방송시스템의 보안강화 - 1

- Part 1. 정보보안이란?

글.
이선응 차장, 김영준 과장(아이크래프트㈜ SNT본부 기술1팀)

연재 목차

최근 들어 방송시스템의 다양한 변화가 일어나고 있다. HD 방송을 넘어 4K UHD 방송이 올해부터 본격적으로 시작되고 있으며, 8K, 16K 등 좀 더 리얼한 영상을 담기 위해 많은 양의 영상정보를 촬영, 편집, 저장해야하고 기존보다 더 고성능, 고용량의 데이터를 처리해야 하는 추세이다.

이렇게 대용량 데이터를 처리하기 위해 대부분의 방송시스템이 기존의 SDI 등의 방송표준방식에서 범용적으로 통신방식에서 활용되는 IP 방식으로 변화하는 추세이다. 모든 세상의 이치가 얻는 게 있으면 잃는 게 있듯이, 데이터전송방식이 표준화되어 빠르고 안정적으로 편리하게 이루어지는 장점이 생기는 반면, 어디에서나 누구나 제한 없이 방송 데이터에 접근할 수 있는 위험성도 같이 증가하게 되었다.

이번 호에서는 정보보안에 대한 개념과 종류 및 최근 보안과 관련된 다양한 이슈에 대해 살펴보도록 하겠다.

우선 보안이라고 하면, 기존의 전통적인 물리보안을 떠 올릴 수 있다. 은행을 예로 들면, 제일 먼저 은행입구 셔터 등의 금속문이 존재하며, 뒤이어 두꺼운 통유리문을 통과하게 되면, 다양한 자동화기기를 만나게 되며, 은행 객장으로 들어가게 되면, 해당 지점의 경비원을 만난 뒤 은행직원창구를 비추는 감시카메라, 그리고 현금을 보관하는 금고, 마지막으로 위급한 상황에 경찰을 호출 할 수 있는 비상벨 등이 있을 것이다.
이 모든 것이 돈을 취급하는 물리적 장소에서 현금을 안전하게 보관하고, 허가된 사용자만 접근하고, 현금을 허용된 사람에게만 전달하기 위해 마련된 시스템이며, 만약 허용되지 않는 사람이 현금을 가져가려는 행위 발생 시 해당 행위를 막거나 최대한 늦추고, 설사 성공하였다고 하더라도 사후에 추적하고 회수할 수 있는 물리적 장치가 완비된 시스템이다.

다음으로 인터넷으로 통장을 개설하고 잔금조회, 잔고이체를 하는 홈뱅킹서비스를 위한 은행의 웹 사이트를 예로 들어 정보보안(사이버보안)을 설명하겠다. 먼저 사용자는 개인 PC 혹은 스마트폰을 통해 먼저 인터넷 주소를 입력하게 된다. 먼저 개인 PC에 다양한 보안프로그램을 설치하여야 한다. 거래정보를 암호화하고, PC에 바이러스나 악성코드가 있는지 검사하고, 키입력으로 암호를 훔쳐보는 행위를 차단하고 마지막으로 공인인증서를 사용할 수 있게 도와주는 다양한 프로그램들이다.
은행의 홈뱅킹 로그인을 위해 공인인증서가 있어야 하며, 공인인증서 패스워드를 입력하게 되면, 개설된 통장의 잔금을 확인할 수 있으며, 타 계좌로 이체를 할 경우 개인이 소지한 보안카드의 특정 번호를 입력하거나, OTP라는 일회용 암호생성기로 출력되는 키 값을 입력하여야 만 계좌 송금이 이루어진다.

돈을 취급하는 물리적인 공간과 인터넷상의 논리적인 공간이 다르지만, 이런 과정에서 필요한 보안 요소들은 비슷하게 적용된다. 아래 [표]과 같이 물리적 보안과 정보보안은 각각의 역할에 따라 비슷한 목적에 따라 구성된다.

역할	은행지점	은행 웹사이트
접근제어	바깥 셔터출입문	외부 방화벽
	안쪽 유리출입문	내부 방화벽
침입/공격 탐지	경비원	보안관제요원
	감시카메라	로그저장시스템
신분확인/권한인증	신분증	개인 공인인증서
	싸인	보안카드/OTP 카드
침입/공격차단	비상벨	로그 모니터링/알람시스템

표 1. 은행의 물리보안과 정보보안의 역할

IT 분야가 발전하고 다양한 시스템이 도입되면서 정보보안분야도 다양한 종류가 추가되었다. 앞에서 살펴본 은행 웹사이트에 적용된 정보보안시스템 이외에도 아래 [표 2]와 같이 다양한 분야의 보안이 존재한다.

분야	종류					
네트워크 보안	Firewall (방화벽)	IDS/IPS (침입탐지/차단)	VPN (가상 사설망)	Anti-Spam (악성코드 탐지)	WIPS (무선보안)	Anti-DDoS
시스템 보안	OS 보안	서버방화벽	원격접속통제	취약점 스캐너	HDD 암호화	통합인증관리
어플리케이션 보안	Web Firewall (웹 방화벽)	웹취약점 스캐너	코드 취약점 스캐너	SSO (싱글 싸인 온)		
DB 보안	DB 접근제어	DB 암호화	DB 조회이력 감사	DB 완전삭제		
클라이언트 보안	바이러스백신	패치관리	키보드보안	클라이언트 가상화	스마트폰 보안	
콘텐츠 보안	DRM(문서보안)	콘텐츠 필터링	문서 출력보안	데이터 완전삭제	보안 USB	문서 중앙화

표 2. 정보보안의 분야와 종류

위의 표 중 평소에 들어본 보안시스템이 얼마나 될까? 제일 먼저 나오는 F/W 즉 Firewall, 한글로 방화벽은 많이 들어 보셨을 것이다. 2006년 해리슨 포드 주연의 파이어월이라는 영화가 개봉되었다. 은행의 보안전문가가 가족을 인질로 잡은 범인의 요구로 자기가 설계한 방화벽시스템을 침투하여 돈을 빼내는 시나리오인데 초기 방화벽 모델을 화면에서 볼 수 있다.

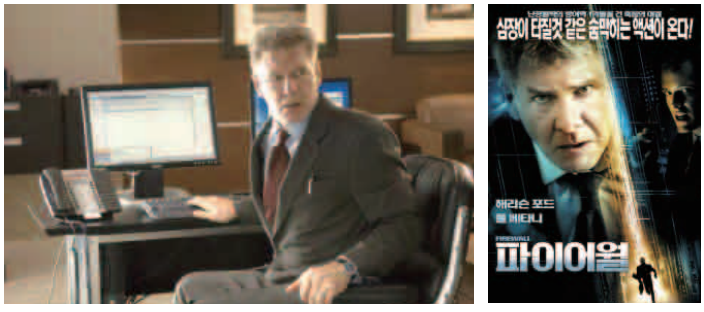

그림 1. 영화 Firewall (파이어월)

이런 방화벽이 담당하는 부분이 네트워크보안이라 부르는 분야이다. 게이트웨이라는 전송경로의 입구에서 사전에 만들어진 정책에 따라서 트래픽을 차단하거나 허용하는 일을 하는 시스템이다. 내부 시스템과 인터넷과 같은 외부 간의 경계에 위치하는 최전방 문지기라고 볼 수 있다.

아무리 잘 설계된 보안시스템이라도 허점은 존재하기 마련이고, 해커(침입자)들은 내부시스템에 접근하기 위해 취약점을 이용하여, 시스템에 침투하고 귀중한 정보를 탈취한다. 그래서, 정보보안 설계 시 정보가 보관된 시스템까지 접근하기 위해서 여러 개의 보안시스템을 통과하도록 설계하여, 모든 보안시스템을 우회하지 않으면 정보에 접근하지 못하도록

이선응 차장 / 김영준 과장
아이크래프트㈜
SNT본부 기술1팀

설계한다. 이런 설계방식을 Defense-in-Depth 혹은 Layered security architecture, 한글로 다계층 보안구조 라고 한다.

[그림 2]와 같이 왼쪽의 해커가 오른쪽 끝의 정보까지 접근하기 위해서 4단계의 문지기를 통과해야 원하는 정보에 접근이 가능하다. 최전방의 네트워크보안을 통과하면 서버(Server)라고 불리는 시스템레벨의 보안시스템을 만나게 되고, 이를 통과하면 프로그램 레벨에서의 보안시스템을 지나, 마지막으로 실제 데이터가 저장되어 있는 DB 시스템의 다양한 보안시스템을 통과해야 최종 원하는 정보에 접근이 가능하다. 물론 이런 설계방식은 널리 권장되는 구조이기는 하나 도입하는 조직의 예산과 인력, 내부 보안프로세스에 따라 생략되거나 축소되는 경우도 많이 있다.

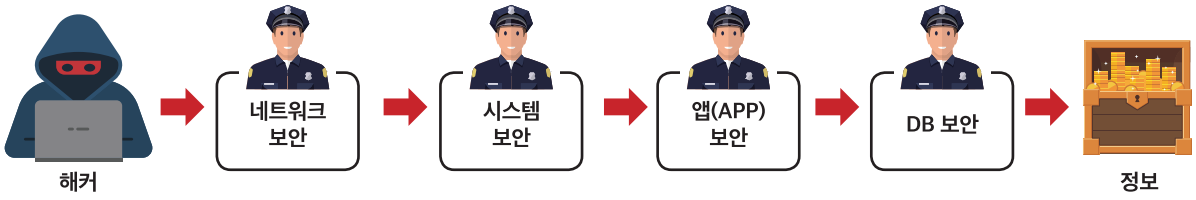

그림 2. 다계층 보안구조

그럼 다음으로 앞에서 설명한 다계층 보안구조에 대해 하나씩 자세히 설명하겠다.

네트워크 보안

외부에서 침투하는 해커가 제일 먼저 만나게 되는 보안시스템으로 방화벽 이외에 IDS/IPS가 있다. IDS는 Intrusion Detection System, IPS는 Intrusion Prevention System의 약자로 침입을 탐지하거나, 침입을 발견 후 차단까지 수행하는 시스템이다. 이때 침입을 식별하기 위해서는 범인의 몽타주를 참고하여 비슷하게 생긴 사람을 범인으로 식별하는 것처럼 아래 [그림 3]과 같이 이미 알려진 공격을 분석하여 공격을 수행하는 트래픽 데이터 내에 특정한 문자열이 규칙적으로 나타나는 패턴을 분석, 해당 공격패턴을 등록하여 평소 트래픽을 검사하다가 동일한 패턴이 보이면 공격으로 인식하는 원리로 작동한다.

```
문 자 열 의  개 수  :  5
문 자 열 의  길 이  :  5
apple
grape
chape
shape
knife
패턴 : ????e
```

```
문 자 열 의  개 수  :  2
문 자 열 의  길 이  :  5
chape
shape
패턴 : ?ha?e
```

그림 3. 문자열 패턴의 예

여기서 문제는 지금까지 발견된 공격의 개수가 어마하게 많기 때문에 이 세상의 모든 공격에 대한 패턴을 등록할 수 없다는 것이다. 설령 가능하다고 하더라도 시스템이 검사해야 하는 패턴이 많을수록 시스템의 부담이 높아지고, 검사속도가 느려지는 문제가 발생되기 때문에, 과거의 공격패턴은 제외하고 최근에 유행하는 공격패턴 위주로 등록하여 운영하는 것이 일반적이다.

다음으로 Anti-Spam의 경우 노출된 이메일 주소를 이용하여, 무차별적으로 광고를 보내거나 바이러스 혹은 악성코드가 포함된 파일을 첨부하는 등 수신자에게 특정 웹주소를 클릭하게 유도하여 사용자의 접속정보(ID, PW) 등 개인정보를 탈취하는 목적으로 보내지는 이메일을 사전에 걸러주는 시스템이다. 최근 가장 문제가 되는 고객정보탈취사고가 이렇게 메일을 통해 첨부되는 파일을 메

일수신자가 의심 없이 업무와 관련된 문서로 보이도록 작성하여 열어보도록 유도하고, 문서파일을 열어보는 순간 수신자의 PC를 해커가 마음대로 접근 가능하도록 만들어, 해당기관의 공격 출발점을 만드는 방법으로 이루어진다.
이런 공격을 통상 스피어 피싱(spear phishing)이라고 불리며, 이는 회사전산관리자나 관리자 레벨과 같이 정보가 저장된 시스템에 접근할 수 있는 충분한 권한이 있는 사람을 타겟으로 하여, 창으로 적을 공격하듯이, 특정한 타켓을 선정하여 해당 사용자의 업무에 맞춤제작된 메일을 제작하여 공격성공율을 높이는 공격유형이다.

그림 4. 랜섬웨어 감염화면

이뿐만 아니라 최근에는 PC에 저장된 데이터를 인질로 삼아 암호화시켜놓고 암호를 풀어주는 조건으로 비트코인 등의 금전을 요구하는 랜섬웨어(Ransomware)가 유행하고 있다. 가족을 인질로 삼아 금품을 요구하는 유괴범과 다름없는 범죄행위가 사이버상에서 중요한 정보로 대상이 바뀌어 동일하게 벌어지고 있는 것이다. 이제 가족의 안전을 지키기 위해 귀가시간을 신경 쓰듯이, 중요한 정보를 지키기 위해서는 받는 편지함으로 오는 수많은 메일에 첨부된 파일을 열어볼 때 신경을 써서 신중히 열어 봐야 하는 세상이 되었다.

무선보안시스템(WIPS)은 최근 스마트폰 등의 휴대정보기기의 보급이 늘어나면서 자연스럽게 가정에서뿐만 아니라 회사 내에서도 무선접속을 원하는 수요가 증가함에 따라 회사 내의 공식적인 무선접속장비(AP)가 아닌, 주위에서 싼값에 구매 가능한 무선공유기 등을 사내에 임의로 설치하여, 전산관리자의 승인 없이 사용하는 경우에 이를 탐지하고 차단하는 것을 주기능으로 사용하는 시스템이다.

사내에 무분별하게 설치되는 공유기의 경우 기본으로 설정된 패스워드를 사용하거나 쉽게 유추할 수 있는 암호를 사용하는 경우가 많은데, 이런 경우 사내 근처의 주차장이나 인접 건물에서 무선망에 접속하여, 사내 망에 침투할 수 있는 뒷문(백도어)을 제공하는 통로가 되어, 사내에서만 접근 가능한 서버를 사무실 밖에서 쉽게 접근할 수 있게된다. 최근에는 무선접속(AP)장비 자체적으로 이런 보안기능을 같이 제공하는 제품도 출시되고 있다.

VPN(Virtual Private Network)의 경우 가상으로 사설망을 제공하는 시스템이다. 예를 들어 서울에 본사가 있고 부산에 지사가 있는 경우 부산지점에서 서울본사의 시스템에 접근이 필요한 경우, 부산에서 서울까지 그 회사가 사용할 수 있는 전용선을 설치할 수도 있으나, 이럴 경우 성능에 비해 유지비가 과도하게 나오는, 즉 가성비가 나오지 않는 문제가 생긴다. 이를 해결하기 위해 저렴하고 속도가 빠른 인터넷망을 이용하여, 트래픽을 암호화시켜 보내고 받는 쪽에서 암호를 풀어서 보는 방식으로 동작하는 시스템이다. 다음 호에서 좀 더 자세한 사항을 소개해 드리겠다.

Anti-DDoS의 경우 DDoS 공격을 막는 시스템이다. DDoS는 공격자가 외부에서 웹사이트로 다량의 트래픽을 보내서 정상사용자가 웹페이지를 볼 수 없도록 만드는 공격으로, 광복절을 기해 독도홈페이지를 일본네티즌이 공격한다거나 중국네티즌이 일본극우홈페이지 등을 공격하는 민족주의적 의사 표현에 많이 사용되거나, 최근에는 쇼핑사이트 등에 협박 메일을 보내 일정기한 내에 약속한 돈을 보내지 않으면 DDoS 공격을 하는 방식으로 진화하였다. 이런 공격들은 공격자가 사전에 공격트래픽을 보내는 일명 좀비

이선응 차장 / 김영준 과장
아이크래프트㈜
SNT본부 기술1팀

PC를 다량 확보하여, 한 번의 명령으로 특정싸이트에 동시에 다량의 트래픽을 보내어 공격하는 것이 일반적이다. 이것 역시 다음 호에서 좀 더 자세히 설명해 드리겠다.

시스템 보안

시스템 보안은 서버 보안이라고도 부르며, 네트워크 보안을 통과하여 서버까지 도착한 공격을 차단하기 위해 준비된 2차 보안체계로써 MS사의 Windows, Linux, Unix 등의 시스템 OS 레벨에 적용되거나 별도의 프로그램을 설치하여 서버의 관리자 권한이 쉽게 탈취되지 않도록 지원하는 보안시스템이다. 예를 들면 개인용 PC에 설치된 윈도우OS의 경우 Windows 방화벽기능이나, Windows defender 등의 자체 백신프로그램, 새로운 프로그램을 설치하거나 옵션을 변경할 경우 경고창이 나타나는 보안컨트롤러 기능, 마지막으로 PC Power-Off 시 나타나서 우리를 귀찮게 하는 Windows 업데이트 기능 등이 모두 이 보안체계에 속한다.

다른 보안체계도 마찬가지겠지만, 보통의 공격들은 OS 레벨에서 root 권한이나 admin 권한을 취득하여, 시스템에 원하는 시간에 자유롭게 접근하고, 시스템에 보관된 다양한 데이터에 제한 없이 접근하는 것이 목적이기 때문에 이를 방어하기 위해 해커의 시간과 노력을 좀 더 많이 소비시켜, 비용대 효용가치를 낮추어서, 해커들의 접근을 회피하는 것이 이 보안 단계의 실제적인 목적이라고 할 수 있다.

어플리케이션 보안

어플리케이션보안은 사용자들이 실제 사용하는 프로그램 레벨에서의 보안을 담당한다. 대표적인 경우가 인터넷을 통해 사용하는 웹(web)서비스이다. 사용자 PC에 익스플로러(explorer)나 크롬(chrome) 등의 웹브라우저를 사용하여 네이버, 다음 등의 포털 웹서버(HTTP server)에 접속하여 뉴스, 동영상 등을 검색하고 열람, 시청과정에서 발생되는 다양한 보안취약점을 방어하는 것이 이 분야의 가장 큰 관심사이다.

그림 5. 홈페이지 해킹 기사

최근 방송에서 “홈페이지 해킹”, “고객정보 유출”이라는 단어를 자주 듣고 있다. [그림 5]와 같이 포탈사이트 뉴스검색에서 홈페이지 해킹이란 단어로 검색을 해보니 그림과 같이 다양한 기사를 볼 수 있다. 이렇게 홈페이지 해킹이 급증하는 이유는 앞에서 설명한 방화벽이 많이 보급되면서, 실제 사용하는 통신연결통로(서비스포트)만 열어두고 사용하지 않는 통로는 막아두기 때문에 방화벽이 없던 시절보다는 외부에서 침입할 수 있는 경로가 많이 줄었기 때문이다. 대부분의 조직에서는 홍보 및 업무 목적의 웹서버를 다양하게 사용하고 있고, 업무 및 출장 목적으로 외부에서 많은 사용자가 사내 서버로 접속해야 하기 때문에 방화벽에서 해당 통로를 열어둘 수밖에 없게 되고, 해커는 이 통로로만 외부에서 침투가 가능하기 때문에 웹해킹이 빈번하게 발생하게 된다.

이렇게 웹서버를 타켓으로 하는 공격을 방어하기 위해서 웹방화벽이 등장하게 되었고, 웹서비스를 통해 회사 매출을 올리고 있는 조직(홈쇼핑, 예약싸이트 등)에서는 대부분 웹방화벽을 운영하고 있다.

DB 보안

해커가 네트워크, 시스템, 웹보안 장비를 통과하게 되더라도 마지막 수문장으로 DB 보안을 만나게 된다. 데이터를 지키기 위한 최후의 보루라고 볼 수 있다. 정보가 저장되어 있는 저장소(DB) 앞에 위치하여, 데이터에 접근을 원하는 다양한 요청 중 정상적인 접속은 허용하고 비정상 접속으로 확인되면 접속을 차단하는 기능 이외에 다양한 보안서비스를 제공한다.

접근제어 : 허가된 사용자만 데이터의 조회 및 삭제가 가능하게 제어하는 기능
접근감사 : 데이터의 접근 요청을 허용하거나 차단한 이력관리, 허용 후 실제 조회하거나 변경한 세부사항을 기록하여,
사고 발생 이후 공격근원을 추적하기 위한 용도로 사용
데이터 암호화 : 저장된 데이터를 암호화시켜서 데이터가 유출되더라도 알아볼 수 없도록 만드는 기능

클라이언트 보안

그 이외에도 일반적으로 바이러스 백신으로 많이 알고 있는 클라이언트 보안이 있다. 사내에 있는 PC가 해킹되어 내부의 저장된 정보가 유출되거나, 해킹된 PC를 이용하여 사내에 있는 다른 PC 및 서버, DB에 접근할 수 있는 출발점이 만들어지는 것을 방지하기 위한 V3 혹은 알약 등의 바이러스 백신 혹은 악성코드 탐지차단프로그램 등이 이 범주에 속한다.

최근에 스마트폰의 사용이 증가하면서, 업무에서도 메신저, SNS를 많이 활용하고 있으며, 중요한 정보가 스마트폰에 많이 저장되고 있다. 이런 스마트폰을 분실 할 경우 원격에서 데이터를 삭제하거나, 분실폰의 위치를 GPS로 알려주거나 혹은 스마트폰에 설치하는 앱의 설치 여부 및 데이터를 원격에서 제어할 수 있는 MDM(Mobile Device Management)이라는 솔루션도 많이 사용되고 있다.

콘텐츠 보안

업무 중에 작성하는 다양한 문서 혹은 제작한 다양한 비디오클립들, 이를 편집하여 만드는 다양한 편집본 등이 모두 콘텐츠가 되는데, 이렇게 제작된 다양한 내용이 제작자의 의도와 무관하게 위조 혹은 변조되는 경우를 차단하거나, 문서로 출력될 경우 출력한 시간과 프린트명, 출력자의 이름이 나타나서, 외부로 유출되더라도 추적이 가능하게 하거나, 반드시 삭제해야 하는 중요 데이터에 대해 복구가 불가능하게 만든 것이 모두 이 분야에 포함된다.

지금까지 정보보안의 다양한 분야를 개략적으로 살펴보았다. ICT 분야가 실생활에 좀 더 깊숙이 관여되고, 금전 거래 및 실생활에 꼭 필요한 필수적인 기능이 사이버공간을 통해 제공되면서, 불법적인 방법을 통해 경제적인 이득을 취할 수 있는 기회가 증가되고 있다. 과거 단순한 호기심, 자기 능력을 과시하는 수준에 머물지 않고, 개인 단위를 넘어 국가 단위에서 사이버공간에서의 공격과 방어가 이루어지고 있는 현실에서 이런 현상에 대한 이해에 조금이라도 도움이 되었으면 하는 바람이다.

다음 호부터는 네트워크보안의 가장 기본 장비인 방화벽과 VPN을 살펴보고, DDoS 공격 및 APT 공격을 차례대로 소개한 뒤, 마지막으로 방송시스템에서 보안적용방안에 대한 내용을 순서대로 연재하겠다.