전파연구소 제50호, 1993년 연구보고서

전파정보누설 방지기술 연구

김장순, 염호선

요 약 문

1. 제목 : 전파정보누설 방지기술 연구

2. 연구의 목적 및 필요성

현대와 같이 정보화사회가 급속히 발전되어감에 따라 정보처리 기기들의 사용이 증가하고 더욱 가속화 되고 있다.

하지만 이렇게 각 분야에 보급되어 이용되는 정보처리 기기로부터 방출되는 불요전자파에는 취급하는 중요정보가 포함되어 있어 정보누출의 위험성이 매우 큰바 주(Host)컴퓨터, 퍼스날컴퓨터 등과 같이 중요 정보를 취급하는 기기 및 주변장치, 데이타 통로(인터페이스)등으로 부터 정보누출을 방지하기 위한 대책을 제시하고 장래 전파정보누설의 보호유지를 위한 관련기술 개발에 대비한 조사 연구

3. 연구내용

가. 정보누설의 형태와 경로 연구

나. 정보누설 방지대책에 관한 기술조사

다. 정보누설 방지대책 관련 동향 조사

라. 정보누설 탐지 기술 조사

4. 연구결과

정보누설 방출원 유형, 정보누설 방사경로 등을 조사하여 정보누출의 원인을 파악하고자 하였으며, 정보누출 방지대책에 대한 기술 및 외국의 동향을 조사하여 컴퓨터 및 그 주변장치, 데이타 통로(인터페이스)등에 대한 정보보호 대책을 제시하고, 정보누설 탐지기술을 조사하여 정보누설의 위험성을 환기시키고 정보보호의 중요성을 부각시키고자 하였다.

5. 기대효과

o 국가기관, 공공기관, 산업체, 은행등의 중요정보를 취급하는 정보기기에서의 정보누출 방지와 보호

o 관련 연구의 중요성에 대한 인식확산 및 심도성 있는 연구 활성화

A B S T R A C T

I. TITLE

Study on TEMPEST shielding technology against leakage from electronic produlct and system

II. Purpose and Necessity of Study

The use of various data processing equipment has been rapidly increasing along with the fast evolaement of information society.

Unwanted frequency emission leaked out by electronic products naturally contain critical information which is vulnerable to technical eavesdropping.

The study presents countermeasures against TEMPEST leaks from host computer, personal computer, periferal and interfacial path, and describes the necessity of technology development associated with shielding against TEMPEST leaks.

III. Contents of Study

- o Type and source of TEMPEST leaks.
- o Technological review of shielding against TEMPEST leaks.
- o Overseas trend of shielding technology asainst TEMPEST leaks.
- o Surveillance technique of TEMPEST leaks.

IV. Results of Study

The study purports to grasp the causes of TEMPEST leaks by examining types of emission sources - TEMPEST leaks, describe shielding technology at large against TEMPEST leaks and review overseas technological development.

At presents a solution for shielding against TEMPEST leaks associated with Computer, periferal and interfacial path, and vulnerability of TEMPEST leaks and importance of shielding by reviewing surveillance techniques TEMPEST leaks.

V. Expected Effects

o Recognition of importance to shield and protect against TEMPEST leaks in operating data processing equipment and system at goverment administration, public organization, industries and banks as well.

o Diffusion of recognition for the importance of the theme (TEMPEST leaks and protection) and activation of the associated research activities.

목 차

제1장 서 론

최근 반도체 및 디지탈 기술의 급속한 발달에 따라 전기·전자장비 및 각종 정보통신 기기들이 경량화, 소형화, 고집적화가 가능하게 되었으나 미소한 전자파 장해에도 민감하게 반응하여 오동작을 일으킬 확률이 높아지게 되었고, 또한 현대 문명사회 전반에 전자파 응용 분야가 확대되어 감에 따라 전자파 밀집도가 증가하게 되어 전자파 환경은 점점 더 열악해져 가는 실정이다.

특히 근래에 정보·통신산업의 급격한 발전에 따라 컴퓨터나 모뎀 또는 프린터 등 전자파적으로 노이즈한 디지탈 신호를 이용하는 디지탈 정보처리 기기들이 사회전반에 널리 보급되고 있어 이들로부터 방사되는 전자파잡음이 경제적, 사회적, 기술적 이슈가 되고 있다.

이러한 추세는 현대와 같이 정보화 사회가 발전되어 감에 따라 개인·사회 및 국가관련 정보의 양과 질이 확대되고 정보의 처리·교환이 시·공간적으로 분산됨으로써 정보처리 기기들의 사용이 급격히 증가함으로 인하여 더욱 가속화 되고 있다.

또한 현대사회의 각 분야에 보급되어 이용되고 있는 디지탈 정보기기로 부터 방출되는 불요전자파에는 이들이 취급하고 있는 실시간 정보를 포함하고 있어서 정보누출의 위험성이 매우 크지만 이에 대한 사실이 거의 알려져 있지 않는 상황이며 우리의 중요정보(개인, 은행, 기업, 공공기관, 국가기관의 자료)는 타인이나 다른나라의 고도 도청기술에 의해 탐지될 수 있으나 우리의 경우는 아무런 대책없이 방치된 상태라 할수 있다.

이미 선진국의 경우는 이러한 디지탈 정보기기로부터 정보누출을 방지하고 탐지하는 연구가 비밀리에 수행되어 오고 있으며 이러한 기술을 타국의 중요산업 정보등을 탐지 하는데 적용시키고 있을 것으로 사료되는 바이다.

따라서 본고에서는 정보누설에 대한 개념과 정보누설의 형태와 경로 등을 다루고 또 정보누설의 문제점을 극복하기 위한 정보누설방지 대책에 관한 기술 및 외국의 동향과 정보탐지기술을 고찰하여 정보누설의 위험성과 정보보호의 중요성을 인식시켜 정보보호 대책 제시에 주안점을 두고자 한다.

제2장 정보누설의 형태와 경로

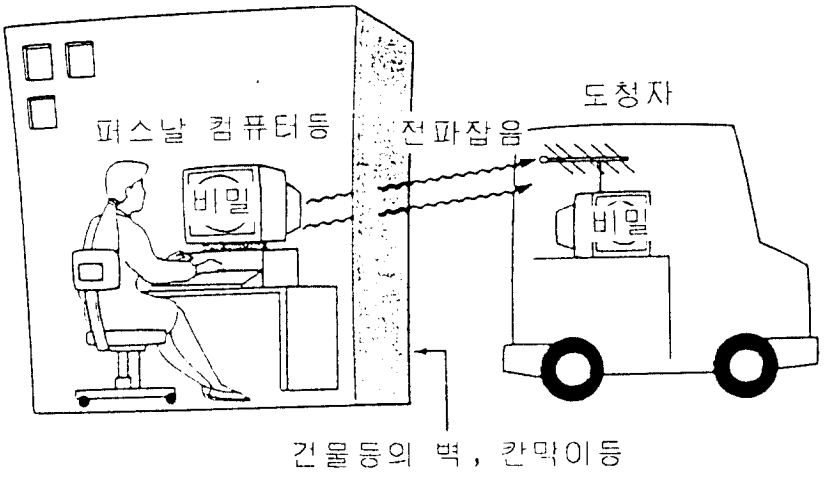
1. 정보누설의 개요

근래 전자기술의 급격한 발전에 따라 컴퓨터, 모뎀, 프린터등 정보처리 기기들이 사회전반에 걸쳐 사용되고 있는 실정이다. 정보누출이란 이러한 정보처리 기기 본체나 주변장치들로부터 기기고유의 미약한 전자파가 방출되는데 이들의 미약한 전자파에는 사람들이 취급하는 실시간 정보가 포함되어져 있고 이러한 정보가 제3자로부터 고도의 탐지기술 행위로 중요정보가 누출될 수 있는 것이다. [그림 2-1 참조]

이렇게 방출되는 전자파는 정보누출의 위험성 뿐만 아니라 그 위해성도 내포하고 있다.

1950년대 미국에서 핵 실험중 공중 핵 폭발로 인한 강한 펄스기파가 발생되어 컴퓨터와 전화기 등에 유도되어 기기의 불통상태를 초래하였고, 그후 미국에서는 1950년대 말부터 TEMPEST(Transient Electromagnetic Pulse Emanation Standard) 라는 과제명하에 극비리 연구가 추진되어 왔고, 근래 1980년대 초부터는 영국, 일본, 프랑스, 스웨덴, 호주, 뉴질랜드, 네덜란드등 여러나라에서 독자적으로 이에 대한 연구가 비밀리 진행되고 있다.

이러한 불요전자파의 방출은 개인이나 기업, 국가기관의 핵심정보 누출은 물론이고 전파환경을 오염시켜 다른 기기들의 통신의 질 저하는 물론 경우에 따라서는 기기들의 오동작이나 기억정보의 변형을 유발시켜 산업재해나 공장, 발전소의 가동정지, 비행기의 경로 이탈이나 추락등을 야기시킬 수 있으며 또한 더 나아가 그 사용이 군사상 목적의 경우 국가 중요 통신시스템의 마비까지 가져올 수 있는 심각한 위해성이 있는 것이다.



[그림 2-1] 정보기기로 부터의 전자파 방출과 정보도청

2. 정보누설과 EMI(Electromagnetic Interference)와의 비교 고찰

가. 정보누설과 EMI 비교평가

정보누설과 EMI(전자파장해)는 전자기기들로 부터 고유하게 발생되는 미약한 전자파의 방출 문제를 대상으로 삼아 연구를 수행하는 점은 같으나 그 각각의 의미와 연구 깊이는 차이가 있으며 정보누설의 경우는 더 한층 까다롭고 어려운 분야라고 할수 있다.

다음은 정보누설과 EMI의 비교되는 차이점이다.

o 정보누설과 EMI 차이점

구 분	내 용	비 고
정보누설	o Classified된 신호를 포함하는 전자파 방사 문제를 대상으로 함 o 주요 정부기관이나 경찰, 은행, 기업등 사용되는 정보처리기기에서 방사되는 전자파	o 비밀을 다루는 정보처리기의 비밀신호를 취급
EMI	o Classified된 신호의 포함 유·무에 관계없이 모든 전자파 방사 문제를 대상으로 포함 o 불특정기관이나 기업, 사무실등 사용되는 전자기기에서 방사되는 전자파	o 비밀신호에 관계없이 전자파장해 규칙에 정해진 신호를 취급

따라서 위의 구별되는 내용에서 알수 있듯이 이러한 방사되는 신호의 규제 문제에서 정보누설 규제와 EMI 규제를 기술적인 면에서 큰 차이가 있으며, EMI 규제를 만족시키는 장비가 반드시 정보누설 규제를 만족시키는 장비가 아님을 알수 있다. 정보누설 대책에 관한 사항과 탐지에 관한 사항은 제3장, 제4장에서 기술하기로 한다.

나. 정보누설과 EMI 방사 기기별 분류 및 분류기준

(1) 기기 분류

정보누설 방사기기에 대해서는 국제적인 분류(안)은 아직 없으며 중요정보를 처리하는 기기들이 대상이 된다.

대체적인 분류는 표 2-1과 같으며, EMI 발생기기의 분류는 CISPR Pub.16의 분류방법과 이에 영향을 받은 독일의 VDE(Verband Deutscher Elektrotechniker) 규정의 분류방법에 근거를 두었다. 표 2-2, 표2-3은 EMI 발생기기 분류표이다.

표 2-1 정보누설 발생기기 분류

구 분	종 류
COMPUTER	o Micro Computer o Desk - Top Computer o Portable Computer o Embedded Computer
PERIPHERALS	o Terminals o Printers o Plotters o Interface o Key board
COMMUNICATIONS	o LAN o Telephone o Modems

표 2-2 EMI 발생기기 분류 (대분류)

분류근거	VDE 규정	CISPR Pub 16	비 고
의 도 성	통신기기	무선 송수신기	10KHz 이상의 고주파 전력 방사(송신)나 감응(수신)을 위한통신의 목적으로 생성시키는 관련장비
	무선주파수기기	ISM (Industrial Scientific, Medical) 정보처리장치	고주파전력(f〉 10KHz)을 의도적으로 생성하거나 저주파 전력을 10KHz 이상의 반복율로 단속하는 관련장치 고주파 영역에서 (f〉 10KHz)협대역 간섭을 발생
비의도성	무선간섭기기	소형 전기전자기기 Ignition System	10KHz 미만의 비율로 전력이 단속되는 기기. 고주파 영역에서 (f〉 10KHz) 광대역 비의도성 에너지를 발생

표 2-3 EMI 발생기기 분류(세부분류)

대분류	중 분 류	소 분 류	비 고
통신기기	무선송수신기	TV 수상기	무선 주파수의 정보를 공중선 장치를 통해 받아 화상으로 변환하는 장치 국부 발진이나 편향신호등의 누설을 검사한다.
		라디오수신기 (휴대용)	밧데리로 동작하는 방송 수신용 라디오 수신기. 일반적으로 인체를 통한 접지나 접지없이 사용됨.
		라디오수신기 (탁상용)	외부 전원으로 사용하거나 외부전원, 밧데리 공용으로 동작하는 방송수신용 라디오 수신기. 원칙적으로 접지되어 사용됨.
		통신용무전기 (고정국용)	용도에 따라 허가된 주파수밴드에서 사용하는 송수신기. 일체형 무전기로 접지되어 사용되어져야 한다.
		통신용무전기 (이동국용 또는 휴대용)	고정국용과 같으나 접지되어 사용이 가능하며, 일반적으로 도선을 통한 접지없이도 사용될 수 있다.
무선 주파수 기기	산업, 과학 의료용고주파 이용기	산업용 고주파 가열 장치	고주파 유도열을 이용해 금속 또는 프라스틱의 용융 용접등에 사용되는 고주파 가열장치
		전자레인지 (마이크로파 오븐)	마크네트론에서 발생되는 강력한 마이크로파를 투과시켜 발생된 열을 이용한 조리장치 또는 과학시험장치
		초음파이용장치	초음파의 특성을 이용한 가습기, 초음파 탐상기, 어군 탐지기, 비파괴 검사장치등
		의료용고주파 이용장치	인체의 기능보조나 치료를 목적으로 고주파를 이용하는 장치
		전자 측정기	측정을 목적으로 입력된 신호에 처리를 가하거나 변환을 시키기 위한 고주파 발진기를 내장한 측정기류

대분류	중 분 류	소 분 류	비 고
무선 주파수 기기	정보처리장치	산업용 정보처리장치	상공업 지역에서 사용되어야 할 장치를 칭하며 그 장치가 피 방해장치로 부터 30m 떨어진 경우를 산정하여 방해파의 혀용치를 정한다.
		가정용 정보처리장치	주택지역 또는 인접지역에서 사용되어야 할 장치를 칭하며 그 장치가 피 방해장치로 부터 10m 떨어진 경우를 산정하여 방해파의 허용치를 정한다.
		휴대용 정보처리장치 (외부전원 공급 없음)	내부 충전 전원이 내장되고 외부 전원 사용도 가능한 접지 연결없이 사용되는 정보처리 장치의 복사 측정에서는 가정용 정보처리 장치의 기준에 준한다.
무선 간섭기기	소형 전기·전자기기	휴대용 공구 (외부전원)	작업자의 신체 접촉이 측정에 영향을 주지 않은 접지되어 사용되는 전기모터 내장 공구
		휴대용 공구 (밧데리 내장)	모의수를 연결하여 작업자의 영향을 고려하여 측정되는 접지없이 사용되는 전기모터 내장 공구
		전열기기 (고주파 가열기 제외)	저항체에 전류를 흘러 발생된 열을 반도체를 이용해 제어하는 기기 블로워가 내장된 경우를 포함한다.
		배선기구류	반도체 장치가 내장된 조절제어기류
		조명기구	외부로부터의 전기에너지로 충전 물질의 고유 스펙트럼의 빛을 발생하여 이를 이용하는 기구
		전동기응용기기 (공구류 제외)	정류자 모터가 내장된 응용기기로써 반도체 장치가 내장된 경우를 포함한다. 다만 공구류는 제외한다.
무선간섭기기	점화시스템	자동차	내연기관이 탑재되어 인원이나 물자의 운송에 사용되는 완성차로서의 차량
		모터 보트	내연기관이 탑재되어 인원이나 물자의 운송에 사용되는 완성된 보트
		내연기관 장착 장치	내연기관이 탑재되는 차량의 보조장치나 기타 원동기

(2) 분류 기준

앞의 표 2-3에서 제시된 분류 기기별 분류기준을 제시한다.

o 무선 송수신기

- TV 수상기

무선 주파수의 변조된 신호를 공중선 장치를 통해 수신하여 화상으로 변환하는 장치. 국부발진 신호나 편향신호등의 누설이 주 검토대상이 된다.

- 라디오 수신기(휴대용)

외부전원이 밧데리로 동작하는 방송수신기. 접지없이 사용되는 기기이며 전도성 잡음측정에서 제외된다. 국부발진 신호의 누설이 검토대상이 된다.

- 라디오 수신기(탁상용)

밧데리와 외부전원 공용일 경우 또는 외부전원 전용일 경우의 방송 수신기. 접지되어 사용하는 것이 원칙이다. 시스템 일부로써 포함될 경우를 포함한다.

- 통신용 무전기(고정국용)

용도에 따라 허가된 주파수 밴드에서 사용하는 음성이나 부호의 수신 또는 송신을 목적으로 하는 장비로 접지되어 사용됨. 송신측의 스퓨리어스 방사나 수신측의 국부발진 신호누설등이 검사된다.

- 통신용 무전기(이동국용 또는 휴대용)

접지없이 사용되는 통신용 무전기

o 산업, 과학, 의료용 고주파수 이용기기

- 산업용 고주파 가열장치

고주파 유도열을 이용해 금속 또는 프라스틱 용융, 용접에 사용되는 장치

- 전자레인지

마그네트론에서 발생되는 강력한 마이크로파를 투과시켜 발생된 열을 이용해 조리 또는 실험에 이용하는 기기

- 초음파 이용장치

초음파의 특성을 이용해 지질단상, 어군탐지, 비파괴 검사등에 사용되는 기기. 의료용 초음파 이용장치는 의료용 고주파 이용기기에 따른 분류

- 전자 측정기

측정을 목적으로 입력된 신호에 처리를 가하거나 변환을 시키기 위한 고주파 발진기를 내장한 고주파 측정기기류

- 의료용 고주파 이용기기

인체의 기능보조나 치료를 목적으로 고주파 에너지를 이용하는 기기

o 정보처리장치

- 산업용 정보처리장치

상공업 지역에서 사용되어야 할 정보처리장치를 말하며, 피 방해장치로부터 30m 떨어진 경우를 산정하여 방해파의 허용치를 정한다.

- 가정용 정보처리장치

주택지역 또는 인접지역에서 사용되어야 할 정보처리장치를 말하며, 피 방해장치로부터 10m 떨어진 경우를 산정하여 방해파의 허용치를 정한다.

- 휴대용 정보처리장치

내부 충전 전원이 내장되어 일반적으로 접지 연결없이 사용되는 정보처리장치

o 소형 전기·전자기기

- 휴대용공구(외부전원)

외부전원으로 동작되는 정류자 전동기 내장공구류. 접지되어 사용됨.

- 휴대용공구(밧데리 내장)

내부 전원을 사용하여 접지없이 사용되는 정류자 전동기 내장공구류. 모의수에 의한 시험실시 전도시험 면제

- 전열기기(고주파가열기 제외)

열량을 조절하기 위해 반도체 장치를 내장한 발열장치 블러워가 포함된 경우

- 배선 기기류

반도체 장치가 내장된 SMPS(Switch Mode Power Supply) 와 조항기등의 조절 제어기류. SMPS의 경우 출력측 잡음 혼입도 고려 대상이 될수 있다.

- 조명 기기류

외부로 부터 전기 에너지로 충전 물질의 고유 스펙트럼의 빛을 발생시켜 이를 이용하는 기기. 국내 실태 조사에서 전자식 형광등, 안전기 등에서 EMI 발생이 문제시 되므로 반도체 장치가 내장된 경우로 한정하는 것이 타당하리라 생각된다.

- 전동기 응용기기(공구류 제외)

일반적으로 많이 사용되는 세탁기, 냉장고, 에어콘디셔너, 선풍기등의 전동기 내장기기. 모터의 제어를 위해 반도체 장치를 내장한 경우를 제외하고 완성품으로서의 규제보다는 전동기부에 대한 시험을 통한 규제가 타당하리라 생각된다.

o 점화 시스템

- 자동차

내연기관이 탑재된 완성차로써의 차량

- 모터 보트

- 내연기관 장착장치
  내연기관이 탑재되는 차량의 보조장치나 기타 원동기

3. 정보누설 방출원의 유형(Type)

최근 각 방면에 보급이 급증되는 마이크로 컴퓨터와 OA(Office Automatic)기기 등의 정보처리 기기와 각종 전기·전자기기에서 발생되는 잡음(미약전자파)은 주로 내장되어 있는 IC(Integrated Circuit)를 중심으로 하는 전자소자 및 프린트기판이 문제의 주된 원인으로 파악되고 있다. 이것에서 발생되는 잡음은 정보누출이 원인이 됨은 물론이고 TV와 라디오, 공공의 통신에 방해를 주는 것까지 광범위하게 걸쳐 있다.

이러한 불요파가 증가 경향을 나타내는 배경으로는 최근 ROM(Read Only Memory), RAM(Random Access Memory)과 마이크로프로세서등의 논리소자에서 연산속도가 고속화되고 동시에 IC의 집적도가 고도화된 것과 프린트기판의 고밀도화가 급격한 변화를 만들어 디지탈회로 고유의 전자파적인 잡음을 발생시키는 하나의 원인으로 분석되고 있다.

이러한 잡음은 레벨이 낮은 것이어도 회로의 고밀도화에 의한 크로스토크 잡음(Crosstalk Noise)과 임피던스 부정합에 의한 잡음과 상승적으로 작용하고 때로는 외부 시스템으로 영향을 미칠 수 있는 잡음레벨에 달하는 것이다.

전자회로에서 방사되는 주된 잡음을 열잡음과 같이 회로망의 종합등가 저항에 의해 생기는 잡음과 외부와의 유도 및 결합에 의해 발생되는 잡음으로 분류되어진다. (표 2-4 참조)

그리고 이렇게 방사되는 미약전자파는 외부에 작용하여 위해와 방해를 일으킬 수 있고 그 방사원이 비밀을 처리하는 정보기기였을 경우 비밀 정보누설 제공의 원인이 될수 있는 것이다.

여기서는 정보기기로 주로 사용되는 컴퓨터의 디지탈 회로의 누설잡음과 그 방사에 대하여 기술하기로 한다.

표 2-4 회로에서 발생되는 잡음의 분류

	분 류	종 류	영 향
회로잡음	능동형	열잡음 (Thermal Noise)	o 자신의 회로망과 외부 회로망에 영향을 끼쳐 위해와 장애를 유발시킴. o 중요정보취급기기 회로망에서의 잡음은 정보누설 제공의 원인이 됨.
		쇼트잡음 (Shot Noise)	
		후릭카잡음(Flicker Noise)	
		팝콘잡음(Pop-Corn Noise)	
	수동형	소자와 배선간의 전자적 결합	
		외부에서의 유도	

가. 디지탈 회로의 잡음

지금까지 디지탈 시스템 설계자들은 설계시 전자기파 적응성(Electromagnetic Compatibility)에 대해서 그렇게 많은 고려를 하지 않았다.

컴퓨터 시스템은 아주 크고 비싸서 큰 업무에만 이용되었다. 이젠 마이크로 프로세서(Micro Processor)가 이 모든것을 바꾸어 놓았다. 디지탈 전자공학은 더욱 발전되어가고 있으며 이의 적용범위는 작은 장난감에 까지 이르게 된 것이다.

이러한 디지탈 공학의 적용범위가 확산됨에 따라 그에 수반되는 부작용 현상이 나타나면서 로봇의 오동작, 타통신의 영향, 인체피해, 중요 정보누설등 디지탈 시스템 설계자들은 더 이상 전자기파 적응성을 무시할 수 없게 된 것이다.

디지탈 전자공학의 잠재적인 상호간섭을 인식한 FCC(미연방통신위원회)에서는 미국에서 판매되는 디지탈 전자제품에 대해 전자파방사(Emission)의 한계에 대한 법규를 지키도록 정하고 있으며, 기타 다른나라들에서도 비슷한 법규를 정해 놓고 있다.

이러한 제반법규들은 외부에 위해와 방해를 가할 수 있다는 측면에서 모든 전기·전자기기 들에 대해서 고려된 사항이지만 정보누설의 방지 측면에서 중요 정보처리 기기만을 대상으로 살펴본다면 위와 같은 규제 조건보다도 보다더 엄밀하고 까다로운 규제 조건이여야만 된다는 것이다.

디지탈 설계는 수행되는 기능이 방정식으로 나타나는 순수한 수학의 세계에서 이루어진다.

그렇지만 그 로직(Logic)이 맞다 하더라도 회로를 만들어보면 잡음 때문에 제대로 동작하지 않는 때가 종종 있다. 그리고 비록 그것이 동작하더라도 전자파방사 문제 때문에 그 제품을 정식 판매할 수 없는 경우도 있다.

따라서 잡음과 전자파방사에 대한 실용적 고려는 초기설계단계, 배치단계 그리고 검사단계를 거치는 동안 계속 고려되어야 한다.

디지탈 시스템은 역시 잡음과 상호간섭의 잠재력을 가지는 Radio-Frequency(RF) 시스템이다. 거의 대다수의 디지탈 설계자들은 디지탈 설계에 대해서는 잘 알고 있지만 그들이 설계하고 있는 바로 그 RF 시스템에 대해서는 잘 대응하지 못할때가 있다.

더우기 요즘 많은 아날로그 회로설계자들이 디지탈 회로를 설계하지만 그들은 그라운딩, 전력분포 그리고 상호연결에 대한 상이한 기술이 필요하다는 것을 알지 못하며 특히 중요정보가 전자파방사에 의하여 누출될 수 있다는 심각성을 대다수 설계자들이 모른다는 사실이다.

예를들면 단일점 그라운딩(One Point Grounding)은 아날로그 회로에서는 아주 바람직한 것이지만 디지탈 회로에서는 잡음과 전자파의 방사 원천이 된다는 것이다. 언뜻 볼때 겨우 수mA의 직류전류를 끌어내는 작은 집적회로(IC) 디지탈 로직 게이트를 잡음의 심각한 원천이라고 여기지 않는다.

그러나 그것이 고속으로 동작할때 도체의 인덕턴스 성분과 결합해서 잡음과 방사의 주요 원천이 된다.

인덕턴를 지나는 전류의 변화에 의해 발생되는 전압은 $V = L \frac{di}{dt}$ 이때 L은 인덕턴스이며 di/dt는 전류변화 비율이다.

예를들면 전형적인 로직게이트는 직류 전원으로부터 ON 상태일때 5mA를 OFF 상태일때 1mA를 끌여 쓴다.

이것은 단지 4mA의 전류변화에 불과하다.

그러나 이것이 2n Sec에서 일어날 수 있는 것이다.

만약 전원의 배선이 500nH의 인덕턴스를 갖는다면 이러한 한개의 게이트가 상태를 바꿀때 전원배선에서 생성되는 잡음전압은 $V = L \frac{di}{dt}$ 에 의해서 1V가 될 것이다.

이것을 전형적인 시스템에서 그러하듯이 많은 게이트 숫자로 곱해보면 보통 시스템의 전원전압이 5V 이므로 이것 역시 잡음의 주요한 원천임을 실감할 수 있다. 디지탈 회로에 있어 잡음과 전자파의 방사는 시스템의 그라운드, 파워, 선(Wire), 신호도체, 주변장치등에서 일어나게 되는 것이다.

나. 디지탈 기기의 방사

o 전자회로로부터 방사

내부에 전기가 흐르고 있는 선(Wire)은 다른 선을 접속시킴으로써 물리적으로 도청될 수 있다.

그러나 선 내부의 전기의 흐름은 직접적인 접속이 없이도 측정할 수가 있는 것이다. 전류속의 변화는 근거리에서 탐지할 수 있는 외부 자기장을 일으킨다.

전자유도의 기술을 이용한 측정기는 보통 상용화 되고 있다. 이 측정기는 문제의 와이어 둘레에 Sensor Assembly를 죄어 붙임으로써 작동시킨다.

자기장은 거리가 멀어지면서 급속히 떨어지므로 물리적 접근이 제한되고 있는 곳에서는 보통 시스템 보안에 별 문제가 발생되지 않는다. 훨씬 먼 거리에서 유선상의 신호를 도청하는 것은 전류 흐름속의 변화가 대기중 빛의 속도로 퍼지며 무한대의 범위를 갖는 전파의 방사를 낳기 때문에 가능하다.

보통의 환경에서 전자회로로 부터의 방사는 회로 진동 주파수와 같다. 복합적 흐름은 한조의 단순조화 진동으로 분석될 수 있으며 방사는 각 성분의 주파수에서 생긴 것이다.

전자기술의 큰 몫은 회로에 있어서의 전이를 되도록 예리하고 날카롭게 하여 한 상태에서 다른 상태로 순간적인 전이의 성질을 갖는 직각과 또는 스텝함수에 가깝게 하는데 주력하고 있다.

직각파의 분석은 기본 주파수의 홀수배인 주파수에서 특히 에너지 용량이 높다는 것을 보여주고 있다. 주파수가 높아짐에 따라 방사된 광자의 에너지도 똑같은 비례로 높아진다.

컴퓨터 회로로부터의 방사는 회로의 주파수가 올라가면서 착실히 증가한다. 누설의 레벨도 마찬가지로 선(Wire) 및 기타 회로소자의 공진주파수 및 컴퓨터 케이스의 홉수 및 반사재료 그리고 주파수에 따른 환경에 달려 있으나 역시 주파수가 올라가면 따라서 올라가는 성질을 갖고 있다.

컴퓨터 회로에서는 기본 주파수가 넓은 범위를 갖는다. RS-232 직렬 데이타 링크는 구식 텔레타이프 텔레프린터용 110Hz로부터 비디오터미날용 19.2KHz 까지 그리고 RS-422는 훨씬 높은 주파수를 사용한다.

그래픽 스크린을 위한 비디오 Dot Clock은 해상도에 따라 1-30MHz 범위를 사용한다. 퍼스날컴퓨터의 프로세서는 2MHz로부터 12MHz까지 사용하며 대형컴퓨터와 최근의 마이크로 프로세서를 이용하는 워크스테이션에서는 더 높은 주파수가 사용된다.

이러한 차폐되지 않는 회로에 의한 방사는 아주 발달된 도청기술을 이용하면 1마일(mile) 정도 떨어진 거리에서도 정보를 탐지해낼 수 있는 것이다.

o 컴퓨터의 방사

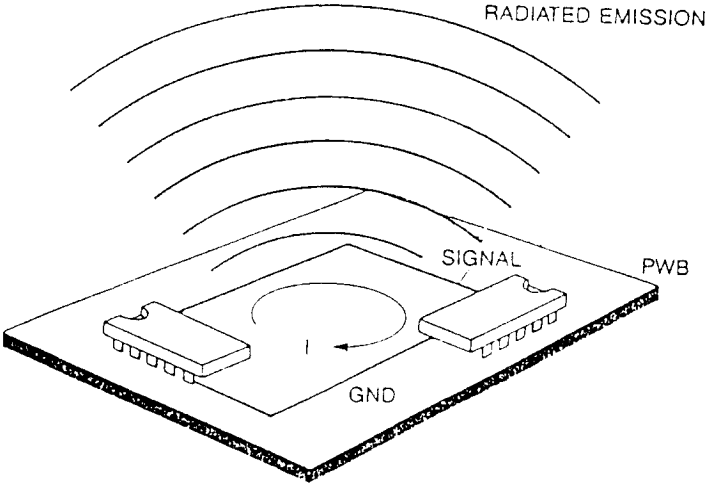
퍼스날 컴퓨터는 약 100MHz에서 텔레비젼이나 FM 라디오에 심한 간섭을 일으키는 전자파 방사를 야기시킨다.

이러한 전자파를 탐지할 수 있는 기기를 사용하면 보다 더 낮은 레벨의 전자파 방사도 아주 먼 거리에서 탐지해 내고 분석될 수 있는 것이다. 또한 컴퓨터의 직접회로 패키지 내의 선(Wire)을 포함하여 회로기판 및 컴퓨터의 후면과 각종 내부 및 외부장치를 연결하는 컴퓨터 내부의 선들은 모두 그 자체의 방사에 도움을 주는 것이다.

CRT(음극선관)안의 고압전자빔은 안테나를 필요로 하지 않는다. 급속한 가속, 변조 및 돌연한 감속이 CRT 표시장치의 요체이기 때문에 자동적으로 RF(Radio Frequency)방사를 일으키는 것이다. 이러한 방사를 고도의 지향성 안테나를 갖춘 도청장비라면 복잡한 사무실이 운집되어 있는 곳에서 목표가 되는 사무실내의 CRT 화면의 내용이나 프린터되는 내용을 탐지해 낼수 있는 것이다.

o 디지탈 회로의 방사형태

디지탈 전자제품에서의 방사형태는 차동모드방사(Differential Mode Emission)와 공통모드방사(Common Mode Emission)의 형태로 일어날 수 있다.
차동모드방사는 그림 2-2에서 보는것과 같이

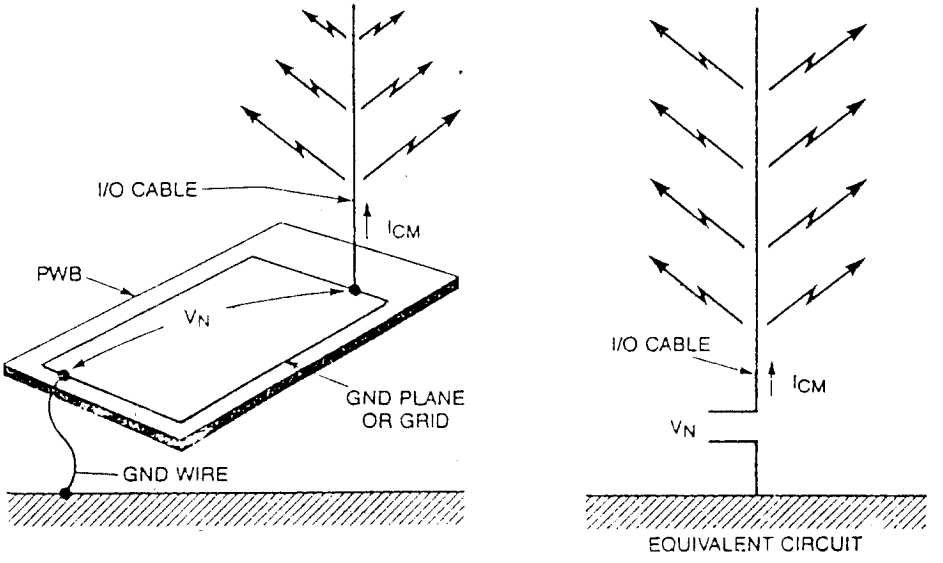


[그림 2-2] 인쇄회로기판(Printed Wiring Board : PWB)에서 발생하는 차동모드방사

회로의 도체로 이루어진 루프(Loop) 둘레를 흐르는 전류 때문에 생긴다. 이러한 루프는 자기장(Magnetic Field)을 복사하는 작은 안테나(Antenna)로써 동작하게 된다.

이러한 신호전류 루프(Signal Current Loop)는 회로의 동작을 위해 필요하지만 정보누설의 원천이 되는 이러한 방사를 최대한 억제키 위해서는 그 크기와 면적을 설계과정에서 반드시 통제하여야 한다.

공통모드방사는 그림 2-3에서 보는것과 같이



[그림 2-3] 시스템 케이블에서 발생하는 공통모드방사

시스템의 어떤 부분을 진짜 그라운드(Ground)위에 공통모드 전위를 가지게 하는 바라지 않는 회로전압 강하의 결과로 일어난다.

이것은 대부분 디지탈 로직(Logic) 그라운드 시스템의 전압강하 때문이다. 외부 케이블이 시스템에 연결 되었을때 이러한 공통모드 전위로 구동되며 그림 2-3에서와 같은 전기장을 방사하는 안테나를 형성한다. 이러한 바라지 않는 전압강하는 시스템의 설계에 의도적으로 포함되는 것이 아니기 때문에 공통모드 방사는 차동모드 방사보다 다루기가 더 힘이 든다. 공통모드 방사 또한 정보누설의 방지를 위하여 설계과정에서 방사를 제한할 수 있도록 고도의 기술적 통제 방법이 요구되는 것이다.

4. 정보누설의 방사경로

디지탈 회로나 컴퓨터를 사용한 전자기기나 정보처리기기의 사용이 정부기관, 사무실, 산업체, 가정 등으로 널리 보급됨에 따라 그 기기에서 방사되는 전자파는 중요정보는 물론 다른 전자기기에 여러가지 장해를 주는 사례가 많이 발생하고 있다. 다음은 방사되는 전자파가 발생원에서 어떤 경로를 지나 방사되는지 알아보기로 한다.

방사전자파의 전파경로는 그 전파형태에 따라서 크게 3가지로 구분된다. 그림 2-4는 그 경로를 도식으로 나타낸 그림이다.

가. 전도에 의한 경로

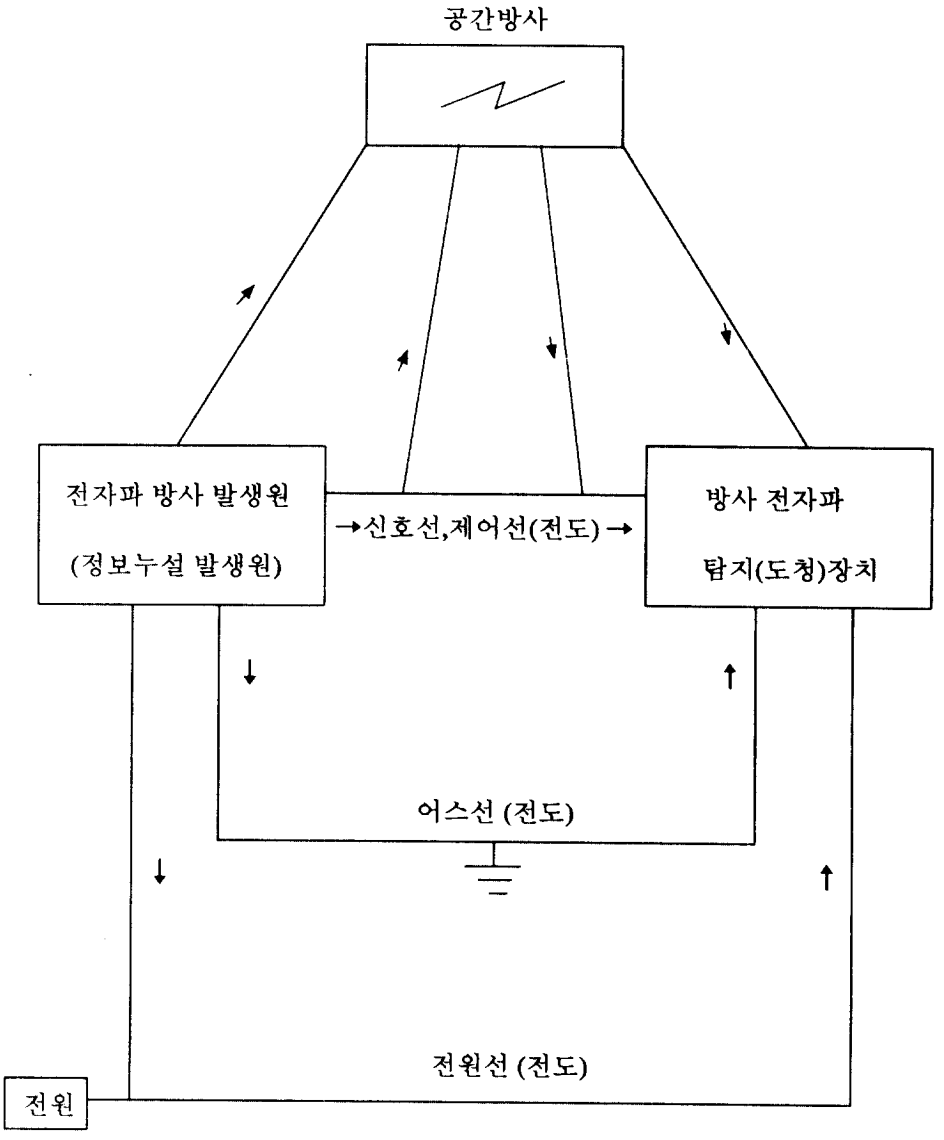
기기에 직접 접속된 전원선을 통하여 전도되는 경로, 기기간에 접속된 신호선이나 제어선을 통하여 전도되는 경로, 어스선을 통하여 전도되는 경로 등이 있다.

나. 복사에 의한 경로

발생원에서 그 주위의 공간에 직접 전자파가 방사되어 발생원 가까이에 놓여진 다른 기기에 직접 전도되는 경로

다. 전도와 복사의 복합경로에 의한 경로

발생원에 접속된 전원선이나 신호선에서 주위의 공간에 전자파가 방사되어 가까이에 놓여있는 다른 기기에 직접 전도되는 경로 또는 발생원에서 방사된 전자파가 다른 기기에 접속된 전원선이나 신호선으로 들어가 그 곳으로 통하여 기기에 전도되는 경로



[그림 2-4] 전자파의 방사경로

제3장 정보누설방지 대책에 관한 기술 및 동향

1. 정보보호 기술의 필요성

컴퓨터나 워드프로세서 또는 단말기, 프린터, 모뎀등 디지탈 기기로부터의 불요전자파는 도체면을 따라서 전도되거나 공간을 통하여 방사된다.

그런데 이렇게 방사되는 전자파를 근거리나 원거리에서 도청하여 정보를 추출해 내는 상대방의 기술은 최첨단의 기술을 요하는 것이다. 즉 이러한 방사전자파로부터 정보를 재생하기 위해서는 안테나기술, RF/MW(Radio Frequency/Micro Wave)수신기 기술 디코딩(Decoding) 기술이 요구되는 것이다.

그리고 먼거리에서 특정 정보기기로부터의 선택된 정보를 도청하기 위해서 안테나는 고지향성, 고이득, 광대역 특성을 갖는 것이어야 하며 수신기는 고 다이나믹 레인지, 고감도, 고분해능의 특성을 가지고 있는 것이어야만 가능한 것이다.

이처럼 상대방이나 상대국이 최첨단의 도청기술을 이용하여 우리의 산업체나 국가기관의 중요기술이나 비밀을 탐지해 낼수 있다는 사실을 생각한다면 그 심각성은 자못 큰 것이다.

정보가 가장 중요한 현대의 정보화 사회에서 정보의 주체가 정부기관이든 공공기관이든 또는 각 개인이든 그 정보의 안정성이 보장되고 보호되어야 한다는 점은 그 사회나 국가가 유지되기 위한 전제 조건이자 필수적 요건인 것이다.

2. 외국의 동향

가. 미국

미국에서는 1950년대말부터 TEMPEST—TEMPEST 란 여러이름을 가지고 있지만 원래는 Transient Electromagnetic Pulse Emanation Standard의 약어로써 미 국방성과 NSA(National Security Agency)간의 공동연구 과제 이름으로, 이 과제는 약 20년간 비밀로 되어 왔으며 TEMPEST란 과제명조차 약 7-8년전까지는 비밀로 되어 있었다. 지금에 있어 TEMPEST란 컴퓨터나 다른 전자장치로부터 방사되는 신호를 조사 연구하고(특별히 거리를 두고 정보를 도청하는것) 또한 이를 방지하기 위한 대책을 연구개발 하는것을 의미한다—라는 이름으로 연구되어 왔으며 국가의 TEMPEST 정책이 1981년 1월에 문서화 했으며 또한 방지대책을 결정하기 위한 방법들이 1984년 1월에 규격화 되었으나 비밀이다.

TEMPEST 관련 시험방법, 설계기준 및 방사기준이 모두 비밀이며 공식적인 학술대회에서의 토론도 금지되어 있다. 1980년대 초에 미 정부에서는 ITP Program (Industrial Tempest Program)이란 제도를 만들어서 정부와 계약하고 있지 않는 관련 산업체에서도 계약에 참여할 수 있는 기회를 주기 위해 국가표준인 NACSIM 5100A를 만족시키는 장비들을 PPL(Preferred Products List)에 게재하고 있다.

현재는(1988년말 기준) 미국에서 약 175개의 회사가 TEMPEST 차폐된 장비를 만들고 또한 시험하도록 허가를 받았으며 그 시장은 1986년 $ 874 million 에서 해마다 급신장의 증가율을 보이고 있으며 고객은 정보사업, 군사분야, 경찰이나 사법부등 정부관련 기관이나 사업체 등이다.

미국의 TEMPEST 규정은 NSA(National Security Agency)가 규정한 템피스트의 필요 조건은 비밀로 분류되어 공개되지 않으며 구 NACSEM 5100을 개정한 현재 NACSIM 5100A 표준에 수록되어 있다.
표 3-1은 TEMPEST 관련 규정에 관한 것이다.

[표3-1] 미국의 TEMPEST 관련규정

구 분	내 용
NACSIM 5100 A/B	Compromising Emanations Laboratory Test Requirement
NACSEM 5201	TEMPEST Guidelines for Equipment / System Design
NACSEM 5109	TEMPEST Testing Fundamentals
NACSEM 5204	Shielded Enclosures
NACSEM 5112	NONSTOP Evaluation Techniques
NACSIM 5203	Guidelines for Facility Design and Red / Black Installation

나. 영국

1980년초까지 TEMPEST 수신기를 미국으로부터 수입해 왔으나 현재는 일부를 외국으로 수출을함. 영국의 TEMPEST 규정은 NSA(National Tempest Authority)의 BID-01/202이다. 중요내용은 비밀로 함.

다. 네덜란드

1985년 봄 전자 Mail Network 구성시 정보유출 문제를 확인하기 위한 연구결과 발표(Post Telecom and Telegraph) 내용은 비밀로 함.

라. 일본

1980년초 미국으로부터 TEMPEST 수신기 수입한 이후, 장기적인 계획을 수립하여 계속적인 연구를 수행해오고 있으며, 1992년도 이후에는 독자적인 TEMPEST 규격 입안과 제정, TEMPEST 규격의 시행지원 체제 정비등을 목표로 연구에 박차를 가하고 있다. 내용은 비밀로 함.

마. 스웨덴, 프랑스

자체연구중이며 모든 내용은 비밀로 함.

바. 뉴질랜드, 오스트리아

1980년초 미국으로부터 TEMPEST 수신기 수입 이래로 현재는 독작적인 연구수행 중이며 내용은 비밀로 함.

3. 정보보호 기술의 종류

제3자나 상대국이 개인이나 기업체, 국가기관의 중요정보를 처리하는 디지탈 기기로부터 거리를 두고 정보를 빼가지 못하게 하기 위해서는 각 정보처리 기기를 차폐하는 기술이 가장 기본을 이루는 기술이라고 할수 있다.

이와 같은 정보처리 기기의 전자파방사를 줄이기 위한 기술로는 차폐 재료기술 전자파방사를 줄이기 위한 회로설계 또는 장비설계기술, 코딩기술, 광섬유기술 등이 주요 기술이라고 볼수 있다.

이러한 주요기술 내지 방법, 규격등은 각 국가에서 비밀로 관리되어 내용을 공개치 않는다. 다음은 이러한 기술에 관계되는 것들을 대략적으로 소개해 보기로 한다.

가. 컴퓨터의 차폐

방사되는 전자파에서 정보 도청으로부터 컴퓨터 시스템을 보호한다는 것은 단순히 금속판으로 감싸는 것만으로 되는 것이 아니다. 예를들면 차폐에 있어서 전체적으로 컴퓨터실을 차폐하지 않는한 사용자에게 접근을 못하도록 완전한 차폐의 준비는 어려운 것이다.

또한 거기에는 편리도 고려해야 한다. 케이블은 신축성이 있어야 장비를 이동할 수 있다.

스크린은 사용자가 볼수 있어야 하며 키보드를 만질 수 있고 디스크와 주변장치의 컨넥터를 위한 공간이 있어야 한다.

컴퓨터나 다른장치에 있어서 이들 공간은 모두 잠재적인 누설점이며 방사를 최소화 하기 위한 적절한 대책이 강구되어야 한다. 컴퓨터에 있어서 설계기사는 이러한 요구 조건에 대처하는데 이용할 수 있는 많은 자재와 기술이 있어야 한다.

나. 전자 자기장의 차폐

진자회로로 부터의 복사는 시초의 지배적인 힘이 전류인지 또는 전압인지에 따라 넓게 두 종류로 나눌 수 있다.

첫번째의 경우에 있어서 웨이브(Wave)의 전기적 구성요소는 자기적 구성요소에 대해 낮은 비율로 시작한다. 이 비율은 웨이브 임피던스(Impedancd)라 부른다.

두번째 경우는 웨이브 임피던스가 높다.

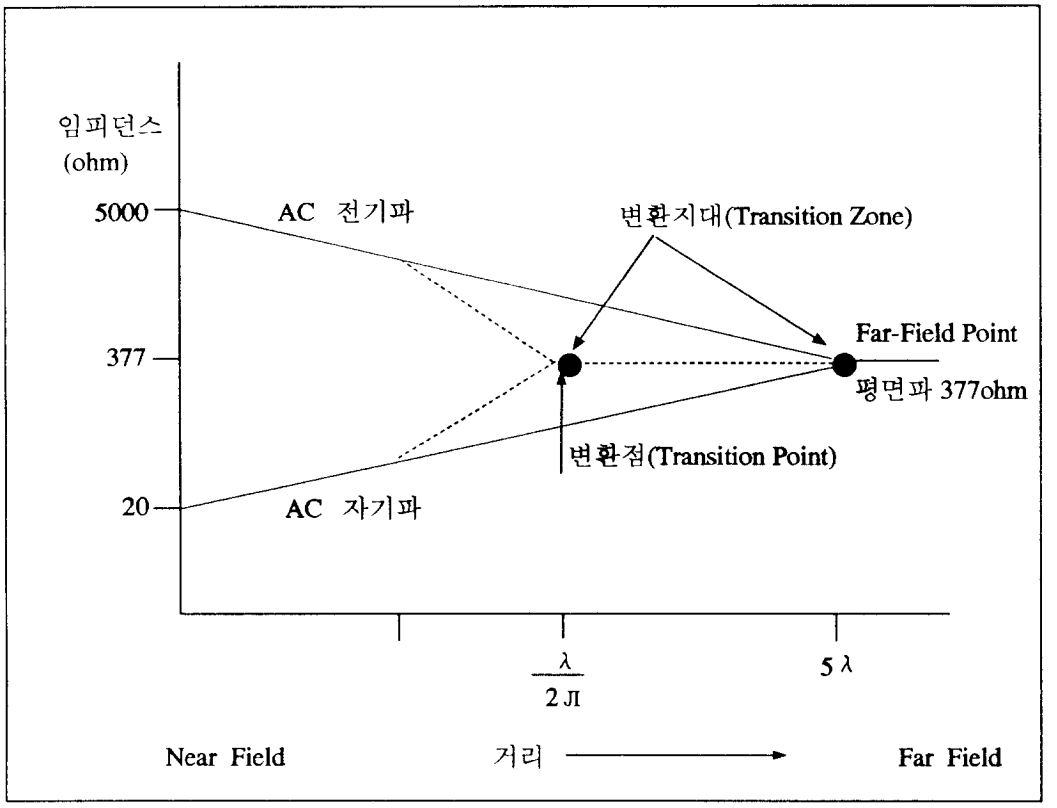
전파는 평형파가 평면파로 불리어지는 자유공간의 자연 임피던스인(파동임피던스) 377ohm에서 급격히 균형이 잡힌다. 2 x Pi(3.14)로 나눈 파장의 거리를 전이점으로 부터 전파가 본질적으로 균형이 잡혀있는 파장의 5배수까지 관례에 따라 측정한 전이구역이 있다.

그림 3-1에서 보는 바와 같이 방사체로 부터 어느 한쪽의 장(Field)이 지배하는 전이점까지의 지역을 근거리음장(Near Field)이라 부르고 전이구역을 넘어선 지역을 자연 원거리음장(Far Field)이라고 부른다.

근거리음장은 저주파와 작은 밀폐함 속에서 매우 중요하다. 그것은 62.8피트의 파 또는 16MHz에 대해서는 10피트의 거리에서 그리고 160MHz의 파에 대해서는 1피트의 거리에서 끝난다.

가장 높은 주파수에서는 방의 차폐는 중요하지 않으며 개별 장치의 차폐가 가장 중요하다. 차폐자재의 효능은 전기와 자기 평면파에 따라서 매우 달라진다. 단순한 경우는 금속평판에 수직으로 접근하는 평면파이다. 우선 첫째로 표면에 흡수 반사된 에너지량은 콘덕턴스(Conductance)가 무한대로 가면서 영(Zero)으로 가는 자재의 임피던스에 의존한다.

정확히 매치(Match)가 될때는 파가 장애를 받지않고 계속되며 임피던스 영(Zero)의 표면에서는 전반사가 이루어진다. 377ohm 사이의 부정합 또는 전기 및 평면파에 대한 보다 높은 임피던스와 금속에 대한 영(Zero)임피던스는 이들파에 대하여 차폐되기 쉽게 한다.



[그림 3-1] 니어필드(Near Field), 파필드(Far Field) 및 변환지역

표면을 침투하는 파중에서 전기와 자기장은 운동방향으로는 직각을 이루고 양극에는 평행을 이루며 금속판 안에 전류와 자기장을 유도한다.

양극의 전도성이 무한하다면 유도전기장은 입사방사의 장과 같을 것이며 또한 방향이 상반 되므로 서로 상쇠될 것이다. 자기장들이 동시에 일어나고 양극에 전류를 유도한다. 전기장이 사라지면 완전 차폐의 신호가 될 것이다.

실제로 금속은 한정된 물체이지만 매우 높은 전도성을 갖고 있으므로 평면파와 전가파에 대해서 매우 효과적이다. 낮은 임피던스의 자기장은 효과적으로 차폐에 연결할 수 있으므로 아주 두껍지 않는한 유도전류가 시트의 다른 면으로 통과하여 거기서 재 방사된다. 얇은 판인 경우 떨어진 표면으로 부터 파의 반사가 두개의 파 사이에 간섭을 일으켜 건설적(내부의 장을 증가 시킴)일 수 있고 또는 파괴적(소멸시킴)일수 있다.

차폐된 밀폐함 안에서 가스켓(Gasket)과 구멍은 차폐의 파 소멸 효과가 작용할 수 있도록 사방으로 차폐의 도전율을 유지하는 것이 매우 중요하다.

재료들간의 부정합, 갭(Gap) 또는 전도에 있어서의 단절은 누설점이 되며 크건 작건 이 누설은 고려되어야 한다.
배기구멍과 케이블 입구는 입사방사의 파장에 따라 누설을 야기시킨다.

파장이 구멍 크기의 두배 이내일때는 자유롭게 통과한다. 파장이 짧아짐에 따라 에 누설하는 힘은 반비례로 감소한다.

달리 말하면 데시벨(dB)에 있어서의 차폐효과는 주파수의 대수와 함께 떨어진다. 한 평면파와 하나의 평면 금속판과 같은 간단한 경우에도 전자 방정식의 정확한 해답은 비 실제적이다. 엔지니어들은 수년간에 걸쳐 꾀 정확한 계산법을 여러가지로 연구해 왔으며 2dB 이내로 밀폐하는 차폐능력을 예견할 수 있는 소프트웨어를 주장하는 회사들도 있다.

다. RFI/EMI에 대한 장벽(Barrier)

차폐의 기본원리는 동판과 같은 우수한 전기도체의 박막이 전파방사에 거의 완전한 장벽이 된다고 하지만 그러나 어떤 틈새에도 강력히 방사할 수 있다.

와이어망(Wire Mesh)도 망의 간격보다 훨씬 긴 파장을 갖는 광자에 대하여 거의 완벽한 장벽이 되고 있다. 1피트의 파장은 1GHz의 주파수에 해당하므로 수분의 1 인치의 간격을 갖는 망이 가장 적당할 것이다.

같은 이치로 ¼인치 까지의 좁은 구멍과 통로는 차폐효과를 희생시키지 않고도 케이블의 설치를 허용하며 또한 와이어망과 기타 전도 가스켓(Gasket)은 보다 큰 틈을 봉할 수 있다. 통풍구를 위해서는 벌집판(Honey-comb Panel)을 이용한다. 이 벌집판은 양축을 따라 적당한 좁은 간격과 균일한 전기적 특성을 갖추고 있다.

라. 벽(Wall)

정보누설 문제에 대한 최초의 포괄적인 해답은 100만달러 내외의 비용으로 컴퓨터실 전체를 동으로 피복하는 것이였다.

이 차폐실에는 창문이 없고 컴퓨터에 전기 및 냉각수 공급과 사용자에게 좋은 환기상태를 제공하는데 까다로운 문제가 있었다. 출입구도 조심스럽게 설계했어야 했다. 출입문을 처리하는 가장 완전한 방법은 일종의 공기차단 방법인데 컴퓨터실에 들어가는 문에 조그마한 차폐실이 있고 또 다른 문이 외부에 달려 있어서 이것이 유일한 출입문이여서 한개 이상의 문이 동시에 열리지 않도록 되어 있다.

정보사회에서는 이러한 방에는 전화가 없다. 원거리 접촉이 전혀 없기 때문에 컴퓨터는 외부로부터 도청당할 염려가 없는 것이다.

그러나 한편으로 시설에 대한 설치나 유지보수를 위해서 진단을 하고져 하는 컴퓨터 기사들에게는 문제점이 되고 있다.

마. CRT(Cathode Ray Tube)의 철망 스크린(Screen)

철망은 많은 해에 걸쳐 CRT 터미날에 대해 유일하게 물리적 차폐 재료로 쓰여져 왔다. 전파의 방사누출을 방지할 수 있을만큼 조밀한 망사조직은 스크린의 조명도를 감소시켰으며, 그리고 만일 철사의 간격과 스크린의 화소가 너무 근접할 때에는 물결모양이 나타날 수 있다.

금속층이 빛을 통과시킬 만큼 얇고 긴 파장의 전파방사를 차단할 만큼 효과적일때 유리-금속 샌드위치를 사용할 만하다.

바. 밀폐(Enclosure)

장치의 밀폐를 재 설계함으로써 많은 보호효과를 얻을 수가 있다. 대개는 구멍이 많아서 그 접합부분에서 누설된다.

이러한 누설은 많은 플러그(Plug)로 아주 쉽게 막을 수 있다. 어떤 컴퓨터와 기타 장치들에 있어서 FCC(Federal Communications Commission) 방사 레벨을 충족한 코딩을 입힌 프라스틱 케이스에 포장되어 있다.

이러한 시스템을 금속 케이스로 바꿈으로써 전파방사를 현저히 줄일 수 있다. 컨넥터 주위의 누설은 내부 차폐를 보다 개선하고 케이스와의 결합을 보다 개선한 컨넥터를 대체할 필요가 있을 것이다.

사. 코딩(Coating)

몇몇의 재료들은 전파방사를 흡수하는데 컴퓨터 케이스 내부에 박막층으로 사용할 수 있다. 그것들은 그것 자체만으로도 꾀 효과가 있으며 그리고 금속판에 적용시킬때와 접합부를 채우는데 사용했을때 아주 효과적이다.

어떤 것은 적은 비용이 드는 프로세스에 의해 뿌려지게 할수 있다.

아. 차폐 케이블(Shielded Cables)

데이타 케이블은 보통 누설을 방지하기 위해서 뿐만 아니라 케이블의 수신 안테나로써의 작용이 있기 때문에 전송중에 데이타의 손실이나 에러를 야기시킬 만큼 강한 외부의 신호를 받는것을 방지하기 위해서도 차폐되고 있다.

편복선 방사 차폐 케이블과 금속 튜브에 밀폐한 외장 동축 케이블을 포함하여 통상적인 상업용으로 몇가지 등급의 차폐가 가능하다.

훨씬 정밀한 차폐가 정보누설보호 응용에 사용될 수 있으며 누설될 수 있는 방사 부분의 차폐에 있어 틈이 없도록 접합부와 컨넥터에 각별한 주의를 기울여야 한다.

자. 광섬유(Fiber Optics)

광섬유 도파관의 유리섬유는 전류를 전도하지 아니하고 주위에 전계가 없으며, 전파방사가 없는 절연체이다. 유리코아로부터 빛의 누설은 매우 낮고 케이블의 전도가 없는 바깥층을 통한 누설은 전무하다.

광섬유 케이블의 실재 도청은 사람의 눈에 띄지 아니한채 섬유를 깨고 심선을 접속하여야 하기 때문에 불가능하다.

전송된 빛의 레벨은 심선의 가닥에서 반으로 내려가기 때문에 도청은 어려운 것이다. 이러한 성질 때문에 광섬유는 TEMPEST(중요정보 누설대책 및 탐지) 시장에서 흔히 LAN(Local Area Network)과 차폐실간의 접속, 그리고 앞으로 거의 모든 지역통신에 사용될 것으로 사료된다.

광섬유는 비밀보안성이 크고 운용거리가 긴 두 요소의 조화로 여러 종류의 유선 케이블을 광섬유로 대체하는데 아주 유리한 특성을 갖고 있다. 물론 비밀 원격통신은 데이타의 암호화 및 음성의 파장을 바꿀것이 요구 되어진다.

광섬유 LAN은 상업시장에서 중요한 자리를 차지해 가고 있으며 현재 유리섬유는 동선보다 더 싸며, 광섬유 케이블은 동축 케이블보다 비싸지 않다.

앞으로 수년간 더 연구하면 전자신호와 광신호를 서로 변환하는데 필요한 값싼 집적 전자광 회로를 얻을 수 있게 될 것이며 그렇게 되면 광섬유 LAN으로 하여금 모든 시스템 가격에서 모든 전자적 LAN과 견줄 수 있게 될 것이다.

한편 TEMPEST 시장은 광섬유 LAN과 기타 통신의 성장에 중요 요소가 될 것이며 민간시장에 침투하는데 필요한 광섬유 LAN의 대량생산 체제와 저렴한 비용을 낳게 할 것이다.

차. 회로의 재설계(Redesign of Circuits)

방사를 차폐하는 것보다 방사를 줄이기 위해 노이즈 있는 부품을 대체하고 회로를 재 설계하는 편이 비용을 훨씬 줄일 수 있게 하는 경우가 많다.
대부분의 경우 방사는 몇개의 접점에서 발생되는데 그 접점을 규명하는 것이 차폐요건을 크게 감소시키거나 이를 제거할 수 있게 할 것이다.

이러한 접근방법은 TEMPEST화된 기종이 한 제품을 두개의 다른 모델로 생산할 수 있을 만큼의 높은 매상고를 올릴 수 있는가에 그 성패가 좌우된다 할 것이다.

제4장 정보누설 탐지기술의 개관

가능한한 먼거리에서 특정한 정보기기로부터 방사되는 미약한 누설전자파를 탐지하여 중요정보를 빼내기 위해서는 고도의 센서(안테나의 고지향성, 고이득 광대역 특성)기술과 수신기의 고 다이나믹 레인지, 고감도, 고분해능 특성을 갖는 것이어야 한다.

또한 암호장치를 사용한 보안장비 신호도 방사되는 누설전자파가 도청자에 의하여 탐지가 되면 암호화 되기전의 전도성방사(Gonducted Emission)신호와 안테나를 통한 복사성방사(Radiated Emission)신호를 비교하여 암호체계 자체의 알고리즘도 분석가능 하게 된다.

각 국가에서는 누설전자파 보호대책 및 탐지기술을 비밀리에 연구수행을 계속하고 있으며 그 내용은 국가 기밀로하여 공개치 않는다.

다음은 그 탐지(도청) 기술의 개요적인 사항을 살펴본다.

1. 전자도청의 물리학(The Physics of Electronic Eavesdropping)

100년전에 제임스 클라크 맥스웰(James Clerk-Maxwell)은 최초로 종합적인 전기 및 자석이론을 공식화 했다.

그 기본적 원리는 단순한 수학공식에 따라 전기장의 변화가 수직적인 자기장을 만들고 반대로 자기장의 변화는 전기장을 일으킨다는 것이다.

전기파는 90° 의 위상차를 갖는 자기파를 발생시키고 자기파는 다시 전기파를 재생한다. 이 이론은 가속화된 전파체로부터 복합 전기 및 자기파가 전파되고 그리고 특히 빛은 이와같이 해서 생긴 것이라고 예견하였고 이 예견은 곧 적중하게 됐던 것이다.

이 이론은 훨씬 긴 파장의 전파를 예견하였고 이 전파는 곧 발견되어 지금처럼 라디오, 레이다 그 밖의 용도에 이용되게 된 것이다.

후에 프랭크(Planck)와 아인스타인(Einstein)은 전파 복사가 지속파라기 보다는 광자의 형태를 취하며 전자가 에너지의 양자레벨을 바꿨을때 복사된다고 설명했던 것이다.

이 발명으로 인하여 나중에 메이져(Maser), 원자시계(Atomic Clock), 레이저(Laser)와 홀로그램(Hologram)을 얻게 된 것이다.

그 양자역학은 또한 트랜지스터 그리고 현대컴퓨터와 코드머신(Code Machine) 나아가서는 원자탄과 그 밖의 위협적인 현대무기를 발명하기에 이른 것이다.

이와같은 여러 갈래의 기술이 중요 정보보호를 위협하는데 모아지고 있다. 컴퓨터 회로는 여러가지 선(Wire)을 따라 대응 에너지의 변화와 함께 전자의 흐름이 급속히 변환하는 원리에 근거하고 있다.

컴퓨터가 매우 강한 전파를 방사하기 때문에 FCC(미연방통신위원회)는 주택가에서 라디오와 TV 수신의 손실을 예방하기 위해서 전파방사의 한계를 정하여 강력히 규제하고 있다.

고감도의 수신기와 컴퓨터화한 첨단의 신호처리 기술로 특수 제작된 기기는 훨씬 낮은 레벨의 미약전파 방사도 탐지되어 중요정보를 빼낼 수 있기 때문에 컴퓨터로 개인, 기업, 국가기관 등에서 중요 정보자료를 처리하기 위해서는 보다 엄격한 보호대책을 세워야 하는 것이다.

2. 전파방사의 탐지(Intercepting Radio Frequency Emission)

컴퓨터 시스템으로 부터의 방사량과 종류에 따라서는 각각의 신호가 다른신호 때문에 잡히지 않는다고 추정되는데, 특정 대형컴퓨터에 있어서는 이것이 틀린 말이 아니며, 내부의 신호는 일반적으로 병렬로 되어 있고 그리고 외부신호는 한번에 많은 신호를 보낼 수 있는 대규모 장치가 보통인 것이다.

그러나 몇몇 요소는 특히 소형 컴퓨터 시스템에 있어서 일반적인 잡음의 해독으로 쉽게 대상신호를 잡을 수 있는 것이다.

첫째로 보통 다른 주파수로써 신호형태가 다른 것이다.
그러므로 한 주파수를 잡게되면 라디오의 주파수를 맞추는 것과 다를바 없이 쉬운 것이다.

둘째는 직렬통신이 아주 흔한데, 특히 터미날 프린트와 모뎀에서 그러하며 게다가 이것들은 전파방사 효과가 큰 케이블에 접속되어 있다.

CRT의 래스터 스캔(Raster Scan)도 역시 직렬신호이다. 게다가 주변장치들에서 방사되는 신호들은 공간에서 분산되며, 고이득 지향성 안테나에 의해 탐지될 수 있다.

표준화된 신호레벨과 직렬통신의 프로토콜(고정데이타 비율 ; 스타트, 스톱 및 패리트비트 ; 인쇄가능 문자의 제한과 제어부호의 한정 ; 자연언어의 사용)과 CRT(동기펄스 ; 수평, 수직 주사의 반복기간 ; 연속적 주사선간의 고도의 유사성)는 백그라운드 노이즈(Background Noise)로부터 방사되는 그들 신호는 탐지가 비교적 용이한 것이다.

사실상 직렬전송은 소음이 많은 장거리 접속을 극복하기 위해 특별히 설계할 필요가 있는 것이다.

3. 신호처리(Signal Processing)

무선국이나 TV국은 깨끗한 신호를 보내고자 노력을 하나 컴퓨터는 그렇치 못하다. 수신상태가 나쁜 지역에 있어서 TV를 시청해본 사람이라면 누구든지 왜곡과 반사 및 잡음이 깨끗한 화면을 볼수 없게 만든다는 것을 알게 된다.

컴퓨터 방사로부터 데이타를 수신하는데는 잡음에 묻히고 찌그러져 들어오는 것을 깨끗히 할 것이 종종 요구되어진다.

비교적 깨끗한 신호를 받기 위해서는 여과하면 되는데 신호레벨이 잡음레벨 보다 낮을 때에는 디지탈 신호처리를 하면 회복될 수 있다.

신호처리와 여과 양쪽은 신호의 규칙성과 잡음을 분리시키기 위한 잡음의 일반적 불규칙성에 의존한다. 예를들면 한 시스템의 전압레벨과 클럭 주파수는 일반적으로 도청자에게 알려져 있으므로 그래서 신호처리자는 특정 진폭과 주파수를 가진 신호를 찾을 수 있는 것이다.

잡음으로부터 신호를 추출하는데 사용하는 방법은 빠른 산술에 달려 있다. 예를들면 각종 디지탈 필터를 위한 이산푸리에 변환과 반사의 제거를 위한 자기상관 함수인데 이것들은 분석된 모든 자료점에 대하여 여러값의 합계를 필요로 한다. 반도체 회사들은 1986년에 디지탈 신호처리 단일칩을 대량으로 생산해오고 있으며 이러한 것으로는 영상 프로세서, 고속 변·복조장치, 레이다 세트 등이며 이러한 대량생산은 다른 시스템과 함께 도청장치의 비용을 낮추는 중요한 요인이 되고 있다.

4. 복호(Decoding)

컴퓨터 시스템이나 이의 주변장치에 있어서 데이타는 두개의 전압 또는 전류 레벨간에 변하는 단순한 ON/OFF 스위치의 형태로 된 비트의 집합으로 표시된다.

마이크로 컴퓨터에 있어서 전형적인 레벨은 내부적으로는 0 볼트와 5 볼트이며 직렬통신 선로상에서는 -12 볼트에서 12 볼트이다.

프로그램의 목적에 따라서 연속되는 데이타 비트는 문자나 숫자의 흐름으로 나타낼 수 있고, 2에서 16, 777, 216 컬러 혹은 기타 다른 정보구조에 있어서 2차원적 그래픽 영상으로 나타낼 수 있다.

특정 형태의 자료는 형식에 있어서 표준화 되어 있으며 경험 있는 기계어 프로그래머 라면 소량의 형식으로도 쉽게 알아볼 수 있다.

이러한 것으로는 ASCII 또는 EBCDIC 문자, 16비트 및 32비트 적분, IEEE 부동소수점 그리고 여러 백터와 영상 그래픽 래스터(Raster)가 포함된다.

그 밖의 다른 형태는 관련 응용에 의해서만 의미가 주어지며 내부 프로그램 구조가 이해될 때만 의미가 통한다. 많은 보안전산 시스템에서는 모든 저장 자료가 암호화 되어 있으므로 어떤 형태의 자료에 해당하는 것까지는 안다고 해도 정확한 내용까지는 전혀 단서를 잡을수가 없는 것이다. 도청자로써 가장 손쉬운 경우는 프린터 또는 CRT로 가는 자료가 사람이 읽기 쉬운 형식으로 되어 있을때가 가장 확실하여 간단히 살피더라도 무엇인지 알수가 있다.

실제로 깨끗한 신호는 종종 도청장치 형태에 의해 바로 도청되어져 중요자료가 누출될 수 있는 것이다.

그 밖의 다른 형태의 정보를 해독하기 위해서 도청자는 전문적인 암호 분석가의 기술을 필요로 할 것이며 세계 어느 정보기관이든 이들은 존재하는 것이다.

때때로 암호화된 자료를 탐지할 필요가 있는데 특히 평상문 또는 기타 원문과 정합될 수 있을때는 그러하다. 그 이유는 정합된 평상문과 암호문은 실제의 키(Key)가 없더라도 암호 해독자로서는 가장 바람직한 자료인 것이다.

제5장 향후전망 및 과제

앞에서 전파정보누설의 탐지 및 대책에 관한 사항을 두루 살펴 보았듯이 이 연구를 수행하기 위하여는 고도의 기술, 전문성과 노력이 수반되어져야 한다는 생각이다.

선진국의 기술은 비밀로 되어 공개치 않는 상황이며 우리의 이 분야의 기술은 열악한 상태에서 국제적인 상황은 냉전체제의 종식과 더불어 경제전쟁을 방불케 하는 경제권 주도를 향하여 뛰고 있는 현실이다.

즉 국가의 정보채널을 상대국의 중요산업등의 기술을 빼어내는 데에 초점을 두고 있는 것이다. 만약 우리가 이에 대처할 수 있는 대책을 서두르지 않는다면 국가나 기업등의 중요 비밀이 상대의 고도 도청기술에 의하여 고스란히 넘어가는 위험성을 지적하면서 향후전망과 우리과제(의견)를 살펴보고자 한다.

1. 향후전망

가. 기술도입 전망

정보탐지를 위한 고가의 수신기를 수입하기 쉽지 않다는 점과 미국의 경우 정보누설 탐지와 정보누설 측정방법, 절차 및 대책기술등이 비밀로 분류되어 있고 대책된 기기도 구입키 어려운 실정이다.

또한 일본, 영국, 프랑스, 독일 등의 국가도 이에 대한 연구는 비밀과제로 분류하여 수행하고 있다는 점을 감안할때 기술도입 전망은 현실적으로 불가능하다 할수 있다.

나. 상용화 전망

보안을 요하는 정보의 처리가 한곳에 집중되어 있던때는 그곳을 완전히 차폐하는 것이 대책의 주를 이루어 왔으나 다양한 개인용 컴퓨터나 단말기 및 주변기기들의 확산과 정부, 공공기관, 군, 단체, 기업, 개인의 정보이용으로 인한 정보처리 분산화로 인해 여러장소에서 쓰이는 각각의 정보처리 기기들에 대한 정보보호의 중요성이 대두되게 되었고 따라서 정보누설에 대책된 기기들의 필요성이 증대되고 있다.

앞으로 1990년대 하반기에는 정보누설에 대책된 기기들의 상용화도 예측되고 있으며 대상기기도 증가할 것으로 예상된다.

이러한 추세는 미국을 비롯한 선진국들의 정보누설 대책규격 등급화에 의한 규격완화 추세이며 각국 정부의 경우 자국의 공공기관이나 금융기관 들에 대한 정보보호법 제정에 대한 요구가 증가되고 전자 및 소재기술들의 발달로 인한 정보누설 대책의 비용절감에 의해 가속화 될 것이라 전망된다.

2. 우리의 과제

가. 우리기술 상태의 취약성

요구되는 기술이 극히 미세한 전파(불요전자파)를 가능한한 먼거리에서 주파수와 방향을 선별하여 수신하고 수신된 신호로부터 정보를 재생할 수 있는 특성을 추출해 내는 최첨단의 탐지기술과 이와는 반대의 최첨단 기술로도 탐지하지 못하게 정보를 포함하고 있는 불요전자파 억제와 신호의 탐지를 못하게 방해하는 방법이 정보보호 기술인데 이것은 우리나라가 외국에 비해 기술적인 열세가 두드러진 전파 및 RF 기술의 최첨단이므로 국내에서의 현 기술상태는 개념적으로는 문제는 없으리라 여겨지나 경험부족이 취약점이라 사료된다.

우리나라에서 '80년대 중반부터 기업체와 연구기관, 정부기관에서 전기·전자제품이나 자동차 등의 수출과 관련하여 EMI/EMC에 관심을 갖기 시작하여 본격적으로 이에 대한 연구가 수행되어 국내규격을 마련한 것은 근래의 일로써 EMI/EMC 관련 측정기술이나 불요전자파 억제기술의 수준이나 이에 필요한 소재나 부품개발의 기술수준은 아직 국제수준에 못미치는 실정이다. 게다가 국내·외 사용규격이나 미국의 군사규격에 적합 수준의 대책된 제품도 고도 정보탐지 기술로써 수십m 에서도 정보탐지가 가능하기 때문에 더욱더 엄격한 억제기술이 필요하며 이에 대한 우리의 경험과 기술이 아주 취약한 상황이다.

나. 우리의 과제(의견)

정보누설 탐지 및 대책기술이 각 나라마다 비밀로 수행되어지고 있으며 또한 선진국의 첨단장비나 고도의 기술도입이 거의 불가능한 상황이나 이 연구의 중요성과 필요성으로 비추어볼때 국가의 주도와 지원체제하에 고도의 전문성을 갖는 전문 연구기관에서 연구가 반드시 이루어져야 된다는 의견이며 정보누설 탐지기술 면에서는 우리 기술의 취약성으로 연구수행의 어려움이 많겠지만 정보누설 대책기술 면에서는 EMI/EMC 등의 대책기술과 밀접한 관련성이 있는바 우리도 이러한 EMI/EMC 기술이 상당히 축적되어 있으므로 정보누설 대책기술 중심으로 연구가 수행된다면 가능하리라는 생각이다.

다음은 연구가 수행되어질때 연구의 기술적 측면에서 수행되어져야 할 기술적 사항을 대략적으로 제시해 보고자 한다.

(1) 정보누설 탐지기술

컴퓨터나 워드프로세서 또는 단말기, 프린터, 모뎀등 디지탈 기기로부터의 불요전자파는 도체면을 따라서 전도되는 것과 공간중으로 방사되는 두 종류가 있다.

이들 미약 신호를 탐지하여 정보를 재생하기 위하여는 ANT기술, Sensor기술, RF/MW수신기기술, 신호처리기술, 디코딩기술 등이 요구된다는 것이다.

가능한한 먼거리에서 특정한 정보기기로 부터의 선택된 정보를 도청하기 위해서는 안테나는 고지향성, 고이득, 광대역 특성과 수신기는 넓은 동작영역, 고감도, 고분해능, 광대역 특성을 가져야 할 것이며 또한 정보처리 기기의 처리속도가 빨라질수록 더욱 고감도, 광대역 특성이 요구된다고 할수 있다.

- o 누설정보 재생기술 연구
  - 안테나 특성(이득, 극성등)
  - 수신기 특성(감도, 동작영역등)
  - Decoding 기술(디스플레이)
  - 정보재생 시스템 구축(안테나,수신기,CRT, 인터페이스)
  - 누설전파 측정방법 및 절차(안테나,수신기 측정시설등)
  - 운용 소프트웨어

- o 누설정보신호 특성분석 연구
  - 주파수영역의 특성
  - 시간영역의 특성
  - 변조영역의 특성
  - 신호추출 기술

(2) 정보누설 대책기술

정보탐지에 대항하는 대책기술은 방사잡음을 크게 낮추어 정보를 포함하고 있는 불요전자파를 수신하지 못하게 하는 기술과 수신하더라도 정보를 추출해 내지 못하게 교란하거나 암호화하는 두가지 기술로 분류된다.

전자는 EMI(전파자장해)대책기술과 개념적으로 유사하나 훨씬 엄격한 차폐, 필터링, 접지 및 인터페이스 기술 등이 요구된다는 점에서 기술상의 어려움이 있다고 할수 있다.

또한 회로 레벨에서의 대책설계시 **Red/Black Interface**를 결정하여 정보가 포함된 Red Interface에 엄격한 대책기술을 가해야 한다는 점이 차이점이며, 후자의 경우는 동작 주파수를 모르게 하거나 신호특성 추출을 불가능하게 하기 위하여 광대역 노이즈나 신호를 동시에 발사하는 방법등을 들수 있다.

중요정보 보호는 정보누설 보호대책이 성공적으로 이루어진 장치나 기기를 사용해야만 정보를 보호할 수 있는데 이를 위해서는 어느 특정기기의 보호대책이 사용하려는 주변여건에 맞게 이루어졌는지를 상용화 하기전에 확인해야 할 것으로 사료되며, 이를 위해서는 측정시설, 설비, 측정장비, 측정방법 및 순서, 항목, 보호레벨별, 신호특성별 누설 허용치 등에 관한 기술적 기준이 필요하고 이중에서 측정시설은 EMI(전자파장해) 측정시설보다 고도의 성능과 기술이 요구되어 질 것이며 측정방법등도 고도의 기술이 요구되어진다 할 것이다.

특히 안테나, 센서 및 측정장비는 펄스폭이나 **Rise/Fall Time, Dwell Time,** 펄스 반복율등 신호의 파형특성을 측정할 수 있어야 하므로 이 역시 최첨단의 수신기 및 신호처리 기술이 요구되어 질 것이며 이는 정보처리 속도가 빨라져 감에 따라 대책기술이 발달되어 감에 따라 더욱더 고도의 기술이 필요하다 할 것이다.

- o 전파정보 보호대책기술 연구
  - 대책부품 및 차폐소재 연구 및 개발
  - 대책부품, 차폐소재 성능 측정
  - 차폐실 설계기술
  - 불요전자파 억제기술
  - PC의 불요전자파 억제기술
  - 대책기기 측정기술 기준
  - 컴퓨터와 주변장치 불요전자파 억제기술
  - 인터페이스(데이타통로)차폐기술
  - 중요정보의 암호화 및 체계기술 연구

제6장 결 론

본 연구는 현대 정보화사회의 각 분야에 보급되어 사용되는 디지탈 정보기기로부터 방출되는 불요전자파에 의한 실시간 중요 정보누출 문제점을 극복할 수 있는 관련대책 기술들을 살펴보았고, 또한 우리가 앞으로 이러한 문제점에 대처하기 위한 심도성 있는 연구가 활성화 되도록 그 연구의 기술적 측면에서 반드시 수행되어야 할 사항을 제시하였다. 그리고 정보누설 탐지기술을 살펴서 개인, 산업체, 국가기관의 중요 비밀을 취급하는 정보처리 기기가 아무런 대책없이 운용되어질때 부지불식간 타인이나 타국에 의하여 도청될 수 있다는 위험성과 정보보호 대책의 중요성을 인식시키고자 하였다.

정보의 생성, 획득 및 유지가 가장 중요한 현대 정보사회에서 정보의 주체가 정부기관이든, 공공기관이든, 군(軍) 또는 기업이나 각 개인이든 그 정보의 안정성이 보장되어 있어야 한다는 점은 그 사회가 유지되기 위한 전제조건인 것이다.

현대의 국가 경영은 국민 개개인에 대한 갖가지 정보를 정부나 공공기관이 관리·유지·이용하고 있으며 군이나 국가기관은 국가경영의 성패를 좌우할 수 있는 중요한 정보(국방안보, 외교, 통상, 치안)를 관리 운용하고 있다.

이러한 국가정보나 개인정보는 이를 부당하게 이용하려고 하는 의도로부터 철저히 보호되어야 한다. 또한 기업의 국내·외 활동에 필요한 기업정보는 그 기밀유지가 기업의 흥망을 좌우할 수 있는 경우가 비일비재한 것이다.

이는 기업의 사업계획, 신제품개발, 수출·입 관련 정보등의 경우에 있어 필수적이며, 기업이나 연구기관의 경우도 신소재개발, 신의학품개발, 첨단기술 연구개발 등에 있어서 정보보호가 점점 더 필수적으로 되어가고 있다.

또한 개인정보를 다루고 있는 금융기관, 보험회사, 신용카드회사 등의 활동에 있어 개인정보의 기밀유지는 필수적이며 이는 정보보호법 제정의 추세가 있는 현 사회에서 그 필요성은 더욱 중대되고 관심사항이 될 것이다.

하지만 우리의 경우는 중요정보가 누출될 수 있다는 위험성과 정보보호 대책의 중요성 및 당위성을 거의 인식하지 못하고 있다는데에 그 심각성이 있는 것이다.

이미 선진국에서는 정보누출을 방지하고 탐지하는 연구가 계속 이루어져 상당한 수준에 있으며, 특히 미국의 경우 1950년대말부터 TEMPEST 라는 과제명하에 비밀리에 진행되어 오고 있다. 하지만 이에 대한 탐지기술이나 대책기술에 대한 정보는 각 나라가 비밀로 하여 공개치 않으므로 인하여 거의 접근할 수 없는 상황이다.

우리는 이제 정보보호 대책의 중요성을 심각히 인식하여 국가의 주도 및 홍보, 지원체제하에 전문 연구기관의 심도성 있는 연구가 하루빨리 이루어져야 하리라는 생각이다.

참 고 문 헌

1) Electromagnetic Radiation from Video Display Units, Laboratories of the Netherlands PTT, 1985

2) Tempest Secure Computing Equipment & Markets, International Resource Developement Inc, 1987

3) Journal of Electronic Defence, 1991

4) An Overview of Tempest Technology, Datapro Research Corporation, 1987

5) パソコソの 情報對策, 三菱電氣(株), 1991

6) 퍼스날컴퓨터용 정보보안 장치개발, 경북대학교, 1991

7) 전자파장해(EMI) 방지기술연구, 전파연구소·한국전자파기술학회, 1991

8) 불요전자파(EMI) 감시대책연구, 한국전기전자학회, 1993

9) 전자파차폐 및 흡수특성을 갖는 복합체개발, 한국전자파기술학회, 1993