방송과 통신의 융합에 따른 취약점 분석 프로세스 연구

류 정 아
배재대학교 전산수학컨텐츠학과
e-mail:mastera@pcu.ac.kr

A Study on the Vunerbility Analysis Process for Convergence of Broadcasting and Communication

JeongA Ryou
Dept. of Computer Mathematics & Content, PaiChai University

요 약

최근 우리나라에서 방송과 통신의 융합에 대한 연구가 활발하게 이루어지고 있다. 실제로 방송과 통신이 기술적으로 융합화되어 가고 있고, 방송통신위원회를 기반으로 각종 방송 통신 정책 및 제도들이 개정되어 운영되고 있다. 융합 환경의 핵심적인 특징은 네트워크가 현재보다 더 광범위한 서비스 제공을 위한 수단으로 이용될 수 있다는 것이지만 융합에 따른 불확실성, 즉 융합에 따른 취약성을 제거하지 않고서는 서비스의 안전성을 보장할 수 없다. 따라서, 방송・통신 융합의 불확실성을 제거하고 향상된 서비스를 제공하기 위하여 방송과 통신의 융합과 관련된 보안 취약점 분석 프로세스 개발이 요구된다.

이에 따라, 본 논문에서는 방송과 통신의 기반시스템이 융합화되는 과정에서 발생되는 취약성에 대한 문제점을 알아보고 이에 대한 취약점을 분석하기 위한 프로세스를 제시한다.

Key word : 융합(Convergence), IPTV, 취약성, 위험분석

1. 서론

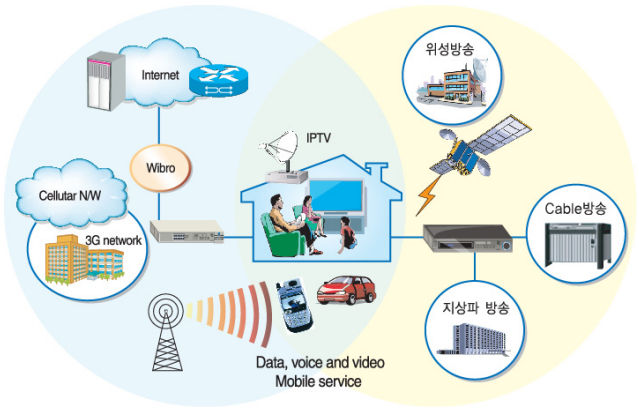
Convergence, 즉 방송과 통신의 융합은 PC, 핸드폰, TV 등 누구나 어떠한 단말기를 이용하여 컨텐츠를 공유하고 이용할 수 있도록 통합하는 것을 가리키는 용어이다. OECD는 방송・통신의 융합을 '통신 네트워크의 광대역화, 방송의 디지털화 등 통신기술의 발달로 음성, 영상 및 데이터 서비스를 제공하고 있고, 서로 다른 용도의 단말기를 통해 원하는 서비스를 받게 되며 신규 서비스가 창출되는 과정'으로 정의하였다[1]. 기술적 융합의 가장 기본적인 단계는 방송사업자가 방송 프로그램을 전송하는 네트워크를 통해서 통신 서비스를 제공하며, 통신사업자는 통신 네트워크를 통하여 방송 및 영상 프로그램을 전송하는 형태이다. 즉, 케이블 TV 사업자가 케이블 네트워크를 이용하여 전화 또는 인터넷 서비스를 제공하고, 통신사업자는 가입자에게 영상 서비스를 제공하는 것이다. 과거에는 방송은 방송 네트워크, 통신은 통신 네트워크를 각각 이용하여 전송되었으나 네트워크의 융합에 따라 방송・통신의 서비스가 모든 전송 네트워크를 통해 제공될 수 있게 된 것이다[2].

또한 서비스도 융합되어 가고 있다[3]. 서비스의 융합은 방송사업자나 통신사업자가 기존에 제공하던 서비스 이외에 다른 서비스를 부가하여 제공하는 것이다. 네트워크의 광대역화와 양방향화는 디지털 콘텐츠를 방송과 통신의 속성을 가진 서비스로 개발하여 제공하는 것으로, 일례로, 웹 캐스팅, VoD(Video on Demand), 데이터 방송, 서비스 등이 있다.

이외에 방송과 통신의 융합은 네트워크와 단말기를 중심으로 나타나고 있다[4]. 광대역으로 진화하는 과정에서 네트워크 부문에서 벌어지는 융합 현상은 궁극적으로 방송시스템과 통신시스템의 구분을 없어지게 함으로써 각종 장비 및 컨텐츠 등 자원을 공유하게 된다. 이용자가 기존에는 TV나 전화기, 컴퓨터 뿐만 아니라 개인 휴대 전화나 신형 셋톱박스 등 단말기를 사용하던 시대에서 이제는 하나의 단말기를 통해 다양한 서비스 제공을 받을 수 있는 시대가 된 것이다. 이미 개인용 컴퓨터나 영상 휴대전화를 통해 방송을 자유롭게 끊김없이 시청하고 디지털 TV를 통해 전자뱅킹과 SMS(Short Message Service)를 편리하게 이용할 수 있게 되었다.

방송・통신의 융합은 (그림 1)과 같이 하나의 네트워크, 하나의 단말기, 나아가 이들을 하나의 디지털 플랫폼에서 방송서비스와 통신서비스의 결합으로 인하여 유비쿼터스 시대가 도래 할 것이다. 이에 따라, 외국에서는 방송・통신의 융합을 위한 대책을 마련하고 있다. 미국의 경우에는 FCC(Federal Communications Commission)[5]를 중심으로 추진 중에 있으며, 국내에서도 방송통신위원회[6]를 새로 설립하여 유비쿼터스 시대에 걸맞는 방송・통신의

융합을 위한 여러 정책 및 기술 대책들이 계획 수립되고 있다.



(그림 1) 통신과 방송의 융합

현재 방송·통신의 융합과 관련하여 인프라 구축에 많은 투자가 이루어지고 있지만 보안 문제도 같이 고려되어야 한다. 방송·통신의 융합과 관련하여 가장 큰 고려사항은 융합으로 발생되는 해킹 피해 및 정보의 역기능이며 이를 해결하지 않으면 국민 생활에 심각한 피해를 발생시키기 때문이다. 디지털 기술의 발전에 맞게 정보 보안 문제에 더욱 관심을 가져야 한다. 현재 방송분야는 저작권 보호와 컨텐츠 보호 분야에 대해 역점[7]을 두는 반면, 통신 분야는 해킹, 바이러스 등 악성코드의 침해사고 예방 및 복구 대책[8]에 더 큰 관심을 갖고 있다. 따라서, 단순히 네트워크 연결만으로는 다른 영역에 보안 공백이 발생할 수 있으므로 본 논문에서는 방송과 통신시스템이 가지고 있는 고유 취약점 분석을 기반으로 융합에 따른 취약점 사례를 분석해 보기로 한다. 이러한 사례 발굴 및 보완만을 가지고는 방송·통신시스템 융합이 안전하고 신뢰성 있는 기반 체계를 구축하는 것이 불가능하므로, 본 논문에서는 방송·통신의 융합 시스템에 활용될 수 있는 취약점 분석 프로세스를 제시하기로 한다. 제시하는 취약점 분석 프로세스는 기존 정보통신기반보호법의 취약점 분석·평가 프로세스에 통방 융합과 관련된 절차를 반영하고 지속적인 교육 및 훈련과 불시 점검을 포함한 프로세스이다.

2. 방송과 통신 기술의 융합 문제점

2.1 기술의 차이점 분석

방송과 통신은 서로 많은 발전을 이루어, 세부분야로 들어가면 매우 다양한 구성과 전문성을 가지고 있다. 따라서, 세부 전문 기술에 대하여 열거식으로 분석하기보다는 본 논문에서는 방송과 통신의 기본적인 사항만을 기반으로 분석해보기로 한다.

통신은 보도 통신, 우편 통신 및 전기 통신으로 크게 구분할 수 있다. 전기 통신은 전화를 비롯하여 전자적인 방식이나 광기술로 컨텐츠를 송수신하는 것을 의미한다. 방송이라 함은 전기통신 기술을 기반으로 하여 불특정 다수인에게 컨텐츠를 일방적으로 보내주는 것을 의미하며, 방송을 수신할 수 있는 수신기를 소유하고 있는 자는 누구든지 방송국에서 송출되는 컨텐츠를 수신할 수 있다.

방송과 통신의 차이는 기술적으로는 모두 동일한 전기통신 기술을 기반으로 하고 있으며, 단지 컨텐츠를 특정인들 간에 유통시키는 것인지 불특정인을 대상으로 하여 유통시키는 것인지에 차이가 있다. 이것은 유통되는 컨텐츠가 미치는 영향의 정도에 큰 차이를 갖게 되는데, 컨텐츠의 보호 측면에서 볼 때 방송은 불특정 다수인에게 컨텐츠가 공개되므로 비밀스런 컨텐츠를 주고받을 수 없지만, 저작권에 대한 보호와 저작권과 관련한 과금을 받기위한 사용자 인증 기법이 요구된다.

통신의 경우에는 당사자 간에 주고받는 정보의 중요도에 따라서 보안 수준의 강도가 달라진다. 이를 기반으로 방송시스템과 통신시스템의 보안 차이점은 <표 1>과 같이 5가지로 구분할 수 있다. 통신시스템에서는 당연하고 타당하다고 여겨지는 가정들이 방송시스템에서는 성립하지 않아 문제가 발생한다.

<표 1> 방송과 통신시스템의 보안 차이점

항 목	방송시스템	통신시스템
성능 요구	무결성>가용성>기밀성	무결성>가용성>기밀성
컨텐츠 보호 수준	저작권 스크램블 과금 수준의 인증	비밀 등급별 차등 암호화 다단계 인증
신뢰성 요구	QoS 실시간 요구	백업, 이중화 대책 등 응답 시간 요구
운영체제와 프로토콜	업체 운영체제 방송 프로토콜	Windows, UNIX 등 TCP/IP, Ethernet 등
단말기 등 주변기기	TV, 카메라, 안테나, 방송시스템	PC, 노트북, 휴대전화, 서버, 라우터

물론, 이러한 차이점들도 IPTV의 도입으로, 방송 통신이 IP기반으로 융합되어가면서 공통적인 요소를 많이 반영하는 추세이지만 과도기적으로 진행되는 현 상황에서는 이러한 운영체제 및 프로토콜 연동 등에 따른 취약성을 고민해야 한다.

2.2 방송의 취약점

현재 공중파와 관련된 해킹 사례가 발생하고 있지 않지만, 컨텐츠 제공 업체와 관련된 방송 컨텐츠 해킹 및 피해가 발생하였다.

예를 들어, 최근 모 컨텐츠 제공업체에서 콘텐츠 전송 네트워크의 보안상 취약점이 발견되었다. 콘텐츠 전송 네트워크는 해커들의 전형적인 방식인 MIMA(Man in the Middle Attack) 방법으로 해킹시 쉽게 유료 콘텐츠를 무료로 다운로드할 수 있었다. MMA란 셋톱박스와 사업자 서버 사이에 유료콘텐츠 요청신호를 무료콘텐츠 요청신호

로 변경할 수 있는 프로그램을 설치, 별도의 과금 과정을 거치지 않고도 영화·드라마 등의 콘텐츠를 받아 볼 수 있게 하는 해킹수단이다.

다음으로, 불법적인 방송 컨텐츠 차단을 위한 방안으로 여러 국가에서는 온라인 검열을 수행하고 있다. 하지만 복잡하고 다양한 네트워크 구조로 인하여 검열에 따른 컨텐츠 차단에 역효과가 발생한 경우가 있다. 기존 방송시스템의 경우에는 사전 점검을 통해 미리 불법적인 컨텐츠를 통제할 수 있지만 다양한 방송 컨텐츠 서버들이 네트워크상에 서비스를 실시하는 경우 국가적으로 중앙 통제가 어려워진다. 최근 파키스탄이 자국 내 네티즌이 유튜브 접속을 하지 못하도록 차단하는 과정에서 유튜브 사이트 이용이 전 세계적으로 중단되는 사태가 벌어졌다.

또한, 디지털 액자서비스를 하는 시스템을 감염시키는 악성코드가 출현하였다. 이는 Offline상의 Digital 주변 기기를 통한 전파 방식이었다. 기존에는 방문자가 많은 사이트를 공격하여 소스코드를 변조함으로써 악성코드를 유포하는 방식을 사용하였으나 이제는 주변기기 제조회사 등을 공격하여 Offline상에서 배포한 후, 주변기기들이 업데이트 또는 컨텐츠 전송을 위하여 네트워크에 접속하는 순간 악성코드가 유입되도록 개발된 것이다.

이러한 공격 사고 사례로 비추어 볼때 방송 분야도 해킹 및 침해 사고가 발생할 수 있는 여지를 보여주므로 이에 대한 대비책이 요구되는 것이다.

2.3 통신의 취약점

통신시스템에 대한 취약점에 대해서는 많이 제시되고 있으므로 본 논문에서는 간단하게 방향만 설명하기로 한다. 통신의 가장 큰 위협은 악성코드의 진화이다. 한 해에 몇 천개 혹은 몇 만개 정도씩 만들어 지는 악성코드는 계속 업그레이드되어 가고 있다. 앞으로 통신상의 취약점은 계속 증가할 것이고 해킹의 세계화, 해킹 자동화 도구의 출현, 온라인 게임을 통한 개인정보 노출에 따른 위험 확대, 금융·증권 등 온라인 생활의 위험 증가가 일반화 될 것이다. 이외에 마이크로소프트 오피스 파일을 이용한 신규 백도어 설치 및 감염, 웹 응용프로그램 공격으로 접근권한 획득과 웹 응용프로그램 소스 코드의 변조를 통한 해킹 등이 더욱 기승을 부릴 것이다.

2.4 방송과 통신간의 융합에 따른 취약점

위에서 언급한 사항처럼 각각의 시스템에서 존재하는 취약점들이 방송과 통신간의 융합으로 인하여 또 다른 피해를 발생시킬 수 있다. 최근 휴대 전화에 대한 바이러스 발생이나 은행 단말기로의 해킹 등이 보고되고 있다. 만일 해커가 통신시스템을 통해 방송 서버를 해킹하여 적성 국가에 전쟁 선포와 같은 내용을 아무런 제약없이 공중파에 타게 하여 전세계에 방송된다면 국가적으로 심각한 이미지 손실 및 국민 안전에 막대한 영향을 미치게 하며 이로 인한 손해 비용은 천문학적으로 클 것이다.

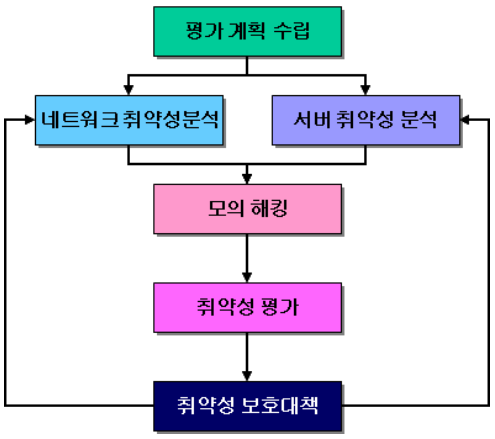
다음은 네트워크 중립성에 관련된 사항으로 네트워크는 누구나 동등하게 접속이 가능해야 한다. 네트워크 융합이 가속화되는 경우 트래픽의 과부하로 인하여 네트워크 사업자가 인터넷 포탈이나 컨텐트 제공자의 접속을 제한할 가능성이 있다.

다음은 개인정보의 유출이다. 방송시스템에서는 통신시스템보다는 정보보호에 대한 대책이 현재까지는 미흡하므로 방송 컨텐츠 가입자에 대한 개인정보 유출을 방지하는 대책이 요구된다.

이외에 융합의 따른 취약점을 살펴보면 IP 및 대역폭 부족으로 인한 자원의 고갈, 컨텐츠 서버에 대한 과부하로 인한 서비스 중단 등 다양한 분야에 많이 나타나게 될 것이다. 따라서 이러한 취약점을 조기에 식별하고 대응해 나갈 수 있는 프로세스가 요구된다.

3. 제안하는 취약점 분석 프로세스

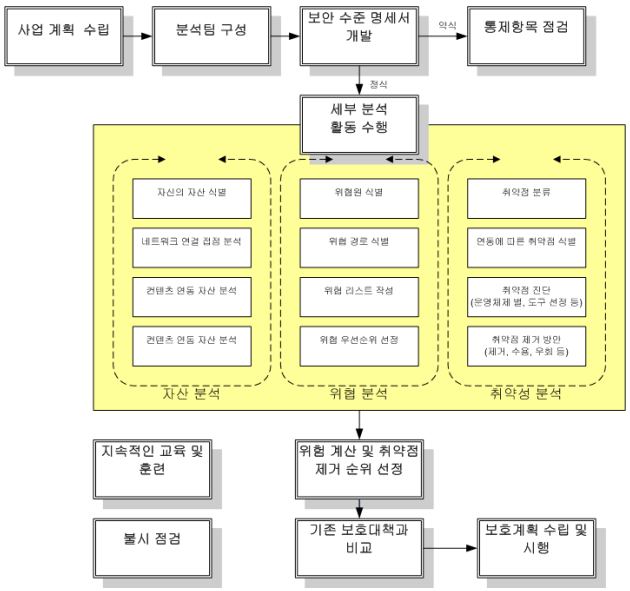
(그림 2)에서 보는 바와 같이 기존의 취약점분석 프로세스는 취약점진단도구를 이용하여 발견되는 취약점에 대하여 분석하고 이를 소프트웨어적으로 해결하거나 패치하는 수준에서 이루어졌다. 이러한 방법은 예방적인 보안대책이 아니며 새로운 위협이나 침해사고가 발생한다면 시스템에 피해가 발생한다. 특히, 네트워크가 연동된 상태에서 발생하게 되면 방송시스템까지 악영향을 받게 된다.



(그림 2) 일반적인 취약점분석 프로세스

제안되는 취약점 분석 프로세스는 (그림 3)와 같다. 취약점 분석 프로세스는 위험분석 프로세스에 통제항목 점검, 불시점검, 지속적인 교육 및 훈련 등 3 가지 요소를 추가된 형태이다.

먼저 기관에서는 사업 계획을 수립하고 분석팀을 구성한다. 분석팀의 경우에는 외부 평가기관을 활용할 수 있다. 분석팀이 구성되면 방송·통신 시스템에 대한 보안 수준을 어느 정도 할 것인지를 정한다.



(그림 1) 제안하는 취약점분석 프로세스

단순히 방송 컨텐츠에 대한 저장 및 배포 수준인 경우에는 해킹 등 침해사고 및 악성 코드에 대한 대비만을 수행하면 되지만, 회원관리 및 방송제작과 관련된 용역 계획 등이 포함된다면 보안 수준을 높여야 한다. 이렇게 보안수준명세서를 개발하고 정식으로 수행하는 방법과 약식으로 수행하는 방법중 하나를 선택한다. 약식은 통제항목에 대한 점검만 수행하면 되지만, 정식으로 하는 경우에는 세부분석 활동으로 자산분석, 위협분석, 취약성분석을 수행하고 위험을 계산하여 취약점 제거 순위를 정해야 한다. 예를들어, 취약성 분석을 수행하는 과정에서 기존 CAS에 대한 취약성으로 셋톱박스와 서버 사이에 전송되는 신호가 DES 암호 알고리즘을 사용하기 때문에 회원정보가 노출될 우려가 발생한다면, 128비트 AES 암호 알고리즘으로 암호화해 복제를 불가능 하도록 보호대책을 수립한다. 컨텐츠에 대한 전송시 스크램블만으로 보호가 되지 않는 것으로 분석되면, 암호 난수를 이용하여 전송 신호 패턴을 실시간으로 변경해주는 논스(Nonce) 기술을 적용하는 것을 명시한다. 이렇듯 방송·통신 융합에 따른 서비스를 안정화하기 위한 기술적인 요구 사항으로 QoS(Quality of Service) 보장 기술, 다양한 서비스를 위한 미들웨어 개발 기술, 인터넷 관제 기술, 바이오 인식 및 PKI 시스템 기술, 콘텐츠 저작권 보호 기술 등을 제시할 수 있다. 다음 절차는 기존 보호대책과 비교하여 취약점에 대한 대책(제거, 수용, 우회 등)을 정한 후 보호 계획을 수립하고 시행에 들어간다.

이와 별도로, 불시점검과 지속적인 교육 및 훈련을 수행한다. 불시점검 활동은 현재의 통상적 위험수준을 정하고 승인된 보안대책이 위험수준의 범위 내에서 유지되고 있는지 보증하기 위하여 독립적으로 불시점검을 수행한다. 불시점검은 취약점 진단 도구를 통해 진단을 수행하여 긴급한 취약점을 제거하고 단기적인 보안 대책을 수립해서 시행한다. 지속적인 교육 및 훈련은 보안업무를 담당하는 보안업무 관계자들에게 제공하며 그들에게 자신의 책임 사항을 알려 주고 임무를 적절히 수행할 수 있도록 도와준다.

분석 활동이 종료되면 최종 승인 여부를 결정한다. 승인 결과에 따라 방송·통신 융합 시스템 운영은 현장별로 관리자 책임 하에 수행되며 방송·통신 융합 시스템 운영 활동의 결과에 따라 새로운 프로세스가 시작될 수도 있다. 설계된 보호 계획 수준이 수용 불가능하다면 분석 팀은 문제를 수정할 것인지를 결정해야 한다. 문제를 수정하기로 했다면 분석 팀은 수정된 문제에 맞도록 수정한 시스템에 대하여 설계 변경을 실시한다. 보호계획 수준이 수용 가능하다면 방송·통신 융합 테스트베드에서 시스템 통합과 시험을 완벽하게 수행한 후 점진적으로 현장에 적용한다. 모든 시스템 구성 요소의 배치가 완료되었으며 보안 수준을 만족시키게 되면 방송·통신 융합시스템의 정보 연동을 승인한다.

이러한 종합적인 취약점 프로세스를 통해 방송·통신 융합 시스템의 보안을 강화하여 안정된 서비스를 제공할 수 있는 선진 시스템 체계를 마련하게 되는 것이다.

4. 결론

방송과 통신의 독자적인 영역을 고집해 온 시대를 벗어나 이제는 방송의 디지털화로 인해 방송과 통신의 구분의 어려운 융합현상이 우리의 생활에 인접해 있다. 정보통신 기술의 발달로 방송과 통신을 분리해서 구분하는 것은 사실상 무의미해졌다. 이러한 융합을 통해 방송과 통신의 영역 및 경계가 무너지고 있는 상황에서 유비쿼터스 시대를 대비하기 위해서는 방송·통신의 융합에 따른 취약성을 제거하고 안전하게 운영할 수 있는 방안을 지속적으로 발굴해나가야 할 것이다.

참고문헌

[1] OECD. 1999. Regulation and competition issues in broadcasting in the light of convergence, DAFFE/CLP(99).

[2] 윤석민외, “방송통신 융합관련 법제도 정비방안 연구,” http://www.kbc.go.kr

[3] 오용수, 정희영, “방송·통신 융합에 따른 규제체계 전환의 정책방향,” 방송연구 2006년 여름호, 138~169pp.

[4] 석주명 외, “개인 맞춤형방송 서비스와 단말플랫폼 개발,” 전자공학회 논문지 2007.1.

[5] Federal Communications Commission, http://www.fcc.gov/

[6] 방송통신위원회, 방송·통신 기술동향 연구- Digital Dividend -, http://www.bcc.go.kr/

[7] 우제학외, “IPTV 컨텐츠보호기술의 비교-CAS와 DRM 중심으로,” 한국컨텐츠학회논문지 pp157-164, 2006. 6.

[8] 국가정보보호백서, www.ncsc.go.kr