

Threat Modeling Analysis on FireStormcx's Webcam System

Jong Jin Cho, Miyoung Kang

School of Cybersecurity, Korea University, 145 Anam-ro, Seongbuk-gu, Seoul, 02841, Korea

jongjcho@korea.ac.kr, dasuni@korea.ac.kr

Abstract- Since the COVID 19 pandemic creates enormous casualties in the world, it rapidly changes the working environment. It significantly increased the virtual meeting among the team members at work. These require many pieces of equipment. Among the components, a webcam is becoming the most important piece of equipment in virtual meetings. Since the webcam becomes the important factor in the meeting, the attacks on the webcam are enormously increased. In many cases, when a group of hackers attacks a webcam, it creates critical privacy breaches. Therefore, to prevent these types of critical breaches, this paper closely conducts the Threat Modeling analysis based on DFD and STRIDE techniques on FireStormcx's webcam. Additionally, these types of Threat Modeling analysis result to create a recommended threat remediation plan.

Keywords—Privacy, Webcam, Threat Modeling, STRIDE, DFD

I. INTRODUCTION

Due to the rapid increase of virtual meetings because of COVID 19, the webcam becomes the essential hardware for both medical treatment and work environment worldwide. The webcam provides not only comfortable work from the home environment but also non faced to faced medical treatment due to the COVID 19 pandemic. The webcam is more and more into our daily environment. However, since webcam usage is massively increasing, the attack on webcams is more comprehensive and sophisticated. For instance, former FBI Director James Comey strongly urged that the attack on the webcam could cause a significant privacy breach [1]. Therefore, in order to prevent these types of attacks, not only secure the network environment, but also webcam has to guarantee the design assurance fully. To fully accomplish the design assurance, the threat modeling analysis must comply. Therefore, in this paper, we fully conduct the Data Flow Diagram (DFD), STRIDE, and comprehensive remediation plan based on the result from the threat modeling process. Lastly, we select the target system as FireStormcx's webcam, a small and simple webcam structure that directly connects to Raspberry Pi.

II. THREAT MODELING

The Threat Modeling process is one of the techniques that is used during the part of design assurance level during the software development stage. It is a process specifically targeted to find structure vulnerabilities and potential threats, which ultimately fully comply with the secure by design approach. In addition, many international standards such as IEC 62443 require threat modeling as part of the necessary process [2]. The threat modeling concept starts in the late 1990s. Especially, one of Microsoft's decorated security software engineers, Jason Garms introduced the first concept of STRIDE analysis via his internal technical document, "The threats to our product"[3][7], which are one of the Threat Modeling Process. On the other hand, security engineers such as Adam Shostack and Loren Kohnfelder significantly dedicated Threat Modeling Process becomes one of the critical processes in the secure by the design process. In this paper, we initiated two essential processes, which are DFD and STRIDE analysis.

A. STRIDE

STRIDE analysis was first conducted by Praeit Garg and Loren Kohnfelder from Microsoft [3][6]. It is a unique process that completely conducts the analysis based on the total attacker's viewpoint. The STRIDE has six attack properties which are shown in Table 1. The STRIDE analysis conducts based on the Target systems' DFD. It can conduct the analysis with all the six properties from STRIDE; however, in some cases, such as Repudiation, it can't apply in the Data Store entity from DFD. The STRIDE application on DFD are shown in Table 2.

Table 1. STRIDE's six properties [6]

Security Theme	Attack Property (STRIDE)
Authenticity	Spoofing
Integrity	Tampering
Non-Repudiation	Repudiation
Confidentiality	Information Disclosure
Availability	Denial of Service
Authorization	Elevation of Privilege

Table 2. The STRIDE application on FireStormcx's webcam DFD

Element	S	T	R	I	D	E
Entity	X		X			
Process	X	X	X	X	X	X
Data Flow		X		X	X	
Data Store		X		X		X

B. DFD

DFD is the abstraction viewpoint of the target system. It is a logical information flow tool that describes the data flow between the process to process in the system. The STRIDE analysis was conducted based on the vulnerabilities from the DFD. This diagram is produced by open platform software Microsoft Threat Modeling tool 2016. The DFD's 5 components are as shown in Table 3. Additionally, in this analysis, DFD is specified from context level to level 2, and those have to describe all the detailed components in the system. The detailed descriptions are as follows [4]:

1) **Cotext Level:** Very high level of the system. Provide the image of the entire system. Significantly abroad overview of the target system.

2) **Level-0:** The high level of the system. Provide an abroad overview of the target system. It offers easily digestible but very little detail.

3) **Level-1:** The middle level of the system. Provide a general overview. It adds more detail compared to level 0. It is broken down into sub processes.

4) **Level-2:** The bottom level of the system. Provide a specific overview of the system. It is generally, broken into functions by function of the target system.

III. DATA FLOW DIAGRAM ON FIRESTORMCX'S WEBCAM

The FireStormcx's webcam is divided from context level to level 2. Each analysis was conducted as follows:

A. Cotext Level

Figure 1 is the Context Level of Data Flow Diagram. The context level has 2 Entities, 2 Processes, and 6 Data Flows. For example, the authorized user commands the E.2 Raspberry Pi (Webcam wired entity). Since The data flow F.1 goes to Raspberry Pi, F.1.1 from the Entity 2 Command flow goes the P.1 fswebcam application, this connects to the next E.3 Webcam lens through the F.1.2 configure data flow. Finally, the webcam lens sends the F.2 image data to fswebcam application. Ultimately, F.2.1 data goes E.2 Raspberry Pi entity. Lastly, these are divided through the entity's trust boundary.

B. Level 0

Figure 2 is the detail-specific version of the context level. The analysis resulted in 3 Entities, 7 Processes, and 14 Data Flows. In the analysis, there are some of the important steps discovered. F.1 flow connected to the P.1, F.1.1 flows to P.2 configure system Firmware in Raspberry Pi. F.1.2 Configure flow connects to the P.3 shell script. The shell script connects

Table 3. DFD's five components [4]

Element	Symbol	Description
Entity		Entities include source and destination of the data. Entities are represented by rectangle with their corresponding names.
Process		The tasks performed on the data is known as process. Process is represented by circle. Somewhere round edge rectangles are also used to represent process.
Data Store		Data storage includes the database of the system. It is represented by rectangle with both smaller sides missing or in other words within two parallel lines.
Data Flow		The movement of data in the system is known as data flow. It is represented with the help of arrow. The tail of the arrow is source and the head of the arrow is destination.
Trust Boundary		location on the data flow diagram where data changes its level of trust

the P.4 via the F.1.3. These data convert the P.5 to F.1.5. Lastly, P7 hits the E.3 via F.1.7 configure data. When E.3 webcam lens processed the data, the F2 to F.2.6 goes the image data file go through the same way from E.1; however, in the end, the data hits E.2 memory in Raspberry Pi

C. Level 1

Figure 3 is the detail-specific version of Level 0. The analysis resulted in 5 Entities, 17 Processes, and 29 Data Flows. This stage adds P.2, P.3, P.4, and P.5, in the Raspberry Pi infrastructure. Additionally, P9.1, P.9, and E.2 are added in P.8. On further analysis, E.4 C was added, and the P13 is the added infrastructure is added. For instance, P 13.1, P13.2, P13.3, and 13.4 are connected all F8.1, F8.2 F8.3, and F8.4 configure data flow to P13.

D. Level 2

Figure 4 is the extremely detailed version of Level 1. The analysis is conducted based on the previous level, which is the last stage level of the analysis. The analysis resulted in 5 Entities, 53 Processes, and 64 Data Flows. In this thesis, the important procedure such as P13.1 General Option breaking into P13.1.1 TO P13.1.3. and P13.2 Capture Option breaking into P13.2.1 to P13.2.8 and, P13.3 Output Option breaking into p13.3.1 to p13.3.8.

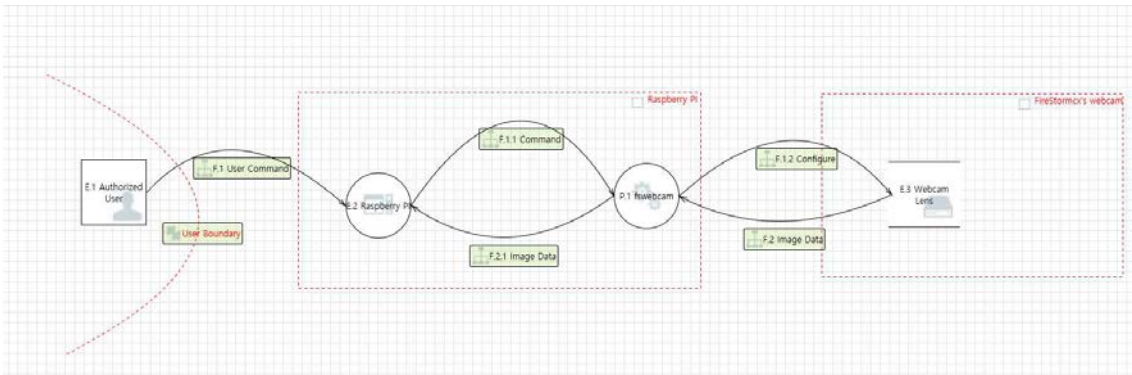


Figure 1. Context Level DFD

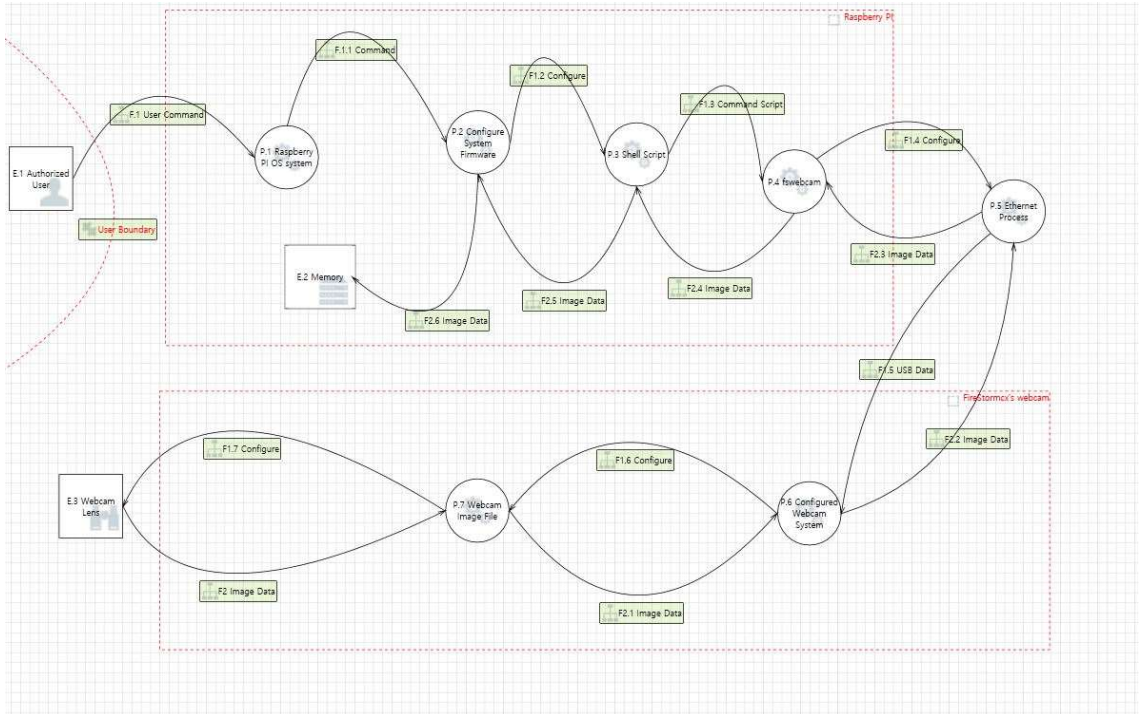


Figure 2. Level 0 DFD

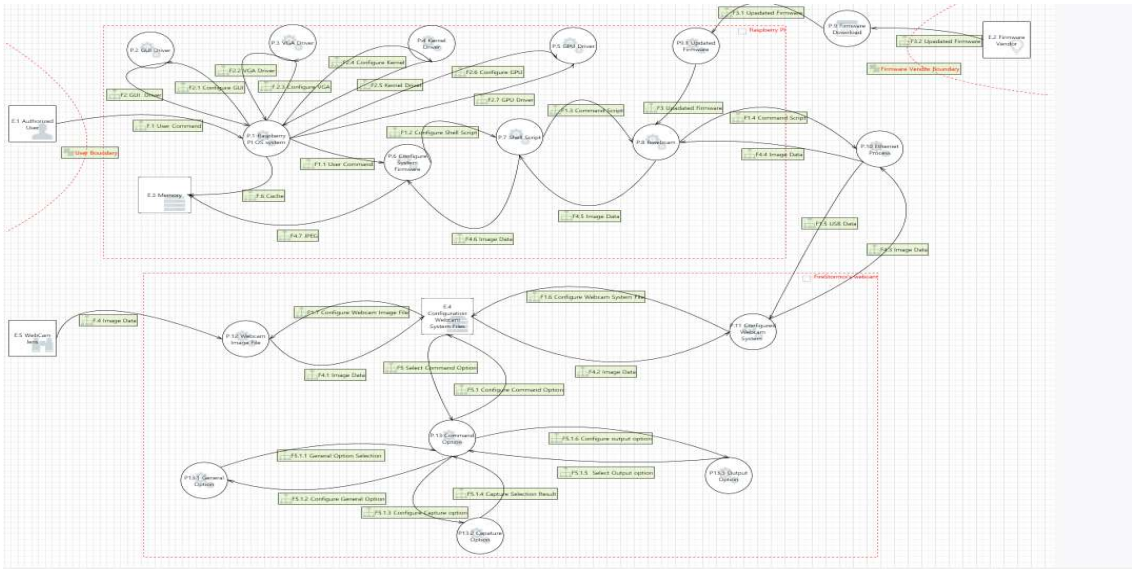


Figure 3. Level 1 DFD

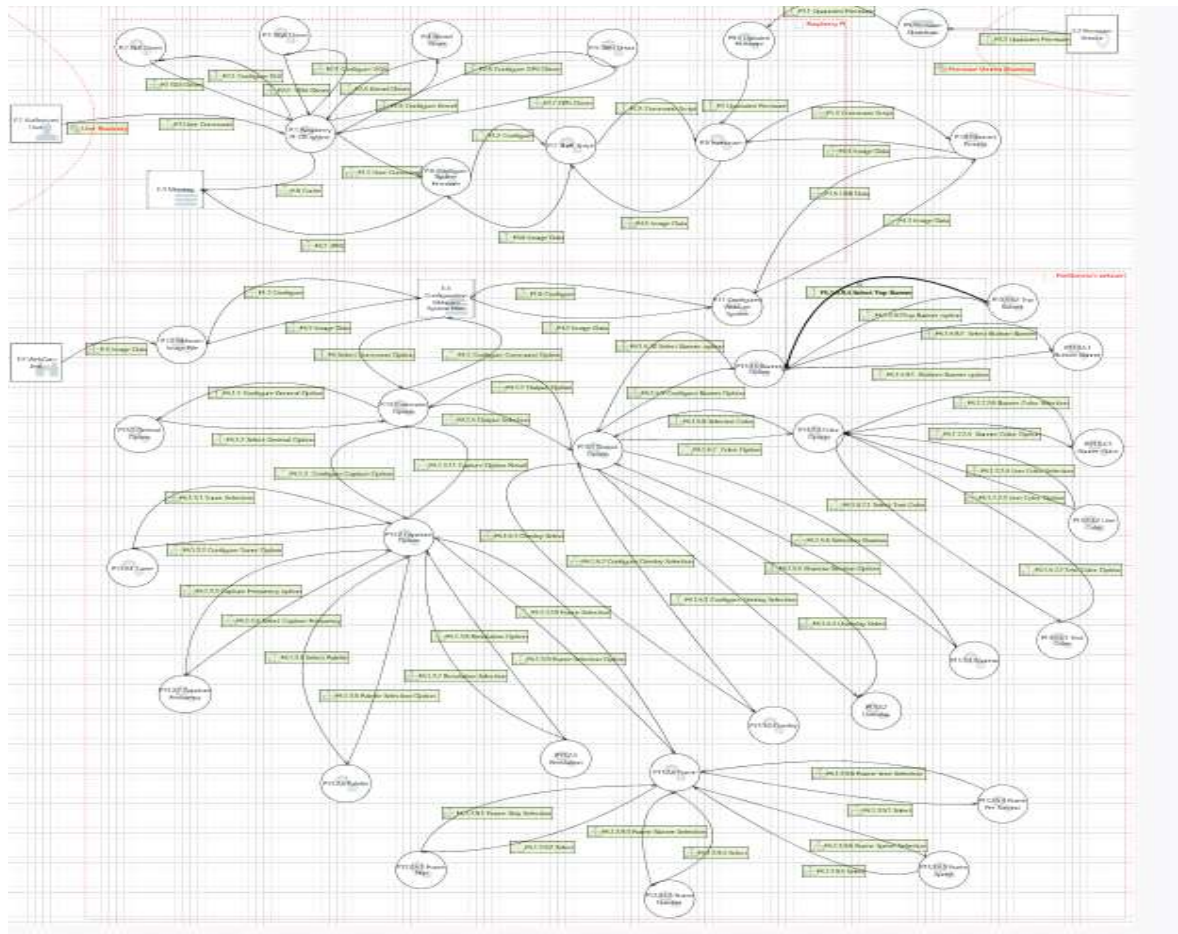


Figure 4. Level 2 DFD

IV. STRIDE ANALYSIS ON FIRESTORMCX'S WEBCAM

The STRIDE analysis was conducted based on the FireStormcx's webcam DFD's Context Level, Level 0, Level 1, and Level 2. Detailed descriptions are as shown in Table 4. The STRIDE analysis was conducted basis on the important functions in the FireStormcx's webcam. The analysis resulted in 6 Spoofing, 15 Tampering, 4 Repudiation, 5 Information Disclosure, and 14 Denial of Service. The camera is a simple structure. These threats can create significant privacy breaches which include turning the camera on at a random time. In the threats, Spoofing, Denial of Service, and Tampering must be considered a critical security threat. Spoofing caused the camera might be controlled by the attacker. Denial of Service can cause the authorized user's availability of a camera. Lastly, Tampering can cause modification of data in the storage. Therefore, in order to prevent these types of critical events, these threats must be considered as priority remediation. Those processes must initiate through a comprehensive remediation process.

Table 4. STRIDE Analysis on FireStormcx's webcam

Element	Name	STRIDE	Threat Description
Entity	Authorized User	S	The user controls the system pretend as Authorized User
Entity	Authorized User	R	An attacker can repudiate the system usage based on the false authentication
Data Store	Memory	I	Using a SQL injection attack, the Attacker can disclose all the sensitive data in the memory
Data Store	Memory	T	The attacker can modify the information in the memory.
Data Store	Memory	E	Unauthorized attacker can steal all the data in the memory
Entity	Firmware Vendor	S	Attack pretend as vendor and distributed all the malware included file
Entity	Firmware Vendor	R	Attacker can repudiated all the firmware traffic from the vendors
Entity	Configured Webcam system files	S	Attacker control the system files pretend as Authorized User

Entity	Configured Webcam system files	T	The attacker can modify the file information in the webcam system files
Process	USB process	E	The attacker can elevate the privilege to using a harmful USB driver
Process	Configured Webcam System	R	Using a data without digital signature, repudiate the camera data
Process	Configured Webcam System	S	Unauthorized users attack the camera software and control all the camera functions.
Process	Configured Webcam System	R	Using Long Injection-Tampering Forging attack to repudiate the camera system usage
Process	Configured Webcam System	I	Attacker controls the camera and occurred serious privacy breached
Process	Configured Webcam System	D	Attack send the repeated large amount of data to the system and causing a Denial of Service
Process	Captured Options	T	The attacker can modify the captured option process
Process	Captured Options	T	The attacker used the code injection attack to modify the code result
Process	Captured Options	I	The attacker modifies the captured option to control the camera system. As a result, it can cause significant privacy breached issues.
Process	Captured Options	D	A large amount of Captured Options requests could cause large network traffic. As a result, it can cause Denial of Service.
Process	Overlay	D	A large amount of Overlay Options requests could cause large network traffic. As a result, it can cause Denial of Service.
Process	Overlay	S	GUI overlay vulnerability in Mozilla Firefox before 2.0.0.13 and SendMonkey before 1.1.9 allows remote attackers to spoof from elements and redirect user inputs via borderless XUL popup windows from a background tab.
Process	Color Options	T	The Attacker can modify the color options process to control the color
Process	Color Options	D	A large amount of Color Options requests could cause large network traffic. As a result, it can cause Denial

			of Service.
Process	Underlay	D	Attacker's large amount of Overlay Options request could cause the large network traffic. As a result, it can cause Denial of Service.
Process	Underlay	T	The attacker can modify the Underlay function. The result can be different from the original command
Process	Resolution	T	The attacker can modify the Resolution function. The Attacker can control the camera's resolution
Process	Resolution	D	Attacker's large amount of Overlay Options request could cause the large network traffic. As a result, it can cause Denial of Service.
Process	Resolution	T	The attacker can modify the Resolution process to downgrade the image file
Process	Palette	T	The Attacker can modify the Palette process to modify the results
Process	Palette	D	Attacker's large amount of Palette Options request could cause the large network traffic. As a result, it can cause Denial of Service.
Process	Command Options	S	An unauthorized user can control the command options in the camera system
Process	Command Options	T	Attackers can modify the command process to modify the results
Process	Command Options	D	Attacker's large amount of Command Options requests could cause the large network traffic. As a result, it can cause Denial of Service.
Process	Command Options	I	Attacker command the camera could cause the significant privacy breach
Process	Frame	T	Attackers can modify the Frame Options to modify the result
Process	Frame	D	Attacker's large amount of Frame Options request could cause the large network traffic. As a result, it can cause Denial of Service.
Process	Capture Frequency	I	Attackers modification capture frequency could cause the privacy breached
Process	Capture Frequency	D	Attacker's large amount of Capture Options requests could cause the large network traffic. As a result, it can cause Denial of Service.

Process	Capture Frequency	T	Attackers can modify the Frame Options to modify the result
Process	Banner Option	D	Attacker's large amount of Banner Options requests could cause the large network traffic. As a result, it can cause Denial of Service.
Process	Banner Option	T	Attackers can modify the Banner Options to modify the result
Data Flow	Shadow Selection	T	The attacker can modify the result
Data Flow	Capture Frequency Option	D	Using an integer overflow attack, It can request large network traffic. As a result, it can cause a denial of service
Data Flow	Capture Frequency Option	T	The attacker can modify the capture frequency
Data Flow	Select Command Option	T	The attacker can modify the selection of command option
Data Flow	Select Command Option	D	It can request large network traffic. As a result, it can cause a denial of service
Data Flow	JPEG	T	The attacker can modify the JPEG result to damage the memory
Data Flow	JPEG	D	The attacker can request large network traffic. As a result, it can cause a Denial of Service
Data Flow	JPEG	I	The attacker can steal the JPEG data flow to a different device. It can cause a Privacy breach
Data Flow	Configure	I	The attacker control the Camera configure flow to take a picture without command from the authorized user

V. RECOMMENDED THREAT REMEDIATION PLAN

The STRIDE analysis created that FireStormcx's webcam system has significant threats. Webcam systems are well known for having vulnerabilities. These vulnerabilities could lead all the way to cause a critical risk. Eventually, those risks would cause actual breaches of privacy. Therefore, In order to solve prevent these types of critical events, systemic threat remediation approaches must be conducted based on the STRIDE analysis. The threat remediation approaches must be conducted among accept, mitigation, avoid, and transfer. In this paper, we initiated the basis of mitigation approaches. The majority of threats from the analysis were Spoofing, Tampering, and Denial of Service. Ultimately, to prevent this problem, authentication capability must increase. This can include Multifactor Authentication. This MFA method will

secure both integrity and confidentiality. It will significantly help to availability as well.

VI. CONCLUSION

This paper abstracts the FireStormcx's webcam using a DFD and conducts the analysis using a STRIDE technique. Furthermore, Using a STRIDE technique resulted in significant threats existing in the FireStormcx's webcam system. Therefore, in order to prevent critical privacy breaches, these threats must be mitigated. Since we conduct the STRIDE analysis on this paper, we have a detailed plan to conduct the risk analysis and produce a comprehensive risk remediation analysis. Our ultimate goal is to comply with design assurance and secure by design on the FireStormcx's webcam system.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2021-0-01774,Development of IEC 62443 based Smart Factory Security Internalization and Embedded Device Security Technology)

REFERENCES

- [1] J. Hattem, (2016, September 15). FBI director: Cover up your webcam. *TheHill*.<https://thehill.com/policy/national-security/295933-fbi-director-cover-up-your-webcam>
- [2] C.Schmittner, P. Tummeltshammer, D. Hofbauer, A. Shaaban, M. Meidlinger, M. Tauber, ... & M. Brandstetter, (2019, June). Threat modeling in the railway domain. In International Conference on Reliability, Safety, and Security of Railway Systems (pp. 261-271). Springer, Cham.
- [3] Adam Shostack, *"Experiences Threat Modeling at Microsoft,"* Microsoft, 2008
- [4] *Data Flow Diagram Symbols*. (2021). Lucidchart. <https://www.lucidchart.com/pages/data-flow-diagram/data-flow-diagram-symbols>
- [5] M. Heinig, & D. Frishman, (2004). STRIDE: a web server for secondary structure assignment from known atomic coordinates of proteins. *Nucleic acids research*, 32(suppl_2), W500-W502.
- [6] Microsoft, Security Development Lifecycle , <https://www.microsoft.com/en-us/sdl/>.
- [7] Cisco, Cisco Secure Development Lifecycle(SDL), <http://www.cisco.com/c/en/us/about/security-center/securit>



Jong Jin Cho received B.S in Security and Risk Analysis, Cybersecurity at the Pennsylvania State University, University Park, PA, USA, in 2019. In addition, he had two years of professional IT industry experience in New York City, Chicago, and Seoul. Currently, he is an M.S candidate in the School of Cybersecurity, Korea University. His current research interests are Threat Modeling, Formal Methods, and Secure Software Engineering



Miyoung Kang received the M.S. degree in the Department of Computer Science and Engineering at Dongguk University and the Ph.D. degree in the Department of Computer Science and Engineering at Korea University, Seoul, Korea. She is a research professor at the graduate school of Information Security at Korea University, Seoul, Korea. Her research interests are Formal Methods, process algebras, software-defined networking (SDN), and security in networks.