한국컴퓨터정보학회 하계학술대회 논문집 제20권 제2호 (2012. 7)

메인 인증 서버와 IVEF를 이용한 VTS 시스템간 사용자 인증 개선방안

조승현°, 정재욱*, 박남제**, 이병길***, 원동호*†
°*성균관대학교 정보보호연구실
**제주대학교, ***한국전자통신연구원
{shc°, jwjung, dhwoon}@security.re.kr*, namjepark@jejunu.ac.kr**, bglee@etri.re.kr***

Using the Main Authentication Server and the IVEF in VTS System for Improve of Client Authentication

Seunghyun Cho°, Jae-Wook Jung*, Namje Park**, Byung-Gil Lee***, Dongho Won*
°*Information Security Group, Sungkyunkwan University
**Jeju National University, ***ETRI

● 요 약 ●

국제해사기구(IMO)에서 진행하는 "e-Navigation" 프로젝트의 구성요소인 해상교통관제시스템(VTS)을 정의하고, VTS 시스템간 정보교류를 위한 기술로 IVEF(Inter-system VTS Exchange Format)를 소개한다. 현재까지 국제항로표지협회(IALA)에서 개발한 IVEF에는 접속자에 대한 신뢰도 높은 인증 기술이 포함되지 않는다. 하지만 해상교통정보는 국가적으로 보안수위가 높은 정보이므로 정보 요청 자에 대한 신뢰 높은 인증이 절대적으로 필요한 부분이다. 따라서 본 논문에서는 메인 인증 서버와 IVEF를 이용하여 VTS 시스템간의 신뢰도를 높일 수 있는 인증 시스템을 제안한다.

키워드: e-Navigation, VTS, IVEF, 해상교통관제시스템

I. 서론

e-Navigation은 해상활동에서의 안전 및 보안 또는 해양환경 보호를 목적으로 2006년 국제해사기구(IMO)에서 제안된 프로젝트로서 국제항로표지협회인 IALA(International Association of Lighthouse Authorities)를 중심으로 기술의 표준화 및 이행전략을 수행하고 있으며, 2012년 현재까지도 연구가 활발히 진행되고 있다. e-Navigation에서 VTS(Vessel Traffic System)는 해상교통관제시스템으로 선박의 항해정보 및 해양 환경에 대한 정보 등이 포함되어 있다.

IVEF는 IALA에서 개발한 VTS간 게이트웨이(gateway) 프로토콜이로서 VTS와 VTS간의 정보를 교환할 수 있도록 개발하였고 현재 국제 표준화가 진행 중이다.[1] 본 논문에서는 IVEF를 이용하여 VTS간의 정보 교환 시, 발생할 수 있는 문제를 해결하기 위한 시스템을 제안한다. 본 논문의 구조는 다음과 같다. 2장에서는 VTS간의 정보교환 프로토콜 및 기존의 제안된 시스템을 분석하고 3장에서는 분석된 내용을 바탕으로 보안 구조를 제안하며 마지막 4장에서는 결론 및 향후 연구 계획으로 끝낸다.

II. 관련 연구

IVEF는 IALA에서 개발이 진행 중인 VTS간 정보교환의 오픈소스식 SDK이며 국제 표준화 진행이 거의 완료 된 게이트웨이이다. IALA에서 제공하는 공식 IVEF기술문서에는 인증(authentication), 승인(authorisation)을 제외한 데이터 보안은 IVEF범주를 벗어난다고 기술되어있다.[2] 현재까지 제안된 IVEF 보안 사항으로는 사용자 인증 정보를 공개키 방식으로 암호화하는 제안밖에 없다.[3] 그러나 VTS와 VTS간에 연결된 물리적인 링크상태를 종료 시켰다가 재접속을 하였을 때, VTS시스템은 일시적인 트래픽 과부하로 인한 지연현상이라는 경우가 발생할 수 있다. 이 같은 경우에 데이터 유출이 발생하게 된다. 따라서 3장에서는 이에 대한 해결 방안으로 메인 인증 서버시스템을 제안한다.

III. 본론

본 장에서는 사용자 인증을 위한 메인 인증 서버를 [그림 2]와 같이 제안한다.

† 교신저자, dhwon@security.re.kr

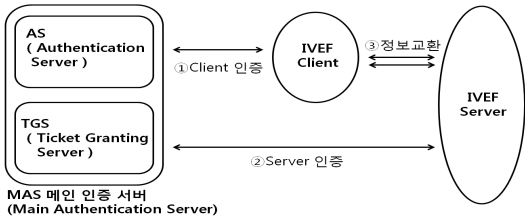

그림 2. MAS를 도입한 IVEF
Fig. 2. Using the MAS in IVEF

[그림 2]는 메인 인증 서버(Main Authentication Server)가 IVEF Client(IC)와 IVEF Server(IS)를 인증 후 정보교환을 하는 시스템을 간략히 요약한 것이다. 메인 인증 서버(MAS)는 AS(Authentication Server) 와 TGS(Ticket Granting Server)로 이루어 져 있다.

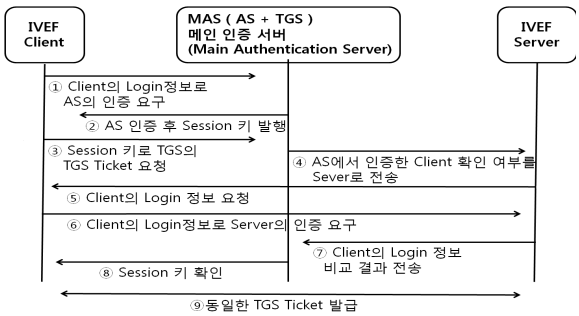

그림 3. IC와 IS, MAS사이의 프로토콜
Fig. 2. A protocol between the IC, IS and MAS

[그림 3]은 IC와 IS 그리고 MAS 사이의 프로토콜을 나타낸다. [그림 3]의 ①번 과정은 IC가 자신의 Login정보를 이용하여 MAS의 AS에게 본인임을 요구한다. ②번 과정은 AS에서 IC를 인증 후 Session키를 발급하여준다. ③번 과정은 발급받은 Session 키로 TGS에 TGS Ticket 발급을 요청한다. TGS Ticket에는 Client의 ID, IP주소, Ticket 발급 시간, Ticket의 유효시간의 정보가 들어있다. ④번 과정은 MAS의 AS에서 인증한 IC의 확인 여부를 IS에게 전송한다. ⑤번 과정은 IS가 직접 IC에게 Login 정보를 요청한다. ⑥번 과정은 Client의 Login정보로 Server의 인증을 요구한다. ⑦번 과정은 Client의 Login 결과와 ④번 과정에서 AS에게 받았던 확인 여부 비교하여 결과를 MAS에 전송한다. ⑧번 과정은 ②번 과정에서 발행한 Session 키를 확인한다. 마지막 ⑨번 과정은 모든 과정에서 오류가 없었을 경우 동일한 TGS Ticket을 IC와 IS에게 발급하여 인증을 하게 된다. 이처럼 MAS가 IC와 IS를 동시에 인증함으로서 특정 부분에서의 링크가 종료되는 현상을 감지할 수 있다. 또한, TGS Ticket의 IP주소 및 Ticket 유효시간 정보를 통해 공격자로부터 불법 접근 및 Replay 공격을 방어 할 수 있다.

IV. 결론

지금까지의 e-Navigation의 기술 표준화 진행을 보면 IVEF가 국제 표준으로서 VTS간의 정보교환 게이트웨이로 사용될 가능성이 높지만 IVEF의 취약점이 존재한다. 기존에는 공개키 방식으로 취약점을 개선하였지만 공개키 방식을 사용함에도 불구하고 또 다른 취약점을 예상할 수 있었다.

본 논문에서는 IVEF의 기본 구조에 대칭키 방식을 사용한 메인 인증 서버(MAS)라는 개념을 도입하여 새로운 인증 개선 방안을 제안하는데 두었으며 향 후 연구에서는 대칭키 방식의 효율적인 키 분배방법을 구체적으로 제시할 것이다.

참고문헌

[1] IVEF Recommendation V-145 on the Inter-VTS Exchange Format(IVEF) Service, Jun. 2011
[2] Open IVEF “www.openivef.org”
[3] A Security Architecture of the inter-VTS System for shore side collaboration of e-Navigation, Feb. 2012

Acknowledge

“본 연구는 방송통신위원회의 방송통신융합미디어원천기술개발사업의 연구결과로 수행되었음” (KCA-2012-12-912-06-003)