Attack Specification Language: Domain Specific Language for Dynamic Training in Cyber Range

Cameron Noakes

January 2022

1 Sentence Overview

Identification of how training engagements for cyber professionals have limited capability and propose an attack specific language development using the ATTCK framework to give more information about attack techniques for cyber learning and to help identify and reduce redundancy.

2 ATTACK SPECIFICATION LANGUAGE

ASL is an external domain specification language serving two purposes. ASL is procedure specification and description which involves understanding fully the procedure information to make the functions clearer and more concise. ASL classifies and describes the requirements, dependencies, and any challenges associated with procedures for streamlining the functions.

ASL provides a specification method to help in the development of dynamic threat scenarios for expert training and cyber professional learning as well as helps other functions of the cyber range through procedure specification (to define prototype procedures that are specified after the main source section).

2.1 Procedure Specification

ASL assimilates and presents four types of domain information for procedures. Domain information can help to map out procedures and the overall usage of them to a higher standard. This paper also references the popular and common Windows CVE Eternal Blue for the description used as a reference.

Eternal Blue is an NSA leaked zero-day for exploiting SMB shares on Windows computers which was one of the exploits used in the NHS Health hack (alongside Double Pulsar, also leaked from NSA).

2.2 Classification

To differentiate between procedures and reduce redundancy, it is necessary to uniquely identify and classify the tactic and technique the procedure is implementing and ATT&CK framework does this well by categorising multiple procedures under one technique.

2.3 EVALUATION

The proposed ASL language encapsulates all main aspects of attack and threat scenarios and d produces dynamic training scenarios that can be used for specialized training while avoiding redundancy. The dynamic testing and specialised training can be widely used for the professional development of cyber employees and gives a range of possible attacks underwent.

Mathematics are used for specific algorithmic calculations in relation to the attack scenario simulations such as '. Payoff of finitely repeated games' and more advanced algorithmic mathematics such as Regret Matching (each time or stage of the game, each action is chosen with probability proportional to its regret).

The proposed ASL language was related to the ATT&CK framework and its techniques and procedures which, in turn, developed the language to a higher standard as more in depth dynamic attacks could be developed.

3 Conclusion

Research was conducted and a proposed solution was given to the problem of static attack scenarios to help provide a better professional development of cyber security blue and red, offence and defence skillsets for the industry.

4 What problem does this solve?

The threat scenarios referenced for cyber professional learning and training is static and has limited applicability. Due to the lack of proper representation of procedures and training scenarios used in cyber attacks, it is hard to recognize redundant procedures through an attacker mindset.

5 How do they solve it?

A proposition is made for the development of an Attack Specific Language (ASL) based on the popular ATTCK framework. It provides one representation for all threat scenarios for cyber professional training and learning. This developed attack language will give information about attack techniques in compact ways for easier digestion and learning and help identify and reduce redundancy.

6 How do they assess it?

The proposed ASL language was integrated with attack machines and tested on the cyber range setup (software that facilities online spaces that enable training and exercises of cyber attack responses), the trainer and trainee both interact with the system through the client tier when engaging in the attack scenarios/ attack simulations for training.