http://dx.doi.org/10.14400/JDPM.2013.11.11.775

N-스크린을 위한 인증 및 보안 위협 해결 시스템

황득영*, 문정경**,김진묵**
강원대학교 컴퓨터공학과*, 선문대학교 IT교육학부**

A System of Authentication and Security threat solution for N-screen services

Deuk-Young Hwang*, Jeong-Kyung Moon, Jin-Mook Kim****
Dept. of Computer Engineering, Kangwoon National University*
Div. of IT Education, Sunmoon University**

요 약 N-스크린은 단일 컨텐츠를 다중 디바이스에서 시간 공간의 제약 없이 제공 받을 수 있는 서비스이다. 네트워크가 달라지거나 디바이스가 달라질 경우 혹은 플랫폼이 달라지는 경우에도 적합한 인증을 거쳐 디바이스에 맞는 영상을 끊김 없이 보낸다. 이에 따라 발생하는 보안 위협 요소로는 사용자 인증에 대한 문제가 발생한다. 이에 본 논문에서는 N-스크린의 특성상 발생하는 다중 디바이스에서 사용 가능한 인증 시스템을 제안하고자 한다. 기존의 인증기법 중 가볍고 처리 절차가 간단한 인증기법인 준동형 암호 알고리즘을 사용하여 사용자 인증을 간소화하였고, DATA의 무결성을 보장하고자 하였다. 또한 다중 디바이스를 사용하는 N-스크린 서비스의 특성상 장비 변경에 따른 추가 인증을 간편하게 처리하고자 하였다. 제안한 인증 프로토콜에 대한 효율성과 안전성에 대한 검토 결과, 암호 알고리즘을 처리하는데 작은 저장 용량과 낮은 프로세서에도 동작하기 쉽기 때문에 다중 디바이스를 사용하는 데 안전하고 적합하였다.

주제어 : N-스크린, 클라우드 서비스, 인증 서비스, 보안 위협요소, 정보보호 서비스,

Abstract N-screen is a Service that can be provide for One Service Multi Device. If the network is changed or if the device is changed after authentication the device fits seamlessly send footage. Security threats that occur here have a problem with user authentication. In this paper proposes available in a multi-device the authentication system. Homomorphic Encryption Algorithm of authentication scheme used. Among the authentication mechanism that already exists is a simple and lightweight authentication mechanism. In addition, N-screen service that uses multiple devices is simple authentication process of the device. Review the results of proposed authentication protocol, encryption algorithm to process a small storage capacity and is easy to work in low processor. And was suitable for use with multiple devices.

Key Words : N-screen, Cloud service, Authentication service, Security threats, Information secure service

Received 22 October 2013, Revised 20 November 2013
Accepted 20 November 2013
Corresponding Author: Jeong-Kyung Moon(Sunmoon University)
Email: moonjk@sunmoon.ac.kr

ISSN: 1738-1916

1. 서론

N-스크린은 AT&T에서 최초로 주장한 3-스크린에서 유래한 개념이다. 3-스크린이란 TV, PC, 네비게이션, 스마트폰을 인터넷으로 연결하여 사용자가 언제 어디서나 컨텐츠를 끊임없이 이용하게 해주는 서비스를 말한다. 현재는 IPTV, PC, 노트북, 스마트폰, 스마트패드 등의 장치가 서로 다른 네트워크에 접속되어도 영상, 음악, e-Book 등의 콘텐츠를 끊김 없이 이용할 수 있는 OSMU(One Source Multi Use)서비스를 제공한다. 또한 다양한 단말의 특성에 맞게 기능을 분할하여 수행하고, 이를 융합하는 양방향 협업서비스를 제공하고 있다. 그리고 통합 애플리케이션이 등장해 외부 공급자에게 컨텐츠를 공급받아 제공하는 서비스로 발전하고 있는 추세이다. N-스크린과 관련해 기술 표준화를 추진하는 OMA(Open Mobile Alliance)는 2011년 5월 개인융합통신서비스인 CPNS(Converged Personal Network Service)를 발표하였다. 이 서비스는 휴대폰, PC, TV, PMP, 디지털 액자, 무선-랜 프린터 등 다양한 디지털 장치를 하나의 네트워크로 연결할 수 있는 기술이다[1, 2].

〈Table 1〉 N-screen services

Categories		Service name
Telecommunication services	SKT	Hoppin
	KT	Olleh TV Now
	LG	U+ Box
Broadcasting services	KBS	K
	MBC	PooQ
	Payment-office	Tving
	Online-office	EveryOn

<표 1>은 국내 통신사와 방송사의 대표적인 N-스크린 서비스들에 대해서 나타냈다. N-스크린 서비스가 생겨나며 점차 경쟁이 치열해지고 있다. N-스크린의 확장의 일환으로 클라우드 활용을 강화하고 있다. N-스크린이 전략적으로 성공한 요인에는 스마트폰의 확산, 스마트TV의 출현 그리고 클라우드 컴퓨팅 환경의 발전을 들 수 있다[1]. 현재 N-스크린 서비스를 위한 단말의 표준은 ITU-T H.721(단말 기본 모델), TDES.3(고급 단말), TDES.4(IPTV 단말) 로 구분하여 표준개발이 추진되고 있다. 네트워크 구조 및 기능에 대한 표준화는 ITU-T SG13에서 담당하고 있다. 유무선 융합(FMC : Fixed and Mobile Convergence) 환경에서의 표준문서를 개발하고 있다[3, 4].

2. 관련연구

2.1 클라우드 서비스

클라우드 서비스란 네트워크로 연결된 물리적 자원을 논리적으로 연결하여 가상화 한 후 IT자원(서버, 스토리지, 응용프로그램 등)을 인터넷을 통해 서비스형태로 제공하고 사용한 만큼 비용을 지불하는 것을 말한다[5].

〈Table 2〉 Cloud computing models

Categories	Explain	Sample
SaaS	User can use the Cloud Software as a Service	Salesforce.com Google Docs
PaaS	Developer can use Cloud Platform as a Service	Google Appengine
IaaS	User can use Infrastructure as a Service	Amazon AWS

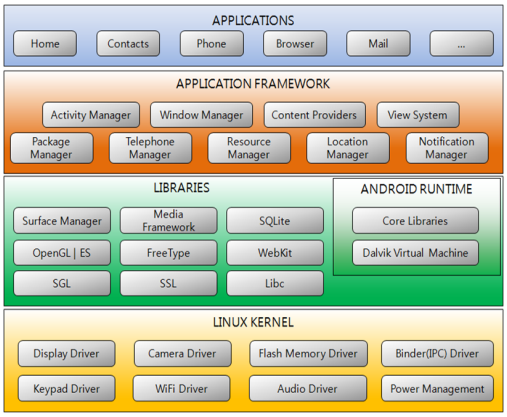
2.2 N-스크린 플랫폼

N-스크린 플랫폼이란, N-스크린 서비스를 구현하기 위한 기술로서 하드웨어 장치와 사용자인터페이스를 제공하기 위한 기초 기술을 말한다. 대표적인 플랫폼으로 안드로이드사의 안드로이드, 애플사의 IOS 플랫폼 등이 있다.

2.2.1 안드로이드 플랫폼

구글사를 중심으로 인텔, 차이나모바일, 삼성, 모토로라 등의 기업들이 연합체(OHA: Open Handset Alliance)를 결성하여 안드로이드 플랫폼을 개발하였다. 이것은 스마트폰 뿐 아니라 스마트TV에서도 크롬 브라우저 기반의 오픈형 TV플랫폼을 제공하여 안드로이드 기반 N-스크린 스마트 컨텐츠 전략을 발표하였다.

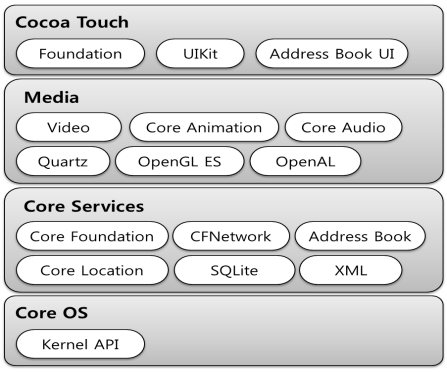
[그림 1]은 안드로이드 플랫폼을 나타내고 있으며, 애플리케이션 개발자들이 SDK(Software Development Kit)를 이용하여 스마트 단말 기능을 추상화시켜 필요한 기능을 사용할 수 있도록 하였다[6].



[Fig. 1] Android Platform(Ref: Atlas DB)

2.2.2 애플사의 IOS 플랫폼

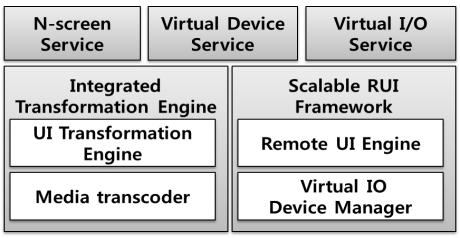
애플사는 PC, 스마트폰, 스마트TV, 스마트패드 장치를 위해서 자사의 아이튠즈(iTunes)를 사용한 IOS 플랫폼에서만 동작할 수 있도록 하여 독립적인 애플 생태계를 구축하고 있다.



[Fig. 2] IOS Platform

2.3 원격사용자 인터페이스

원격 사용자 인터페이스 기술은 원격에서 스마트 기기를 제어하는 기술이다. Native UI 전송방식과 Mark-Up 언어를 사용하는 방법이 있다. N-스크린용 원격 사용자 인터페이스 기술은 네트워크에 연결된 다양한 인터페이스를 표현하고 주변의 IO장치를 결합하여 가상의 IO를 제공하는 인터페이스 기술이다. [그림 3]은 N-스크린 원격 사용자 인터페이스 시스템 구조도이다.



[Fig. 3] Interface architecture of N-screen

[그림 3]에서 나타낸 바와 같이, 원격 사용자 인터페이스는 동적명령어 결합을 제공하는 Remote UI엔진과 IO 장치 성능에 따라 UI 생성 및 변환하는 UI변환 엔진, Networked IO 장치를 결합하여 가상의 IO를 제공하는 Virtual IO 장치 관리자 그리고 장치에 맞게 포맷 변환 및 경험 기반 필터링을 하는 미디어 트랜스코더로 구성된다[7].

3. 제안시스템

본 논문에서는 다중 장치에서의 사용자 인증을 가볍게 하기 위해 초기 등록시 장치를 등록하여 사용 중에 장치간 이동을 간편하도록 하였고, 간단한 인증기법인 준동형 암호 알고리즘을 사용하도록 하였다. 이를 통해 빠른 인증 처리 절차를 갖는다. 그리고 인증에 대한 신뢰도를 위해서 NAMS(N-screen Authentication Management Server)를 설계하였다. 이를 통해 인증을 간소화하고 중간자 공격과 같은 보안 위협을 해결할 수 있다.

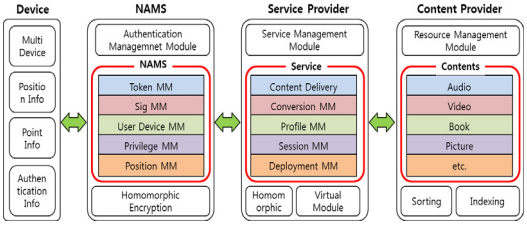
3.1 제안시스템 구조

본 연구에서 우리가 제안하는 N-스크린을 위한 사용자 인증 시스템의 구조는 콘텐츠 관리자, 서비스 관리자, 인증 시스템인 NAMS, 그리고 사용자들이 사용하는 장치들로 구성된다.

[그림 4]와 같이 N-스크린의 내부 구조를 보여준다. 각각의 구성 요소들의 역할과 기능은 다음과 같다.

콘텐츠 관리자의 역할은 영화, 드라마 등의 비디오자료와 음악파일, 그리고 그림과 신문이나 책과 같은 제작물 자료 등의 자료 보유하고 있는 컨텐츠 제공 업체에서 보유하고 있는 서버들과 디지털 자료들이다. 이 자료들

은 DB에 보관되고 서비스 관리자의의 요청에 따라 제공된다.



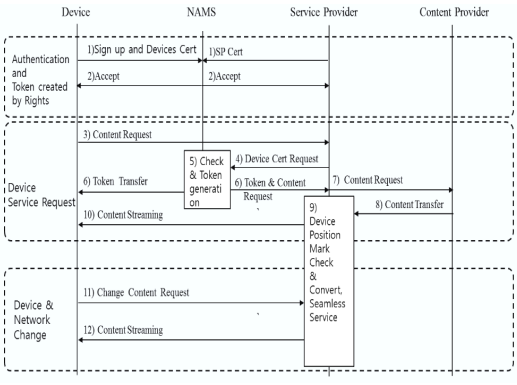
[Fig. 4] Architecture of proposed system

서비스 관리자는 정당한 인증을 거친 사용자의 요청에 따라서 콘텐츠 관리자로부터 디지털 자료를 전달받아 원활한 스트리밍 혹은 버퍼링 서비스를 제공하는 중간 관리자 역할을 수행한다.

본 논문의 가장 핵심 구조인 NAMS 에는 5개의 모듈을 갖는다. 사용자 토큰 관리 모듈, 서명 관리 모듈, 사용자 장치 관리 모듈, 권한 관리 모듈, 장치의 위치 관리 모듈이이에 대해서는 다음 절에서 동작절차에 대해 자세히 설명한다.

3.2 제안시스템 동작절차

전체적인 동작절차는 사용자 장치들에서 NAMS에 인증요청을 통해 사용자 인증 및 네트워크 상태에 대한 인증을 수행한다. 두 번째로 서비스 관리자가 서비스에 대해 인증을 수행하고 해당 콘텐츠 관리자에게 자료를 얻어 전달하도록 설계하였다.



[Fig. 5] Procedures of proposed system

사용자 인증과 서비스 인증을 수행하는 구체적인 동작절차는 [그림 5]에 나타냈다. 제안시스템은 독립된 인증 시스템을 가지고 있어 한 번의 등록으로 Device(이하 장치) 목록을 저장하여, 서비스를 요구할 때 생성되는 토큰에 장치 정보를 담고 있으므로 장치를 변경할 때마다 인증을 거쳐야하는 번거로움을 줄일 수 있다.

그리고 사용자 장치들에 대한 인증은 물론 SP를 인증함으로서 양방향 인증이 가능하다. 장치들에 대한 확인을 위해서 MAC(Media Access Code) 주소와 IP 주소, 그리고 최초 등록시 입력한 e-mail 주소를 암호화하여 사용하기 때문에 인증 확인과 함께 중간자 공격에 대한 대비가 가능하다.

NAMS는 사용자 인증을 위해서 아래와 같이 12단계의 인증처리 절차는 갖는다.

첫 번째 처리 절차는 회원가입과 인증 절차이다.

1) D -> NAMS : Login(User_Info)
   SP -> NAMS : Login(SP_Info)
2) NAMS -> D : Accept & Save
   User_Info : ϕSK{ID | PWD | Device(s) | e-mail}
   SP_Info : ϕSK{ID | PWD | Device}

사용자는 정당한 접속임을 확인받기 위해 자신의 정보와 각 장치에 대한 정보를 회원 가입할 때 입력한다. 정보 전송시 Homomorphic Encryption 알고리즘을 사용하여 암호화하여 전송한다. NAMS는 이를 허가하고 저장하여 차후 사용자 인증과 장치에 사용한다.

두 번째 처리 절차는 장치 서비스 요청과 전송 절차이다.

3) D -> SP : Content 요청
4) SP-> NAMS : 장치의 인증 요청
5) NAMS : 장치 확인 및 토큰발행
6) NAMS -> D & SP : 토큰 전달
   Token_Info : ϕSK{IP | De_MAC | Se_ID | De_GPS | nonce}
7) SP -> CP : Content_request
8) CP -> SP : Content_response
9) SP : 전송받은 De_MAC 주소를 사용하여 그에 맞게 변환하는 작업을 진행한다.
10) SP -> D : Content_Info 전송

Content_Info : ϕSK{Token_Info | Content}

이때 Token_Info 내부의 De_MAC과 GPS를 함께 가져감으로써 장치를 확인한다.

세 번째 처리 절차는 장치 변경 및 네트워크 변경시 처리 절차이다.

11) D -> SP : 장치 변경 혹은 추가 요청

장치 변경을 한 경우 토큰에 등록되어있는 장치정보를 확인하고, 인증이 되면 SP에 전달하여 장치에 맞는 변환을 거치도록 알린다.

12) SP -> D : 변환된 Content를 전송한다.

Content_Info : ϕSK{Token_Info | Content}

지금까지 본 논문에서 제안한 사용자 인증과 보안위협 요소인 중간자 공격에 대비하기 위한 절차에 대해서 수식과 함께 간단한 설명에 대해서 기술하였다.

4. 실험 및 고찰

4.1 실험 시나리오 1

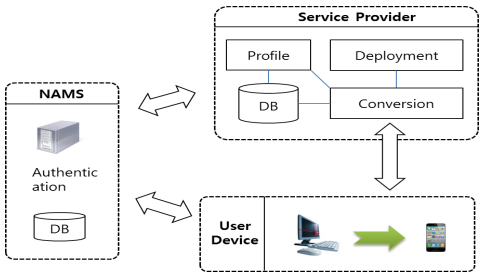
첫 번째 실험은 사용자가 기존에 사용하던 스크린 장치를 다른 장치로 변경해서 지속적인 N-스크린 서비스를 이용하기를 원하는 경우에 대한 실험이다.

1) 사용자가 PC로 드라마를 보고 있다가 스마트 폰으로 변경한다.
2) Profile Management가 장치가 달라진 것을 인식하고 확인하고 이를 알린다. 이때 이어보기 포인터를 함께 전송한다.
3) Conversion Management Module에서 장치에 따른 변환을 한다.
4) Content Delivery Module이 변환된 자료를 장치로 전송한다.

4.2 실험 시나리오 2

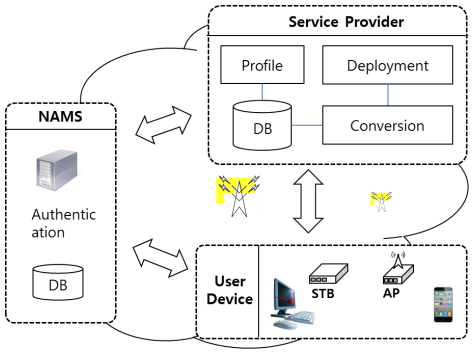
두 번째 실험은 사용자가 사용하는 단말장치는 동일하나 위치를 이동하여 네트워크가 변경된 경우에 대한 실험이다.

1) 사용자가 스마트 폰을 보면서 이동하던 중 네트워크가 변경되었다.



[Fig. 6] Experiment scenario of device change

2) Profile Management가 네트워크가 달라진 것을 인식하고 확인하고 이를 알린다.
3) 네트워크 확인 후 네트워크 제공자의 최적의 서비스를 제공한다. 라우터 내의 STB(Set Top Box)나 AP(Access Point) 등의 리스트에서 최적의 서비스를 선택할 수 있다.
4) Content Delivery Module이 전송을 계속한다.



[Fig. 7] Experiment scenario of network change

4.3 고찰

위에서 제안한 2가지 실험 시나리오에 따라 제안 시스템이 보안성과 무결성, 서비스 거부 공격 그리고 사용자 인증 서비스를 제공하는지 여부를 검토하였다.

1) NAMS에 최초 사용자 정보와 장치 정보 전달할 때와 토큰 전송시 Homomorphic Encryption 알고리즘을 사용한다. 그리고 Content 정보를 제공할 때에 토큰 정보와 Content 정보를 다시 한 번 암호화 하여 전송함으로서 보안성과 무결성 서비스를 제공한다.
2) 장치나 네트워크 변경을 할 때 악의적으로 접속을 시도하는 공격에 대해 De_MAC 리스트를 확인함으

로서 공격을 차단할 수 있다. 그러므로 서비스 거부 공격(DoS)에 대한 공격에 대비할 수 있다.

3) 인증기관인 NAMS에 신분 인증을 한 후 장치를 등록하는 단계를 거친다. 그러므로 사용자 인증과 함께 장치 인증 서비스를 제공한다. 장치 정보는 토큰 요청시 암호화 하여 전달함으로서 Content 전달 도중 다시 확인을 거치지 않고 자체적으로 제어할 수 있다.[그림1]은 안드로이드 플랫폼을 나타내고 있으며, 애플리케이션 개발자들이 SDK(Software Development Kit)를 이용하여 스마트 단말 기능을 추상화시켜 필요한 기능을 사용할 수 있다.

5. 결론

본 논문에서는 N-스크린 서비스 이용시 드라이브가 변경되거나 네트워크가 변경되어도 끊김 없는 서비스를 제공하며, 사용자 인증과 장치의 인증이 빠르게 진행될 수 있도록 시스템을 설계하였다. 기존의 여러 가지 인증 방법 중 준동형 암호 알고리을 사용하여 인증을 간소화 하였다.

최초 인증기관에 사용자 등록과 장치 등록을 하고, 등록된 정보를 암호화한다. 콘텐츠 요청시 장치 정보들을 암호화하여 토큰에 포함하여 전달하고, 이를 장치에 등록하여 NAMS를 거치지 않고 바로 인증할 수 있도록 하였다.

N-스크린은 클라우드 기반 위에서 새로운 서비스를 생산, 유통, 가공함으로서 차세대 미디어 혁명에 대처할 수 있도록 하기 위하여 안전하고 간소한 인증구조를 가져야 한다. 본 논문에서 제안한 시스템은 현재의 클라우드 기반 구조에서 사용자에게 안전하고 간편한 양방향 서비스를 제공함으로서 N-스크린의 보급화와 새로운 분야의 발전을 기대할 수 있다.

REFERENCES

[1] Jong-Seol Lee, Se-Jin Jang, Seok-Pil Lee, Design and Implementation of personalized service in the 3-screens environment, The Korean Society of Broadcast Engineers, pp.337-380, 2010.7.

[2] Hun-gyu Park, Se-Jun Park, Jeong-Bae Kim, KT's N-Screen Business Status and Evolution, Korea Information Processing Society, Vol. 19. No. 1, pp.72-76, 2012.

[3] Jin-Mook Kim, A Security Trend and Future works of N-Screen, The Korea Contents Association, Vol. 4, No. 9, pp.40-48, 2012

[4] Sin-Gak Kang, N-Screen Technology Standardization, It's Smart Media, Vol. 1, No. 3, pp.56-61, 2012.

[5] Jeong-Kyung Moon, Jin-Mook Kim, Hwang-Rae Kim, An efficient user authentication protocol for cloud computing environments, Journal of the Korea Academia-Industrial cooperation Society, Vol. 12, No. 5, pp.2353-2359, 2011.

[6] Heon-Ju Lee, Seok-Won Lee, Jun-Woo Lee, Chang-Jun Park, N-screen service for the development of key technologies and content direction, The Korea Contents Association, Vol. 19. No. 1, pp9-18, 2012.

[7] Tae-Yeon Gu, Yu-Seok Bae, Bong-Jin O, Jong-Yeol Park, N-screen service for remote user interface technology, It's Smart Media, Vol. 1, No. 3, pp.42-47, 2012.

황 득 영(Hwang, Deuk-Young)

- 1988년 2월 : 광운대학교 전자계산학과(이학사)
- 1990년 2월 : 광운대학교 전자계산학과(공학석사).
- 1999년 2월 : 광운대학교 전자계산학과(공학박사)
- 1990년 3월 ~ 1994년 2월 : 전주기전대학교 전자계산학과 조교수
- 1994년 3월 ~ 현재 : 강원대학교 삼척캠퍼스 컴퓨터공학과 교수
- 관심분야 : 프로그래밍 언어, 컴파일러, 정보보안, 클라우드 컴퓨팅, N-스크린
- E-Mail : dyhwang@kangwon.ac.kr

문 정 경(Moon, Jeong-Kyung)

- 1993년 2월 : 배재대학교 원예학과 (학사)
- 2006년 2월 : 단국대학교 인터넷정보학과(공학석사).
- 2013년 2월 : 공주대학교 컴퓨터공학과(공학박사)
- 2012년 3월 ~ 현재 : 선문대학교 IT 교육학부 계약교수
- 관심분야 : 클라우드 컴퓨팅, N-스크린, 네트워크, 정보보안
- E-Mail : moonjk@sunmoon.ac.kr

김 진 묵(Kim, Jin-Mook)

- 1998년 2월 : 배재대학교 전자계산학과(공학사)
- 2000년 2월 : 배재대학교 컴퓨터공학과(공학석사).
- 2006년 2월 : 광운대학교 컴퓨터과학과(공학박사)
- 2006년 9월 ~ 2008년 2월 : 선문대학교 컴퓨터공학과 연구교수
- 2008년 3월 ~ 현재 : 선문대학교 IT교육학부 조교수
- 관심분야 : 유.무선 네트워크, 센서네트워크, 정보보안, N-스크린
- E-Mail : calf0425@sunmoon.ac.kr