MITRE ATT&CK^{TM} and Threat Intelligence

Presenter: Dr. Manikantan Srinivasan

Overview:

This tutorial will give an introduction to cyber security threat hunting and threat intelligence. MITRE ATT&CK™ – a treat hunting model that is rapidly gaining traction in the security industry will be introduced and discussed in detail. The use of MITRE's open source tools i.e., CALDERA and NAVIGATOR developed by MITRE to assist in threat hunting for Enterprises and Mobile will be reviewed. Open source tools from the Unfetter Project developed based on MITRE ATT&CK™ model will be discussed. A Hands-on session using MITRE CALDERA and NAVIGATOR will be carried out to enable the participants gain knowledge of these tools, and how it can be used as part of Red Teaming / Blue Teaming exercises. The tutorial is designed as a full day event, where the first half of the tutorial will build the necessary background and inputs. The second half of the tutorial will be hands-on sessions where teams will work with the MITRE tools, based on guided exercises.

Details:

This tutorial makes no assumption regarding a participant's knowledge on cyber security. Starting with an overview this tutorial will introduce the participants to the essential aspects of cyber security. Building on the basics the participant will be made to appreciate and understand the concept of threat hunting and threat intelligence, the roles of various teams (Red, Blue, and Purple) in enabling effective security assessment, threat detection, and defensive mechanisms.

The next part of the tutorial will focus on the MITRE ATT&CK™ model which is widely and well accepted by the cyber security community. The participants will be introduced in detail to the model, its components and the benefits of the model. The tutorial will then enable the participant to understand and appreciate two tools from MITRE, i.e., MITRE CALDERA and MITRE ATT&CK Navigator.

- CALDERA is an automated adversary emulation system, built on the MITRE ATT&CK™ framework. CALDERA works by attaching abilities to an adversary and running the adversary in an operation.
- The ATT&CK Navigator is designed to provide basic navigation and annotation of ATT&CK matrices. It is a simple and generic tool that one can use to visualize one's defensive coverage, their red/blue team planning, the frequency of detected techniques or anything else one wishes to do. This tool helps in planning, prioritizing and building needful defences on ATT&CK techniques in a prioritized way.

Many tools (commercial and open source) are now evolving/evolved based on MITRE ATT&CK™ model. The tutorial will look at the current offerings from "The Unfetter Project". Unfetter is a community-driven suite of open source tools leveraging the MITRE ATT&CK™ framework, shifting the focus from indicators to a behaviour-based methodology. The tools – Unfetter Discover and Unfetter Analytics enables a cyber security personnel to more effectively assess the risk, advance the security posture, and implement mitigations in a systemic, measurable, and meaningful way.

After necessary background and introductions to the concepts and the scope of the tools (using short demos), the participants will be provided with a guided hands-on experience with MITRE CALDERA, MITRE ATT&CK Navigator. Based on time availability, participants will have a hands-on experience using Unfetter Discover and Unfetter Analytics or detailed demonstration will be provided.

Tutorial outline:

I. Cyber Security Overview
II. MITRE ATT&CK™ Model
III. MITRE Tools – CALDERA, ATTC&K Navigator
IV. Unfetter Project, and project's tools – Unfetter Discover and Unfetter Analytics
V. Hands-on
   a. MITRE CALDERA
   b. MITRE ATT&CK Navigator
   c. Unfetter Project tools

Presenter Biography

Manikantan Srinivasan, Ph.D. is currently an adjunct faculty member in the Computer Science and Engineering Department at Indian Institute of Technology Madras. As part of his current role in Industry, he plays the role of Senior Vice President at Veryx Technologies Private Limited, Chennai and is a Cyber Security consultant at NEC Technologies India Private Limited. His industry experience spans 20+ years in the domain of networking and network security. He is a senior member of IEEE, a Comsoc member and an ACM member.

He obtained his Ph.D. degree (CS&E) with specialization in mobile communications from IIT-Madras in 2018. He obtained his Masters in Engineering (CS&E) degree from IISc Bengaluru in 1994, and his Bachelors in Science (Physics, Electronics and Mathematics) degree from Bengaluru University in 1990.

He co-invented and has filed a patent related to privacy preservation and mutual authentication security protocols for 5G networks. As an author and co-author he has many technical journal and conference publications to his credit. He has authored the chapter "IP Switching and MPLS" in the book "Enterprise Networking: Multilayer Switching and Applications".

His current research interests are in the domain of 5G network virtualization, modelling cyber treats and designing solutions to enable efficient defensive mechanisms.