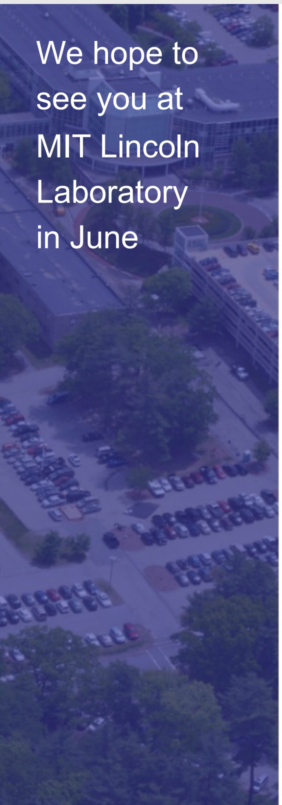
Cyber Technology for National Security 2022

REGISTRATION NOW OPEN!

You are invited to MIT Lincoln Laboratory's annual Cyber Technology for National Security (CTNS) workshop, 28–29 June, 2022

Keynotes

Mr. David E. Frederick Executive Director, USCYBERCOM	Lt Gen Timothy D. Haugh Commander, 16th Air Force	Dr. Robert J. Runser Technical Director, Research Directorate National Security Agency	BG Paul T. Stanton Commanding General, United States Army Cyber CoE	Mr. Neal Ziring Technical Director, Cybersecurity Directorate National Security Agency



We hope to see you at MIT Lincoln Laboratory in June

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

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

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.

Featured Short Courses

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.

WORKSHOP AGENDA, DAY ONE

Tuesday, June 28, 2022

Cyber Technology
for National Security
2022

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**
Mr. Douglas E. Stetson, *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 **Top 4 Cyber Threats**
Ms. Amanda Olson,
Deputy National Intelligence Officer for Cyber,
National intelligence Council (NIC)

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 **Keynote Introduction**
Mr. Jeffrey Gottschalk, *Assistant Division Head,*
MIT Lincoln Laboratory

1040 **Workshop Keynote**:
BG Paul T. Stanton
Commanding General,
US Army Cyber Center of Excellence

1125 **A Novel Covert Channel for Packet Switched Networks**
Dr. Kevin Bauer, *MIT Lincoln Laboratory*

1150 **Lunch**

1250 **Keynote Introduction**
Mr. Stephen B. Rejto, *Division Head,*
MIT Lincoln Laboratory

1255 **Workshop Keynote:**
Dr. Robert J. Runser
Technical Director, Research Directorate
National Security Agency

1340 **AI Applications for Cyber**
Mr. Ritesh Patel, *MIT Lincoln Laboratory*

1405 **Tactical Edge Cyber Applications**
Dr. Kyle Morrison, *MIT Lincoln Laboratory*

1430 **Changing Classification Level**

1440 **Data-driven Exploit Prioritization for Augmenting Red Teams (DEPART)**
Mr. Kenny Alperin, *MIT Lincoln Laboratory*

1505 **Precision Cyber Discovery of the Electric Grid**
Ms. Karen Uttecht, *MIT Lincoln Laboratory*

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**
Mr. Douglas E. Stetson, *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

Cyber Technology for National Security 2022

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

0700 **Check-in and Breakfast**

0800 **Welcome and Administrative Notes**
Mr. Douglas E. Stetson, *MIT Lincoln Laboratory*

0830 **Deception Operations**
Mr. Daniel Shim, *Raytheon Technologies*

0855 **MITLL Zero Trust Strategy**
Mr. Jeffrey Gottschalk,
MIT Lincoln Laboratory

0920 **Applying the Concepts of Zero Trust to Non-Enterprise Systems**
Dr. Sandeep Pisharody,
MIT Lincoln Laboratory

0945 **Break**

1000 **Keynote Introduction**
Dr. Eric Evans**,** *Director,*
MIT Lincoln Laboratory

1005 **Workshop Keynote:**
Lt Gen Timothy D. Haugh,
Commander, 16th Air Force

1050 **Stopping Kernel Hacks with HAKC**
Dr. Nathan Burow, *MIT Lincoln Laboratory*

1115 **Automatic Cryptographic Data-Centric Security**
Dr. Tyler Kaczmarek, *MIT Lincoln Laboratory*

1140 **Assessing and Mitigating Disclosure Risk in Datasets**
Mr. Evan Young, *MIT Lincoln Laboratory*

1205 **Lunch**

1305 **Keynote Introduction**
Dr. Marc A. Zissman**,** *Associate Division Head,*
MIT Lincoln Laboratory

1310 **Workshop Keynote:**
Mr. Neal Ziring
Technical Director, Cybersecurity Directorate
National Security Agency

1355 **WEATHERVANE: Remote Internet of Things Compromise Detection**
Mr. Ryan Noonan, *MIT Lincoln Laboratory*

1420 **Internal Research and Development (IRAD) Cyber Portfolio at MIT Lincoln Laboratory**
Dr. David Bigelow, *MIT Lincoln Laboratory*

1445 **Keylime Tech Transition (Story Plus Lessons Learned)**
Dr. Charles Munson, *MIT Lincoln Laboratory*

1510 **MITLL Counter Influence Operations Study**
Dr. Marc Zissman, *MIT Lincoln Laboratory*

1535 **Closing Remarks**
Mr. Douglas E. Stetson, *MIT Lincoln Laboratory*

1540–1740 **Short Courses**

S2-222 **Fundamentals of Zero Trust (ZT) for the DoD**
Ms. Karen Uttecht, et al.,
MIT Lincoln Laboratory

TBD **Dynamic Analysis Using PANDA Emulation**
Mr. Tim Leek,
MIT Lincoln Laboratory

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.