A.8. Systems Security

Systems Security and Risk Mitigation. Management and mitigation of security risk is an essential component of modern technical and socio-technical systems. This stream will explore identification, management, and mitigation of risks in systems security themes, including security in electronic and information systems, physical systems, and cyber-physical systems.

Lead: Obaid Khan, Khairulzaman Kamarulzaman
Domains: Cybersecurity

Submissions Summary:

1. **Vehicle Diagnostic Security Advancement using an MBSE Approach**
   Full Paper
   Sarah Rudder 1, Enola Technologies, ST. PETERSBURG, FL, United States
2. **Aligning System Engineering and Cyber Security Architecture using the SABSA Framework**
   Paperless Presentations
   Bruce Large 1, Secolve, Sydney, NSW, Australia
3. **Empowering you with ATT&CK+D3FEND. A common language to understandcyber criminals and disrupt the Kill-Chain**
   Paperless Presentations
   Nico Riquelme-Ramirez 1, QInetiQ Australia, Brindabella Business Park, ACT, Australia

20734 Vehicle Diagnostic Security Advancement using an MBSE Approach

Authors
Sarah Rudder 1, Enola Technologies, ST. PETERSBURG, FL, United States
Provided Keywords
security, MBSE, safety, reliability
Natural Language Keywords
analysis, assessment, diagnostic, diagnostics, maintenance, raaml, risk, security, using, vehicle
Presentation format decision
Full Paper - Presentation Preference
Stream submitted
A.8. Systems Security
Stream proposed
A.8. Systems Security

Abstract

Overview

Medium and Heavy-duty (MHD) vehicles often require maintenance and diagnostics during normal operations. Vehicle Diagnostic Adapters (VDAs) are the service tools that connect the vehicle network systems to the diagnostics and maintenance software. These diagnostic tools are intermittently, but frequently connected to the vehicle by a trusted technician, but many security models ignore technicians physically connecting to the vehicle.

Context

VDAs are made by third parties and the specification for them lacks security controls around this operation has prompted the trucking industry to develop new security protocols for diagnostics in the International Organization of Standards (ISO) 14229. In light of the potential security concerns associated with MHD vehicle diagnostics, a Threat Analysis and Risk Assessment (TARA) is presented using Risk Assessment and Analysis Modeling Language (RAAML).

Purpose

This research seeks to understand how RAAML can be utilized to follow a cybersecurity approach in a modeling environment in the context of Systems Engineering (SE) activities throughout the system lifecycle. SE responsibilities that pertain to risk identification, assessment, and management include, but are not limited to, deliverables such as Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA).

Approach

A digital representation of the MHD vehicle diagnostic and maintenance system can be designed using Model-based Systems Engineering (MBSE). The presentation will start with a model-based description of the diagnostics system of interest, then do a deep dive into the threat analysis and risk assessment using RAAML.

Insights

Capturing FMEA and FTA inputs and outputs in the model enables more complete traceability and re-usability, reducing re-work and giving more transparency for risk analysis of the system design.

21305 Aligning System Engineering and Cyber Security Architecture using the SABSA Framework

Authors
Bruce Large 1, Secolve, Sydney, NSW, Australia
Provided Keywords
Natural Language Keywords
architecture, cyber, engineering, framework, overview, present, presentation, sabsa, security, using
Presentation format decision
Paperless - Presentation or Poster
Stream submitted
A.8. Systems Security
Stream proposed
A.8. Systems Security

Abstract

Bruce will present how to Align System Engineering and Cyber Security Architecture using the SABSA framework. This presentation will start with an overview of Enterprise Security Architecture and the SABSA framework. The session will present an overview of the SABSA Matrix and the SABSA life cycle and how it aligns with System Engineering activities. The session will specifically focus on SABSA Attributes and how they relate to the requirements engineering sub process. Finally, this presentation will include a worked example for an OT system using a Cloud SCADA system. A key objective for this presentation is to discuss the ways of working between System Engineers and Cyber Security Architects.

21248 Empowering you with ATT&CK+D3FEND. A common language to understandcyber criminals and disrupt the Kill-Chain

Authors
Nico Riquelme-Ramirez 1, QInetiQ Australia, Brindabella Business Park, ACT, Australia
Provided Keywords
Cybersecurity, Threat Surface, Common language between fron liners - managers - decision makers - shareholders - vendors, Cybersecurity Risks
Natural Language Keywords
approach, att, ck, d3fend, frameworks, participants, security, systems, threat, ttps
Presentation format decision
Paperless - Presentation or Poster
Stream submitted
A.8. Systems Security
Stream proposed
A.8. Systems Security

Abstract

Overview: This session offers practical tools for everyone, from beginners to seasoned information security professionals. By understanding and utilising MITRE's ATT&CK (Adversarial-Tactics-Techniques-and-Common-Knowledge) and D3FEND (Detection-Denial-and-Disruption-Framework-Empowering-Network-Defence) frameworks, participants will gain insights into securing systems using a risk-based and holistic approach to cyber exposure in both Information Technology (IT) and Operational Technology (OT).

Context: In the ever-evolving realm of IT/OT cybersecurity, threats advance faster than organisations can keep up. The ATT&CK+D3FEND frameworks provide an effective approach to understanding and counteracting the Tactics, Techniques, and Procedures (TTPs) used by threat actors. These frameworks are enablers for managing and mitigating security risks in modern technical and socio-technical systems.

Purpose: The presentation shows how ATT&CK+D3FEND offer a common language to guide professionals in current offensive and defensive TTPs. This enables participants to assess current systems and inform development of secure-by-design systems. By mapping and understanding the threat surface, participants will be able to determine how to secure systems and data assets effectively, considering the risk exposure involved.

Approach: The session will use real-world examples of the ATT&CK+D3FEND frameworks to demonstrate their application. The Cybersecurity-and-Infrastructure-Security-Agency (CISA) generated a report explaining how to defend against Volt-Typhoon, a Chinese state-sponsored hacker group. This report, co-authored by the Australian-Signals-Directorate (ASD) and the Australian-Cyber-Security-Centre (ACSC), details how Volt-Typhoon accessed US critical infrastructure over the past five years.

Insights: Participants will learn how to leverage ATT&CK+D3FEND to identify TTPs related to Advanced-Persistent-Threat (APT) groups targeting specific industries, and how to detect and mitigate these TTPs. This knowledge is crucial for enhancing systems security and risk mitigation when it comes to designing and testing systems in the current threat environment. The dual-framework approach of ATT&CK+D3FEND improves chances of preventing breaches, as it is not a matter of IF, but WHEN.