IEICE TRANS. INF. & SYST., VOL.E102–D, NO.2 FEBRUARY 2019

LETTER

Comprehensive Damage Assessment of Cyberattacks on Defense Mission Systems

Seung Keun YOO[†], ***Member and*** **Doo-Kwon BAIK**[†a)], ***Nonmember***

SUMMARY This letter proposes a comprehensive assessment of the mission-level damage caused by cyberattacks on an entire defense mission system. We experimentally prove that our method produces swift and accurate assessment results and that it can be applied to actual defense applications. This study contributes to the enhancement of cyber damage assessment with a faster and more accurate method.

key words: *cybersecurity, damage assessment, mission-level damage, defense mission system, cyberattack*

1. Introduction

In the defense domain, enemies may attempt to destroy or degrade the mission capability of our forces using cyberattacks [1]. Defense mission systems, such as a missile defense system, must maintain sufficient mission capability to accomplish their missions despite cyber damages. A damage assessment provides information on how seriously these systems are affected. Many studies have proposed methods for damage assessment of cyberattacks, but they are not strong enough to be utilized in the defense domain. Their purpose was mainly to detect a cyberattack, not to evaluate its damage, and the assessment results had low accuracy to correctly determine the actual situation. They also needed a long assessment time, and thus, have limitations for a swift response to cyber incidents. To resolve these problems, accurate and fast damage assessments of cyberattacks are required. We define measures to precisely evaluate the cyber damage and develop a comprehensive method to rapidly assess the damage to the entire system at the mission level. Experiments are performed to demonstrate that our method has superior performance and that it can be successfully applied to defense applications. This study contributes to the enhancement of cyber damage assessment with a faster and more accurate method.

2. Related Works

Early studies on the damage assessment of a cyberattack focused on developing methods to judge if it occurred on equipment, such as computers or network devices. Lala et al. [2] and Grimaila et al. [3] proposed methods to detect the intrusion of cyberattacks based on the values of special variables or measures, beyond a system log analysis. The damage in these studies indicated only the existence of a cyberattack. They are more suitable for intrusion detection of cyberattacks rather than damage assessment.

Yang et al. [4] also proposed a method to divide the process of a cyberattack into multiple stages and predict its possibility in the early stages using statistical methods. Moreover, Ralston et al. [5] and Ten et al. [6] evaluated the risk or vulnerability that indicates the probability of a cyberattack. These methods showed the effects of cyberattacks in various ways, but these assessments were different from those of cyber damage.

Argauer et al. [7] developed a graph representing the spread of the impact of a cyberattack and evaluated the propagation of the damage. After this study, Jakobson [8] and Kotenko et al. [9] proposed an improved damage assessment method by not only considering the spread of the cyber impact but also producing quantitative damage. However, these damages have limitation to indicate the status of the attacked target owing to low accuracy. Thus, it was difficult to apply them in the defense domain, which requires accurate situational awareness.

Recent studies have tried to represent specific and practical damage. Musman et al. [10] defined a measure of effectiveness (MOE) applicable to the defense domain, Patel et al. [11] represented the damage as an economic loss, and Wagner et al. [12] assessed the mission impact using mission delay. These studies contributed to enlarge the level and extent of the assessed damage, but required a long time to actually determine the values of particular variables after the cyberattacks.

Therefore, we focus on comprehensively and quantitatively assessing the cyber damage for defense applications.

3. Damage Assessment of Cyberattacks

3.1 Basic Concept

In the defense domain, mission capability is the possession of the means to use military force to achieve an intended effect within the battlespace [13]; it simply means the ability to accomplish a certain mission. A defense mission system is also defined as a system designed to accomplish missions such as combat, reconnaissance, or missile defense in the defense domain.

We define the damage of a cyberattack

Manuscript received April 4, 2018.
Manuscript revised September 21, 2018.
Manuscript publicized November 6, 2018.

[†]The authors are with the Department of Computer and Radio Communications Engineering, Korea University, Republic of Korea.
a) E-mail: baikdk@korea.ac.kr (Corresponding author)

DOI: 10.1587/transinf.2018EDL8068

($damage_{cyberattack}$) on a defense mission system as the degradation of its mission capability owing to the cyberattack and quantitatively calculate this damage as the change in the mission capability (*Mcapability*) between the pre- and post-cyberattack:

$$damage_{cyberattack} = 1 - \frac{Mcapability_{post\text{-}cyberattack}}{Mcapability_{pre\text{-}cyberattack}} \quad (1)$$

A comprehensive damage assessment evaluates the damage not to a certain part of an objective system but to the entire system at the mission level.

3.2 Layers and Components

A defense mission system consists of physical (tangible) components such as people or computers, and conceptual (intangible) components such as a mission or function. To identify the characteristics of the system for cyber damage assessment, we classify its components into a hierarchical structure according to their roles and define four layers: *mission*, *task*, *function*, and *asset*. The mission layer includes the missions that a defense mission system must achieve (e.g., intercepting an enemy's missile in a missile defense system); the task layer includes the tasks that members of a defense mission system must perform (e.g., tracing the trajectory of the missile in the missile defense system); the function layer includes the functions that a defense mission system provides (e.g., visualization of the missile trajectory in the missile defense system); and the asset layer consists of the assets of a defense mission system, such as equipment, software, or data. Then, we identify each component in the system and classify it into the appropriate layer.

3.3 Measures

We define two measures for comprehensive damage assessment: *contribution* and *utility*. Contribution measures the extent to which a component in a lower layer helps a component in the upper layer to perform a duty. Subject matter experts (SMEs) set a value from 0.0 (no contribution) to 10.0 (perfect contribution) based on their expertise. Utility measures the usefulness of a component for the ultimate accomplishment of the entire system's mission. This measure is calculated by summing the products of the utilities of related lower-layer components and their contributions as

$$utility_i = \sum_{j=1}^{n} (utility_j \times contribution_{ij}) \quad (2)$$

where $utility_i$ is the utility of C_i (i^{th} component in a layer), $utility_j$ is the utility of C_j (j^{th} component in the lower layer), $contribution_{ij}$ is the contribution between C_i and C_j, and n is the number of components in the lower layer related to C_i (the number of C_js related to C_i).

The utility of the component in the asset layer is set to 1 before the cyberattacks. Figure 1 shows a simple example.

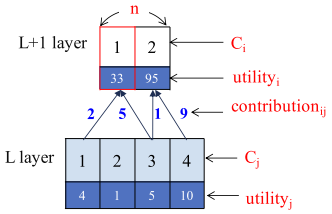

Fig. 1 Example utility calculation.

In Fig. 1, the contribution is the value labeling the arrow from a component in the lower layer to a component in the upper layer, whereas the utility is the value below the component in each layer. For example, the utility of the first component (C_1) in the $L+1$ layer is 33 ($4 \times 2 + 5 \times 5$).

3.4 Damage Assessment

When a defense mission system is under cyberattack, the attack first damages the asset-layer components and the damage spreads up to the mission layer. At the asset layer, the cyberattack decreases the utility of a targeted component according to the utility decline rate defined in the damage table. The utility decline rate indicates how much the utility of the asset-layer component decreases owing to the cyberattack from 0.0 to 1.0 and is determined by SMEs considering the lethality of the cyberattack and the vulnerability of the targeted asset. The damage table lists these rates. Therefore, the utility of the targeted asset-layer component is changed by the cyberattack as

$$utility_{post\text{-}cyberattack} = utility_{pre\text{-}cyberattack} \times UDrate \quad (3)$$

where $utility_{pre\text{-}cyberattack}$ and $utility_{post\text{-}cyberattack}$ are the utilities of the asset-layer component before and after the cyberattack, respectively, and *UDrate* is the utility decline rate for the cyberattack and the target in the damage table.

As the asset-layer components' utilities change, the related upper-layer components' utilities change accordingly up to the mission layer. We finally determine the ultimate damage as expressed in Eq. (1). The mission capability is calculated by summing the products of the utilities of the mission-layer components and their contributions (to the entire system) as

$$Mcapability = \sum_{i=1}^{n} (utility_i \times contribution_{i\text{-}system}) \quad (4)$$

where $utility_i$ is the utility of a component in the mission layer, n is the number of components in this layer, and $contribution_{i\text{-}system}$ is the contribution of the mission-layer component to the entire system.

4. Experiment and Discussion

4.1 Experiment and Results

We conducted experiments to demonstrate the practicality

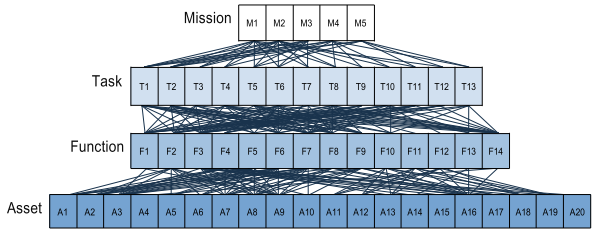

Fig. 2 Hierarchical structure of the missile defense system.

Table 1 Damage table.

Cyberattack	Server	Router	Optical switch	User data	OS
Malware	0.60	0.00	0.00	1.00	1.00
DDoS	0.70	0.20	0.20	1.00	1.00
Hacking	0.75	1.00	1.00	0.30	1.00

Table 2 Experimental results.

	Intermediate damage (average)				Mission Capability	Damage
	Asset	Function	Task	Mission		
Pre-	-	-	-	-	407725.11	-
Scn #1	7.00%	10.25%	12.66%	13.10%	353963.73	13.19%
Scn #2	4.00%	0.41%	1.12%	1.02%	403686.34	0.99%
Scn #3	4.75%	14.96%	17.63%	19.11%	328509.60	19.43%

and performance of the method proposed in this study.

We applied our method to a missile defense system as an actual defense mission system. Twelve SMEs were selected for the experiments and were divided into three groups of four people according to their area of expertise: *missile defense*, *cybersecurity*, or *both*. The missile defense SMEs identified the components of the missile defense system, classified them into each layer, and assigned the relationships between the components shown in Fig. 2.

The cybersecurity SMEs determined the utility decline rates in the damage table as presented in Table 1.

Every SME determined all the contributions in Fig. 2 and every utility was calculated based on them. We developed three scenarios for our experiment as follows:

- Scenario #1: An enemy troop in another country infects the missile defense system using malware. This cyberattack affects the main server (A9 in Fig. 2) and the router (A10 in Fig. 2) of the system.
- Scenario #2: An outer hacktivist conducts DDoS attack on the optical switch (A20 in Fig. 2) in the missile defense system.
- Scenario #3: A hacker steals the administration information from the system manager and corrupts data in the missile defense system. This hacking affects the main server (A9 in Fig. 2) and user data in the operation console (A3 in Fig. 2) of the system.

Table 2 lists the results of the experiments. The intermediate damage is the average of the changes in the utilities in a layer between the pre- and post-cyberattack and indicates the progress of cyber damages by layer. We only used it for display, instead of listing too many values of our measures for the experiments. It is calculated as

Table 3 Results of comparison with other studies.

Layer	Argauer et al. [7]	Jakobson [8]	Our study
Asset (A20)	75.00%	75.00%	80.00%
Task (T1)	0.93%	5.36%	0.83%
Mission (M1)	NA	5.61%	0.91%
Overall	NA	NA	0.99%

$$damage_{Intermediate} = \frac{\sum_{i=1}^{n}\left(1 - \frac{post\_utility_i}{pre\_utility_i}\right)}{n} \quad (5)$$

where $pre\_utility_i$ and $post\_utility_i$ are the utilities of the i^{th} component in each layer before and after the cyberattack, respectively, and n is the number of components in the layer.

In Table 2, the experimental results reveal that the damage to asset-layer components caused by the cyberattack (e.g., 40% damage of the main server and 100% damage of the router from the damage table) hierarchically spreads to a comprehensive damage for the overall system (e.g., 13.19% damage in Scenario #1), while a cyberattack to an insignificant asset (e.g., 80% damage of the optical switch from the damage table) has little effect on the mission capability of the overall system (e.g., 0.99% damage in Scenario #2). The intermediate damages also show that the comprehensive damage of the overall system depends on its composition and the relationship among the components of the system. As shown in the results of Scenario #3, minimal damage (4.75% intermediate damage of the asset layer) is escalated into large damage (19.43% overall damage).

These experiments demonstrate that our comprehensive assessment method can accurately assess real-world cyber damages to the overall defense mission system at the mission level.

4.2 Discussion

Recent studies of cyber damage assessment tried to obtain the quantitative mission damage. Some utilized the common vulnerability scoring system (CVSS) [14] to determine the damage in the asset level, such as [7] and [8], whereas others estimated measures that represent the mission damage from cyberattacks, such as [10] and [12]. However, compared with these representative studies, our method has better performance.

To verify this assertion with respect to accuracy, we apply the method of [7] and [8] to Scenario #2 in our experiment. Table 3 lists the results of the comparison.

As explained in the result of Scenario #2 in our experiments, the role of A20, as an auxiliary asset, is almost negligible in the missile defense system. Thus, the overall system will only be marginally affected by the cyberattacks, despite the damage of A20. Table 3 proves that our method assesses the cyber damage with higher accuracy and correctly indicates this situation.

For another verification, we compared the method in this study with [10] and [12] with respect to rapidity. Our method immediately assesses the cyber damage once a cyberattack is identified at the asset layer. It only needs the in-

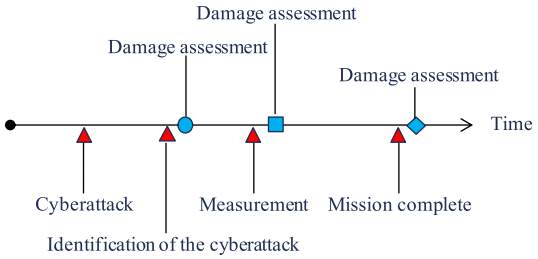

Fig. 3 Time diagram of cyberattack and damage assessment.

formation on the cyberattack and the targets, without any estimation of the measures. However, during the assessment, [10] and [12] require some time to estimate their measures, such as MOEs for missions in [10] and mission delay in [12]. To easily understand the differences among these studies, Fig. 3 shows the time diagram of a cyberattack and the damage assessment.

In Fig. 3, the red triangles mean major events about the cyberattack. The blue circle, square, and diamond are the moments of damage assessment in our study, in [10], and in [12], respectively. Our method is the fastest to assess the damage of the cyberattack.

As we discussed in this section, the method proposed in this study has strength in terms of accuracy and rapidity for the damage assessment of cyberattacks.

5. Conclusion

We developed a comprehensive method for assessing damage from cyberattacks on an entire defense mission system at the mission level, and proved the performance and practicality of our method with experiments. The outcome of this study can be applied in a real cyber war situation and provide accurate and fast results of cyber damage assessment. Therefore, this comprehensive method contributes to overcome the limitations of the existing studies, such as insufficient accuracy, late assessment, and impractical measures on cyber damages, by enhancing the mission-level damage assessment of a cyberattack.

References

[1] F. Yildiz, "Modeling the effects of cyber operations on kinetic battles," Calhoun: The NPS Institutional Archive DSpace Repository, Dudley Knox Library, Naval Postgraduate School, Monterey, CA, 2014.
[2] C. Lala and B. Panda, "Evaluating damage from cyber attacks: A model and analysis," IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol.31, no.4, pp.300–310, 2001.
[3] M.R. Grimaila and L.W. Fortson, "Towards an information asset-based defense cyber damage assessment process," IEEE Symposium on Computational Intelligence in Security and Defense Applications, Honululu, HI, USA, pp.206–212, 2007.
[4] S.J. Yang, J. Holsopple, and M. Sudit, "Evaluating threat assessment for multi-stage cyber attacks," IEEE Military Communications Conference, Washington, DC, USA, 2006.
[5] P.A.S. Ralston, J.H. Graham, and J.L. Hieb, "Cyber security risk assessment for SCADA and DCS networks," ISA Trans., vol.46, no.4, pp.583–594, 2007.
[6] C.-W. Ten, C.-C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," IEEE Trans. Power Syst., vol.23, no.4, pp.1836–1846, 2008.
[7] B.J. Argauer and S.J. Yang, "VTAC: Virtual terrain assisted impact assessment for cyber attacks," Proc. SPIE – The International Society for Optical Engineering, vol.6973, 2008.
[8] G. Jakobson., "Mission cyber security situation assessment using impact dependency graphs," 14th International Conference on Information Fusion, Chicago, IL, USA, 2011.
[9] I. Kotenko and A. Chechulin, "A cyber attack modeling and impact assessment framework," 5th International Conference on Cyber Conflict, Tallinn, Estonia, 2013.
[10] S. Musman, A. Temin, M. Tanner, D. Fox, and B. Pridemore, "Evaluating the impact of cyber attacks on missions," International Conference on Information Warfare and Security, 2010.
[11] S. Patel and J. Zeveri, "A risk-assessment model for cyber attacks on information systems," J. Comput., vol.5, no.3, 2010.
[12] N. Wagner, C.Ş. Şahin, M. Winterrose, J. Riordan, D. Hanson, J. Peña, and W.W. Streilein, "Quantifying the mission impact of network-level cyber defensive mitigations," Journal of Defense Modeling and Simulation: Applications Methodology, Technology, vol.14, no.3, pp.201–216, 2017.
[13] C. Dickerson and S. Soules, "Using architecture analysis for mission capability acquisition, research development and acquisition," Office of the assistant secretary of Navy, Washington D.C., 2002.
[14] Common Vulnerability Scoring System, https://www.first.org/cvss
[15] B. Genge, I. Kiss, and P. Haller, "A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures," International Journal of Critical Infrastructure Protection, vol.10, pp.3–17, 2015.