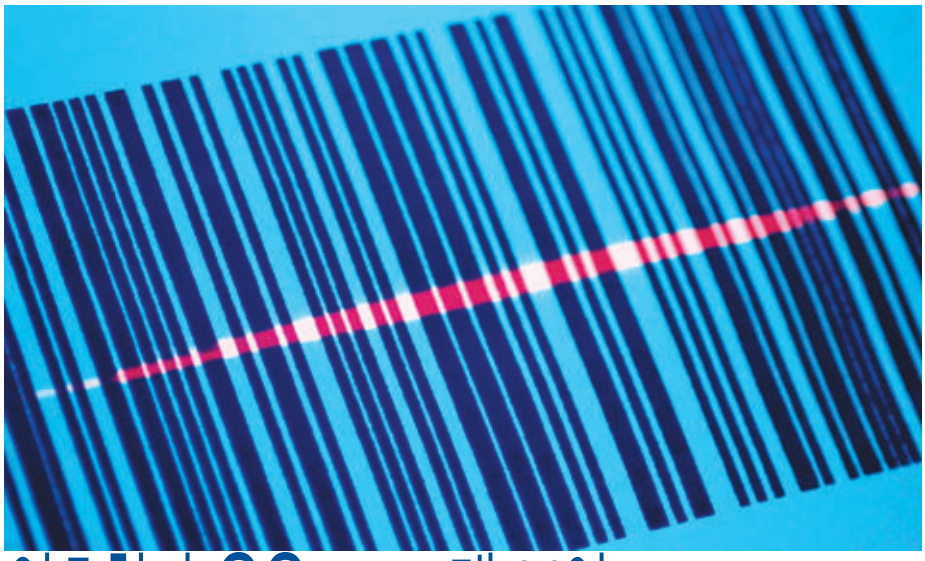
+ 허종오 · 한국 CISSP협회 연구분과 이사, 전자계산기기술사



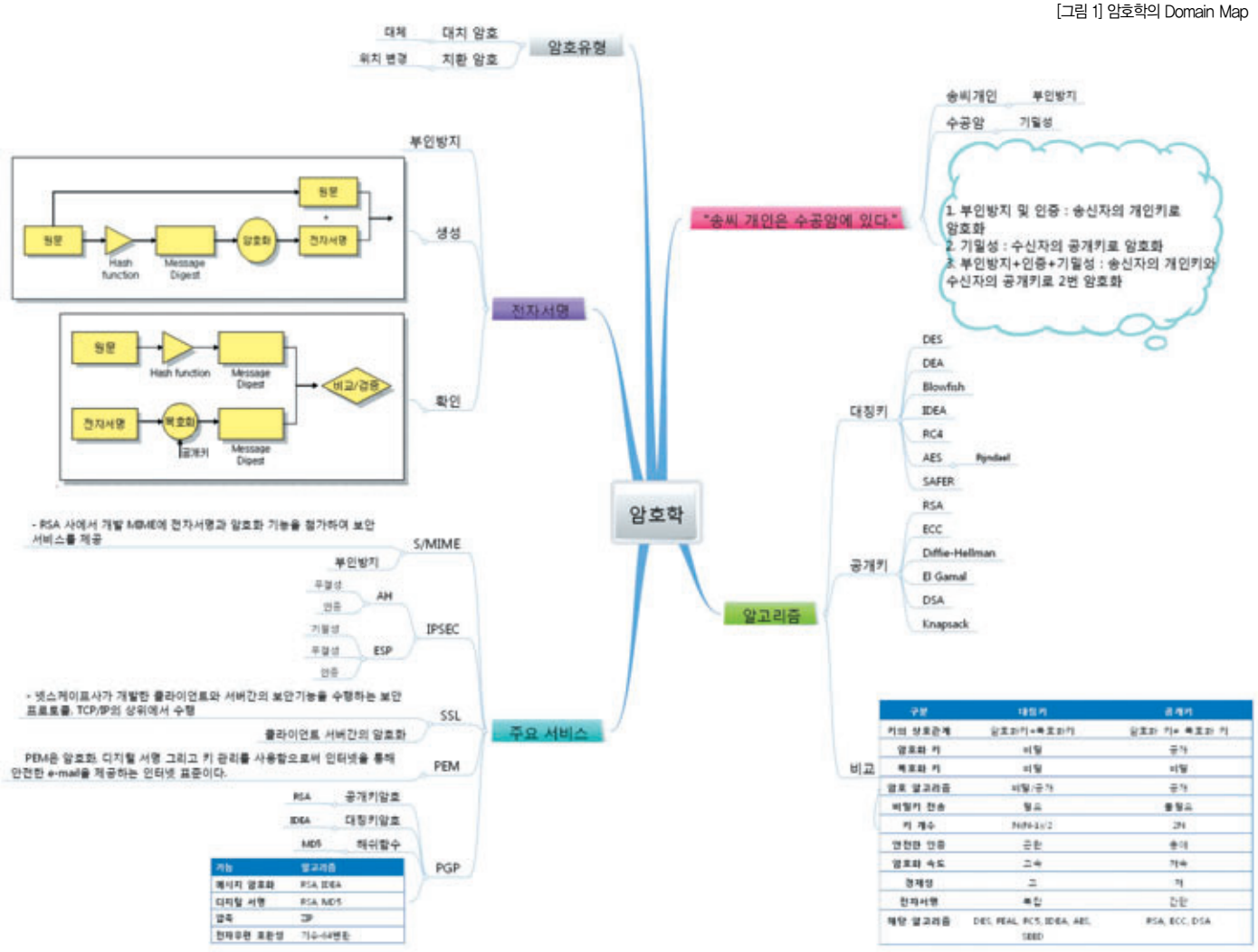
암호학과 응용프로그램 보안

지난 호에서는 접근 통제, 통신 및 네트워크 보안 도메인에 대한 요점정리와 연습문제를 통해 CISSP가 되기 위해서 기술적 부분에서 어떤 내용을 학습해야 되며, 어떤 문제가 출제가능 한지를 알아보았다. 이번 호에서는 CISSP의 10개 도메인 중에서 기술적 보안의 기반 지식이 되는 암호학과 사용자와 가장 밀접한 분야인 응용프로그램 보안에 대해서 알아보고자 한다.

1. 암호학(Cryptography) 요점정리

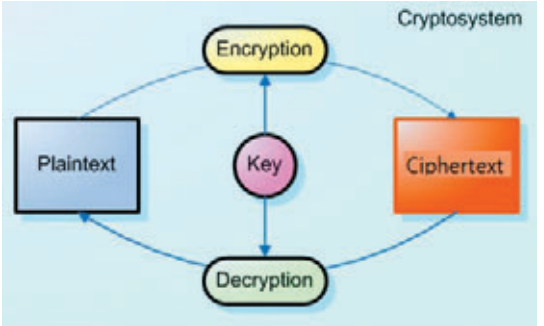
암호학 도메인은 보안의 가장 기본 지식이 되는 암호화 방법과 암호 알고리즘 등을 알 수 있다. 즉, CISSP가 관리하는 보안 시스템이 사용하는 암호화 알고리즘을 이해함으로써, 정보들의 기밀성을 보호 할 수 있으며, 전송되는 정보들의 무결성을 어떻게 보호하는지 안내해주는 도메인이라고 볼 수 있다.
암호학 도메인에서 학습해야 할 요점들은 다음 Domain Map을 통해 한 눈에 알 수 있다.

[그림 1] 암호학의 Domain Map



1-1. 암호학의 정의

Data의 기밀성, 무결성, 사용자 인증 등과 같은 정보보안을 위해 수학적 기술을 이용하는 연구. 암호학을 구성하는 주요 용어들은 다음 [그림 2]와 같다.



[그림 2] 암호학의 주요 용어

[표 1] 암호학의 주요 용어

주요 용어	설 명
Plaintext	평문, 암호화되지 않은 포맷. 공격자에 의해서 읽힐 수 있는 문서
Ciphertext	의도된 사용자에게만 읽힐 수 있는 형식으로 작업된 메시지 공격자가 해석 할 수 없거나 그 콘텐츠를 확인 할 수 없는 메시지
Encryption	평문을 암호문으로 바꾸는 암호화 과정
Decryption	암호화 알고리즘과 키를 이용하여 암호화된 데이터를 평문으로 바꾸는 과정
Key	데이터를 암호화 및 복호화하는 알고리즘의 동작을 결정짓는 값

1-2. 암호학의 용도

암호학이 사용되는 용도는 다음의 표를 통해 알 수 있다.

[표 2] 암호학의 용도

구분		용 도
주요 용도	기밀성	– 정보의 부적당한 유출을 방지(Preventing), 탐지(Detecting), 제지(Deterring) 하는 것 – 일부 부서에만 공개되는 정보가 다른 부서에 노출되는 것을 방지
	무결성	– 정보의 부적절한 변경을 예방하고 감지하는 특성 – 타인이 다른 사람의 정보를 임의 또는 불법적으로 변경하지 못하도록 하는 경우
	가용성	– 시스템이 제공하는 서비스에 대한 부적절한 거부를 예방하고 감지하는 특징 – 사용자가 데이터에 접근하지 못하거나 자원을 사용하지 못하도록 하는 경우가 발생되지 않도록 하는 부분이 해당
부가적 용도	부인 방지	– 부인방지는 메시지의 송수신에 참여한 당사자들의 행위를 부인 할 수 없도록 고안된 보안 서비스
	인증	– 정당한 사용자임을 확인 – 인증을 통하지 않은 데이터베이스의 정보 누출 방지
	접근 통제	– 비인가자가 정보통신 시스템에 부정한 방법으로 접근하여 사용하는 것을 방지

1-3. 암호학의 유형

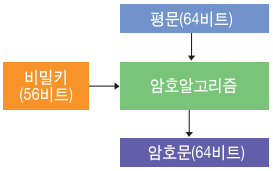
암호화 방식에 따른 유형은 블록 암호와 스트림 암호로 구분된다.

(1) 블록 암호

– 비트의 평문을 입력으로 하며, k 비트의 키를 변수로 하여 n 비트 암호문을 출력하는 함수를 이용하는 암호.

– 스트림 암호에 비해 기밀성이 요구되는 분야뿐만 아니라, 해쉬 함수, 인증 방식 등에 응용되므로 스트림 암호에 비해 매우 다양하다.

– 사례: DES, IDEA, SEED, RC5, AES



[그림 3] 블록 기반 암호화

(2) 스트림 암호

– 비트 단위로 암호화 하는 함수를 이용하는 암호이며, 에러 전파 현상이 없고, 블록 암호에 비해 속도가 빠르며, 구현이 쉽다.

– 수학적 분석이 가능하며, 여러 가지 수치에 대한 이론적인 값을 정확히 구할 수 있다.

– 사례: LFSR, MUX generator, BRM generator

[그림 4] 스트림 기반 암호화

1-4. 암호 시스템

앞에서 설명한 암호화 유형인 블록 기반 암호화와 스트림 암호화는 암호화 단위에 따른 암호화 유형이었다. 이제부터 설명 할 암호 시스템은 암호화를 하는 가장 기본적인 방법을 의미하며, 대치 암호화 치환 암호로 구분 할 수 있다.

(1) 대치 암호(Substitution Cipher)

– 하나의 기호를 다른 기호로 대체하는 암호화 방식.

– 예: 알파벳 26자를 각각 다른 알파벳에 일대일로 매칭.

(2) 치환 암호

– 한 기호의 위치를 바꾸는 암호화 방식.

– 예: 첫 번째에 위치한 기호를 열 번째 위치로 이동한다.

1-5. 암호화 알고리즘

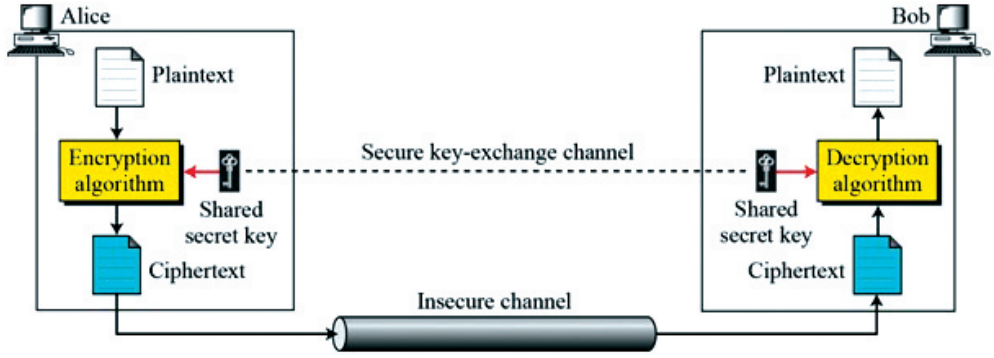
우리는 암호 유형과 암호 시스템을 실제로 구현한 암호화 알고리즘을 사용하고 있다. 대표적인 암호화 알고리즘은 대칭키 알고리즘과 비대칭키 알고리즘으로 구분된다.

(1) 대칭키 알고리즘

– 암호키와 복호화키가 동일한 암호화 방식.

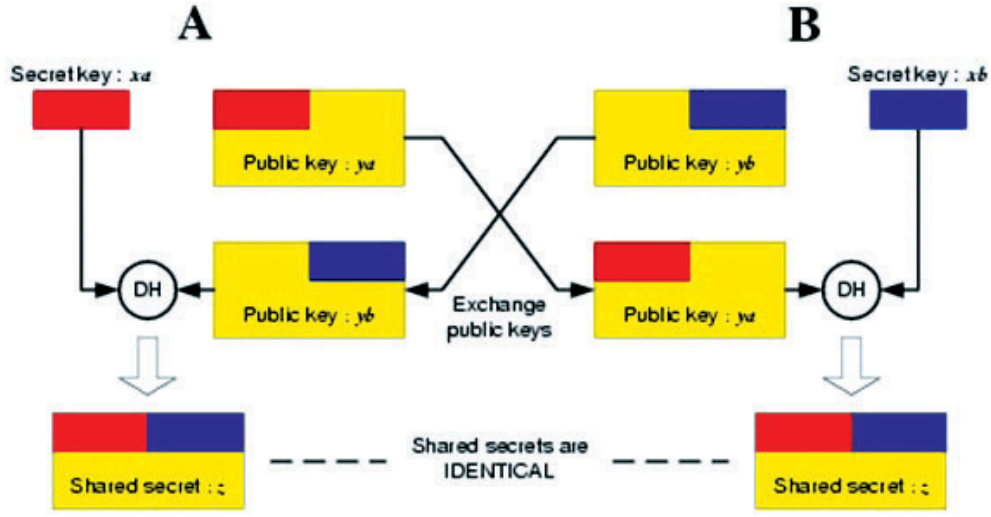
– 송신자와 수신자는 항상 동일한 비밀키를 공유해야 하는 방식.

– 비대칭키에 비해 상대적으로 처리 속도가 빠른 것이 장점.
– 비밀키를 교환하는 방법에 취약하여, 보안 문제 발생 가능이 상존.
– 전체키의 수는 N(N–1)/2개의 키가 필요함.
– N = 송신자와 수신자 수



[그림 5] 대칭키 알고리즘 작동 방식

(2) 비대칭키 알고리즘
– 암호화와 복호화를 위한 키가 서로 다른 암호화 방식.
– 주로 인증과 전자서명에 유용하게 사용되는 방식.
– 대칭키와는 달리 키를 분배하는 알고리즘을 가지고 있는 것이 장점.
– 대칭키에 비해 상대적으로 처리 속도가 느린 것이 단점.
– 전체키의 수는 2N개의 키가 필요함.



[그림 6] 비대칭키 알고리즘 작동 방식

[표 3] 대칭키 암호화와 비대칭키 암호화 비교

항목	대칭키	공개키
키의 상호관계	암호화키=복호화키	암호화 키≠ 복호화 키
암호화 키	비밀	공개
복호화 키	비밀	비밀
암호 알고리즘	비밀/공개	공개
비밀키 전송	필요	불필요
키 개수	N(N-1)/2	2N
안전한 인증	곤란	용이
암호화 속도	고속	저속
경제성	고	저
전자서명	복잡	간단
해당 알고리즘	DES, FEAL, RC5, IDEA, AES, SEED	RSA, ECC, DSA

지금까지 암호학에 대해서 살펴보았다. 암호학은 정보보호 시스템의 가장 기본적인 기술로써, CISSP 합격을 위해서는 꼭 필요한 기술적인 기본 지식을 제공한다. 따라서, 충분한 학습이 필요하다.

정리해보면, 암호학에서 주로 출제되는 주요 부분(Key Factor)은 [표 4]와 같다. 또한, 암호학은 전통적으로 많은 문제가 출제되는 중요한 도메인이나, 최근에는 그 비중이 줄고 있다. 따라서, 출제비중은 "보통"이다.

[표 4] 암호학 Key Factor

분야	Key Factor	출제 비중
암호학	– 대칭 및 비대칭 알고리즘 이해 – 공개키 기반구조(PKI), 커버로스(Kerberos) 이해 – 암호화 프로토콜과 구현 방식 학습 – 공격 방식 및 대응방법 학습	보통

2. 응용프로그램 보안 (Application Security) 요점정리

컴퓨터에서 우리가 접하는 것은 모두 응용프로그램(Application)이라고 볼 수 있다. 즉, 응용프로그램이 있어야 컴퓨터라는 물리적인 시스템을 운영할 수 있으며, 우리가 원하는 결과를 얻을 수 있다. 컴퓨터가 몸체라면 응용프로그램은 뇌가 된다고 볼 수 있다. 이렇게 응용프로그램의 중요성이 높음에 따라, 이러한 뇌를 감염시키고, 파괴하려는 응용프로그램을 공격 또는 착취하는 공격들이 증가하고 있다. 따라서, 응용프로그램 보안 도메인은 오늘날의 응용프로그램이 구동되는 환경과 매커니즘에 대한 지식 기반 위에 대표적인 응용프로그램 공격인 악성코드에 대한 유형과 대응책을 설명하고, 이러한 응용프로그램의 자원이 되는 데이터베이스에 대해 알려주는 도메인이다.

최근에는 대부분의 공격이 악성코드로 대표되는 응용프로그램을 이용한 공격으로서, 도메인의 중요도가 증가하고 있다.

응용프로그램 보안 도메인에서 학습해야 할 요점들은 다음 Domain Map을 통해 한 눈에 알 수 있다.

[그림 7] 응용프로그램 보안 Domain Map

2-1. 오늘날의 응용프로그램의 환경

(1) 오픈 소스

- 소프트웨어의 소스코드가 사용자의 상황에 맞게 변경 될 수 있도록 배포되는 방식.
- 오픈 소스에 대한 대중의 시각은 두 가지로 구분된다. 하나는 오픈 된 소스 코드를 여러 사람이 보게 되면 모든 버그들이 드러나게 되어 보안성이 높아진다는 찬성의견을 가진 시각과 다른 하나는 단지 소스를 오픈하는 것만으로는 모든 버그들을 발견할 수 없으며, 정직하지 못한 프로그래머가 오픈 소스의 취약점을 발견하여 이를 공개하지 않고 소프트웨어 벤더를 협박하는데 이용 할 수 있다라는 반대 시각으로 구분된다.
- (ISC)²의 CBK에 따르면, 시스템에 대한 정보를 숨겨서, 보안을 강화하는 방안인 은닉을 통한 보안(Security by obscurity)은 제일 좋은 효과를 낼 수 없다. 또한, 역공학을 통해 충분히 소스 또는 실행 파일 형태에 상관없이 보안 취약점을 분석 할 수 있기 때문에, CBK에서는 소스의 오픈 여부가 중요한 게 아니라, 어떻게 설계되었는지가 보안에 중요하다고 말하고 있다. 즉, 설계 초기에서부터 보안을 고려하여 설계해야 하는 것이 중요하다는 것을 강조하고 있다.

(2) 응용프로그램의 주요 보안 위협

- 버퍼 오버플로우(Buffer overflow): 프로그램이 통제하는 버퍼 길이보다 많은 양의 데이터로 버퍼를 채울 때 발생하는 문제로, 버퍼 길이를 넘어서 메모리를 채울 때 프로그램 실행 경로가 변경되어 관리자 권한 등 특수 권한을 획득하기 위해 사용하는 방법.
- 은닉 채널(Covert Channel): 인가되지 않은 사람에게 정보를 전달하기 위한 의도로 만든 숨겨진 정보교환 통로이며, 메모리나 디스크 섹터와 같은 저장 공간에 데이터를 공유하는 Covert Storage Channel과 Timing 관찰을 통해 정보를 전달하는 Covert Timing Channel로 구분된다.

지금까지 응용프로그램의 위협에 대해서 살펴보았다. 언급한 위협 외에 사회공학, 모바일 코드, TOC/TOU들이 있으나, 지면 관계상 주요한 위협만을 설명하였다. 특히, 악성코드는 많은 유형을 가지고 있으므로 다음 장에서 상세히 설명하겠다.

2-2. 악성코드(Malware)

시스템에 침투하고, 보안 정책을 위반하고, 피해를 입히는 기능을 하는 소프트웨어.

(1) 악성코드의 유형

- Virus: 다른 프로그램의 소스 내에 자신을 포함시켜서 원하는 목적을 수행하고자 하는 프로그램이다. 감염기능을 가지고 있어 확산이 가능하다. 치료를 위해서는 소스코드를 수정해야 한다.
- Worm: 네트워크 공유 폴더나 취약점을 통해 자체 확산되며, 주로 네트워크 공격을 위한 목적을 가진 악성 프로그램이다. 자체 확산 기능을 가지고 있으며, 치료를 위해서는 해당 파일을 삭제하면 된다.
- Torjan: 정상적인 일을 수행하는 척하면서 다른 비정상 일을 수행하여 주로, 사용자의 정보를 탈취하는 프로그램이다. 자체 확산 기능이 없으며, 치료를 위해서는 해당 파일을 삭제하면 된다.
- Logic Bomb: 조용하게 특정 조건을 모니터링하다가 특정 조건을 만족한 순간에 실행되는 악의적인 프로그램이다.

- Spyware/Adware: 광고나 개인정보를 수집하기 위한 목적으로 사용자의 동의 없이 설치되는 악의적인 프로그램이다. 다양한 기능(자체 업데이트 기능, 정보 수집 기능 등)을 가지고 있어, 치료를 위해서는 해당 프로그램 전체를 Uninstall해야 한다.
- DDoS: 특정 대상을 공격하기 위해 여러 대의 시스템을 이용하여 대상이 되는 시스템의 가용성을 저해하는 공격을 한다.

(2) 악성코드에 대한 대응책

- 훈련과 보안 정책: 사용자에 대한 훈련과 명확한 보안 정책, 가이드라인 등을 통해 악성코드로 인한 위험을 지킬 수 있다.
- Anti-Virus 소프트웨어: 악성코드를 탐지하여 치료 및 삭제를 통해 원래 상태로 시스템을 교정하는 프로그램이다. 악성코드의 특정 내용을 탐지하는 Signature 기반의 Scanner와 의심스러운 행동 모니터링을 통해 탐지하는 Activity Monitor, 시스템 및 프로그램 파일의 구성정보 변화를 통해 탐지하는 Change Detecting 등이 있다.

지금까지 악성코드의 유형과 대응책에 대해서 살펴보았다. 지금부터는 이러한 악성코드의 위협부터 응용프로그램을 보호하기 위해서 정책적으로 수행해야 하는 감사, 보증 매커니즘에 대해서 알아보겠다.

2-3. 감사, 보증 매커니즘

외부의 위협으로부터 응용프로그램을 보호하기 위한 정책적인 방법으로 감사 및 보증 매커니즘이 사용된다. 감사 및 보증 매커니즘에는 인증, 인가, 변경관리가 있다.

- 인증(Certification): 응용프로그램의 보안 준수사항을 기술적으로 평가하고 시스템이 기능적 요구사항을 만족하는지를 사용자 및 관리자가 평가하여 승인하는 절차.
- 인가(Accreditation): 인증 받은 응용프로그램의 사용여부를 경영진이 공식적으로 사용을 승인하는 절차. 따라서, 최종적으로 응용프로그램의 기술적 여부를 판단하여 인증여부를 결정하고, 인증 받은 응용프로그램의 최종 적용여부는 경영진에서 판단한다고 볼 수 있다.
- 변경관리(Change Management): 응용프로그램의 내외부 환경변화로 인해 수정이 필요 할 경우, 응용프로그램의 품질보증을 위해 공식화된 절차에 의해서 변경을 수행하고 이를 적용하는 관리 기법.
- 형상관리(Configuration Management): 응용프로그램뿐 아니라, 프로그램과 관계된 문서들에 대해서 변경관리를 수행하는 기법으로써, 모든 구성품에 대한 무결성과 가용성 보장을 위해 전체 구성물의 변화를 관리하는 기법. 변경관리는 형상관리의 부분이라고 볼 수 있다.

지금까지 응용프로그램의 보안성을 높이기 위한 정책적인 절차에 대해 학습하였다. 하지만, 궁극적으로 응용프로그램이 보호하고자 하는 것은 자료. 즉, 데이터이다. 이제부터는 데이터를 공유하기 위한 목적으로 축적된 데이터베이스에 발생하는 위협과 대응책에 대해 알아보자.

2-4. 데이터베이스

(1) 데이터베이스 위협

- Aggregation: 개별적인 여러 소스로부터 민감하지 않은 정보를 수집, 조합하여 민감한 정보를 생성하는 보안 위협.
  예) 각 지사의 영업 실적을 조합하여 대외비인 회사의 총 매출액을 알아냄.
- Inference: 접근 가능한 정보를 관찰하여 또 다른 정보를 유추하는 보안 위협.
  예) 보안 등급이 없는 사용자가 비밀로 분류되지 않은 정보에 정당하게 접근하여 비밀 정보를 유추해 내는 행위.

(2) 데이터베이스 위협에 대한 대응책

- Lock 통제: 한 번에 한 사용자만이 특정 데이터에 대한 작업을 수행하도록 제어하는 방법.
- View 기반의 접근 통제: 논리적으로 민감한 정보들이 비인가된 사용자들에게 숨겨지도록 하는 방식으로 관리자는 사용자별로 View를 설정 할 수 있음.

지금까지 응용프로그램 보안에 대해서 알아보았다. 응용프로그램 보안은 최근에 많이 출제되므로, 응용프로그램의 위협과 대응책에 대해서 잘 알고 있어야 한다. 주요 출제분야를 확인하기 위해 Key Factor를 참고하기 바란다.

[표 5] 응용프로그램 보안 Key Factor

분야	Key Factor	출제 비중
응용프로그램 보안	– 데이터 웨어하우징과 데이터 마이닝 이해 – 다양한 개발수행과 수반되는 위험 숙지 – 시스템 스토리지와 처리 구성요소 숙지 – 시스템 개발 수명 주기 이해 – 악성 코드 및 대응법 숙지	높음

이번 호에는 암호학 및 응용프로그램 보안 도메인을 살펴보았다. 암호학은 전통적으로 출제빈도가 높았으나 차츰 낮아지는 추세이며, 응용프로그램은 최근의 보안 이슈들로 인해 출제빈도가 높아지는 추세이다. 따라서, 암호학은 기본적인 지식위주의 학습이 필요하며, 응용프로그램 보안은 위협과 대응책을 상세히 학습해야 한다.

다음 호에는 나머지 4가지 CISSP 도메인 중에서, 지금까지 학습한 관리적, 기술적 지식들을 현장에서 활용하는 분야인 BCP와 운영 보안 도메인에 대해서 알아보고자 한다.

3. 연습 문제

간단한 문제를 통해서 이번 호에서 배운 도메인에 대한 이해능력을 키우자. 중요한 것은 실제 시험에서는 이보다 어려운 문제가 출제되나, 기본을 알면 충분히 풀 수 있는 문제이니, 문제를 풀고 잘못 이해하는 부분은 요점정리를 통해 재학습이 필요하다.

▣ 암호학

1. 어떤 이미지 속에 숨겨서 의미를 전달하고자 하는 다른 이미지를 넣어서 정보를 특정인에게만 모르게 전달하는 방식을 무엇이라고 하는가?
   ① 워터마킹 ② 스테가노그라피 ③ 암호화 ④ Scytale

2. 공개키 암호 시스템을 개발한 사람은 누구인가?
   ① Hellman ② David Kahn ③ Fred Cohen ④ Adi Shamir

3. Bob과 Alice가 암호화된 문서를 전송 할 때 사용하는 비밀키(개인키)를 교환할 때 사용하는 암호키 교환방식은 무엇인가?
   ① 스테가노그라피 ② 전자서명
   ③ 비대칭키(공개키) 암호화 ④ 대칭키 암호화

4. DES의 여러 모드 중 한 방식으로 초기화 벡터인 IV(Initialization Vector)와 평문블록을 XOR하여 송신자와 수신자 모두 IV를 알고 있으며, 보안성을 강화하는 방식은?
   ① ECB ② CBC ③ CFB ④ OFB

5. 인접한 노드 사이의 통신에서 통째로 암호화 하는 방식은 무엇인가?
   ① 공개키 암호화 ② 개인키 암호화 ③ 터널 암호화 ④ 링크 암호화

▣ 응용프로그램 보안

1. 소스가 변경되었을 경우 언제 릴리즈해야 하는가?
   ① 테스트가 정상적으로 수행되었을 때
   ② 보안관리자가 확인하였을 때
   ③ 경영진이 승인하였을 때
   ④ 소스가 변경되는 즉시

2. SMTP, Telnet, FTP를 보다 안전하게 사용하기 위해 사용하는 것은?
   ① SSL ② SSH ③ S/MIME ④ WEP

3. 다음 중 바이러스의 한 유형에 속하지 않는 것은?
   ① Multipartite ② Mimic ③ Macro ④ Parasitic

4. 네트워크를 통해 전파하는 악성코드는 무엇인가?
   ① 바이러스 ② 트로이목마 ③ 매크로 ④ 웜

5. 다음 보기 중 모바일 악성코드로부터 시스템을 보호하기 위해 믿을 수 있는 벤더에서 제작된 ActiveX라는 것을 확인시켜주는 방법은 무엇인가?
   ① SSL ② Applet ③ Sandbox ④ 디지털인증서

정답 : ②, ①, ③, ②, ④, ③, ②, ②, ④, ④

+ 서영우 · KBS 방송기술연구소 수석연구원

분산중계기와 DOCR 시스템의 이해

1. 개요

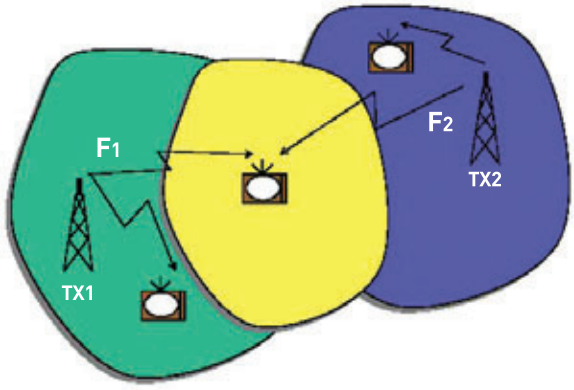
2012년 지상파 TV의 디지털 전환을 앞두고 2010년 9월 경북 울진군에서는 의미 있는 행사가 있었다. 전국 최초로 아날로그 TV를 종료하고 디지털 TV(DTV)로 완전 전환을 한 것이다. 울진의 DTV 전환에는 또 다른 의의가 있다. ATSC를 채택한 국가 중 최초로 기존 DTV 중계 방식인 다중 주파수 방송망(MFN, Multiple Frequency Network)이 아닌 지역적 단일 주파수 방송망(RSFN, Regional Single Frequency Network)이 도입된 것이다.

RFSN이란 기존의 광역 SFN(Single Frequency Network)과는 달리 국부적인 지역을 하나의 주파수 망으로 묶는 방식을 의미하며, SFN으로 구축하기엔 고스트 처리 능력이 부족한 디지털 방송 방식에서도 채택가능한 방식이다. RFSN에서는 주로 중계기들이 SFN을 구성하게 되며, 대부분 소출력으로 운용되며, 분산중계기, DOCR(Digital On-Channel Repeater) 등이 그 예이다.

[그림 1]에서 2대의 송신기(TX, Transmitter)가 서비스 하고 있을 때 두 송신기의 주파수(F, Frequency)가 같다면(F1=F2) SFN이고, 다르다면(F1≠F2) MFN이라고 한다. 이 때 가운데 영역의 시청자는 둘 중 하나의 신호를 수신 할 수 있는데 SFN인지 MFN인지에 따라서 수신 환경이 매우 달라진다.

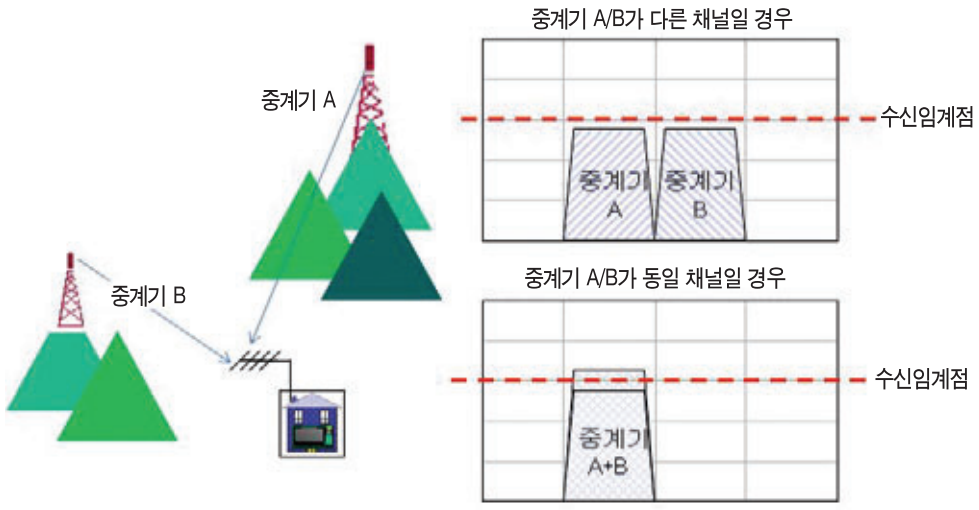
중계기간의 주파수가 다른 MFN에서 수신기는 일반적으로 둘 중 하나의 채널로 고정하여 수신하므로 다른 채널의 중계기 신호가 좋더라도 현재 수신 채널의 상태가 좋지 않다면 수신을 못 할 수 있다. 대신 주파수가 상이하므로 출력을 높여서 각 중계기의 수신율을 확보하기 위한 조치를 취할 수 있다.

RSFN에서와 같이 두 중계기의 신호가 같다면 수신기 입장에서는 두 중계기의 신호를 모두 수신하고 있다가 더 좋은 상태의 신호를 기준으로 수신신호를 선택할 수 있으므로 다이버시티(diversity) 효과를 기대 할 수 있다. 다만 두 중계기의 신호가 시차를 두고 들어오므로 선택되지 않은 신호는 간섭신호로 작용하기 때문에, 각 중계기의 출력이 매우 정밀하게 조정이 되어야 하며, 수신기의 고스트에 대한 처리 성능이 양호한 한도 내에서 해당 방식의 적용이 가능하다.



[그림 1] 방송망의 구성

따라서, RSFN이 성공적으로 도입되려면, ATSC 수신기의 수신 성능을 고려한 방송망 설계가 필수적이며, 이는 엄밀한 방송망 설계 및 측정을 통한 검증이 반드시 이루어져야 한다.



[그림 2] MFN과 RSFN의 비교

본 글에서는 ATSC에서 RSFN이 어떻게 구현이 가능한 지 SFN의 구성 원리와 울진 등 디지털 전환 시범지역에 도입된 RSFN 중계기 기술에 대해 간략히 소개하고, ATSC에서 RSFN이 어디까지 적용이 가능 할 수 있을 지 논의해 보고자 한다.

2. SFN의 기본 원리

SFN이 가능하려면, 송신 측면에서는 다음의 세 가지 요건이 반드시 충족되어야 한다.

① 주파수 일치 ② 타이밍 일치 ③ 데이터 일치

첫 번째, 주파수 일치란 SFN을 구성하는 두 개 이상의 송신기의 주파수가 완벽하게 동일해야 함을 의미한다. 만약, 주파수가 일치되지 않으면 수신기는 도플러(doppler) 효과처럼 두 개의 주파수 편차만큼 주파수 동기 성능이 나빠지는데 이는 마치 이동하며 수신하는 것과 같은 결과를 유발한다. 일반적으로 주파수 동기는 GPS위성에서 수신되는 10MHz 기준 주파수에 의해 맞추게 되나 중계기의 경우는 수신하는 모국의 주파수를 이용해 동기를 맞추는 방법도 제안되어 있다.

두 번째, 타이밍 일치란 송신기들의 송출 타이밍이 거의 일치해야 함을 의미한다. 앞서 주파수 일치와는 달리 완벽한 일치라고 하지 않는 이유는 송신점에서 동시에 송출하더라도 수신 위치에 따라서 전파 도착시간이 차이나기 때문에 완벽한 일치란 불가능하기 때문이다. 따라서, 송출 타이밍의 일치는 서비스하고자 하는 지역의 평균적인 수신점에서 송신기들로부터 수신한 신호가 적절한 시차 내에서 수신 될 수 있도록 하는 것을 의미한다. 이와 같은 송출 타이밍의 일치를 위해서는 각 송신기들이 마이크로웨이브 등으로 구성되는 연주소로 부터의 STL(Studio to Transmitter Link) 구간거리와 평균적인 수신점을 기준으로 한 수신기까지의 상대거리가 고려되어야 한다. 그리고, 수신점에서 각 송신기로부터 오는 신호를 식별해 낼 수 있도록 송신기에 TxID(Transmitter IDentification) 정보가 삽입되어 있어야 한다. 일반적으로 송출 타이밍 동기는 수신점에서 TxID를 분석 할 수 있는 수신기를 통해서 각 송신기로부터 오는 신호의 크기와 지연시간을 측정한 후, 원하는 범위 안으로 각 송신기의 지연시간이 위치하도록 송신기 내부에 위치한 송출 타이밍 조절장치를 이용하여 조정한다.

세 번째, 데이터 일치란 송신기들로부터 송출되는 데이터가 완벽히 일치함을 의미한다. 일반적으로 송신기들은 연주소로부터 MPEG TS(Transport Stream) 형태의 신호를 수신하여 이를 채널 부호화와 변조를 통해 송출하게 된다. MPEG TS가 전송을 위한 심벌로 변환되는 과정에서 부호화를 위한 메모리의 초기 값, 프레임 구성 방법 등이 정의되어 있지 않으면 같은 TS입력에 대해서도 서로 다른 송출 데이터로 변환하게 된다. 일반적으로 OFDM(Orthogonal Frequency Division Multiplexing) 전송 방식을 사용하는 시스템들은 SFN을 위해서 데이터 동기를 맞추기 위한 기준 신호가 제공된다. 따라서, 그러한 기준 신호에 의해 부호화 메모리와 프레임 구조를 동기 시킬 수 있으며, 이를 통해 데이터 동기를 이룰 수 있다.

SFN은 방송망이 하나의 주파수로 구성되는 것을 의미하며 분산송신이라는 용어로 설명되기도 한다. 그러나, 앞서 설명한 RSFN의 개념에서 주로 고려되는 것은 분산중계기와 동일채널중계기이다.

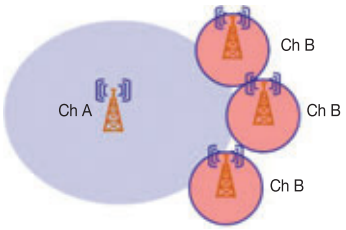
3. 분산중계기

분산중계(DTxR, Distributed Transmission Translation)란 주송신기(모국)의 신호를 받는 중계기들을 단일 주파수로 구성하는 것으로 [그림 3]과 같이 구성된다. 일반적으로 주송신기의 신호를 수신하는 중계기들과 수신점 사이의 방송망으로 구성되고, 주파수 동기는 GPS나 주송신기의 송신 주파수 정보를 이용해서 이루어진다. 송출 타이밍은 중계기마다 다른 주송신기 신호의 수신 시점과 각 중계기와 수신점까지의 지연시간을 종합적으로 고려하고, TxID의 측정 결과를 반영하여 조정한다.

분산 중계기를 구현하는 방법은 다양하다. ATSC의 분산송신표준(A/110)에서 제안한 분산송신 환경에서 적용되는 분산중계기와 국내 기술로는 ETRI에서 제안한 E-DTxR(Equalization DTxR), KBS에서 제안한 수신신호동기 DTxR이 있다.

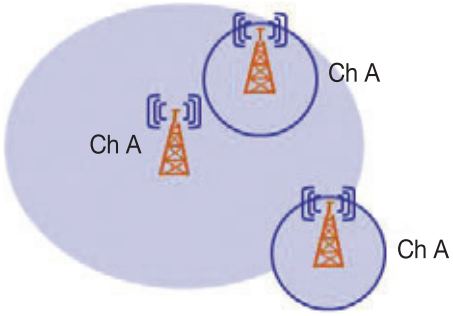
E-DTxR은 모국으로부터 수신한 RF 신호를 VSB 심벌수준까지만 복조한 후 이를 지능적 등화기를 통해서 8레벨의 심벌로 완벽히 복원한 후 원하는 채널로 재전송하는 시스템이다. 수신신호동기 DTxR은 모국의 수신 신호의 데이터 프레임 구조를 이용하여 패킷을 재변조하는 과정에서 새로운 패킷을 생성하여 데이터 동기를 구현한 시스템이다. [그림 4]는 KOBA 2009에서 전시된 2대의 수신신호동기 DTxR을 이용한 시연 시스템을 보여준다.

2010년 울진, 강진, 단양에 적용된 분산중계기는 E-DTxR 방식과 수신신호동기 DTxR이 설치되었다.



[그림 3] 분산중계의 개념

[그림 4] KOBA 2009에 전시된 KBS의 수신신호동기 DTxR

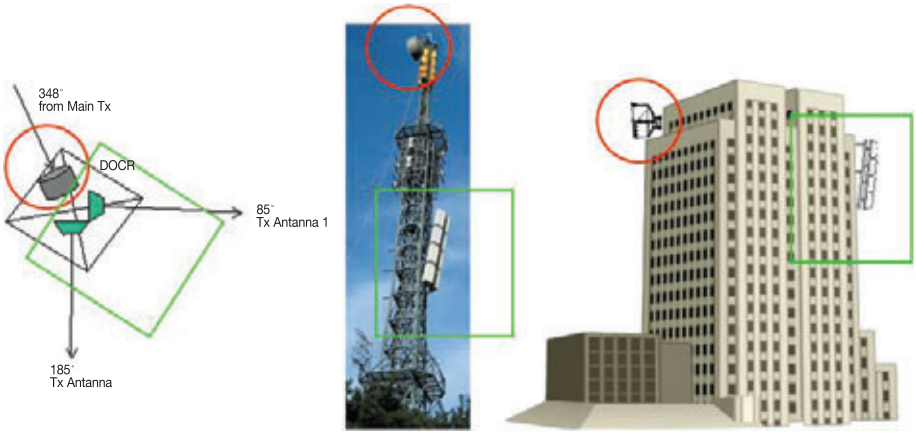


[그림 5] 동일채널중계의 개념

4. 동일채널중계기

동일채널중계(OCR, On-Channel Repeating)란 주송신기(모국)의 신호를 받는 중계기들이 주 송신기와 같은 주파수로 재송신하는 것으로 [그림 5]와 같이 구성된다. 일반적으로 주송신기의 신호를 수신하는 중계기들과 수신점 사이의 방송망으로 구성되고, 주파수 동기는 주송신기의 송신 주파수 정보를 이용해서 이루어진다. 다만, OCR의 특성상 송출 타이밍은 중계기 내부의 지연시간에 의해 정의되며, 이를 최소화하는 것이 서비스 지역의 수신 성능을 개선하는데 용이하므로 TxID를 삽입하여 송출은 가능하지만 타이밍을 추가적으로 조정하기 위한 구성을 갖지 않는 것이 일반적이다.

DOCR은 중계용 주파수를 따로 받을 필요가 없으므로 난시청 지역에 적극적으로 활용이 가능하다. 다만, 중계 신호가 다시 중계기로 들어오는 RF 피드백 간섭의 문제점이 있으므로 송신 및 수신안테나 사이의 적절한 격리(isolation)가 필요하며, 송신안테나 방향 역시 수신안테나에 간섭을 덜 주는 방향으로 조정해야 하므로 송출 출력 및 방향에 제약이 있다. 송수신 안테나 사이의 격리를 확보하는 방법은 [그림 6]과 같이 송신방향조정, 건물, 전파차단재 등의 활용을 통한 물리적인 차단 방법이 있다.



(a) 안테나 송출 방향 조정 (b) 안테나 설치 위치 조정 (c) 건물을 이용한 안테나 배치

[그림 6] 동일 채널 중계기를 위한 송수신 안테나 격리도 확보 방법

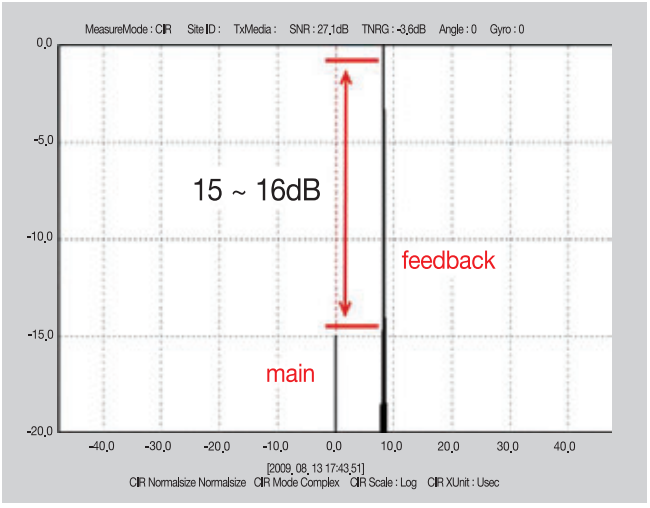
그러나, 이러한 물리적 방식의 한계를 극복하고 송출 신호 품질을 개선하기 위해 등화기(equalizer)와 ICS(Interference Cancellation System) 적응 필터 기술 등의 디지털 신호 처리 기술이 개발되어 DOCR의 응용 범위가 개선되었다.

현재 제안된 DOCR 방식으로는 RF 및 IF의 아날로그 채널 필터 방식의 아날로그 OCR, ETRI에서 제안한 E-DOCR(Equalization DOCR), 그리고 KBS와 (주)답스가 제안한 ICS DOCR 등이 있다.

E-DOCR은 모국으로부터 수신한 RF 신호를 VSB 심벌수준까지만 복조한 후 이를 지능적 등화기를 통해서 8레벨의 심벌로 완벽히 복원한 후 수신 주파수에 완벽히 동기를 시켜 재전송하는 DOCR이다.

ICS DOCR은 중계기에서 출력된 신호가 다시 수신안테나를 통해 유입되는 커플링 간섭(interference)을 제거하는 시스템을 의미한다. [그림 7]은 개발된 DOCR의 ICS 성능을 측정한 것으로 입력신호대비 최대 16dB 더 큰 간섭신호 상황에서도 정상적인 출력이 가능하므로 ICS 방식이 아닌 DOCR 대비 약 20dB 이상의 신호 마진을 더 확보할 수 있다. 이 방식은 2008년도에서 2009년도에 걸쳐서 KBS 여수 TVR에서 성공적으로 성능 검증이 완료되었으며, 2010년 미국 NAB 2010에 전시되어 미국 방송 관계자들의 많은 관심을 모은 바 있다.
E-DOCR과 ICS DOCR은 2010년 현재 미국에서 상용 시범 서비스가 진행 중인 ATSC 모바일 방송 방식(ATSC-M/H)에도 모두 적용이 가능하므로 국산 기술로서 향후 미국 수출 전망도 매우 밝다.

2010년 울진, 강진, 단양에 적용된 DOCR은 개선된 형태의 E-DOCR 방식이 설치되었다.



(a) KBS DOCR의 ICS 성능

(b) 여수 TVR에서 실험 중인 ICS DOCR

[그림 7] KBS ICS DOCR의 성능과 외관

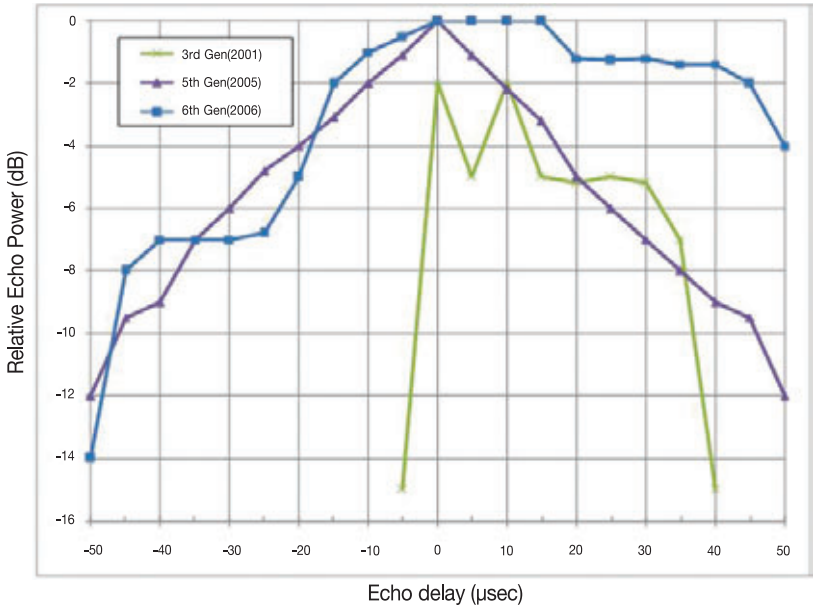
5. ATSC에서의 SFN 적용 가능성

ATSC는 1990년대 후반 미국과 우리나라에서 DTV 표준으로 채택되었다. 기술 표준 제정당시 ATSC는 2층 건물에서 안테나를 고정하여 수신하는 수신자를 표준 수신자로 하였으며, 송신기 및 중계기마다 다른 주파수를 사용하는 MFN을 기본 방송망으로 하였다. 따라서, 수신기의 고스트 처리 능력은 3㎲sec의 선행 고스트와 20㎲sec의 후행 고스트를 처리하도록 표준 수신기를 지정하였으며, SFN을 위한 데이터 동기 기준 신호는 송출 규격에서 고려하지 않았다.

전파의 진행 속도(30만km/sec)를 고려하면 1㎲sec는 약 300m를 진행한 고스트를 의미하며, 이를 수신 모델에 대입해보면 약 900m를 앞서온 선행고스트 및 6km를 돌아온 후행 고스트를 처리 할 수 있도록 하였다. 즉, 바로 인접한 건물의 반사파를 주 신호로 하거나 6km 이내의 지형 등에 의한 고스트의 발생을 표준 수신 환경으로 고려한 것이다.

그러나, 미국과 우리나라에서 방송엔지니어들을 중심으로 ATSC의 수신 성능에 대한 문제점이 제기 되었는데, 그것이 이 표준 수신환경에 대한 불합리성이었다. 그 이유는 표준 수신환경으로 제시된 것이 80년대의 일반 주택으로 이미 90년대부터 발달한 도심지 고층 빌딩이나 아파트의 수신환경이 제대로 반영되지 못한 것이었기 때문이다. 도심지에서 수신을 하면 직접파에 의한 수신보다는 반사파에 의한 수신이 많아지고 이 경우 후행 고스트만큼의 선행 고스트가 발생 할 수 있으므로 ATSC의 초기 비대칭 수신기 성능은 도심지의 수신율 저하라는 결과를 가져왔다.

ATSC는 문제를 해결하기 위해 가전사를 중심으로 ATSC 표준의 수신 성능을 개선하기 위한 많은 노력을 기울였으며, 그 결과 2003년 LG전자에서 제안한 5세대 수신기부터 선행 고스트에 대한 수신 성능이 비로소 개선되어 도심지의 수신 성능이 획기적으로 개선 할 수 있었다. 그리고, 선행 고스트의 성능 개선을 통해 다중 경로 간섭환경에 대한 수신율이 높아짐에 따라, SFN의 도입이 제한적으로 가능하게 되었으며, ATSC에서도 SFN을 구축하기 위한 전송 방식 개선 표준을 발표하였다.



[그림 8] ATSC 수신기의 세대별 고스트 처리 성능(괄호는 실험 대상 수신기의 출시년도)

다만, 수신기의 선행 고스트 처리 성능이 긴 지연시간을 갖는 고스트에 대해서는 2010년 현재에도 문제가 예상되므로 긴 지연시간의 선행 고스트를 유발하는 넓은 지역의 SFN보다는 국부적인 지역을 SFN으로 구성하는 RSFN의 도입이 지금 시점에서는 좀 더 실용적으로 판단된다.

여기서 수신 고스트 전력(receive echo power)이란 수신기가 수신하는 주 신호 대비 고스트의 상대 크기를 의미한다. 즉, 0dB의 고스트는 주 신호와 같은 전력의 고스트를 의미하고 3dB의 고스트는 주 신호보다 50% 정도 전력의 고스트를 의미한다. [그림 8]에서와 같이 2000년대 초반에 출시된 수신기보다 최근의 수신기가 선행 고스트 처리 성능이 월등히 개선된 것을 알 수 있다.

다만, 0dB의 선행 고스트를 50μsec 이상까지 무난히 처리하는 OFDM 방식의 수신기와는 달리 고스트의 지연이 길어질수록 선형적으로 감소하는 특성이 있다. 이 특성 때문에 긴 지연의 고스트가 발생하는 경우 강한 고스트는 처리하지 못 할 가능성이 있으므로 현재 시점에서는 긴 고스트가 발생하지 않도록 하는 RSFN을 적용하는 것이 바람직하다. 그리고, RSFN을 구성하였을 때 위의 수신기 고스트 처리 성능을 참고하여 서비스 구역 내의 고스트 발생 유형을 분석하고, 이에 따른 대책 마련이 필요하다.

RSFN의 서비스 구역 내에서 발생하는 강한 선행 고스트에 의한 수신 불량을 해소하기 위해서는 수신안테나의 방향을 조정하여 간섭신호의 크기를 좀 더 약하게 만드는 방법, 중계기의 송신 타이밍을 조정하여 간섭 신호가 좀 더 주 신호에 가까이 위치하도록 하는 방법, 중계기의 송출 출력을 좀 더 약하게 조정하여 혼신지역 내의 간섭 신호의 크기를 줄이는 방법 등이 제안되어 있다.

RSFN의 고스트 환경 측정을 위한 장비로 KBS에서 개발한 채널분석기가 주로 활용된다. 이 장비는 세계 최초로 개발된 장비로 ATSC 수신환경에서 ± 50μsec의 고스트를 실시간으로 분석하여 [그림 9]와 같이 그래프로 출력한다. 분산중계 및 DOCR은 다중경로 간섭. 즉, 강한 고스트를 유발하는 중계방식이며, 이는 수신기 입장에서는 이득이 될 수도 있고 또 손실이 될 수도 있으므로 적절한 방송망 관리를 위해서는 고스트의 관리를 통한 방송망의 조정 역시 매우 중요한 과정이다.

이와 같이 RSFN은 수신 환경에 대한 면밀한 분석을 통해 수신기의 수신 범위에서 운용 될 수 있도록 적절한 망 설계가 필수적이다.

[그림 9] KBS DTV 채널분석기 외관과 여수지역 측정 결과 예시

6. 결론

우리나라의 DTV 방식으로 ATSC 방식이 선정되고 2001년 본방송이 시작된 이래, DTV의 수신 성능은 초장기의 우려를 딛고 많은 발전을 통해 공시청 안테나를 통한 도심지 수신 성능이 비약적으로 개선되었다.

SFN을 구축하기 위해서는 송신 주파수, 타이밍 및 데이터의 동기를 이루는 송신망의 구축이 필수적이다. 하지만, 현재 우리나라에서 서비스하고 있는 ATSC 표준은 SFN이 고려된 규격이 아니어서 일반 표준 송·중계기를 SFN에 활용 할 수 없다. 그러므로, 국내 기술진은 이를 극복하기 위해 다양한 기술을 제안하였으며, 마침내 분산중계기와 DOCR 및 다중채널환경을 측정하는 계측기 등을 상용화하는데 성공하였다.

2010년 9월에 울진을 시작으로 강진, 단양으로 이어지는 디지털 전환 시범지역은 국내 기술진이 개발한 분산중계기와 DOCR이 설치되어 RSFN 구축하는 시범지역이기도 하다. RSFN 기술을 활용하면 주파수를 변환하는 중계기와 달리 수신자가 두 개 이상의 송신 신호 중 더 좋은 것을 수신하는 수신 성능 개선 효과를 기대 할 수 있다. 하지만, 수신기가 처리 할 수 없는 강한 선행 고스트에 의한 수신 불량도 발생할 수 있어 일부 지역의 수신 환경이 열악해 질 수 있다.

향후, 이들 시범지역의 방송 신호 환경을 면밀히 분석한다면, 방송사에서 추구하는 지상파 DTV 난시청 해소와 안테나를 통한 직접 수신율의 개선을 위해 분산중계기와 DOCR를 어떻게 활용 할 수 있는지 다양한 수신환경 변화 및 혼신발생 유형 등의 분석을 통해 확인 할 수 있을 것이다. 이들 분석결과는 2012년의 아날로그 TV 종료 이후 적극적인 DTV 난시청 해소 전략을 세우는데 많은 기여를 할 것으로 기대된다.

참고 문헌

[1] ATSC, "Standard A/53: ATSC Digital Television Standard," Advanced Television Systems Committee, April 2001.

[2] ATSC, "Standard A/110: Synchronization Standard for Distributed Transmission," Advanced Television Systems Committee, July 2004.

[3] H. M. Kim, S. I. Park, H. M. Eum, Y. T. Lee, J. H. Seo, J. Y. Lee, and J. S. Lim, "Development of Distributed Translator," 57th IEEE Broadcast Symposium, Oct. 2007.

[4] Young-Woo Suh, Jaekwon Lee, Jin-Yong Choi and Jong-Soo Seo, "A Novel Data Synchronization Method for ATSC Distributed Translator", IEEE PIMRC, Sep. 2009.

[5] Young-Woo Suh, Sung Ik Park, Ha-Kyun Mok, Heung Mook Kim, Jin-Yong Choi, Jong-Soo Seo, "Network Design and Field Application of ATSC Distributed Translators," IEEE Trans. On Broadcasting, Vol. 56, Issue 2, June 2010.

[6] S. W. Kim, Y.-T. Lee, S. I. Park, H. M. Eum, J. H. Seo, and H. M. Kim, "Equalization digital on-channel repeater in single frequency networks," IEEE Trans. on Broadcasting, vol. 52, no. 2, pp. 137-146, June 2006.

[7] Jaekwon Lee, Young-Woo Suh, Ha-Kyun Mok, Man-Sik Kim, Min-Ho Park, Jong-Soo Seo, "Performance of Feedback Cancellation for Digital On-Channel Repeater in ATSC DTV System", Broadcast Asia, Singapore, 2009.