Multimed Tools Appl (2019) 78:3153–3170
https://doi.org/10.1007/s11042-018-5897-5

Modified cyber kill chain model for multimedia service environments

Hyeob Kim[1] · **HyukJun Kwon**[2] · **Kyung Kyu Kim**[1]

Received: 10 September 2017 / Revised: 28 January 2018 / Accepted: 13 March 2018 /
Published online: 7 April 2018

Abstract The sudden rise in the frequency and sophistication of cyber threats has become a hindrance to the steady development of internet of things (IoT)-based multimedia service environments. The framework currently in use for understanding and analyzing cyber threats in the information security (IS) field is the *cyber kill chain* model. Of these threats, a particular threat that involves advanced and persistent attacks on a designated target (company that provides multimedia services) and causes large-scale damage is referred to as an advanced persistent threat (APT). As there can be numerous threat points in an IoT-based multimedia service environment with networks of various heterogeneous devices connected through multiple routes, an understanding of the potential routes of the threats is crucial. APTs are generally divided into the infiltration stage from the outside into the inside of an organization, and a threat stage that occurs within an organization. The existing kill chain model in the IS field is problematic in that it cannot fully express the actions that occur inside an organization. However, many attacks that occur in today's IoT-based multimedia service environments are performed after infiltration of an insider or the organization. Thus, it is important for actions that occur on the inside to be clearly schematized to secure visibility in the multimedia service environment. This study analyzes the limitations of the existing model, and proposes a revised cyber kill chain model for multimedia security that can explain threats within an organization in addition to external threats.

✉ HyukJun Kwon
gloryever@sch.ac.kr

Hyeob Kim
hyubiii@yonsei.ac.kr

Kyung Kyu Kim
kyu.kim@yonsei.ac.kr

[1] Graduate School of Information, Yonsei University, Seoul, South Korea

[2] Department of IT-Finance Management, Soonchunhyang University, Asan, South Korea

Keywords Multimedia service environment · Cyber kill chain · Endpoint detection and response · Internet of things environment · Multimedia security

1 Introduction

With the recent advances in information and communication technology (ICT), various services are now being offered by connecting the internet with objects. The internet of things (IoT) is currently being used in various fields, particularly in the field of multimedia service environments. The IoT has many merits in multimedia service environments, such as the ability to provide convenient data transmission and receipt, and expanding new service markets. However, these merits are accompanied by security threats that may occur based on various heterogeneous cable and wireless communication pathways [28]. Therefore, the current generation is in need of research on multimedia security to account for threats that may occur at the endpoints (smart devices, cloud services, networks, etc.) of various platform environments [13].

Cyber attacks in the past were typically indiscriminate without a designated target. However, attacks on today's multimedia service environments are transforming into goal-oriented attacks on specific targets. Although personnel and material resources are being invested to defend against cyber attacks across the world, these attacks continue to increase, and the amount of damage they cause has also risen as a result [20]. Hence, information security (IS) for multimedia service environments is regarded as one of the key topics of interest among executives and decision makers in leading corporations around the world [12, 21]. Nevertheless, the resources that can be dedicated to addressing increasing cyber threats are limited.

Recent cyber threats have become more advanced and complex [20]. To easily understand and quickly react to cyber threats in multimedia service environments, we need a framework to analyze the concept of threats in a structured manner [27, 28]. The cyber kill chain model is used in various ways as a framework that explains today's advanced persistent threats (APTs). Using this model, the processes of complex, advanced persistent threats in a multimedia service environment can be easily understood, and a quick counterstrategy can be established against threats at each stage.

As the name "kill chain" implies, attacks can be successfully blocked by cutting off a link in each stage of a threat that is connected by a chain of links. However, IoT-based endpoints, including people, objects, and services, are easily infiltrated by phishing, SMishing, and social engineering attacks, and an attacker is able to infiltrate an organization through these attacks [16, 23].

Many years have passed since the introduction of the cyber kill chain model as a framework for understanding advanced persistent threats in the information security field. While our understanding of threats has improved through this model, there are still endless security accidents resulting from advanced persistent threats. There has been very little research on the protection of endpoints that are located inside an organization in a multimedia service environment. Moreover, researchers continue to argue that the kill chain model in the existing information security field is insufficient to explain threats that occur within an organization. If the model that explains threats is inaccurate or imperfect, the counterstrategies formed against these threats will inevitably be inadequate.

In this paper, we revise and supplement the courses of action matrix that is currently used in the information security field, by focusing on endpoint protection at each cyber kill chain stage

in multimedia service environments. This can provide prevention, detection, and counteraction functions from the installation stage to the C2 (command and control) stage that are relevant to endpoint areas based on the cyber kill chain. This will lead to a multi-level security effect in the multimedia service environment, where counteractions are automated to increase the efficiency of endpoint security management in enterprise security. Moreover, this will enable real-time blocking and counteraction through an analysis of actions that occur at the C2 stage, analysis of future accidents, and the recording of inspection traces.

Finally, we analyze the characteristics and limitations of the cyber kill chain models (linear and circular models) that have been proposed in the information security field. Based on this analysis, we propose a revised cyber kill chain model that can explain threats inside an organization that have not been accurately expressed in the existing kill chain models in multimedia service environments.

2 Related work

2.1 Multimedia services, internet of things, and multimedia security

Multimedia services in the IoT environment can be defined as services that are provided through various terminals and media, such as smartphones, laptops, and IPTVs, which combine audio and video broadcasts or multicasts based on the IoT with data, and connect voices via wired and wireless communication networks and broadcasting networks [11]. Moreover, these services provide multimedia content through interactions with various types of content, networks, and devices based on the IoT.

Specifically, user and IoT device authentication involves security measures, ranging from the use of access control and capability certificates to mutual authentication between server and user for multimedia in the IoT environment. Among these, several aspects of the user side involve critical securities issues [17]. First, regarding access control, the multimedia server controls a list of hosts who are either authorized to join the service group or excluded from it. When a user or an IoT device sends a request, the server checks its access rights in the access control list to determine whether the IoT devices are permitted. It is necessary to note that updating this list regularly is important because the list may change dynamically with new authorizations or exclusions. Second, ability certificates are usually issued by a designated certificate authority. An ability certificate contains information about the identity of the host and a set of rights. It is used to authenticate the user and give each device right to access multimedia data. A third aspect is mutual authentication in which the server, user, and IoT devices authenticate each other via cryptographic means.

The IoT refers to technology that can connect the internet and various devices, including smart devices, radio frequency identification (RFID) tags and sensors with limited resources, which can interact and cooperate to implement communications, enhancements, or service tasks [2, 28]. Such networks enable the provision of high-capacity multimedia services based on increased demand for applications, such as VoD, IPTV, and VoIP. Gartner predicts that over 26 billion companies will be interconnected and will create various innovation and business opportunities, such as multimedia services, by the year 2020 [9]. Figure 1 below shows an example of an IoT-based multimedia service structure.

Security in the IoT has become extremely important for various multimedia application programs. This is because the IoT is designed so that multiple application programs can be

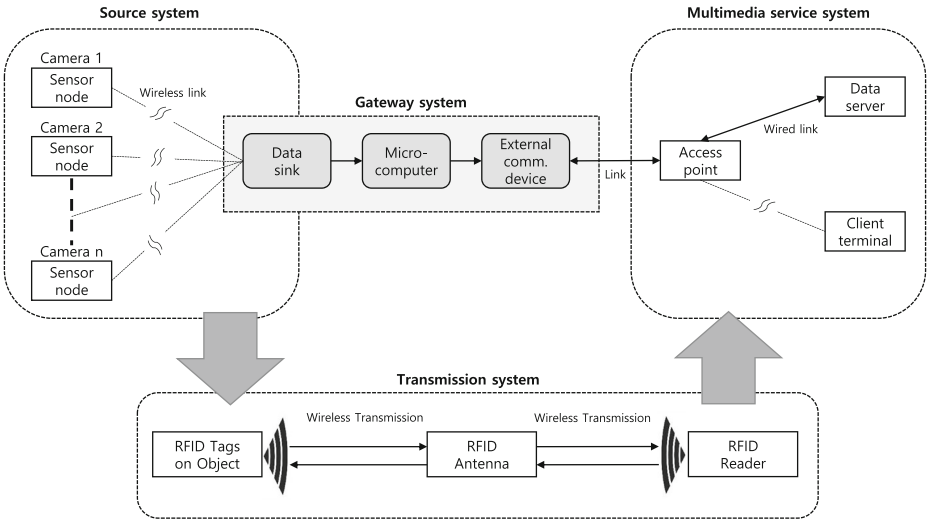

Fig. 1 Example of multimedia service architecture in the context of IoT [28]

operated across a wide range without verifying their users, which means that both the application programs and users are vulnerable to security threats [18]. For example, hackers can misuse the weaknesses of application programs and sensors, and malicious users can access the IoT to perform malicious service attacks. Further, attackers can steal IDs belonging to legitimate users and manipulate shared multimedia data or overconsume network resources so that the service is restricted or suspended for other users. Table 1 lists the countermeasures and technology that can be applied in response to security threats to existing multimedia services.

Denial of service attacks can occur when the sender of a data packet cannot be authenticated. As the sender is not authenticated, the system is prone to malicious codes, and this may lead to a distributed denial of service (DDoS) attack. In the multimedia service environment, it is important to prevent infection by malicious codes by authenticating the packet sender and only sending appropriate data while converting it for services, such as mobile IPTV or open IPTV. Moreover, the business owner must install a firewall and computer vaccine program in user devices so that swift measures can be applied when a new malicious code is detected through an immediate security update.

Table 1 Countermeasures and technology applied to address security threats to existing multimedia services [11]

Types of Attack	Countermeasure	Applied Technology
Denial of Service Attacks	Only receive messages from legitimate users	Authentication protocol, firewall, security update
Content Disclosure	Application of copy prevention technology, increasing the penalty	DRM (water marking, finger printing)
Watching Disturbance	Mutual authentication between user devices and servers	Authentication protocol, cryptographic methods
Charging Information Manipulation	Buyer and seller authentication, ensuring integrity of payment information	Authentication protocol, cryptographic methods, message signature

Content disclosure is a vulnerability that occurs during the transmission and management of multimedia content. To prevent content disclosure, a multimedia content copy prevention method must be applied. Some applied technology includes watermarking, fingerprinting, and other Digital Right Managements (DRMs).

Watching disturbance occurs owing to a vulnerability in which messages from the IGMP protocol, which is used for user group management in the multimedia system, and the RTSP protocol, which is used to control multimedia streaming, are not authenticated. Message verification through mutual authentication between the user device and server is needed to resolve such issues. This requires the sending and processing of only legitimate messages through a mutual authentication protocol, and the prevention of message forgery by encryption of transmitted data, thus ensuring integrity.

Charging information manipulation is a vulnerability that may occur when authentication or encryption is not properly designed for use in payment systems in multimedia services. To solve this issue, there must be a mutual authentication process between the purchaser and vendor before the payment system can be used. This requires the verification of legitimate vendors and purchasers through an authentication protocol, and ensuring of integrity through the encryption of transmitted data. Non-repudiation functions must be provided in the future through signatures on payment information, and time stamps or random sampling numbers must be added to prevent retransmission attacks.

However, there have only been a few studies thus far on security mechanisms that can respond to the above threats. Therefore, it is essential to establish security strategies to protect multimedia application programs that are streamed through the IoT.

Multimedia security is required in order to provide continuous IoT-based multimedia services. To achieve this, the various risk factors that may occur during the production and delivery of multimedia data must be considered, and a framework that can address these risk factors at each stage is needed.

2.2 Advanced persistent threat

Advanced persistent threats are known to have originated from the United States Air Force (USAF). In 2009, Cloppert wrote in a blog that he first heard the term “advanced persistent threat” in a meeting of the USAF in 2006, describing it as an “extremely high-level enemy that participates in the information war with long-term goals and strategies” [5]. As another frequently used definition, Mandiant (currently M&A with FireEye), which is an information security company in the United States, defined advanced persistent threats in a report titled “M-Trends: The Advanced Persistent Threat” as “a group of attackers who perform systematic attacks on the computer networks belonging to the United States government or private enterprises, and interact and work together with a high-level objective”, and this definition is still widely cited [15].

In this paper, we focus on advanced persistent threats because traditional threats and threats in multimedia service environments have drastically different characteristics. Further, this paper will clearly indicate the direction in which threats are evolving, and discuss many implications. Advanced persistent threats are “advanced” and “persistent” threats, and this viewpoint is shared in many different papers. Two papers were selected by referencing preceding studies for common keywords that appear in the definition and description of risks, and the relevant content has been compiled into Table 2.

Table 2 Characteristics of APT [26]

	Bejtlich [3]	Command Five [6]	Keywords that Convey Risk
Advanced	Refers to attackers who can handle a wide range of computer invasions. They can use vulnerabilities that are well known by the public or research new vulnerabilities, and develop an exploit that matches their target.	Hackers have the ability to avoid detection. They can connect to well-protected networks and maintain their connection. Hackers generally adjust very well.	Well-known vulnerabilities Research new vulnerabilities Multiple attack methodologies
Persistent	Attackers are officially assigned work to complete a mission. They do not invade by using a coincidental opportunity. They receive orders like in an intelligence unit, and work to satisfy the commissioner.	Hackers attempt to access our computer network and we attempt to block them. However, the persistence of their threats makes it difficult. Hackers are extremely difficult to eliminate once they gain access.	Master Period Maintain the level of interaction
Threat	The enemy does not perform simple code manipulation attacks without a purpose. The enemy is a threat. They are organized, have funding, and have motivation. Some people refer to them as a diverse group that is composed as a gang.	Hacker threats include the ability to access and obtain sensitive information that is electronically stored in addition to the intent or idea of attacking.	Organization Goal Target Attack method

"Advanced" refers to the attacker's abilities, and is indicative of the ability to invade all domains in a system. Various attack methods and tools are combined as needed for an attack. Well-known vulnerabilities can be used, but they can also research new vulnerabilities or develop exploits that match their target. Finally, they also have the ability to avoid detection for discreet attacks.

"Persistent" refers to discreet attacks that occur endlessly over a long period of time until the attacker succeeds in achieving their goal. They maintain continuous interaction with the target system until the last attack.

Unlike traditional threats, there is a clear purpose regarding the motive of the attack, and a clearly identified target for the attack. The threatening attacker can be one individual or an organized group of individuals. They also have sufficient funds to perform their attacks. Unlike in the past, the attack targets have been expanded to include the government, defense industry, and civilians (multimedia services, etc.), and attacks are performed for the extraction of core information or intellectual property rights, in addition to political, economic, and military purposes.

2.3 Endpoint detection and response

Endpoint detection has once again become a subject of interest because existing anti-virus solutions are unable to cut off the chains of advanced persistent threats. Although it has been years since the concepts of advanced persistent threats and the kill chain model were introduced, endpoints are still vulnerable to advanced persistent threats, and refer to people, which are the weakest link in the information security field. It is important to note here that the

existing kill chain model is unable to fully schematize the threat activities that occur in an organization, including endpoints.

Advanced persistent threats can generally be divided into two categories. There is the stage of infiltrating an organization from the outside, and the threat stage that occurs within the organization. In general, once an attacker infiltrates an organization, the first base they arrive at is an endpoint, meaning a PC (terminal) that is used by members of the organization. Therefore, endpoint protection is extremely important to defend against internal threats.

We first became interested in the cyber kill chain model when endpoint security began to be emphasized in the corporate security market. As endpoint detection and response (EDR) solutions were released after 2015, a new market was formed. These solutions were proposed to quickly respond to advanced persistent threats to corporate security. As implied by the name, they refer to solutions that respond automatically after detection of an infiltration or threat based on actions that occur at endpoints within an organization [8].

Because existing defense systems are insufficient to protect against current vulnerabilities, there must be an understanding of threats. The intention of each threat, the attacker's ability, doctrine, task patterns, and invasion patterns must be analyzed. Thus, policies that identify and defend against attack symptoms can be prioritized, and attackers' rates of success can be minimized.

As shown in Table 3, a defender will match the stage of the cyber kill chain with the detection, denial, disruption, degradation, deception, and destruction processes that need to be performed, and respond accordingly. We have revised and supplemented the courses of action matrix that is used in the existing information security field by focusing these processes on endpoint protection.

There are many different solutions for counteracting threats at each stage of the cyber kill chain. Traditional security solutions perform single security control functions for each of the three security controls that are represented by prevention, detection, and response. For example, NIDS performs detection functions, while a firewall is an example of a prevention control security solution.

Security can be improved by establishing diverse, multi-level security solutions. However, the solutions that are implemented involve an increased complexity of management as the number of attack surfaces increases. Further, as shown in the above table, the majority of traditional security solutions focus on prevention and detection. This shows the insufficiency of standardized services and solutions regarding how a security accident is countered when it occurs and if recovery is even possible.

The EDR solution overcomes the above limitation and focuses on automatic counteractions. Prevention, detection, and counteraction functions are provided simultaneously starting from the installation stage, which is part of the endpoint domain in the cyber kill chain, and up to the C2 stage. Therefore, it has the effect of multi-level security, and the efficiency of endpoint security management in multimedia security is improved by the automation of counteraction. Moreover, this enables real-time blocking and counteraction through an analysis of actions that occur at the C2 stage, analysis of future accidents, and recording of inspection traces.

The EDR solution first collects information on various actions that occur at endpoints in a multimedia service environment from the server, such as hashes of files that are currently in use, network connection data, processes and system events, and then detects threats through the indicator of compromise (IOC), and performs instant countermeasures. Further, it can analyze diverse actions through a time series analysis or machine learning by including

Table 3 Courses of modified action matrix [10]

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall access control lists (ACLs)				
Weaponization	Network-based intrusion detection system (NIDS)	Network-based intrusion prevention system (NIPS)				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	Host-based intrusion detection system (HIDS)	Patch	Data execution prevention (DEP)			
Installation	EDR HIDS	EDR “chroot” jail	Antivirus (AV)			EDR
C2	EDR NIDS	EDR Firewall, ACL	NIPS	Tarpit	DNS redirect	EDR

Table 4 EPP vs. EDR

Category	Endpoint Protection Platform (EPP)	Endpoint Detection and Response (EDR)
Detection Site	Endpoint	Server
Detection Method	Signature, machine learning, etc.	Indicator of compromise (IOC), machine learning, etc.
Security Accident Survey	Unsupported	Supported
Interested Security Control	Prevention, detection	Counteraction

security information and event management (SIEM) roles [1]. Therefore, the goal of endpoint security may be the same, but there are distinctions from the existing signature-based anti-virus programs.

Gartner defined the endpoint protection solution market in the corporate environment by dividing it into endpoint protection platforms (EPPs) and EDR approaches. An EPP solution combines anti-malware, personal firewalls, ports, and device control functions [26]. Many EPP solutions are composed of a combination of almost all security functions that are available at endpoints, such as keyboard security functions, data leakage prevention functions, and vulnerability scans including the above functions. Differences from EDR solutions are shown in Table 4.

The boundaries between the two enterprise markets of today that are shown in the Table are gradually disappearing, and Gartner predicts that EPP and EDR will merge into a single market by 2019 [19].

2.4 Characteristics of cyber kill chain model

The term “kill chain” was initially used as a military concept. It referred to the preemptive detection of a target, selection of an attack method based on this, and a series of steps to be carried out until the target was destroyed. Since then, Lockheed Martin integrated this concept to fit the cyber attack scenario, which led to the birth of the cyber kill chain [10]. Table 5 shows the different operations of the attackers at each stage.

Lockheed Martin [10] established defense standards regarding advanced persistent threats and created resistance methods; they called their process the intrusion kill chain. They also wrote that if the attacker’s threat, intention, capacity, principles, and patterns are understood, the organization’s resilience can be secured even through the processes and systems at the core

Table 5 Kill chain stages from attacker’s perspective

Stage	Content
Stage 1 (Reconnaissance)	Collect information such as e-mail addresses and conference information.
Stage 2 (Weaponization)	Combine exploits and backdoors to insert payload.
Stage 3 (Delivery)	Transfer the weaponized file to the victim system through an e-mail, web, or USB.
Stage 4 (Exploitation)	Use vulnerabilities in order to run the code in the victim system.
Stage 5 (Installation)	Install a malicious program in the attack target’s asset.
Stage 6 (Command & Control)	Open a channel to remotely control the victim system and command accordingly.
Stage 7 (Action on Objectives)	When access that is equivalent to handling the actual keyboard becomes possible, the invader has achieved their purpose.

of vulnerability. The intrusion kill chain is becoming a method that can quickly prevent system damage because it facilitates preemptive and systematic countermeasures at each stage of a cyber attack, increases intrusion costs when the attacker attempts another attack as a preemptive defense measure, and provides useful analyses of all damage incurred by taking a survey after that attack.

The attacker of an advanced persistent threat performs endless attempts at invasion, and attacks by making changes based on their success or failure. The Lockheed Martin model [10] shows the entire defense procedure from the combined start to finish. In this model, if every repetitive attempt from the attacker is predicted from a defense perspective and countermeasures are taken for the next stage before the attack advances to the next stage, or if even one of the attack attempts is blocked during the current stage, the entire attack will be disrupted, and the attacker will be unable to succeed in their attack [25].

The cyber kill chain refers to a model of advanced persistent threats, which represents cyber attacks that are becoming more complex. This model not only helps us easily understand and analyze cyber threats, but can be utilized to establish strategies for defending against or mitigating threats. The kill chain models that have been proposed in the information security field thus far can be divided into linear and circular models.

2.4.1 Linear model

Lockheed Martin, the organization that introduced the cyber kill chain model with the concept of advanced persistent threats, explained "threat" using a 6-stage flow, beginning from reconnaissance and leading up to actions on objectives [4]. In a study that was presented subsequently, this flow was expanded into 7 stages as shown in Fig. 2, and this has become the kill chain model that is most frequently cited today [10].

In this linear model, the flow of a threat is described in a linear direction, and when the attacker completes their goal, the threat is considered to be terminated. Unlike Lockheed Martin, FireEye (previously Mandient) proposed a model, shown in Fig. 3, that emphasizes the persistency of threats. Although this is also a linear model, the last stage is the stage of maintaining persistence, which stresses that a threat does not end after one cycle.

2.4.2 Circular model

Command Five introduced a circular kill chain model in which each threat is repeated as shown in Fig. 4. Each stage and order of a threat is similar to that of the linear model, but the circular diagram emphasizes that the threat is repetitive. Advanced persistent threats certainly have the characteristic that all stages are repeated from when an attack begins until it is finished. A threat is a state in which a connection is made with the C2 (Command and Control) server. Moreover, as the word "persistent" in the term "advanced persistent threat" implies, all stages are maintained for a long time. Expressing persistence as a single stage, as in Fig. 3, is not logical. This is because vulnerability attacks from the reconnaissance and the installation stages are continuously repeated while a connection is maintained with the C2 server. Therefore, the circular model is more logical than the linear model.

The dwell time of a malicious code is used as an index that shows the persistence of an advanced persistent threat. According to a report by FireEye, it takes a global average of

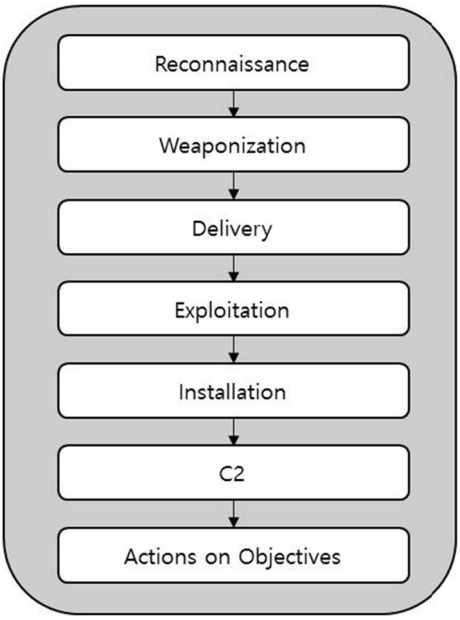

Fig. 2 Lockheed Martin's cyber kill chain model [10]

99 days until an organization discovers that there is an invasion through an APT attack, and this average is even longer in the Asia region at 172 days [7]. Fortunately, this time period is gradually decreasing every year. However, the fact that it takes an extremely long time to detect an invasion implies that it is very difficult for an endpoint user to become aware that their PC is being controlled by the C2 server.

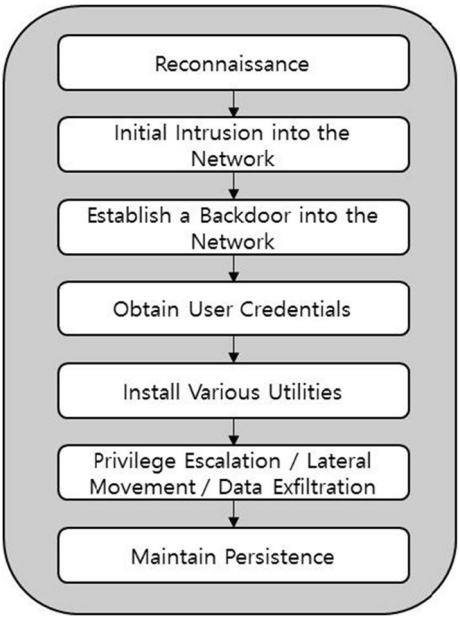

Fig. 3 FireEye's cyber kill chain model [15]

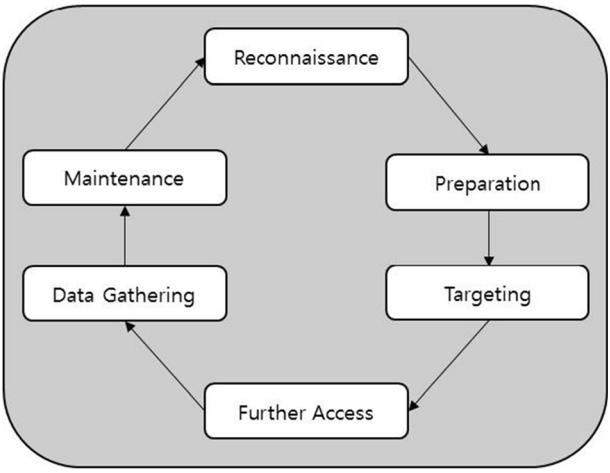

Fig. 4 Command Five's cyber kill chain model [6]

2.5 Limitations of cyber kill chain models

The aforementioned two kill chain models have the limitations listed in Table 6.

The argument that existing kill chain models are limited when it comes to explaining internal threats has continued to this day. At Black Hat USA 2016, Malone argued that the existing kill chain models are unable to properly explain internal risks and that the entire process from reconnaissance to actions on objectives focuses on the actions for external risks. He pointed out that the final actions at the objective stage particularly fail to adequately explain internal risks. There is also insufficient explanation of the stage of accessing the target system after infiltration of the organization as well as the stage of manipulating the target system to achieve the objective; Malone referred to these stages as the internal kill chain and target manipulation kill chain, respectively [14].

Rutherford proposed the model shown in Fig. 5 by modifying Lockheed Martin's model. This model assumes that the existing installation stage occurs in the exploitation stage. Further, the stage that comes after C2 was expanded to intelligence gathering, objective execution, and exfiltration of information [24].

The newly expanded stages include an explanation of internal risks, unlike Lockheed Martin's existing model that only explains internal risks through C2. The three stages also emphasize that a threat does not only occur in a single direction. However, it is still not without the limitations of the existing linear models because its explanation of internal risks is abstract, and the attack objective is limited to exfiltration of information.

Table 6 Limitations of existing kill chain models

Model Type	Limitation
Linear Model	Advanced persistent threats have the characteristic of repeating each stage, and the channel is often maintained even after the attack is completed. However, the linear model is unable to account for this point.
Circular Model	The cycle of threats that occur outside the organization and the cycle of threats that occur from the inside have different threat attributes. However, the circular model is unable to explain these differences.

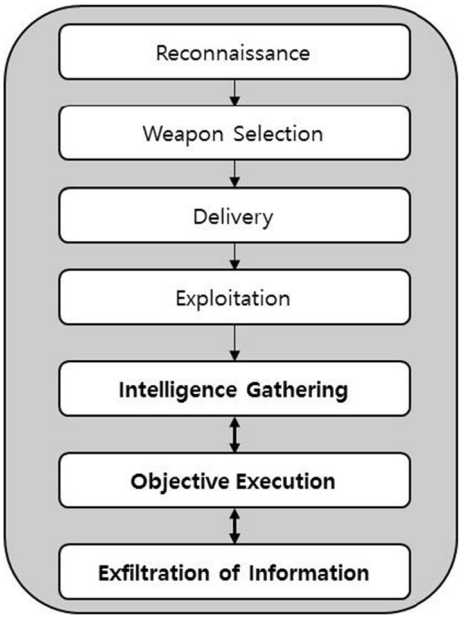

Fig. 5 Rutherford's cyber kill chain model [24]

3 Proposed modified cyber kill chain model for multimedia environments

The focus of today's information security is changing from defending against attacks that come from outside to defending against threats that occur from within [22]. Today, cyber invasions are more often caused by the actions of an insider rather than an outsider. Further, while advanced persistent threats may be considered external threats, actions that occur upon infiltration of an organization actually appear in the form of using an insider's rights, such as attempting to raise rights through an insider's endpoint. Therefore, there must be an explanation of the actions of threats that occur in a multimedia environment, and this explanation may be regarded as important information for endpoint protection.

While existing cyber kill chain models may be appropriate for explaining external attacks, those models that also explain internal risks come with the aforementioned limitations. Therefore, this paper proposes a revised cyber kill chain model to schematize internal threats for a multimedia environment as shown in Fig. 6.

The model proposed in this study divides threats into two levels (external threats and internal threats). Internal threats are further categorized, and the model emphasizes the fact that the reconnaissance, weaponization, delivery, exploitation, and installation processes that occur in external threats are also present in internal threats. The processes from the reconnaissance stage to the installation stage are repeated and cycled in the same way for both external and internal threats, but their characteristics differ.

For example, in the reconnaissance stage, the attacker collects information on members of the organization through internet searches or social media in order to invade the organization's internal network. However, after invading the organization, technical reconnaissance is performed, such as by assessing the structure of the internal network and scanning the system. During the weaponization stage, the attacker may use a dropper that is disguised as a normal task document to infiltrate the organization, but after invading the organization, they use

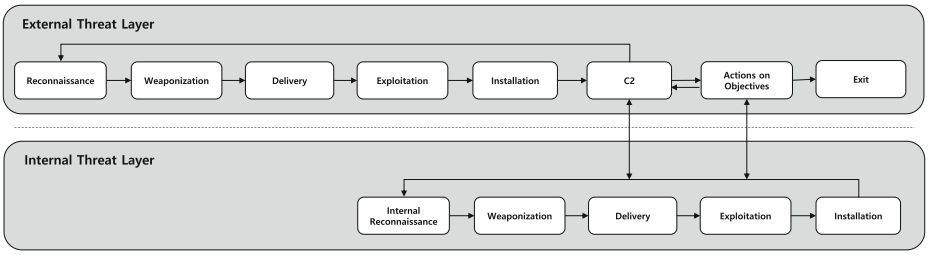

Fig. 6 Proposed revised cyber kill chain model

various hacking tools, compression files, encryption tools, etc. For delivery methods, the attacker uses sociotechnological methods, such as spear phishing to infiltrate the organization, but after invading, they use technical attacks.

As such, reconnaissance, weaponization, exploitation, and many other stages may be repeated in the same way in the organization, but external and internal threats have different attributes in terms of methodology. Therefore, countermeasures must differ for external threats and internal threats.

The existing models are unable to adequately express each stage of internal threats in detail, and attempt to explain them using one stage (C2). C2 may certainly imply connectivity and persistence, but if the model is abstract, the countermeasures cannot be detailed. The proposed model emphasizes the fact that internal risks must also be properly countered by securing visibility regarding threats that are made to endpoints, which are the weakest links in an organization. Table 7 below compares the countermeasures and limitations of the characteristics and threats of the previous models and the proposed revised model.

Table 7 Comparison of proposed model with previous models

	Linear Model	Circular Model	Proposed Revised Model
Features	- Expresses reconnaissance to installation as external risk, and C2 to the last stage as internal risk.	- Expresses the repetition of risks that were not explained by the linear model.	- Schematizes the internal risks that occur through C2 in detail. - Emphasizes that the reconnaissance, weaponization, and delivery processes differ for internal and external threats.
Measures Against Threats	- Measures for internal risks focus on countering the C2 server through NIDS.	- Measures for internal risks focus on countering the C2 server through NIDS.	- Emphasizes that focus should be on countering sociotechnological attacks for external threats, and focus should be on endpoints through HIDS and EDR for internal threats.
Limitations	- Unable to express the internal threats that occur while connected to the C2 server in detail.	- Internal risks and external risks are not distinguished.	

4 Conclusions

Most traditional information security solutions focus on prevention and detection. This reveals the insufficiency of standardized services and solutions regarding how a security accident is countered when it occurs and if recovery is even possible. EDR solutions attempt to overcome the above limitations and focus on automating counteractions in IoT-based multimedia service environments. This study revised and supplemented Lockheed Martin's courses of action matrix in the information security field, and used EDR solutions based on the cyber kill chain to construct a framework in which prevention, detection, and countermeasure functions are provided simultaneously from the installation stage to the C2 stage, which are relevant to the domain of endpoints in IoT-based multimedia service environments.

The EDR solution for multimedia service environments that was introduced in this study first collects information on various actions that occur at endpoints in the multimedia service environment from the server, such as hashes of files that are currently in use in the system, network connection data, processes, and system events, and then detects threats through the IOC, and takes instant countermeasures. Further, it can analyze diverse actions through a time series analysis or machine learning by including SIEM roles.

The existing kill chain models in the information security field merely explain internal threats through the C2 server that is connected to external threats. Access to the C2 server implies that threats have connectivity and persistence, and the agent of the threat is postulated as an outsider. Therefore, countermeasures made regarding threats thus far have involved blocking IP addresses to restrict access to C2 servers. However, securing visibility regarding actions that occur at endpoints in the actual multimedia service environment and quickly countering actions at each stage is even more critical. Thus, in addition to external threats, internal threats can be detected and countered in the multimedia service environment.

We have determined that threats posed by an outsider to the organization and threats posed by an insider are both extremely important factors for enterprise security with respect to advanced persistent threats that may occur in a multimedia service environment. Hence, a model that also emphasizes internal threats was formulated so that countermeasures can be taken against internal threats. Further, the proposed cyber kill chain model for multimedia service environments also addresses the limitations of existing models in the information security field and defines internal threats in a multimedia service organization in more detail.

This model can help security managers establish strategies against threats, secure the visibility of threats that occur within an organization in a multimedia service environment, and build countermeasures for each stage of infiltration. In future work, we intend to present detailed threat characteristics and countermeasures based on the model proposed in this study.

Acknowledgements This research was supported by the Soonchunhyang University Research Fund.

References

1. Alam M, Javed Q, Khan A et al (2017) Formal modeling and verification of security controls for multimedia systems in the cloud. Multimedia Tools Appl 76(21):22845–22870

2. Atzori L, Iera A, Morabito G (2010) The internet of things: a survey. Comput Netw 54(15):2787–2805
3. Bejtlich R (2010) What Is APT and What Does It Want? TaoSecurity Blog. https://taosecurity.blogspot.kr/2010/01/what-is-apt-and-what-does-it-want.html. Accessed 17 May 2017
4. Cloppert M (2009) Security intelligence: attacking the cyber kill chain. SANS Computer Forensics Blog. https://digital-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain. Accessed 17 May 2017
5. Cloppert M (2009) Security Intelligence: Introduction (pt1), SANS Computer Forensics Blog. https://digital-forensics.sans.org/blog/2009/07/22/security-intelligence-introduction-pt-1. Accessed 17 May 2017
6. Command Five Pty Ltd (2011) Advanced Persistent Threats: A Decade in Review. http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf. Accessed 17 May 2017
7. FireEye (2017) M-Trends 2017 Report. https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html. Accessed 17 May 2017
8. Firstbrook P (2017) Market guide for endpoint detection and response solutions. Gartner
9. Gartner (2011) Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. http://www.gartner.com/newsroom/id/2636073. Accessed 17 May 2017
10. Hutchins E, Cloppert M, Amin R (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Lead Issues Inf Warf Secur Res 1(1):80–106
11. Jung CS, Shin YT (2013) A study on verification of security threat and method of response for multimedia broadcasting and communication convergence services. J Korea Academia-Industrial Coop Soc 14(6):3032–3042
12. Kim H, Kim Y, Chang H (2016) Information security research classification for future multimedia environment. Multimedia Tools Appl 75(22):14795–14806
13. Kim H, Park S, Chang H (2016) A gap analysis study between multimedia security research and education by meta data analysis. Multimedia Tools Appl 75(20):12779–12793
14. Malone ST (2016) Using an Expanded Cyber Kill Chain Model to Increase Attack Resiliency. https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain-Model-To-Increase-Attack-Resiliency.pdf. Accessed 17 May 2017
15. Mandiant (2010) M-Trends 2010, The Advanced Persistent Threat. https://www2.fireeye.com/WEB-2010-MNDT-RPT-M-Trends-2010_LP.html. Accessed 17 May 2017
16. Moore JF (1993) Predators and prey: a new ecology of competition. Harv Bus Rev 71(3):75–83
17. Ndibanje B, Lee HJ, Lee SG (2014) Security analysis and improvements of authentication and access control in the internet of things. Sensors 14(8):14786–14805
18. Oracevic A, Dilek S, Ozdemir S (2017) Security in internet of things: A survey. In Networks, Computers and Communications (ISNCC), 2017 International Symposium on (pp. 1–6). IEEE
19. Ouellet E, McShane I, Litan A (2017) Magic quadrant for endpoint protection platforms. Gartner
20. Park W, Na O, Chang H (2016) An exploratory research on advanced smart media security design for sustainable intelligence information system. Multimedia Tools Appl 75(11):6059–6070
21. PWC (2015) Key Findings from the 2015 US State of Cybercrime Survey. http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf. Accessed 17 May 2017
22. Reidy P (2013) Combating the Insider Threat at the FBI: Real World Lessons Learned. https://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf. Accessed 17 May 2017
23. Rho S, Yeo S-S (2013) Bridging the semantic gap in multimedia emotion/mood recognition for ubiquitous computing environment. J Supercomput 65(1):274–286
24. Rutherford JR, White GB (2016) Using an improved cybersecurity kill chain to develop an improved honey community. In System Sciences (HICSS), 2016 49th Hawaii International Conference on (pp. 2624–2632). IEEE
25. Ryan J (2011) Leading issues in information warfare and security research. Academic Conferences Limited
26. Ryu H, Jeong S, Kwon T (2014) Advanced persistent threats: new paradigm of the evolving threat. The Magazine of the IEIE 41(4):16–30
27. Yoo T, Chang H (2013) The IT convergence framework design in the internet of things environment. EURASIP J Wirel Commun Netw 2013(1):53
28. Zhou L, Chao HC (2011) Multimedia traffic security architecture for the internet of things. IEEE Netw 25(3):35–40

Hyeob Kim is a Ph.D. candidate in Graduate School of Information at Yonsei University, Korea. He received a master degree in Information Systems from Graduate School of Information at Yonsei University, Korea in 2014. He has published a few research papers in domestic journals and conferences. His current research interests are in the areas of Industrial Security, Security Management, and System in Internet of Things Environment.

HyukJun Kwon is a professor of IT-Finance Management at Soonchunhyang University, Korea. He received his Ph.D. in Information System Management from Graduate School of Information at Yonsei University, Korea. He has published many research papers in international journals and conferences. He has been serve as session chairs and program committee for few international conferences and workshop; UNESST, CSA, ISA, and so on. His works have been published in Journals such as Journal of Computational Information Systems, and Computing and Informatics. His areas of concern are Multimedia Security, Blockchain Systems, Information Security Management, and Digital Currency.

Kyung Kyu Kim is Professor of Information Systems at Yonsei University, Korea. His current research interests are in the areas of virtual worlds, knowledge management, IT-enabled supply chain management, and behavioral issues in e-business. He has published his research works in Accounting Review, MIS Quarterly, Journal of MIS, Journal of the Association for Information Systems, Omega, Decision Sciences, Information and Management, Database, Journal of Organizational Computing and Electronic Commerce, Journal of Business Research, Electronic Commerce Applications and Research, Journal of Information Science, International Journal of Information Management, and Journal of Information systems.