REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05/01/2022	Technical Report	

4. TITLE AND SUBTITLE

Platform Independent Vectors of Techniques (PIVOT): An Approach for System-of-System Attack Path Analysis

5a. CONTRACT NUMBER

FA8702-22-C-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Mario F. Zuniga; Matt Janson;

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

The MITRE Corporation
300 Sentinel Drive, Suite 500 & 600
Annapolis Junction, MD 20701

8. PERFORMING ORGANIZATION REPORT NUMBER

PRS-22-1418

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Fighters and Advanced Aircraft and Bombers Program Executive Offices

10. SPONSOR/MONITOR'S ACRONYM(S)

AFLCMC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

Contact pivot@mitre.org

14. ABSTRACT

MITRE created a concept called Platform Independent Vectors of Techniques (PIVOT), designed to connect multiple ATT&CK matrices based on potential adversary TTPs overlaid on SoS components. PIVOT also identifies the PIVOT points, or components that translate the data from one protocol format to another (e.g., TCP/IP to MILSTD 1553B). These PIVOT points are seldom understood or enumerated, leaving gaps in SoS cyber assessments that could allow an adversary to laterally move across technology domains undetected.

15. SUBJECT TERMS

Computer Security; Modeling and Simulation; PIVOT; ATT&CK; Platform Independent Vectors of Techniques; cyber attacks

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE		6	Susan Carpenito
					19b. TELEPHONE NUMBER *(Include area code)* 781-271-7646

MITRE

MP220278
MITRE PRODUCT

Platform Independent Vectors of Techniques (PIVOT)

An Approach for System-of-System Attack Path Analysis

Sponsor: Fighters and Advanced Aircraft and Bombers Program Executive Offices
Dept. No.: N151
Contract No.: FA8702-21-C-0001
Project No.: 100933.10.100.4JB0.CS0

Annapolis Junction, MD

Authors
Mario F. Zuniga
Matt Janson

May 2022

Acknowledgments

The authors would like to acknowledge multiple contributors towards the research and development of PIVOT. In particular, the authors would like to thank Steve Luke, Amy Robertson, Rory Jennings, Rob Miller, Kristin Esbeck, Adam Bairos, and Jon Salisbury for making this concept a reality.

Overview

Risk analysis for traditional systems security engineering is based on well-defined system and component boundaries. In comparison, assessing the risk of cyber-attacks against systems-of-systems (SoS) poses unique challenges. Cyber assessments for SoS are faced with complex, hyperconnected environments and a diverse set of technology domains with unique architectures, protocols, and embedded technologies.

The MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics, techniques, and procedures (TTP), enables organizations to effectively assess risks, identify security gaps and eliminate vulnerabilities. However, the diverse and complex cyber risk challenges in SoS environments require a tool that systematically leverages the Enterprise, Mobile, and Industrial Control System (ICS) ATT&CK matrices simultaneously to provide an effective evaluation. Additionally, as ATT&CK documents TTPs based on real world observations, embedded systems and real-time operating systems are not addressed in the existing ATT&CK matrices due to a lack of open reporting of cyber-attacks on those technologies.

To address these challenges, MITRE created a concept called Platform Independent Vectors of Techniques (PIVOT), designed to connect multiple ATT&CK matrices based on potential adversary TTPs overlaid on SoS components. PIVOT also identifies the PIVOT points, or components that translate the data from one protocol format to another (e.g., TCP/IP to MIL-STD 1553B). These PIVOT points are seldom understood or enumerated, leaving gaps in SoS cyber assessments that could allow an adversary to laterally move across technology domains undetected.

The multidisciplinary PIVOT effort included a gap analysis of the application of ATT&CK matrices to embedded systems, the creation of a new threat matrix, the design of an informed decision methodology, and validation of this methodology through a real-world use case.

Technical Approach

A gap analysis of the ATT&CK Enterprise, Mobile, and ICS matrices was undertaken to identify the disparities when applied to embedded system environments. The three matrices were combined into a single matrix and each tactic and technique were assessed for their applicability. The TTPs relevant to embedded systems were consolidated into a new matrix called the Embedded System Tactics, Techniques, and Procedures Matrix (ESTM). The gap analysis also revealed the need for a tool capable of assessing multiple cyber threat matrices in relation to each other and a methodology for a conducting a cross-cutting assessment of multiple technology domains.

PIVOT Methodology

The PIVOT methodology and ESTM were designed to seamlessly integrate into cyber assessments by enhancing attack path discovery and identifying what steps could be taken to detect, prevent, or mitigate cyber-attacks by breaking the adversary's attack lifecycle throughout SoS environments.

The steps in the PIVOT methodology are shown below:

1. Conduct mission decomposition
2. Conduct system decomposition
3. Identify mission-critical components and identify components that act as PIVOT points
4. Map attack paths from mission critical component to entry access points and identify the adversarial behavior and TTPs that could be used to perform a cyber-attack
5. Determine what steps could be taken to break the cyber-attack path

PIVOT Use Case

The PIVOT methodology development process started with identifying a real-world use case, the TRITON ICS attack, to model a baseline methodology. The TRITON use case depicts adversary behaviors described using MITRE ATT&CK tactics and techniques spanned multiple ATT&CK matrices within a storyboard format (Ref. Appendix A)[1]. Examples like this exhibit the growing understanding of adversaries leveraging SoS integration to their advantage, by pivoting across technology domains.

The TRITON use case, derived from multiple open sources, demonstrates how leveraging PIVOT as a methodology to integrate multiple cyber threat matrices, enables the proactive identification of potentially unknown attack paths into and within critical operational systems. The TRITON storyboard depicts adversary behaviors, using MITRE ATT&CK for Enterprise Tactics and Techniques, to show how the adversary gained a foothold in the IT infrastructure initially and then pivoted to the ICS environment. At which point, the depiction of the adversary's behavior also changed and was described using MITRE ATT&CK for ICS. Each step that the adversary took is described in the TRITON storyboard by correlating tactics and techniques correlated to system components.

While current cyber assessments focus on well-defined system and component boundaries within specific technology domains, PIVOT seeks to identify weaknesses across those boundaries to provide a more holistic picture of how adversaries may identify and exploit vulnerabilities of these systems.

Summary

PIVOT seeks to integrate multiple ATT&CK matrices and the Embedded System TTP Matrix to identify PIVOT points and generate cross-technology domain attack paths during cyber threat assessments in SoS environments. PIVOT is meant to fill a niche area commonly overlooked in cyber vulnerability assessments and is designed to act as a force multiplier with existing tools, capabilities, or methodologies. Users can take advantage of ATT&CK tools and resources to integrate PIVOT into their specific use-case. If you're interested in learning more about PIVOT, please contact pivot@mitre.org.

[1] Multiple open sources. See Reference List.

Reference

FireEye, TRITON Actor TTP Profile, Custom Attack Tools, Detections, and ATT&CK Mapping, April 10, 2019

US-CERT Malware Analysis Report, MAR-17-352-01 HatMan—Safety System Targeted Malware, February 17, 2019

Dark Reading, Triton/Trisis Attack Was More Widespread Than Publicly Known, January 16, 2019

SCOR, TRITON CYBER ATTACK: HACKERS TARGET THE SAFETY SYSTEMS OF INDUSTRIAL PLANTS, March 6, 2018

CyberArk, Anatomy of the Triton Malware Attack, February 8, 2018

Midnight Blue Labs, Analyzing the TRITON industrial malware, January 16, 2018

FireEye, Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure, December 14, 2017

Dragos, TRISIS Malware, Analysis of Safety System Targeted Malware

Appendix A TRITON ICS Cyber Attack Depiction Using PIVOT

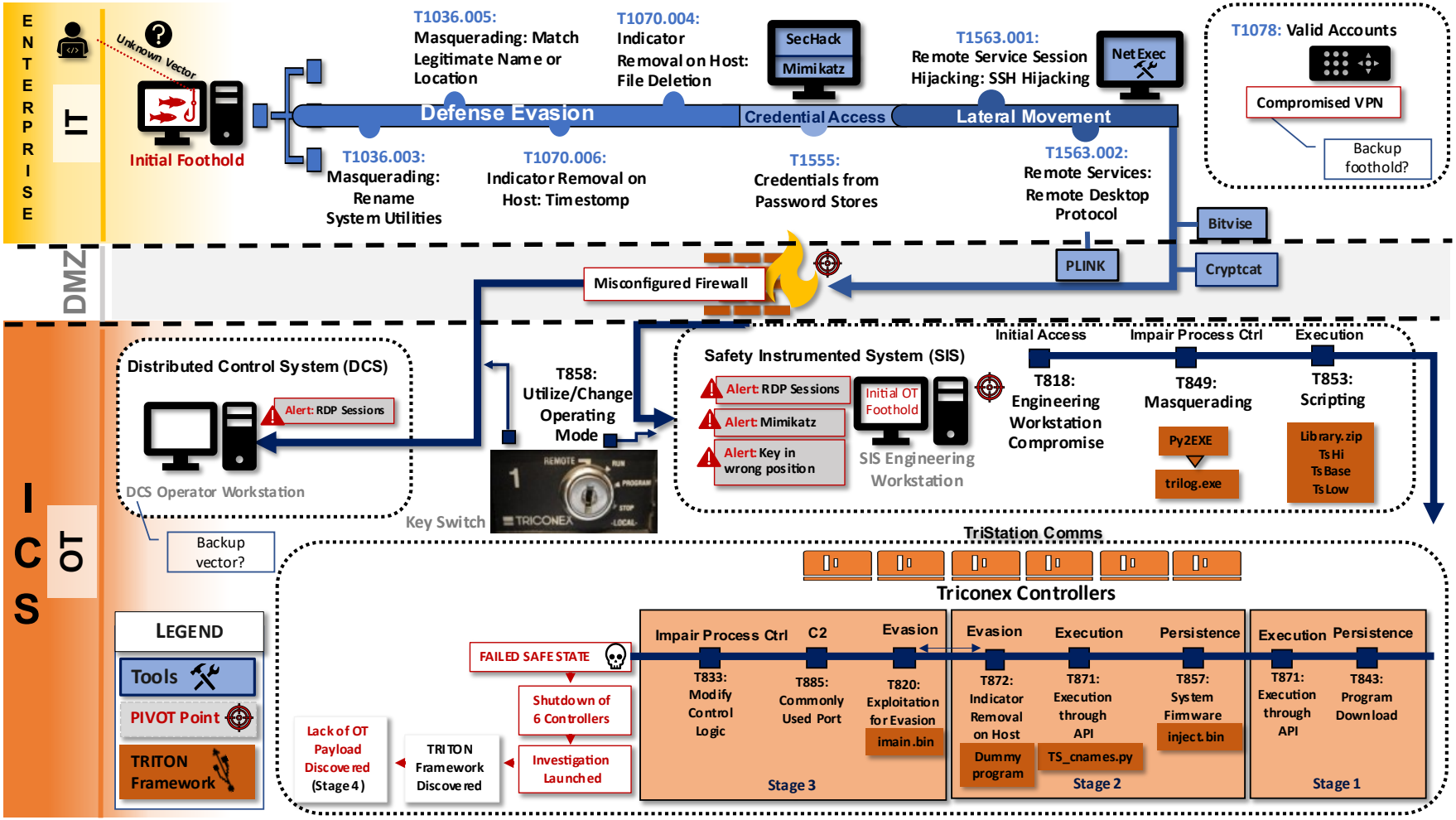

Figure A-1. TRITON ICS Cyber Attack Depiction Using PIVOT