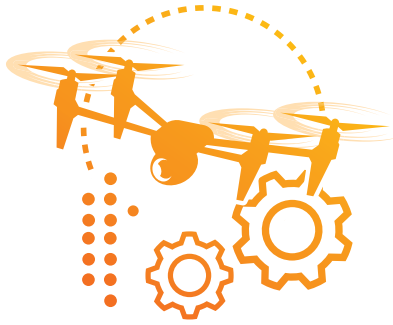
드론 ICT 보안기술 표준화 동향



강유성 _ 한국전자통신연구원 지능보안연구그룹 책임연구원(PL)
김건우 _ 한국전자통신연구원 지능보안연구그룹 책임연구원
김주한 _ 한국전자통신연구원 지능보안연구그룹 책임연구원
이상재 _ 한국전자통신연구원 지능보안연구그룹 책임연구원

1. 머리말

드론 보안은 기존의 다른 디지털 디바이스와 달리 드론이 피해자임과 동시에 공격자가 될 수 있는 양면성을 고려해야 한다. 드론 기반 서비스 제공자 입장에서는 드론이 피해자라는 측면을 고려하여 드론(데이터 포함)을 보호대상으로 두고 안정적 운영을 위한 기술개발 및 서비스 출시를 계획한다. 드론 ICT 보안기술이 그 예가 될 수 있다. 반면에 건물 관리자나 제3자 입장에서는 드론이 물리적 공격자가 될 수 있다는 염려가 있어 드론으로부터 내 건물, 나 자신을 보호해야 한다는 생각을 하게 된다. 안티드론 기술로 불리는 드론 격추 기술[1]이 그 대표적인 예가 될 수 있다.

드론 보안의 양면성 중 ICT 관점에서 드론과 데이터를 보호하고자 하는 드론 ICT 보안기술에 대한 관심이 점점 커지고 있으며, 일부 국내외 표준화 그룹에서는 드론 ICT 보안기술에 대한 표준화 작업을 진행하고 있다. 안티드론 기술과 달리 드론 ICT 보안기술은 통신 상대방이 존재하기 때문에 상호 호환성이 보장되는 표준화가 필수적으로 요구된다. 국내에서는 TTA와 사물인터넷융합포럼에서 표준화 활동을 하고 있고, 국제적으로는 JTC 1 SC 17에서 드론식별모듈(DIM, Drone Identity Module)[1] 중심의 드론 ICT 보안기술 표준화가 진행 중이다. 본고에서는 드론 및 드론의 데이터를 보호하고자 하는 관점에서 진행되고 있는 국내외 드론 ICT 보안기술 표준화 현황을 소개하고자 한다.

2. 국내 표준화 동향

2.1 응용보안/평가인증 프로젝트 그룹(PG504)

TTA PG504는 응용/융합 보안기술에 대한 표준화를 담당하고 있다. 드론 ICT 보안기술이 하나의 응용/융합 보안기술로써 표준화가 진행되었으며, 〈표 1〉과 같이 2건의 표준이 도출되었다.

2.1.1 드론 기반 서비스를 위한 보안 요구사항

1) 드론 식별정보 또는 드론 등록정보 등 최소 1개 이상의 드론 관련 정보를 저장하고 있으며 암호연산 동작을 수행할 수 있는 기능 모듈

<표 1> TTA 응용보안/평가인증 프로젝트 그룹(PG504) 표준

번호	표준번호	표준명	제정·개정	제·개정일
1	TTAK.KO-12.0317	드론 기반 서비스를 위한 보안 요구사항	제정	2017-12-13
2	TTAR-12.0033	드론 기반 서비스를 위한 보안 메시지 흐름(기술보고서)	제정	2018-11-07

<표 2> TTA 사물인터넷 융합서비스 프로젝트 그룹(SPG11) 표준

번호	표준번호	표준명	제정·개정	제·개정일
1	TTAK.KO-10.1058-Part4	사물인터넷 기반 저고도 무인 항공기 관리 및 운영 시스템 - 제4부: 경량 인증 절차	제정	2018-06-27

이 표준의 목적은 드론이 가지는 무인비행이라는 특성과 디지털 디바이스라는 특성을 고려하여 드론 기반 서비스를 위한 보안 요구사항을 정의하는 것이다[2]. 이 표준에서는 드론을 이용한 서비스를 제공하고자 할 때 필요한 6개의 구성요소(서비스 요청자, 서비스 제공기관, 지상 제어 장치, 구역 관리 장치, 정보 제공 장치, 드론)에 대한 기능적 특성을 먼저 정의하였다. 또한, 각각의 역할을 가진 구성요소에 대한 보안 요구사항과 각 구성요소 간 인터페이스 보안 요구사항을 정의하였고, 키 노출의 위험을 방지하기 위한 키 은닉 요구사항도 포함하고 있다.

드론을 이용한 다양한 서비스 제공 시 필요한 디지털 보안 서비스인 식별, 인증, 데이터 기밀성, 데이터 무결성, 가용성, 키 보호 등의 보안 요구사항을 담고 있는 매우 중요한 표준으로 TTA 저널을 통해 별도의 표준소개가 게재되기도 하였다[3].

2.1.2 드론 기반 서비스를 위한 보안 메시지 흐름(기술보고서)

TTA PG504에서 논의된 이 문서는 기술보고서이다. 이 기술보고서의 목적은 드론 기반 서비스 제공을 위한 구성요소 사이의 인증 및 데이터 보호를 위한 보안 메시지 흐름을 정의하는 것이다[4]. TTAK.KO-12.0317 '드론 기반 서비스를 위한 보안 요구사항'에서 정의한 시스템 구성요소 및 보안 요구사항을 고려하여 드론 기반 서비스에서의 드론 내부 키 은닉, 구성요소 간 통신 데이터 보호, 인증 등을 제공할 수 있는 보안 메시지 흐름을 정의한다. 이 기술보고서에서 정의한 보안 메시지 흐름은 보안 프로토콜로 구현되는 토대가 된다.

부록에는 드론 기반 무인배달 서비스에 적용되는 보안 프로토콜의 예시를 포함하고 있다. 부록에서 보이는 보안 프로토콜의 핵심적인 목표는 드론과 정보 제공 장치 사이의 암호키 노출 방지이다. 이 보안 프로토콜은 Peer Review를 거쳐 학술논문으로 발표되었으며, 부록 II-4에 해당 논문을 참고문헌으로 명시하고 있다. 드론 외의 주요 구성요소는 기존의 디지털 디바이스 또는 서버급 장치로 구성이 가능하며 보안 채널 구성은 기존의 검증된 메커니즘을 적용할 수 있다. 따라서 이 기술보고서에서는 드론 기반 서비스 구성요소 중 서비스 요청자, 서비스 제공기관 및 지상 제어 장치 간 보안 채널 구성은 따로 고려하지 않으며 안전한 채널이 형성되어 있다고 가정한다.

2.2 사물인터넷 융합서비스 프로젝트 그룹(SPG11)

TTA SPG11은 사물인터넷 특별기술위원회 산하 프로젝트 그룹 중 하나로, '사물인터넷 기반 저고도

무인 항공기 관리 및 운영 시스템'이란 제목으로 표준 시리즈 제정을 추진하였다. 그 결과, 제1부 요구사항과 제4부 경량 인증 절차를 제정 완료하였다. 〈표 2〉는 드론 보안기술과 관련된 표준목록이다.

2.2.1 사물인터넷 기반 저고도 무인 항공기 관리 및 운영 시스템 - 제4부: 경량 인증 절차

이 표준의 목적은 지상 통제 센터에서 저고도 무인 항공기(드론)를 인증할 수 있는 경량 인증 절차를 정의하는 것이다[5]. 기존 X.509 인증서가 아닌 축약된 형태의 인증서를 별도로 정의하고 있으며, 이러한 인증서 기반의 인증 키 생성 및 인증 절차를 정의하고 있다. 일반적인 인증서 기반의 인증 방식과 유사하며 경량 인증서를 사용한다는 특징을 가지고 있다. 별도의 보안성 분석서를 포함시키지 않았고 또한 Peer Review를 거쳐 발표된 학술논문을 참고문헌에 제시하지 않았기 때문에 해당 기술에 대한 보안성 분석이 별도로 필요할 것으로 보인다. 이 표준의 또 다른 특징은 부록 II-1 지식재산권 확약서 정보에 '안전한 드론 통신 프로토콜(국내 출원번호 10-2017-0168298)' 특허가 선언되어 있다는 점이다.

2.3 사물인터넷융합포럼 IoT정보보호분과위원회

사물인터넷융합포럼은 산·학·연·관 협력을 통해 사물인터넷 기술과 서비스 보급 및 국내외 표준화 활동을 통한 사물인터넷 산업 활성화에 기여하고자 설립된 포럼으로 그 뿌리는 2005년 시작된 모바일 RFID포럼에 두고 있다. IoT정보보호분과위원회에서는 드론 역시 사물인터넷 디바이스 중 하나로 인식하면서 〈표 3〉과 같이 드론 기반 사물인터넷 서비스에서의 보안기술을 포럼표준으로 제정하였다.

2.3.1 사물인터넷 기반 무인 배달서비스에서의 키 은닉 보안 요구사항

이 표준의 목적은 드론의 불법 포획에 이은 메모리 공격 등으로 내부에 저장된 키가 노출될 위험을 극복하기 위한 키 은닉 보안 요구사항을 정의하는 것이다[6]. 이 표준에서 정의한 키 은닉 요구사항은 화이트박스 암호 기술의 사용을 전제로 한다. 무인배달 시스템 구성요소 중 드론과 배달지점 장치가 마스킹된 화이트박스 암복호 테이블을 통해 키 해킹 공격에 안전한 키 은닉 기술을 구현할 수 있는 기능적 요구사항도 포함하고 있다. 이는 드론이 비행 중 탈취당하는 위협 상황을 고려한 보안 요구사항이라 할 수 있다.

2.3.2 드론 기반 사물인터넷 서비스를 위한 보안 요구사항

이 표준의 목적은 드론이 비행 대기 또는 비행 중 다양한 사물인터넷 디바이스와 통신을 수행하는 데 필요한 보안 요구사항을 정의하는 것이다[7]. 2015년 12월 1일에 제정되었으며, 드론을 이용한 서비스(무인 배달서비스, 무인 감시서비스 등) 제공을 위한 시스템 구성요소 정의, 구성요소별 보안 요구사항, 구

<표 3> 사물인터넷융합포럼 IoT정보보호분과위원회 표준

번호	표준번호	표준명	제정·개정	제·개정일
1	IoTFS-0039	사물인터넷 기반 무인 배달서비스에서의 키 은닉 보안 요구사항	제정	2014-12-09
2	IoTFS-0079	드론 기반 사물인터넷 서비스를 위한 보안 요구사항	제정	2015-12-01
3	IoTFS-0039-R1	드론 기반 배달서비스를 위한 키 은닉 요구사항	개정	2016-12-01
4	IoTFS-0079-R1	드론 기반 배달서비스를 위한 보안 요구사항	개정	2016-12-01
5	IoTFS-0096	드론 기반 배달서비스 프레임워크	제정	2016-12-01
6	IoTFS-0097	드론 기반 배달서비스를 위한 보안 프로토콜	제정	2016-12-01

성요소 간 인터페이스 보안 요구사항을 담고 있다. 이 표준은 포럼표준 완료 후 TTA 단체표준으로 제안되었으며, 2017년 제정된 TTA 표준인 TTAK.KO-12.0317의 모체가 된다.

2.3.3 드론 기반 배달서비스를 위한 키 은닉 요구사항

이 표준은 2014년에 제정된 IoTFS-0039 '사물인터넷 기반 무인 배달서비스에서의 키 은닉 보안 요구사항'을 개정하여 2016년 12월에 승인된 개정판이다[8]. 2014년 제1판과 키 은닉 요구사항은 동일하지만 연계표준들과의 연관성을 고려하여 제목을 수정하였고, 제1판의 부속서에 있던 무인배달 서비스에 특화된 보안 요구사항이 본문으로 들어왔다.

2.3.4 드론 기반 배달서비스를 위한 보안 요구사항

이 표준은 2015년에 제정된 IoTFS-0079 '드론 기반 사물인터넷 서비스를 위한 보안 요구사항'을 개정하여 2016년 12월에 승인된 개정판이다[9]. 2015년 제1판과 구성요소 보안 요구사항과 인터페이스 보안 요구사항은 동일하다. 그러나 개정판에는 드론 기반 무인 배달서비스를 위한 시스템 구성요소에 대한 정의가 삭제되었다. 그 이유는 구성요소 정의 및 구성요소 역할을 설명하는 부분을 발췌하여 드론 기반 배달서비스 프레임워크를 별도의 표준으로 추진하였기 때문이다. 이에 따라 각 표준의 연관 관계를 재구성하게 되었다. 각 표준 간의 연관 관계는 이 표준의 부록 I-3에 설명되어 있다.

2.3.5 드론 기반 배달서비스 프레임워크

이 표준의 목적은 드론을 이용한 다양한 서비스 중 물품운송이라는 고유의 역할을 가진 무인배달 서비스에 특화된 구성요소 및 각각의 역할을 정의하는 것이다[10]. 2015년에 제정된 IoTFS-0079 '드론 기반 사물인터넷 서비스를 위한 보안 요구사항' 표준에 정의되어 있던 시스템 구성요소 부분을 발췌하여 재구성한 표준으로 연계 표준들이 준용하는 드론 기반 무인배달 서비스 프레임워크를 제공하고 있다.

2.3.6 드론 기반 배달서비스를 위한 보안 프로토콜

이 표준의 목적은 드론 기반 무인 배달서비스에서 드론을 중심으로 한 데이터 통신 환경과 보안 요구사항을 고려하여 데이터 기밀성, 무결성, 구성요소 간 인증, 물품수신 부인방지 등의 보안 서비스를 제공하는 보안 프로토콜을 정의하는 것이다[11]. 이 표준의 구현은 IoTFS-0079-R1 '드론 기반 배달서비스를 위한 보안 요구사항'과 IoTFS-0039-R1 '드론 기반 배달서비스를 위한 키 은닉 요구사항'을 준용하여 드론 기반 무인 배달서비스에서의 드론 내부 키 은닉, 구성요소 간 통신 데이터 보호, 인증 등을 제공할 수 있다. 이 표준은 포럼표준 완료 후 TTA 단체표준으로 제안되었으며, 2018년 제정된 TTA 기술보고서인 TTAR-12.0033의 모체가 된다.

3. 국제표준화 동향

3.1 JTC 1 SC 17 WG 12

최근 드론 ICT 보안기술과 관련해서 드론식별모듈 및 드론 조종자(일대일), 드론 운영자(일대다) 면허증 규격 관련한 국제표준화 활동이 시작되었다. JTC 1 SC 17 WG 12가 해당 표준화 그룹이며 표준그룹 명칭은 'Drone license and drone identity module'이다. SC 17은 IC 카드 물리적 규격, 보안기술 규격, ISO 운전면허증 규격 등 IC 카드 관련 국제표준을 제정한 표준위원회이며, 산하 표준그룹인 WG 12는 2018년 4월에 제1차 회의를 시작하였다. 이 표준그룹의 표준화 대상은 드론 면허증(라이선스)과 드론

<표 4> JTC 1 SC 17 WG 12 표준

[2019년 3월]

번호	표준번호	표준명	현단계	에디터
1	ISO/IEC 22460-2	ISO License and Drone Identity Module for Drone(Ultra Light Vehicle or Unmanned aircraft system) — Part 2: Drone Identity Module	2nd WD*	- 강유성(한국 ETRI) - Haiying Lu(중국 CESI)

* WD(Working Draft, 작업 초안): 위원회 승인받기 전, 작업반이 작성 중인 문서

<표 5> ITU-T Q11/17 표준

[2019년 3월]

번호	표준번호	표준명	현단계	에디터
1	ITU-T X.uav-oid	Identification mechanism for unmanned aerial vehicles using object identifiers	TD**	- Wenjing Ma(중국 CESI)

** TD(Temporary Document): 표준화가 진행 중인 과정에서 발표되는 논의 문서

식별모듈이다.

'Unmanned aircraft systems'란 명칭으로 운영되고 있는 ISO TC 20 SC 16 표준위원회는 드론 생산과 관리, 운영절차, 드론 교통관리체계 등을 표준화 대상으로 삼고 있으나 드론 ICT 보안기술은 표준화 대상에서 빠져 있다. 그러나 점차 드론 ICT 보안기술 표준화의 중요성을 인식하면서 ISO TC 20 SC 16과 JTC 1 SC 17 WG 12는 Liaison officer를 통해 드론 ICT 보안기술 표준화 협력을 강화해 갈 것으로 보인다. 〈표 4〉는 JTC 1 SC 17 WG 12에서 표준화를 진행 중인 드론 ICT 보안기술 관련 표준인 드론식별모듈 표준이다.

3.1.1 ISO/IEC 22460-2 Drone Identity Module

이 표준의 목적은 드론식별모듈(DIM, Drone Identity Module)의 데이터세트와 암호연산 기능을 정의하는 것이다[12]. 드론식별모듈은 드론 식별정보 또는 드론 등록정보 등 최소 1개 이상의 드론 관련 정보를 저장하고 있으며 암호연산 동작을 수행할 수 있는 기능적 모듈로 정의된다. 구현 형상에 대해서는 하드웨어(USIM 타입, uSD 타입, eSIM 타입 등) 또는 소프트웨어 구현이 가능하다. 그리고 이 표준은 드론식별모듈을 기반으로 하여 드론과 주변 구성요소 사이의 인증과 보안채널 설립을 위한 보안 프로토콜 정의를 표준화 범위에 포함하고 있다.

2018년 10월 일본에서 개최된 제3차 WG 12 회의에서 이 표준의 첫 번째 WD가 논의되었으며, 2019년 4월 제5차 싱가포르 회의에서 두 번째 WD가 논의될 예정이다. 두 번째 WD에 따르면, 드론식별모듈의 데이터세트는 드론 식별정보, 드론 등록정보, 드론 비행정보, 그리고 키, 인증서, 난수와 같은 암호연산용 데이터들로 구성된다. 보안 프로토콜은 비대칭키 기반의 인증 및 키 설립, 대칭키 기반의 인증 및 키 설립, 그리고 드론 비행정보 무결성 보장을 위한 전자서명 등의 보안 동작이 포함되어 있다.

드론 보안의 양면성인 드론 ICT 보안기술과 안티드론 기술 모두 그 시작은 정상 드론과 비정상 드론의 식별이다. 따라서 드론식별모듈 표준은 드론 보안에 있어 매우 중요한 표준이 될 것으로 보인다. 이 표준은 2021년 상반기에 IS 제정을 목표로 하고 있다.

3.2 ITU-T SG 17 Question 11

드론 식별과 관련하여 중요한 표준화 기술 중 하나가 글로벌 식별체계 구축이다. ITU-T의 Q11/17은 트리 구조의 계층화 식별로 사용할 수 있는 OID(Object

Identifiers) 표준화를 성공적으로 수행하였다. 자연스럽게 이 표준그룹은 드론을 전 세계적으로 유일하게 식별할 수 있는 드론 식별체계에 OID 체계를 적용하려는 표준화를 시작하였다. 〈표 5〉는 ITU-T Q11/17에서 추진하고 있는 드론 식별체계 표준이다.

3.2.1 ITU-T X.uav-oid Identification mechanism for unmanned aerial vehicles using object identifiers

이 표준의 목적은 OID를 이용하여 드론을 식별하는 체계를 정의하는 것이다[13]. 이미 글로벌 IoT 시장에서 널리 사용하고 있는 OID 체계를 드론 식별에 준용하려는 내용을 담고 있다. OID는 ITU-T와 ISO가 공통표준(ITU-T X.660, ISO/IEC 9834-1)으로 제정한 국제표준이다. 현재 표준화가 진행 중인 ITU-T의 X.uav-oid 표준은 드론 식별체계 구축 시 확장성과 호환성 측면에서 합리적인 표준이 될 것으로 보인다. 2019년 3월 현재 논의 중인 TD는 'Base text of ITU-T X.uav-oid'이다.

4. 맺음말

과거에는 특정 서비스나 제품을 만들 때, 보안기술 적용은 우선순위에서 밀려 있었던 것이 사실이다. 일단 서비스 개시 후 취약점이 발견되면 '소 잃고 외양간 고치기' 식의 후속조치를 취하는 것이었다. 그러나 최근에는 개발 프로세스에서 애초에 보안 내재화(Security by Design) 설계를 추구하는 경향이 생겼다. 드론 보안 역시 이러한 보안 내재화 설계가 필수적이다.

특히 드론 보안의 양면성을 모두 고려해서 서비스 아키텍처 설계부터 제품 구현까지 모두 보안 내재화 설계가 필요하며, 이런 경우에 표준화된 보안 요구사항과 이를 준용하는 드론식별모듈, 식별체계 구축은 드론 보안기술의 첫걸음이라 할 수 있다. 본고에서 소개하는 표준화 동향뿐만 아니라 향후 지속적으로 발전해 나갈 기술 및 표준화는 안전하고 신뢰할 수 있는 드론 운행 환경 구축에 활용될 수 있을 것으로 기대된다.

※ 본 연구는 과학기술정보통신부의 재원으로 한국연구재단, 무인이동체미래선도핵심기술개발사업단의 지원을 받아 수행되었음(NRF-2017M1B3A2A01056680, 저고도 무인비행장치 교통관리체계 보안기술 및 불법 행위 억제 기술 개발).

[참고문헌]

[1] Dronedefender, https://www.battelle.org/government-offerings/national-security/aerospace-systems/counter-UAS- technologies/dronedefender, Battelle.
[2] TTAK.KO-12.0317, 드론 기반 서비스를 위한 보안 요구사항, TTA PG504, 2017.12.13.
[3] 강유성, 김건우, 김주한, 드론 기반 서비스를 위한 보안 요구사항, TTA 저널, Vol. 177, pp. 74-79, 2018.06.
[4] TTAR-12.0033, 드론 기반 서비스를 위한 보안 메시지 흐름(기술보고서), TTA PG504, 2018.11.07.
[5] TTAK.KO-10.1058-Part4 사물인터넷 기반 저고도 무인 항공기 관리 및 운영 시스템 - 제4부: 경량 인증 절차, TTA SPG11, 2018.06.27.
[6] IoTFS-0039, 사물인터넷 기반 무인 배달서비스에서의 키 은닉 보안 요구사항, 사물인터넷융합포럼 IoT정보보호분과위원회, 2014.12.09.
[7] IoTFS-0079, 드론 기반 사물인터넷 서비스를 위한 보안 요구사항, 사물인터넷융합포럼 IoT정보보호분과위원회, 2015.12.01.
[8] IoTFS-0039-R1, 드론 기반 배달서비스를 위한 키 은닉 요구사항, 사물인터넷융합포럼 IoT정보보호분과위원회, 2016.12.01.
[9] IoTFS-0079-R1, 드론 기반 배달서비스를 위한 보안 요구사항, 사물인터넷융합포럼 IoT정보보호분과위원회, 2016.12.01.
[10] IoTFS-0096, 드론 기반 배달서비스 프레임워크, 사물인터넷융합포럼 IoT정보보호분과위원회, 2016.12.01.
[11] IoTFS-0097 드론 기반 배달서비스를 위한 보안 프로토콜, 사물인터넷융합포럼 IoT정보보호분과위원회, 2016.12.01.
[12] ISO/IEC 2nd WD 22460-2, ISO License and Drone Identity Module for Drone(Ultra Light Vehicle or Unmanned aircraft system) — Part 2: Drone Identity Module, JTC1 SC17 WG12, 2019.03.
[13] ITU-T X.uav-oid, Identification mechanism for unmanned aerial vehicles using object identifiers, ITU-T SG17: Q11/17, 2019.03.