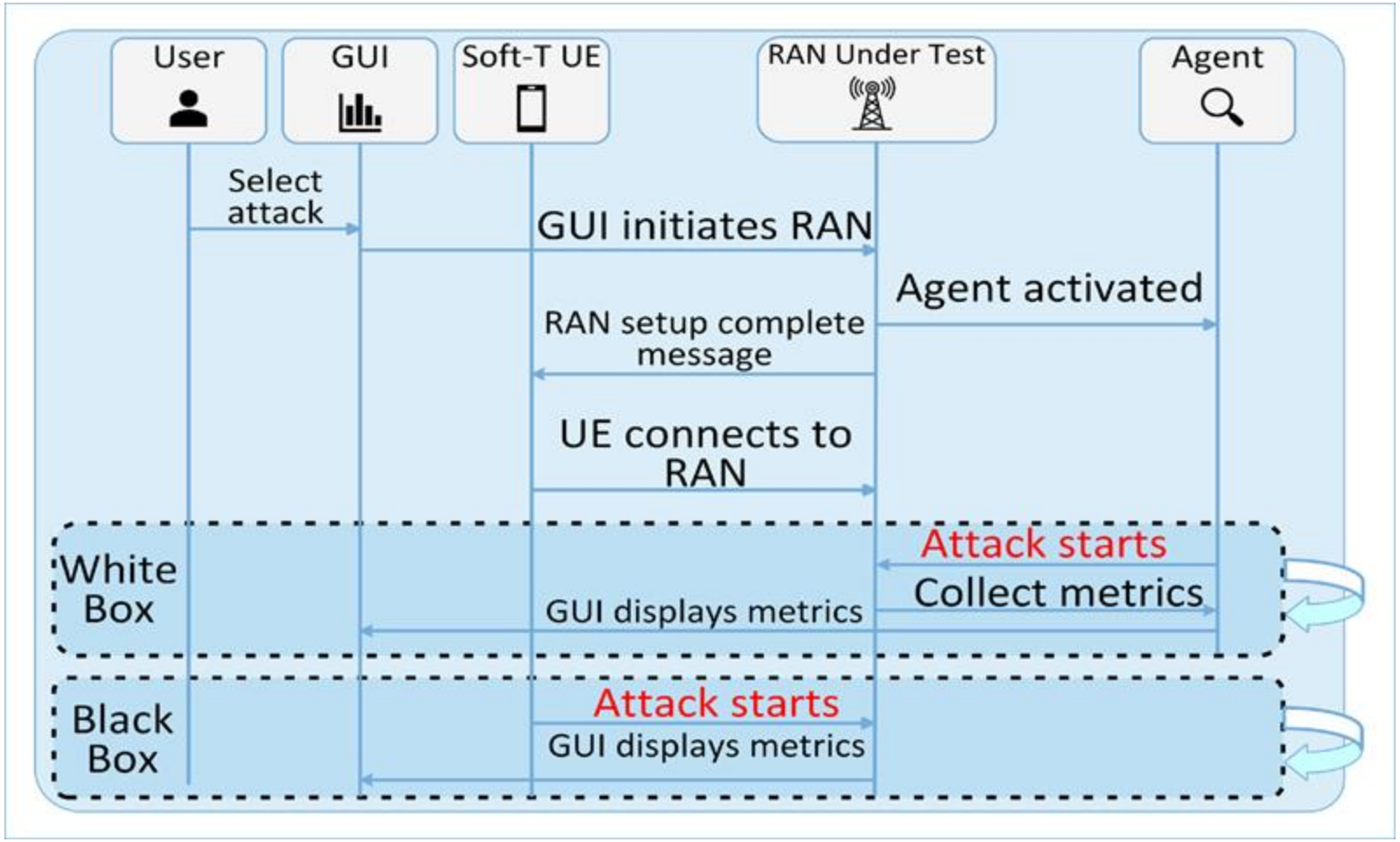
Soft T-UE Architecture



Mississippi State University

Security Test Procedure

1. Configure test parameters
2. Launch the Test
3. Establish Connection
4. Execute Test Scenarios
5. White-Box testing
6. Black-Box testing
7. Monitor Real-Time Data
8. Data Collection
9. Data Analysis



Why Soft T-UE?

Software-Based Tester UE (Soft T-UE):

- Tool enabling the exploration of new security metrics and test procedures
- Security testing that is accessible, comprehensive, and cost-effective

Soft T-UE	Existing Commercial Solutions
• Free to use	• High initial cost & ongoing fees
• Open Source	• Large scope
• Extensible and community driven	• Limited customization
• Security focused	• Fixed metrics
• Limited professional support	• Vendor support

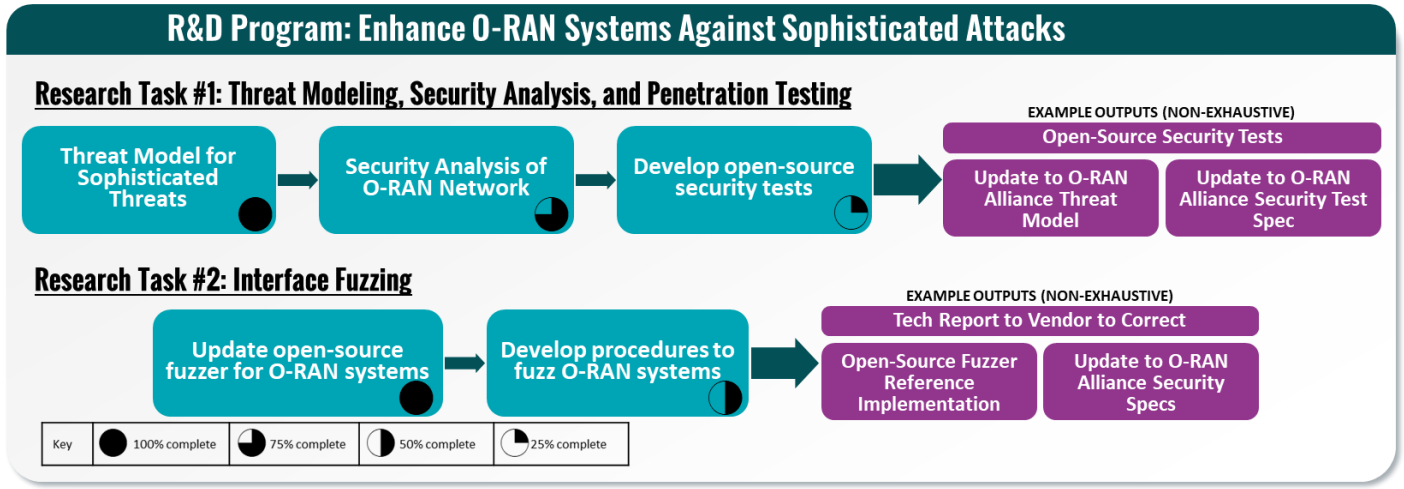
Booz Allen Hamilton

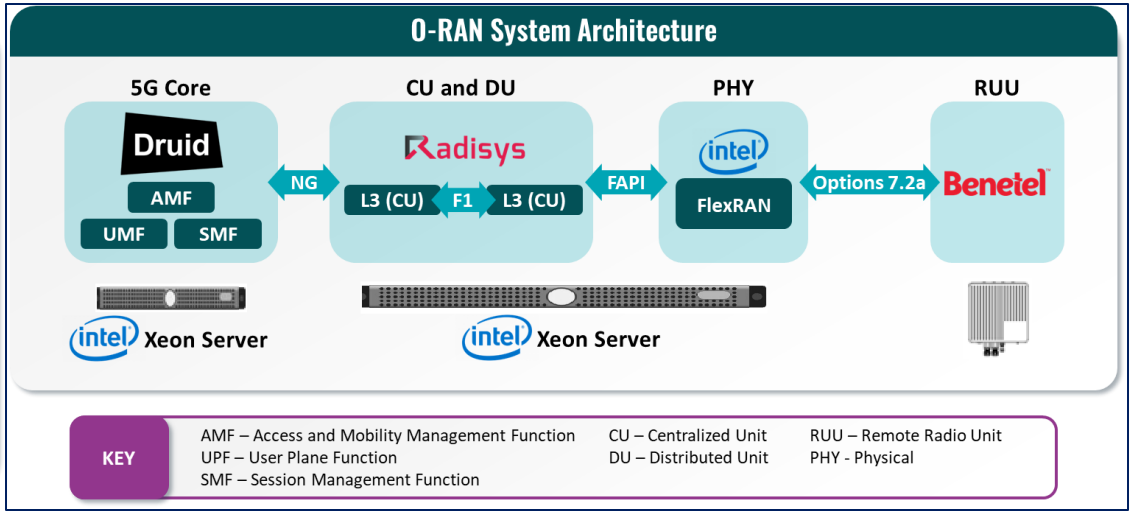
Booz Allen Hamilton

NTIA PWSCIF Grant: Enhancing O-RAN Systems against sophisticated Attacks

Booz Allen in collaboration with Virginia Tech will look to achieve the following objectives by the end of calendar year 2025:

- Drive **advanced security tests for sophisticated attackers** into specifications.
- **Increase industry and community adoption** of advanced security tests for sophisticated attackers, through open-source reference implementations and building relationships with commercial test vendors .
- **Procure and deploy O-RAN** lab for security analysis, penetration testing, and interface fuzzing.





Booz Allen Hamilton

Achievements to date and anticipated industry impacts - RA#1

Table. FiGHT Matrix Attack Categories Mapped to ORAN threats

FiGHT Attack Categories	ORAN threat Applicable	ORAN specific treats
Reconnaisssance	No	
Resource Develpoment	No	
Initial Access	Yes	RogueX Apps Unauthorized access
Execution	Yes	gNodeB Component Manipulation
Persistence	No	
Privelege Escalation	No	
Defense Evasion	No	
Credential Access	Yes	Network Sniffing
Discovery	Yes	Network Sniffing
Lateral Movement	No	
Collection	Yes	Network Sniffing
Command & Control	N/A	
Exfiltration	N/A	
Impact	N/A	
Fraud	N/A	

Table. Example: Initial Access MiTRE FiGHT O-RAN Gap Analysis

Technique	Architecture Segments	O-RAN Consideration
Rogue xApps Unauthorized access	5G	Y

Booz Allen-VT Considerations:

- Authorized xApps that have been compromised to become rogue agents in the O-RAN network.
- Unauthorized xApps that injected or infiltrate the O-RAN network to exploit the system components or end users.

Threat Modeling & Penetration Testing

Achievements to Date

- Completed O-RAN threat matrix via evaluation of 80 threats.
- Concluded Gap analysis by assessing the O-RAN Alliance Threat Model compare MITRE FiGHT categories.
- Progressed through phases of Pentest analysis of ORAN systems. Analysis helped provide better security recommendations for security enhancement of ORAN systems.
- Attended industry events such as TechNet Cyber to share findings from the ORAN tasks.

Anticipated Industry Impacts

- Publish results to community on how to better security O-RAN systems from all threat actors such as nation state actors.
- Integration of outputs with O-RAN Alliance WG11 security Threat Models.

Achievements to date and anticipated industry impacts - RA#2

Interface Fuzzing

Achievements to Date

- Assessed 9+ open-source fuzzers and down selected the best candidate as basis for fuzzer development.
- Developed RRC ASN.1 encoder and decoder.
- Developed RRC fuzzer generation module to deliver RRC payloads to ORAN system.

Anticipated Industry Impacts

- Open source of fuzzing tool that will support numerous O-RAN interfaces to enable flexible fuzz testing of ORAN systems.
- Fuzzer integration into OTIC Lab systems.
- Collaboration with O-RAN testing Vendors to integrate tool and validate O-RAN systems.

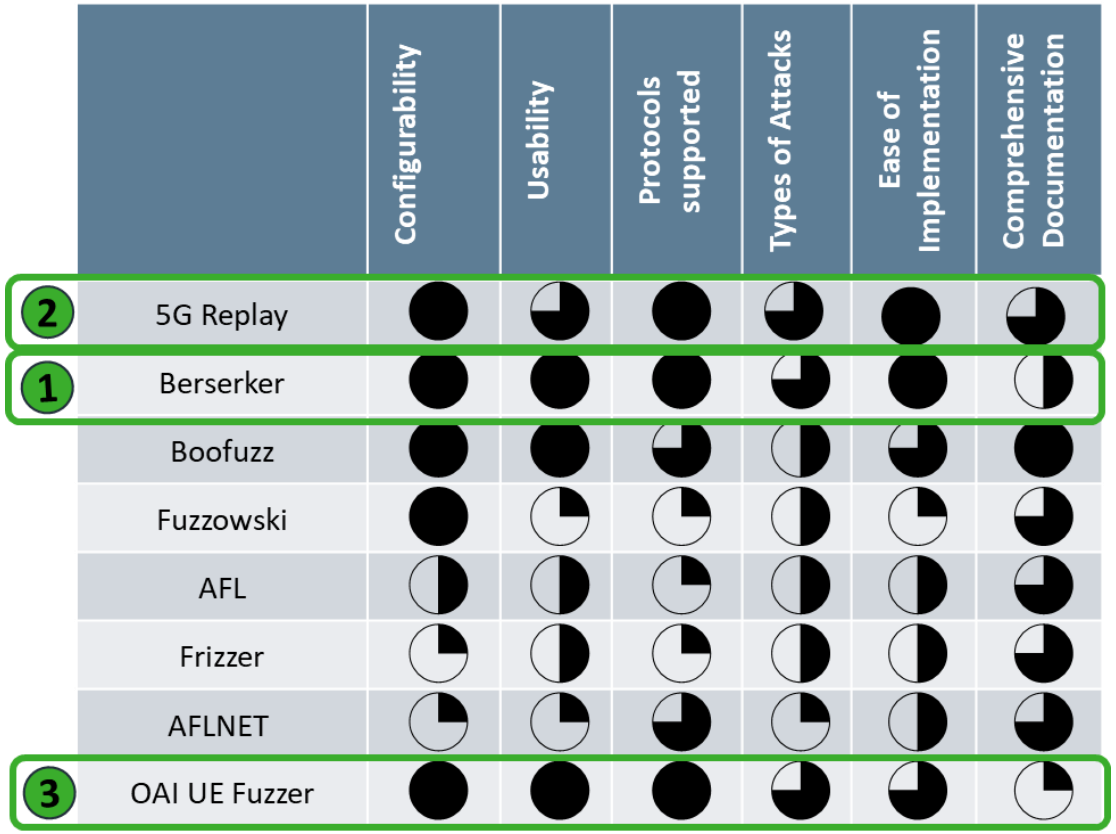


Table: Fuzzer Gap analysis and down selection Process.

Booz Allen Hamilton

Industry Engagement

Conferences and Panels

- ✓ MWC Barcelona 2024
- ✓ TechNet Cyber 2024
- • IORS 2024
- • MWC Las Vegas 2024
- • IEEE MILCOM 2024
- • i14Y Summit 2024

Publications, Blogs, & Social Media

- ✓ Booz Allen 5G Website – O-RAN Testbed
- ✓ Shaping the Future of 5G and NextG
- • ORAN Threat Model paper
- • 5G/O-RAN Security Automated Testing Demo/Paper via IEEE
- • Open-Source Fuzzer Tool Releases

Industry Connections

- Virginia Tech
- Penn State
- Ericsson
- Viavi
- Keysight
- OAI Development Community
- Orchid Lab
- Fuzzer integration into OTIC Lab systems

Standards

- O-RAN Alliance Security WG 11

EchoStar/DISH - ORCID

Open RAN Center for Integration and Deployment

ORCID, located in Cheyenne, Wyoming, is a Testing and Evaluation facility under the Public Wireless Supply Chain Innovation Fund.

Comprehensive Security Assessment: Performs in-depth security evaluations of O-RAN components, focusing on real-world operational scenarios to identify and mitigate vulnerabilities.

Vendor-Neutral Testing Environment: Provides a neutral platform for testing and validating the security of multi-vendor O-RAN solutions, ensuring interoperability without compromising security.

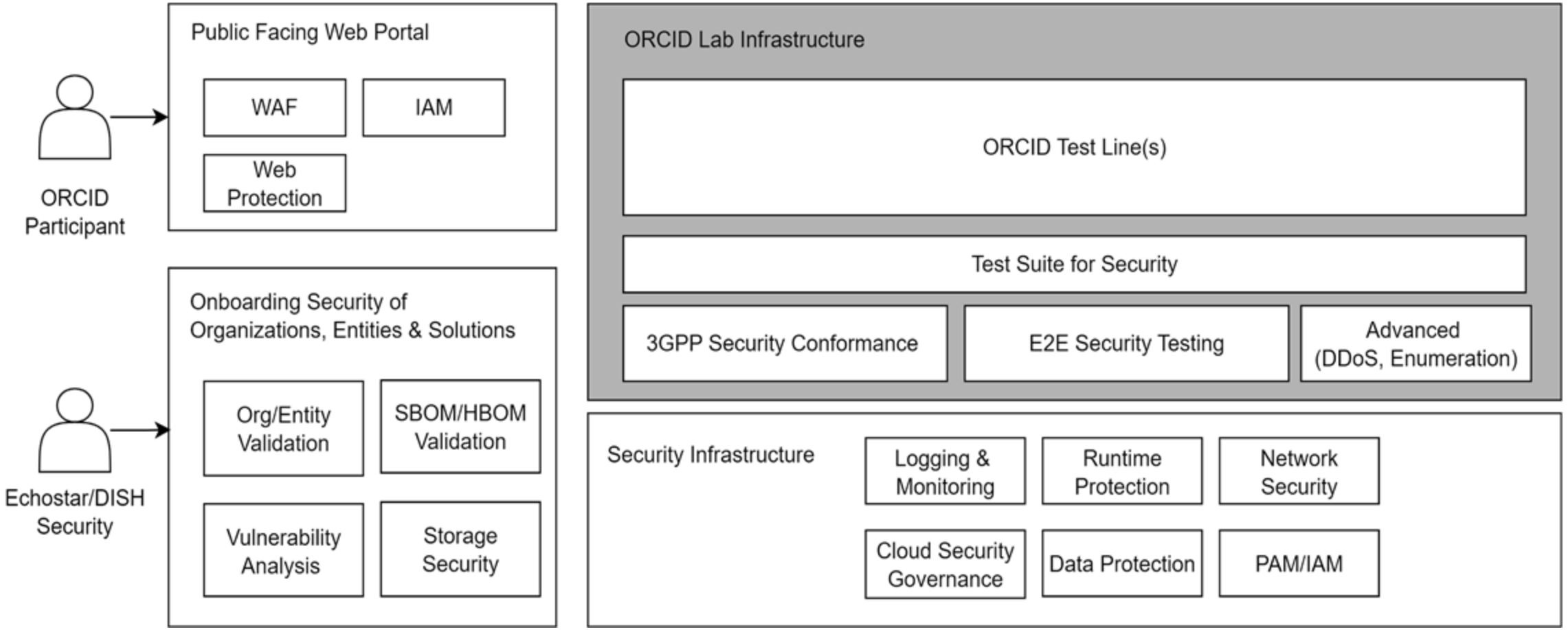
Advanced Threat Detection: Emphasizes proactive detection and response to security threats, using cutting-edge techniques to safeguard against potential breaches in O-RAN deployments.

Field Testing Integration: Combines lab-based evaluations with real-world field testing, ensuring that security measures are robust enough for commercial-grade deployments in live networks.

Web Portal: ORCID's web portal is active and can be accessed at orcid.us.

EchoStar/DISH - ORCID

Security Overview for ORCID



Q&A

PWSCIF

NTIA

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

THANK YOU

Brian Gomez
Federal Program Officer

bgomez@ntia.gov

https://www.ntia.gov/program/innovation-fund