KIPS Trans. Softw. and Data Eng.
Vol.8, No.6 pp.223~234 pISSN: 2287-5905

https://doi.org/10.3745/KTSDE.2019.8.6.223

A Design of Risk-Based Security Threat Assessment Process for Fighter-Aircraft Airworthiness Security Certification

Hyunju Kim† · Dongsu Kang††

ABSTRACT

Cyber attacks are an important factor that determines the victory and defeat of Network-centric wars in which advanced weapon systems are highly interlinked. In addition the increasing dependability on software as its develop as the latest fighter is demanding enhanced security measures for fighter software to Cyber attacks. In this paper, we apply the DO-326A, which is an airworthiness security certification standard, to design a risk-based security threat assessment process by reflecting characteristics and operational environment of fighter aircraft. To do this, we add the following steps in security threat assessment stage of DO-326A's airworthiness security certification process. First, we derive security threats of fighter. And then, we scored the security threat in terms of possibility and impact on the fighter. Finally, we determine the security risk severity.

Keywords : Airworthiness Certification, Cyber Attack, Fighter-Aircraft Software, Security Threat, Risk Assessment, Airworthiness Security Certification Process

전투기 감항 보안 인증을 위한 위험기반 보안위협 평가 프로세스 설계

김 현 주† · 강 동 수††

요 약

첨단 무기체계들이 고도로 연동되어 수행되는 네트워크 중심전에서는 사이버 공격이 전쟁의 승패를 좌우하는 커다란 위협으로 대두되었다. 또한 최신예 전투기로 발전할수록 증가하는 소프트웨어 의존도는 사이버 공격에 대한 전투기 소프트웨어의 강화된 보안대책을 요구하고 있다. 본 논문에서는 항공기 감항 보안 인증 표준인 DO-326A를 적용함에 있어 전투기의 특성 및 운용환경을 반영하여 위험기반 보안위협 평가 프로세스를 설계한다. 이를 위하여 DO-326A의 감항 보안 인증 프로세스의 보안위협 평가 단계에서 전투기 보안위협을 도출하고 사이버 공격의 발생 가능성과 전투기에 미치는 영향력의 관점에서 위협을 점수화하며 보안위험 심각도를 결정하는 단계를 추가하여 적용한다.

키워드 : 감항인증, 사이버 공격, 전투기 소프트웨어, 보안위협, 위험평가, 감항 보안 인증 프로세스

1. 서 론

미국의 한 매체에서는 항공기 엔터테인먼트 시스템에 접속하여 실제 운항중인 항공기의 엔진을 조작한 보안 전문가를 미국 FBI에서 조사하고 있다고 보도하였다. 또한 중국에서 개최된 국제 모바일 해킹 보안 컨퍼런스에서는 항공기에서 사용하는 무선 통신 신호를 해킹하여 통신 내용을 조작함으로써 항공기에 악의적인 영향을 미칠 수 있다는 연구 결과를 발표하였다. 현재까지 전 세계적으로 항공기에 대한 사이버 공격으로 인적·재산적 피해를 입은 직접적인 사례는 보고된 바가 없지만 이러한 공격이 실제로 일어나고 성공할 수 있다는 가능성이 지속적으로 제기됨[1]에 따라 항공기 보안에 대한 경각심이 요구되고 있다.

한편 군사적 차원에서는 사이버 공간이 육, 해, 공, 우주에 이어 제5의 전장으로 포함되고 전쟁 교리에 사이버 작전 개념이 도입됨에 따라 전투기도 사이버 공격으로부터 안전할 수 없게 되었다. 특히 최신 전투기로 발전할수록 증가하는 소프트웨어의 의존도와, 전투기 자체가 하나의 노드로써 전장지휘체계와 연동되어 운용되는 네트워크 중심전(NCW: Network Centric Warfare)으로 작전 수행 개념의 변화, 지속적으로 증가하는 무기체계에 대한 사이버 위협은 전투기 소프트웨어에 대한 강화된 보안 대책을 요구하고 있다[2].

감항인증이란 항공기가 설계 단계부터 도태 시까지 전 수명주기 동안 비행 안전성이 있다는 것을 정부에서 인증해 주는 제도이다. 1944년에 최초로 항공기 감항인증에 관한 국제표준인 시카고 조약이 마련된 이래로 항공기에서 소프트웨어

† 준 회 원 : 국방대학교 컴퓨터공학전공 석사
†† 종신회원 : 국방대학교 컴퓨터공학전공/사이버전과정 부교수
Manuscript Received : November 13, 2018
Accepted : December 12, 2018
* Corresponding Author : Dongsu Kang(greatkoko@kndu.ac.kr)

가 차지하는 비중이 점차 증가함에 따라 소프트웨어가 항공기 안전에 미치는 영향에 대한 감항인증 표준인 DO-178이 1980년에 발표되었다. 그리고 항공기 소프트웨어 보안에 대한 인식이 점차 확산됨에 따라 사이버 위협으로부터 항공기 소프트웨어의 안전을 보증하기 위한 지침인 DO-326A가 2014년에 발표되었다. 방사청에서는 소프트웨어가 군용 항공기의 안전에 미치는 영향을 보증하기 위하여 「군용항공기 비행안전성 인증에 관한 업무규정」과 DO-178을 적용하고 있으나 항공기 소프트웨어의 보안과 관련된 표준은 적용하고 있지 않다. 미국 CMU 소프트웨어 공학 연구소의 보고서에 따르면 소프트웨어 보안 취약점의 70%가 설계과정의 오류로부터 발생하며 미국 Microsoft 社는 개발단계에서 SDL (Security Development Lifecycle) 적용 시 보안 취약성이 50% 이상 감소한다고 보고하였다[3]. 따라서 앞으로 개발되는 차세대 전투기 사업에서는 전투기 운용 및 소프트웨어 결함에 대한 감항인증 뿐만 아니라, 전투기 소프트웨어의 사이버 위협 방지 대책에 대한 감항인증도 함께 고려되어야 한다. 전투기의 운용환경 및 특성이 고려된 감항 보안 인증이 적용된다면 한국에서 개발되고 있는 차세대 전투기 사업에서 보안성이 보다 강화된 전투기 개발에 기여할 수 있을 것이다.

본 논문에서는 전투기 감항 보안 인증을 위하여 DO-326A에서 제시하고 있는 감항 보안 인증 프로세스의 보안위험 평가 단계에서 전투기의 특성이 고려된 보안위협을 도출하고 이를 바탕으로 위험기반 보안위협 평가 프로세스를 설계하고자 한다. 이를 위하여 2장에서는 관련연구로 항공소프트웨어 감항 보안 인증 표준 및 보안위협 도출 기법, 그리고 보안위험 평가와 관련된 표준을 소개하고 3장에서는 보안위협 도출 및 평가 프로세스에 대한 설계 방법을 제시한다. 4장에서는 전투기 소프트웨어에 적용한 사례를 제시하고 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

2.1 감항 보안 인증 표준

소프트웨어가 항공기 시스템에 처음 사용되기 시작한 이래로 소프트웨어가 항공기 안전에 미치는 영향에 대한 중요성은 비교적 오래전부터 인식되어 1980년 처음으로 항공기 시스템과 장비 인증에 관한 소프트웨어 고려사항인 DO-178이 발표되었다. 그러나 항공소프트웨어 보안과 관련된 인증기준인 DO-326A, DO-355, DO-356은 비교적 늦은 시기인 2014년에 발표되었다. DO-326A(Airworthiness Security Process Specification)는 의도적인 비인가 전자적 상호작용의 위협으로부터 항공기 소프트웨어의 안전을 보증하기 위한 지침이고, DO-355(Information Security Guidance for Continuing Airworthiness)는 항공소프트웨어의 지속적인 감항성을 유지하기 위한 작동 및 유지 보수에 대한 지침이며, 마지막으로 DO-356(Airworthiness Security Methods and Consideration)은 항공기 개발 수명주기 동안 감항성을 확보하기 위한 방법과 고려사항을 제공한다[4].

DO-326A에서는 사이버 공격으로부터 항공기의 안전을 보증하기 위하여 인증 및 보안위험 평가, 보안개발 활동의 세 가지 영역으로 구성된 총 7단계의 보안 프로세스를 제공한다. 첫 번째는 보안 인증 계획(Plan for Security Aspects of Certification) 단계로 인증 신청자가 계획하고 인증기관에서 동의함으로써 달성된다. 두 번째는 보안영역 정의(Security Scope Definition) 단계로 보안위험 평가에 앞서 항공기의 내·외적 자산의 보안영역을 정의하며, 세 번째는 보안위험 평가(Security Risk Assessment) 단계로 보안위험이 항공기에 미치는 영향의 심각성과 공격 성공 가능성을 식별 및 평가한다. 네 번째 단계에서는 감항 보안 수락 매트릭스(Airworthiness Security Acceptability Matrix)를 적용하여 보안위험의 수용 가능 여부를 판단하고 보안대책이 필요한 경우 다섯 번째인 보안개발(Security Development) 단계로 넘어간다. 보안개발은 보안위험을 포함하는 시나리오에 대응하는 보안대책인 보안 아키텍처를 설계하는 과정이다. 여섯 번째는 보안효율 인증(Security Affectiveness Assurance) 단계로 다섯 번째 단계인 보안개발의 결과 만들어진 보안대책으로 보안위협이 수용 가능함을 인증하기 위해 수행되어 진다. 마지막 단계는 이 모든 과정을 보안 활동 결과 보고서(PSecAC Summary)로 작성하는 것이다[5].

특히 항공기 감항 보안 인증 프로세스의 네 번째 단계에서는 감항 보안 수락 매트릭스(Airworthiness Security Acceptability Matrix)를 적용하여 항공기가 보안위험을 수용할 수 있는지 여부를 결정한다. 이는 위협 시나리오에서 사이버 위협이 항공기에 미치는 영향력의 정도와 공격 성공 가능성의 조합에 따라 보안위험의 수용 가능 여부를 판단하게 하는 도구이다. 감항 보안 수락 매트릭스에서는 사이버 위협이 항공기에 미치는 영향력의 정도를 Catastrophic, Hazardous, Major, Minor, No Effect의 다섯 단계로 구분하였으며, 사이버 공격의 성공 가능성에 따라서 Frequent, Probable, Remote, Extremely Remote, Extremely Improbable 의 다섯 단계로 구분한다. Table 1은 감항 보안 수락 매트릭스를 나타낸 것이다[6].

Table 1. Airworthiness Security Acceptability Matrix

Risk Level		Threat Scenario Impact				
Threat Scenario Likelihood		V	Ⅵ	Ⅲ	Ⅱ	Ⅰ
		No Effect	Minor	Major	Hazard-dous	Catast-rophic
pV	Frequent	A	U	U	U	U
pⅥ	Probable	A	A	U	U	U
pⅢ	Remote	A	A	A	U	U
pⅡ	Extremely Remote	A	A	A	A	U
pⅠ	Extremely Improbable	A	A	A	A	A

A: Acceptable / U: Unacceptable

2.2 보안위협 도출 기법

본 논문에서는 전투기 감항 보안 인증을 위한 보안위협 평가 프로세스 설계 시 첫 번째 단계로 전투기에서 발생 가능한 보안위협을 도출한다. 이와 관련해서 DO-356의 시나리오 기법

과 Microsoft 社의 소프트웨어 보안 개발 방법론으로 대표되는 보안위협 모델링 기법, 그리고 보안 요구사항을 도출하기 위한 Misuse Case 기법과 CC Toolbox/PKB 및 OCTAVE의 보안 위협 도출 기법에 대해 확인한다.

1) DO-356의 시나리오 기법

항공기 감항 보안 인증 표준에 하나인 DO-356[6]에서는 다양한 위협 시나리오의 생성을 통해 항공기에 미치는 위협 상태 및 영향력을 정의함으로써 항공기의 보안위험을 평가한다. 위협 시나리오는 공격자의 특성 및 보안 취약점, 사이버 공격을 방어하기 위해 설치된 장치 및 보안조치, 그리고 취약자산 및 목표자산 등으로 구성된다. 위협 시나리오를 통해 위협원이 시스템의 취약점을 이용하여 보안조치를 뚫고 취약자산을 통해 목표자산까지 침투하는 과정을 나타낼 수 있으며 사이버 공격이 침투 할 수 있는 정도에 따라 공격 발생 가능성의 등급이 결정되고 항공기에 미치는 영향력의 정도에 따라 보안위험의 수락 가능 여부가 최종 결정된다.

2) 보안위협 모델링

1990년대부터 연구되기 시작한 보안위협 모델링은 1999년 Microsoft社에서 보안위협 모델링 방법으로 Loren Kohnfelder와 Praerit Garg의 STRIDE 방법론을 자체적으로 사용하면서 크게 발전하였다. 위협 모델링이란 소프트웨어에 발생 가능한 보안문제를 발견하기 위해 모델을 이용하는 것을 말한다. 이는 소프트웨어 개발 주기의 초기 단계에서 소프트웨어에 악영향을 미칠 가능성이 있는 위협을 예측하는 수단으로 활용되며 보안위협 모델링을 통한 보안 요구사항의 도출로 보안이 보다 강화된 소프트웨어를 개발 가능하게 한다[7]. 위협 모델링의 핵심이라 할 수 있는 위협을 찾는 방법으로는 위장(Spoofing), 변조(Tampering), 부인(Repudiation), 정보 노출(Information Disclosure), 서비스 거부(Denial of Service), 권한 상승(Elevation of Privilege)의 앞 글자를 딴 STRIDE 기법이 사용된다[8]. STRIDE 기법을 통해 소프트웨어에서 발생 가능한 위협을 발견하고 이를 완화함으로써 보안이 강화된 소프트웨어를 개발하는 것이 위협 모델링의 궁극적인 목적이라 할 수 있다. 위협 모델링은 데이터 흐름도(DFD: Data Flow Diagram)를 통해 애플리케이션을 분석하고 STRIDE와 위협 트리의 작성을 통해 시스템에 대한 위협을 결정하며 DREAD (Damage potential, Reproducibility, Exploitability, Affected users, Discoverability)기법을 이용하여 위험도를 계산하고 위협 우선순위를 결정한다[7].

3) Misuse Case 모델

소프트웨어공학 분야에서는 소프트웨어에 대한 분석 및 명세를 위한 다양한 연구가 진행되어 왔으며 대표적으로 UML[9]을 활용한 Use Case 모델은 요구사항을 분석하는 강력한 도구로써 소프트웨어의 개발 과정에서 널리 활용되고 있다. Use Case 모델은 시스템이 제공하고 있는 기능 및 그와 관련된 외부요소를 사용자의 관점에서 표현하는 다이어그램을 통해 사용자의 기능적 요구사항을 직관적으로 표현하고 시스템이 제공하는 기본적인 기능을 설명한다. 그러나 Use Case 모델을 통해 시스템의 기능 요구사항을 분석하기는 용이하지만 보안과 관련된 비기능 요구사항을 분석하기에는 한계가 있으며, 이를 해결하기 위하여 Use Case 모델을 확장한 Misuse Case 모델에 대한 연구가 활발히 이루어지고 있다. Misuse Case 모델은 시스템에 악영향을 미치는 보안위협을 식별하고 이를 통해 보안 요구사항을 도출하는 보안 요구사항 명세 모델이다. 보안 요구사항은 시스템에 대한 위협을 예방 및 완화시키기 위한 목적으로 도출되기 때문에 보안위협을 식별하는 과정이 선행되어야 한다.

Misuse Case란 용어는 1990년대의 노르웨이 과학 기술 대학의 Guttorm Sindre와 노르웨이 베르겐 대학교의 Andreas L. Opdahl에 의하여 처음 사용되었다. Use Case가 소프트웨어의 기능 및 정상적인 동작을 나타낸다면 Misuse Case는 시스템에 악영향을 미치는 위협으로 시스템에서 허용해서는 안 되는 기능을 나타낸다. Sindre & Opdahl의 Misuse Case 모델[10]은 Use Case 모델을 확장하여 Misuse Case와 Misuser라는 중요 엔티티를 추가한다.

- Misuse Case : 시스템에 해를 끼치기 위해 어떤 사람이나 객체가 수행할 수 있는 일련의 동작
- Misuser : 의도적이거나 비의도적인 부주의로 인하여 Misuse Case를 수행하는 주체

또한 Misuse Case 모델은 Use Case 모델에서 사용하는 포함, 확장, 일반화 및 연관 등의 관계 유형을 그대로 사용하면서 다음의 두 가지 관계 유형을 추가하였다[10].

- Prevents : 해당 기능이 Misuse Case의 활성화를 방지함
- Detects : 해당 보안기능이 Misuse Case의 활성화를 탐지함

Sindre와 Opdahl이 제안하는 Misuse Case를 사용하여 보안 요구사항을 식별하기 위한 과정은 먼저 시스템의 중요 자산을 식별하여 각 자산에 대한 보안목표를 정의하고 시스템에 해를 가할 수 있는 이해 관계자를 식별하여 각 보안 목표에 대한 위협을 식별하고 분석한다. 그리고 마지막으로 각 위협에 대한 보안 요구사항을 정의하게 된다[11].

4) CC Tool Box와 PKB

공통평가기준(CC)[12]은 사람 또는 사물에 의해서 의도적이거나 비의도적으로 발생하는 보안위험에 대하여 IT 제품의 기능 및 평가과정에 적용되는 보증수단에 대한 공통 요구사항들을 제시하기 위해 합의된 국제표준이다. CC를 IT 제품에 적용하기 위해서는 평가대상물(TOE: Target of Evaluation)의 제품 유형에 따라 CC 보안기능요구사항을 선택하고 EAL 등급에 따라 보호프로파일(PP: Protection profile) 또는 보안목표명세서(ST: Security Target)를 구성해야 한다. PP는 IT 제품이 가져야 할 공통의 보안 요구사항을 모아 놓은 것으로 동일

유형의 시스템에 적용 가능한 일반적인 기능이나 보증사항을 정의한다. PP의 구성요소에는 보안환경(가정사항, 보안위협, 보안정책), 보안목적, 보안요구사항(보안기능요구사항, 보안보증요구사항) 등이 있다. ST는 특정 제품이나 시스템의 요구사항을 구현할 수 있는 보안기능 및 보증수단을 정의한다.

미국정부의 NIST에서는 CC의 보호프로파일(PP)과 보안목표명세서(ST)의 작성을 지원하는 도구로서 CC Tool Box와 이를 위해 '미리 정의된' 위험, 공격, 보안목적, 가정사항 및 정책 문장 데이터베이스인 Profiling Knowledge Base(PKB)를 개발 및 공개하고 있다. CC Tool Box를 위한 PKB 내의 미리 정의된 위협문장은 위협원 - 방법-결과의 조합으로 기술된다. Table 2는 CC ToolBox내 PKB의 위협문장 구조를 나타낸다[13].

Table 2. Threat Sentence Structure of CC ToolBox/PKB

Aspect 1	Aspect 2	Aspect 3
Threat agent	Type	· Human · Non-human
	Certification	· Privileged · Authenticated
	Attitude	· Accidential · Intentional
	Motivation	· Constructive · Malicious · negligence
	Elaboration	· Low · Med · High
	Locality	· Remote · Local
	Power	· Full strength · Unusual condition
Method	Life cycle	· Operation · Development
	Human role	· System obligations · Service user
	Behavior	· Modifying or destroying data/code · Error · ---
	Vulnerability	· Inappropriate authentication mechanism & Inappropriate authentication mechanism · ---
Result	Type of loss	· Integrity · Availability · Confidentiality
	IT ability	· User data · System
	Location	-
	Security function	-

5) OCTAVE

OCTAVE 보안위험 평가기준[14]은 위험분석 시 조직의 운영 요구사항과 IT 요구사항간의 갭을 최소화하기 위해 1999년에 미국의 카네기 멜론 대학 SEI(Software Engineering Institute)의 NSS(The Network System Survivability)에서 위험분석을 위한 프로그램의 일환으로 정보보호 위험평가를 기술하기 위해 개발하였다. OCTAVE의 전체 단계 중 1단계인 '자산기반 위협 프로파일 생성' 단계는 위협문장을 도출하는데 응용될 수 있다.

OCTAVE에서는 자산에 대한 위협 및 취약성을 위협형태/행위자/동기로 인한 결과로 구분하여 보안위험을 평가하고 있다. 또한 각각의 속성의 조합으로 생성 가능한 경로의 집합인 위협트리를 작성하여 위협문장을 도출한다. Table 3과 Fig. 1은 OCTAVE의 위협문장 구조와 위협트리의 형태를 보여준다[13].

Table 3. Threat Sentence Structure of OCTAVE

Asset	Threat Type	Actor	Motivation	Result	Impact
· Server · Networking Component · Security Component · Desktop Workstation · Assumption Computer · Laptop · Storage · Wireless Component · etc.	· Network · Phisical	· Inside · Outside	· Intentional · accidental	· Exposure · Revise · Loss/Destruction · Interruption	· Low · Medium · High
	· System Problem	· SW Failure · Virus · System Destruction · Communication Trouble or Instability	N/A		
	· Other Problem	· Power Supply · Manpower Shortage for Maintenance · Unmatched User Needs · Natural Disaster · Composition of Equipment · Control Lack of HW/SW	N/A		

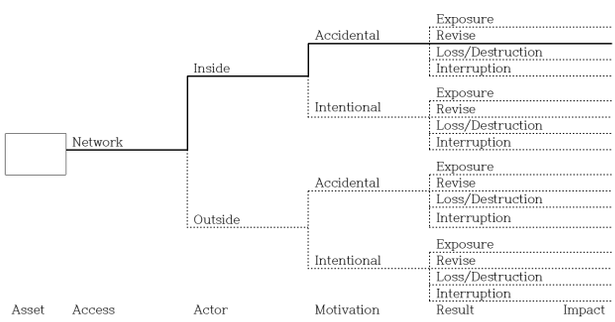

Fig. 1. Example of Threat Tree

6) 보안위협 도출 기법의 비교

보안위협 도출 기법으로 앞서 설명된 시나리오 기법, 보안위협 모델링, Misuse Case 모델, CC Tool Box/PKB, OCTAVE의 특성을 비교하면 Table 4와 같다. 각각의 기법은 공통적으로 위협원 및 취약점(공격방법)을 위협분석 요소로 포함하고 있으며, 위협 모델링 기법과 OCTAVE에서는 도출한 위협목록을 위협트리로 작성함으로써 가시성을 향상시키고 체계적인 위협분석을 용이하게 하였다. 본 논문에서는 위협분석 요소로 위의 기법들이 포함하고 있는 위협원과 취약점(공격방법) 요소와 함께 ISO/IEC 27005(정보보호 위험관리 표준)에서 제시하고 있는 자산 및 공격 결과 요소를 포함하여 전투기의 특성을 반영하고자 한다. 또한 위협트리 작성을 통해 전투기에서 발생 가능한 다양한 위협들을 도출하여 목록화 한다.

2.3 보안위험 평가 표준

보안성 평가와 관련된 국제표준은 정보보호 경영시스템의 수립, 구현, 유지 및 개선에 필요한 요구사항을 제공하기 위하여 개발된 ISO/IEC 27001과 정보보호 위험관리를 위한 지

Table 4. Comparison of Security Threat Derivation Methods

Division	Threat Analysis Element	Automation Tools	Create a threat tree	Advantages	Disadvantages
Scenario	· Threat agent · Vulnerability · Assets	X	X	Detailed and accurate threat analysis is possible	There is a limit to the derivation of various threats list
Threat Modeling	· DFD · STRIDE	O	O	Various threat lists can be derived by automated tools	It is tool dependent and there is a limit to the detailed analysis of the threat.
Misuse Case	· Misuser · Misuse Case	X	X	As the corresponding concept of Use Case easy to draw Misuse Case. And user misuse including cyber attacks, threats due to system / SW malfunctions are possible to derivate	It is difficult to analyze the limitations, vulnerabilities, and impacts on the assets of various threat lists
CC ToolBox/ PKB	· Threat agent · Attack method · Result	O	X	Predefined threat statements are applicable	There is a limit to the derivation of a threat sentence that matches the characteristics of a fighter
OCTAVE	· Assets · Approach type · Agent · Motivation · Result · Effect	O	O	Threat analysis and threat tree creation from various perspectives enables systematic threat management	There is a limit to the detailed analysis of the threat situation

침을 제공하는 ISO/IEC 27005, 조직의 모든 분야 및 범위에서 위험관리 지침을 제공하는 ISO/IEC 31000 등이 있다.

ISO/IEC 27001 정보기술-보안기술-정보보호 경영시스템-요구사항(Information technology - Security techniques - Information security management systems-Requirements)에 의해 수립, 구현 및 유지, 관리가 되는 정보보호 경영시스템은 위험관리 프로세스의 적용을 통해 정보의 기밀성, 무결성, 가용성을 보존하고 이해당사자에게 위험이 적절하게 관리된다는 믿음을 제공한다. 이 표준은 조직의 상황에 맞게 정보보호 경영시스템의 수립, 구현, 유지, 개선을 위한 요구사항 및 정보보호 위험의 평가와 처리에 대한 요구사항을 명시하고 있다.

ISO/IEC 27001의 정보보호 위험평가 프로세스에서는 조직의 정보보호를 위한 위험기준을 수립하는 단계를 시작으로 정보보호 경영시스템의 기밀성, 가용성, 무결성의 손실을 유발하는 위험 및 위협원을 식별한다. 다음으로 식별된 위험이 실제 발현됨으로써 나타나는 결과에 대한 잠재적 영향력 및 가능성을 평가하는 정보보호 위험분석 단계를 거쳐 초기 단계에서 수립된 위험기준과 위험분석 결과를 비교하여 위험처리를 위한 위험우선순위를 결정하게 된다[15].

ISO/IEC 27005 정보기술 - 보안기술 - 정보보호 위험관리(Information technology - Security techniques - Information security risk management)는 조직의 정보보호 위험관리를 위한 일반적인 지침을 제공한다. ISO/IEC 27005에서는 ISO 31000에서 제공하고 있는 위험 관리 프로세스를 바탕으로 정보보호 위험 관리 프로세스를 제시한다.

Fig. 2는 ISO/IEC 27005에서 제시하고 있는 정보보호 위험 관리 프로세스이다. 먼저 정보보호 위험 관리에 필요한 기본 기준을 수립하고 범위와 경계를 정의하는 상황 설정 단계 이후에 위험을 식별하고 분석하며 이렇게 수행된 위험 자산 평가 결과를 바탕으로 위험수준을 평가한다. 위험수준 평가 결과가 이후의 단계를 수행하기 위한 충분한 정보를 제공한다면 위험처리가 뒤이어 수행된다. 위험처리 단계에서는 잔여 위험의 수준이 수용 가능한 수준인지에 대한 결정을 내리며 수용 가능하다면 조직이 위험을 수용하는 활동을 하도록 명시적으로 나타내며 수용 불가하다면 위의 과정을 다시 반복한다[16].

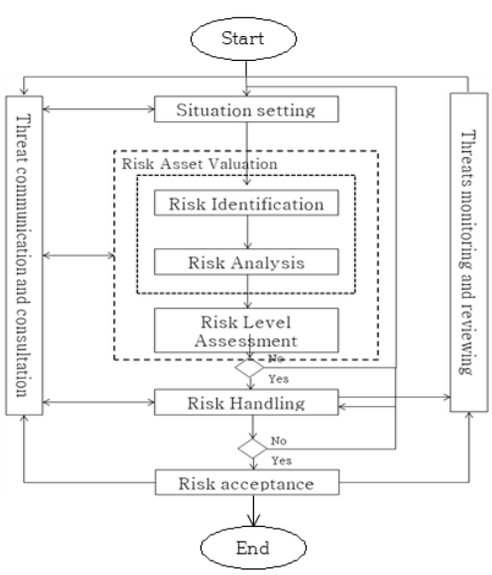

Fig. 2. Information Security Risk Management Process

위험식별의 목적은 어떤 자산에 대한 잠재적 손실 가능성이 있는지 결정하고 그 손실을 일으킬 수 있는 방법 및 이유를 찾기 위함이다. 이를 위하여 자산 식별, 위협 식별, 기존 통제의 식별, 취약성 식별, 결과 식별 등의 세부 활동 내용이 포함된다. 위험분석은 자산의 중대성, 취약성의 범위, 조직에 관련된 통제 문서에 따라 다양한 정도로 수행되어 질 수 있다. 식별된 위협, 취약성, 자산 및 자산에 미치는 결과를 포함하는 시나리오를 기본으로 정성적/정량적 위험분석 방법을 모두 사용할 수 있으며 자산의 기밀성, 무결성, 가용성의 손실을 고려하여 조직에 미치는 영향력을 산정한다.

또한 시나리오를 통해 사이버 공격이 얼마나 자주 발행하고 취약성이 얼마나 쉽게 이용될 수 있는지를 고려하여 발생 가능성에 대한 평가를 수행한다. 위험수준 평가는 위험분석을 통해 도출된 위험의 발생 가능성과 영향력의 결과 값의 조합으로 조직의 이해관계와 환경을 고려하여 위험 우선순위 목록을 작성하는 것이다. 이처럼 정보보호 위험관리의 핵심은 위험을 식별하고 분석하여 정해진 위험 우선순위를 통해 조직에서 수용 가능한 위험으로 처리하는 과정이라 볼 수 있다[16].

본 논문에서는 ISO/IEC 27005에서 위협과 취약점을 식별하고, 자산 및 자산에 미치는 결과를 고려하여 보안위험이 발생할 가능성과 시스템에 미치는 영향력의 관점에서 보안위험을 분석한 것을 적용하여 위험기반의 보안위협 도출 프로세스를 제시한다.

3. 전투기 보안위험 평가 프로세스

2장에서 언급된 DO-326A에서는 항공기 감항 보안 인증 프로세스를 7단계로 제안하고 있다. 그러나 본 연구에서는 보안위협을 구체화하고 보안위협이 전투기 소프트웨어 안전에 미치는 영향을 명확히 반영하기 위해 DO-326A의 세 번째 단계인 보안위험 평가 단계에 세 가지 단계를 추가하여 제시한다. 첫 번째는 보안위협 도출 단계로 위협문장 생성 규칙과 위협트리의 작성을 통해 전투기에서 발생 가능한 보안위협을 위협문장의 형태로 도출한다. 두 번째는 보안위험 평가를 위한 문장 구성 요소 점수화 단계로 앞에서 생성한 보안위협 문장의 각 요소들을 사이버 공격의 발생 가능성과 전투기에 미치는 영향력의 관점에서 분석하여 점수화 한다. 세 번째는 위험 심각도 결정 단계로 점수화한 공격 발생 가능성 및 항공기에 미치는 영향력 평가 요소를 다섯 등급으로 분류하여 전투기 보안위험 심각도를 종합적으로 판단할 수 있는 표를 작성한다. 그리고 다시 DO-326A의 네 번째 단계로 돌아가서 작성된 전투기 보안위험 심각도 표를 바탕으로 보안위험의 수락 가능여부를 최종 결정하게 된다. Fig. 3은 위에서 설명한 프로세스를 도식화한 그림이다.

DO-326A에서는 감항 보안 인증 프로세스의 첫 번째 단계로 보안인증을 위한 계획을 세우고 결과물로 PSecAC (Plan for Security Aspects of Certification)를 작성한다. 이를 바탕으로 두 번째 단계에서는 보안영역을 정의하는데 이 단계에서는 Aircraft Level에서부터 System Level까지 항공기 자산, 보안영역, 보안환경을 정의하며 결과물로 ASSD(Aircraft Security Scope Definition)와 SSSD(System Security Scope Definition)를 작성한다. 다음으로 보안위험 평가 단계에서는 System Level을 시작으로 Aircraft Level까지 앞서 제시한 보안위협 도출 및 보안위험 요소 점수화, 위험 심각도 결정의 세 가지 활동을 수행한다. 이 활동의 결과물로는 ASRA (Aircraft Security Risk Assessment)와 SSRA(System Security Risk Assessment), 그리고 보안위험 심각도 결정표가 작성되며 DO-326A의 네 번째 단계에서 이를 바탕으로 보안위험 수락 여부를 결정하게 된다.

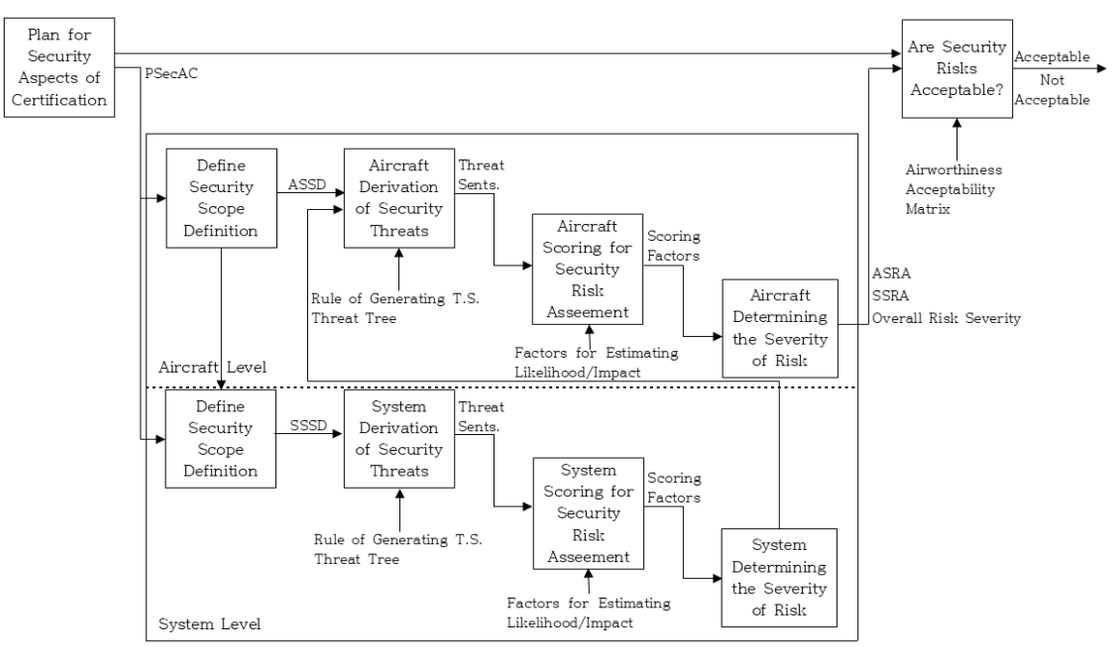

Fig. 3. Airworthiness Security Certification Process based on Risk

3.1 보안위협 도출

본 논문에서는 전투기의 보안위협을 도출하기 위하여 위협원, 공격방법, 자산, 결과의 4가지 요소를 포함하여 위협 문장을 도출한다. 이는 관련연구에서 설명된 보안위협 도출 기법에서 공통으로 포함하고 있는 위협분석 요소와 ISO/IEC 27005의 위협분석 프로세스를 반영하여 전투기의 보안위협을 도출하기 위함이다. Fig. 4는 보안위협 문장 생성 규칙을 도식화한 것이다. 각각의 항목(주어, 동사, 목적어, 결과)은 보안위험을 평가하기 위한 요소들로 구성되어 있으며 주어, 동사, 목적어 요소들을 조합한 위협트리의 작성으로 보안위협 문장을 도출할 수 있다[17]. 위협트리의 작성을 통해서 전투기에서 발생 가능한 위협목록을 가시화할 수 있을 뿐만 아니라 다양한 위협들을 체계적으로 관리할 수 있다. Fig. 5는 위협문장 생성 규칙에 의해 작성된 위협트리이다. 위협트리에 의해서 “외부 공격자가 삽입공격을 통해 항공기체계의 가용성을 손상시킨다”라는 위협문장이 생성됨을 알 수 있다.

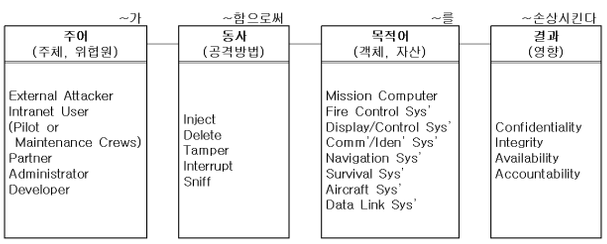

Fig. 4. Rule of Generating Security Threat Sentence

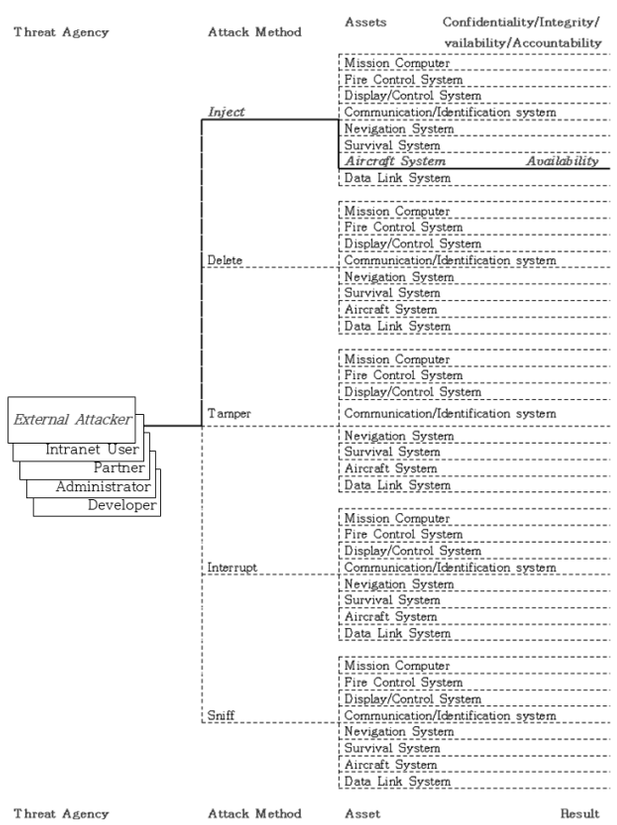

Fig. 5. Generating of Threat Tree

3.2 보안 위험 평가를 위한 요소

보안위험 평가를 위한 요소를 도출하기 위하여 사이버 공격의 발생 가능성과 항공기 및 임무에 미치는 영향력의 관계를 고려하였으며 공격 발생 가능성에는 위협원과 취약점요소가 영향력에는 자산과 공격결과에 관련된 요소가 각각 포함되어 있다. 이는 ISO/IEC 27005의 정보보호 위험 관리 프로세스에서 위험분석 부분[16]을 적용한 것이다.

$$Risk = Likelihood * Impact$$

1) 공격 발생 가능성 평가 요소

공격 발생 가능성 평가 요소는 위험원의 기술수준, 동기, 규모, 공격 기회와 수행하는 공격방법의 보안 취약점 발견 용이성, 공격 수행 용이성, 보안 취약점 인식수준, 탐지 가능성 등으로 구성되어 있으며 0점에서 10점까지 점수화 된다.

a) 위협원 평가

위협원을 평가하기 위한 첫 번째 요소는 위협원의 기술수준에 따라 기술이 매우 낮은 수준부터 약간의 기술을 갖고 있는 수준, 그리고 일정 수준 이상의 컴퓨터 사용자와 네트워크나 소프트웨어를 프로그래밍 할 수 있는 수준, 마지막으로 보안 장비를 뚫고 목표 자산에 침투할 수 있는 수준 등의 다섯 단계로 구분하여 차등적으로 점수를 주었다[18]. 두 번째는 위협원이 사이버 공격을 감행함으로써 얻을 수 있는 보상과 관련된 요소로써 보상 수준이 낮거나 없는 경우, 어느 정도 보상이 예측되는 경우, 보상 수준이 높은 경우의 세 단계로 구분하여 점수화 하였다. 세 번째 요소는 위협원의 규모, 즉 위협원의 수에 따라 숫자가 많은 불특정 외부 공격자나 관련업체 등에게는 높은 점수를 부여하였고 개발자, 시스템 관리자 등에게는 낮은 점수를 부여하였다. 마지막으로 공격을 할 수 있는 기회와 관련하여 공격을 하기 위한 엑세스 권한이나 자원의 필요 정도에 따라 네 등급으로 점수를 차등 부여하였다. 이상의 내용을 정리하면 아래 Table 5와 같다.

Table 5. Threat Agent Factors

Threat Agent Factors	1. Skill level : How technically skilled is this group of threat agents?				
	No technical skills	Some technical skill	Advanced computer user	Network & programming skills	Security Penetration skills
	0 ~ 1	~ 3	~ 5	~ 7	~ 10
	2. Motive : How motivated is this group of threat agents to find and exploit this vulnerability?				
	Low or no reward		Possible reward		High reward
	0 ~ 2		~ 5		~ 10
	3. Size : How large is this group of threat agents?				
	Developers	System administrators	Intranet users(Pilots/ Maintenance crews)	Partners	External attackers
	0 ~ 2	0 ~ 2	~ 4	~ 6	~ 10
	4. Opportunity : What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability?				
	Full access or expensive resources	Special access or resources	Some access or resources	No access or resources	
	0	~ 4	~ 7	~ 10	

b) 공격방법 평가

공격방법의 평가는 취약점과 관련된 요소로서 위협원이 공격에 이용할 취약점을 얼마나 쉽게 발견할 수 있는지에 따라 네 등급으로 점수를 차등 부여하였고 위협원이 취약점을 이용하여 실제로 얼마나 쉽게 공격을 수행할 수 있는지 여부에 따라서도 네 등급으로 점수를 부여하였다. 또한 이 취약점이 얼마나 널리 알려졌는지 여부와 공격 수행 이후 탐지 여부에 따라서도 네 등급으로 점수를 차등 부여하였다[18]. 아래의 Table 6은 이상의 내용을 정리한 표이다.

Table 6. Attack Method Factors

Attack Method Factors	1. Ease of discovery : How easy is this group of threat agents to discover this vulnerability?			
	Practically impossible	Difficult	Easy	Automated tools available
	0 ~ 1	~ 3	~ 7	~ 10
	2. Ease of exploit : How easy is this group of threat agents to actually exploit this vulnerability?			
	Theoretical	Difficult	Easy	Automated tools available
	0 ~ 1	~ 3	~ 7	~ 10
	3. Awareness : How well known is this vulnerability to this group of threat agents?			
	Unkown	Hidden	Obvious	Public knowledge
	0 ~ 1	~ 4	~ 6	~ 10
	4. Intrusion detection : How likely is an exploit to be detected?			
	Active detection in application	Logged and reviewed	Logged without reviewed	Not logged
	0 ~ 1	~ 3	~ 8	~ 10

2) 영향력 평가 요소

영향력 평가 요소는 전투기를 구성하고 있는 임무컴퓨터, 사격통제계통, 시현 및 제어계통, 통신 및 식별계통, 항법계통, 생존계통, 항공기체계 데이터링크체계 등에 미치는 기밀성, 무결성, 가용성, 책임성의 침해 정도에 따라 0점에서 10점까지 점수화 된다.

a) 항공기 및 임무에 미치는 영향력 평가

전투기에 미치는 영향력 평가에 있어서 전투기가 민항기와 구분되는 가장 큰 특징은 사이버 공격이 항공기 기체에 미치는 영향뿐만 아니라 전투 임무의 성패에 미치는 영향도 함께 고려되어야 한다는 것이다. 사이버 공격이 전투기에 미치는 영향력을 평가하기 위해서는 각 계통이 비행 안전에 미치는 영향력의 정도와 임무 성패에 미치는 영향력의 정도를 함께 고려해야만 한다. 예를 들어 사격 통제 시스템과 데이터 링크 시스템의 경우 비행 안전에 미치는 영향력은 미비하지만 임무에 미치는 영향력은 상대적으로 높은 것을 알 수 있다. 이 밖의 계통들도 항공기 안전 및 임무 성패에 미치는 영향력의 관점에서 각각 점수가 고려되었다. Table 7은 사이버 공격이 전투기의 각 계통에 미치는 영향력을 점수화한 표이다.

Table 7. Aircraft & Mission Impact Factors

Aircraft & Mission Impact Factors	1. Aircraft damage : How about the impact of an attack on aircraft system to flight safety?							
	Fire control sys'	Data link sys'	Survival sys'	Nevigation sys'	Comm'/ Iden' sys'	Display/ control sys'	Mission Computer	Aircraft sys'
	0	0	0	~ 2	~2	~ 4	~ 7	~ 10
	2. Mission fail : How about the impact of an attack on aircraft system to Mission Fail?							
	Nevigation sys'	Comm'/ Iden' sys'	Data link sys'	Survival sys'	Display/ control sys'	Aircraft sys'	Fire control sys'	Mission Computer
	~2	~2	~3	~4	~ 4	~ 6	~ 8	~ 10

b) 기술적 영향력 평가

기술적 영향력은 사이버 공격으로 전투기에서 기밀성, 무결성, 가용성, 책임성이 침해된 정도에 따라 점수가 차등적으로 부여된다. 기밀성은 노출된 데이터의 양과 민감도에 따라서, 무결성은 손상된 데이터의 양과 민감도에 따라서, 가용성은 제공되는 서비스의 중요도와 수행 가능 정도에 따라서, 마지막으로 책임성은 사이버 공격의 추적 가능 여부에 따라서 점수가 부여되며 아래의 Table 8은 기술적 영향력 요소들을 점수화한 표이다[18].

Table 8. Technical Impact Factors

Technical Impact Factors	1. Loss of confidentiality : How much data could be disclosed and how sensitive is it?				
	Minimal non-sensitive data disclosed	Minimal critical data disclosed	Extensive non-sensitive data disclosed	Extensive critical data disclosed	All data disclosed
	0 ~ 2	~ 6	~ 6	~ 8	~ 10
	2. Loss of integrity : How much data could be corrupted and how damaged is it?				
	Minimal slightly corrupt data	Minimal seriously corrupt data	Extensive slightly corrupt data	Extensive seriously corrupt data	All data totally corrupt
	0 ~ 1	~ 3	~ 5	~ 7	~ 10
	3. Loss of availability : How much service could be lost and how vital is it?				
	Minimal secondary services interrupted	Minimal primary services interrupted	Extensive secondary services interrupted	Extensive primary services interrupted	All services completely lost
	0 ~ 1	~ 5	~ 5	~ 7	~ 10
	4. Loss of accountability : Are the threat agents' actions traceable to an individual?				
	Fully traceable		Possibly traceable		Completely anonymous
	0 ~ 1		~ 7		~ 10

3.3 보안위험 심각도 결정

보안위험 심각도 결정 단계에서는 앞에서 도출된 공격 발생 가능성과 전투기에 미치는 영향력 요소 점수들의 평균값을 다섯 등급으로 분류하여 보안위험 심각도 결정표를 작성한다. 공격 발생 가능성의 경우 도출된 총 0에서 10점까지의 점수 범위 중에서 8에서 10점까지는 Frequent, 6에서 8점까지는 Probable, 4에서 6점까지는 Remote, 2에서 4점까지는 Extremely Remote, 0에서 2점까지는 Extremely Improbable로 분류된다. 또한 전투기에 미치는 영향력의 경우 0에서 2점까지는 No Effect, 2에서 4점까지는 Minor, 4에서 6점까지는 Major, 6에서 8점까지는 Hazardous, 8에서 10점까지는 Catastrophic의 다섯 단계로 분류된다.

Frequent는 전투기 각각의 수명주기 동안 빈번하게 발생

가능할 것으로 예상되는 사이버 공격을 의미하며, Probable은 각각의 전투기 수명주기 동안에 1회 또는 그 이상이 발생 가능할 것으로 예상되는 사이버 공격을 의미한다. Remote는 몇몇 기종의 전투기에서 전 수명주기 동안 수차례 발생할 가능성이 예상되는 사이버 공격을 의미하며 Extremely Remote는 전투기의 모든 기종에서 전체 수명주기 동안 1에서 2회 정도 발생 가능한 사이버 공격을 의미한다. 마지막으로 Extremely Improbable은 모든 전투기의 전체 수명주기 동안 발생할 가능성이 예측되지 않는 사이버 공격을 의미한다. 또한 No Effect는 전투기에 영향이 없음을 의미하며 Minor는 전투기 안전에 약간의 영향을 미치는 사이버 공격을 의미한다. Major는 전투기 안전에 심각한 영향을 미치는 사이버 공격을 의미하고 Hazardous는 위험한 영향을, Catastrophic은 전투기 안전에 재난수준의 영향을 미치는 사이버 공격을 의미한다. Table 9는 사이버 공격의 발생 가능성과 전투기에 미치는 영향력 요소를 점수화 하여 평균값을 계산하고 등급을 분류한 예이다. 또한 Table 10은 공격 발생 가능성과 전투기에 미치는 영향력의 정의를 정리한 표이다.

Table 9. Example of Likelihood & Impact Scoring

Threat agency factor					Attack method evaluation factor			
Skill level	Motivation	Size	Attack opportunity		Ease of discovery	Ease of exploit	Awareness level	Detectability
5	2	7	1		3	6	9	2
Likeliness = 4.375(Medium)								

Impact Assessment factor about Aircraft/Mission			Technical Impact Assessment Factor			
Aircraft damage	Mission failure		Confidentiality	Integrity	Availability	Accountability
3	5		9	7	5	8
Impact= 6.167(High)						

Table 10. Likelihood & Impact Definition

Likelihood			Impact		
Level	Term	Definition	Level	Term	Definition
Ⅴ (8~10)	Frequent	Anticipated to occur routinely in the life of each fighter-aircraft	Ⅴ (0-2)	No Effect	Would not affect the operational capability of the fighter-aircraft & Mission, Would not increase crew workload
Ⅵ (6-8)	Probable	Unlikely to occur to each fighter-aircraft during a routine flight but may occur or more times in the life of each fighter-aircraft	Ⅵ (2-4)	Minor	Slight reduction in safety margins or functional capabilities, or Slight increase in crew workload
Ⅲ (4-6)	Remote	Unlikely to occur to each fighter-aircraft during its total life but may occur several times in the total life of a number of fighter-aircraft of the type	Ⅲ (4-6)	Major	Significant reduction in safety margins or functional capabilities, or Significant increase in crew workload
Ⅱ (2-4)	Extremely Remote	Not anticipated to occur to each fighter-aircraft during its total life but which may occur a few times in the total life of all fighter-aircraft of the type	Ⅱ (6-8)	Hazardous	Large reduction in safety margins or functional capabilities, or physical distress or higher workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely
Ⅰ (0-2)	Extremely Improbable	Not anticipated to occur during the entire operational life of all fighter-aircraft of the type	Ⅰ (8-10)	Catastrophic	Occurrence of multiple fatalities, usually with the loss of the fighter-aircraft

Table 9의 사이버 공격 발생 가능성 및 전투기에 미치는 영향력 점수의 예를 적용하여 위험 심각도 결정표를 작성하면 사이버 공격 발생 가능성 점수는 4.375(Ⅲ, Remote)이며 몇몇 기종의 전투기 수명주기 동안 수차례 발생 가능한 위협임을 알 수 있다. 또한 영향력 점수는 6.167(Ⅱ, Hazardous)이며 전투기의 안전 및 임무에 위험한 영향을 미치는 위협임을 알 수 있다. 각각 도출된 점수의 조합으로 Table 11의 보안위험 심각도 결정표에서는 도출된 위협의 수준이 High 임을 알 수 있고 <Table 1> DO-326A의 감항 보안 위험 수락 매트릭스에 적용하면 전투기에서 수용 불가하여 보안위협에 대한 대책이 필요한 위험으로 분류할 수 있다.

Table 11. Determining the Severity of the Risk

Overall Risk Severity						
		Ⅴ No Effect	Ⅳ Minor	Ⅲ Major	Ⅱ Hazar-dous	Ⅰ Catastro-phic
Likeli-hood	Ⅴ Frequent	Medium	High	Very High	Critical	Critical
	Ⅳ Probable	Low	Medium	High	Very High	Critical
	Ⅲ Remote	Very Low	Low	Medium	High	Very High
	Ⅱ Extremely Remote	Note	Very Low	Low	Medium	High
	Ⅰ Extremely Impro-bable	Note	Note	Very Low	Low	Medium
	Impact					

4. 사례 적용

4.1 전투기 특성 및 체계 구성

한국 공군은 전투기를 성능에 따라 High, Middle, Low 급으로 분류하여 도입 및 운용하고 있다. High급 전투기는 유사 시 모든 임무를 수행할 수 있으며 평시에는 보유 자체만으로 전쟁 억제력을 갖는 고성능 전투기이고, Middle급 전투기는 적지 침투 및 고강도 위험지역에서 임무를 수행할 수 있으며 High급 전투기를 보조하는 중간 성능의 전투기이다. 마지막으로 Low급 전투기는 저강도 위험지역에서 운용하며, 근거리 방어제공과 근접항공지원 등의 전술 임무를 수행하는 전투기이다. 현재 공군에서 운용되고 있는 Middle급 전투기인 F-4와 Low급 전투기인 F-5가 노후됨에 따라 이들 전투기를 대체할 국산 전투기 체계를 개발하는 사업인 KFX 사업은 Middle급 성능의 세미 스텔스 성능이 있는 4.5세대 전투기의 개발을 목표로 하고 있다.

KFX 사업의 개발 목표인 Middle급 전투기의 소프트웨어는 전투 임무 수행에 필요한 시스템들의 집합인 항공전투체계, 기체 운용에 필요한 시스템들의 집합인 항공기 체계, 타 전투체계와 연동되어 운용되는 전술데이터 링크 체계로 구성되어 있다. Fig. 6은 전투기 내부 시스템들 간의 데이터 연동과 외부 데이터 연동에 대한 개략적인 구성과 상호 관계를 나타낸다. 임무 컴퓨터를 중심으로 사격통제 계통, 시현 및 제어 계통, 통신·식별 계통, 항법 계통, 생존 계통이 전투기 내부에서 연동되어 있고 엔진, 유압, 전기, 비행제어 등 항공기의 각 계통을 통제하는 항공기 계통과 타 체계와 함께 임무를 수행하는 데이터 링크 계통이 외부적으로 연동되어 있

다[19]. 각 계통들은 사이버 공격에 의해 항공기 손상 및 임무 실패에 영향을 받는 정도가 서로 상이하며 이를 반영하여 영향력 요소에서 점수화 된다.

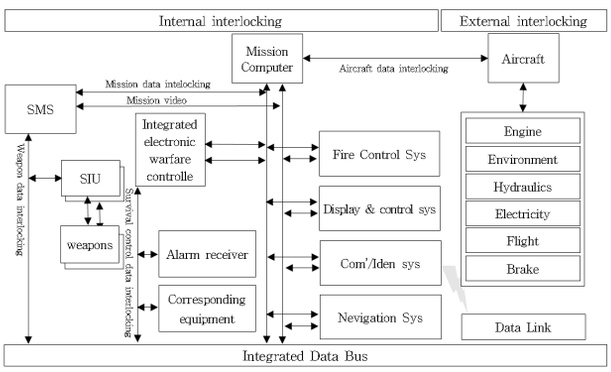

Fig. 6. Data Interlocking System of Fighter-Aircraft

4.2 전투기 보안위험 평가 프로세스

1) 전투기 보안위험 평가를 위한 시나리오

보안위험 평가 프로세스를 전투기에 적용하기 위하여 현재 공군에서 운용되는 항공기인 T-50 계열 및 F-15K 전투기에서 임무 컴퓨터의 운영체제로 사용하고 있으며 차세대 전투기 및 무인기 사업에서 사용 가능한 Vxworks를 대상으로 상황을 설정한다. Vxworks는 RTOS(Real Time Operating System)의 한 종류로 항공기, 철도, 자동차, 의료기기, 제조공장 등에서 사용되는 소프트웨어를 개발하는 Windriver 社에서 개발한 항공기용 실시간 운영체제이다.

Vxworks와 관련된 CVE(Common Vulnerability and Exposures)[20]는 2008년부터 현재까지 총 13개가 보고되었다. Vxworks와 관련된 CVE 중에서 전투기 사례에 적용하기 위하여 2017년에 보고된 오버플로 취약점을 활용한 CVE를 선정하여 시나리오를 작성한다. Vxworks에서 svc_auth.c에 있는 _authenicate 함수의 정수 오버플로는 원격 프로시저 호출 프로토콜을 사용할 때 공격자가 서비스 거부를 일으키거나 사용자 이름과 암호를 통해 임의의 코드를 실행 가능하게 한다. 오버플로 공격의 결과로 모든 시스템 파일 노출이 가능하고 전체 시스템이 손상 될 수 있으며 공격자가 사용자 리소스를 완전히 사용할 수 없게 만들어 기밀성, 무결성, 가용성에 심각한 피해를 초래할 수 있다. 이 공격을 수행하기 위하여 액세스나 인증 권한을 획득할 필요는 없다.

위의 내용을 바탕으로 인트라넷 사용자인 정비사가 삽입공격(오버플로)을 통해 전투기 엔진계통에 무결성, 가용성을 침해하는 상황을 가정할 수 있다. 앞서 언급한 바와 같이 CVE를 활용한 공격이 액세스나 인증 권한을 따로 획득할 필요는 없지만 오버플로 상황에서 서비스 거부 또는 코드실행 공격을 수행하기 위해서는 상당수준의 기술이 필요할 것으로 판단된다. 또한 인트라넷 사용자로서 공격을 수행함으로써 높은 수준의 보상을 기대할 수 있을 것이다. Vxworks 운영체제에 오버플로 공격을 수행하는 것은 CWE와 CVE를 통해 비교적 잘 알려져 있지만 이 공격을 수행하기 위한 자동화된 도구나 키트는 따로 개발되어 있지 않아 공격 수행에 상당한 어려움이 수반된다. 또한 오버플로 공격의 최종 목표인 전투기 엔진 시스템의 무결성과 가용성이 침해된다면 전투기의 안전과 임무 수행에 매우 부정적인 영향을 미칠 수 있다. 이상의 시나리오를 바탕으로 전투기를 대상으로 하여 보안위협을 도출하고 위험 평가 요소를 점수화하며 최종적으로 보안위험 심각도가 결정되는 과정을 설명한다.

2) 전투기 보안위협 도출

전투기 보안위협 도출을 위해서는 먼저 위협문장 생성 규칙에 의해 위협트리를 작성한다. Fig. 7은 “인트라넷 사용자가 삽입공격으로 항공기체계의 무결성 및 가용성을 침해한다”라는 위협문장이 트리에 의하여 생성되는 예를 보여준다.

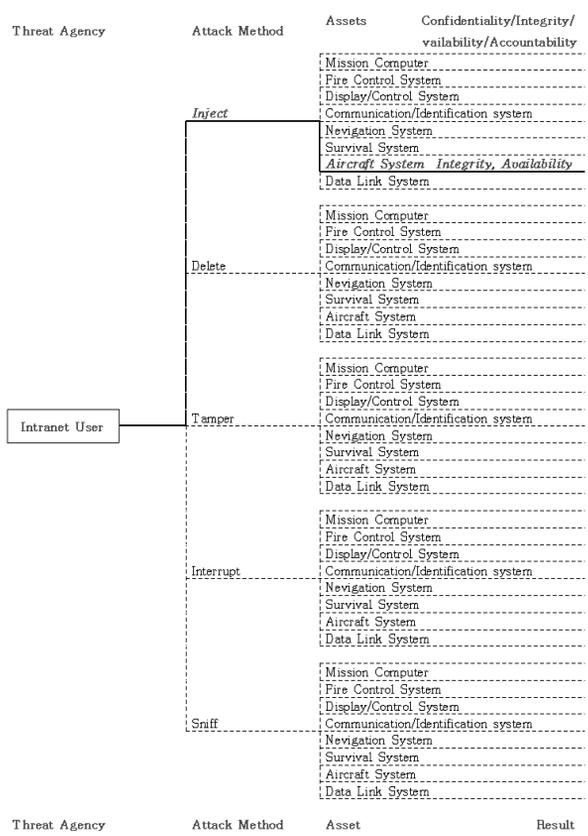

Fig. 7. Example of Threat Tree

3) 보안위험 평가를 위한 요소 점수화

앞서 생성된 보안 위협문장은 공격 발생 가능성 및 전투기에 미치는 영향력 관점에서 점수화 된다. 공격 발생 가능성 요소에는 위협원과 공격방법의 취약점과 관련된 내용이 포함되어 있고 영향력 요소에는 항공기 및 임무, 그리고 기술적 영향과 관련된 내용이 포함되어 있다.

a) 공격 발생 가능성 요소

“인트라넷 사용자가 삽입공격으로 항공기 체계의 무결성 및 가용성을 침해한다”는 위협문장에서 공격 발생 가능성 요소를

점수화하기 위하여 대상 위협원의 기술수준, 동기, 규모, 공격 기회에 대한 분석을 수행하며 이들 점수의 평균값은 6.88이다. 또한 공격방법을 평가하기 위하여 취약점의 발견 용이성, 공격 수행 용이성, 취약점 인식수준, 탐지 가능성에 대한 평균값을 계산하면 4.68이 된다. 따라서 공격 발생 가능성은 위협원과 공격방법 평가에 의해 6.88과 4.68의 평균인 5.78이 도출된다.

Table 12. Likelihood & Impact Definition

Threat Agency	Intranet User		Attack Method	Inject	
Skill level	Ⅵ	7.2	Ease of discovery	Ⅲ	5.6
Motivation	Ⅵ	7.8	Ease of exploit	Ⅱ	2.3
Size	Ⅱ	3.6	Awareness level	Ⅴ	8.1
Attack opportunity	Ⅴ	8.9	Detectability	Ⅱ	2.7
Average	Ⅵ	6.88	**Average**	Ⅲ	4.68
Total Average	Likelihood = 5.78(Ⅲ)				

b) 영향력 평가 요소

영향력 평가 요소를 점수화하기 위하여 사이버 공격이 항공기 손상 및 임무 실패에 미치는 영향력과 기밀성, 무결성, 가용성, 책임성 침해 등의 기술적 영향력을 점수화 하여 평균값을 구하면 최종적으로 7.4가 도출된다.

Table 13. Likelihood & Impact Definition

Aircraft & Mission Impact	Aircraft System		Technical Impact	Integrity / Availability	
Aircraft damage	Ⅰ	8.2	Confidentiality		
			Integrity	Ⅱ	7.3
Mission failure	Ⅲ	5.9	Availability	Ⅱ	8.2
			Accountability		
Average	Ⅱ	7.05	**Average**	Ⅵ	7.75
Total Average	Impact = 7.4(Ⅱ)				

4) 전투기 보안위험 심각도 결정

전투기 보안위험 심각도를 결정하기 위하여 앞서 도출된 공격 발생 가능성 점수와 전투기에 미치는 영향력 점수를 다섯 단계로 분류하여 보안위험 심각도 결정표에 적용한다. 공격 발생 가능성은 레벨 Ⅰ(0<R≦2), 레벨 Ⅱ(2<R≦4), 레벨 Ⅲ(4<R≦6), 레벨 Ⅵ(6<R≦8), 레벨 Ⅴ(8<R≦10)로 분류하며, 영향력은 레벨Ⅴ (0<R≦2), 레벨 Ⅵ(2<R≦4), 레벨 Ⅲ(4<R≦6), 레벨 Ⅱ(6<R≦8), 레벨 Ⅰ(8<R≦10)로 분류한다. Table 13은 앞서 도출한 점수를 보안위험 심각도 결정표에 적용한 것이다. 공격 발생 가능성 및 영향력 점수는 각각 5.78과 7.4로 각각 레벨 Ⅲ와 레벨 Ⅱ이며 보안위험 심각도는 최종적으로 High가 도출된다. 이렇게 도출된 보안 위험 심각도는 DO-326A의 감항 보안 수락 매트릭스에 의해 수락 불가하여 보안 조치가 필요한 위험임을 알 수 있다.

Table 14. Determinig the Severity of the Risk & Apply Airworthiness Security Acceptability Matrix

Overall Risk Severity						
		Ⅴ No Effect	Ⅳ Minor	Ⅲ Major	Ⅱ Hazar-dous	Ⅰ Catastro-phic
Likeli-hood	Ⅴ Frequent	Medium	High	Very High	Critical	Critical
	Ⅳ Probable	Low	Medium	High	Very High	Critical
	Ⅲ Remote	Very Low	Low	Medium	High	Very High
	Ⅱ Extremely Remote	Note	Very Low	Low	Medium	High
	Ⅰ Extremely Impro-bable	Note	Note	Very Low	Low	Medium
	Impact					

⇓

Risk Level		Threat Scenario Impact				
Threat Scenario Likelihood		Ⅴ	Ⅵ	Ⅲ	Ⅱ	Ⅰ
		No Effect	Minor	Major	Hazar-dous	Catast-rophic
pⅤ	Frequent	A	U	U	U	U
pⅥ	Probable	A	A	U	U	U
pⅢ	Remote	A	A	A	U	U
pⅡ	Extremely Remote	A	A	A	A	U
pⅠ	Extremely Improbable	A	A	A	A	A

A: Acceptable / U: Unacceptable

5. 결 론

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 야기할 수 있다. 따라서 전쟁 양상의 변화에 맞추어 사이버 보안위협에 대한 전투기의 감항 인증에 대한 연구가 필요하다.

본 논문에서는 항공기 및 시스템 감항 보안 인증 기준인 DO-326A에서 제시하고 있는 감항 보안 인증 프로세스의 보안 위험평가 단계에서 전투기 보안위협을 보다 구체화 하고 전투기의 특징을 반영할 수 있도록 위험기반의 보안위험 평가 프로세스를 제시하였다.

이를 위하여 먼저 위협문장 생성 규칙 및 위협트리 작성을 통하여 전투기에서 발생할 수 있는 보안위협을 식별하였다. 다음으로 식별된 위협을 점수화하기 위하여 문장의 각 요소들을 사이버 공격의 발생 가능성과 전투기에 미치는 영향력의 관점에서 분석하였다. 마지막으로 점수화된 공격 발생 가능성 및 영향력 요소들을 DO-326A의 네 번째 단계인 보안위험 수락 여부 판단에 적용할 수 있도록 5등급으로 분류하여 보안위험 심각도 결정표를 작성하였다. 또한 FA-50 및 F-15K 등 전투기 운영체제로 널리 사용되고 있는 Vxworks의 CVE

중 하나를 선정하여 보안위협 프로세스에 적용하였다.

현재 전투기에 적용되고 있지 않은 감항 보안 인증 표준을 전투기의 운용환경 및 특성을 고려하여 적용할 수 있다는 점에 있다. 전투기에서 발생 가능한 보안위협 목록을 작성하기 위하여 위협문장을 구성하는 각 요소들에 전투기 운용환경 및 전투기를 구성하고 있는 자산을 반영하였으며 이를 점수화하기 위한 세부적인 항목 들을 선정하여 적용함으로써 보다 객관적으로 보안위험 수준을 결정 가능하도록 하였다. 또한 DO-326A의 감항 보안 인증 프로세스와 연계하기 위하여 5단계로 구성된 보안위험 심각도표를 작성하였다.

본 연구는 전투기 보안에 관한 국내의 최초 연구로 전투기 보안 요구사항에 대한 지속적인 연구가 이루어진다면 한국에서 개발하고 있는 KFX 사업에서 보안성이 보다 강화된 차세대 전투기 개발에 기여할 수 있을 것이다.

References

[1] Government Accountability Office, FAA Needs a More Comprehensive Approach to Address Cybersecurity As Agency Transitions to NextGen, *GAO Report*, 2015.

[2] H. J. Kim and D. S. Kang, "A Study of Fighter-plane Airworthiness Security Certification," in *Proceedings of KIPS*, Vol.25, No.1, pp.117-120, 2018.

[3] D. M. Seo, K. J. Cha, Y. S. Shin, C. H. Jeong, and Y. M. Kim, "Assessment Method of Step-by-Step Cyber Security in the Software Development Life Cycle," *Jounal of KIISC*, Vol.25, No.2, pp.363-373, 2015.

[4] M. G. Han and T. K. Park, "A Study on Intergrated Airworthiness Certification Criteria for Avionics Software Safety and Security," *Journal of the Korean Society for Aeronautical & Space Sciences*, Vol.46, No.1, pp.86-94, 2018.

[5] RTCA, DO-326A, Airworthiness Security Process Specification, Aug. 6, 2014.

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

[7] Adam Shostack, *Threat Modeling: Designing for Security*, H.Y., Yang, etc., Acorn Publisher, 2016.

[8] E. J. Park and S. J. Kim, "Derivation of Security Requirements of Smart Factory Based on STRIDE Threat Modeling," *Journal of the Korea Institute of Information Security & Cryptology*, Vol.27, No.6, pp.1467-1482, 2017.

[9] J. S. Han, K. J. Kim, and Y. J. Song, Introduction of UML, Hanbit Academy, 2008.

[10] G. Sindre and A. L. Opdahl, "Templates for Misuse Case Description," *Proceeding of. 7th International Workshop on Requirements Engineering*, pp.26-28, 2001.

[11] S. S. Choi, S. J. Jang, M. G. Choi, and G. S. Lee, "A Methodology for CC-based Security Requirements Analysis and Specification by using Misuse Case Model," *Journal of KIISC*, Vol.14, No.3, pp.85-100, 2004.

[12] Common Criteria, Common Criteria for Information Technology Security Evaluation Version 3.1, 2017.

[13] K. S. Lee, J. H. Ko, S. J. Jang, S. J. Choi, and S. H. Hwang, Analysis of Security Environment for the Common Criteria based protection Profile, Research Report, *Korea Information Security Agency*, 2002.

[14] C. J. Alberts and A. J. Dorofee, OCTAVE Criteria, Version 2.0. *Technical Report, Carnegie Mellon Software Engineering Institute*, 2001.

[15] ISO/IEC 27001, Information technology, Security techniques, Information security management systems, Requirements, 2014.

[16] ISO/IEC 27005, Imformation Technology, Security techniques, Information security risk management, 2014.

[17] J. H. Ko and K. S. Lee, "A Threat Statement Generation Method for Security Environment of Protection Profil," *Journal of Society for e-Business Studies*, Vol.8, No.3, pp. 69-86, 2003.

[18] Matteo Meucci, Andrew Muller, "Testing Guide 4.0 Release," 2015.

[19] J. S. Choi and K. H. Kook, "Secure Coding Rule Selecting Evaluation for Air Warfare System Considering Military Air Worthiness," *Journal of Security Engineering*, Vol.11, No. 6, pp.439-454, 2014.

[20] CVE Details [Internet], https://www.cvedetails.com/(Search 2018. 12.16.)

김 현 주

http://orcid.org/0000-0001-8398-1665
e-mail : st9280fly@naver.com
2005년 공군사관학교 국제관계학(학사)
2019년 국방대학교 컴퓨터공학전공(석사)
관심분야 : SW Engineering, Weapon System Software, Airworthiness Certification

강 동 수

https://orcid.org/0000-0001-6481-5071
e-mail : greatkoko@kndu.ac.kr
2011년 고려대학교 컴퓨터공학과(박사)
2015년~현 재 국방대학교 컴퓨터공학전공/사이버전과정 부교수
관심분야 : Weapon System Software, Software Security Testing, Defense Acquisition