국내 DLNA 인증 제품의 보안 취약점 및 해결책 연구

오지수*, 민재원*, 한선희*, 정태명**
* 성균관대학교 전자전기컴퓨터공학과
** 성균관대학교 정보통신공학부
e-mail : {jsoh, jwmin, shhan}@imtl.skku.ac.kr*, tmchung@ece.skku.ac.kr**

A Study on Security Vulnerabilities and Countermeasures of Domestic Product Certified by DLNA

Ji-Soo Oh*, Jae-Won min*, Sun-Hee Han*, Tai-Myoung Chung**
* School of Information Communication Engineering, SungKyunKwan University
** Dept. of Electrical and Computer Engineering, SungKyunKwan University

요 약

홈 네트워크 시스템에서 여러 기업간의 상호 운용 프레임워크를 제공하기 위하여 DLNA(Digital Living Network Alliance)가 결성되었다. DLNA 에서는 기기 간 상호운용을 위한 가이드를 제시하여 업체간의 통합을 목표로 한다. DLNA 인증을 받은 제품은 유· 무선 통신을 통해 기기 간에 컨텐츠를 공유하는 홈 네트워크 시스템을 제공한다. 하지만, 유· 무선 통신으로 컨텐츠를 공유할 때 공유기의 비밀번호를 사용하지 않은 경우, 인증되지 않은 외부 침입자가 사용자의 컨텐츠에 접근할 수 있는 보안 상 취약점이 있다. 본 논문에서는 이러한 취약점을 시나리오로 기술하고, 그에 따른 해결방안을 제안하여 안전한 홈 네트워크 시스템 구축에 도움을 주고자 한다.

1. 서론

언제 어디서나 네트워크에 접속할 수 있는 유비쿼터스 환경의 구현을 목표로 하여, 전자정부가 구축되고 u-city 가 지속적으로 개발되고 있다. 최근 기업에서도 이러한 유비쿼터스 실현을 목표로 많은 프로젝트들을 진행하고 있는데, 이 중의 하나가 홈 네트워크 시스템이다. 홈 네트워크 시스템은 가정에서 쓰이는 모든 전기, 전자 제품들이 네트워크에 연결되어 하나의 시스템을 구성하고, 이로써 기기간에 컨텐츠를 공유할 수 있는 시스템을 의미한다. 홈 네트워크 시스템에서 기기 간 공유되는 컨텐츠에는 사용자의 개인정보가 다수 포함되어 있기 때문에, 이 시스템에서의 보안 문제는 다른 무엇보다 중요하게 다뤄져야 한다.

DLNA(Digital Living Network Alliance)는 가전, 컴퓨터, 이동통신 단말기 제조 업체간의 홈 네트워크 상호 운용 프레임워크를 제공하는 단체이다. DLNA 에서는 네트워킹, 디바이스 발견 및 제어, 미디어 관리, 미디어 포맷, 미디어 전송 등에서의 상호운용을 위한 가이드를 제시하여 업체간의 통합을 목표로 하고 있다. 삼성, LG, 소니, 노키아, 마이크로소프트 등 200 여 개 업체가 참여하고 있으며, DLNA 는 업계 표준을 토대로 서로 호환 가능한 플랫폼을 통해 업계간 통합을 목표로 하고 있다.[4] DLNA 에서는 제품들이 서로 같이 작동할 수 있음을 소비자에게 알리기 위하여 Certification and Logo 프로그램을 진행하고 있다. DLNA 인증을 받았다는 것은 서로 상호운용 가능하다는 것을 의미하며, DLNA 인증 제품은 컨텐츠를 USB 에 업로드하여 다른 기기에서 다시 다운로드하는 복잡한 방식에서 벗어나, 기기간 유· 무선 통신을 통해 컨텐츠를 공유하는 서비스를 제공할 수 있다. 국내에서 DLNA 인증을 받은 대표적인 제품은 스마트 TV, 스마트폰, 노트북 등이 있다. 최근 국내에서 출시된 스마트 TV 제품들은 대부분 기본적으로 DLNA 기반의 컨텐츠 공유 기능을 제공하고 있다. 스마트 TV 의 개발 및 판매가 활성화된 시점에서, DLNA 인증 제품간 컨텐츠 공유 기능의 보안 문제 또한 활발히 다뤄져야 할 문제이다.

스마트 TV 에서 DLNA 기반 컨텐츠 공유 기능을 사용하기 위해서는 유· 무선 공유기를 이용해서 PC, 스마트폰 등의 다른 DLNA 인증 기기들과 연결 되어야 한다. 만약 공유기에 비밀번호가 설정되어있지 않은 경우, 인증되지 않은 사용자도 공유기에 접속할 수 있다. 따라서 컨텐츠 공유 프로그램이 실행 중일 때마다, 인증되지 않은 사용자도 공유 잠금이 풀려있는 모든 컨텐츠에 접근 할 수 있기 때문에 개인정보가 유출될 위험이 있다. 이러한 위험을 제거하고 보안을 향상시키기 위해서 본 논문에서는 DLNA 기반 홈 네트워크 시스템의 보안 문제점에 대한 해결책을 제안한다.

본 논문의 구성은 다음과 같다. 2 장에서는 DLNA 의 목적과 제공하는 상호 운용 프레임워크 그리고 DLNA 인증 제품의 국내 현황 등을 설명한다. 3 장에

서는 DLNA 기반 컨텐츠 공유 기능을 사용할 때 발생할 수 있는 보안 상의 문제점에 대해 설명하고, 그에 따른 해결책을 제시하며 4 장에서 결론을 맺는다.

2. DLNA (Digital Living Network Alliance)

본 장에서는 DLNA 에서 제공하는 Certification and Logo 프로그램에 대해 설명하고, DLNA 가이드라인에서 설명하는 디바이스 카테고리 및 클래스에 대해 기술한다. 본 장의 마지막 절은 국내에 출시된 DLNA 기반 제품 현황에 대해 설명한다.

2.1 DLNA Certification and Logo 프로그램

DLNA 에서는 소비자가 구매한 제품간의 상호 작동을 확신할 수 있도록 Certification and Logo 프로그램을 제공한다. PC 뿐만 아니라 기타 가전에서도 상호호환성을 제공하기 위한 시스템이라고 볼 수 있다. 모든 DLNA 회원은 인증신청을 할 수 있으나, 인증신청 전에 적합성 시험을 통과해야 한다. 적합성 시험을 통과한 다음 UPnP 와 Wi-Fi 에 대한 인증까지 완료해야 DLNA 로고를 받을 수 있다. DLNA Certification and Logo 프로그램을 통해 인증을 받은 제조업체의 제품은 DLNA 로고를 마케팅에 사용할 수 있다[2].

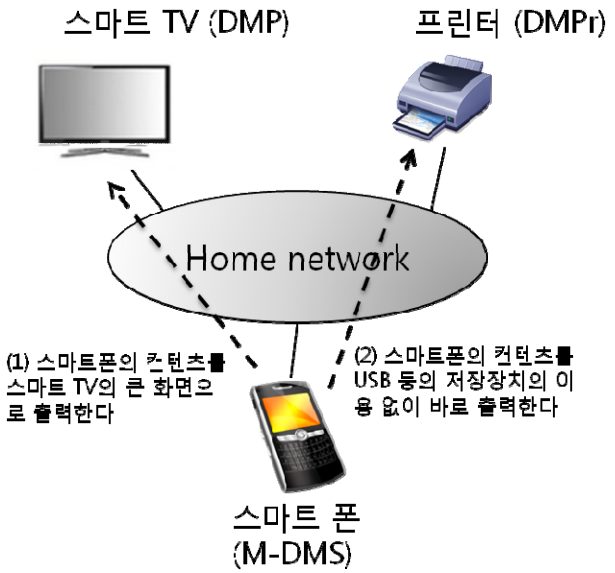
2.2 DLNA 디바이스 카테고리 및 디바이스 클래스

DLNA 는 홈 네트워크 시스템에서 미디어의 공유와 제어를 수행하는 디바이스들을 3 가지 카테고리로 분류하는데, 각각의 카테고리는 Home Network Device, Mobile Handheld Device 그리고 Home Infrastructure Device 이다. 각 디바이스 카테고리의 디바이스 클래스가 <표 1>에 정의되어 있다. <표 1>의 첫 번째 카테고리인 Home Network Device 의 한 클래스인 DMS 는 컨텐츠를 네트워크에 등록하고 분배하는 역할을 한다. PC, 홈시어터 등이 DMS 의 예이다. DMP 는 DMS 의 컨텐츠를 찾아 DMR 에 재생할 수 있도록 하고 DMR 과 DMS 사이의 연결을 유지시킨다. 스마트 TV 가 대표적인 DMP 이다. DMPr 은 이미지를 프린트하는 디바이스를 말한다. <표 1>의 두 번째 카테고리인 Mobile Handheld Device 의 M-DMS, M-DMP, M-DMC 는 각각 Home Network Device 카테고리의 DMS, DMP, DMC 와 기능이 같고 M-DMU 는 M-DMS 에 컨텐츠를 업로드하며, M-DMD 는 M-DMS 가 등록한 컨텐츠를 다운로드하는 기능을 한다. DLNA 인증을 받은 스마트폰이 Mobile Handheld device 카테고리의 모든 클래스의 기능을 가진다. Home Infrastructure Device 는 Home Network Device 와 Mobile Handheld Device 두 카테고리의 디바이스 간 상호 운용성을 제공하는 카테고리이다. M-NCF 는 서로 다른 네트워크에 대한 연결성을 보장하고 MIU 는 미디어 형식을 변환해준다.

예를 들어, DLNA 인증을 받은 스마트 TV, 스마트폰, 프린터가 있다면 사용자는 스마트폰에 있는 컨텐츠를 따로 USB 에 옮겨 스마트 TV 에서 실행시킬 필요 없이, 바로 DLNA 기반의 컨텐츠 공유 프로그램을 사용하여 스마트 TV 의 큰 화면으로 실행시킬 수 있다. 또한, 프린터를 이용할 때도 PC 로 컨텐츠를 옮길 필요 없이, 스마트폰과 프린터 간에 컨텐츠를 공유함으로써 (그림 2)와 같이 곧바로 출력할 수 있다. 여기서 스마트폰은 컨텐츠를 등록하는 M-DMS 클래스에 속하고 스마트 TV 와 프린터는 각각 DMP, DMPr 클래스에 속한다고 볼 수 있다.

<표 1> DLNA 디바이스 카테고리 및 클래스 [1]

Device Category	Device Classes
Home Network Device	Digital Media Server (DMS)
	Digital Media Player (DMP)
	Digital Media Renderer (DMR)
	Digital Media Controller (DMC)
	Digital Media Printer (DMPr)
Mobile Handheld Device	Mobile Digital Media Server (M-DMS)
	Mobile Digital Media Player (M-DMP)
	Mobile Digital Media Renderer (M-DMR)
	Mobile Digital Media Uploader (M-DMU)
	Mobile Digital Media Downloader (M-DMD)
Home Infrastructure Device	Mobile Network Connectivity Function (M-NCF)
	Media Interoperability Unit (MIU)



(그림 2) DLNA 기반 컨텐츠 공유 예시

2.3 국내 DLNA 인증 제품 현황

국내의 DLNA 대표 기업으로 삼성과 LG 를 들 수 있다. 두 기업 모두 스마트 TV 를 출시 하였고, 이 스마트 TV 에 모두 DLNA 기반의 컨텐츠 공유 기능을 제공하여 다른 DLNA 인증 제품과의 공유가 가능하도록 하고 있다. 삼성에서는 AllShare 프로그램을, LG 에서는 SmartShare 프로그램을 제공한다[5,6]. 스마트 TV 뿐만 아니라 노트북과 스마트폰도 DLNA 인증을

받아 제품 간 컨텐츠 공유가 가능하게 되었고, 홈 네트워크 시스템의 구성을 통해 국내 유비쿼터스 실현에도 한발 다가섰다.

3. DLNA 공격 시나리오 및 해결책

유비쿼터스의 실현을 위해 개발된 홈 네트워크 시스템은 가정에서의 편리함이 제공되는 대신, 외부로 유출되지 않던 개인 정보에 외부의 접근이 가능해지는 위협이 존재한다. DLNA 기반 홈 네트워크 시스템에서 스마트 TV, 스마트폰 등의 디바이스는 사진, 영상 등의 컨텐츠를 유· 무선 통신으로 공유하여 복잡한 과정 없이 컨텐츠를 사용할 수 있다. 그러나 외부에서도 이 공유 컨텐츠에 접근할 수 있어서 개인정보 유출을 야기하는 보안상의 취약점이 존재한다.

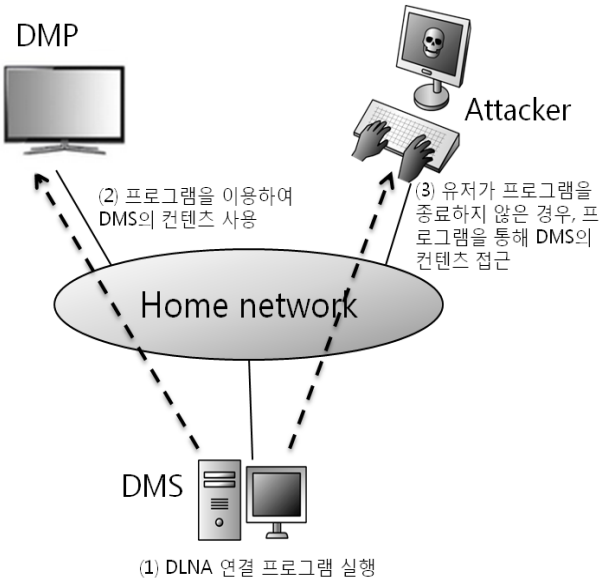
국내의 DLNA 인증 제품들은 컨텐츠를 공유하기 위해서 동일한 유· 무선 공유기에 접속해야만 한다. 컨텐츠에 외부의 접근을 막기 위해서 컨텐츠의 공유를 잠금 시키는 방법이 있으나, 이런 경우에는 인증된 사용자도 컨텐츠를 사용할 수 없다는 단점이 있다. 공유기에 비밀번호를 설정해서 비밀번호를 알고 있는 사용자만 연결할 수 있도록 하는 방법이 있으나, 공유기 사용에 익숙하지 않은 사용자들이 비밀번호를 설정하지 않고 사용하여 외부 접근에 무방비하게 노출되어 있는 경우가 많다. 비밀번호를 설정해두지 않고 DLNA 공유 기능을 사용하게 되면, DLNA 인증 제품을 사용하는 공유기 범위 안의 다른 사용자들도 그 사용자의 개인정보에 접근할 수 있게 된다. 시나리오 1, 2 를 통해 공격 가능한 상황에 대해 설명한다.

3.1 시나리오

● **시나리오 1**

(그림 3)은 DLNA 인증 제품을 사용하는 다른 사용자 또는 공격자가 개인정보에 접근하는 시나리오를 보여준다. 먼저, 사용자는 컨텐츠를 사용하기 위해서 DMS 에서 컨텐츠를 공유하는 프로그램을 실행시킨다. DMC, M-DMC 를 이용하여 '해당 기기를 통해 서버의 미디어를 다른 기기에서 재생'하는 기능으로 스마트 TV 에서 DMS 의 컨텐츠를 사용하거나, 스마트 TV 에서 직접 '다른 기기의 미디어를 해당 기기에서 재생' 기능을 실행 하는 등의 방법으로 컨텐츠를 사용한다. 일반적으로 사용자는 컨텐츠를 사용하고 난 후 DMS 의 프로그램을 종료하지만, 프로그램을 종료하지 않고 계속해서 TV 시청을 하는 등의 상황이 발생할 수 있다. 이런 경우 공유기에 접속할 수 있는 범위 안의 다른 DLNA 인증 제품에서도 사용자의 DMS 를 인식할 수 있고, 공격자가 일반 사용자의 컨텐츠를 사용할 수 있다. 악의적 목적을 가지지 않더라도 사용자의 공유기에 외부 접속이 있을 수 있기 때문에 컨텐츠 유출의 위험이 크다

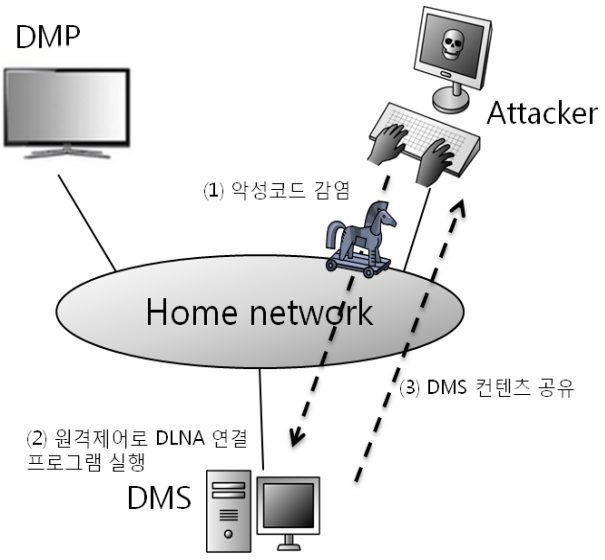
예를 들어 국내의 경우에는 삼성에서 제공하는 AllShare 서비스에서 이러한 시나리오가 가능하다. DMS 에서 PC Share Manager 프로그램을 실행시키고 삼성 스마트 TV 에서 AllShare 기능을 사용함으로써 (그림 3)에서 설명하는 시나리오가 실제로도 적용될 수 있다.



(그림 3) 시나리오 1

● **시나리오 2**

(그림 4)는 사용자가 DMS 에서 DLNA 시스템을 전혀 이용하지 않았음에도 컨텐츠가 유출되는 시나리오이다. 공격자는 먼저 사용자의 DMS 를 악성코드에 감염시킨다. 트로이 목마 등의 악성코드는 사용자의 DMS 에 백도어를 생성한다. 공격자는 이 백도어를 통해 DMS 를 원격제어 할 수 있으며, DMS 에서 DLNA 연결 프로그램을 실행시킬 수 있다. 프로그램이 실행되면 공격자는 아무런 방해 없이 DMS 의 컨텐츠에 접근하여 사용할 수 있다. DLNA 기반의 컨텐츠 공유 프로그램을 사용하는 경우, 사용자의 컴퓨터에서 공격자의 컴퓨터로 컨텐츠를 업로드 및 다운로드 하는 등의 복잡한 과정 없이 바로 컨텐츠를 사용할 수 있기 때문에 단순히 원격제어를 하는 경우 이상의 피해가 빠른 시간 내에 발생시킬 수 있다.



(그림 4) 시나리오 2

3.2 취약점에 대한 해결책 제안

DLNA 기반의 홈 네트워크 시스템에서 컨텐츠를 공유하기 위한 유· 무선 공유기에 비밀번호가 없는 경우 발생하는 보안상의 문제점을 해결하기 위해서는, 1 차적으로 공유기 비밀번호의 사용을 강력히 권고해야 한다. 일반 사용자들은 개인정보 보안의 중요성을 크게 인식하지 못할 수 있다. 그래서 사용자에게 보안의 중요성과 공유기 비밀번호 사용의 필요성에 대해 강조하여 강력히 권고하거나, 사용자가 비밀번호를 강제적으로 설정하도록 해야 한다.

또한, 공유기에만 비밀번호를 둘 것이 아니라, 2 차적으로 비밀번호를 입력하는 시스템을 두어야 한다. 아이디와 비밀번호를 입력하여 로그인을 하는 시스템도 가능하고, 사용자가 기밀이라고 생각하는 특정 자료에 대해서만 따로 비밀번호를 입력하여 한번 더 인증을 받을 수 있는 시스템도 컨텐츠 보안을 향상시킬 수 있다.

인증 받은 사용자가 사전에 등록한 제품만 홈 네트워크에 접근할 수 있도록 제어하는 방법도 가능하다. 단말기 MAC 주소로 이루어진 데이터베이스를 구성하여, 데이터베이스에 등록되어 있지 않은 외부 접근을 차단하는 것이다.

이러한 시스템의 도입으로 DLNA 인증 제품들의 보안이 향상되고 사용자는 보다 안전하게 DLNA 기반의 컨텐츠 공유 시스템을 사용할 수 있게 될 것이다.

4. 결론

지금까지 본 논문에서는 DLNA 기반 홈 네트워크 시스템에서 기기 간 컨텐츠를 공유할 때 발생할 수 있는 보안상의 문제점과 그에 따른 해결방안에 대해 살펴 보았다. DLNA 인증 제품은 앞으로 스마트 TV 의 보편화와 함께 점점 많이 사용될 것으로 전망되며, 홈 네트워크 시스템에서 공유되는 컨텐츠가 중요한 개인정보라는 점에서, DLNA 인증 제품의 공유 컨텐츠 보안이 보다 강조되어 중요하게 다뤄져야 할 것으로 보인다. 본 논문에서 제안된 해결책은 사용자가 컨텐츠를 사용할 때의 편이성과 결합되어 보완이 되어야 한다. 또한 조금 더 편리하면서 향상된 보안을 제공하기 위한 새로운 기술에 대한 적극적인 연구 또한 필요할 것이다.

참고문헌

[1] 강기철, “홈 미디어 기기의 DLNA 소프트웨어 효율적 적용” , 방송공학회논문지 제 17 권 제 1 호, Jan 2012

[2] 임형수, “DLNA 시험인증제도”, TTA 저널 104 122-128, 2006

[3] 박준희, “홈네트워크 미들웨어 기술 및 표준화 동향”, 전자통신동향분석 제 19 권 제 5 호 통권 89 호 (2004. 10) pp.53-58 ISSN 1225-6455, Oct 2004

[4] DLNA, “http://www.dlna.org/”, Mar 2012

[5]삼성, “http://www.samsung.com/sec/consumer/themes/allshare/index.html”, Mar 2012

[6] LG, “http://kr.lgappstv.com/appspc/overview/overview/moveUsageIntroView.lge”, Mar 2012