키보드 누설 방사에 의한 정보 누설 취약성 분석

Analysis on the Vulnerability of Information Leakage through Electromagnetic Emanations from PC Keyboard

이 대 헌 · 황 인 호

Dae-Heon Lee · In-Ho Hwang

요 약

본 논문에서는 PC 키보드의 누설 전자파에 의한 정보 누설 취약성을 분석하였다. 먼저 키보드 프로토콜과 하드웨어 구조를 살펴보고, 키보드에서 PC 본체로 전송되는 데이터 신호와 본체 전원선에 누설된 신호 사이의 상호 관계를 분석함으로써 키보드 전도성 방사의 원인을 파악하였다. 또한 키보드 누설 전자파의 크기를 계산하고 CISPR 22 규격의 허용 레벨과 비교하였다. 간단한 실험을 통하여 PC 본체 전원선의 신호를 분석하여 키보드 글쇠 내용을 얻을 수 있음을 보임으로써, PC 사용자의 중요 정보가 누설될 수 있음을 확인하였다.

Abstract

In this paper, we analyzed the vulnerability of information leakage due to the leakage electromagnetic waves of a PC keyboard. First, we reviewed the keyboard protocol and hardware structure, we analyzed the correlation between the data signal, which is transmitted from the keyboard to the main body, and the leakage signal on the power cable. With the result, we grasped the cause of the Conducted Emission of a PC keyboard. Also, we compared the limit level of the CISPR 22 standard with the amplitude of the keyboard leakage electromagnetic waves we calculated. By analyzing the signal on the power cable of the PC main body through the simple experiment, we show that it is possible to extract the contents of the PC key. Therefore it is verified that the secret information of the PC user could leak out.

Key words : Electromagnetic Emanations, Conducted Emission, Information Leakage, Keyboard

Ⅰ. 서 론

PC 모니터에서 비의도적으로 발생되는 누설 전자파에 의해 중요 정보를 포함하는 화면 정보의 누출 현상은 여러 논문을 통해서 보고되었다[1],[2]. 누설 전자파를 이용한 공격 패턴은 기존의 하드웨어를 이용한 물리적인 공격이나 네트워크를 통한 소프트웨어 공격과는 달리 전혀 비파괴적, 비접근성이라는 특성 때문에 문제의 심각성은 매우 크다. 따라서 미국과 유럽 국가들은 이미 1950년대 이전부터 연구를 시작하여 PC와 같은 정보기기에서의 전자파 누설 방사 문제를 해결하기 위하여 TEMPEST 규격을 제정하고 관련 기술을 엄격히 보호하고 있다[3].

PC의 주요한 정보 입력 장치의 하나인 키보드에서도 PC 사용자가 정보를 입력할 때 키보드 각각의 글쇠에서 발생되는 고유한 음파를 원격지에서 측정함으로써 PC 사용자의 로그인 암호, 인터넷뱅크 비밀번호들이 유출될 수 있음이 발표되었다[4]. 뿐만 아니라 키보드의 LED 지시자를 통한 광파 누설 가능성이 모의 시험을 통해 제시되었다[5]. 1999년 Anderson과 Kuhn은 누설 전자파에 의한 키보드 입력 정보 누설 현상을 수동 위협, 능동 위협 두 가지로 언급하였

한국전자통신연구원 부설 국가보안기술연구소(National Security Research Institute, ETRI)

· 논 문 번 호 : 20061117-145
· 수정완료일자 : 2007년 1월 4일

다[6]. 수동 위협은 키보드 스캔 사이클의 고조파에서 RF 누설 방사가 일어나는 것이고 능동 위협은 PC 키보드 케이블에 공진 주파수를 의도적으로 조사시켜, 재 방사된 고조파 성분을 복조하여 키보드 스캔 코드를 분석하는 방법이다. 본 논문에서는 전도 누설의 주요 경로가 될 수 있는 PC 본체 전원선에 존재하는 키보드의 누설 전자파를 측정하여 키보드 스캔 코드와의 상호 관계를 알아봄으로써 키보드의 수동 전자파 누설 방사를 입증하였다. 키보드의 누설 전자파를 통한 정보 유출의 원인을 분석하기 위하여 키보드의 구조와 작동 원리를 알아보고, 누설 위협을 정량적으로 분석하기 위하여 누설 스펙트럼과 전력을 계산하고 관련 규격과 비교하였다.

Ⅱ. 키보드 프로토콜

2-1 PC 키보드 인터페이스

우리가 사용하는 대부분의 PC 키보드는 PC 본체에 스캔 코드를 전송한다. 스캔 코드는 사용자가 입력한 키보드의 글쇠 정보를 의미하는데, 예를 들어 A 글쇠를 입력하면 키보드는 A 글쇠를 의미하는 스캔 코드 '1C(hex)'를 시리얼 라인을 통해 PC 본체에 전달한다. 만약 전송 시간 이상 계속 누르고 있으면 다른 글쇠가 입력되거나 A 글쇠를 떼지 않는 이상

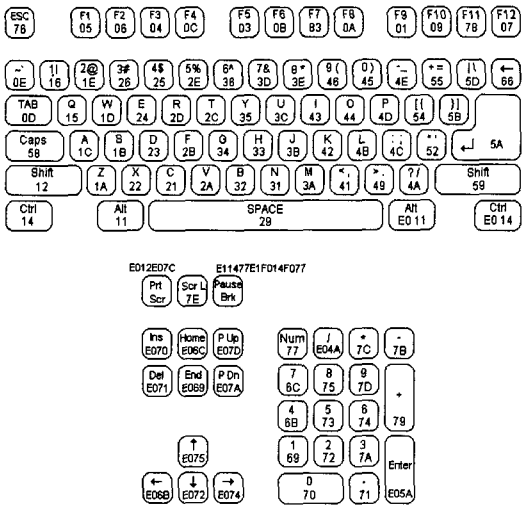

그림 1. 101 키보드의 스캔 코드
Fig. 1. Scan code of keyboard.

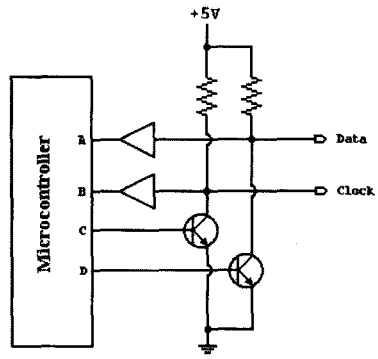

그림 2. 키보드 개방 컬렉터 인터페이스
Fig. 2. Open collector interface of keyboard.

계속 전달하게 된다. 그리고 A 글쇠를 떼면 키보드는 이를 알리기 위해 스캔 코드 'F0(hex)'를 마지막으로 보낸다. 따라서 PC 키보드 각각의 글쇠에는 그림 1과 같은 해당 스캔 코드가 이미 할당되어 있다.

기본적으로 PC 키보드에는 Clock, Data, Ground, Vcc(+5 V) 라인이 있는데, Data와 Clock 라인은 그림 2와 같이 풀업 저항(pullup resistor)을 통해 Vcc에 연결된 개방 컬렉터(open collector) 구조로 되어 있다. 개방 컬렉터 인터페이스는 저 임피던스(low impedance)와 고 임피던스(high impedance) 상태를 갖는다. 저 임피던스 상태에서 트랜지스터는 해당 라인을 접지 레벨로 떨어뜨려 'low' 상태가 되고, 고 임피던스 상태에서 트랜지스터는 개방 회로로 동작되어 해당 라인은 풀업 저항을 통해 Vcc에 연결되어 있기 때문에 'high' 상태가 된다.

2-2 통신 프로토콜

키보드에서 본체로의 정보 전송은 그림 3과 같이 11 비트가 1 프레임을 구성한다. 첫 번째 비트는 시작 비트(로직 0)이고, 이어서 8개의 데이터 비트, 1개의 패리티 비트, 정지 비트(로직 1) 순이다. 여기에서 데이터 비트는 LSB(Least Significant Bit) 우선이고, 패리티 비트는 홀수 패리티이다. 각 비트는 클록의 하강 에지에서 읽는다. 클록 신호는 키보드가 발생시키는데 그것의 주파수는 전형적으로 10~30 kHz 이다.

본체에서 키보드로의 전송 프로토콜은 먼저 Data 라인을 'low' 상태로 만들어 초기화한다. 그러나 동시

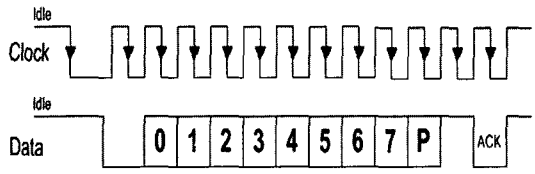

그림 3 본체에서 키보드로의 데이터 전송
Fig. 3. Communication: main body - keyboard.

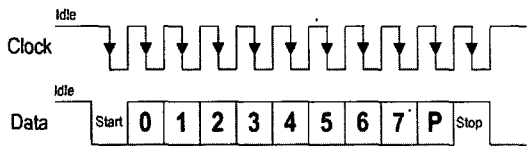

그림 4. 키보드에서 본체로의 데이터 전송
Fig. 4. Communication: keyboard - main body.

에 키보드의 데이터 전송을 막기 위해 일반적으로 본체 전송 요구 상태 전에 Clock 라인을 60 μs 이상 'low' 상태로 떨어뜨린다. 그런 다음 Data 라인을 'low' 상태로 하고 Clock 라인을 'high' 상태로 하여 초기화한다. 초기화되면 키보드는 Clock 라인을 통해 클록 신호를 약 10 ms 동안 발생시킨다. 첫 번째 하강 에지에서 본체는 Data 라인에 첫 번째 데이터를 전송한다. 전송된 데이터 비트는 클록의 다음 번 하강 에지에서 키보드에 의해서 읽혀진다. 이때 두 번째 데이터 비트를 전송한다. 이러한 과정은 8개의 데이터 비트에 대해 반복적으로 수행되고, 이후 홀수 패리티 비트가 전송된다. 일단 패리티 비트가 전송되면 다음 번 클록 사이클에서 Data 라인은 'high'(아이들) 상태로 설정된 다음 키보드는 ACK(ACKnowledgement) 신호를 수신한다. 만약 이후에 Data 라인이 아이들 상태로 설정되지 않으면 키보드는 Data 라인이 아이들 상태가 될 때까지 클록 신호를 계속해서 보낸다.

Ⅲ. 키보드 누설 측정

키보드의 중요 정보를 포함하고 있는 누설 전자파가 PC 본체 전원선을 따라 전도되는 위협 현상을 관측하기 위해 PC 본체 전원선에 전류 프루브를 이용하여 오실로스코프로 시간 영역 파형을 측정하였다. PC 본체 전원선에는 많은 노이즈 신호가 존재하나, 본 논문에서는 사용자가 입력한 키보드 글쇠와의 연관성을 조사하기 위해 키보드에서 누설되어 PC 본체 전원선으로 전도되는 누설 전자파 신호에만 관심을 두었다.

우리가 일반적으로 사용하고 있는 PC 환경에서 PC 본체 전원선상에 존재하는 전도 누설 전자파를 측정하였다. EUT(Equipment Under Test) 및 측정 계측기 대표 사양을 아래 표에 정리하였다. 전류 프루브와 LISN(Line Impedance Stabilization Network: 전원 임피던스 안정화 회로망)은 EMC(Electromagnetic Compatibility) 국제 규격인 CISPR 요구 조건을 만족한다. LISN은 EUT에 표준화된 RF 부하 임피던스(50 Ω)를 부여한다. 이런 목적으로 LISN은 EUT와 회로망 단자에 직렬로 삽입되어 외부로부터 유입되는 잡음 신호는 격리시켜 주고, EUT에서 발생되는 잡음 신호는 반사 없이 통과시키는 역할을 한다.

그림 5는 측정 구성도이다. 편의상 PC 본체 전원 연결과 전류 프루브, 오실로스코프 사이의 동축선 연결 부분만 표시하였다. 차폐실 내부에 80 cm 높이의 비 전도성 탁자를 이용하여 금속 벽면으로부터 40 cm 이격시킨 후 EUT를 설치하였다. 그 밖의 EUT와 계측기 동작 요구 조건 및 케이블 위치 등은 CISPR 요구 조건을 준수하였다. PC 본체는 LISN을 통해 교류 220 V 전원이 공급되고, PC 본체와 LISN

표 1. EUT 사양
Table 1. EUT specification.

Item	Model	Spec.
키보드	삼성 K291	106키, PS/2, 멤브레인
PC 본체	COMPAQ Evo	Pentium 4 2.66 GHz
모니터	LG L1530S	15인치 LCD

표 2. 측정 계측기
Table 2. Measuring instruments.

Item	Model	Spec.
오실로스코프	Tektronix TDS7704B	20 GS/S
전류 프루브	Rohde Schwartz ESV-Z1	9 kHz~600 MHz
LISN(Line Impedance Stabilization Network)	Rohde Schwartz ENV216	9 kHz~30 MHz

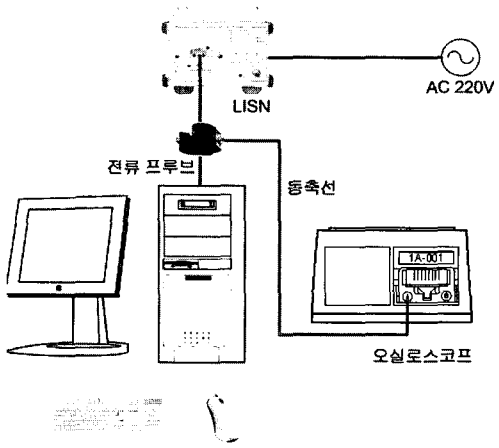

그림 5. 측정 구성도
Fig. 5. Measurment setup.

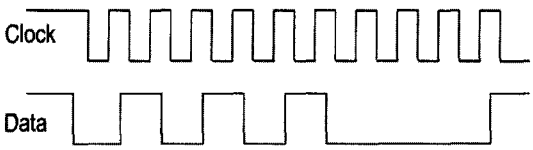

그림 6. Q 글쇠의 전송 신호
Fig. 6. Signal for Q key.

사이에 클램프형 전류 프루브를 삽입하고 디지털 오실로스코프의 입력 단자에 동축선을 연결한다.

사용자가 Q 글쇠를 입력하면 PC 키보드는 스캔 코드, '15(hex)'를 본체에 전송한다. '15(hex)'는 2진 코드로 '00010101' 이므로 키보드는 이를 직렬로 본체에 전송한다. 그림 6은 Q 글쇠를 입력하였을 때 PC 키보드 라인을 통해 전송하는 클록 신호와 데이터 신호를 나타낸다.

Ⅳ. 결과 분석

4-1 키보드 누설 신호 파형

그림 7의 채널 3 누설 신호 파형은 Q 글쇠를 눌렀을 때, PC 본체 전원선에서 전류 프루브로 측정한 신호 파형이다. 키보드 라인에서의 데이터 및 클록 신호 파형과의 상호 관계를 분석하기 위해 데이터 신호 파형(채널 1), 클록 신호 파형(채널 2)과 함께 나타내었다. PC 본체 전원선에서 임펄스 신호가 관측되는데, 이러한 임펄스 신호의 시간적 위치는 키보드의

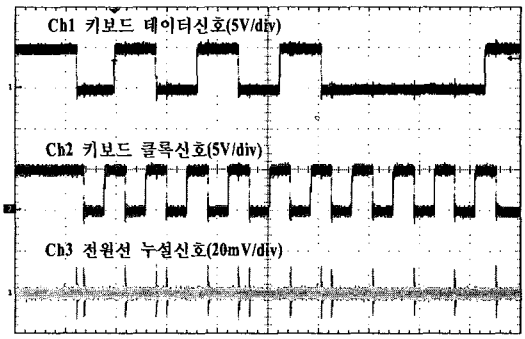

그림 7. 키보드 신호와 전원선 누설 신호
Fig. 7. Keyboard signal and leakage signal on power cable.

데이터와 클록 구형파 신호의 하강 에지와 일치함을 알 수 있다. 따라서 PC 본체 전원선에 존재하는 누설 신호의 간단한 측정 및 분석을 통해 키보드 입력 정보를 알 수 있다. 역으로 말하면 키보드의 중요 정보는 전도 누설 전자파에 의해 유출 가능성이 존재한다고 할 수 있다.

키보드 누설의 원인을 분석하기 위해 먼저 키보드 데이터 신호의 상승 특성과 하강 특성을 알아보았다. 상승 시간은 그림 8과 같이 약 1.4 μs, 하강 시간은 약 84 ns 로 측정되었다. 데이터 신호의 하강 특성은 상승 특성에 비해 급격한 과도 특성 및 오버슈트(overshoot) 현상을 보이고 있다. 디지털 신호의 과도 시간이 짧을수록 고조파 성분이 많이 포함되고 이러한 고조파 성분은 누설의 주요 발생원이 되고 있다.

키보드 신호의 하강 에지, 즉 'low' 상태로 될 때 누설 신호가 발생되는 원인은 앞의 그림 2에서 본 바

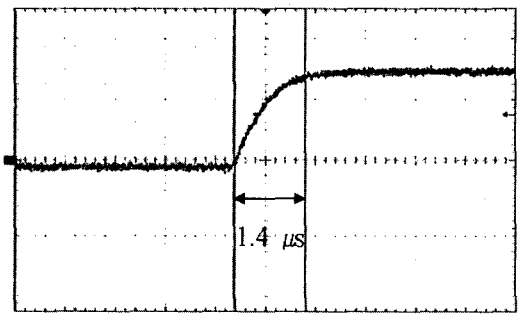

그림 8. 키보드 데이터 신호의 상승 특성
Fig. 8. Rising characteristics of keyboard data signal.

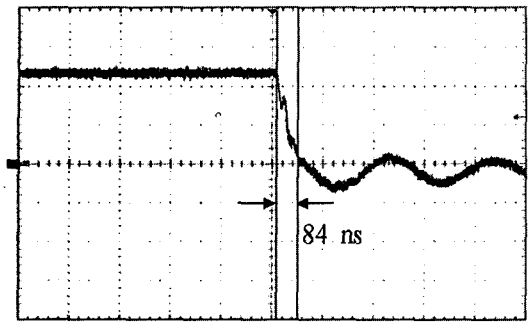

그림 9. 키보드 데이터 신호의 하강 특성
Fig. 9. Falling characteristics of keyboard data signal.

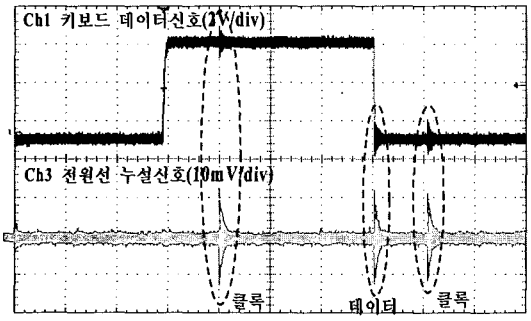

그림 10. 키보드와 전원선의 노이즈 신호
Fig. 10. Noise signal of keyboard and power cable.

와 같이 키보드의 Data, Clock 라인은 트랜지스터의 컬렉터 단자에 연결되어 있는데, 트랜지스터의 턴온(turn on) 동작 시에 Data, Clock 라인은 'low' 상태로 된다. 그런데 트랜지스터의 턴온 시간은 턴 오프 시간에 비해 상대적으로 시간이 짧고 오버슈트(overshoot) 현상도 나타난다. 이는 트랜지스터와 회로상에 존재하는 표유 인덕턴스 성분에 의한 환류 전류(free-wheeling current) 때문이다[7]. 따라서 트랜지스터가 턴온될 때 발생하는 오버슈트(overshoot) 및 꼬리(tail) 성분은 그림 10과 같이 Data 및 Clock 라인이 'low' 상태로 될 때 노멀 모드(normal mode) 노이즈 성분으로 작용하고 이러한 노이즈 성분이 PC 본체 전원선으로 전도되는 것으로 판단된다.

4-2 키보드 누설 신호 스펙트럼

다음은 누설 신호 크기를 계산하여 관련 규격인 EMC 규격과 비교하였다. 글쇠를 눌렀을 때, 키보드 라인에서 전류 프루브와 오실로스코프를 이용하여

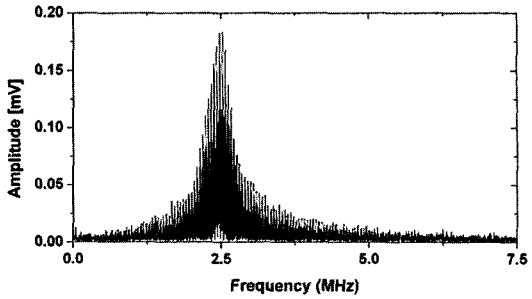

그림 11. 키보드 라인의 누설 신호 스펙트럼
Fig. 11. Spectrum of keyboard leakage signal.

시간 영역의 누설 신호 파형을 얻고 이를 FFT(Fast Fourier Transform)하여 주파수 영역으로 변환하였다.

그림 11은 누설 신호의 스펙트럼으로 2.5 MHz에서 0.183 mV 정도 되었고, 이를 CISPR 22의 B급 기기에 대한 허용 레벨과 비교해 보았다.

스펙트럼의 크기를 $dB\mu V$로 바꾸고, CISPR 22의 RBW(Resolution Bandwidth: 분해능 대역폭) 측정 규격인 10 kHz로 환산하기 위하여 먼저 FFT로 얻은 스펙트럼의 RBW를 아래와 같이 계산하였다.

$$RBW_{FFT} = \frac{1}{N_{points} \times T_s} = \frac{1}{32,768 \times 2 \times 10^{-8}} = 1.526\ kHz$$

여기에서 N_{points}는 FFT 계산 사이즈(size)에 해당하며, T_s는 샘플링 주기, RBW_{FFT}는 FFT 스펙트럼의 RBW이다. 계산된 FFT 스펙트럼 RBW를 이용하여 CISPR 22 규격의 RBW로 환산한 스펙트럼의 크기를 $dB\mu V$ 단위로 계산하면 다음과 같다.

$$S_{CISPR} = 20\log\left(\frac{S_{FFT}}{1\ \mu V}\right) + 10\log\left(\frac{RBW_{CISPR}}{RBW_{FFT}}\right) = 20\log\left(\frac{0.183\ mV}{1\ \mu V}\right) + 10\log\left(\frac{10\ kHz}{1.526\ kHz}\right) = 53.5\ dB\mu V$$

여기에서 S_{CISPR}은 CISPR 22 규격의 RBW로 환산한 스펙트럼의 크기, S_{FFT}는 FFT로 계산한 스펙트럼 크기, RBW_{CISPR}은 CISPR 22 규격의 측정 RBW에 해당한다.

CISPR 22 규격으로 환산한 결과, 53.5 $dB\mu V$는 CISPR 22 규격의 B급 기기를 위한 0.55~30 MHz의 주파수 영역에서의 통신 단자에서 발생하는 전도성

방해의 허용 레벨 64 $dB\mu V$보다는 작으므로 규격을 만족시키고 있다. 그러나 키보드에서 누설된 전자파에는 키보드 사용자의 입력 정보가 그대로 포함되어 있으므로 EMC 규격인 CISPR 22 규격을 만족한다고 하더라도 정보 유출 가능성은 존재한다고 판단된다.

V. 결 론

본 논문에서는 PC 키보드의 누설 전자파에 의한 정보 누설 취약성을 분석하였다. PC 키보드의 트랜지스터가 턴온될 때 발생하는 오버슈트(overshoot) 및 꼬리(tail) 성분의 노이즈 신호가 본체 전원선까지 전도되어 사용자가 입력한 글쇠 내용이 누설될 수 있음을 확인하였다. PC 키보드 누설 전자파의 크기는 EMC 규격인 CISPR 22의 방해 허용 레벨 이하임에도 불구하고 정보 누설에 취약한 것으로 생각된다. 따라서 우리나라도 TEMPEST 규격과 같은 누설 전자파에 의한 정보 누설을 방지할 수 있는 규격 및 관련 기술에 대한 연구가 시급하다.

향후에는 복사성 방사(Radiated Emission)에 대한 누설 취약성 분석과 중요 정보 누설 방지 기술에 대한 연구가 필요하다.

참 고 문 헌

[1] Wim van Eck, "Electromagnetic radiation from video display units: an eavesdropping risk", *Computers & Security*, vol. 4, pp. 269-286, 1985.

[2] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays", *Technical Report UCAM-CL-TR-577*, Computer Laboratory, University of Cambridge, 2003.

[3] National Security Agency, "NACSIM 5000 TEMPEST Fundamentals", Fort George G. Meade, Maryland, Partially declassified transcript: http://cryptome.org/nacsim-5000.htm., Feb. 1982.

[4] D. Asonov, R. Agrawal, "Keyboard acoustic emanations", *IEEE Symposium on Security and Privacy*, pp. 3-11, 2004.

[5] Joe Loughry, David A. Umphress, "Information leakage from optical emanations", *ACM Transactions on Information and System Security*, vol. 5, no. 3, pp. 262-289, Aug. 2002.

[6] Ross J. Anderson, Markus G. Kuhn, "Soft tempest - an opportunity for NATO", *Proceedings of Protecting NATO Information Systems in the 21st Century, IST Symposium*, Washington D.C., U.S.A., Oct. 1999.

[7] Eiji Sakai, Koosuk Harada, "A new synchronous rectifier using bipolar transistor drivern by current transformer", *IEEE Telecommunications Energy Conference INTELEC '92 14th International*, pp. 424-429, 1992.

이 대 헌

1999년 2월: 경북대학교 전자전기공학부 (공학사)
2001년 2월: 경북대학교 전자공학과 (공학석사)
2001년 1월~2003년 5월: Actipass Inc. R&D Research Staff
2003년 6월~현재: 한국전자통신연구원 부설 국가보안기술연구소
[주 관심분야] EMI/EMC, 안테나공학, 전파전파

황 인 호

1980년 2월: 한양대학교 전파 및 통신공학과 (공학사)
1982년 2월: 중앙대학교 전자공학과 (공학석사)
1986년 2월~2000년 1월: 국방과학연구소
1992년 3월~1999년 2월: 한국과학기술원 전기 및 통신공학과 (공학박사)
2000년 2월~현재: 한국전자통신연구원 부설 국가보안기술연구소
[주 관심분야] 정보보호, 이동통신, 통신신호처리, EMI/EMC