Improving the effectiveness of media control auditing in nuclear facilities by log analysis

Seongyeol Oh, Min Woo Lee, Yongju Lee, Hyosoo Kang, Taigil Song
Korea Atomic Energy Research Institute
seongyeol@kaeri.re.kr

1. Introduction

In recent years, cyber security issues related to nuclear facilities have become a big challenge for every nuclear licensee. Due to increasing cyber threats toward nuclear facilities, the Nuclear Safety and Security Committee (NSSC) and Korea Institute of Nonproliferation and Control (KINAC) published Regulatory Standard on Computer and Information System Security for Nuclear Facilities (RS-015) [1]. Thus, as the nuclear licensee, the Korea Atomic Energy Research Institute (KAERI) established the Cyber Security Plan (CSP) and implemented cyber security requirements. If the Defense-In-Depth strategies are well implemented, the attack vectors towards nuclear facilities can be minimized. At this point, auditing the usage of media, which is one of the common interfaces between security boundaries, should be important. However, in the implementation stage of cyber security requirements, there are some limitations to audit media control. In this paper, we suggest a more effective way to audit media control by log analysis.

2. Cyber security regulations for nuclear facilities

The RS-015 provides general approaches and technical guidance to apply cyber security requirements to nuclear facilities. In particular, the RS-015 describes technical, operational and management security controls in Appendix II, to guide how to implement detailed cyber security requirements. However, applying all security controls immediately to operating nuclear facilities is not reasonable and some preprocessing steps such as identifying Critical Digital Assets (CDAs) should be considered. For these reasons, KAERI developed an implementation plan that divides cyber security controls into 7 stages as shown in Table I.

Table I: 7 stages of cyber security plan

Stage	Security Controls
1	Cyber Security Team(CST) & Cyber Security Incident Response Team(CSIRT) composition
2	Critical Digital Assets(CDA) identification & analysis
3	Development of Defense-In-Depth strategy & CSIR plan
4	Portable Media/Mobile Device(PMMD) & Maintenance, Test/Calibration Device(MTCD) control
5	System integrity & Access control
6	Operational & Management security controls
7	Technical security controls

3. Ineffective media control auditing

According to RS-015, the nuclear licensee should document and answer the questions about media control, as shown in Table II.

Table II: Questions for media control

Question	Description
Q1	When is the media connected/disconnected to the CDAs?
Q2	Which media is connected/disconnected to the CDAs?
Q3	Is the media connected/disconnected to the CDAs valid and registered?
Q4	Does the CST audit system record/log about media control?

To answer these questions, KAERI designed paper sheets that include connection/disconnection time, device id (registered by admin), user name, etc. The operators in nuclear facilities should write down every media usage related to CDAs – sounds reasonable. However, writing down media usage by hand involves human errors, malicious modification and intentional missing risks. To reduce and prevent these risks, CST should audit the media control performance.

Unfortunately, for most of the digital assets in nuclear facilities, security requirements related to media control were not considered in the design phase. As a result, relevant functions are not supported. Therefore, auditing media control is hard to perform in the field because many CDAs provide unnecessary or insufficient data to identify media usage. Only paper check with the media usage sheet without cross-validation is not sufficient to mitigate cyber security threats.

In the next section, we suggest common concepts of media log analysis to overcome these limitations.

4. Concept of media log analysis

We developed the concept of media log analysis into 4 steps, as shown in Figure I. To describe our concept clearly, we assumed that the target CDA is a single computer with Windows OS, as an example.

First, the nuclear licensee should pre-analyze system configurations, i.e., – system categories, operating systems, hardware specifications, supporting functions about media usage, etc. The nuclear licensee may maintain system specs and design documents, so it is not difficult to acquire system configurations. For example, we can summarize the pre-analyze system configuration as below.

1) System category: PC
2) Operating System: Windows 8
3) Hardware specs: 3 USB 3.0 ports, 1 CD-ROM drive, 2 LAN ports.
4) Supporting functions: Windows registry hive, Windows event log, Antivirus inspection log, SWAP files.

The result can vary depending on the target CDAs, e.g., – no registry hive in Linux systems.

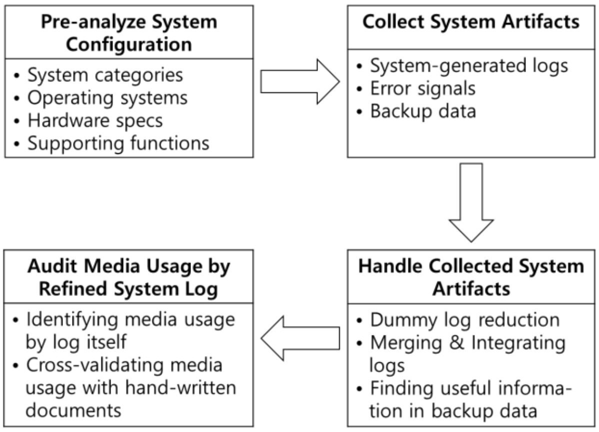
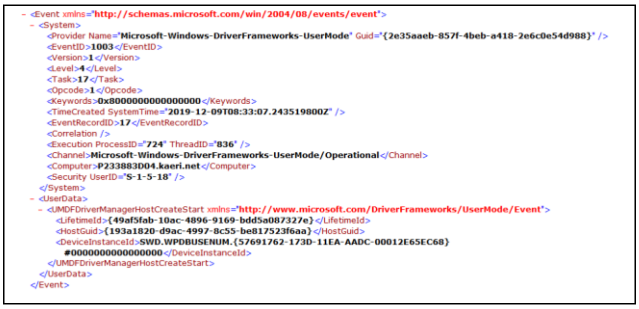

Pre-analyze System Configuration
• System categories
• Operating systems
• Hardware specs
• Supporting functions
Collect System Artifacts
• System-generated logs
• Error signals
• Backup data
Handle Collected System Artifacts
• Dummy log reduction
• Merging & Integrating logs
• Finding useful information in backup data
Audit Media Usage by Refined System Log
• Identifying media usage by log itself
• Cross-validating media usage with hand-written documents

Figure I: Media log analysis procedure

Next, the nuclear licensee should collect system artifacts about the media usage – system-generated logs, error signals, backup data, etc. For example, the Windows registry that is stored and recorded automatically in the system holds important information about the media identification and connectivity [2]. These can be definite hints to answer the Q2 (Which media is connected/disconnected to the CDAs?) in Table II after filtering out unnecessary data. Windows event logs also include valuable evidence to specify the connection and disconnection time of media, mentioned in Q1 in Table II (When is the media connected/disconnected to the CDAs?).

However, only collecting system artifacts in raw is not sufficient to analyze media usage. This is because the system artifacts are usually represented in unfamiliar expressions for the user. For example, as shown in Figure II, the Windows event log related to media connection is represented in xml format and includes dummy information that is not related to media usage analysis.



```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  - <System>
      <Provider Name="Microsoft-Windows-DriverFrameworks-UserMode" Guid="{2e35aaeb-857f-4beb-a418-2e6c0e54d988}" />
      <EventID>1003</EventID>
      <Version>1</Version>
      <Level>4</Level>
      <Task>17</Task>
      <Opcode>1</Opcode>
      <Keywords>0x8000000000000000</Keywords>
      <TimeCreated SystemTime="2019-12-09T08:33:07.243519800Z" />
      <EventRecordID>17</EventRecordID>
      <Correlation />
      <Execution ProcessID="724" ThreadID="836" />
      <Channel>Microsoft-Windows-DriverFrameworks-UserMode/Operational</Channel>
      <Computer>P233883D04.kaeri.net</Computer>
      <Security UserID="S-1-5-18" />
    </System>
  - <UserData>
    - <UMDFDriverManagerHostCreateStart xmlns="http://www.microsoft.com/DriverFrameworks/UserMode/Event">
        <LifetimeId>{49af5fab-10ac-4896-9169-bdd5a087327e}</LifetimeId>
        <HostGuid>{193a1820-d9ac-4997-8c55-be817523f6aa}</HostGuid>
        <DeviceInstanceId>SWD.WPDBUSENUM.{57691762-173D-11EA-AADC-00012E65EC68}
          #0000000000000000</DeviceInstanceId>
      </UMDFDriverManagerHostCreateStart>
    </UserData>
  </Event>
```

Figure II: An example of raw system artifact

Moreover, merging and integrating various kinds of logs is also necessary to make sense of the data. In view of the media control, the most important information is “which” media was connected or disconnected to CDA at the “specific time”. Unfortunately, most of the system artifacts cannot provide this information alone, so we should find something in common among the system artifacts and combining them into meaningful results. In our example, “DeviceInstanceId”, which is the unique parameter and found in Windows registry hive and Windows event log, can be strong candidate. If CST and operators document “DeviceInstanceId” parameter of registered media, they can identify legal/illegal media usage by verifying that field.

Finally, CST can use system artifacts to audit media usage after previous refining processes. If the analyzed logs are fully reliable, the results can be used to identify media usage. However, digital evidence involves a system log overflow, system error, and malicious modification risks. Also, these digital evidence cannot guarantee whether permitted person uses media devices. Therefore, we recommend validating the analysis results with documented paper sheets – registered user information, media information etc.

5. Conclusion

In this paper, we briefly introduced cyber security regulations for nuclear facilities and argued that only documented media usage is not sufficient to handle cyber security threats via a media interface. Therefore, we suggested the concept of media log analysis. With this concept, the nuclear licensee can develop improved media usage auditing procedures for each target system. Furthermore, identifying what contents in media is our next challenge. It should be important to achieve complete media control.

REFERENCES

[1] KINAC, Regulatory Standard KINAC/RS-015, Security for Computer and Information of Nuclear Facilities, December 2016.
[2] A. Arshad, W. Iqbal and H. Abbas, USB Storage Device Forensics for Windows 10, The Journal of Forensic Sciences, Vol.63, 2017.