IVEF 무결성을 위한 확장된 IVEF 프로토콜 설계

김주영*, 이병길*, 정병호*, 신상욱**
*한국전자통신연구원 ICT 융합보안연구실
**부경대학교 IT 응용공학과
e-mail : {ap424,bglee,cbh}@etri.re.kr, shinsu@pknu.ac.kr

Design of Expanded IVEF Protocol for Integrity

Juyoung Kim* Byunggil Lee* Chung Byungho Sang Uk Shin**
* Electronics and Telecommunications Research Institute ICT Convergence Security Research Lab
** Dept. of IT Convergence and Application EngPukyoung National University

요 약

최근 선박의 연안 선박의 안전사고가 증가함에 따라 기존 항만 중심으로 운영되고 있던 해상교통관제센터의 관제 범위가 연안까지 확대되고 있다. 이에 따라 해상교통관제센타(Vessel Traffic Service Center, VTS) 간에 데이터 교환의 필요성도 증가하고 있다. 국제항로표지협회 IALA(International Association of Lighthouse Authorities, IALA)는 이러한 필요성을 인지하고 해상교통관제센타간 데이터 교환 프로토콜인 IVEF(Inter-VTS Exchange Format)를 제정하였다. 그러나 IVEF 프로토콜 특성상 외부 해상교통관제센터간 데이터가 전송됨으로 데이터 변조등의 위험성이 있다. 하지만 IVEF 프로토콜은 보안 관련 요소들이 미미한 실정이다. 본 논문에서는 IVEF 데이터의 무결성을 보장하는 방법을 제안한다.

1. 서론

최근 연안 해역의 잦은 선박사고로 그동안 항만 위주로 운영되던 해상교통관제센터의 범위가 확대되는 추세이다. 또한, 효율적인 항만운용을 위해서 e-Navigation 이 대두 됨에 따라 해상교통관제센터간 데이터 교환의 필요성이 제기 되었다. 이에 따라 국제항로표지협회 IALA 는 해상교통관제센타간에 데이터 교환 표준프로토콜인 IVEF 를 제정하게 되었다. IVEF 는 XML 형태의 메시지로 구성되어 있는 프로토콜로 선박의 위치, 제원, IVEF 서비스 상태 등 을 나타낸다. IVEF 프로토콜이 정의된 V-145 recommendation 에서는 보안에 대해서는 별도의 정의 없이 SSL 과 같은 표준 기술들을 사용하는 것을 권고하고 있는 실정이다. 특히 인증, 인가를 제외한 데이터 보호에 대한 부분은 별도로 정의하지 않고 있다. IVEF 데이터는 관제를 목적으로 함으로 데이터가 위변조될 경우 심각한 문제를 발생시킬수 있다.

본 논문에서는 IVEF 데이터의 무결성을 보장하기 위해 IVEF 프로토콜의 확장 엘리먼트를 이용하는 방법에 관해서 설명한다.

2. IVEF 프로토콜

IVEF 프로토콜은 해상교통관제센터간의 데이터 교환을 위한 프로토콜로 표 1 과 같이 8 개의 XML 데이터 형식으로 정의되어 있다[1]. 8 개의 메시지 중 선박정보를 저장하는 8 개의 메시지 중 ObjectData 메시지는 선박의 제원, 위치, 타임스탬프 등의 정보가 담겨 있으며 사용자가 임의로 정의하여 사용할 수 있는 Taggeditem 엘리먼트를 지원한다.

<표 1> IVEF 메시지 구성

Message		Description
Control Information Message	Login	로그인요청
	Login Response	로그인 요청 응답
	Logout	로그아웃 요청
	Ping	서비스 상태확인
	Pong	서비스 상태확인 응답
	Service Request	서비스 요청
	Service Request Response	서비스 요청 응답 메시지
	Service Status	서비스 상황

Real Time Message	Object Data	선박의 운항, 위치, 제원, 상태등의 정보

3. IVEF 서비스

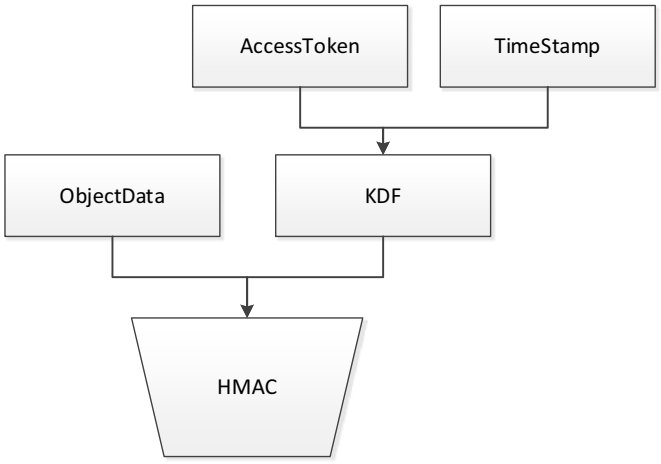
IVEF 를 정의한 V-145 recommendation 에서는 IVEF 데이터 보안에 대해서는 따로 정의하지 않고 구축하는 환경에 따라 표준 보안 기법을 사용하도록 정의되어 있다[1]. 본 논문에서는 설명하는 IVEF 서비스는 더욱 폭 넓게 활용할 수 있도록 웹을 통한 데이터 공유 서비스로 가정한다. IVEF 메시지는 XML 형태로 제공되기 때문에 웹을 통한 공유가 용의하다. 특히 Open API 로 제공될 경우 다양한 형태로 가공하여 사용할 수 있는 이점이 있다.

OpenAPI 형태로 데이터를 공유할 경우 AccessToken 을 기반으로 사용자를 인증하는 Oath 프로토콜을 활용할 수 있다. OAuth 2.0 은 타사 프로그램에서 HTTP 서비스에 대한 제한된 액세스를 허용하는 인증 프레임 워크이다.[2] Oauth 프로토콜 3rd Party 서비스가 사용자의 아이디, 패스워드 정보에 접근하지 않고 AccessToken 을 이용하여 API 를 호출하는 방식의 프로토콜이다. 사용자는 3rd Party 서비스에 직접 로그인 하지 않고 실제 OpenAPI 서버에 로그인 하고 인증이 되면 AccessToken 을 3rd party 앱으로 전송한다. 이 때 AccessToken 은 무작위의 난수 값으로 128bit 이상의 값을 사용한다.

4. 무결성 인증 방법

본 논문에서는 키 유도 함수와 HMAC 을 이용한 무결성 인증 방법을 제안한다. 키 유도 함수는 키 유도 함수는 공유된 비밀값을 이용하여 비밀키를 생성하는 함수로 해쉬 함수를 기반으로 사용한다.[3] HMAC 은 Bellare 등이 제안한 해쉬 함수 기반메시지 인증 코드로서, 단순한 구조로 설계되었으며 안전성에 대한 증명이 이루어졌다. 현재, ANSI, IETF, ISO, NIST 표준으로 제정되어 있으며, SSL, TLS, SSH, IPsec 등 다양한 프로토콜에서 사용되고 있다.[4]

IVEF 서비스를 제공하는 서버는 인증된 Oauth 클라이언트에게 AccessToken 을 발급한다. AccessToken 은 유효기간이 정해져 난수로써 유효기간이 지나면 새로 발급하여 사용해야 한다. 키 유도 함수 KDF 에 AccessToken 와 타임스템프를 삽입하여 그림 1 과 같이 선박의 제원 및 위치 정보가 삽입된 ObjectData 메시지에 대한 HMAC 값을 생성할 키를 유도한다.



(그림 1) HMAC 값 생성

키 유도 함수로 생성된 키를 이용해 HMAC 에 ObjectData 메시지값을 삽입하여 HMAC 값을 생성 한다. 생성된 HMAC 값은 ObjectData 메시지내의 Taggeditem 엘리먼트 key 값을 “HMAC”으로 표시하고 Value 값에 HMAC 값을 삽입하여 최종적으로 ObjectData 메시지를 생성한다.

5. 결론

본 논문에서는 IVEF 데이터의 무결성 검증을 위해 HMAC 과 키 유도 함수를 이용한 방법을 제안하였다. 하지만 이러한 방식은 Oauth 를 사용할 수 있는 환경에서만 적용 가능하다.

향후 TCP/IP 나 UDP 기반의 IVEF 서비스 모델의 경우에도 무결성을 보장할 수 있는 방법에 대해서 연구가 더 필요하다.

Acknowledgement

* 본 연구는 해양수산부/한국해양과학기술진흥원 해양안전 및 해양교통시설기술개발사업 연구비지원(ETRI 수행 과제번호 20090403)에 의해 수행 되었습니다.

참고문헌

[1] V-145 Recommendation, IALA, 2011
[2] RFC 6749. “The OAuth 2.0 Authorization Framework”, IETF, 2012
[3] 정현철,이향진 “해쉬함수 이용 가이드라인”, 한국정보통신기술협회, 2009
[4] 정기태, 이유섭, 성재철, 홍석희, “오류 주입 공격을 이용한 HMAC 에 대한 키 복구 공격”,한국정보보호학회논문지 제 21 권 제 5 호,2011