항공통신망에서의 보안 요구사항에 관한 연구

김도우* · 이성현* · 이덕규* · 한종욱*

*한국전자통신연구원

The Study on the Security Requirement at Aeronautical Telecommunication Network

Do-woo Kim* · Lee, Seoung Hyeon* · Lee Deok Gyu* · Jong-wook Han*

*Electronics and Telecommunications Research Institute

E-mail : dwkim@etri.re.kr

요 약

항공기가 비행을 위한 준비단계에서 목적지에 도착할 때까지 항공기를 안전하고 보다 경제적이고 효율적으로 운항하기 위해 항공기와 지상시설 사이, 지상시설과 지상시설 사이의 정보전달과 교환이 필요하다. 현재는 AFTN이라는 폐쇄망을 이용하여 통신이 이루어지고 있지만, 첨단 통신기술을 적용하여 차세대 항공통신망이 구축되어 운영될 예정이다. 이로 인하여 외부 네트워크에 연결된 지상시설은 공격에 의한 보안 취약성을 가진다. 따라서 항공통신망에서의 안전한 운용환경 구축을 위한 취약성 분석 및 보안 요구사항 연구가 필요하다.

ABSTRACT

The information transfer between the ground facilities and the ground facilities and exchange are necessary for an aircraft and ground facilities so that it is safe, it is economic, an aircraft can operate an aircraft to the high efficiency until it arrives at the destination location from the stand-by for the fly. Presently, by using the AFTN which is closed network, a communication is made. However, by applying the leading edge communication technology, the aeronautical telecommunication network of the next generation is constructed and it is planning to be managed. Due to this, the ground facilities connected to the foreign network has the security vulnerability by an attack. Therefore, the vulnerability analysis for the safe operational environment build-up at the aeronautical telecommunication network and security requirement research are needed

키워드

Ⅰ. 서 론

항공기가 출발공항에서 목적공항까지 안전하게 비행하기 위해서는 지상 관제기관과의 정보교환이 필요하며, 지상관제기관 또한 항공기의 관제에 필요한 관제이양 정보, 비행정보, 기상정보 등을 다른 지상 관제기관과 서로 주고받을 수 있도록 해야 한다. 따라서 지상과 항공기 사이, 지상과 지상 사이에 통신을 하기 위한 각종 설비와 네트워크가 구성되어 있어야 원하는 정보를 주고받을 수 있다.

항공분야에 있어 앞으로의 통신환경은 항공통신망(ATN: Aeronautical Telecommunication Network)이라 불리우고 있는 범세계적인 통신네트워크를 이용하게 되므로 현행과 같은 전 근대적인 통신 운영환경에서 벗어나 항공기 운항과

*본 연구는 건설교통부 항공선진화사업의 연구비 지원(과제번호# 07항공-항행-03)에 의해 수행되었습니다.

관련된 제반 통신 시스템들을 통합 운영할 수 있는 여건이 조성된다. 항공통신망은 개방형 상호연결(OSI:Open System Interconnection)방식을 채택하고 있어 서로 다른 통신 프로토콜을 최대한 지원할 수 있으므로 서로 상이한 기종간의 상호 호환성 문제가 해소되고 국제항공고정통신망(AFTN: Aeronautical Fixed Telecommunication Network)/공통ICAO데이터교환망(CIDIN: Common ICAO Data Interchange Network)과 같은 기존의 네트워크들도 항공통신망 환경에 최대한 수용할 수 있게 되므로 기존 통신환경을 항공통신망으로 전환하는 데에 따른 구축비용을 상당히 절감할 수 있다. 이처럼 항공통신망은 현행보다 더욱 개선된 항공정보 서비스를 제공하기 위하여 지상과 항공기간, 지상과 지상간의 정보교환에 필요한 자동화 구현을 용이하게 하는 통신환경을 조성해 주므로 결국은 항공기의 안정운항 확보는 물론 경제적인 면에서도 많은 기여를 하게 될 것이다.

항공통신망은 일반통신 목적으로 사용하는 것이 아니라 항공기 안전운항에 관련된 데이터 통신서비스를 제공할 목적으로 제공된다. 전송되는 데이터에는 비행계획메시지, 출발메시지, 위치메시지, 관제승인, 관제이관 등 항공관제에 관한 메시지와 기상메시지, NOTAM 메시지 등 항공기 안전운항에 직접 관계되는 정보들이다. 현재는 국제고정항공통신망이라는 폐쇄망을 이용하여 통신이 이루어지고 있지만, 차세대 항공통신망은 개방형으로 구축되어 운영될 예정이다. 이로 인하여 외부 네트워크에 연결된 주요 기반시설은 공격에 의한 보안 취약성을 가진다[1,2].

따라서 항공통신망 환경에서 안전하고 신뢰성 있는 정보교환을 제공하기 위해 보안 요구사항과 정책(policy)의 수립은 상당히 중요한 요소이다. 본 논문에서는 항공통신망 환경에서 발생할 수 있는 보안 취약성을 분석하고, 이를 바탕으로 안전한 운용환경 구축을 위해 필요한 보안 요구사항 및 정책을 제시하고자 한다.

II. 항공종합통신망에서 요구되는 보안 서비스

항공종합통신망에서 요구되는 보안 서비스는 정보교환의 주체에 따라 달라질 수 있다. 그리고 교환되는 정보에 어떠한 데이터들이 포함될 것인가에 따라 달라질 수 있다. 현재와 같이 항공통신망이 공중망과 연결되어 있지 않다고 가정하면, 안전한 정보교환 환경을 제공하는 것은 어렵지 않다. 그러나 외부 공중망과 연동되어 운용된다면, 안전한 네트워크 서비스를 제공하기 위해 고려해야할 요소들은 많아진다.

또한 정보 이용의 주체가 한 명만 존재한다면, 안전한 항공통신망 구축이 쉬울 수 있다. 하지만, 정보 이용의 주체가 여러 명이 존재한다면 한 명이 이용하는 형태와 비교해볼 때 훨씬 복잡한 보안 정책이 필요하다.

항공종합통신망 환경에서 요구되는 정보보호 서비스는 공중망과 마찬가지로 다음과 같은 기능을 보장해야 한다[1,3].

- *인증(Authentication)* : 관제기관이나 항공사의 누구에게 전송된 정보를 사용하도록 허락할 것인가?
- *기밀성(Confidentiality)* : 관제기관이나 항공사로 전달된 메시지를 누구에게 읽도록 허락할 것인가?
- *무결성(Integrity)* : 관제기관이나 항공사 사이에 전송되는 정보는 권한을 가진 사용자만이 정보를 수정할 수 있어야 한다.
- *가용성(Availability)* : 사용자가 필요할 때 원하는 정보를 사용할 수 있도록 보장해야 한다.
- *인가(Authorization)* : 각 관제기관이나 항공사에서 제공하는 정보에 대해 구성원 각각에 대해 어느 정도의 접근권한을 주어야 하는가?

III. 항공종합통신망에서의 보안 취약성 분석

항공종합통신망 환경에서의 보안 위협(threat)은 부정확한(incorrect) 네트워크 구축, 관제기관이나 항공사 구성요소들의 변화 혹은 악성코드와 같은 외부 공격을 포함한 다양한 요소들로부터 발생할 수 있다. 이러한 위협은 관제기관이나 항공사 내의 보안 취약성(Vulnerability)과 대외 보안 취약성으로 분류할 수 있다. 그림 1은 항공통신망 환경에서의 보안 취약성을 보여주고 있다.

관제기관이나 항공사 내의 보안 취약성은 불법적인 접근, 인증되지 않은 디바이스의 접속, 메시지의 유출 등으로 분류할 수 있다.

불법적인 접근(Unauthorized access) : 침입자는 합법적인 사용자를 가장하여 관제기관이나 항공사의 서비스를 사용하거나 정보를 얻기 위해 접근할 수 있다.

인증되지 않은 디바이스의 접근(Uncertified device access) : 인증되지 않은 디바이스를 관제

기관이나 항공사의 네트워크 환경에 연결함으로써 시스템 환경의 보안 정책을 변화시킬 수 있다. 또한 합법적인 시스템으로 가장하여 네트워크 환경에 연결함으로써 서비스를 이용하거나 중요한 정보를 얻을 수 있다.

메시지 유출(Release of message contents) : 해커가 관제기관이나 항공사의 네트워크 환경에서 무선을 통한 전송이 이루어지는 경우, 전송되는 내부 트래픽을 가로채 분석을 할 수도 있다.

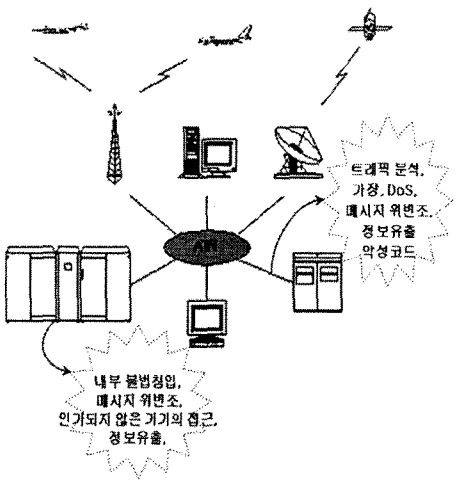

그림 1. 항공통신망 환경에서의 보안 취약성

댁외 보안 취약성은 악성코드, 가장, 가로채기, 메시지 유출, DoS, 트래픽 분석 등으로 분류할 수 있다.

트래픽 분석(traffic analysis) : 해커는 관제기관과 관제기관 사이, 관제기관과 항공사 사이, 관제기관과 항공기 사이에 전송되는 트랜잭션으로부터 중요한 정보를 가로채거나 시간, 양, 방향, 빈도 등 트래픽 흐름을 분석하여 사용자나 외부 노드의 위치 등을 추측할 수 있다.

가장(Masquerading) : 해커가 합법적인 정보 사용자를 가장하여 네트워크 환경에 원격 접속하여 서비스를 사용하거나 중요한 정보를 얻을 수 있다.

DoS(Denial of Service) : 침입자는 서비스의 가용성을 줄이거나 서비스 거부를 초래할 수 있는 다양한 방법으로 서비스나 트래픽을 방해할 수 있다. 침입자는 관제기관이나 항공사로 엄청난 양의 패킷을 보내어 공격할 수 있다. 이로 인해 시스템 자원이 고갈되고, 권한을 가진 사용자가 서비스를 사용할 수 없게 될 것이다.

정보 추론(Information inference) : 해커가 질의나 시그널을 네트워크 환경으로 보내거나 직접적으로 관제기관이나 항공사의 시스템으로 보내어 전달된 응답을 관찰해서 해커가 필요로 하는 정보를 추론할 수 있다.

정보 누출(Information leakage) : 침입자는 원격으로 네트워크 환경에 합법적인 접근을 해서 네트워크 시스템에 저장된 중요한 정보들을 유출시킬 수 있다.

악성 코드(malicious code) : 항공통신망 환경에서는 악성 코드로 인한 위협이 항공기 추락과 같은 대형 사고를 초래할 수 있기 때문에 다른 네트워크 환경과 비교해 훨씬 더 파급 효과가 크다. 현재 악성 코드는 소프트웨어 핏폴(pitfall), 전자우편, 웹 페이지 등을 통해서 전파된다. 악성 코드들은 관제기관이나 항공사의 시스템 자원을 크게 소모하고, 관제기관이나 항공사의 시스템을 심각하게 파손하고, 항공통신망을 통해 급속도로 빠르게 다른 관제기관이나 항공사로 전파될 수 있다.

IV. 항공종합통신망에서 필요한 보안 요구사항

항공통신망 환경에서 보안 정책은 관제기관과 관제기관 사이, 관제기관과 항공사 사이, 관제기관과 항공기 사이 등의 안전한 정보전달과, 전달된 정보를 안전하게 사용하기 위한 규칙(rule)을 명시해야 한다. 이 규칙은 시스템 자원의 사용, 정보의 저장 및 수정, 사용자에 대한 권한과 책임, 인증과 접근권한 제어 등으로 구성되어야 한다.

이 절에서는 3절의 보안 취약성 분석을 통하여 안전한 항공통신망 환경 설계 시 요구되어지는 정보보호 요소들을 기술할 것이다.

인증(authentication) : 항공통신망 환경에 불법적인 접근을 시도하여 관제기관이나 항공사 시스템의 불법 사용은 관제기관이나 항공사의 내·외에서 발생할 수 있다. 항공통신망 환경에 접근을 시도하는 사용자나 디바이스를 식별하는 기능은 보안 단계의 가장 첫 번째이며 가장 중요한 단계이다. 또한 인증 기능을 수행하기 위해 네트워크를 통하여 전송되는 인증 데이터는 합법적인 사용자를 가장한 침입자에 의해 유출될 수 있기 때문에 암호에 기반한 인증 기술을 사용함으로써 침입자로 하여금 네트워크를 통해 정보를 얻을 수 없도록 해야 한다.

인가(Authorization) : 관제기관이나 항공사의 내·외에서 항공통신망에 연결된 시스템의 안전

한 운용은 단지 인증만으로 이루어질 수 없다. 항공통신망 환경에서 접근권한 제어를 사용하여 관제기관이나 항공사 등의 구성원에 대해 미리 설정된 규칙에 기반하여 사용자가 시스템이나 서비스에 접근이 이루어질 수 있도록 하여야 한다. 이를 위해 시스템이나 서비스는 구성원 각각에 대해 혹은 다른 사용자에 대해 시스템이나 서비스의 어떤 기능이나 정보를 제공해야 되는지에 관한 접근권한 정보를 갖고 있어야 한다.

암호화(Encryption) : 중요한 트래픽 데이터의 무결성과 기밀성을 보장하기 위하여 항공통신망을 통해 전송되는 제어 메시지와 같은 중요한 데이터는 트래픽 분석이나 도·감청과 같은 위험성을 줄이기 위해 암호화되어져야 한다. 또한 패스워드, PIN과 같은 사용자 인증과 관련한 데이터도 시스템이나 서비스에 대한 불법적인 접근에 노출되는 위험성을 줄이기 위해 암호화되어져야 한다.

침입차단시스템(Firewall) : 침입자는 노출된 보안 취약성을 통해 지속적으로 항공통신망에 연결된 시스템을 스캐닝(scanning)한다. 침입차단시스템은 인터넷과 같은 외부 네트워크에 연결되어 있는 항공통신망의 중요한 정보 및 자원을 외부 네트워크를 통한 불법적인 침입으로부터 안전하게 보호할 수 있다. 침입차단시스템은 외부에서 항공통신망에 연결된 시스템 내부로의 공격이나 침입을 시도한다 할지라도 접근하려면 침입차단시스템을 반드시 거쳐야 하기 때문에 이를 탐지하고 방어할 수 있는 기능을 제공함으로써 어느 정도의 외부 공격으로부터 시스템을 보호할 수 있다.

침입탐지시스템(Intrusion Detection System) : 방화벽의 경우 침입이 발생하지 않도록 항공통신망에 연결된 시스템의 출입구를 제어하는 기능을 수행하므로 인증을 받지 않은 외부의 접근 시도는 차단할 수 있지만 이미 인증된 사용자나 이를 가장한 침입자에 의한 공격에는 취약하다. 특히 관제기관이나 항공사 등의 내부 사용자 혹은 허가된 외부 사용자에 의해 자주 발생하는 시스템 침입을 다룰 때에는 침입을 즉각적으로 탐지하고 대처하는 기술이 필요하다. 침입탐지시스템은 침입을 탐지하여 이를 관리 시스템에게 관련 정보를 전달하고 관리 시스템에서는 정해진 대응방침에 따라 연동되는 침입차단시스템, 바이러스 백신 프로그램 및 자체 보안기능 등을 통해 다양한 방법을 수행할 수 있다.

V. 결 론

본 논문에서는 항공통신망 환경에서 발생 가능한 보안 취약성을 분석하고, 이를 바탕으로 보안 요구사항들을 제시하였다.

다른 네트워크 환경과 비교해서 항공통신망 환경에서의 보안 취약은 항공기 충돌 및 추락과 같은 대형 사고를 유발할 수 있다는 점에서 상당히 많은 차이를 가진다.

현재 국제항공고정통신망과 같은 폐쇄망의 사용으로 인해 보안 인식 수준이 낮고, 관제기관이나 항공사 등의 관계자들에 대한 물리적 보안 정도가 제공되고 있는 실정이다. 이러한 요소들은 향후 항공통신망의 보안 위협을 증가시켜 항공기 안전성을 확보하는데 저해 요인으로 작용할 수 있다.

따라서 항공통신망 환경 설계 시, 적합한 정보보호 기술의 고려는 안전하고 신뢰성 있는 항공 운항비스 제공을 위해 반드시 필요하고, 중요한 요소이다.

참고문헌

[1] ICAO, AERONAUTICAL TELECOMMUNICATIONS. International Civil Aviation Organization, ICAO Annex 2., 2007,

[2] ICAO, *Rules of the air and air traffic services: procedures for air navigation services.* International Civil Aviation Organization, ICAO Doc 4444., 2001

[3] Gollmann Dieter, Computer Security, John Wiley & Sons, England, 1999.

[4] Cooper Frederic J., Coggans Chris, etc., Implementing Internet Security, New Riders Publishing, 1995.

[5] Hayes Keith, Active Security Monitoring and Containment with Cross Technology Correlation: The Next Generation in Computer Security Technology, 2002.