Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.3, Jun. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.3.591

정찰 드론 보안성 평가 기준에 대한 연구*

구 도 형,[1†‡] 김 승 주,[2] 이 상 진[2]
[1,2]고려대학교 (대학원생, 교수)

A Study of Security Evaluation Criteria for Reconnaissance Drone*

Do-hyung Gu,[1†‡] Seung-joo Kim,[2] Sang-jin Lee[2]
[1,2]Korea University (Graduate Student, Professor)

요 약

드론이 활용되는 분야가 다양해짐에 따라 드론의 취약점을 이용한 공격 시도가 늘어나고 있고 드론 보안의 중요성 또한 강조되고 있다. 본 논문은 관공서에 납품되는 정찰용 드론에 대해 위협모델링을 통해 보안요구사항을 도출하였다. 드론의 데이터 흐름을 분석하고 발생할 수 있는 취약점을 수집하여 위협 분석 및 공격 트리를 작성하였다. 공격 트리로부터 보안요구사항을 도출하고 국가에서 제시한 보안요구사항과 비교하였다. 본 논문에서 도출된 보안요구사항을 활용하면 안전한 정찰 드론 개발과 평가에 도움이 될 것이다.

ABSTRACT

As drones are widely used, attack attempts using drone vulnerabilities are increasing, and drone security is growing in importance. This paper derives security requirements for reconnaissance drone delivered to government office through threat modeling. Threats are analyzed by the data flow of the drone and collecting possible vulnerabilities. Attack tree is built by analyzed threats. The security requirements were derived from the attack tree and compared with the security requirements suggested by national organizations. Utilizing the security requirements derived from this paper will help in the development and evaluation of secure drones.

Keywords: Drone, Security Requirement, STRIDE Threat Modeling

I. 서 론

드론은 4차 산업 혁명을 맞아 공공분야와 민간 산업에서 활용이 증가하고 있다. 영국에서는 드론을 활용하여 병원 간 혈액, 장기를 운반하려 하고 있고, 미국의 아마존사는 드론으로 상품을 배송하기 위한 '프라임 에어' 프로젝트를 진행 중이다. 이렇게 드론 산업이 성장함에 따라 드론 보안의 중요성도 증가하고 있으며 관련 국가 기관에서는 드론 사이버 보안 가이드를 발표하였다 [1].

촬영용 드론이라고도 불리는 정찰 드론은 군사적 목적으로 기지 경계와 적진 정찰 뿐만 아니라 산림보호, 화재방재, 범죄지역 조사 등 소방, 경찰과 같은 공공분야에서도 활용도가 높다 [2]. 정찰 드론은 일반적인 조종 신호에 대한 보안과 주고받는 영상 데이터와 카메라에 대한 보안을 모두 고려해야 하므로 활용성과 보안성 측면에서 모두 중요하다.

본 논문에서는 Microsoft에서 개발한 위협모델링 기법을 적용해 정찰 드론을 위한 보안요구사항을 도출하였다 [3]. 보안요구사항 도출은 제품의 구성요소로부터 발생할 수 있는 취약점을 엮어 최종적으로 공격에 달성하지 못하도록 킬체인을 끊는 작업이다 [4]. 본 논문은 관공서에 납품되는 정찰 드론을 대

Received(04. 15. 2022), Accepted(05. 23. 2022)
* 본 연구는 국방암호기술 특화연구센터(UD210027XD)를 통한 방위사업청과 국방과학연구소의 연구비 지원으로 수행되었습니다.
† 주저자, iamkdh@korea.ac.kr
‡ 교신저자, iamkdh@korea.ac.kr(Corresponding author)

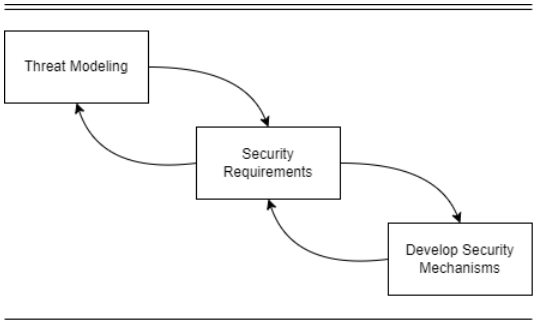


Fig. 1. System Security Engineering[4]

상으로 구성요소를 분석하고 보안성 평가 기준을 수립하였다. 도출된 평가 기준을 활용하여 안전한 드론 개발, 제품 평가를 위한 보호프로파일 작성, 드론 간 보안성 비교의 기준 등으로 활용될 수 있다. Fig.1.과 같이 위협모델링으로부터 보안요구사항을 도출하고 보안 메커니즘을 개발하는 일련의 과정을 통해 정찰 드론의 보안성을 평가하고 안전한 정찰 드론을 개발할 수 있다[4].

본 논문의 2절에서는 드론 취약점, 보안요구사항 도출 관련 연구와 위협모델링 방법을 소개한다, 3절에서는 위협모델링 프로세스에 따라 드론에 발생할 수 있는 위협과 공격 방식을 분석한다. 4절에서는 3절의 결과로부터 보안요구사항을 도출하고 평가한다. 마지막으로 5절에서는 결론을 기술한다.

II. 관련 연구

이 절에서는 선행연구와 본 논문에서 필요한 기본 개념을 소개한다. 2.1절에서는 드론 취약점과 관련된 연구, 2.2절에서는 보안요구사항 도출에 관한 연구, 2.3절에서는 본 논문에서 사용한 위협모델링 방법에 대해 설명한다.

2.1 드론의 취약점 분석 관련 연구

드론 취약점에 대한 연구는 공격 대상에 따라 통신채널에 대한 취약점과 드론 비행을 위해 탑재된 다양한 센서에 대한 취약점이 있다. 이러한 기법들은 3.2절에서 구축한 공격 라이브러리에 포함되어 있다.

드론은 조종기 또는 지상제어장치와 통신하며 비행 제어에 관한 신호와 촬영한 영상을 통신한다. 통신 채널의 취약점에 대한 연구는 다양한 드론의 통신 채널에 대해 공격하는 것으로서 많은 드론이 사용하는 WiFi 통신채널에 대한 취약점, 저전력 프로토콜인 Xbee와 드론 간 통신 프로토콜인 MAV Link에 대한 취약점이 있다[5-13]. 영상채널에 대해서는 재밍 공격을 가해 사용자가 드론에서 촬영한 영상을 정상적으로 수신하지 못하도록 할 수 있다[14]. 이러한 무선 통신구간에 대해 보안성 강화방안을 제시한 연구도 있다[15].

드론에는 항법을 위한 GPS 모듈과 가속도계, 기압계, 나침반, 자이로스코프센서 등 다양한 센서가 탑재된다. 이러한 센서 값에 오류를 일으키게 되면 추락하거나 제자리에 착륙하는 등 정상적인 비행이 불가능해진다. GPS 모듈에 대해서는 수신하는 GPS 값을 변조하는 스푸핑 공격과 재밍을 통해 정상적인 통신을 못하도록 하는 재밍 공격이 있다[7,9,14,16-21]. 다른 센서들에 대한 공격으로는 가속도계에 초음파를 보내 에러를 발생시키는 취약점, 자이로스코프에 대한 취약점, 드론에 탑재된 나침반센서에 대한 취약점이 있다[22-24]. 이외에도 드론 하드웨어에 관한 공격이나 다양한 센서 공격들의 한계와 대응 방안에 대해 정리한 논문도 있다[25,26].

2.2 보안성 평가 기준 관련 연구

드론 보안 관련 연구는 2.1절과 같이 취약점 중심의 연구가 많이 진행되고 있으며 드론의 보안성 평가에 대한 연구는 국내와 국외에 1건씩 있다. 국내 연구는 중국과 프랑스에서 생산된 4종의 상용 드론에 대해 기존에 알려진 드론 취약점을 분석하고 이를 바탕으로 보안요구사항을 도출하였다[27]. 국외 연구는 알려진 일부의 드론 취약점에 대해 STRIDE와 DREAD를 통해 취약점을 평가하였으나 기준을 제시하지 않았다[28]. 한국인터넷진흥원(KISA)는 드론 보안에 대한 위협과 대응 방안을 공유하고자 드론 사이버 보안 가이드를 발표하였다[1]. 보안성 평가 기준이 없는 새로운 기술과 제품에 대한 관련 연구로 블록체인이라는 분산화된 참여자들이 존재하는 시스템에 대해 평가 범위와 요구사항을 도출한 연구와 IP카메라와 스마트TV에 대해 위협모델링을 기반으로 보안요구사항을 도출한 연구가 있다[29-31].

2.3 위협모델링

위협모델링은 제품에서 발생할 수 있는 위협을 체계적으로 도출하는 프로세스다. 위협모델링 방법의 종류는 Microsoft에서 개발한 STRIDE, 위험 중심의 위협모델링 프레임워크인 PASTA, 프라이버시를 고려한 LINDDUN 등 도출하고자 하는 위협에 따라 다양하다 [32,33]. 본 논문에서는 정찰 드론의 보안성 평가 기준을 도출하기 위한 방법으로서 STRIDE 방법을 적용하였다.

STRIDE는 안전한 시스템이 갖춰야 할 6가지 요소로 인증, 무결성, 부인방지, 기밀성, 가용성, 권한 부여에 대한 위협을 도출하기에 효과적이며 낮은 false-positive를 가지는 특징 때문에 STRIDE 방법을 통해 보안성 기준을 도출하기에 적합하다 [34]. 사이버 영역에서만 사용되던 STRIDE 방법을 스마트 그리드에 적용함으로서 사이버-물리 시스템으로 확장할 수 있음을 보인 연구가 있으며, 드론 시스템도 이와 유사하게 STRIDE 방법을 적용해 체계적으로 위협을 도출하는 것이 가능하다 [35].

III. 드론 위협모델링

본 논문에서는 정찰 드론 보안성 평가 기준을 수립하기 위해 위협모델링을 수행하였다. 3.1절에서는 본 논문에서 분석한 정찰 드론에 대해 기술하고 3.2절에서는 드론의 데이터흐름도를 작성하였다. 3.3절에서는 2.1절에서 소개한 선행 연구를 포함하여 관련 CVE 취약점들을 모아 공격 라이브러리를 구축하였다. 3.4절에서는 3.2절에서 작성한 데이터흐름도에 3.3절에서 구축한 공격 라이브러리를 적용하여 발생할 수 있는 위협을 분석하였다. 3.5절과 3.6절에서는 분석한 위협을 바탕으로 실제 발생할 수 있는 공격에 대한 공격 트리를 작성하였다.

3.1 정찰 드론

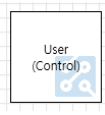
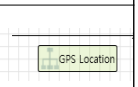
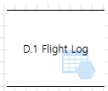
본 논문에서는 국방분야에 납품되고 있는 마이크로크기(0.1~25kg)의 드론 중 2019년 조달청 혁신시제품으로 선정된 드론을 대상으로 하였다. Fig.2.와 같이 대상 드론은 카메라와 드론, 암호모듈이 탑재된 컨트롤러로 구성되며, 드론에는 기체 제어를 위한 센서와 GPS 모듈, 비행로그 저장소가 포함되어 있다.

Fig. 2. Reconnaissance drone components

3.2 데이터흐름도 작성

데이터흐름도(dataflow diagram)는 시스템의 프로세스(process), 저장소(data store), 외부객체(external entity) 사이의 데이터흐름(dataflow)를 도식화 한 것으로 Table 1과 같이 구성된다. 대상 드론이 비행하고 영상을 스트리밍하는 과정을 분석하여 Fig. 3.과 같이 나타냈다. 드론은 미리 정한 경로대로 비행하는 자동 비행 모드와 사용자가 직접 제어하는 수동 비행 모드가 있으며 조종 신호는 별도의 암호화를 거치지 않고 무선으로 전송된다. 비디오처리 프로세스는 촬영한 영상을 인증받은 암호 모듈을 통해 암호화하여 전송한다. 대상 드론을 분석한 결과 총 20개의 프로세스와 5개의 데이터저장소, 54개의 데이터 흐름을 식별했다.

Table 1. DFD Components

Element	Description	Example
External Entity	Indicates out boundary component of drone system	
Process	All processes must have input and output data.	
Data Flow	Data packet among process, data store, external entity	
Data Store	Stores log data or video data	
Trust Boundary	Indicates the same level of trust	

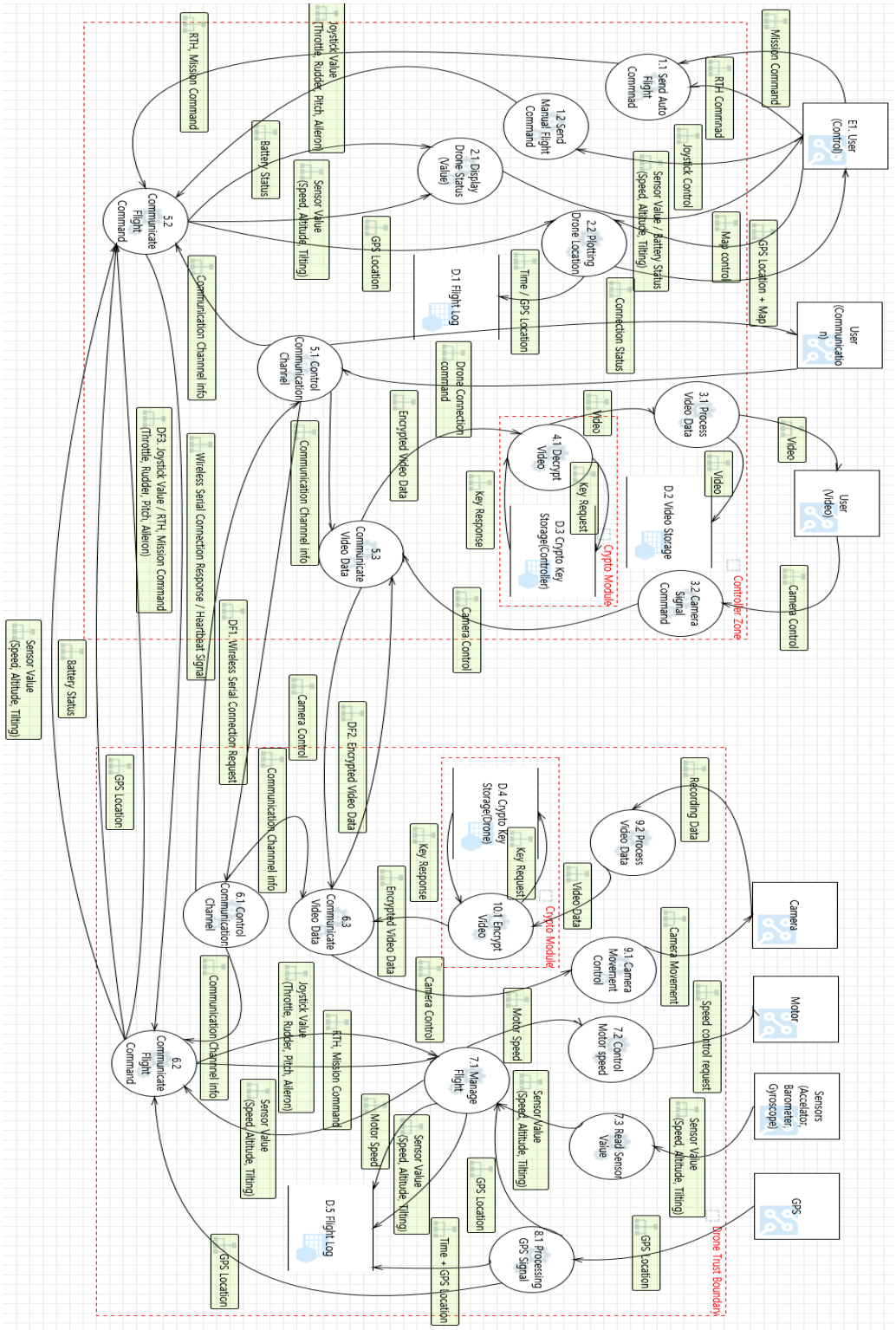


Fig. 3. Data Flow Diagram for Reconnaissance Drone

3.3 공격 라이브러리 구축

공격 라이브러리는 해당 시스템과 관련된 취약점들을 수집해 데이터베이스화 한 것으로 다른 분석자에 의해 수행되어도 일련의 결과를 얻을 수 있도록 한다 [36]. 3.1절과 3.2절에서 분석한 내용에 따라 카메라, GPS모듈 등 정찰 드론을 구성하고 있는 요소와 관련된 취약점들을 최근 5년 안에 발표된 유명 드론 보안 관련 논문이나 해킹 컨퍼런스, 보안 블로그, github에 공개된 취약점들을 수집한 것과 고려대학교와 연세대학교, 성균관대학교에서 합동으로 수행한 고등급 마이크로커널 개발 프로젝트에서 구축한 드론 공격 라이브러리를 참고하여 데이터베이스화하였다 [37]. Table 2는 카메라에서 발생할 수 있는 취약점, Table 3은 GPS 신호에 관한 취약점, Table 4는 펌웨어에서 발생 가능한 취약점, Table 5는 메인보드나 가속도계 센서 등 하드웨어에서 발생할 수 있는 취약점, Table 6은 네트워크 프로토콜상에서 발생할 수 있는 취약점이다. 컨퍼런스 4건, CVE 37건, 논문 18건, 취약점 시연 2건으로부터 총 80개의 취약점을 수집하였다.

Table 2. Attack Library(Camera)

No	Type	Attack Method	Ref
AL25	T	debug script	[37]
AL26	S	inadequate access control	[37]
AL27	E	inadequate access control	[37]
AL28	T	use after free	[37]
AL29	I	weak crypto algorithm	[37]
AL30	S, E	inadequate access control	[37]
AL31	S, E	root shell	[37]
AL32	S	remote code execution	[37]
AL33	S	remote code execution	[37]
AL34	S	remote code execution	[37]
AL35	E	remote code execution	[37]
AL36	I	local Information Leakage	[37]
AL37	I	memory information leakage	[37]
AL38	S	directory listing	[37]
AL39	D	http header dos	[37]
AL40	T	http header bof	[37]
AL41	I	data leakage	[37]
AL42	D	integer overflow	[37]
AL43	E	stack bof	[37]
AL44	D	ipv4 flooding	[37]
AL45	S, T	remote file deletion	[37]
AL46	D	post request	[37]
AL47	D	network config interface request	[37]
AL48	I	network traffic sniffing	[37]
AL49	T	stack bof	[37]
AL50	E	command injection	[37]
AL51	T, E	firmware downgrade	[37]
AL52	T, E	command injection	[37]
AL53	E	command injection	[37]
AL54	S, E	root shell	[37]
AL59	D	noise injection	[37]
AL68	T	stabilization algorithm	[37]

Table 3. Attack Library(GPS)

No	Type	Attack Method	Ref
AL1	S	inducing off-path	[19]
AL2	S	inducing off-path	[20]
AL4	S	drone hijacking	[7]
AL8	S	inducing off-path	[9]
AL14	I, T	drone hijacking	[37]
AL64	S	drone hijacking	[16]
AL69	S	inducing off-path	[17]
AL74	S	force landing	[14]
AL79	T	inducing off-path	[18]
AL80	D	inducing off-path	[21]

Table 4. Attack Library(Firmware)

No	Type	Attack Method	Ref
AL10	T	custom firmware	[37]
AL11	I	protocol reversing	[37]
AL12	T, I	sensor data error	[37]
AL16	E	root shell	[10]
AL19	I, E	video leakage	[37]
AL20	E	root shell	[37]
AL21	E	change drone config	[37]
AL71	E	malware	[26]
AL72	E	application SDK	[14]
AL76	E	killing main process	[26]
AL77	R	inadequate access control	[26]

Table 5. Attack Library(Hardware)

No	Type	Attack Method	Ref
AL13	I, (E)	getting sensor information	[37]
AL22	I	unencrypted packet	[37]
AL23	D	acoustic injection	[37]
AL24	I	data Information Leakage	[37]
AL67	T	acoustic injection	[22]
AL70	T	supply chain attack	[26]
AL75	T	acoustic injection	[23]
AL78	D	ban take-off	[26]

Table 6. Attack Library(Network)

No	Type	Attack Method	Ref
AL3	I	packet decryption	[7]
AL5	I	packet sniffing (control, video)	[8]
AL6	E	deauthentication	[37]
AL7	T	data blocking	[9]
AL9	D	deauthentication	[9]
AL15	S, T	man in the middle	[10]
AL17	S	custom controller	[10]
AL18	I, E	mac address Spoofing	[11]
AL55	S	message injection	[37]
AL56	I	memory information leakage	[37]
AL57	D	heap bof	[37]
AL58	D	integer overflow	[37]
AL60	S, T	drone hijacking	[37]
AL61	I	location information leakage	[37]
AL62	S, I	man in the middle	[12]
AL63	D	deauthentication	[5]
AL65	D	SYN flooding	[6]
AL66	S	replay attack	[13]
AL73	D	video channel jamming	[14]

3.4 위협 분석

3.2절에서 도출된 데이터흐름도의 프로세스, 데이터플로우 등 각 요소에 대해 STRIDE 방법을 적용하여 발생할 수 있는 위협을 분석하였다. Table 7에 제시한 결과와 같이 총 106개의 위협이 도출되었으며 이를 3.3절의 공격라이브러리와 매핑하였다. 식별한 주요 위협은 통신 프로세스 P6.1이 취약한 통신프로토콜을 이용할 경우 통신 내용이 유출되거나 변조 될 수 있는 위협이 있다. 위협 도출 시 드론의 암호모듈 내부에 속한 프로세스와 데이터저장소는 별도의 인증을 받아 안전하다고 가정하였기 때문에 부채널 공격과 같이 암호 모듈에 대한 공격은 범위에서 제외하였다.

3.5 공격 트리 작성

공격 트리는 공격목표에 달성하기 위해 필요한 공격 방법들을 조건에 따라 트리형태로 표현한 것이다. 본 논문에서는 3.4절에서 수행한 위협 분석 결과를 바탕으로 드론 비행, 영상, 펌웨어, 로그에 대한 공격 트리를 작성하였다. Table 8~11은 공격 트리를 표 형식으로 작성한 것으로 공격 목표를 달성하기 위한 보조 공격 목표와 공격 방식을 3.4절에서의 식별한 위협과 연관지었다. 공격 목표를 달성하기 위한 조건은 표의 구분선으로 나타나며 실선은 공격을 달성하기 위한 or조건, 점선은 and조건을 나타낸다. 예를 들어, Table 8내의 1.1 드론의 자동 비행실패를 유도하기 위해서는 1.1.1 gps에 대한 공격을 수단으로 이용할 수 있고, 해당 공격을 성공하기 위해서는 1.1.1.1 공격 대상 드론의 위치를 알아내야 1.1.1.2에 해당하는 GPS 신호 재밍이나 스푸핑을 성공시킬 수 있다. 드론에 대한 공격 목표로 Table 8은 드론 비행을 실패하기 위한 목표, Table 9는 영상을 수신하지 못하거나 유출시키는 등 영상과 관련된 공격목표, Table 10은 펌웨어와 관련된 공격목표, Table 11은 로그와 관련된 공격목표로 크게 4개로 분류하여 공격 트리를 나타냈다.

Table 7. Threat analysis

DFD	Threat	STRIDE	Description	AL no.
P1.1	T1	S	The threat that unauthorized person sends mission flight command	-
	T2	T	The threat that mission flight command modifies by malware	-
	T3	R	The threat that user avoids responsibility of mission command	-
	T4	I	The threat that the information about mission flight command leaked via process memory	-
		D	-	-
		E	-	-
..... omit				
P6.1	T37	S	The threat that receiving unauthenticated packet via unnecessary service	AL15
	T38	S	The threat that communicate with custom controller (MAC address spoofing)	AL17
	T39	T	The threat that receiving modified packet via unnecessary service	AL15
	T40	R	The threat that repudiates received data packet changing physical address	-
	T41	I	The threat that packet sniffing with protocol vulnerability	AL3, AL22
	T42	D	The threat that deauthentication attack	AL9, AL63,AL65
	T43	E	The threat that gain root shell and kill main process via unnecessary service	AL16,AL20,AL76
	T44	E	The threat that malicious backdoor installed	AL71
	T45	E	The threat that develop elevating previlege C&C application via analyzing manufacturer SDK	AL72
P6.2	T46	S	The threat that controlled by abnormal controller	AL60
	T47	T	The threat that drone hijacking	AL60
	T48	R	The threat that repudiates received control command	-
	T49	I	The threat that sending unencrypted location information	AL61
	T50	D	The threat that jamming flight control channel	-
	T51	E	The threat that deauthentication attack	AL6
..... omit				
DF3	T102	T	The threat that unauthenticated person exploits authentication process of Xbee protocol and MITM attack	AL62
	T103	I	The threat that attacker exploits encryption scheme of Xbee protocol and sniff network packet	AL62
		D	-	
DF4		T	-	
	T104	I	The threat that the leakage of drone GPS information	
		D	-	
E1	T105	S	The threat that unauthenticated person control drone	
	T106	R	The threat that repudiates responsibility of drone control	

Table 8. Attack Tree (flight control)

Attack Goal	Attack Subgoal	Attack Method	Threat
1.1 auto flight failure	1.1.1 gps	1.1.1.1 get current drone location	T30, T75, T76, T104
		1.1.1.2 jamming or spoofing gps signal	T72, T73, T77, T78
	1.1.2 sensor	1.1.2.1 get current drone location	T30, T75, T76, T104
		1.1.2.2 gain sensor hardware info	T60, T64
		1.1.2.3 cause sensor error	T66, T67, T68, T71
	1.1.3 camera	1.1.3.1 exploit camera stabilizing algorithm	T88
	1.1.4 unintentional flight	1.1.4.1 man in the middle	T1, T4, T102
		1.1.4.2 install malware	T2, T65
1.2 manual flight failure	1.2.1 authentication bypass	1.2.1.1 custom controller	T5, T6, T7, T105
		1.2.1.2 replay attack	T46, T47, T56
	1.2.2 communication failure	1.2.2.1 jamming control signal	T31, T50, T100
		1.2.2.2 drone-controller deauthentication	T32, T42, T51
	1.2.3 unintentional flight	1.2.3.1 man in the middle	T28, T102
		1.2.3.2 install malware	T27

Table 9. Attack Tree (video)

Attack Goal	Attack Subgoal	Attack Method	Threat
2.1 recording failure	2.1.1 causing camera error	2.1.1.1 cam control disability	T18, T19, T20, T80
		2.1.1.2 exploit camera firmware	T79, T81, T86, T90
	2.1.2 causing communication error	2.1.2.1 video channel jamming	T101
		2.1.2.2 dos attack via network	T17, T25, T36, T83
2.2 fake video	2.2.1 storage	2.2.1.1 storage access	T95
	2.2.2 streaming	2.2.2.1 spoof streaming packet	T14, T15
2.3 video leakage	2.3.1 memory	2.3.1.1 memory leak	T16, T82
	2.3.2 network	2.3.2.1 network sniffing	T24, T35, T54, T89

Table 10. Attack Tree (log)

Attack Goal	Attack Subgoal	Attack Method	Threat
4.1 log tampering	4.1.1 modify saved log	4.1.1.1 access drone storage	T62, T97, T98
		4.1.1.2 access controller storage	T3, T92, T93
	4.1.2 logging fake information	4.1.2.1 exploit audit process	T11
4.2 insufficient data	4.2.1 service terminate	4.2.1.1 kill audit process	T10
	4.2.2 design error	4.2.2.1 manufacturer	T58

Table 11. Attack Tree (firmware)

Attack Goal	Attack Subgoal	Attack Method	Threat
3.1 unauthorized update	3.1.1 custom firmware	3.1.1.1 gain firmware info	T57, T59
		3.1.1.2 build firmware	T55, T61, T62
	3.1.2 downgrade	3.1.2.1 tampering during normal update process	T55, T61, T62
3.2 get root shell (including rce)	3.2.1 backdoor	3.2.1.1 install malware	T33
		3.2.1.2 manufacturer	T45
	3.2.2 exploit service	3.2.2.1 unnecessary service	T39, T43
		3.2.2.2 1-day vulnerability	T84, T85, T87, T91

IV. 드론 보안요구사항 도출

4절에서는 3절에서 수행한 위협모델링을 기반으로 정찰용 드론에 대한 보안요구사항을 도출하였다. 4.1절에서는 본 논문에서 도출한 보안요구사항을 제시하고, 4.2절에서는 한국인터넷진흥원에서 발표한 드론 사이버 보안 가이드에 제시된 보안요구사항과 본 논문에서 도출한 요구사항을 비교하였다.

4.1 드론 보안요구사항

본 논문에서는 3.5절에서 작성한 공격 트리의 공격 목표를 달성할 수 없도록 공격 트리의 최하위 노드인 공격 방법에 대한 대응책으로서 24개의 보안요구사항을 도출하였다. 정찰용 드론 개발 시 Table 12의 보안요구사항을 고려하면 본 논문에서 수집하고 분석한 위협과 공격으로부터 안전한지 정찰 드론을 평가할 수 있다.

Table 12. Security requirement of reconnaissance drone

No.	Security Requirement	Attack method
SR1	Drone should detect or react against GPS based attack	1.1.1.2
SR2	Flight control channel should be able to respond to jamming attacks	1.2.1.2
SR3	Flight control protocol should not allow replay attack	1.2.1.2
SR4	Video channel should be able to respond to jamming attacks	2.1.2.1, 2.1.2.2
SR5	Drone and controller should connect to a secure network	1.2.2.2, 1.2.3.1, 2.1.2.2, 2.3.2.1
SR6	Vulnerability of sensors mounted on drone should be unknown	1.1.2.3, 3.2.2.1, 3.2.2.2
SR7	Vulnerability of camera mounted on drone should be unknown	1.1.3.1, 2.1.1.1, 2.1.1.2, 3.2.2.1, 3.2.2.2
SR8	It should be difficult to know which model of sensors and chips are on the drone	1.1.2.2
SR9	The flight software running on drone should be secure coded and safe	1.1.3.1
SR10	No malware is installed in operating system(including firmware) on drone and controller	1.1.4.2, 1.2.3.2, 3.2.1.1
SR11	Only authenticated user can operate drone	1.2.1.1
SR12	Drone and controller should do mutual authentication	1.1.4.1, 1.2.2.2, 1.2.3.1
SR13	Communicating location information should be encrypted	1.1.1.1, 1.1.2.1
SR14	Recorded video data should be encrypted	2.2.1.1, 2.3.1.1
SR15	Video should not be leaked by memory	2.2.2.1, 2.3.1.1
SR16	Firmware should be hard to analyze and modify	1.1.1.1, 1.1.2.1, 3.1.1.1

SR17	Only authenticated administrator can update firmware	3.1.1.2, 3.1.2.1
SR18	Updating firmware should be kept integrity like digital signature	3.1.1.2, 3.1.2.1
SR19	Operating system and firmware should not operate vulnerable service	3.2.1.2
SR20	Saving log data should be reliable timestamp and location	4.1.1.1, 4.1.1.2
SR21	Log data should contain sufficient information with tracebility	4.1.2.1
SR22	System need to monitor if the log process is running normally	4.2.1.1
SR23	Log data should contain sufficient information with tracebility	4.2.2.1
SR24	Cryptographic algorithm used in network protocol must be secure	1.1.1.1, 1.1.2.1

4.2 보안요구사항 평가

4.1절에서 도출한 보안요구사항과 한국인터넷진흥원에서 제시한 드론 사이버 보안 가이드의 보안요구사항을 비교하였다. 드론 사이버 보안 가이드는 드론의 구성요소 및 기능을 분석하고 각 요소에서 발생할 수 있는 위협을 나열하여 6가지 위협 시나리오를 작성하였다. 작성된 위협 시나리오로부터 보안과 안전한 비행, 프라이버시 측면을 모두 고려하여 HW 및 SW의 안전성, 인증 등 7개 보안 항목에 대해 27개의 대응 방안을 제시하였다 [1].

본 논문에서 도출한 요구사항과 항목별로 비교한 결과는 Table 13과 같다. 가이드라인은 본 논문에서 제시한 24개의 보안요구사항 중 17개의 요구사항을 포함하고 있다. 본 연구에서 제시하였지만 가이드라인에 포함되지 않은 요구사항은 정찰용 드론에 탑재되는 센서와 카메라 보안, 영상 처리 과정에서 메모리에 대한 보안, 펌웨어 분석 및 수정에 대한 보안, 로그 프로세스가 정상 작동하는지를 확인하는 것에 대한 요구사항이다. 가이드라인에서 도출되지 않은 요구사항이 본 논문에서 도출할 수 있었던 이유는 두 가지가 있다.

첫 번째는 대상으로 삼은 드론의 구성요소가 다르다. 실제로 가이드라인에서 설명하는 드론 구성 요소를 보면 촬영용 카메라를 드론의 페이로드로 취급하는 반면, 본 논문에서는 정찰 드론을 대상으로 삼았기 때문에 카메라 역시 정찰드론에 포함되는 구성 요소로서 포함하였다.

두 번째는 가이드 라인의 경우 보안요구사항 도출 과정의 각 단계가 독립적이다. 가이드라인의 보안요구사항 도출 과정을 살펴보면 2장 2절의 위협 시나리오에서 센서 취약점에 대한 위협을 식별하였으나 이로부터 관련된 보안요구사항이 3장 2절에 도출되지 않았다.

반면, 본 논문에서 도출한 요구사항에는 포함되어 있지 않으나 가이드라인에서 제시한 항목은 드론간 통신시 식별 수단, 비행 금지구역에 대한 접근 차단, 드론 비행 시 충돌 회피 기능, 프라이버시, 드론 시스템 설계에 대한 요구사항이다. 드론간 통신시 식별 수단과 비행 금지구역, 충돌 회피 기능에 대해서는 본 논문에서 대상으로 삼은 정찰 드론이 수행하는 임무상 요구되지 않는 기능에 대한 보안요구사항이고, 프라이버시와 시스템 설계에 대한 요구사항은 본 논문의 정찰 드론에도 적용 가능한 요구사항이지만, 본 논문의 위협모델링 과정에서 고려하지 않은 영역이다.

V. 결 론

드론이 활용되는 분야가 다양해짐에 따라 드론 취약점을 이용한 공격 시도가 늘어나고 있다. 드론 취약점 관련 연구들이 꾸준히 수행되고 있고 관련 국가기관에서도 드론 사이버 보안 가이드라인을 제시하는 등 드론 보안의 중요성이 강조되고 있다.

본 논문에서는 다양한 분야에서 활용되고 있는 정찰용 드론이 해킹이나 무선신호 위협으로부터 안전할 수 있도록 개발되고 이미 개발된 드론의 보안성 평가를 돕기 위해 드론 보안요구사항을 도출하였다. 네트워크, 펌웨어 등 드론 구성요소별로 발생할 수 있는 공격 방식 80개를 수집하여 공격 라이브러리를 구축하였고, 이를 바탕으로 발생할 수 있는 106개의 위협을 분석하였다. 분석한 위협으로부터 드론의 비행 실패나 영상 유출 등 4가지의 목표를 달성하기 위한 조건을 도출한 위협과 연관지어 공격 트리를 작성했다. 최종적으로 공격을 달성하기 위한 조건을 충족시키지 못하도록 하는 24개의 드론 보안요구사항을 도출했다.

Table 13. Drone security countermeasure assessment

Main category	Requirement	O/-	Assessment
hardware & software security	secure update	O	identical to SR17.
	respond to tampering	O	identical to SR18.
	respond to malware	O	identical to SR10.
	secure 3rd party library	O	identical to SR19.
authentication	**drone identification**	-	**communication between drone not considered in this paper**
	user authentication	O	identical to SR11.
	mutual authentication	O	identical to SR12.
secure communication	rf signal protection	O	identical to SR3.
	communication channel / jamming reaction	O	identical to SR2.
	data packet protection	O	identical to SR5.
	message detection code	O	identical to SR5.
flight safety	auto flight	O	included in DFD
	alternative method of gps	O	identical to SR1.
	restricted area	-	**physical safety not considered in this paper**
	collision avoidance	-	
cryptography	key management	O	identical to SR24.
	secure algorithm	O	identical to SR24.
	secure random seed	-	- ()
	secure crypto module	O	included in DFD
data protection	saved data protection	O	identical to SR14. SR20.
	operating data protection	O	identical to SR13.
	access control	O	identical to SR20.
	privacy	-	**privacy not considered in this paper**
audit	log data	O	identical to SR21. SR23.
	monitoring	-	**designing process not considered in this paper**
-	-	-	SR6. Vulnerability of sensors mounted on drone should be unknown
		-	SR7. Vulnerability of camera mounted on drone should be unknown
		-	SR8. It should be difficult to know which model of sensors and chips are on the drone
		-	SR9. The flight software running on drone should be secure coded and safe
		-	SR15. Video should not be leaked by memory
		-	SR16. Firmware should be hard to analyze and modify
		-	SR22. System need to monitor if the log process is running normally

본 논문에서 도출한 요구사항은 안전한 드론 개발, 상용 드론 평가, 이미 제시된 보안요구사항과의 비교 등 드론의 보안성 향상에 도움이 될 것으로 기대한다.

안전한 드론의 활용을 위해 고려해야 할 문제는 보안과 프라이버시이다. 본 논문에서는 보안성을 고려하기 위해 STRIDE 위협모델링 방법을 활용하였지만, 향후에는 프라이버시 영역에 초점을 둔 위협모델링 방법인 LINDDUN 방법을 적용한다면 프라이버시 관련 위협과 요구사항을 도출할 수 있을 것이다.

References

[1] Korea Internet & Security Agency, Cyber security guide for drone, Dec. 2020.

[2] Seung bae Sim,Hun yeong Kwon, Ho sang Jung, "A study on Utilization of Drone for Public Sector by Analysis of Drone Industry," Journal of Information Technology Service, vol. 15, no. 4, pp. 25-39. Dec. 2016.

[3] N. Shevchenko, T.A. Chick, P. O'Riordan, T.P. Scanlon and C. Woody, "Threat Modeling: A Summary of Available Methods," AD1084024, Software Engineering Institute, Carnegie Melon University, Jul. 2018.

[4] S. Myagmar, A.J. Lee and W. Yurcik, "Threat Modeling as a Basis for Security Requirements," National Center for Supercomputing Applications, University of Illinois at Urbana-Champaign, 2005.

[5] S. Kamkar, "Skyjack," https://github.com/samyk/skyjack, Dec. 2013.

[6] E.Deligne, "ARDrone corruption," Journal in Computer Virology, vol.8, no. 1-2, pp. 55-27, May. 2012.

[7] D. He, S. Chan and M. Guizani, "Drone-Assisted Public Safety Networks: The Security Aspect," in IEEE Communications Magazine, vol. 55, no. 8, pp. 218-223, Aug. 2017.

[8] C. Rani, H. Modares, R. Sriram, D. Mikulski, FL. Lewis, "Security of unmanned aerial vehicle systems against cyber-physical attacks", The Journal of Defense Modeling and Simulation, vol. 13, no. 3, pp. 331-342, 2016.

[9] J. Yaacoub, H. Noura, O. Salman, A. Chehab, "Security analysis of drones systems: Attacks, limitations, and recommendations", Internet of Things, vol. 11, Sep. 2020.

[10] I. Astaburuaga, A. Lombardi, B. La Torre, C. Hughes and S. Sengupta, "Vulnerability Analysis of AR.Drone 2.0, an Embedded Linux System," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0666-0672, 2019.

[11] N. M. Rodday, R. d. O. Schmidt and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles," NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, pp. 993-994, 2016, doi: 10.1109/NOMS.2016.7502939.

[12] N. M. Rodday, "Hacking a Professional Drone," blackhat asia, 2016.

[13] K. Highnam, K. Angstadt, K. Leach, W. Weimer, A. Paulos and P. Hurley, "An Uncrewed Aerial Vehicle Attack Scenario and Trustworthy Repair Architecture," 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W), pp. 222-225, 2016, doi: 10.1109/DSN-W.2016.63.

[14] A. Luo, "Drones hijacking - multi-dimensional attack vectors and

countermeasures," Defcon 24, 2016.
[15] Dae-geon Kim, "Security Enhancement of Drone Considering the Characteristics of Data Transmitted between Wireless Channel," Journal of Defense and Security, vol. 3, no. 1, pp. 51-70, 2021.
[16] T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, P.M. Kintner and Jr, "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS), Savannah, GA, pp. 2314-2325, Sep 2008.
[17] A. Vervisch-Picois, N. Samama and T. Taillandier-Loize, "Influence of GNSS spoofing on drone in automatic flight mode, " International Symposium of Navigation and Timing 4th, Toulouse, France. pp. 1 - 9, Nov. 2017.
[18] D. He et al., "A Friendly and Low-Cost Technique for Capturing Non-Cooperative Civilian Unmanned Aerial Vehicles," in IEEE Network, vol. 33, no. 2, pp. 146-151, Apr. 2019, doi: 10.1109/MNET.2018.1800065.
[19] A.J. Kerns, D.P. Shepard, A.B. Jahshan and T.E. Humphreys, "Unmanned Aircraft Capture and Control Via GPS Spoofing," Journal of Field Robotics vol. 31, pp. 617-636, 2014.
[20] Seong-Hun Seo, Byung-Hyun Lee, Sung-Hyuck Im, Gyu-In Jee, "Effect of Spoofing on Unmanned Aerial Vehicle using Counterfeited GPS Signal," Journal of Positioning, Navigation, and Timing, vol. 4, no. 2, pp. 57-65, June 2015.
[21] J. Farlik, M. Kratky and J. Casar, "Detectability and jamming of small UAVs by commercially available low-cost means," 2016 International Conference on Communications (COMM), 2016, pp. 327-330, doi: 10.1109/ICComm.2016.7528287.
[22] T. Trippel, O. Weisse, W. Xu, P. Honeyman and K. Fu, "WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks," 2017 IEEE European Symposium on Security and Privacy (EuroS&P), 2017, pp. 3-18, doi: 10.1109/EuroSP.2017.42.
[23] Yun-mok Son, Ho-cheol Shin, Dong-kwan Kim, Young-seok Park, Ju-hwan Noh, Ki-bum Choi, Jung-woo Choi, and Yong-dae Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," 24th USENIX Conference on Security Symposium (SEC'15), pp. 881 - 896, 2015.
[24] M. robbinson, "Knocking my neighbors kids cruddy drone offline," Defcon 23, 2015.
[25] B. Nassi, R. Bitton, R. Masuoka, A. Shabtai and Y. Elovici, "Sok: security and privacy in the age of commercial drones," 2021 IEEE Symp. on Security and Privacy (SP), pp. 1434-1451, 2021.
[26] B Nassi, A Shabtai, R Masuoka, Y Elovici. "Sok - security and privacy in the age of drones: threats, challenges, solution mechanisms, and scientific gaps." ArXiv abs/1903.05155, 2019.
[27] Daegeon Kim, Huy Kang Kim, "Security Requirements of Commercial Drones for Public Authorities by Vulnerability Analysis of Applications," arXiv, 2019.
[28] J. Gordon, V. Kraj, J. H. Hwang and

A. Raja, "A Security Assessment for Consumer WiFi Drones," 2019 IEEE International Conference on Industrial Internet (ICII), 2019, pp. 1-5, doi: 10.1109/ICII.2019.00011.

[29] C. Hennebert, "A first Step towards a Protection Profile for the Security Evaluation of Consensus Mechanisms," 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), pp. 1-6, 2020, doi: 10.1109/IOTSMS52051.2020.9340216.

[30] Ji-soo Park, Seung-joo Kim. "Security Requirements Analysis on IP Camera via Threat Modeling and Common Criteria". KIPS Transactions on Computer and Communication Systems, vol. 6, pp.121-134, 2017.

[31] In-Kyung Oh, Jae-Wan Seo, Min-Kyu Lee, Tae-Hoon Lee, Yu-Na Han, Ui-Seong Park, Han-Byeol Ji , Jong-Ho Lee, Kyu-Hyung Cho, Kyoung-gon Kim, "Derivation of Security Requirements of Smart TV Based on STRIDE Threat Modeling," Journal of the Korea Institute of Information Security & Cryptology, vol. 30, no. 2, pp. 213-230, 2020.

[32] Shevchenko, Nataliya, "Threat Modeling: a Summary of Available Methods," Jul. 2018.

[33] A. Shostack, "Threat Modeling: Designing for Security," Wiley, 2014.

[34] R. Scandariato, K. Wuyts, W. Joosen, "A descriptive study of Microsoft's threat modeling technique," Requirements Engineering, vol. 20, no. 2, pp. 163–180, Jun. 2015.

[35] R. Khan, K. McLaughlin, D. Laverty and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), pp. 1-6, 2017, doi: 10.1109/ISGTEurope.2017.8260283.

[36] Paul Hong, Yejun Kim, Kwangsoo Cho, Seungjoo Kim, "A study on Security Requirements for 5G Base Station", Journal of The Korea Institute of Information Security & Cryptology, vol. 31, no. 5, Oct. 2021.

[37] Seung-hoon Park, "The CHAOS (ChibiOS based High Assurance Operating System) Project," https://github.com/HackProof/CHAOS

〈저자소개〉

구 도 형 (Do-hyung Gu) 정회원
2016년 2월: 고려대학교 사이버국방학과 학사
2017년 9월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호, 보안공학, 보안성 평가

김 승 주(Seung-joo Kim) 종신회원
1994년~1999년: 성균관대학교 정보공학과(학사, 석사, 박사)
1998년~2004년: 한국인터넷진흥원(KISA) 팀장
2004년~2011년: 성균관대학교 정보통신공학부 부교수
2004년~현재: 한국정보보호학회 이사
2007년: 국가정보원장 국가사이버안전업무 유공자 표창
2010년: 방송통신위원회 정보통신망 침해사고 민관합동조사단 위원
2011년~현재: 고려대학교 사이버국방학과/정보보호대학원 정교수
2012년: 선관위 디도스 특별검사팀 자문위원
2014년~2015년: 육군사관학교 초빙교수
2014년~2016년: 다음카카오 프라이버시 정책 자문위원회 위원
2015년~현재: 방위사업청 방산기술보호 자문관
2016년~2018년: 개인정보분쟁조정위원회 위원
2016년~현재: 산업통상자원부 전략물자기술 자문위원
2016년~현재: 한국카카오뱅크 정보보호부문 자문교수
2017년~현재: 고려대학교 국방RMF연구센터(AR2C) 센터장
2018년~2020년: 4차산업혁명위원회 위원: 대통령직속 4차산업혁명위원회 위원
2018년~현재: 고신뢰 보안운영체제 연구센터(CHAOS) 센터장
2020년~현재: 합동참모본부 정책자문위원회 자문위원
〈관심분야〉 보안공학 및 보안내재화 방법론, 보안성 평가/인증, RMF A&A, 암호학 및 블록체인

이 상 진(Sang-jin Lee) 종신회원
1989년 10월~1999년 2월: ETRI 선임 연구원
1999년 3월~현재: 고려대학교 교수
2008년 3월~현재: 고려대학교 디지털포렌식연구센터 센터장
〈관심분야〉 디지털포렌식