A study on the application of mission-based cybersecurity testing and evalulation of weapon systems

Ikjae Kim
Dept of Computer Engineering,
Sejong University
R.O.K Cyber Operations Command
Seoul, South Korea
kij397@mnd.go.kr

Hansung Kim
R.O.K Cyber Operations Command
Seoul, South Korea
khs4284@mnd.go.kr

Dongkyoo Shin*
Dept of Computer Engineering,
Sejong University
209 Neungdong-ro, Gwangjin-gu,
05006
Seoul, South Korea
shindk@sejong.ac.kr
*Corresponding author:Dongkyoo Shin

***Abstract*— In this paper, we investigate the ongoing research on ways to improve cybersecurity throughout the life cycle of weapon systems applied in advanced countries such as the United States(U.S.), and present effective security evaluation measures by analyzing restrictions on acquiring weapon systems in Republic of Korea. We consistently performed mission-based risk assessment in cybersecurity tests and evaluation plans at the entire stage to support decision-making by providing key information to major decision-making organizations in a timely manner. We propose a plan to carry out simulated penetration by establishing rules of engagement so that protection measures can be verified for vulnerabilities identified in terms of cybersecurity. In addition, we identified the areas where artificial intelligence can be applied to the proposed cybersecurity test and evaluation system, and suggested future development plans. Through this, we supplemented our ability to support major decisions by integrating mission-based risk assessment factors into the cybersecurity test and evaluation system research conducted so far to identify risks in a timely manner between acquisition projects.**

Keywords—mission, cybersecurity, test and evaluation

I. INTRODUCTION

With the rapid development of information technology (IT) around the world, the use of software is increasing in many parts of society throughout the world. Software is increasing in all fields such as home appliances and automobiles, and the same is true of the defense weapon systems. This increase in the proportion of such software in the field of defense weapon systems helps to implement the excellent performance, but vulnerabilities may be inherent in the software, and the possibility of exposure to cyber threats using these vulnerabilities increases. In particular, since South Korea has a higher software utilization rate than North Korea, North Korea is using this asymmetry to openly attack cyberattacks, which is a factor that can cause serious damage to the allies in a war situation.

In order to respond to such cyber-attacks, research to remove security vulnerabilities in software is increasing, and in particular, research on software development security to remove factors that cause security vulnerabilities in advance in the software development stage is being actively conducted.

This work was supported by the National Research Foundation of Korea through the Basic Science Research Program, Ministry of Education, under Grant 2018R1D1A1B07047395.

The U.S. applies the cybersecurity test and evaluation system to efficiently identify and eliminate vulnerabilities throughout the weapon system acquisition stage to safely deploy it, and operates it by integrating it with a cybersecurity system called Risk Management Framework (RMF) are doing.

In this regard, the paper [1] proposed the introduction of a “weapon acquisition cybersecurity test and evaluation system” that applies the US cybersecurity test and evaluation to the defense weapon system acquisition stage. In this paper, we supplement and propose procedures to enable the identification and management of cyber-related risks by performing mission-based risk assessment in addition to the identification of technical and management vulnerabilities in the "Weapon Acquisition Cybersecurity Test and Evaluation System".

Following the introduction, this paper examines the related work in Chapter 2, the limitations of the “Weapon Acquisition Cybersecurity Test and Evaluation System” proposed in [1] in Chapter 3, and combines the mission-based risk assessment in Chapter 4. Suggest ways to improve the security evaluation system. Chapter 5 identifies the areas where artificial intelligence can be applied to the proposed cybersecurity test and evaluation system and presents the application plan.

II. RELATED WORK

A. U.S. military cybersecurity test and evaluation

The United States government defines cybersecurity as preventing, protecting, and restoring damage to computers, electronic communications systems, electronic communications services, wireline communications, electronic communications, and information contained therein to ensure availability, integrity, authentication, confidentiality, and non-repudiation [2].

Test and evaluation is a compound word of test and evaluation as a field in the weapon system acquisition stage. The main purpose of test and evaluation is to provide timely information necessary for decision-making to policy makers [3]. Test and evaluation verifies whether the target weapon system conforms to the user's requirements and meets the operational capability by obtaining basic data for verifying and evaluating the objective performance of the weapon

system and comparing and analyzing it with preset test standards through various tests. to judge suitability. Through this, it is the decision-making support stage to determine whether the purchase, R&D, design, and manufacture of weapons systems meet the requirements of the military [1].

The U.S. guarantees the rationality and efficiency of test evaluation by defining NIST SP800-related reference documents related to cybersecurity by the National Institute of Standards and Technology (NIST) to apply the same criteria and share evaluation results at the national level for rational cybersecurity test and evaluation [1][4][5][6][7][8][9].

The U.S. Department of Defense incorporates a risk management framework (RMF) and a cybersecurity test and evaluation system into the defense acquisition system to effectively realize cybersecurity in the entire life cycle of weapons systems [1][3][10][11][12].

The U.S is carrying out a six-step cybersecurity test and evaluation process to implement cybersecurity throughout the entire life cycle of a weapon system. This process proceeds continuously from the initial required analysis stage to the final electrification stage during the weapon system acquisition stage, and is performed by integrating with the system engineering and RMF process processes. This cybersecurity test and evaluation process consists of six steps and is as follows [13].

Step 1, Understanding cybersecurity requirements

Step 2, Identifying the cyber-attack surface

Step 3, Identifying vulnerabilities through collaboration

Step 4, Adversary cybersecurity development test and evaluation

Step 5, Vulnerability assessment and penetration assessment through collaboration

Step 6, Hostile evaluation

B. Korea's cybersecurity test and evaluation

The acquisition of weapons systems for the Republic of Korea (ROK) military is defined in the 'Defense Forces Power Generation Work Order' [14], which defines guidelines for the overall life cycle, including the requirement, acquisition, operation and maintenance of weapons systems. In Article 52 of the Ordinance (Weapon System Research and Development), the weapons system research and development process is divided into the exploration and development stage, the system development stage and the mass production stage. In particular, the following detailed guidelines are provided for cybersecurity in the weapon system introduction stage.

- Article 52 (Research and Development of Weapon Systems) ⑤ In the case of research and development of weapons systems, the following activities are carried out in relation to security.

  1. The Defense Acquisition Program Administration (DAPA) submits the search and development result report including the results of the security support company's review of the protection measures for the information system of the weapon system.
  2. The DAPA requests the security support company to review the protection measures for the information system of the weapon system before starting the system development, and reflects the review results in the system development plan.
  3. In the system development stage, the DAPA requests the security support company to review the protection measures for the built-in SW, and when a change in the development plan is required, such as when a change in operational performance is required or when jointness and interoperability are affected, the Ministry of National Defense (Informatization Planning Office), the Joint Chiefs of Staff, and the armed forces should be consulted in advance, and re-requested to the Security Support Agency to review the protection measures for the weapon system information system and embedded SW.

In addition, in relation to Articles 25 and 26 of the 'Defense Cybersecurity Ordinance' of Korea, the security support officer reviews the protection measures for the information system and embedded SW of the weapon system during the weapon system search and development and system development stage, and transfers weapons system test and evaluation, etc. to full power. In this step, security measures are performed [14].

As for the cyber security test and evaluation items of the ROK military, the details of interoperability test and evaluation in Article 81 (Classification and Method of Test and Evaluation) of the Defense Power Generation Work Order are set to follow the Defense Interoperability Management Directive. Test and evaluation items related to information assurance and cyberthreat response are included [14].

In the Power Generation Work Order, the responsibility for compiling the interoperability field is defined as the Joint Interoperability Technology Center. In the development test and evaluation, software reliability test and information protection are evaluated, and in the operation test and evaluation, only information protection is evaluated.

Information protection test and evaluation items for weapon systems specified in the Defense Interoperability Management Directive include information protection level, network information protection, control system establishment, key management system establishment, application system, server, terminal, encryption equipment application, cyber threat response capability, It is divided into SW vulnerability removal, and details are shown in "Table I." [15].

C. Cyber security test and evaluation system for weapon system

D.

The "weapon acquisition cybersecurity test and evaluation system" proposed in [1] proposes the advantage of systematically conducting cybersecurity test and evaluation from the early stage of weapon systems applied in the United States as ROK domestic cybersecurity process. The application of cyber security within the weapon system has been improved by increasing connectivity. The article referenced in [1] divides the cybersecurity stage in the defense acquisition system into four stages and suggests the

process to be performed at each stage. In particular, the process of actively identifying and removing vulnerabilities was added by applying vulnerability analysis, evaluation and simulated penetration in the development/operation test and evaluation stage. This is to strengthen cybersecurity by extending vulnerability analysis and evaluation and simulated penetration, which are currently applied only in the operational stage in the defense field, to the acquisition stage.

The "weapon acquisition cybersecurity test and evaluation system" in [1] is divided into stage 1 cybersecurity requirements identification, stage 2 cyber - attack surface identification, stage 3 cybersecurity development test and evaluation, and stage 4 cybersecurity operation test and evaluation. Is as follows.

- Stage 1, Identifying Cybersecurity Requirements: Develop an initial approach and plan to identify cybersecurity requirements by looking at all target system-related documentation and conduct cybersecurity testing and evaluation
- Stage 2, Identifying of the cyber-attack surface: Identifies the attack path that an attacker can access to the target system's network, hardware, firmware, physical interface, software, etc., and identifies possible vulnerabilities in that path
- Stage 3, cybersecurity development test and evaluation: Perform test and evaluation of the target system using the vulnerability analysis/evaluation report, security evaluation report, and development test and evaluation output
- Stage 4, cybersecurity operation test and evaluation: Perform vulnerability penetration test from the attacker's perspective by referring to the vulnerability analysis/evaluation report, cybersecurity development test and evaluation output, etc. and evaluate the cybersecurity level of the target system

TABLE I. ROK MILITARY WEAPON SYSTEM INFORMATION SECURITY TEST EVALUATION ITEMS

Evaluation items	
Information protection level	
Network information protection	
Establishment of control system	
Establishment of key management system	
Application system information protection	
Server information protection	
Terminal information protection	
Encryption equipment application	
Cyber Threat Response Capability	Cyber Threat Response Capability
	Ability to respond to identity-disguised threats
	Ability to respond to data tampering threats
	Denial of aggression threat response capability
	Ability to respond to threats of information leakage
	Denial of Service (DoS) Threat Response Capability
	Ability to respond to elevation of privilege threats
SW Vulnerability Removal	SW Vulnerability Removal
	Appropriateness of applying secure coding rules
	Relevance of removing open-source vulnerabilities

III. LIMITATIONS OF "WEAPON ACQUISITION CYBERSECURITY TEST AND EVALUATION SYSTEM"

The "weapon acquisition cybersecurity test and evaluation system" proposed in [1] consists of four stages. Each stage identifies cybersecurity requirements by examining all target system-related documents, and identifies the target system's network, server, firmware, and physical Identifies the attack surface using interfaces, etc.

In the cybersecurity development and operation test and evaluation stage, the level of cybersecurity is evaluated by using the vulnerability analysis/evaluation report and development test and evaluation output, and by adding the technical vulnerability penetration test to it. As a result of these activities, technical and managerial weaknesses can be derived, but information on risks arising from the identified weaknesses to project managers is not considered.

The purpose of test and evaluation is to provide information for key decision-making to decision-making organizations in a timely manner.

To this end, it is necessary to supplement the mission-based risk assessment process that can identify and manage risks by identifying cyber-dependent missions based on the mission performed by the target weapon system and deriving major cyber threats related thereto.

IV. PROPOSED MISSION-BASED CYBERSECURITY TEST AND EVALUATION

In this chapter, we propose a mission-based cybersecurity test and evaluation procedure suitable for the acquisition stage of the ROK military weapon system. The proposed mission-based cybersecurity test and evaluation is performed as shown in "Table II.".

TABLE II. CLASSIFICATION OF CYBERSECURITY TEST AND EVALUATION STAGES

Division	Weapon system acquisition	Mission-based cybersecurity test and evaluation
Step 1	Understanding cybersecurity requirements	Risk/threat modeling
Step 2	System development	Attack Surface Listing
Step 3	Development test evaluation	Attack surface vulnerabilities analysis and evaluation
Step 4	Operational test evaluation	Analysis and evaluation of simulated penetration and vulnerability based on rules of engagement

A. Risk/threat modeling

Step 1, risk/threat modeling is performed in the cybersecurity requirements identification step in weapon system acquisition stage, and initial risk/threat modeling

based on power requirements is performed for mission-based risk assessment.

For the mission-based risk assessment, the cyber-dependent mission is identified, the detailed functions for the mission are subdivided, and the diagram is shown in “Fig. 1”.

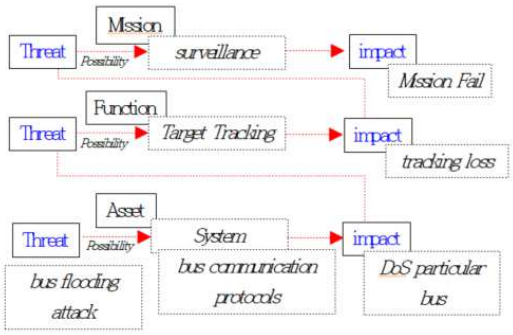

Fig. 1. Risk/threat modeling as an example

B. Attack Surface Listing

Step 2, attack surface inventorying is performed in the system development step, and risk/threat modeling is performed again based on supplementary documents such as RFP and the attack surface is listed.

Identification of the attack surface establishes a cyber boundary around the weapon system, identifies the entry point that approaches the system from the outside through this attack surface, and divides and expresses the system nodes from the assets entering the system step by step. Currently, the node with the vulnerability becomes the main node that becomes the attack target. If this is expressed as a figure, it is shown in “Fig. 2”.

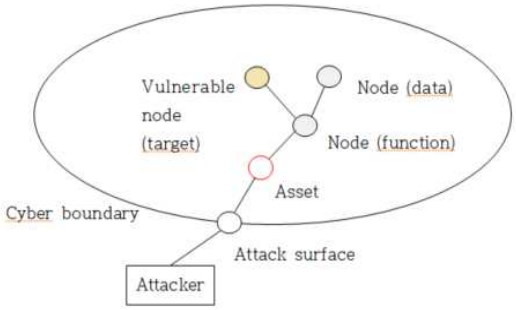

Fig. 2. Identification of the attack surface of a weapon system

The identified attack surface can be schematized as shown in “Fig. 3” by identifying sub-functions, data, and assets from the mission of the weapon system. This allows the attack surface to connect which assets, which data, which functions, and which missions it ultimately wants to achieve.

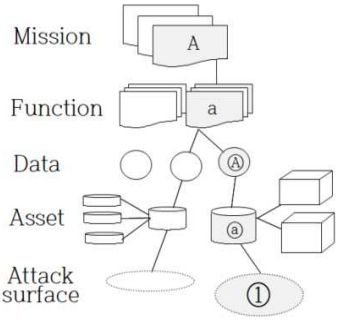

Fig. 3. Identify the attack surface of cyber-dependent missions

C. Attack surface vulnerability analysis and evaluation

Step 3, attack surface vulnerability analysis and evaluation is performed in the development test and evaluation step, and risk/threat modeling is performed again based on the development document, and vulnerability analysis and evaluation of the attack surface is performed.

By performing vulnerability analysis and evaluation on the attack surface, vulnerable assets are identified in the asset layer, and related data and functions are identified. Based on this, weak missions can be identified.

Using this to supplement the threat scenario, “Asset ⓐ has identified vulnerability (1), and using it, assets ⓑ and ⓒ can be seized, and related data Ⓐ can be stolen or altered. This limits function a and consequently cannot perform mission A”.

Accordingly, the project manager can take measures to mitigate risks by devising protection measures for vulnerabilities.

“Fig. 4” derives protection measures to mitigate vulnerability(1) for vulnerable asset ⓐ, and the derived protection measures are indicated by a blue dotted line on the border of asset ⓐ.

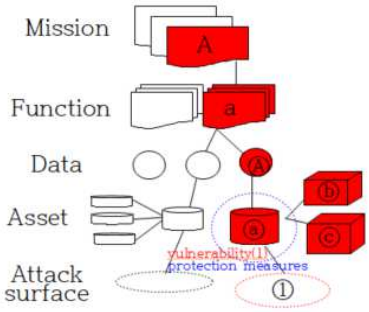

Fig. 4. Deriving protection measures for vulnerable assets

The vulnerabilities supplemented by these protection measures can mitigate the risk of the entire weapon system, and by taking protection measures for asset ⓐ, assets ⓑ and ⓒ were returned to their normal state as shown in “Fig. 5”. As a result, data Ⓐ, function a, and task A all show a normal state.

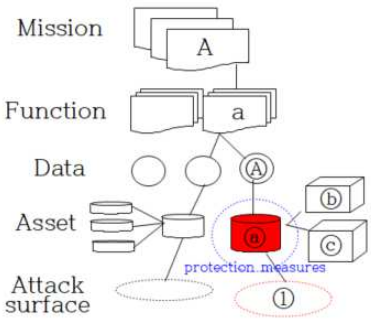

Fig. 5. Mitigation of vulnerabilities through protection measures

Based on these measures, a mission-based risk assessment can be performed, and the results are reported to the decision-making organization and provided for quick decision making, thereby facilitating the communication of the unplanned acquisition process.

In particular, if it takes a long time to acquire a weapon system, it is realistically limited to completely eliminate all threats that develop rapidly within a limited project period and within the project budget. Therefore, it is necessary to manage risk through this process.

In this way, all possible threat scenarios for each attack surface can be set as rules of engagement for simulated infiltration, and become a standard to verify the effectiveness of protection measures for each asset.

D. Simulated penetration based on rules of engagement and vulnerability analysis / evaluation

Step 4, the simulation penetration based on rules of engagement and vulnerability analysis/evaluation is performed in the operational test and evaluation step, and simulated penetration is performed using the threat scenario for each attack surface identified above as the rules of engagement.

The threat scenario is to neutralize the protection measures of the blue dotted line through the attack surface ①, and to perform a simulated penetration so that the mission A cannot be performed using the vulnerability (1) of the asset ⓐ.

Through this, using the vulnerability of the initially identified attack surface, simulated penetration is performed following the threat scenario to verify the effectiveness of the devised security measures. It verifies the risk mitigation status of assets, data, functions, and missions through simulated penetration based on rules of engagement and performs mission-based risk assessment based on the results. At this time, if vulnerabilities are continuously identified, security measures are supplemented and re-verified through retesting to ensure a safe state before electrification.

V. "MISSION-BASED CYBERSECURITY TEST AND EVALUATION" AND FIELDS OF APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGY

The "Mission-based cybersecurity test and evaluation" is a proposal to strengthen cybersecurity by combining the US cybersecurity process with ROK domestic weapon system test and evaluation from a cybersecurity point of view. In addition, it emphasized the implementation of reinforced cybersecurity by setting the rules of engagement as a guideline for conducting test and evaluation and supplementing the protection measures of the weapon system through retesting if the response was insufficient.

In this paper, iterative risk/threat modeling is performed step by step by adding risk assessment to the domestic weapon systems test and evaluation, and vulnerability analysis and evaluation based on mission-based threat scenarios. It was proposed by improving the system that can verify the effectiveness of security measures in the operational test and evaluation stage by executing simulated penetration under the rules of engagement and settling.

"Table III." compares the test and evaluation of domestic weapon system and the proposed method from the perspective of cyber security.

TABLE III. COMPARISON WITH DOMESTIC WEAPON SYSTEM TEST AND EVALUATION

Division	Domestic weapon system test and evaluation	Mission-based cybersecurity test and evaluation
Threat Scenarios	None	O
Risk Assessment	None	O
Vulnerability analysis and evaluation	1 time	3 times
Simulated Penetration	None	1 time

If artificial intelligence technology, which is being actively researched, is applied to the mission-based cybersecurity test and evaluation of the weapon system proposed in this paper, the level of cybersecurity activity will increase.

In particular, with the advancement of the weapon system, the vast attack surface is continuously increasing, and numerous networks are formed between the asset nodes constituting the weapon system. Therefore, it is necessary to check all cases by applying artificial intelligence technology including machine learning and deep learning rather than activities by professional personnel to identify all paths available for attack among the networks between all asset nodes centering on this attack surface and perform simulated penetration [16][17].

The use of artificial intelligence technology can evaluate and predict all possible penetration paths for an attack, and it will be possible to derive priorities for establishing security measures according to the evaluation results, thereby supporting the timely decision of policy makers.

It will be possible to implement more effective protection measures if a series of procedures for identifying threat scenarios and performing simulated infiltration against the

vast attack surface of increasingly complex weapon systems are made with artificial intelligence technology.

VI. CONCLUSION

In this paper, based on the cybersecurity test and evaluation of the United States, the mission-based risk assessment is consistently performed in the cybersecurity test and evaluation method suitable for ROK domestic situation studied earlier, and important information is provided to major decision-making organizations in a timely manner. To support decision-making and to verify protection measures against identified vulnerabilities in terms of cybersecurity, it is proposed to set up rules of engagement to conduct simulated infiltration.

This can facilitate communication between related organizations throughout the acquisition phase, and improve the cybersecurity capabilities of acquired weapon systems by improving vulnerabilities through information sharing, verifying their effectiveness, and institutionalizing them so that they can be retested if insufficient.

In particular, if AI technology is used for vulnerability analysis and evaluation and simulated penetration in the mission-based weapon system cybersecurity test evaluation, it is judged that cybersecurity will be able to develop dramatically through evaluation and verification of all possible attackable weapon system access paths. do.

Considering that efforts to strengthen cybersecurity activities and manage risks throughout the entire life cycle of weapon systems pursued in the United States and advanced countries are continuing, this paper is one way to evaluate cybersecurity tests applicable to domestic weapon systems. It can be said that it contributed to the specification of the methodology.

REFERENCES

[1] Ji-seop Lee, Sung-yong Cha, Seung-soo Baek, Seung-joo Kim, " Research for Construction Cybersecurity Test and Evaluation of Weapon System," Journal of The Korea Institute of information Security & Cryptology Vol.28, No.3, Jun. 2018. https://doi.org/10.13089/JKIISC.2018.28.3.765

[2] THE WHITE HOUSE WASHINGTON, "National Security Presidential Directive-54/Homeland Security Presidential Directive-23," January 8. 2008.

[3] Jong Wan Park, "The Action of the Reliability Enhancement in Test and Evaluation of the Weapon Systems," Journal of Applied Reliability Vol. 15-2, pp. 108-123, 2015.

[4] Congressional Research Sercive, "Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process," May 23, 2014.

[5] "Guide for Conducting Risk Assessment," NIST SP 800-30 Rev.1. 2012.

[6] "Guide for Applying the Risk Management Framework to Federal Information systems," NIST SP 800-37 Rev.1. 2010.

[7] "Managing Information Security Risk," NIST SP 800-39, 2011.

[8] "Security & Privacy Controls for Federal Information Systems and Organizations,"NIST SP 800-53 Rev.4, 2013.

[9] "Guide for Assessing the Security Controls in Federal Information Systems and Organizations," NIST SP 800-53A Rev.1, 2010.

[10] "Cybersecurity & Acquisition Lifecycle Integration Tool(CALIT)," DAU ver 3.1, sep 2018.

[11] Hyun-suk Cho, Sung-yong Cha, Seung-joo Kim, "A Case Study on the Applicaion of RMF to Domestic Weapon System," Journal of The Korea Institute of Information Security & Cryptology Vol.29, No.6, Dec.2019.

[12] Sungyong Cha, Seungss Baek, Sooyoung Kang and Seungjoo Kim, "Security Evaluation Framework for Military IoT Devices." Security and Communication Networks. Vol. 2018, Article ID 6135845, 12 pages, Jul. 2018.

[13] Department of Defense, "Cybersecurity Test and Evaluation Guidebook," 2015.

[14] "National Defense Power Generation Business Instruction," Ordinance of the Ministry of National Defense, 2021.

[15] "Defense Interoperability Management Directive," Ministry of National Defense, Jan. 2021.

[16] Philip W. Shin, Jack Sampson, V Narayanan "Context-Aware Collaborative Object Recognition For Distributed Multi Camera Time Series Data," in *Tenth International Symposium on Information and Communication Technology (SoICT) Dec. 2019,* Hanoi - Halong Bay, Vietnam, pp. 154–161. https://doi.org/10.1145/3368926.3369666

[17] Philip W. Shin, Jinhee Lee, Seung Ho Hwang, "Data Governance on Business/Data Dictionary using Machine Learning and Statistics," in *International Conference on Artificial Intelligence in Information and Communication (ICAIIC) 2020,* Fukuoka, Japan, pp.547-552. https://doi.org/10.1109/ICAIIC48513.2020.9065194