US Citizenship is required for application.

Apply by sending email to iojobs@ll.mit.edu and attaching your cover letter, resume, and indicating the research or position you’re interested in.

**Project title: Dynamically measuring network security**

**PIs: Kyle Ingols and Matthew Chu**

Desired type of student: MS or an advanced senior with a strong user interface design background and prior work experience.

Required background: User Interface/CS, with some background in networks

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.

A student 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.

**Project title: Modeling and Analysis of Computer and Network Data**

**PI: Charles Wright**

Desired type of student: MS or an advanced senior with a strong statistics or machine learning background and prior work experience.

Required background: Math/CS/Stats, with some background in networks

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, students will examine newly-collected data from operational hosts and networks, seeking to answer these questions and more.
**Project title: Malicious Software Analysis and Reverse Engineering**  
**PI's: Graham Baker and Chris Connelly**  
Desired type of student: MS or Senior Undergraduate  
Required background: CS, EE, or EECS. 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.

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 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 student will collaborate with 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. A successful student will gain both breadth and depth of understanding in the latest techniques for analysis and authorship of malicious software.

**Project title: LARIAT Summer Research Intern**  
**PI: Lee Rossey**

LARIAT is a collection of tools that has been developed over the past 10 years in order to provide network emulation and traffic generation at very high levels of detail for large scale networks. In order to expand the traffic generation capabilities of the LARIAT project we want to investigate the Android platform for cellular phone traffic. The goal is to create instrumentation and automation for the Android platform, and show initial capability on an actual Android development phone. This effort would include learning and developing against the Android SDK, and developing a toolset to instrument and control the system. Possible automation includes, but is not limited to, email, web browsing, text messaging, and phone calls.

The successful candidate will be working towards a BS/MS/PhD in Computer Science or Electrical Engineering with experience in networking and software development. Candidate be able to propose and explore new techniques with the ability to design, implement, test, and debug software.

Experience with software development, algorithm design, or user interface development using C++, PERL, or Java 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.