MIT Lincoln Laboratory

CYBER SECURITY RESEARCH POSITIONS

Information Systems Technology Group

Full-Time Positions

MIT Lincoln Laboratory is a Federally Funded Research and Development Center operated by MIT for the Department of Defense (DoD) and other government agencies. Rapid growth in the Laboratory’s Cyber Security research program has created a number of full-time positions. Positions will be located in Lexington, Massachusetts, approximately 15 miles from Boston. A description of the hiring group and available positions follows.

The group's information operations R&D efforts focus on techniques for protecting from, and detecting and reacting to, intrusions into networked information systems, and for preventing software faults and understanding malicious code that exploits those faults. The group is involved in testing and evaluating the security of U.S. Government systems and networks and in identifying and demonstrating vulnerabilities in such systems. The group is also initiating new R&D in analysis of social networks based on speech, text, and network communications and activities. In each of the group's R&D areas, emphasis is placed on realistic data and experimental evaluation of techniques in test beds.

Interested candidates must apply via the Laboratory’s web site at http://www.ll.mit.edu. At the homepage, click on Employment and select Employment Opportunities. To upload a resume select 06-62- Information Systems Technology in the Group dropdown field and click search. To apply for positions, click on the Job Title and then click on Create a Profile to upload a resume.

CRITICAL NOTE: Mozilla Firefox users will need to enable acceptance of third party cookies to view the full list of openings (Tools/Options/Privacy- check Accept Third Party Cookies).

Due to the nature of the work, all positions require US Citizenship.

#1623 – The Computer Security Architect will work with a team to conduct research and development in the areas of architectures for cyber operations and analysis of computer network defenses, computer network exploitation, and computer network attack tools and systems. Will analyze current DoD cyber systems, identify gaps and
weaknesses, develop unifying architecture, develop & evaluate qualitative metrics of
mission performance, and lead prototyping of key architectural components.
Requirements: PhD in Applied Mathematics, Computer Engineering, or Computer
Science. In lieu of a PhD, an MS with 3-5 years of experience in software engineering
will be considered. Must be able to design, implement, test, and debug net-centric
software and contribute to the formulation of overall architectures and approaches for the
creation of cyber command and control systems for the DoD. Must be able to propose
and explore new techniques and technologies and be able to design, develop, test and
validate these new capabilities. Familiarity with NCES and related initiatives is useful.
Strong communication skills with sponsors and other research sites are essential.
Desired Skills: Knowledge of C, C++, Java, Python, and Perl is highly desired.
Experience with any combination of the following is desired: system-level software,
operating system internals, distributed systems, network protocols, automation
techniques, virtualization, visualization, computer security, vulnerability assessment,
machine learning, pattern classification, statistical models, Markov models, and
regression analysis.

#1559 - The Malicious Code Analysis Researcher will participate in ongoing research
into novel algorithms and techniques for understanding programs containing both
intentional and unintentional malicious behaviors. Some of the work will involve
designing and building systems to detect these behaviors, unassisted by an analyst. Other
work will be in the area of building tools that enable deeper or faster human analysis. The
tools involved will incorporate and extend existing static and dynamic analyses, so it will
be necessary to be able to work with an established code base. However, the ideal
candidate will propose and investigate new approaches when appropriate, where
investigation includes everything from invention and design through implementation and
testing. The ability to make progress independently is extremely valued, but much of the
work will also require strong collaborative skills. Requirements: PhD in Computer
Science, Computer Engineering or another related discipline with experience in software
development. In lieu of a PhD, a MS and 3 years of directly related experience will be
considered. Extensive previous experience with at least one of the following is required:
static analysis, dynamic analysis, compiler internals, systems programming, malware
analysis, or x86 assembly. Strong programming skills in C as well as a mainstream
scripting language such as Python or Perl are additionally required. Willingness to apply
for or possession of an elevated clearance is desired.

#1558 – The Malicious Code Analysis Engineer will work with a team to conduct
research and development in the areas of malicious software collection, development and
analysis. The successful candidate will work on reverse engineering of existing malware
and creating techniques to help automate reverse engineering, and/or analysis of
malware. Requirements: MS in Computer Science, Computer Engineering or another
related discipline with 3-5 years of experience. In lieu of a MS, a BS and 5+ years of
directly related experience will be considered. Knowledge of x86 assembly and IDA Pro,
Immunity Debugger, OllyDbg, or similar tools. Must be able to unpack, analyze, and
understand unknown binaries. Must be able to understand state of the art detection,
forensic, and other defensive tools and be able to analyze and understand their
weaknesses. Candidate must be familiar with Operating Systems internals and with anti-
Debugging and anti-instrumentation techniques and countermeasures. Familiarity with Python, Ruby, C/C++ as well as with network protocols, file formats, compiler idioms, and virtualization technology is highly desired. Experience with penetration testing, vulnerability discovery, and/or exploit development is a plus. Willingness to apply for or possession of an elevated clearance is also desired.

**#1398 – Cyber Architect/Analyst** will work with a team to conduct research and development in the areas of architectures for cyber operations and analysis of computer network defenses, computer network exploitation, and computer network attack tools and systems. Will analyze current DoD cyber systems, identify gaps and weaknesses, develop unifying architecture, develop & evaluate qualitative metrics of mission performance, and lead prototyping of key architectural components. Requirements: PhD in Applied Mathematics, Computer Engineering, or Computer Science. In lieu of a PhD, an MS with 3-5 years of experience in software engineering will be considered. Must be able to design, implement, test, and debug net-centric software and contribute to the formulation of overall architectures and approaches for the creation of cyber command and control systems for the DoD. Must be able to propose and explore new techniques and technologies and be able to design, develop, test and validate these new capabilities. Familiarity with NCES and related initiatives is useful. Strong communication skills with sponsors and other research sites are essential. Desired Skills: Knowledge of C, C++, Java, Python, and Perl is highly desired. Experience with any combination of the following is desired: system-level software, operating system internals, distributed systems, network protocols, automation techniques, virtualization, visualization, computer security, vulnerability assessment, machine learning, pattern classification, statistical models, Markov models, and regression analysis.

**#1204 – Cyber Test Engineer** will work with a team to conduct research and development in the areas of test-bed development and program evaluation of computer network defenses, computer network exploitation, and computer network attack tools and systems. The successful candidate will work on developing models of user and network behavior as well as metrics to enable quantitative testing in realistic environments. Requirements: MS in Applied Mathematics, Computer Engineering, or Computer Science. In lieu of a MS, a BS with 3-5 years of experience in software engineering will be considered. Must be able to design, implement, test, and debug complex cyber attack software and contribute to the formulation of overall architectures and approaches for the creation of cyber attack systems in mobile environments. Must be able to propose and explore new techniques and technologies and be able to design, develop, test and validate these new capabilities. Familiarity with the DETER or EMULAB test beds is useful. Strong communication skills with sponsors and other research sites are essential. Desired Skills: Knowledge of C, C++, Java, Python, and Perl is highly desired. Experience with any combination of the following is desired: system-level software, operating system internals, distributed systems, network protocols, automation techniques, virtualization, visualization, computer security, vulnerability assessment, machine learning, pattern classification, statistical models, Markov models, and regression analysis.
#1197 – Cyber Test Engineer will work with a team to conduct research and development in the areas of test-bed development and program evaluation of computer network defenses, computer network exploitation, and computer network attack tools and systems. The successful candidate will work on developing models of user and network behavior as well as metrics to enable quantitative testing in realistic environments. Requirements: BS in Applied Mathematics, Computer Engineering, or Computer Science. Must be able to design, implement, test, and debug complex cyber attack software and contribute to the formulation of overall architectures and approaches for the creation of cyber attack systems in mobile environments. Must be able to propose and explore new techniques and technologies and be able to design, develop, test and validate these new capabilities. Familiarity with the DETER or EMULAB test beds is useful. Demonstrated strong communication skills with sponsors and other research sites are desired. Desired Skills: Knowledge of C, C++, Java, Python, and Perl is highly desired. Experience with any combination of the following is desired: system-level software, operating system internals, distributed systems, network protocols, automation techniques, virtualization, computer security, vulnerability assessment, machine learning, pattern classification, statistical models, Markov models, and regression analysis.

#1172 – The Computer Security Architect will work with a team to conduct research and development in the areas of architectures for cyber operations and analysis of computer network defenses, computer network exploitation, and computer network attack tools and systems. Will analyze current DoD cyber systems, identify gaps and weaknesses, develop unifying architecture, develop & evaluate qualitative metrics of mission performance, and lead prototyping of key architectural components. Requirements: PhD in Applied Mathematics, Computer Engineering, or Computer Science. In lieu of a PhD, an MS with 3-5 years of experience in software engineering will be considered. Must be able to design, implement, test, and debug net-centric software and contribute to the formulation of overall architectures and approaches for the creation of cyber command and control systems for the DoD. Must be able to propose and explore new techniques and technologies and be able to design, develop, test and validate these new capabilities. Familiarity with NCES and related initiatives is useful. Strong communication skills with sponsors and other research sites are essential. Desired Skills: Knowledge of C, C++, Java, Python, and Perl is highly desired. Experience with any combination of the following is desired: system-level software, operating system internals, distributed systems, network protocols, automation techniques, virtualization, visualization, computer security, vulnerability assessment, machine learning, pattern classification, statistical models, Markov models, and regression analysis.

# 837 – The Computer Network Risk Assessment Engineer will work with a team to design and develop tools that generate and use attack graphs to measure and improve the security of enterprise networks. Tasks could include (1) Analyze router configuration files and outputs of network vulnerability scanners to extract important information, (2) Enhance algorithms that compute host-to-host reachability and attack graphs, (3) Develop algorithms that analyze attack graphs to compute security metrics and make recommendations to improve security, (4) Generate graphical displays of networks and
attack graphs, (5) Enhance and extend an existing interactive graphical user interface, and
(6) Analyze new tools that characterize security on individual hosts or network devices
and incorporate information generated from these tools into our current analysis tool.
We're looking for bright and creative people who can work on a team, learn quickly, and
have strong written and verbal communication skills. They should have the ability and
desire to span the range from coding to higher-level research, analysis, and design.
Requirements: MS in Computer Science or Electrical Engineering with experience in
networking and software development. In lieu of an MS, a BS with 3+ years of directly
related experience will be considered. Must be able to propose and explore new
techniques with the ability to design, implement, test, and debug software. Desired
Skills: Experience with user interface design (preferably Java), code development using
C++ and PERL is desired. It would help, but is not necessary, to have an understanding
of algorithms and computational complexity, graph algorithms, host and network
security, TCP and common network services, vulnerability scanners, routers, firewalls,
and current network and host security threats.

#274 – The Computer Network Risk Assessment Engineer will work with a team to
design and develop tools that generate and use attack graphs to measure and improve the
security of enterprise networks. Tasks could include (1) Analyze router configuration
files and outputs of network vulnerability scanners to extract important information, (2)
Enhance algorithms that compute host-to-host reachability and attack graphs, (3) Develop
algorithms that analyze attack graphs to compute security metrics and make
recommendations to improve security, (4) Generate graphical displays of networks and
attack graphs, (5) Enhance and extend an existing interactive graphical user interface, and
(6) Analyze new tools that characterize security on individual hosts or network devices
and incorporate information generated from these tools into our current analysis tool.
We're looking for bright and creative people who can work on a team, learn quickly, and
have strong written and verbal communication skills. They should have the ability and
desire to span the range from coding to higher-level research, analysis, and design.
Requirements: MS in Computer Science or Electrical Engineering with experience in
networking and software development. In lieu of an MS, a BS with 3+ years of directly
related experience will be considered. Must be able to propose and explore new
techniques with the ability to design, implement, test, and debug software. Desired
Skills: Experience with user interface design (preferably Java), code development using
C++ and PERL is desired. It would help, but is not necessary, to have an understanding
of algorithms and computational complexity, graph algorithms, host and network
security, TCP and common network services, vulnerability scanners, routers, firewalls,
and current network and host security threats.

#274 - The Computer Security Visualization Engineer will work with a team to design
and develop analysis and visualization tools for understanding the security and
configuration of a network, as well as the protocols and data flowing over that network.
Tasks range from low-level protocol parsing and analysis, to higher level system
architecture and GUI/presentation issues. Challenges may include dealing with high
volume data; sampling and characterization techniques; storage, aging, and aggregation
of data; prioritization of processing resources; and flexible and configurable presentation of data for multiple audiences. We're looking for bright and creative people who have the ability and desire to span the range from low-level coding to higher-level research, analysis, and design. Requirements: MS in Applied Mathematics or Computer Science with experience in networking and software development. In lieu of an MS, a BS with 3+ years of directly related experience will be considered. Must be able to propose and explore new techniques with the ability to design, implement, test, and debug software. Desired Skills: Experience with user interface design, computer graphics, artificial intelligence, operating systems, distributed systems, and modern, web-based application technologies are desired.

MIT Lincoln Laboratory is committed to diversity and inclusion in the workforce as core values. All employees contribute to an environment founded upon technical excellence and outstanding innovation. The Laboratory recognizes that its continuing success is achieved through the appreciation and support of the diverse talents, ideas, cultures, and experiences of its employees.