Integrating Security Behavior into Attack Simulations

Cameron Noakes

February 2022

1 Sentence Overview

The authors present an approach for integrating user actions of "security behaviour", by mapping SBA to a Meta Attack Language (MAL) based language through the use of ATT&CK framework matrix techniques.

2 Introduction

The researchers discuss how attackers exploiting the controls of power grids, energy providers, and other critical infrastructure often happens and can aim to disrupt the normal order of processes such as the attacks can result in real-world physical damage, like major power outages or city-wide disruptions. One counter measure to address these threats are assessments of the power domain's cyber security.

The researchers cite a paper which identifies key elements of protecting critical infrastructure such as to assess the cyber security of a domain and its entities, the security professionals have to identify vulnerabilities, security-relevant parts must be understood, and potential attacks should be identified for every entity of the infrastructure. From the discussion previous, the use of attack simulations based on system architecture models have been proposed in the cited references.

3 Background

The researchers present the Security Behavior Analysis (SBA) tool that is used in their project to assess the security behavior of organization's employees and

an end result of an explanation of the Vulnerability Assessment (VA) tool that takes the information of the SBA and performs attack simulations to determine choke points in the organization's system architecture.

4 Security Behavior Analysis

The researchers have stated that the Security Behavior Analysis (SBA) Tool has its foundations in the cyber-security culture framework. It co-examines the security factors formulating the external and internal conditions under which individuals perform.

The specific levels within the SBA Tool are analyzed into dimensions, which are then further organized into domains reaching down to a measurable level of analysis.

The Security Behavior Analysis Tool, is described to allow using a variety of assessment techniques, such as surveys, tests and empowers users to evaluate the cyber-security culture of their organizations while securing assets. Identified weaknesses are further elaborated and correlated with possible cyber-threats.

5 Vulnerability Assessment

The VA tool depends on two components:
1) The tool securiCAD that facilitates modeling of concrete architectures and perform attack simulations on them.

2) icsLang based on the MAL framework, which codifies the meta model used in securiCAD.

To bring all the information together of the SBA and VA a mapping from SBA's levels and dimensions to icsLang is necessary. It is mentioned that. The use of icsLang was how securiCAD relies on MAL as underlying meta model, a language framework that combines probabilistic attack and defense graphs with object-oriented modeling, for securiCAD t use the MAL a development of icsLang was used.

The Mapping and relationships from SBA to ATT&CK framework. The researchers aimed to map the derived values of the mitigations to certain mit-

igations in icsLang in which was outlined by 3 key elements for the mapping process discussed which can be seen below:

• One-to-one: There is one value in SBA that can be mapped to one mitigation in ATT&CK. • One-to-many: There is one value in SBA that can be mapped to many mitigations in ATT&CK. • Many-to-one: There are multiple values in SBA that are mapped to one mitigation in ATT&CK.

This was able to allow the researchers to accurately detail the mapping from and to the ATT&CK framework for SBA and icsLang respectively.

6 Conclusion

The researchers wanted to provide an answer to the question 'how security behavior findings can be integrated into attack simulations.' and thus the research in this literature and the proposed solution was modelled and conducted.

The researchers suggested a mapping from SBA, that provides organization specific knowledge about security behavior to the ATT&CK framework. This is followed by the second process of mapping from ATT&CK to icsLang.

7 What problem does this solve?

The researchers wanted to provide an answer to the question 'how security behavior findings can be integrated into attack simulations.' and thus the research in this literature and the proposed solution was modelled and conducted.

8 How do they solve it?

They proposed a two-stepped mapping process, the researchers suggested a mapping from SBA, that provides organization specific knowledge about security behavior to the ATT&CK framework. This is followed by the second process of mapping from ATT&CK to icsLang.

9 How do they assess it?

There was no mention of any evaluation approaches to assess the overall proposed solution.