NRL BAA Announcement
55-15-03

HIGH ASSURANCE ENGINEERING AND COMPUTING

The Center for High Assurance Computer Systems of the Naval Research Laboratory (NRL) is seeking white papers for innovative research, advanced system concepts and security architectures, and the development of prototypes, new analysis tools and techniques in the areas of information assurance (IA), cyber security, software engineering, mobile system security, and real-time systems. Current and anticipated areas of research focus include:

A. Communications Security (COMSEC) Systems

1. Advanced Cryptographic Technologies – We are interested in the research and development of advanced cryptographic technologies for the Cryptographic Modernization Initiative (CMI), that include but are not limited to, software-based cryptography, secure kernel development for embedded real-time environments supporting MILS and MLS, cryptographic interoperability specifications for modern cryptographic waveforms, software definable radio architectures, modernized/dispensable cryptographic devices for the tactical edge, and modeling and emulation of high speed secure cryptographic techniques.
2. Key Distribution Technologies – We are interested in the research and development of net-centric key distribution systems. Additionally, we are interested in secure key management architectures and advanced key management techniques, such as key net broadcast, group key concepts, quantum cryptography for COMSEC and secure key distribution, and integrated key/mission planning.
3. IA Enabling Technologies – We are interested in innovative solutions and developing IA enabling technologies in a broad spectrum of research areas that include, but are not limited to, network threat visualization mapping, secureBIOS/secure hardware platform/secure root of trust technologies, trusted execution flow and data filtering frameworks, and security enhanced/trusted operating system (OS) development (including, not limited to SELinux policy development).
4. Guarding Solutions – We are interested in the research and development of high assurance Cross Domain Solutions (CDS) to support assured information sharing, e.g., security policy management across disparate enclaves/domains. Likewise, we are interested in the research and development of secure gateway technology and new analysis tools and techniques for enabling remote monitoring/administration/configuration of such security devices.

B. Computer Security

1. Security Architecture – We are interested in the design and development of security architectures for enterprise systems. Federated identity management systems and access control solutions for data sharing are of particular interest. In addition, we are interested in data protection mechanisms and vulnerability assessments of systems.

2. Application Security – We are interested in innovative solutions and developing practical approaches that enhance and apply security to Service Oriented Architectures (SOA). Emphasis will be placed on security ontologies for machine-understandability, automated machine understandable security policies and tools, application-specific security monitoring, and flexible run-time binding to enhance survivability. Techniques, tools, and solutions for automatic web service composition, as well as cross-domain web service discovery and invocation for multilevel secure SOA are also of interest.

3. High-assurance Software and Safe Execution Environments – We are interested in software engineering methods, processes, and tools that are required to build high-assurance software. Additionally, we are interested in creating a safe software execution environment by using virtualization techniques to prevent failure propagation.

C. Network Security

1. Computer Network Defense – We are interested in the research and development of high assurance network security architectures and solutions (e.g., components, toolkits, equipment, software, and systems). We are interested in the development of tools and solutions for security information, configuration management, and event management. Emphasis on providing a single, holistic view of network health and status, aggregating data feeds from diverse sources, and optimization of network monitoring processes is of particular interest. Additionally, we are interested in development of tools, techniques, and solutions for network intrusion detection, as well as visualization capabilities to dynamically and visually display network situational awareness.

2. Malicious Code Analysis – We are interested in developing methods, tools, solutions for malicious code analysis, reverse code engineering, and other anti-forensic/anti-reversing techniques. The customization and maintenance of malware analysis tools, the application of knowledge of malicious code trends and concepts, and diverse reporting capabilities, such as compilation of malware research findings and identification of unique malware characteristics are also of interest. Additionally, we are interested in scrutinization of coding techniques, language usage/proficiency, and file format properties to identify the level of code sophistication and potential origin are also of interest.

D. Modern Mobile and Wireless Communications Systems Security

1. Discovery and Vulnerability Analysis – We are interested in tools and techniques for wireless network discovery in support of computer network defense and for the visualization of wireless networks using Geographic Information Systems (GIS).

2. Wireless Security Protocols – We are interested in the research of next generation wireless communications and security-enabled protocols suitable for operation over heterogeneous networks. Novel analysis techniques to assess network and security performance of secure wireless protocols are also of particular interest.

3. Next Generation Wireless Networks & Components – We are interested in security engineering and research for next generation mobile ad hoc networks. This includes, but is not limited to emulation and simulation environments for next generation wireless networks; traffic analysis in

support of anonymization of next generation wireless networks; cognitive radio technology; and security of cognitive and software defined radios.

4. Geo-location Technologies – We are interested geo-location techniques and technologies for wireless transmitters, including Time Difference of Arrival (TDoA), Angle of Arrival (AoA) and received signal strength-based techniques. Phased array antennas and smart antennas in support of mobile, dynamic communications and information operations systems are of particular interest.

E. Software Engineering

1. Software Development and Analysis – We are interested in the development of mathematically based methods, models, algorithms, and theories supporting both the construction as well as the analysis of software at different levels of abstraction from requirements through binary code. Techniques, tools, and solutions for fault-tolerant computing, real-time computing, hardware/software co-design, secure software construction & analysis, and binary analysis is also of interest.

2. Middleware for Secure and Dependable Distributed Systems – We are interested in the research and development of reconfigurable and secure middleware that includes, but is not limited to, transformational code development, multi-agent systems, agent-oriented software engineering, and the formal analysis of software engineering artifacts.

Address White Papers (WP) to 5540info@ccs.nrl.navy.mil. Allow one month before requesting confirmation of receipt of WP, if confirmation is desired. Substantive contact should not take place prior to evaluation of a WP by NRL. If necessary, NRL will initiate substantive contact.