디지털 사이니지를 활용한 재난안전 정보 보호에 대한 연구

이수연* · 안효범**

요 약

최근 세계적으로 자연재해 등의 피해를 줄이기 위해 각 국가마다 통합재난안전관리시스템을 운영하고 있다. 특히, 재난경보 메시지를 보내기 위한 방법으로 디지털 사이니지(Digital Signage) 활용에 대한 연구가 이루어지고 있다. 본 논문에서는 디지털 사이니지에 대한 개념과 재난안전관리시스템을 살펴보고 재난안전통신망에서 요구되어지는 보안요구사항을 알아보았다. 또한, 디지털 사이니지를 활용한 재난안전 서비스에서 공통경보 메시지를 안전하게 디지털 사이니지 터미널에 전송하기 위해 공개키 인증기법을 사용한 프로토콜을 제안하였다. 제안 된 프로토콜은 공통경보 메시지를 해당 지역에 안전하게 표시될 수 있도록 하였다.

Study of Disaster Safety Information Protection using Digital Signage

Suyeon Lee* · Hyobeom Ahn**

ABSTRACT

Recently, each country should operates a integrated disaster safety management system in order to reduce the damage, such as the world-natural disasters. In particular, research on digital signage use has been made by a method for transmitting a disaster warning message.

In this paper, we tried to examine the security requirements that are required by the disaster safety network by looking at the digital signage concept and disaster safety management system. Also, in order to be transmitted to the safe digital signage terminal a common alarm message in the disaster safety services using digital signage, we propose a protocol that uses a public key authentication mechanism. The proposed protocol is to be safely displayed a common alarm message to the appropriate area.

Key words : integrated disaster safety management system Digital Signage, Public key authentication mechanism

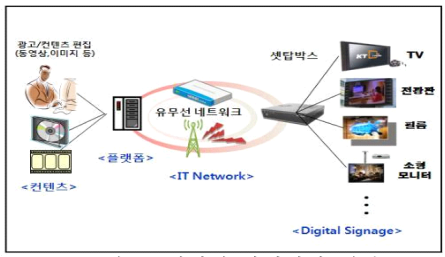
접수일(2015년 12월 1일), 수정일(1차: 2015년 12월 20일), 게재확정일(2015년 12월 30일)

* 백석문화대학교 인터넷정보학부
** 공주대학교 정보통신공학부 (교신저자)

1. 서 론

최근 세계적으로 자연재해, 인공재해 등에 의한 피해를 줄이기 위해 범국가적으로 통합재난관리시스템이 구축되고 있다. 한편, 역이나 터미널, 버스 등 일반 대중들에게 쉽게 눈에 띄는 곳에 설치된 디지털 사이니지 단말은 재난 발생 시에 사람들에게 재난경보 발령 및 대피 요령 정보 등을 일반 대중들에게 효과적으로 알려주기 위해 활용될 수 있다.[1]

디지털 사이니지(Digital Signage)는 다양한 이동공간에서 네트워크에 접속 된 디스플레이 등의 전자적 표시 기구를 이용해 다양한 정보를 제공하는 시스템이라고 정의할 수 있다. 즉, 네트워크를 통해 원거리에서 콘텐츠 설치와 운용, 교체가 가능하게 하는 것이다.



(그림 1) 디지털 사이니지 개념

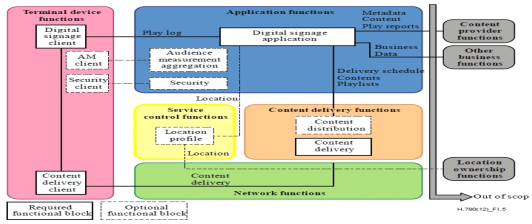
2015년 디지털 사이니지 전망을 보면 재난, 재해정보 등 공공 정보 제공을 위한 디지털 사이니지 서비스를 다양화하고 확대해 공공서비스의 효율성을 확보할 필요성이 있다고 한다.[2] 이렇듯, 디지털 사이니지를 활용한 재난정보시스템 구축은 현재 우리나라에서도 추진되고 있는 정책이다.

따라서 본 논문에서는 디지털 사이니지를 활용한 재난정보시스템과 이에 필요한 보안요구사항 살펴보고 재난정보 서비스 보호에 대한 방법을 제시하고자 한다. 본 논문의 구성은 다음과 같다. 먼저 2장에서는 디지털 사이니지와 재난경보 서비스를 알아보았다. 3장에서는 재난안전통신망에서 필요한 보안요구사항을 살펴보았다. 4장에서는 디지털 사이니지를 활용한 재난정보 서비스 보호에 대한 방법을 제시하였다. 5장에서는 결론과 향후 연구계획에 대해서 설명하였다.

2. 디지털 사이니지(Digital Signage)와 재난경보 서비스

2.1 디지털 사이니지 시스템 구조 및 역할

H.780에서는 IPTV 구조에 기반을 둔 디지털 사이니지 시스템 구조를 정의하고 있다[3]. 이 구조는 (그림 2)에서와 같이 5개의 필수 기능그룹과 1개의 선택 기능그룹으로 구성되어 있으며 각 기능들은 다수의 기능들로 이루어져 있다.



(그림 2) ITU-T 디지털 사이니지 시스템 구조[3]

디지털 사이니지 터미널은 디지털 사이니지 클라이언트와 콘텐츠 전달 클라이언트로 구성되며 사이니지 서비스 제공자는 디지털 사이니지 서버와 콘텐츠 전달 서버로 구성된다.

디지털 사이니지 클라이언트 기능은 플레이 제어(Play control) 기능, 미디어 처리(Media processing) 기능스토리지(Storage) 기능, 서비스 발견(Service discovery) 기능이다. 클라이언트의 기능 중 스토리지 기능과 서비스 발견 기능은 취약점에 노출될 수 있다. 즉, 제3의 공격자에 의해서 스토리지가 탈취된다면, 디지털 사이니지에서 거짓 정보를 보여줄 수 있다. 또한 서비스 발견 기능은 잘못된 정보를 제 3자가 보내거나 악의를 갖는 정보를 보여 줄 수 있다. 이러한 취약점을 방지하기 위해서는 저장장치에 대한 접근 제한과 서비스 발견 기능에는 정당한 서비스 제공자인지를 인증할 수 있는 기능이 포함되어야 한다.

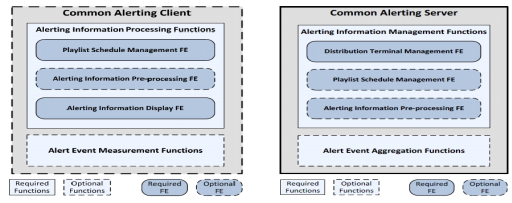
2.2 재난안전통신망

재난안전통신망은 두 가지의 기술이 사용되는데 하나는 미주지역에서 사용되는 P25와 유럽지역에서 사용되는 테트라 망 방식이 있다.

미주에서 사용되는 P25표준은 2001년에 APICC(APdo Projet 25 Interface CCommittee)의 Inter-RF Subsystem Interface Task Group에 의해서 초안이 작성되었고, 표준 작업은 TIA의 TR-8 기술위원회에서 완성하였다. 이 TR 그룹 중 보안에 관련된 작업을 하는 분과는 TR-8.3에서 암호화를 다루고 있으나 인증 작업과 같은 부분을 지정하지는 않고 있다.

유럽에서 사용되는 TETRA(TErrestrial Trunked Radio) 표준은 1994년에 표준이 완성되었다. TETRA의 표준은 ETSI TC TETRA에서 이루어지고 있고 작업그룹 중 WG6에서 보안을 담당하고 있다. TETRA표준에서는 4개의 암호화 표준인 TEA1, TEA2, TEA3 그리고 TEA4를 사용한다. 이 암호화 알고리즘은 허가된 사용자의 유형에 따라 다르게 사용된다[4]

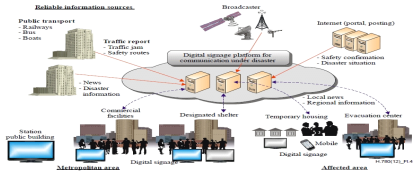
재난안전 서비스 목표는 재난 관련 정보를 수집하여 관련 응용 시스템을 통하여 예측·추측한 결과를 재난 현장에서 활용할 수 있도록 하는 것이다. 공통경보 클라이언트는 공통경보 서버로부터 전달받은 공통경보 메시지를 표시하며 단말의 상태를 서버에 전달하기도 한다. 경우에 따라 경보의 형태를 변환하여 표시할 수 있다. 공통경보 서버는 경보지역 선택, 단말의 선택 등 공통경보 서비스에 관련된 데이터 관리를 지원한다.



(그림 3) 공통경보 시스템 역할[3]

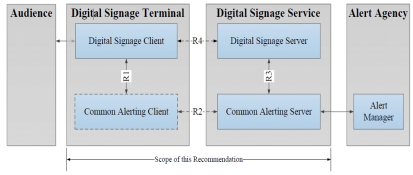
2.3 디지털 사이니지를 활용한 재난안전 서비스

ITU-T H.DS-DISR(Digital Signage: Requirements of Disaster Information Services)는 재난 발생 이전 예보 시점부터 재난 상황 종료 시점까지 요구되는 다양한 재난정보 서비스에 대한 4가지 요구사항을 기술하고 있다. 즉, 재난 발생하기 전 준비사항, 재난 발생하기 직전 재난 상황, 재난 상황에서 정보 제공, 재난 발생 이후 정보 제공이다. H.DS-DISR 권고초안에서는 이러한 다양한 고려사항을 바탕으로 재난정보의 전파 관련 요구사항은 7개로 나눈다. 그리고 디지털 사이니지 서비스 기반의 재난정보 전파모델을 정의한다. 기본적으로 디지털 사이니지 서비스 플랫폼에는 방송, 언론, 정부, 대중교통 수단, 기상청, 포털 등 다양한 출처로부터 다양한 유형의 정보를 수진하여 일반 대중들에게 제공하고 있다. 특히, 재난 발생 지역에는 재난정보, 대피정보, 지역 뉴스를 제공한다. 또한 모바일과 연동하여 생존자 유무 확인 및 개인화된 정보 제공 등 다양한 재난정보를 제공할 수 있다.[6]



(그림 4) 디지털 사이니지 서비스 기반 재난정보 전파모델(H.780)

디지털 사이니지를 활용하여 재난경보 서비스 프레임워크가 개발 중이며 현재까지 개발 된 구조는 (그림 5)와 같다.



(그림 5) 디지털 사이니지를 위한 공통 재난경보 서비스 구조

이 구조는 ITU-T 디지털 사이니지 시스템 구조에서 콘텐츠 전송 클라이언트 위치에 공통경보 클라이언트를 넣었고 콘텐츠 전송 서버 위치에 공통경보 서버를 넣었다.

3. 재난안전통신망 보안요구사항

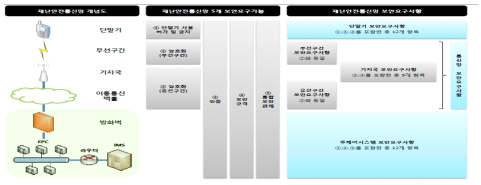
H.DS-DISR 권고안에서는 재난정보 오남용을 방지하기 위한 보안 요구사항도 포함되어 있다. 따라서

본 장에서는 재난안전통신망에서 요구되어지는 보안 요구사항을 대해 살펴보고자 한다.[7]

재난안전통신망은 단말기, 통신망, 주제어시스템으로 나뉘어 보안요구사항을 가지고 있다.

3.1 재난 안전망시스템에서의 보안취약점

재난안전망시스템의 구분에 따라 통신망에서의 보안, 단말기와 주제어시스템에서의 보안이 요구된다.



(그림 6) 재난안전통신망 보안요구사항

통신망에서 나타날 수 있는 보안 취약점은 재난 안전에 대한 데이터를 전송할 때 도청을 통한 재전송 공격과 변조공격이 가능하다. 단말기와 주제어시스템에서는 위장을 통한 잘못된 알람을 전송하는 경우가 발생할 수 있다. [표 1]은 이러한 취약점을 방지하기 위한 보안서비스를 제시한다.

[표 1] 취약점 방지를 위한 보안서비스

분류/보안 서비스	재난 통신망	단말기	주제어기
기밀성	○	○	○
무결성	○		
인증	○	○	○

재난통신망에서는 기밀성, 무결성, 인증을 제공함으로써 전달되는 알람에 대한 도청과 재전송공격 그리고 위장 공격을 방지할 수 있다. 또한 단말기나 주제어기는 기밀성을 통해 저장된 데이터에 대한 보호를 수행하고 인증을 통해 단말기와 주제어기가 올바른 개체임을 확인하는 상호 인증이 요구된다. 정보서비스의 상호 인증은 재난통신망에서 가장 중요한 서비스로서 본 논문에서는 이를 중심으로 단말기와 주제어기의 인증방법에 대한 부분을 다루게 된다.

3.2 재난안전망에서의 보안요구사항

3.1절의 내용을 바탕으로 각 구성요소에 대한 보안요구사항을 다시 정의한다.

■ 단말기 측면

단말기 사용자 식별 및 인증, 가입자 및 단말기 식별 및 인증, 매체제어 및 통신경로 접근통제, 저장데이터보호, USIN 복제 및 도용방지, 악성코드 탐지, 인증서 보호 및 전자서명 검증 요구사항이 있다.

■ 통신망(유/무선구간, 기지국) 측면

기지국, 백홀망 장비 관리자 식별 및 인증, 전송 데이터보호, 저장데이터보호, 보안관리, 자체시험, 안전한 세션 관리, 감사기록, 불필요한 서비스 제어, 보안약점 제어 요구사항이 있다.

■ 주제어시스템 측면

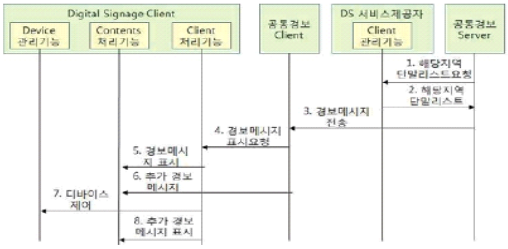
주제어시스템 관리자 식별 및 인증, 가입자 및 단말기 식별 및 인증, 보안관리, 자체시험, 안전한 세션 관리, 감사기록, 전송데이터 보호, 불필요한 서비스 제거, 통합보안관제, 외부 망 연계 트래픽 통제, 보안약점 요구사항이 있다.

(그림 6)에서처럼 재난안전통신망 보안요구사항에서 공통적으로 요구되는 항목은 인증이다. 따라서 아직까지 디지털 사이니지를 활용한 재난정보 서비스에서 각 구간 인증에 대한 연구가 부족한 실정이다.

4. 디지털 시니어를 활용한 재난정보서비스 보호에 대한 방법

4.1 디지털 사이니지(DS)를 활용한 재난 정보 흐름

공통경보 서버가 일단 경보발령기관으로부터 경보발생 명령을 받았다면 다음과 같은 단계로 디지털 사이니지를 통해 경보 메시지를 표시한다.[8]



(그림 7) 디지털 사이니지를 활용한 재난정보 흐름

① 공통경보 서버는 디지털 사이니지(DS) 서비스 제공자에게 해당 지역의 단말 리스트 정보를 요청한다.
② 디지털 사이니지 서비스 제공자는 요청 정보를 받고 해당 지역 단말 리스트 정보를 공통경보 서버에 보낸다.
③ 단말의 공통경보 클라이언트로 경보 메시지를 전송한다.
④ 공통경보 클라이언트는 디지털 사이니지 클라이언트 즉, 클라이언트 처리기능, 콘텐츠 처리기능, 단말 관리 기능을 이용하여 경보 메시지를 표시하게 한다.

(그림 7)에서 보여준 디지털 사이니지를 활용한 재난정보 흐름에서 단말기와 공통경보 서버사이에 보안 요구사항에 대한 해결책이 제시되어있지 않다. 특히, 공통경보 클라이언트가 디지털 사이니지 클라이언트 사이에 경보메시지 표시 요청 할 때 공통경보 클라이언트에 대한 인증이 필요하다. 왜냐하면 공통경보 클라이언트를 가장한 클라이언트가 메시지를 보낼 때 다른 지역에 메시지가 전송되어 혼란이 야기되기 때문이다. 따라서 본 논문에서는 공통경보 클라이언트(CAC)와 디지털 사이니지 클라이언트(DSC) 사이의 공개키 인증 기법을 제시하고자한다.

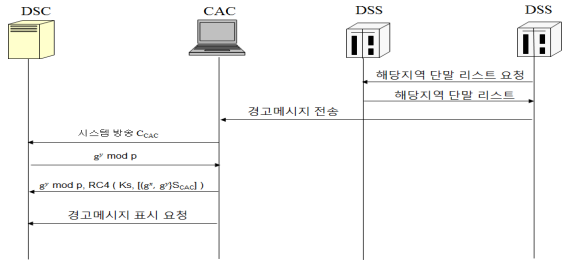
4.2 공개키 인증 기법을 적용한 재난 정보 흐름

외부 공격자는 특정 디지털 사이니지 클라이언트를 가장하여 계속해서 서비스를 제공받을 수 있게 되거나, 공통경보 클라이언트를 가장해서 디지털 사이니지 클라이언트에게 재난메시지를 표시하도록 요청할 수 있다. 이러한 공격을 방지하기 위한 방법으로 인증기법을 사용할 수 있다. 디지털 사이니지 디바이스는 어느 정도의 계산 능력을 가지고 있다고 가정할 수 있기 때문에 인증을 위한 방법으로 공개키를 도입할 수 있다. 먼저 공통경보 클라이언트(CAC)와 디지털 사이니지 클라이언트(DSC)사이에 수행되는 공개키 방식의 인증서 개념을 추가하여 공통경보 클라이언트(CAC)가 자신의 신분을 디지털 사이니지 클라이언트(DSC)에 입증하게 된다.

제안 프로토콜에 사용되는 프로토콜은 (그림 8)과 같다. 여기서 전달되는 인증서 C_{CAC}는 다음과 같이 생성된다.

$$C_{CAC} = \{CAC, P_{CAC}, g, p, CAC, P_{CAC}, g, pS_T\}$$

g,p : *Diffie-Hellman 파라메터*
P_{CAC} : *CAC의 공개키*
$\{ \square.. \}S_T$: *인증서 발급 기관 T의 비밀키로 서명한 값*



(그림 8) 공개키 인증 기법을 이용한 재난 정보 흐름

CAC에서 방송되는 시스템 정보에 인증서(C_{CAC})를 통해 DSC가 정당한 CAC에 대한 확신을 갖게 된다. 먼저 공통된 세션 키($g^{xy} \bmod p$)를 이용해 복호화 한 후에 인증서(C_{CAC}) 포함 된 CAC의 공개키(P_{CAC})를 이용해서 CAC에 의해서 서명 된 $g^x, g^y S_{CAC}$를 확인할 수 있다. 인증이 된 후 CAC는 DSC에 경고메시지 표시 요청을 하게 된다.

5. 결 론

본 논문에서는 디지털 사이니지를 활용한 재난정보

서비스 흐름을 살펴보았다. 특히, 안전한 재난정보 서비스 제공을 위하여 재난정보통신망에서 필요한 보안 요구사항을 살펴보았다. 만약, 재난정보를 제공하는 서버가 정당한 디지털 사이니지 클라이언트에게 재난정보를 보내지 못하고 다른 지역에 있는 디지털 사이니지 클라이언트에게 보내게 되면 재난이 발생하지 않은 지역에 큰 혼란이 야기되게 된다. 따라서 본 논문에서는 재난정보를 제공하는 서버와 해당 지역 디지털 사이니지 클라이언트 사이에 인증이 필요하므로 공개키를 이용하여 인증하는 방법에 대하여 제안하였다. 향후 연구방향으로는 국내표준으로 도입된 재난방송망 TETRA와 디지털 사이니지를 접목시키기 위한 방법과 보안에 대한 부분 즉, 인증과 암호화에 사용되는 키 관리에 대한 다각적인 검토가 필요하다.

참고문헌

[1] 강신욱, 현욱, 김성혜, 허미영 “디지털 사이니지 표준화 동향”, 한국통신학회지, 2013.7

[2] 정보통신기술진흥협회, “디지털 사이니지 최근 동향 및 발전방향”, 2012.4

[3] ITU-T H.780, “Digital signage: Service requirements and IPTV-based architecture,”2012.6.

[4] http://www.tandcca.com/about/page/12027

[5] 한국전파학회, “재난현장대응에 필요한 재난통신망 구축관련 상용망 구축 가능성”, 최종보고서, 2012.3

[6] 강신각, “디지털 사이니지 기반 재난대응 및 사회안전 표준기술”, 2014년 제2차 창조경제 ICT 융합포럼 2014.6.20

[7] 한국정보통신기술협회, “재난안전통신망 보안요구사항”, 2015.3

[8] 김희동, “디지털 사이니지를 통한 재난정보 전달방식”, 정보통신설비 학술대회 논문집, 2015.8

[9] W.Diffie and M.Hellman, “New Directions in Cryptography ,” IEEE Trans. On Inform. Theroy, vol22, pp644-655, 1976.

[10] M.J.Beller, L.F.Chang, and Y.Yacobi, “Privacy and Authentication on a Portable Communication System”, IEEE Journal on Selected Areas in Communication, vol.11, no.6, pp821-829, Aug.1993

[11] 채송화, “디지털 사이니지 기반의 콘텐츠 산업 현황과 전망”, 한국콘텐츠진흥원, 2012.6.20.

[12] 김찬, “디지털 사이니지 기술 현황 및 전망”, 한국통신학회지(정보와 통신), 2013.7

[저 자 소 개]

이 수 연 (Suyeon Lee)

1990년 단국대학교 전자계산학과 (이학사)
1993년 단국대학교 전산통계학과 대학원 석사(이학석사)
2003년 성균관대학교 전기전자 및 컴퓨터공학부 대학원 박사 (공학박사)
1997년 3월 ~ 현재 백석문화대학교 인터넷정보학부 교수

안 효 범 (Hyobeom Ahn)

1992년 단국대학교 전자계산학과 (이학사)
1994년 단국대학교 전산통계학과 대학원 석사(이학석사)
2002년 단국대학교 전산통계학과 대학원 박사(이학박사)
1997년 9월 ~ 2005년 3월 천안공업대학 정보통신과 부교수
2005년 3월 ~ 현재 공주대학교 정보통신학부 교수