Cyber System Exploitation Engineer

The Cyber System Assessments Group provides the U.S. government with independent assessments of cyber systems and capabilities. These assessments are accomplished through the research and development of unique, cutting-edge technical capabilities for understanding, testing, assessing, and analyzing cyber technologies. In addition to the principal mission of planning, constructing, supporting, and executing testing and evaluation activities of cyber capabilities, the group also focuses on red-teaming to identify weaknesses in U.S. systems and characterization of adversary capabilities. The group achieves success through excellence and experience in core technical competencies, including the planning and execution of cyber evaluations, development of realistic, high-fidelity test environments to model the Internet and networks of interest, modeling of adversary capabilities, development of threat surrogates, low-level systems analysis for vulnerability discovery and malicious software analysis, low-observable system instrumentation and forensic analysis, and reverse engineering.

The selected candidate will join a team of experts and contribute to the development of tools and techniques for software or hardware cyber security or cyber capability development, and participate in software or hardware system reverse engineering and exploitation. We define system exploitation as gaining and maintaining unauthorized control over a system. Principal areas of research include cyber tool development and system analysis of offensive or defensive cyber tools and systems, automated vulnerability discovery, reverse engineering, software protection mechanisms, static analysis and dynamic instrumentation. The selectee will effectively communicate their work to non-domain experts through writing, public speaking, and hands-on training sessions.

Requirements:
Bachelor’s in Computer Science, Computer Engineering or related discipline. Proficiency programming a high level language, such as Java, or a systems programming language, such as C, as well as one or more scripting languages, such as Python, is required. Understanding of an instruction set architecture (such as x86), operating systems, or virtualization.

Desired Skills:
Experience with any of the following is desired:

- Operating system internals
- Driver development
- Network protocols
- Virtualization
- Computer security
- Vulnerability assessment
- Measurement and metrics
- Debugging using WinDbg or similar tools,
- Static analysis using IDAPro or similar tools
- SAT/SMT solvers
- Symbolic execution
- Dataflow analysis for compiled binaries
- Binary intermediate representations
- Binary translation
- Vulnerability discovery and analysis
- Virtualization implementation or instrumentation techniques
- Compiler construction
- Embedded systems firmware reverse engineering
- Anti-debugging or anti-instrumentation techniques and countermeasures and detection thereof

MIT Lincoln Laboratory is an Equal Employment Opportunity (EEO) employer. All qualified applicants will receive consideration for employment and will not be discriminated against on the basis of race, color, religion, sex, sexual orientation, gender identity, national origin, age, veteran status, disability status, or genetic information; U.S. citizenship is required.