MIT Lincoln Laboratory is hosting our second Cyber Technology for National Security (CTNS) workshop on Tuesday, June 28 and Wednesday, June 29, 2022. After all of the dramatic changes in work and life routines due to the pandemic, cyber security issues are increasingly important in our ever-changing world. We are planning an in-person event to discuss the threats and opportunities in the evolving cyber landscape.

CTNS is a forum for presentation and discussion of the latest research, prototyping, assessment, and operational uses of cyber technology in the interest of national security with a focus on military and national mission systems. We are preparing a technology-focused program to include talks, demonstrations, hands-on short courses and keynote addresses. The program will include material at the collateral secret and SCI classification levels.

For registration information, please contact CTNS@ll.mit.edu
Fundamentals of Zero Trust (ZT) for the DoD

This course will provide participants with an understanding of Zero Trust (ZT) concepts laid out in a product-agnostic way, giving them ability to cut through product marketing speak and triage their organization’s ZT requirements effectively. ZT is based on the key idea that a system should not implicitly trust any network traffic, device, or user solely based on their physical or logical network location. ZT has become increasingly emphasized within the DoD by high level leadership and the principles are beginning to be applied to many projects. However, definitions of ZT vary, and guidance is still in its infancy. This course will provide participants with an understanding of the basic concepts of ZT, what different reference architectures and guidance documents cover, and how they relate to successful real-world ZT architectures. Several ZT use cases will be covered, providing an insight into how successful organizations have approached implementing ZT. The course will include an exercise in identifying ZT requirements and prioritizing implementation based on an example system. Several other advanced ZT topics will also be covered: a threat centric approach to ZT, ZT trust and policy engines, and utilizing modeling and simulation to evaluate ZT architectures.

Dynamic Analysis using PANDA Emulation

PANDA is the Platform for Architecture-Neutral Dynamic Analysis and it has been in active development at Lincoln for almost a decade, with use-cases ranging from malware analysis to reverse engineering and vulnerability discovery. This introductory class will combine lectures and hands-on-keyboard activities (roughly a 25%-75% mix). We will walk you through what PANDA is, how it works, and what you can do with it. You will set PANDA up to run on your laptop, use it to perform a few stock analyses, and be guided through interpreting the output. Time permitting, we will make a small foray into using the new Python interface to script a simple analysis. Topics covered will include whole-system record/replay, operating system introspection, system call introspection, and taint analysis.

Prerequisites:
Users should bring their own laptops with Docker installed (https://www.docker.com/products/docker-desktop).

Registration: The registration website is now open. We encourage you to register early. To be added to the mailing list or for more information, contact CTNS@ll.mit.edu.
Agenda is tentative. Workshop sessions are CLASSIFIED with clearance instructions available on the registration site.

0700  Check-in and Breakfast

0800  Security Brief
Ms. Holly Mackinnon,
MIT Lincoln Laboratory

0805  Welcome and Administrative Notes
Dr. W. Mark Smith, MIT Lincoln Laboratory

0810  Welcome and Keynote Introduction
Dr. Eric Evans, Director,
MIT Lincoln Laboratory

0815  Workshop Keynote:
Mr. David E. Frederick
Executive Director, USCYBERCOM

0900  A Novel Covert Channel for Packet Switched Networks
Dr. Kevin Bauer, MIT Lincoln Laboratory

0935  THUNDERCLAP Technology Transition to Government SDR Platform
Mr. Sean McCandless,
MIT Lincoln Laboratory

1000  The Threat of Audio Deepfakes
Mr. Robert Dunn, MIT Lincoln Laboratory

1025  Break

1035  AI Applications for Cyber
Mr. Ritesh Patel, MIT Lincoln Laboratory

1100  Tactical Edge Cyber Applications
Dr. Kyle Morrison, MIT Lincoln Laboratory

1125  WEATHERVANE: Remote Internet of Things Compromise Detection
Mr. Ryan Noonan, MIT Lincoln Laboratory

1150  Keynote Introduction
Mr. Stephen B. Rejto, Division Head,
MIT Lincoln Laboratory

1155  Workshop Keynote:
Dr. Robert J. Runser
Technical Director, Research Directorate
National Security Agency

1240  Lunch

1340  Keynote Introduction
Dr. Marc A. Zissman, Associate Division Head,
MIT Lincoln Laboratory

1345  Workshop Keynote:
BG Paul T. Stanton
Commanding General
US Army Cyber Center of Excellence

1430  Data-driven Exploit Prioritization for Augmenting Red Teams (DEPART)
Mr. Kenny Alperin, MIT Lincoln Laboratory

1455  Precision Cyber Discovery of the Electric Grid
Ms. Karen Uttecht, MIT Lincoln Laboratory

1520  Break

1530  Semantic Similarity for Malware Analysis
Ms. Lisa Baer and Mr. Benjamin Dumas,
MIT Lincoln Laboratory

1555  Securing ABMS Data
Ms. Bich Vu, MIT Lincoln Laboratory

1620  Using GANs for Automated Signal Generation
Dr. Pierre Trepagnier, MIT Lincoln Laboratory

1645  Lightning Talks Introduction
Dr. W. Mark Smith, MIT Lincoln Laboratory

Overcoming Analysis Paralysis with Lightweight Cyber Table Tops
Mr. Orton Huang, MIT Lincoln Laboratory

Security Through Formal Reasoning
Dr. Timothy Braje, MIT Lincoln Laboratory

AI for Hardware Design Attribution: Feasibility Study, Rapid Prototyping, and Evaluation
Mr. Stephen Eng, MIT Lincoln Laboratory

1705  Workshop Reception and Poster/Demo Session
**WORKSHOP AGENDA, DAY TWO**

*Wednesday, June 29, 2022*

*Agenda is tentative. Workshop sessions are CLASSIFIED with clearance instructions available on the registration site.*

<table>
<thead>
<tr>
<th>Time</th>
<th>Session</th>
</tr>
</thead>
<tbody>
<tr>
<td>0700</td>
<td>Check-in and Breakfast</td>
</tr>
<tr>
<td>0800</td>
<td><strong>Welcome and Administrative Notes</strong>&lt;br&gt;Dr. W. Mark Smith, <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>0830</td>
<td>Deception Operations&lt;br&gt;Mr. Daniel Shim, <em>Raytheon Technologies</em></td>
</tr>
<tr>
<td>0855</td>
<td><strong>MITLL Zero Trust Strategy</strong>&lt;br&gt;Mr. Jeffrey Gottschalk, <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>0920</td>
<td>Applying the Concepts of Zero Trust to Non-Enterprise Systems&lt;br&gt;Dr. Sandeep Pisharody, <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>0945</td>
<td>Break</td>
</tr>
<tr>
<td>1000</td>
<td><strong>Keynote Introduction</strong>&lt;br&gt;Dr. Eric Evans, <em>Director, MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>1005</td>
<td><strong>Workshop Keynote:</strong>&lt;br&gt;Lt Gen Timothy D. Haugh&lt;br&gt;<em>Commander, 16th Air Force</em></td>
</tr>
<tr>
<td>1050</td>
<td>Stopping Kernel Hacks with HAKC&lt;br&gt;Dr. Nathan Burow, <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>1115</td>
<td>Automatic Cryptographic Data-Centric Security&lt;br&gt;Dr. Tyler Kaczmarek, <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>1140</td>
<td>Assessing and Mitigating Disclosure Risk in Datasets&lt;br&gt;Mr. Evan Young, <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>1205</td>
<td><strong>Lunch</strong></td>
</tr>
<tr>
<td>1305</td>
<td><strong>Keynote Introduction</strong>&lt;br&gt;Dr. Marc A. Zissman, <em>Associate Division Head, MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>1310</td>
<td><strong>Workshop Keynote:</strong>&lt;br&gt;Mr. Neal Ziring&lt;br&gt;<em>Technical Director, Cybersecurity Directorate, National Security Agency</em></td>
</tr>
<tr>
<td>1355</td>
<td>Internal Research and Development (IRAD) Cyber Portfolio at MIT Lincoln Laboratory&lt;br&gt;Dr. David Bigelow, <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>1420</td>
<td><strong>Keylime Tech Transition</strong>&lt;br&gt;(Story Plus Lessons Learned)&lt;br&gt;Dr. Charles Munson, <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>1445</td>
<td><strong>MITLL Counter Influence Operations Study</strong>&lt;br&gt;Dr. Marc Zissman, <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>1510–1740</td>
<td><strong>Short Courses</strong></td>
</tr>
<tr>
<td>S2-222</td>
<td>Fundamentals of Zero Trust (ZT) for the DoD&lt;br&gt;Ms. Karen Uttecht, et al., <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>TBD</td>
<td>Dynamic Analysis Using PANDA Emulation&lt;br&gt;Mr. Tim Leek, <em>MIT Lincoln Laboratory</em></td>
</tr>
<tr>
<td>1740</td>
<td><strong>Adjourn</strong></td>
</tr>
</tbody>
</table>

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited. This material is based upon work supported by the United States Air Force under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Air Force.