전투기 감항 보안 인증에 관한 연구

김현주*, 강동수**
국방대학교 컴퓨터공학전공
e-mail: *st9280fly@naver.com, **greatkoko@kndu.ac.kr

A Study of Fighter-plane Airworthiness Security Certification

HyunJu Kim*, DongSu Kang**
* **Dept of Computer Science and Engineering, Korea National Defense University

요 약

최신 전투기로 발전할수록 증가되는 소프트웨어 의존도와 네트워크 중심전으로의 작전 수행 개념의 변화, 그리고 무기체계에 대하여 지속적으로 발전하는 사이버 위협의 증가는 전투기 소프트웨어에 대한 강화된 보안 대책을 요구하고 있다. 이러한 상황의 변화는 전투기의 운용 및 소프트웨어 결함에 대한 감항인증 뿐만 아니라, 전투기 소프트웨어에 대한 사이버 위협의 보안 대책도 함께 요구한다. 따라서 본 연구에서는 항공기 및 시스템 감항 보안 인증기준인 DO-326A와 DO-356을 적용하여 전투기 운용 환경을 고려한 항공무기체계의 특성과 항공기에 대한 사이버 공격에 대해 살펴보고, 이를 바탕으로 감항 보안 프로세스를 적용해 본다.

1. 서론

현대전에서 공중우세의 확보는 전쟁 승리의 필수 요소이며, 이에 따라 각국은 최신 전투기의 도입 및 개발 사업 등을 통해 공군력의 향상을 위하여 지속적인 노력을 기울이고 있다. 1960년대 소프트웨어가 항공기 시스템에 처음 사용되기 시작한 이래로 소프트웨어의 비중과 역할은 비약적으로 증가해왔다. 전투기에서 소프트웨어를 통해 기능을 구현하는 비중은 1960년대에 개발된 F-4 전투기에서는 8%에 불과했지만, F-15는 35%, F-16은 45%로 증가하였으며 F-35에서 소프트웨어가 차지하는 비중은 90%로 F-4에 비해 11배가 증가하였다.[1]

최신 전투기로 발전할수록 소프트웨어의 의존도는 높아지고 있고, 네트워크 중심전(NCW: Network Centric Warfare)으로 작전 수행 개념이 변화되면서 전투기 자체가 하나의 노드로써 전장지휘체계와 연동되어 운용되고 있으며, 네트워크화 되는 무기체계에 대한 사이버 위협의 증가는 전투기 소프트웨어에 대한 강화된 보안 대책을 요구하고 있다.

이러한 현실을 고려할 때, 앞으로는 전투기를 개발함에 있어서 전투기 운용 및 소프트웨어 결함에 대한 감항인증 뿐만 아니라, 전투기 소프트웨어에 대한 사이버 위협 방지 대책도 함께 고려되어야 한다. 따라서 본 논문에서는 항공기 및 시스템 감항 보안 인증기준인 DO-326A와 감항 보안 방법 및 고려사항을 제공하는 DO-356을 기본으로 전투기 운용 환경의 특징을 고려한 전투기 소프트웨어 보안 인증기준을 적용해 보고자 한다.

2. 관련연구

2.1 항공소프트웨어 감항 보안 인증 표준

항공소프트웨어 비중의 증가와 함께 소프트웨어가 항공기 안전에 미치는 영향에 대한 중요성은 오래전부터 인식되어 1980년 처음으로 항공기 시스템과 장비 인증에 관한 소프트웨어 고려사항인 DO-178이 발표되었다. 그러나 항공소프트웨어 보안 관련 인증기준은 비교적 늦은 시기인 2014년에 발표되었는데 DO-326A(Airworthiness Security Process Specification), DO-355(Information Security Guidance for Continuing Airworthiness), DO-356 (Airworthiness Security Methods and Considerations) 등이 그것이다.[2] DO-326A는 사이버 위협으로부터 항공기 소프트웨어의 안전을 보증하기 위한 지침이고, DO-355는 항공소프트웨어의 지속적인 감항성을 유지하기 위한 작동 및 유지 보수에 대한 지침이며, 마지막으로 DO-356은 항공기 개발 수명주기 동안 감항성을 확보하기 위한 방법과 고려사항을 제공한다.

2.2 감항 보안 프로세스 및 보안 위협 평가

감항인증 보안 프로세스는 인증 프로세스와 관련된 인증 활동(Certification related Activities), 항공기와 시스템에 대한 위협 시나리오를 항공기가 수용 가능한지 여부를 평가하는 보안 위협 평가 활동(Security Risk Assessment related Activities), 보안 위협 평가 활동 결과에 의해 필요한 보안 대책을 구현하기 위한 보안 개발 활동(Security Development related Activities)의 세가지 영역으로 구성

된다.

DO-326A[3]는 의도적인 비인가 전자적 상호작용의 위협으로부터 항공기 안전을 보증하기 위하여 7단계의 보안 프로세스를 제공한다. 첫 번째는 보안 인증 계획(Plan for Security Aspects of Certification) 단계로 인증 신청자가 계획하고 인증기관에서 동의함으로써 달성된다. 두 번째는 보안 영역 정의(Security Scope Definition) 단계로 보안 위험 평가를 위한 보안 영역을 정의하며, 세 번째는 보안 위험 평가(Security Risk Assessment) 단계로 보안 위험을 식별하고 평가한다. 네 번째는 보안 위험의 수용 가능 여부를 판단하여 보안대책이 필요한 경우 다섯 번째인 보안 개발(Security Development) 단계로 넘어간다. 보안 개발은 보안 위험을 포함하는 시나리오에 대응하는 보안 대책인 보안 아키텍처를 설계하는 과정이다. 여섯 번째는 보안효율 인증(Security affectiveness assurance) 단계로 다섯 번째 단계인 보안 개발의 수행 결과로, 보안 위협이 수용 가능함을 인증하기 위해 수행되어 진다. 여기서 "보안효율"이란 비인가 상호작용에 대응하여 항공기를 얼마나 잘 보호하는지에 대해 설명하는 용어로 보안 위험 평가 단계에서 식별되는 위협 시나리오에 대하여 항공기 및 시스템을 보호하기 위한 보안대책 능력으로 정의할 수 있다. 마지막 단계는 결과 종합으로 위험이 수용 가능한 경우, 감항 보안 활동 결과를 보고서(PSecAC Summary)로 종합하는 것이다.

전투기 운용 환경을 고려한 감항 보안 프로세스를 적용하기 위해서는 시나리오 작성을 통해 공격 위협을 식별하는 보안 위험 평가와 관련된 활동이 중요하다. 보안 위험 평가는 비인가된 상호작용에 의한 시스템 및 항공기의 보안 위험을 평가하는 것을 뜻한다. 이 단계에서는 위협 상태를 식별하고 평가하여 위협 시나리오를 작성하고 보안 대책을 반영하여 위협 평가 레벨을 선정한다. 보안 위험 평가의 역할은 위협 시나리오에서 도출된 위협 레벨과 위협 상태 심각도에 기초하여 항공기가 보안 위험을 수용할 수 있도록 보안 대책을 수립하는데 충분한 근거를 제공하는데 있다.

항공기가 보안 위험을 수용할 수 있는지 여부를 결정하기 위해서 감항 보안 수락 매트릭스(Airworthiness Security Acceptability Matrix)를 사용하는데 이는 위협 시나리오에서 사이버 위협이 항공기에 미치는 영향력의 정도와 공격 성공 가능성의 조합에 따라 보안 위험의 수용 가능 여부를 판단하게 하는 도구이다. 감항 보안 수락 매트릭스에서는 사이버 위협이 항공기에 미치는 영향력의 정도를 Catastrophic, Hazadous, Major, Minor, No Safety Effect의 다섯 단계로 구분하였으며, 사이버 공격의 성공 가능성에 따라서 Frequent, Probable, Remote, Extremely Remote, Extremely Improbable의 다섯 단계로 구분한다. <표 1>은 감항 보안 수락 매트릭스를 나타낸 것이다.[4]

<표 1> Airworthiness Security Acceptability Matrix

위험 레벨		위협 시나리오 영향력				
위협 시나리오 성공가능성		V	IV	III	II	I
		No Effect	Minor	Major	Hazadous	Catastrophic
pV	Frequent	수용	수용 불가	수용 불가	수용 불가	수용 불가
pIV	Probable	수용	수용	수용 불가	수용 불가	수용 불가
pIII	Remote	수용	수용	수용	수용 불가	수용 불가
pII	Extremely Remote	수용	수용	수용	수용	수용 불가
pI	Extremely Improbable	수용	수용	수용	수용	수용*

*=Risk acceptability must include demonstrating the absencce of a single point of vulnerability

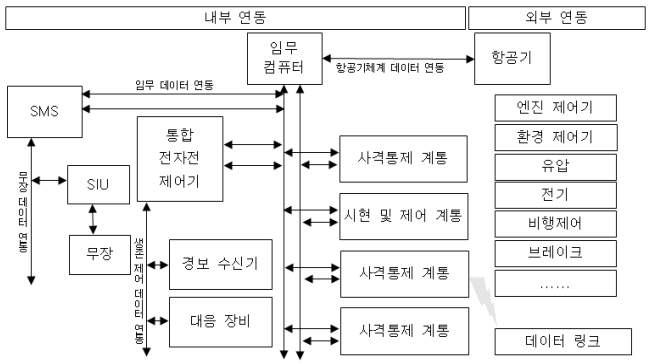
3. 전투기 감항 보안 적용 방안

전투기 운용 환경을 고려한 감항 보안 프로세스를 적용하기 위해서 본 장에서는 항공무기체계의 특성과 항공기에 대한 사이버 공격에 대해 살펴보고, 이를 바탕으로 감항 보안 프로세스를 적용하도록 하겠다.

3.1 항공무기체계의 특성

항공무기체계는 고정익과 회전익, 무인기 등으로 분류되고 고정익은 다시 임무 및 기능에 따라 전투기, 공격기, 폭격기, 전자전기, 수송기, 정찰기, 해상 초계기, 훈련기 등으로 분류된다. 한국 공군의 항공무기체계 중 가장 큰 비중을 차지하고 있는 전투기는 모든 전쟁의 시점과 다양한 전장 상황하에서 운용되는 공군의 핵심 전력이다. 전투기의 임무는 크게 공대공(Air to Air)과 공대지(Air to Surface)로 나뉘며 이러한 임무를 수행하는데 필요한 시스템들의 집합인 항공전투체계와 기체를 운영하는데 필요한 기능을 수행하는 항공기체계, 그리고 타 전투체계와 연동되어 운영되는 전술데이터 링크 체계로 구성되어 있다. 특히 항공전투체계는 통합 임무 컴퓨터를 중심으로 사격통제체계, 시현 및 제어체계, 생존체계, 통신 및 식별체계, 항법체계 등으로 구성되어 있다.

최신 전투기로 발전할수록 항공기 체계 자체의 내부 시스템들 간의 데이터 연동이 중시 된다. 항공기의 내부 시스템들 간의 통신은 내부 데이터 버스를 활용하여 데이터 연동이 이루어지며, 이와 동시에 전투 임무 수행을 위한 외부 데이터와의 연동도 함께 이루어 진다. 항공기 시스템들 간의 내부 데이터 버스를 활용한 데이터 연동과 외부 데이터 연동에 대한 개략적인 구성과 상호 관계는 (그림 1)과 같이 나타낼 수 있다.[5]



(그림 1) 전투기 체계간 데이터 연동

3.2 항공기에 대한 사이버 공격

보안 위험 평가 단계의 중요 활동 중에 하나인 위협 시나리오를 작성하기 위하여 항공기를 대상으로 실제 발생하였거나 발생 가능성이 있는 사이버 공격 사례들을 식별하고자 한다.

먼저 민항기에서 실제로 발생한 사례로 항공기 내 엔터테인먼트 시스템 해킹을 통해 엔진 제어 시스템의 접근권한을 획득한 사례와, 항공기 위치탐지시스템과 운항정보 교신시스템을 해킹하여 비행중인 항공기의 제어권을 획득 가능하다는 보고를 들 수 있다. 또한 미국 Worcester 공항의 항공관제 시스템에 침입하여 항공기 및 지상 유무선 통신을 차단한 사례가 있었으며 2010년 이후로 북한의 지속적인 GPS 전파 교란은 항공기 항법체계의 이상작동을 유발하였다.

다음은 전투기의 임무 단계별로 발생 가능한 사이버 공격 유형과 그에 따른 결과를 정리한 표이다.

<표 2> 전투기 사이버 공격유형 및 결과

임무 단계	계통	공격 유형	결과	비고
정비	DTRS	데이터 유출	· 정비용 노트북 연결을 통한 전투기 성능 및 엔진 데이터 유출	T1
	IMDC	서비스 거부	· 임무컴퓨터 성능 개량 및 암호코드 업데이트 시 악성코드 주입을 통한 서비스 거부	T2
지상 작동	IMDC	서비스 거부	· DTC(Data Transfer Cartridge) 장착 시 임무컴퓨터 내 악성코드 주입을 통한 서비스 거부	T3
항법	COM	서비스 거부	· 항공관제 시스템 해킹을 통한 무선통신 차단	T4
	NAV	권한 상승	· 항법장비 해킹을 통한 전투기 제어권 획득	T5
	GPS	변조	· GPS 재밍에 의한 항법 교란	T6
임무	Data Link	서비스 거부	· 전투지휘체계 해킹을 통한 Data Link 체계 무력화	T7
	GPS	변조	· GPS 재밍에 의한 GPS 유도 미사일 무력화 및 오폭 유발	T8
	S/W	서비스 거부	· EMP탄에 의한 전투기 전자장비 기능 상실	T9

전시 상황에서 적은 군 지휘통제체계 해킹을 통해 전술데이터 링크를 마비시킬 수 있으며, EMP(Electronic Magnetic Pulse)탄을 이용하여 전투기 내 전자장비의 기능을 무력화 시킬 수도 있다. 이러한 상황이 실제 전투기에 발생하게 된다면 치명적인 결함의 발생으로 인해 막대한 전투력의 손실을 유발하게 될 것이다. 따라서 감항 보안 프로세스의 적용을 통해 전투기의 운영 환경 하에서 발생 가능한 위협 시나리오를 식별하여 전투기가 감내 할 수 있는 수준의 위협들로 관리하는 것은 매우 중요하다.

3.3 전투기 감항 보안 프로세스 적용

우리나라 최초로 국내에서 개발된 전투기인 FA-50에 감항 보안 프로세스를 적용해 보면 다음과 같다. 앞서 기술한 바와 같이 감항 보안 프로세스는 총 7단계로 진행된다.

첫째, 항공기 보안 인증 계획 단계로 FA-50이 전·평시 운용 중에 보안 위협으로부터 안전성을 인증 받을 수 있도록 한다.

둘째, 보안 영역 정의 단계로 FA-50이 안전성을 보증받아야할 내·외부 자산을 식별한다. 내부 자산으로는 임무컴퓨터를 중심으로 한 항공전투체계, 엔진/전기/유압 등의 항공기 체계 등이 있으며 외부 자산으로는 Link-16 시스템과 항법 및 통신 장비 등이 있다.

<표 3> Airworthiness Security Acceptability Matrix

위험 레벨		위협 시나리오 영향력				
위협 시나리오 성공가능성		Ⅴ	Ⅳ	Ⅲ	Ⅱ	Ⅰ
		No Effect	Minor	Major	Hazadous	Catastrophic
pⅤ	Frequent	수용	수용 불가	수용 불가	수용 불가	수용 불가
			T6			T8
pⅣ	Probable	수용	수용	수용 불가	수용 불가	수용 불가
			T1		T2, T3	T9
pⅢ	Remote	수용	수용	수용	수용 불가	수용 불가
pⅡ	Extremely Remote	수용	수용	수용	수용	수용 불가
				T4	T5	
pⅠ	Extremely Improbable	수용	수용	수용	수용	수용
					T7	

셋째, 보안 위험 평가 단계이다. 이 단계는 민항기와는 다른 전투기만의 운용 특성을 반영할 수 있다는 측면에서 매우 중요하다. 먼저 위협 상황을 식별하고 평가하는데 FA-50의 운용 중에 발생 가능한 위협 상황에는 중요 데이터 유출 및 악성코드 주입, 통신 및 항법망 해킹, 전투지휘체계 해킹을 통한 Link-16 무력화, GPS 재밍을 통한 오폭 및 EMP탄에 의한 전자장비 기능 무력화 등을 들 수 있다. 이러한 위협 상황들로부터 위협 시나리오를 작성하여, <표 1>의 감항 보안 수락 매트릭스에 적용하고

FA-50이 보안 위험을 수용할 수 있는지 여부를 결정한다. <표 3>은 감항 보안 수락 매트릭스에 FA-50이 직면할 수 있는 위협 상황을 적용한 예이다.

민항기와 달리 전투기는 사이버 공격에 의한 항공기의 생존성 유지 외에 유사시 전투 임무 성공이라는 목표를 동시에 가진다. 따라서 감항 보안 수락 매트릭스를 적용함에 있어서 전투기의 이러한 특성을 반영하여 사이버 공격이 임무 수행에 미치는 영향도 함께 고려하였다. <표 3>에서는 T1, T4, T5, T7이 수용 가능한 보안위협으로 식별되었으며, T2, T3, T6, T8, T9는 수용불가하여 별도의 보안대책이 필요한 보안위협으로 식별되었음을 보여주고 있다.

감항 보안 수락 매트릭스 결과에 따라 T1, T4, T5, T7은 바로 일곱 번째 단계로 넘어가서 이에 대한 감항 보안 활동 결과 보고서를 작성하고, T2, T3, T6, T8, T9은 다섯 번째 단계인 보안 개발로 넘어간다. 이 단계에서는 FA-50이 수용할 수 없었던 보안 위협에 대한 대책을 보완하며, 여섯 번째 단계에서는 보안 대책이 적절하게 수립되었는지 평가한다. 보안 대책이 적절하게 수립되었다면 최종 단계로 진행하여 감항 보안 활동 보고서를 작성한다.

4. 결론 및 향후 연구

미래전의 양상이 플랫폼 중심전에서 네트워크 중심전으로 변화함에 따라 미래의 전쟁에서는 물리적 공격과 사이버 공격이 함께 이루어지게 될 것이다. 핵심 무기체계 중 하나인 전투기 역시 이러한 사이버 공격에서 자유로울 수 없으며 사이버 공격에 의한 전투기의 피해는 매우 큰 전력 손실을 가져오게 된다. 이러한 전쟁 양상의 변화에 맞추어 사이버 보안 위협에 대한 전투기의 감항 인증에 대한 연구가 필요하다.

따라서 본 논문에서는 항공기 및 시스템 감항 보안 인증기준인 DO-326A와 감항 보안의 방법과 고려사항에 대해 기술하고 있는 DO-356을 기본으로, 전투기의 체계 구성 및 발생 가능한 공격 사례들을 식별하여 감항 보안 프로세스에 적용해 보았다.

향후 연구에서는 DO-326A의 감항 보안 프로세스를 적용하여 그에 따른 산출물을 작성하고, 전투기 구성 체계를 통해 발생 가능한 보안 위협 시나리오를 도출하여 전투기 개발에 필요한 보안 요구사항을 만들고자 한다.

참고문헌

[1] 강동수외, “무기체계 SW발전방향 및 추진전략 연구”, 방위산업진흥회, 2016.

[2] 한만군, 박태규, “항공소프트웨어 안전과 보안을 위한 통합 감항 인증기준 개발 연구,” J. of The Korean Society for Aeronautical and Space Sciences 46(1), 2018, pp. 86~94.

[3] RTCA, DO-326A, Airworthiness Security Process Specification, Aug. 6, 2014, pp.8~9,19~23,

[4] RTCA, DO-356, Airworthiness Security Methods and Consideration, Sep. 23, 2014, pp.27.

[5] 최준성, 국광호, “군용항공기 감항인증을 고려한 항공무기체계 보안 강화 코딩룰 선정평가,” 보안공학연구 논문지, 2014, pp.439~454.