MIT MANAGEMENT
SLOAN SCHOOL

Cybersecurity at
MIT Sloan

Cybersecurity at MIT Sloan 2019 IAP Activity

(DRAFT 12/17/18 Subject to change and update)

Tuesday - Friday, January 22 - 25, 2018

Location: E51-335 • Cambridge, MA 02142

CYBERSECURITY INSIGHT

Cybersecurity at MIT Sloan with Kaspersky Labs

AGENDA

January 22, 2019 (Tuesday) Kaspersky Think Security 2019
9:30 am Registration & Continental Breakfast

10:00 am – 11:45 am: Session 1: Think Security: During the first session, researchers from Cybersecurity at MIT Sloan and scientists from Kaspersky Labs will share research from ICS CERT files and new ways of APT hunting.

11:45 am – 12:00 pm Coffee Break

12:00 pm – 1:00 pm Session 1 continues: Right before lunch, the team will share their security maturity model for industrial internet security.

1:00 pm – 2:00 pm: Lunch

2:00 pm – 5:00 pm: Session 2: Capture the Flag: During this session, Kaspersky Labs ICS CERT Team will lead a Capture the Flag competition with prizes for the winning participants. We will walk through key tasks after the competition so everyone leaves with new knowledge about the web, reversing, forensics, and crypto. Knowledge of programming and computer science/engineering useful for this competition. ***Please bring your laptop for this session***

5:00 pm: Adjourn

January 23, 2019 (Wednesday)
9:00 am Registration & Continental Breakfast

9:30 am – 10:00 am Results of the Game from Session 2 and Awarding of Prizes

10:00 am – 12:00 pm Session 3: Inclusion Metrics for Managers: Engineering Accessible Leadership Pathways in Tech Contexts: Robyn Allen, MIT alum and Executive Director with Project Alloy, will lead a talk on discuss inclusion metrics and best practices, from a management perspective, related to retention and promotion of underrepresented engineering talent. Robyn's organization focuses on building a more inclusive technical community by offering financial grants, access to subject matter experts, and other resources to people who are early in their careers and underrepresented in the technology industry. Technical Program Management training often revolves around agile development processes or six sigma practices. How do core technical program management skills naturally lend themselves to creating a more inclusive workplace? Because program managers both create norms (within a team or within an organization) and oversee technical product development, even mid-level managers have the opportunity to impact company-wide inclusion practices.

12:00 pm – 1:00 pm: Lunch

1:00 pm – 4:00 pm: Session 4: Cyber-Physical Systems: In this session, researchers from Cybersecurity at MIT Sloan will share latest thinking on vulnerabilities that can be exploited via cyberattacks and STAMP-Based systems that can capture and manage cybersafety analysis information in cyber-physical systems. In the first part of this session, participants will learn, through practical examples, how to identify vulnerabilities and design mitigation strategies in complex cyber-physical systems using a structured framework based on Systems Thinking (STAMP). Then the session will continue with a brief overview to review the STAMP-based workflow and a brief overview of the types of software tools and features available to begin performing basic cybersafety analysis. Participants can select which tools they are interested in, and can use remaining time to explore them as they work through a basic analysis of a system of their choosing. All feedback will help guide the development of future software features.

> *****If you would like to participate in the STAMP tools session in the second half of the Cyberphysical / Cybersafety session, please bring a Windows machine (or at least Microsoft Office). Participants will work in groups so a laptop is not mandatory to attend.*

4:00 pm: Adjourn

<u>January 24, 2019 (Thursday)</u>
9:00 am Registration & Continental Breakfast

9:15 am – 10:15 am: Session 5: Securing IoT Devices: CAMS researchers have been working on new ways to secure end point devices connected to the internet (IoT) using blockchain and white lists. Participants will learn how this is done and practice with hands on activities to simulate securing IoT devices. ***Please bring your laptop for this session***

10:15 am – 11:15 am: Session 6: Cyber attacks as a service: CAMS researchers will share the latest approaches to understanding the Dark Web. If cyber attacks can be created by linking existing ‘as a service’ offerings together, then attackers need only understand how to access this ecosystem. Participants will learn about this new approach to creating attack vectors and simulate how it can be done.

11:15 am – 11:30 am: Break

11:30 am – 12:30 pm: Session 7: Building a Culture of Cybersecurity: Banca Popolare. Research has shown that people are a key vulnerability for securing organizations from cyber attacks. CAMS researchers have recently written a new case study on the Italian Bank, Banca Popolare di Sondrio, and will debut it in this session. Participants will have the opportunity to discuss what decisions the Bank executives made and how those increased the security profile of the organization.

12:30 pm – 1:15 pm: Lunch

1:15 pm – 2:30 pm: Session 8: How Do You Decide to Spend your Budget? CAMS researchers have built a game to practice managing a cybersecurity investment budget. In this lively interactive session, participants will have the opportunity to spend their budget on activities and products to secure their fictitious organization and then see what results. The game will run in the afternoon, and results and prizes awarded Friday morning.

2:30 pm – 2:45 pm: Break

2:45 pm – 3:45 pm: Session 9: Defense in Depth. CAMS researchers have prepared a session to discuss defense in depth. Single layers of defense are more easily penetrated by the bad guys. How might you build your cybersecurity architecture using layers of defense to protect your organization? In this session we will learn about defense in depth and design an architecture for an organization.

3:45 pm – 4:45 pm: Session 10: Measuring Cybersecurity: There are many methods for measuring how secure an organization is. Some measures look at the network and identify vulnerable endpoints. Others look at organizational factors and measure how vulnerable your team is to phishing exercises. Still others measure risk and the cost to reduce risk. In this session, we will build a framework for measuring and communicating how secure an organization is.

5:00 pm: Adjourn

<u>January 25, 2019 (Friday)</u>
9:00 am Registration & Continental Breakfast

9:15 am – 9:45 am: Results of the Game from Session 8 and Awarding of Prizes

9:45 am – 12:00 pm: Session 11: Securing our WiFi networks. Participants will get a chance to understand how vulnerable today's Wi-Fi networks really are. They will also experience an ethical hacking exercise—a practical evaluation of Wi-Fi network (in-)security using publicly available tools. ***Please bring your laptop for this session***

12:00 pm: Adjourn