Expansion of ICS Testbed for Security Validation based on MITRE ATT&CK Techniques

Seungoh Choi Jongwon Choi Jeong-Han Yun Byung-Gil Min HyoungChun Kim

The Affiliated Institute of ETRI
Republic of Korea
{sochoi, jwchoi5790, dolgam, bgmin, khche}@nsr.re.kr

Abstract

To respond to cyber threats, all systems in an industrial control system (ICS) should be comprehensively monitored and analyzed. However, there is no dataset to perform this integrated monitoring and analysis study. In previous research, the testbed and dataset represented only one specific area, such as the network or physical level. This imposes limitations upon the testing, validating, and user training of the integrated monitoring system. Therefore, we are developing datasets to test systems that integrate and monitor the ICS operated in a wide range of areas. In this paper, we introduce a method to expand the existing testbed so that information can be collected and monitored during an ICS attack based on the MITRE ATT&CK framework. In addition, to create a dataset for simulating large-scale and long-term attack scenarios, a security dataset enrichment tool is proposed.

1 Introduction

As industrial control systems (ICSs) become intelligent and digitized, operational technologies (OTs) is being exposed to a multitude of information technology (IT) security threats and complicated attack chains. In BlackEnergy3, the adversary persistently attempted to attack the ICS by residing in the target environment for six months or more for reconnaissance [11] [2]. To proactively respond to such sophisticated attacks, it is required to detect abnormalities and threats by continuously monitoring all levels in the ICS.

We are currently working on the development of a security monitoring system that allows ingesting and analyzing various data to gain security visibility into the ICS environment. To achieve full coverage, we aim to identify an event of interest (EoI) that is obtained from various data sources, such as system, network, and control device logs.

Data obtained from the actual operating environment are ideally suited for ICS security monitoring and analysis. However, actual data are difficult to obtain owing to availability issues in the ICS operating environment. Even if the data are available, a lot of information must be deleted or modified owing to confidentiality issues. Further limitations arise when validating and testing elaborate security systems because obtaining attack-related data is challenging [6].

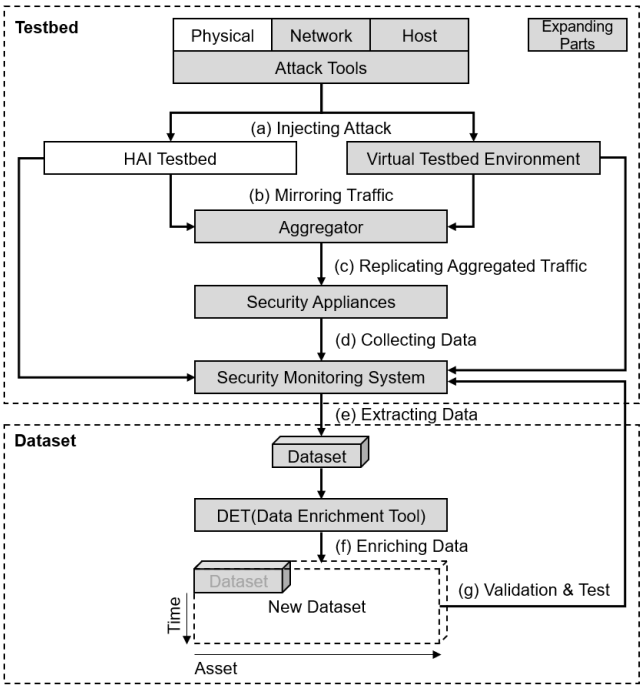

Figure 1: Framework to expand testbed and dataset

Existing testbeds and datasets mostly include network traffic or operation information because attack scenarios typically target a specific area or system [10] [14]. Moreover, testbeds are not provided as integrated datasets and the type of information in them may be highly limited [4] [15]. To the best of our knowledge, no dataset consisting of an EoI for all areas of an ICS has been released.

In this study, we expanded the hardware-in-the-loop (HIL)-based augmented ICS (HAI) testbed and dataset to assess the monitoring system under development for different attack

scenarios. It should be noted that the results presented in this paper are of a preliminary nature. Figure 1 illustrates the expansion process of the HAI testbed and dataset. The factors that we focused on in the testbed and dataset development include:

- **Monitoring field selection.** The selection of the fields and collection methods to detect security threats in the control system was achieved by analyzing the MITRE ATT&CK framework. We dealt with fields that are difficult to collect in ICS-related EoI like programmable logic controller (PLC) diagnosis logs as security information, from the data source indicated by MITRE ATT&CK [3].
- **HAI testbed expansion [13].** We built the HAI testbed consisting of a GE turbine system, Emerson boiler system, and Siemens water treatment system. Depending on the attack scenario, the HAI testbed can reproduce and collect changes in the operation information of the control system. We expanded the HAI testbed to collect and process the information of the previously derived fields based on the MITRE ATT&CK framework. In addition, we considered a reconfigurable and scalable architecture for evaluating security systems.
- **Dataset enrichment.** When collecting the dataset from the testbed, there are limitations in terms of the availability of controllers and collection periods. Control system simulators (e.g., PLC simulators) can be used to resolve this problem, however, such simulators only simulate the operational situation and do not generate security information suitable for the attack scenario. To overcome these limitations, we developed a data enrichment tool (DET) that improves dataset scalability in various attack scenarios and modifies previously collected datasets.

The remainder of this paper is organized as follows. Section 2 discusses the background of this study. In Section 3, the analysis of techniques based on MITRE ATT&CK is introduced to identify a monitoring field. The expansion of the HAI testbed to generate datasets based on full-chain attack scenarios is presented in Section 4. In Section 5, the DET to supplement the dataset obtained from the HAI testbed is described. Section 6 concludes the work and discusses the scope of future research.

2 Background

2.1 HAI Testbed

We built the HAI testbed implementing real control systems (i.e., GE turbine and Emerson boiler system) that are widely used in critical infrastructure [13]. To test the processes of individual control systems, feedback is acquired by interlocking each control system based on the dSPACE HIL simulator.

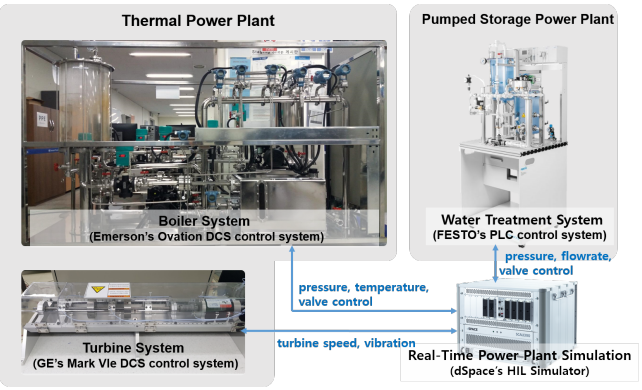

Figure 2: HAI testbed [13]

HAI testbed also provides *a physical attack tool* that can configure and reproduce all possible attack scenarios using the process control loop as the operation changes.

- **Control systems.** The HAI testbed consists of three different types of controllers. The boiler system is composed of a distributed control system (DCS) and field devices to control and measure the pressure, flow, and temperature. The turbine system controls the speed and monitors the vibration of the DCS. The water treatment system is controlled by a PLC using measurement values obtained by sensors.
- **HIL simulator.** The control loops of the three control systems (boiler, turbine, and water treatment) are tightly coupled on a HIL simulator to form a thermal power plant in real-world processes. The HIL simulator controls the field devices in each control system according to the input load required for generation, based on the actual signal values of these control systems.
- **Physical-based attack tool.** This tool implements a physical-based attack scenario that modulates the control output (CO), set point (SP), and process value (PV) based on the process control loop (PCL) using the OLE for process control (OPC). It also generates label data details corresponding to the physical-based attack.

2.2 MITRE ATT&CK Framework

The MITRE ATT&CK framework is a threat knowledge database that contains tactics and techniques utilized by attackers based on real-world observations. When the ATT&CK was announced in 2013, it mainly focused on enterprise environments using Windows but included both Linux and Mac targets. The tactics and techniques used in the reconnaissance and weaponization of the cyber kill chain were materialized as a PRE-ATT&CK. Further, the ATT&CK has been continuously expanding its domain to mobile and ICSs.

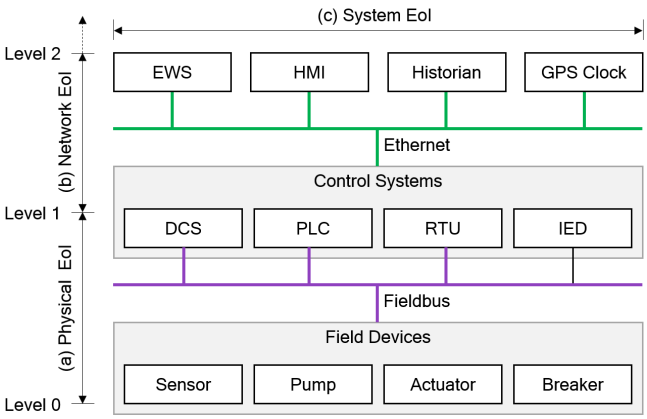

Figure 3: The categories of EoI in ICS

The MITRE ATT&CK provides common knowledge, including tactics and techniques, data sources, detection, and mitigation. In the MITRE ATT&CK for Enterprise, a total of 12 tactics and 266 techniques (excluding duplicates) were described. The tactics represent the target of an attack, and the corresponding techniques refer to the methods used by attackers to achieve their objectives. The MITRE ATT&CK framework has been widely used in several studies regarding adversary emulation, red teaming, behavioral analytics, defensive gap assessment, and cyber threat intelligent (CTI) enrichment.

As high-level threat knowledge databases, Lockheed Martin's cyber kill chain and Microsoft's STRIDE have been proposed [9] [12]. However, these databases cannot effectively explain the relation between the actions and tactical goal of an adversary; therefore, they fail to appropriately respond to all actions [16]. Contrarily, exploit databases often provide proof of concept for exploitation as low-level threat knowledge databases. Nevertheless, simulations are challenging to set up and the obtained results do not match observations. Therefore, the MITRE ATT&CK framework, which is a mid-level threat knowledge, is appropriate for generating a dataset based on realistic attack scenarios.

2.3 EoI Categories in ICS

As shown in Figure 3, the categories of EoI used in this study are classified according to the control system hierarchy of the ISA-99 model adopted from the Purdue Enterprise Reference Architecture (PERA) [1].

First, the network EoI includes network traffic information collected using port mirroring or tapping. Second, the system EoI includes event information generated by systems, such as heterogeneous security appliances (intrusion detection system, firewall, etc.), and network equipment (switch, router, etc.). The data also covers alert information generated within the host and server. Finally, the physical EoI include physical analog and digital signals, that are generated during the control of field devices such as sensors and actuators.

3 Monitoring Field Extraction from MITRE ATT&CK Techniques

Prior to creating a dataset for security research on the ICS, it is necessary to identify what information is needed to detect security threats. For this, we classified the data source according to the attack techniques following on the MITRE ATT&CK framework. We identified the fields that could be extracted from the data source and specified particular fields including the collection methods.

To determine monitoring fields, we set 52 techniques excluding duplicates in ten tactics mapped to 92 Elastic detection rules[1] based on the MITRE ATT&CK for enterprise, as a baseline. Table 1 and Table 2 show the monitoring fields that we selected based on the MITRE ATT&CK techniques.

It was able to specify as a monitoring field to be monitored from 29, which is part of the data sources suggested in the MITRE ATT&CK technique. Even if a data source complies with the detection rules, we confirmed that additional fields might be required for security monitoring. Hereafter, the initial monitoring fields are indicated in italics and the additional monitoring fields are represented in boldface text. Some fields, such as '*netflow.**', are abbreviated using an asterisk for brevity. Wherever possible, we represent the additional monitoring fields according to the Elastic Common Schema (ECS)[2], referenced by the existing Elastic detection rules. When collecting the additional fields, the collectors distributed by Elastic were given priority.

In the following subsections, we considered the EoI category and application domain to derive the monitoring fields at the data source suggested by MITRE ATT&CK.

3.1 Consideration of EoI Categories

As shown in Table 1 and Table 2, system EoI can be obtained from security appliances, network equipment, servers, and hosts. The monitoring fields and collection methods rely on data sources. Because data sources mainly target servers and hosts, other types of system are required to determine the monitoring fields. For example, in case of a data source from the web application firewall T1190 (T819) and the network intrusion detection system T1193 (T865), the *event.** fields should be included in monitoring fields for a security alert.

Network EoI typically contains network traffic information. When capturing a packet from a server or a host, no limitations are imposed on program installation. Contrarily, installing a program on an ICS may be restricted due to availability;

[1]We used Elastic Stack release 7.6.0 retrieved from https://www.elastic.co/guide/en/siem/guide/current/prebuilt-rules.html

[2]https://github.com/elastic/ecs/

therefore, we consider port mirroring on a network switch or tapping to passively capture packets.

3.2 Consideration of Target Domains

Although the target domain of the MITRE ATT&CK framework is different from enterprise and ICS, the data source corresponding to the attack technique is the same at both ICS and enterprise domains. Namely, MITRE ATT&CK for ICS requires additional data sources which are not used for ATT&CK for enterprise. Even with the same data sources between ICS and enterprise domains, it could be a problem to collect arbitrary information from the ICS data source because ICSs have functional gaps compared with the enterprise.

We further analyzed the data source according to the ICS attack scenario by targeting the new tactics, i.e., 'Inhibit Response Function', 'Impair Process Control', and 'Impact' of the MITRE ATT&CK for ICS. As a result, we confirmed that OPC-based log should be collected. When detecting ICS-specific techniques, such as 'Module Firmware (T839)', 'Modify Control Logic (T833)', 'Utilize/Change Operating Mode (T858)', and 'Manipulation of View (T832)', the diagnostic information of the controller and the operational information between the controller and field device must be used as physical data sources.

When selecting monitoring fields from these data sources, it is possible to detect whether the operation mode or control logic have been changed by utilizing existing ECSs, such as *event.created*, *event.action*, *service.state*, *os.version*, *package.version*, and *package.checksum*. However, additional schema definitions, such as *point.name*, *point.type*, and *point.value* (e.g., PIT0001, Analog and 0.3, respectively), are required to extract operation and control information. Therefore, the control device should provide an OPC-based log delivery function or an alternative method [3].

4 Testbed Expansion for Security Visibility on Monitoring Fields

We expanded the HAI testbed as shown in Figure 4 with the aim of creating a dataset containing the monitoring fields. Based on the analysis of the techniques of the MITRE ATT&CK framework, we emphasized the following.

- **Data diversity.** When the testbed is expanded, information must be collected from various data sources. In case of security appliances, as there are fundamental differences in the detection function and appliance performance, the operation of each appliance is not identical under the attack situation. Even if the same attack is detected, the types of logs generated by the security appliances differ. In practice, operators deploy different security appliances depending on their security objectives.

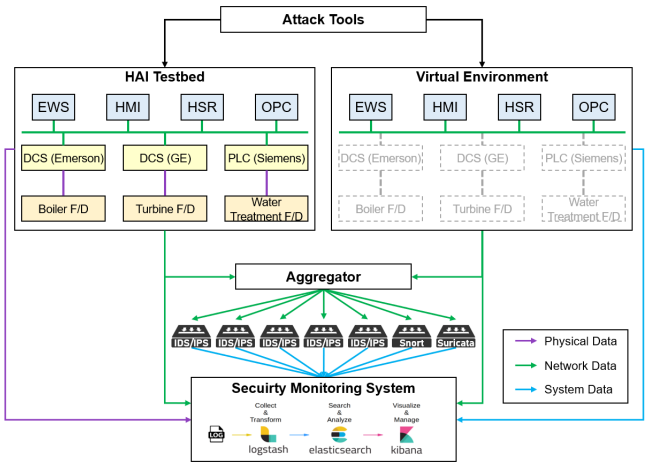

Figure 4: Architecture of our expanded HAI testbed

- **Data ingestion.** Various types of EoI that can be obtained from the components of a testbed should be collected in real-time. Additionally, for research purposes, the monitoring field can be processed and stored as EoI using a common schema. Furthermore, it is possible to search and analyze the stored information for security monitoring with visualization.

- **Attack scenario.** To handle a dataset including all levels of ICS hierarchy, the attack tools can provide a full attack chain for reproducing the attack scenario. Therefore, the scenario on the control system begins with collecting proactive information about the operating environment and executes the attack when a vulnerable service is identified.

- **Time synchronization.** There can be a time difference between devices, such as control systems and security appliances. Strict time synchronization is essential to monitor and analyze control system conditions. If EoI is collected from devices without time synchronization, time-shift problems occur, so that a time series-based analysis cannot be applied in real-time.

4.1 Attack Tools

We implemented three attack tools that take into account the EoI categories. To simulate attack scenarios targeting all areas of ICS, we will synchronize all three attack tools to reproduce attack scenarios in all areas of ICS.

- **Physics-based attack.** Through the *physical attack tool* corresponding to control systems level 0 and 1 included in the HAI testbed, we implemented 14 single attacks that focus on a single physical point among the control output, setpoint, and process value. We also implemented 19 sophisticated attacks that targeted multiple physical points.

Table 1: Selected monitoring fields based on MITRE ATT&CK techniques

Tactics	Techniques (ICS)	EoI category	Data source	Monitoring fields	Collection methods
TA0001	T1190 (T819) Exploit Public-Facing Application	Network	Packet capture	*network.transport*	*Packetbeat, Mirroring*
				destination.port	
				network.direction	
				source.ip	
				destination.ip	
		System	Web application firewall logs	***rule.description***	***Syslog, SNMP***
				rule.name	
			Application logs	***process.name***	***Auditbeat, Winlogbeat, Packetbeat***
				event.action	
				destination.ip	
				network.application	
			Web logs	***http.request.body.content***	***Filebeat, Packetbeat***
				http.request.method	
				http.response.body.content	
				url.full	
				url.query	
TA0002	T1193 (T865) Spearphishing Attachment	Network	Packet capture	***file.extension***	***Packetbeat, Mirroring***
				file.code_signature	
				file.hash	
				pe.imphash	
				network.application	
				source.ip	
				destination.ip	
		System	File monitoring	*event.action*	*Winlogbeat, Auditbeat*
				process.parent.name	
				process.name	
			Network intrusion detection system	***rule.description***	***Syslog, SNMP***
				rule.name	
			Detonation chamber	***event.code***	***Winlogbeat***
			Email gateway	***rule.description***	***Syslog, SNMP***
				rule.name	
			Mail server	***event.action***	***Winlogbeat, Auditbeat, Filebeat***
				log.original	
TA0003	T1136 Create Account	System	Process monitoring	*event.action*	*Winlogbeat, Auditbeat*
				process.name	
				process.parent.name	
			Process command-line parameters	*process.args*	*Winlogbeat, Auditbeat*
				process.command_line	
			Authentication logs	***event.action***	***Winlogbeat, Auditbeat***
				user.group	
				user.name	
			Windows event logs	***event.action***	***Winlogbeat***
TA0004	T1138 Application Shimming	System	Loaded DLLs	***dll.name***	***Winlogbeat, Auditbeat***
				dll.path	
			System calls	***event.name***	***Winlogbeat, Auditbeat***
				event.action	
			Windows registry	***process.name***	***Winlogbeat***
				event.action	
				registry.*	
			Process monitoring	***process.parent.name***	*Winlogbeat, Auditbeat*
				process.name	
				event.code	
			Process command-line parameters	***process.args***	***Winlogbeat, Auditbeat***
				process.command_line	
TA0005	T1064 (T853) Scripting	System	Process monitoring	*process.parent.name*	*Winlogbeat, Auditbeat*
				process.name	
			Process command-line parameters	*event.code*	*Winlogbeat, Auditbeat*
				process.name	
				process.args	
				process.command_line	
			File monitoring	***event.action***	***Auditbeat***

Table 2: Selected monitoring fields based on MITRE ATT&CK techniques (*continued*)

Tactics	Techniques (ICS)	EoI category	Data source	Monitoring fields	Collection methods
TA0006	T1040 (T842) Network Sniffing	Network	Network device logs	***rule.description***	***Syslog, SNMP***
				rule.name	
			Netflow/Enclave netflow	***netflow.****	***Filebeat***
			Host network interface	***event.name***	***Auditbeat***
				event.action	
		System	Process monitoring	*process.name*	*Winlogbeat, Auditbeat*
				event.action	
TA0007	T1057 Process Discovery	System	Process monitoring	*event.code*	*Winlogbeat*
				process.name	
			Process command-line parameters	***process.args***	*Winlogbeat, Auditbeat*
				process.command_line	
TA0008	T1210 (T866) Exploitation of Remote Services	System	Windows error reporting	***event.type***	***Winlogbeat***
				event.action	
			Process monitoring	*event.action*	*Winlogbeat, Packetbeat*
				destination.port	
				prosess.pid	
				destination.ip	
			File monitoring	***event.action***	***Auditbeat***
TA0010	T1048 Exfiltration Over Alternative Protocol	Network	Packet capture	*network.transport*	*Packetbeat, Mirroring*
				destination.port	
				network.direction	
				source.ip	
				destination.ip	
			Network protocol analysis	***event.original***	***Packetbeat, Mirroring***
		System	Netflow/Enclave netflow	***netflow.****	***Filebeat***
			Process use of network	***process.name***	***Winlogbeat, Auditbeat, Packetbeat***
				event.action	
				destination.port	
			Process monitoring	***process.name***	***Winlogbeat, Auditbeat***
				event.action	
			User interface	***process.name***	***Winlogbeat, Auditbeat***
				event.action	
TA0011	T1043 (T885) Commonly Used Port	Network	Packet capture	*network.transport*	*Packetbeat, Mirroring*
				destination.port	
				network.direction	
				source.ip	
				destination.ip	
		System	Netflow/Enclave netflow	***netflow.****	***Filebeat***
			Process use of network	***process.name***	***Winlogbeat, Auditbeat, Packetbeat***
				event.action	
				destination.port	
			Process monitoring	***process.name***	***Winlogbeat, Auditbeat***
				event.action	

- **Network-based attack.** We installed *Ixia's Ixload-Attack* to generate malicious network traffic based on known vulnerabilities between Levels 1 and 2 in ICS. This tool reproduces the attack situation through packet crafting when probing an access control list or a signature-based policy on the appliances. In addition, it reproduces denial of service and distributed denial of service attacks targeting various service types.
- **System-based attack.** Using the *Purple team ATT&CK automation*[3], we built a system-based attack environment for Level 2. This attack tool is a post module of *Metasploit* that reproduces the technique of the MITRE ATT&CK framework and can target various operating system environments (including Windows and Linux). *Msfrpcd* can be used to inject user-defined attack scenarios through remotely command and control the testbed.

[3] https://github.com/praetorian-code/purple-team-attack-automation

4.2 Virtual environment

A direct attack on assets in the testbed during the operation to create datasets can affect testbed availability. When a network-based attack occurs, a performance load may arise because of a preset security function such as storm control. Additionally, if attack traffic is directly injected into the operating and man-

agement systems, such as the operating workstation, problems may occur in the system.

To solve this problem, we built an Exsi-based hypervisor server to form a virtual environment that is physically separated from the HAI testbed and similar to the existing operating environment (i.e., operating system, service, etc.). The virtual environment basically excluded the attack effect when generating the control system attack dataset and facilitated recovery to the situation before the attack. Packetbeat, Auditbeat for Linux, Winlogbeat for Windows, and Filebeat were installed at the virtual host to deliver various data sources to the security monitoring system based on the results of the MITRE ATT&CK analysis [7].

4.3 Aggregator

Security appliances require network traffic to generate security information. We applied the mirroring setting to the network switch in each control system of the HAI testbed as surveillance network traffic to generate an EoI.

To forward the traffic received from each network switch to each security appliance, we deployed an aggregator capable of traffic integration, replication, and distribution. When the mirrored traffic was delivered to the aggregator, the network traffic was simultaneously forwarded to each security appliance via traffic integration and replication.

4.4 Security Appliances

We built five commercial security appliances based on two widely used open-source network intrusion detection systems (Snort and Suricata). We configured whitelist-based rules according to the IP addresses of the operating assets of the HAI testbed. In addition, we applied signature-based rules provided by each appliance.

We activated the log functions at the appliances to generate an EoI. Once a security violation occurs, the security appliances report it to the security monitoring system. At this time, five commercial appliances report via Syslog (514/UDP), while Suricata and Snort provide the content of the log files.

4.5 Security Monitoring System

We developed a security monitoring system using Elastic Stack[4] to selectively collect and process the monitoring fields from the data sources as required by the MITRE ATT&CK techniques for all areas of the ICSs.

The security monitoring system includes a collection module for gathering monitoring fields from various data sources and a process module for normalizing the different field types in a common structure via the ECS. Furthermore, Elasticsearch and Kibana were used for storing the processed data and for querying and visualizing stored data, respectively. To

[4] https://www.elastic.co/products/elastic-stack

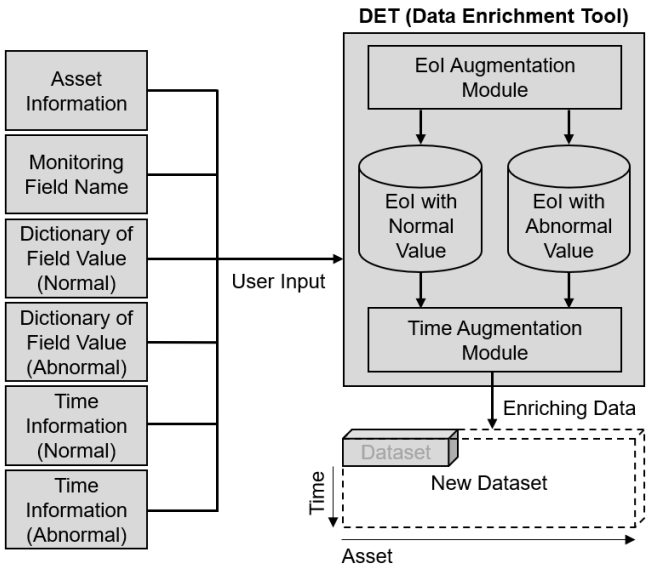

Figure 5: Architecture of the DET

validate our experimental environment, we confirmed that 35 monitoring fields that we selected as EoI were successfully collected and processed from various sources in the expanded HAI testbed.

5 Dataset Enrichment for Scenario Expansion

Recently, cyber-attacks have occurred on various ICS sites, regardless of the industrial field. Therefore, it is necessary to simulate various ICS sites using a single testbed. Although we built the expanded HAI testbed, it remains challenging to simulate all ICS-site attacks with this testbed alone. Further, additional efforts are required for creating a dataset based on a specific scenario; e.g., repeatedly changing the settings of the virtual environment and attack tools. Besides, the sophisticated cyber-attacks targeting ICSs, called advanced persistent threats (APTs), have persisted over a long period of time. This means that the dataset should reveal these threats [5] [8]; however, collecting data over a long period of time for simulations remains inefficient.

To overcome these problems, we implemented the DET, shown in Figure 5, to enrich the dataset created through the expanded HAI testbed. First, through the DET EoI module, a virtual asset can be generated, and a virtual EoI can be generated from the asset. At this time, the virtual asset information and the virtual EoI information are user input values, which are the results of analyzing the existing EoI. It is much more efficient to reproduce EoI by analyzing the characteristics of existing EoI. Additionally, the DET time augmentation module can temporally inflate the existing expanded HAI testbed dataset. Therefore, the DET extends the existing dataset through user input so that it can reproduce a dataset

that reflects the characteristics of the APT over a long period of time.

For this tool to operate, the asset information, monitoring field name, dictionary of field value for normal/abnormal, and time information for normal/abnormal should be applied as inputs by the user. The development of this tool is ongoing, and now the tool works with user input from a security expert or stakeholder. When development is completed in the future, the tool will be updated to enrich the security information by inputting data generated from the testbed and the real-world ICS systems. With this DET, we can simulate various ICS sites and temporally expand datasets, which enables scenario expansion.

5.1 EoI Augmentation

The DET EoI augmentation module virtually adds assets on the testbed for dataset enrichment and generates potential EoI. To this end, the user inputs the asset information, monitoring field name, and dictionary of field value for normal/abnormal.

The asset information refers to the identification of assets to be virtually added and includes the asset name, manufacturer, operating system, and version. The monitoring field name corresponds to the data described in Section 3. Through monitoring, we can select the monitoring fields to be virtually added. the dictionary of field value for normal/abnormal is a dictionary of values that can be stored in the monitoring field. Based on these inputs, the EoI augmentation module generates various EoIs with values. At this time, EoI is classified as normal or abnormal and stored.

5.2 Time Augmentation

The DET generates EoIs of assets according to the time when ICS operates normally or when an attack occurs according to a user-defined scenario. In order to accurately simulate what EoI each asset generates under normal/abnormal situations, the characteristics of EoI generated by the EoI augmentation module and collected in the testbed are utilized.

6 Conclusion and Future work

In this paper, we built a testbed that can collect control system security datasets based on Elastic by analyzing MITRE ATT&CK tactics and techniques. To overcome the limitations of datasets collected in the testbed, we are developing tools to transform and extend the datasets obtained from the testbed according to different user scenarios. In our future work, we intend to develop a dataset, including information from various data sources, that can be used for security monitoring according to the cyber-attack scenarios in ICSs.

References

[1] Pascal Ackerman. *Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems*. Packt Publishing, 2017.

[2] Defense Use Case. Analysis of the cyber attack on the ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 388, 2016.

[3] Jongwon Choi, HyungKwan Kim, Seungoh Choi, Jeong-Han Yun, Byung-Gil Min, and HyoungChun Kim. Vendor-independent monitoring on programmable logic controller status for ICS security log management. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security (AsiaCCS)*, Asia CCS '19, page 682–684. ACM, 2019.

[4] Seungoh Choi, Jeong-Han Yun, and Sin-Kyu Kim. A comparison of ICS datasets for security research based on attack paths. In *The 13th International Conference on Critical Information Infrastructures Security (CRITIS)*, 2018.

[5] Michael K Daly. Advanced persistent threat. *USENIX, Nov*, 4(4):2013–2016, 2009.

[6] Suresh K. Damodaran and Paul D. Rowe. Limitations on observability of effects in cyber-physical systems. In *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security (HotSoS)*, HotSoS '19. ACM, 2019.

[7] Elastic. Beats platform reference. Retrieved July 21, 2020 from https://www.elastic.co/guide/en/beats/libbeat/current/index.html.

[8] Nicolas Falliere, Liam O Murchu, and Eric Chien. W32. stuxnet dossier. *White paper, Symantec Corp., Security Response*, 5(6):29, 2011.

[9] Eric M Hutchins, Michael J Cloppert, and Rohan M Amin. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, 1(1):80, 2011.

[10] A. P. Mathur and N. O. Tippenhauer. SWaT: a water treatment testbed for research and training on ICS security. In *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*, pages 31–36, 2016.

[11] S Raval. Blackenergy a threat to industrial control systems network security. *International Journal of Advance Research in Engineering, Science & Technology (IJAREST)*, 2:12, 2015.

[12] Riccardo Scandariato, Kim Wuyts, and Wouter Joosen. A descriptive study of microsoft's threat modeling technique. *Requir. Eng.*, 20(2):163–180, June 2015.

[13] Hyeok-Ki Shin, Woomyo Lee, Jeong-Han Yun, and HyoungChun Kim. Implementation of programmable CPS testbed for anomaly detection. In *12th USENIX Workshop on Cyber Security Experimentation and Test (CSET 19)*. USENIX Association, August 2019.

[14] Ahnaf Siddiqi, Nils Ole Tippenhauer, Daisuke Mashima, and Binbin Chen. On practical threat scenario testing in an electric power ICS testbed. In *Proceedings of the 4th ACM Workshop on Cyber-Physical System Security (CPSS)*, CPSS '18, page 15–21. ACM, 2018.

[15] Branka Stojanović, Katharina Hofer-Schmitz, and Ulrike Kleb. APT datasets and attack modeling for automated detection methods: A review. *Computers & Security*, 92:101734, 2020.

[16] Blake E Strom, Andy Applebaum, Doug P Miller, Kathryn C Nickels, Adam G Pennington, and Cody B Thomas. MITRE ATT&CK: Design and philosophy. Technical Papers MP180360, MITRE Corporation, July 2018.