Development of a Bayesian Network to Model Malicious Cyber-Activity in Operational Technology Environments

Lee T. Maccarone[1] **Dennis M. Buede**[2] **Scott T. Bowman**[3] **Charles D. Burdick**[2] **MacLeod C. Bracken**[3]
Jeremy M. Jones[3] **Gabriel A. Weaver**[3]

[1]Sandia National Laboratories, Albuquerque, New Mexico, USA
[2]ITA International, Newport News, Virginia, USA
[3]Idaho National Laboratory, Idaho Falls, Idaho, USA

Abstract

Critical infrastructure and other operational technology (OT) environments face increasing cybersecurity risks from adversarial behavior. This workshop presentation provides insight into the development of a Bayesian network to enhance the perception and comprehension of observable cyber-events caused by malicious activity in OT environments. The core of the Bayesian network is a process model that describes the stages of adversary behavior. The remainder of the model is based on the MITRE ATT&CK® for Industrial Control Systems (ICS) taxonomy, which includes tactics and techniques that may be used by the adversary. The observables provide evidence for adversary behavior through the intermediary technique and tactic nodes. One challenge in constructing this model is a lack of open-source data from cyber-attacks on OT systems. This workshop presentation discusses learning from limited data and the elicitation of expert opinion to construct the conditional probability tables when data is scarce. Finally, this workshop presentation demonstrates the refinement of the most difficult conditional probabilities tables using several forms of sensitivity analyses.

1 INTRODUCTION

Critical infrastructure and other operational technology (OT) environments face increasing cybersecurity risks from adversarial behavior. The Cybersecurity for the Operational Technology Environment (CyOTE) program seeks to enable asset owners and operators (AOOs) to secure their OT environments [Office of CESER, 2021]. The cornerstones of the CyOTE methodology are the perception of observable cyber-events and the comprehension of these observables in broad context including people, processes, and technologies. This cycle of perception and comprehension enables business decisions on whether the observables suggest malicious cyber activity or a benign reliability failure. A Bayesian network is one tool that can be used to assist AOOs in the perception and comprehension of observables.

2 BAYESIAN NETWORK MODEL

This workshop presentation provides insight into the development of a Bayesian network to enhance the perception and comprehension of adversarial cyber-activity in OT environments. Figure 1 shows a simplified version of the model. This simplified version is necessary because the model contains 53 nodes. The core of the Bayesian network is a process model that describes the stages of adversary behavior. The remainder of the model is based on the MITRE ATT&CK® for ICS taxonomy, which includes tactics and techniques [The MITRE Corporation, 2022]. Tactics are objectives that an adversary may seek to accomplish, and techniques are the means by which a tactic is achieved. Tactics may be connected to one, two, or all three phases of adversary behavior as discussed below. The observables provide evidence for adversary behavior through the intermediary technique and tactic nodes.

In the Early Phase, the adversary obtains limited privileges and access to the network, and has partial visibility of the network with a basic user presence. In the Middle Phase, the adversary attempts to escalate privilege and access to the network and expand visibility of the network with capabilities common to power users. In the Late Phase, the adversary often obtains elevated privileges on the network and is able to cause an impact to the asset. This model was constructed with separate nodes for early, middle, and late behavior because these behaviors are not mutually exclusive. Three states characterize each phase of adversary behavior: (1) "None" corresponds to no adversary activity in that phase, (2) "Ongoing" corresponds to active adversary activity in that phase, and (3) "Complete" corresponds to completed adversary activity in that phase.

Accepted for the 16th Bayesian Modelling Applications Workshop (@UAI2022) (BMAW 2022).

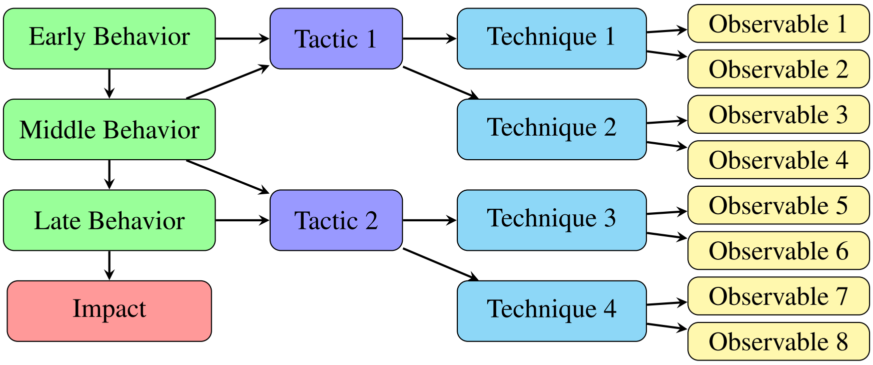

Figure 1: The structure of the Bayesian network.

3 REFINING THE MODEL

One challenge in constructing this model is a lack of open-source data from cyber-attacks on OT systems. This workshop presentation discusses the elicitation of expert opinion to construct the conditional probability tables (CPTs) when data is scarce. A panel of cybersecurity and ICS experts were interviewed to define the CPTs relating techniques to observables. The experts were asked to characterize the frequency of each observable during the normal operation of the OT system and the probability of the observable given an adversary's use of the corresponding technique. The CPTs were then assigned from a predefined set of tables corresponding to the appropriate expert assessment.

Limited data can be leveraged for the definition of the CPTs relating tactics to techniques. This data comes from high-profile historical case studies of cyber-attacks on OT systems. Each technique was assigned a prior distribution, which was then updated based on the frequency with which the technique appeared over the set of case studies.

Finally, this workshop presentation demonstrates the refinement of the most difficult CPTs using coherence judgments based on several forms of sensitivity analyses. The CPTs relating adversary behavior to tactics were first estimated based on a survey of cybersecurity and ICS experts that assessed the frequency of each tactic in each behavior phase. Those CPTs were then adjusted after several sensitivity analyses, the most significant of which was examining the effect of evidence in the adversary behavior nodes on the tactic nodes (i.e., $p(\text{Tactic} = \text{Complete}|\text{Phase} = \text{Complete})$).

4 EKANS CASE STUDY

This model was applied to a case study of the EKANS ransomware in an OT environment. In the summer of 2020, three victim organizations in the manufacturing sector experienced interruptions to operations and loss of revenue due to the EKANS ransomware targeting OT-specific application services. The results presented in this case study are based upon open-source reporting about Honda's experience of the EKANS ransomware Office of CESER [2022].

ID	Technique
T0886	Remote Services
T0859	Valid Accounts
T0849	Masquerading
T0840	Network Connection Enumeration
T0881	Service Stop
T0809	Data Destruction
T0826	Loss of Availability
T0828	Loss of Productivity & Revenue

Table 1: The techniques used in the EKANS ransomware attack.

Table 1 lists the MITRE ATT&CK$^{®}$ for ICS techniques used by the adversary. The adversary gained initial access to the victim's network using the Remote Services technique, then achieved persistence with the Valid Accounts technique, evaded detection using the Masquerading technique, and conducted discovery using the Network Connection Enumeration technique. The triggering event (anomalous event that prompted investigation by the victim) was the Service Stop technique, which stopped systems including data historians and human machine interfaces. This caused the Loss of Availability and Loss of Productivity and Revenue impacts.

A total 21 observables were identified, with 15 observables reported for the precursor techniques, and six observables reported for the triggering event and all subsequent techniques. The results show the probability of ongoing adversary behavior in each of the three phases as the reported observables were perceived. Figure 2 shows an example for the Late Phase of adversary behavior. 150 days before the triggering event (D-150), observables provide limited evidence for adversarial activity in the Late Phase. Little further evidence is obtained until the triggering event at D-0.

The model also demonstrates opportunities for improved comprehension in cases where the observables did not provide strong evidence for the adversary's use of a technique.

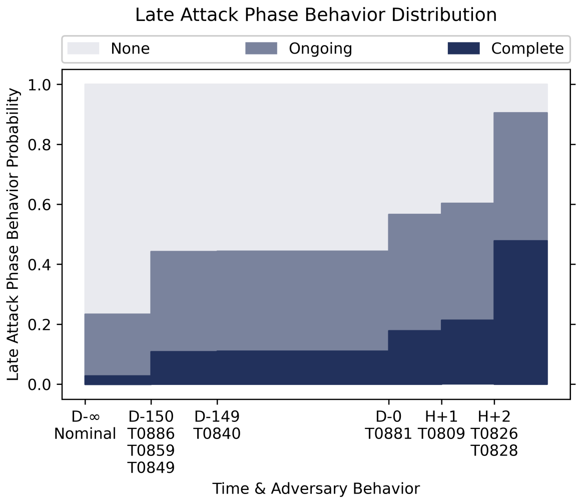

Figure 2: The probability of adversary behavior in the late attack phase given the perception of EKANS observables.

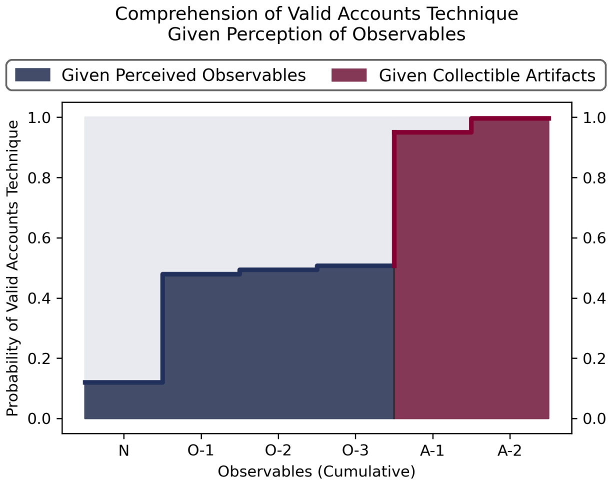

Figure 3: The comprehension of the Valid Accounts technique given the perception of observables.

In these cases, several potential artifacts of the technique were identified which, if collected, could have resulted in improved comprehension of the technique. Figure 3 shows the comprehension of the Valid Accounts technique given the cumulative perception of observables. Descriptions of the observables and artifacts can be found in Table 2. Observables O-1, O-2, and O-3 only provide enough evidence to conclude that there is a roughly even chance of the technique, but artifacts A-1 and A-2 provide enough evidence to conclude that the use of the technique is almost certain.

ID	Description
N	No observables or artifacts
O-1	Accessing domain controller
O-2	RDP authentication
O-3	System log entries
A-1	Permission elevation requests
A-2	Configuration changes

Table 2: The observables and artifacts of the Valid Accounts technique.

Author Contributions

D.M. Buede, L.T. Maccarone, and C.D. Burdick were the primary developers of the model. S.T. Bowman, M.C. Bracken, G.A. Weaver, and J.M. Jones provided cybersecurity and OT systems expertise in developing the model and eliciting expert opinion. L.T. Maccarone was the primary author of this paper, D.M. Buede was the secondary author, and all other authors reviewed the paper.

Acknowledgements

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2022-9824C.

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

The authors gratefully acknowledge the support of Andjelka Kelic, Eric Vugrin, Michael Rowland, and Lon Dawson of Sandia National Laboratories, Michael Chaney, Cory Baker, Jamie Richards, and Samuel Chanoski of Idaho National Laboratory, Tim Westran of Blackmere Consulting, and Dan Gunter of Insane Forensics.

References

Office of CESER. Methodology for Cybersecurity in Operational Technology Environments. Technical report, U.S. Department of Energy, 2021. URL `https://inl.gov/wp-content/uploads/2021/09/CyOTE-Methodology_2021.pdf`.

Office of CESER. Case Study: EKANS Randomware Attack on Honda. Technical report, U.S. Department of Energy, 2022.

The MITRE Corporation. ICS Matrix, 2022. URL `https://attack.mitre.org/matrices/ics/`.