MIT Lincoln Laboratory

CYBER SECURITY RESEARCH POSITIONS

Information Systems Technology Group

Summer Research Internships

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

Interested candidates must apply via the Laboratory’s web site at http://www.l2.mit.edu/college/ocampus.html. To view positions, on the Group menu, select 06-62 - Information Systems Technology 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.

The MIT Lincoln Laboratory Information Systems Technology Group is engaged in a wide range of information processing-related projects focusing on speech and language processing and information operations. The group’s speech and language processing R&D efforts include speech recognition, speaker recognition (identification, verification, and authentication), language and dialect identification, word spotting, speech coding, speech and audio signal enhancement, and machine translation. 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 this group’s R&D areas, emphasis is placed on realistic data and experimental evaluation of techniques in test beds.

1497: Secure Group Communication in Dynamic Mission-Critical Environments

The group seeks a Summer Research Program participant to contribute to an ongoing research project in secure group communication in dynamic mission-critical environments. The project involves studying and experimenting with available solutions, as well as designing and prototyping new solutions (Java, C, and C++), which are driven by specific applications and environment characteristics. The successful candidate will have an MS in Electrical Engineering or Computer Science with experience in network programming, practical network security, distributed systems, and cryptography.
1496: Security Architecture Development for a Satellite Terminal
Information security is a key consideration in designing a satellite based communication system. This project will explore the threat model for such a system, and design and develop the security architecture for a satellite terminal. The successful intern will help implement and demonstrate security mechanisms on a prototype satellite terminal. This could involve developing an assured start-up solution for the terminal that guarantees that the terminal components always start-up to a known good state. This will require both high level and systems programming skills. It will require modifications to the application layer as well as the boot-loader and kernel. The intern will get valuable experience in developing the security architecture for a large system and will play an important role in implementing specific security mechanisms for this system. The successful candidate will have an MS degree or be an advanced senior with a major of Computer Science or Computer Engineering with a strong background in systems programming. Network and systems security background a plus.

1495: Hardware/Software Design for Computer Test Infrastructure
Today’s test infrastructures monitor computer systems while consuming resources on the system being tested. As a result, these measurement infrastructures impact the system being measured—so a better approach is needed. This project will explore hardware and software required to perform computer system monitoring for the purpose of understanding the impact of software that performs computer network operations (CNO). The successful intern will work with laboratory personnel to develop equipment and algorithms to periodically sample the memory of a computer system. These samples will be further analyzed to determine the impact and overhead of the CNO software. The successful candidate will have an MS in Electrical or Computer Engineering with familiarity with the x86 instruction set architecture and FPGA design skills. Python programming experience a plus.

1494: Large Scale Network Flow Analysis
Bro-IDS is an intrusion detection system that has been commonly used by many organizations. Unlike SNORT, a popular IDS which operates based on strict rules, Bro has a scripting language which enables more advanced behavior-based IDS methods to be implemented. Historically, both SNORT and Bro have operated on full packet capture data; recently Bro implemented support for Netflow v5. Unfortunately, this support is limited to receiving/reading the flow record and parsing the record into the appropriate fields. None of the detection modules have been appropriately ported to work with flow data. With support from Lincoln Laboratory staff, the successful intern designated for this project will be responsible for developing full flow detection support under the Bro-IDS architecture. The tasks include porting existing modules, implementing new modules based on leading-edge algorithms, and developing file support for reading differently formatted flow databases. The successful candidate will have an MS or be an advanced senior with a major of Electrical Engineering or Computer Science with a strong computer science and networking background with prior work experience.

1493: Modeling and Analysis of Computer and Network Data
Computer networks like the Internet are constantly evolving and the fast pace of change that has characterized their growth over the past 20 years does not appear to be ending soon. New applications, like the World Wide Web in the early 90’s and P2P several years later, appear on the scene and quickly become dominant factors in the network. This has many important implications for developers of simulation tools, emulation environments, and isolated network testbeds, requiring constant re-evaluation and analysis. How realistic are our models of networks and their traffic? Are we modeling the right things? How do different kinds of networks differ from one another? How are they the same? In this project, the successful intern will examine newly-collected data from operational hosts and networks, seeking to answer these questions and more. The successful candidate will have an MS or be an advanced senior with a major in Mathematics, Computer Science or Statistics with a strong statistics or machine learning background. Experience with networks is required.
1492: Dynamically Measuring Network Security
MIT Lincoln Laboratory has developed a tool to import computer network configuration data, automatically construct network topology, generate an attack graph for a specific threat, and create metrics that summarize attacker effort required to capture system assets. This tool’s analyses can be used to compare the effectiveness of alternative countermeasures, to prioritize patching, and to compare the danger posed by different threats. The network picture created can be used to gain a better understanding of a network topology, of how attackers progress through a network, and of how countermeasures protect network components. The successful intern participating in this project would develop NetSPA’s ability to assess overall network security as the network evolves. This could include upgrading the import system to handle real-time updates from network devices, developing visualization techniques to convey the security impact of recent changes, and creating metrics that summarize the network security over time.
The successful candidate will have an MS or be an advanced senior with a major in Electrical Engineering or Computer Science with a strong user interface design background and prior work experience. Experience in networks is required.

1674: Malicious Software Reverse Engineering.
Malicious software takes many forms and can be very difficult to understand. Authors of such software often take great pains to disguise their intent or to deter analysis of their product. This summer project will endeavor to produce an understanding of a collection of malicious software with the goal of deducing the hidden intent in each piece of code. The intern will collaborate with MIT Lincoln Laboratory security professionals using state of the art reverse engineering tools and techniques to identify software as malicious or not, analyze the subtleties and techniques of each malicious sample, and to gain an understanding of the behavioral aspects of the sample.
Advanced students will develop improved tools and techniques for automated and manual analysis. The successful intern will gain both breadth and depth of understanding in the latest techniques for analysis and authorship of malicious software. The successful candidate will be completing his/her senior year or pursuing an MS in electrical engineering, computer science or electrical engineering and computer science. C/C++, Python, or Ruby programming skills are required. Familiarity with any of the following is beneficial: x86 Assembly, binary executable formats, shellcode, packers, operating system internals, IDAPro, OllyDbg, or other binary analysis tools.

*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.*