Smart TV 구조 및 취약점 동향 분석

김지훈, 손강원, 윤종희
영남대학교 컴퓨터공학과
e-mail : youn@yu.ac.kr

Smart TV structure & vulnerability trend analysis

Ji-Hun Kim, Kang-Won Son, Jonghee M. Youn
Dept of Computer Engineering, Yeungnam University

요 약

최근 급속도로 기술이 발전하면서 스마트폰, 태블릿 등 스마트 기기의 보급률이 늘어나고 있다. 스마트TV, 스마트청소기, 스마트세탁기 등 가정에서 사용하는 가전제품으로 그 영역이 늘어나고 있는데 특히 Smart TV의 보급률이 늘어나고 있다. 네트워크인터페이스의 제공과 USB를 통한 펌웨어 업데이트 등 SmartTV의 기능적인 측면 때문에 Smart TV 대한 Dos공격부터 펌웨어 취약점 공격 등의 여러 형태의 보안문제가 발생하고 있다. 본 논문에서는 Smart TV시장에서의 점유율 1위를 기록하고 있는 Samsung SmartTV의 구조 및 보안문제 동향을 분석해 본다.

1. 서론

SmartTV의 사전적 의미는 운영체제와 중앙처리장치를 탑재하고, 인터넷 접속 기능을 결합한 다기능 TV이다. 쉽게 말하면 TV와 PC의 결합이라고 볼 수 있다. 디스플레이 시장조사기관 디스플레이서치에 따르면 Smart TV 보급률이 2014년에는 약 1억2천만대 수준으로 전체 TV시장의 40%이상의 수준이 될 것으로 예측하고 있다. 하지만 SmartTV의 보급률은 높아지지만, 스마트폰이나 컴퓨터와는 달리 보안문제에 대해 크게 인지하지 못하는 경우가 대부분이다. SmartTV가 네트워크 인터페이스 사용이 가능함에 따라 다른 컴퓨터나 네트워크에서 사진, 영화, 음악 등을 전송받을 수 있고, 비디오나 오디오 스트리밍을 위한 인터넷기반 서비스를 제공한다. 그리고 USB 인터페이스가 제공되고 스마트폰이나 태블릿과 같은 어플로의 무선조정이 가능하다. 이러한 SmartTV의 여러 가지 기능적인 측면 때문에 해커들은 여러 방법으로 접근 또한 가능하다. 이로써 티비싱(TV와 Pishing의 합성어, 해커가 TV를 조작할 수 있는 것)으로 가정에서는 사생활 침해, 회사에서는 중요한 기밀정보들이 외부로 유출되는 피해를 받을 수 있다. 본 논문의 2장은 SamyGO 프로젝트 단체[1]를 소개하고, SamyGO에서 배포하고 있는 patcher를 통해 암호화된 Firmware를 복호화해본다. 3장은 Firmware patcher를 이용해 복호화 된 Firmware를 통해서 SmartTV(모델 : T-MST10PDEUC) Firmware의 구조를 알아 본다. 4~6장은 최근 2년(2012년~2013년) 간의 화두가 된 보안문제동향을 살펴볼 것이고, 7장은 결론으로 끝을 맺는다.

2. SamyGO

Samsung SmartTV의 Firmware는 다운로드 되거나 USB를 통해서 설치된다. 암호화방법(AES + XOR)로 펌웨어는 열어 볼 수 없게 되어 있는데 SamyGO는 대부분의 Samsung Firmware를 복호화/암호화를 할 수 있는 Firmware python patcher tool[2] 등을 개발, 배포하고 있다. SamyGO는 Firmware rooting과 Firmware Reverse Engineering의 관심을 공통으로 하는 사람들이 모여 포럼 형태로 운영되고 있다.

그림 1. Firmware patcher를 이용한 복호화 파일.

3. Samsung SmartTV Firmware 구조

2장에서 SmartTV모델 e시리즈 T-MST10PDEUC을 SamyGO Firmware patcher를 이용해 복호화 된 펌웨어를 살펴본다. 목표는 암호화된 roofts, appext.img, exe.img를 복호화하는 것이다. patcher를 통해 복호화하여 내부를 들여다 본다. rootfs.img와 appext.img는 각각 파

일 시스템과 데이터/프로그램 이미지이며 exe.img는 Wifi 등 하드웨어 드라이버를 지원하는 Library와 시스템의 부팅순서가 정의된 파일들이 포함되어 있다. 그림2는 T-MST10PDEUC의 Firmware 구조를 간단히 도식화 한 것이다.

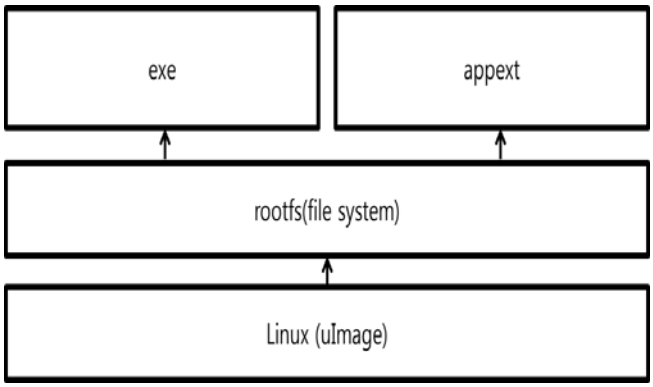

그림 2. 모델 T-MST10PDEUC의 Firmware 구조

4. Long String Vulnerability

2012년 4월 이탈리아의 루이지 알리엠마(Luigi Auriemma)는 Samsung D6000의 모델을 대상으로 하여 MAC 주소와 같은 필드를 긴 문자열 또는 유효하지 않은 문자열로 지정하면 무한 루프에 빠져 5초마다 TV가 꺼졌다 켜졌다를 반복하게 되고 결국 TV의 기능이 정지됨을 보였다. 또한 이 취약점은 로컬 네트워크 상에서 나타난 문제이고, 이것이 인터넷을 통해서도 가능한지는 불분명하지만 D6000 TV 상에 개방되어 있는 TCP 포트만 40개 이상이다. 이것은 집에 설치된 와이파이 네트워크와 연결된 TV의 경우 무선랜을 통해 외부에서도 공격이 가능하다는 것이다. Samsung SmartTV의 원격제어 기능은 인터넷 접속 기능이 있는 Samsung Entertainment Device들에 기본으로 내장되어 있다. Samsung Remote Application이라는 앱을 스마트폰에 설치해서 이용하면 아이패드와 안드로이드 디바이스에서 원격제어 가능하다. 알리엠마는 최신 펌웨어가 설치된 삼성 D6000 TV를 대상으로 테스트 했지만 해당 앱이 지원하는 다른 기기도 마찬가지로 취약 할 것으로 예측하였다.

5. IP address HTTP GET Vulnerability

2013년 7월 보안전문가 말릭 미셀름(Malik Mesellem)은 공격자가 TV의 IP주소의 취약점을 통해 TV가 재부팅이 되고 DoS(Denial of Service)공격을 성공하였다. 미셀름은 이를 입증하기 위해 Samsung PS50C7700을 대상으로 하여 TV의 IP주소로 길이가 긴 HTTP GET 요청을 보내는 경우 TCP/5600 포트에 설정된 웹 서버(DMCRUIS/0.1)에 이상이 발생해 TV가 재부팅 되었다. TV는 Ethernet Cable을 통해 홈 네트워크로 연결됐고 공격자는 TV를 공격하기 위해서 TV가 연결된 LAN에만 접근하면 가능하다는 것을 의미한다. TV가 연결된 LAN에 접근하기 위해서는 무선 액세스 포인트를 통해 침입하거나 동일한 네트워크에 있는 컴퓨터에 악성코드를 감염시키기만 하면 된다. 해당 취약점은 CVE-2013-4890로 등록 됐다.

6. Camera Hooking program

2013년 8월 미국 라스베이거스에서 열린 해킹 컨퍼런스인 '블랙 햇'에서 한국의 이승진(Seung-jin Lee)은 Smart TV의 플랫폼을 Reversing 하여 Smart TV app store와 Network Interface의 취약점을 발표하였다. 이승진은 ARM코드 기반의 Hooking Program을 제작 후 탑재되어 있는 카메라를 시청자를 몰래 녹화, 녹음 한 후 이를 인터넷으로 생중계하는 것을 실제로 시연하였다. SmartTV의 플랫폼이 Linux 기반의 O/S를 사용하고 있다는 것을 토대로 볼 때 Smart TV 플랫폼이 취약점이 Linux나 Android에서 쉽게 발견될 수 있는 취약점유형이라 예상할 수 있다.

그림3은 이승진의 app store 공격 시나리오를 나타낸 것이며 원문은 이승진이 대표로 있는 grayhash[3]에서 열람 할 수 있다.

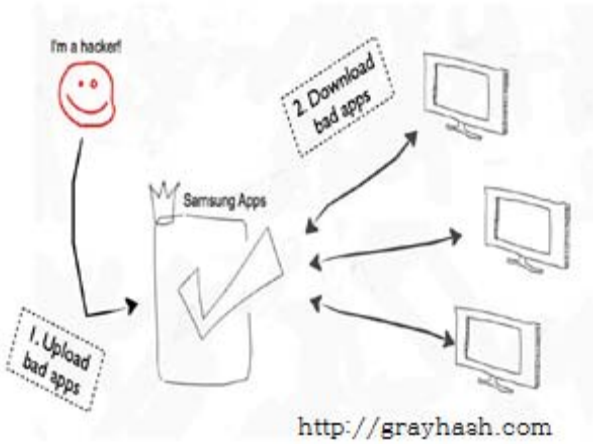

그림 3. app store공격 시나리오.

7. 결론

위의 보안문제 동향을 살펴볼 때 대부분의 취약점은 Smart TV의 Network Interface 기능을 이용하였다. 그리고 Samsung SmartTV에도 Sandbox[4]와 같은 보안대책이 마련되어 있으나 쉽게 무력화 될 수 있다. 또한 많은 삼성 제품이 프로토콜과 핵심 컴포넌트 및 공유 라이브러리가 동일하기 때문에 다른 모델의 SmartTV도 이 취약점의 영향을 받을 가능성이 있다는 것이다. 그렇기 때문에 한 모델의 취약점이 발견된다면 다른 SmartTV에도 공격받을 위험이 있기 때문에 그 전에 대책방식을 수립하여 철저히 대처할 수 있게 해야 한다.

참고문헌

[1]SamyGO 프로젝트 단체, http://www.samygo.tv/
[2]Firmware python patcher tool, http://wiki.samygo.tv/index.php5/SamyGO_Firmware_Patcher
[3]grayhash, http://grayhash.com/
[4]sandbox, http://en.wikipedia.org/wiki/Sandbox_(computer_security)