

Tempest Hacking



2011.12.18

hkdakuo@gmail.com (김종민)

Content

- 팀
- 템페스트
 - 예
 - 정의
 - 신호
- CRT 템페스트 해킹
- 시연
- 대응방안
- 참조

Team

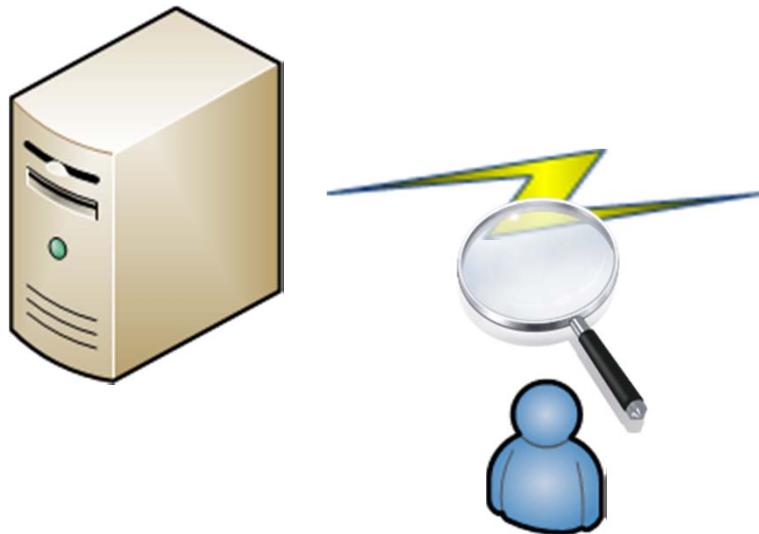
- **dakuo**
 - 김종민
 - 인하대학교
 - hkdakuo@gmail.com
 - <http://dakuo.tistory.com>
- **decinc**
 - 윤진수
 - 인하대학교
 - decinc@naver.com
 - <http://decinc.tistory.com>

Tempest – example 1

Title: 템페스트 공격 TEMPEST attack

예전에 누가 키즈에서 이야기할 때는 뺑이 아닐까 의심했는데 이런게 진짜로 있었다.

내용인즉슨, 키보드를 칠 때 키보드와 컴퓨터 본체 사이에 이어진 전선에 흐르는 미약한 전류에서 발생하는 전자기파를
검출해 내어 사용자가 무슨 키를 치고 있는지 알아내는 해킹을 템페스트 공격이라고 한다.



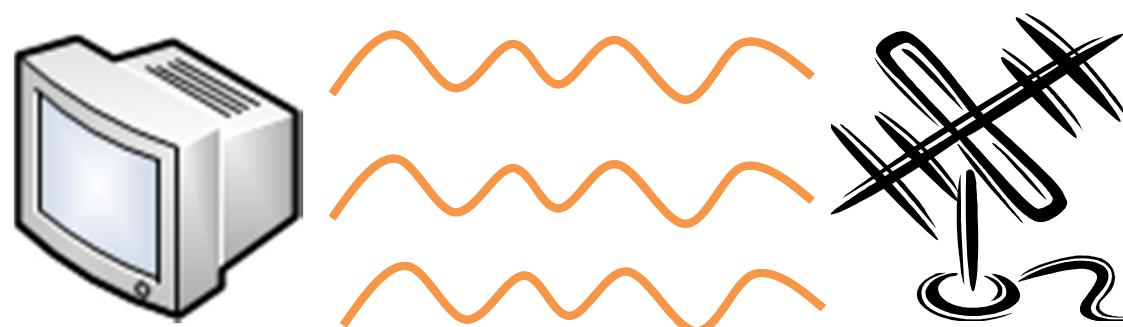
Tempest – example 2



템페스트 해킹

이창무 교수 한남대 경찰행정학과 | 제215호 | 20110424 입력

컴퓨터가 인터넷 등 통신망에 연결돼 있지 않으면 안전하다고 생각할지 모른다. 그래서 중요 정보를 다루는 곳에서는 실제로 외부와의 네트워크를 아예 차단한다. 그러나 컴퓨터 스크린에서는 일정한 전자파가 발생한다. 그래서 어느 정도 거리가 떨어져 있어도 컴퓨터 스크린에서 발생하는 전자파를 안테나로 잡아 이를 증폭한 뒤 다른 컴퓨터 스크린에 나타내는 것이 가능하다. 이른 바 템페스트라고 불리는 기법이다. 실제로 미 연방수사국(FBI)이 중앙정보국(CIA) 요원 앤드리치 에임스(Aldrich Ames)의 간첩행위를 적발할 때 사용했다.



Tempest – example 3

breaking secrecy of the
ballot with a radio scanner

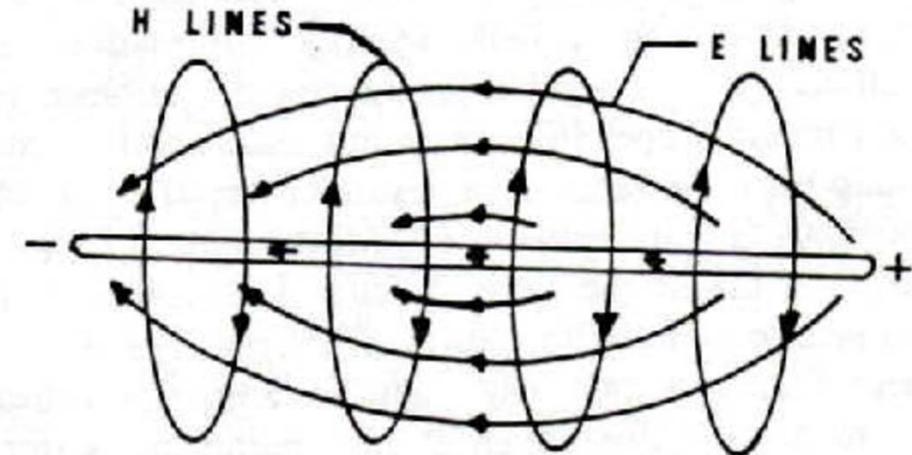
10 October 2006

Tempest – 정의

- 용어
 - 전자기 발산을 줄이기 위해 사용되는 특정 표준에 관한 code word (원래 의미)
→ 전자기파를 수신한 후 이를 재생하여 정보를 가로채는 해킹기법
- 공격 원리
 - 컴퓨터 모니터 및 기타 장치는 전자기 발산함
 - 수신기로 이러한 발산 신호를 원격지에서 수신
 - 수신된 전자기를 기록 및 재생

Tempest - 정의

- 전자기 필드 구성

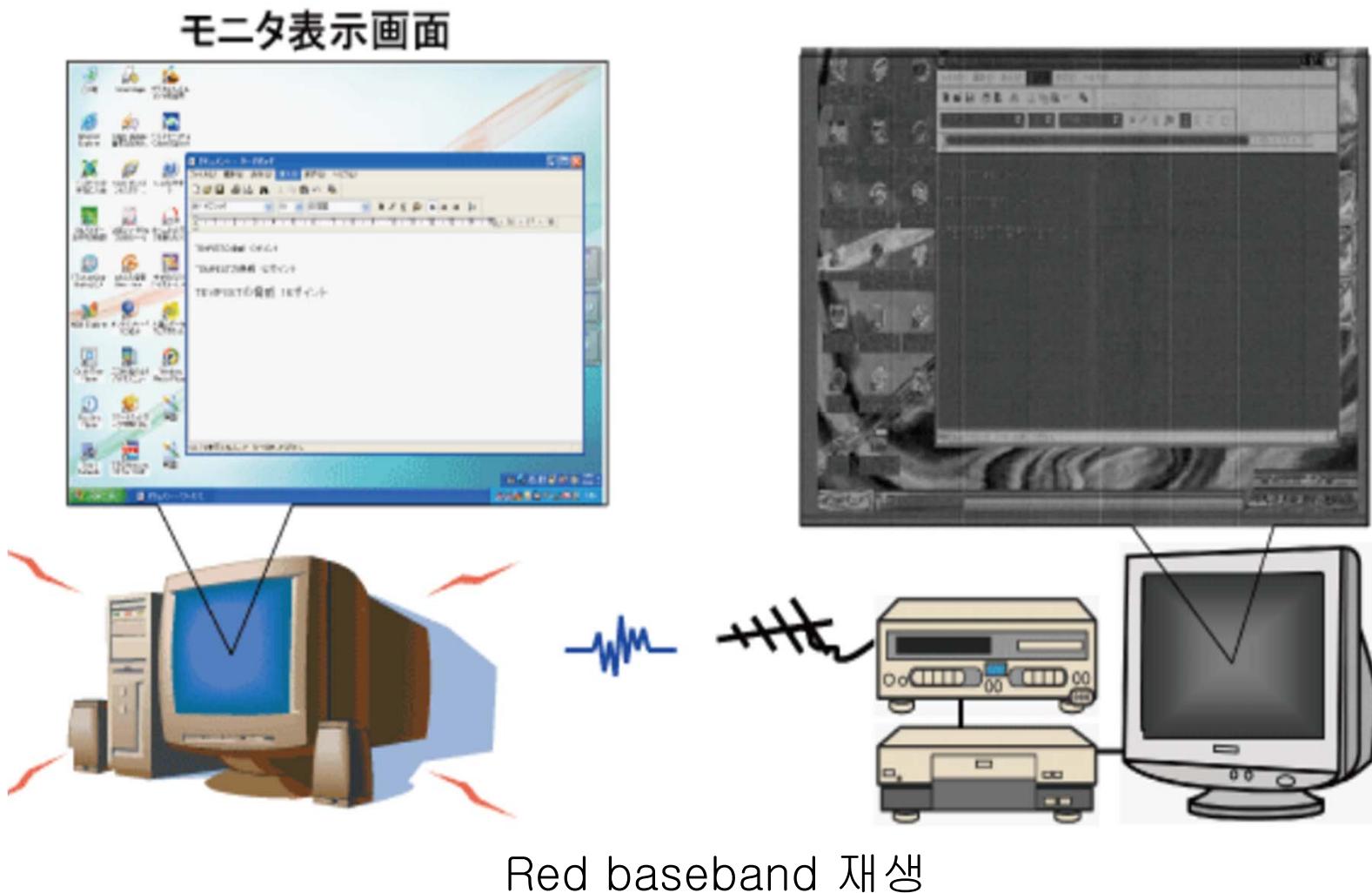


- **Tempest Three Signals**
 - RED Baseband
 - Modulated Spurious Carriers
 - Impulsive Emanations

Tempest – Red baceband

- Red Baceband
 - Red
 - 빨간색
 - Baceband
 - 기저 대역 신호
 - 변조되지 않은 원래의 정보 신호
 - 펄스의 유무(or 전압의 '+', '-')를 1과 0으로 표시
 - 가장 쉽게 알아볼 수 있는 신호

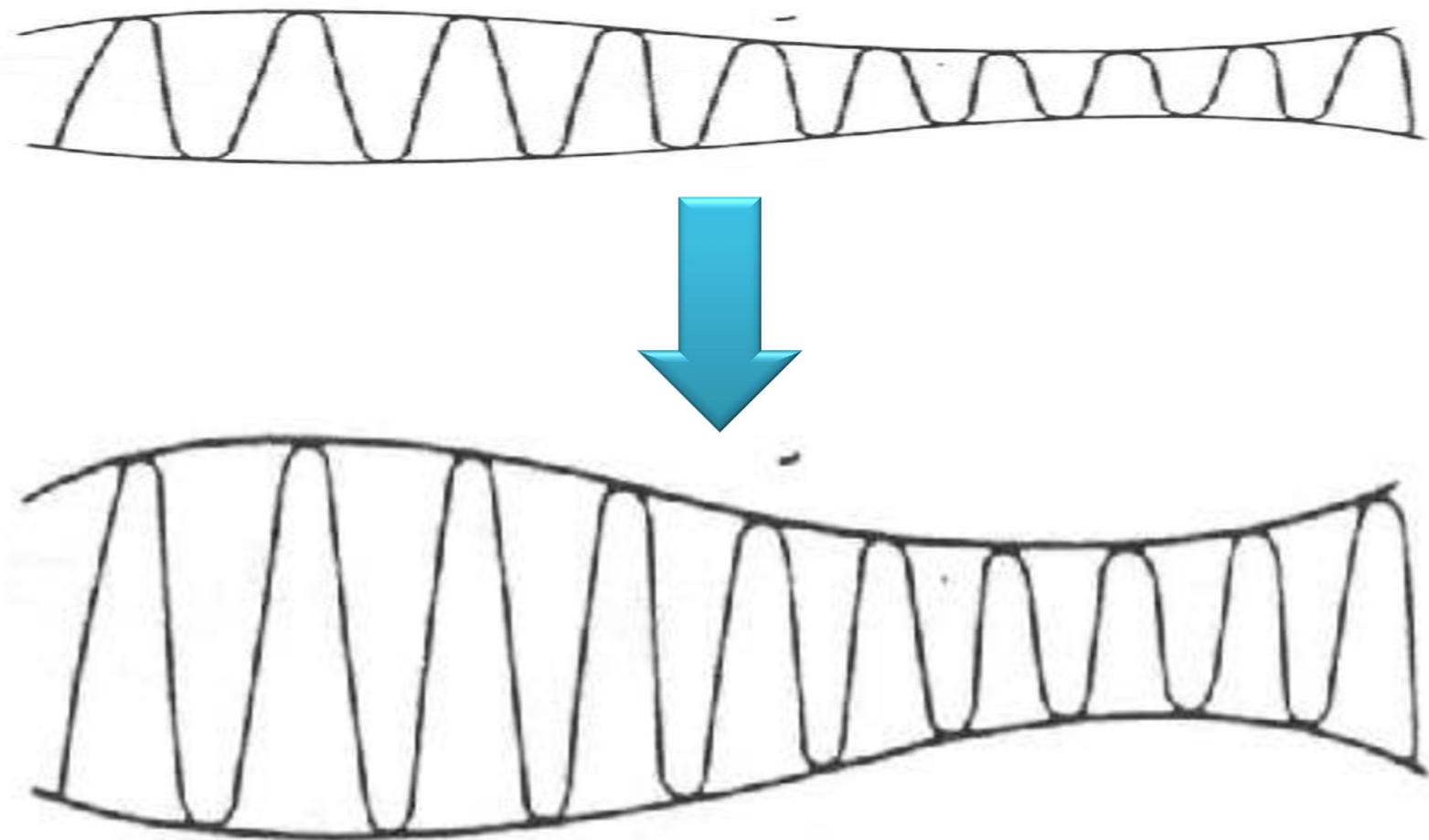
Red baseband – example



Tempest – Modulated Spurious Carriers

- **Modulated Spurious Carriers**
 - RED data에 의한 신호를 변조하여 생성
 - 진폭 변조(AM)
 - 주파수 변조(FM)
 - 위상 변조(PM)
 - 데이터를 용도에 맞게 사용하기 위해 변조
(전송거리 등)

Modulated Spurious Carriers – example



신호의 진폭을 변경

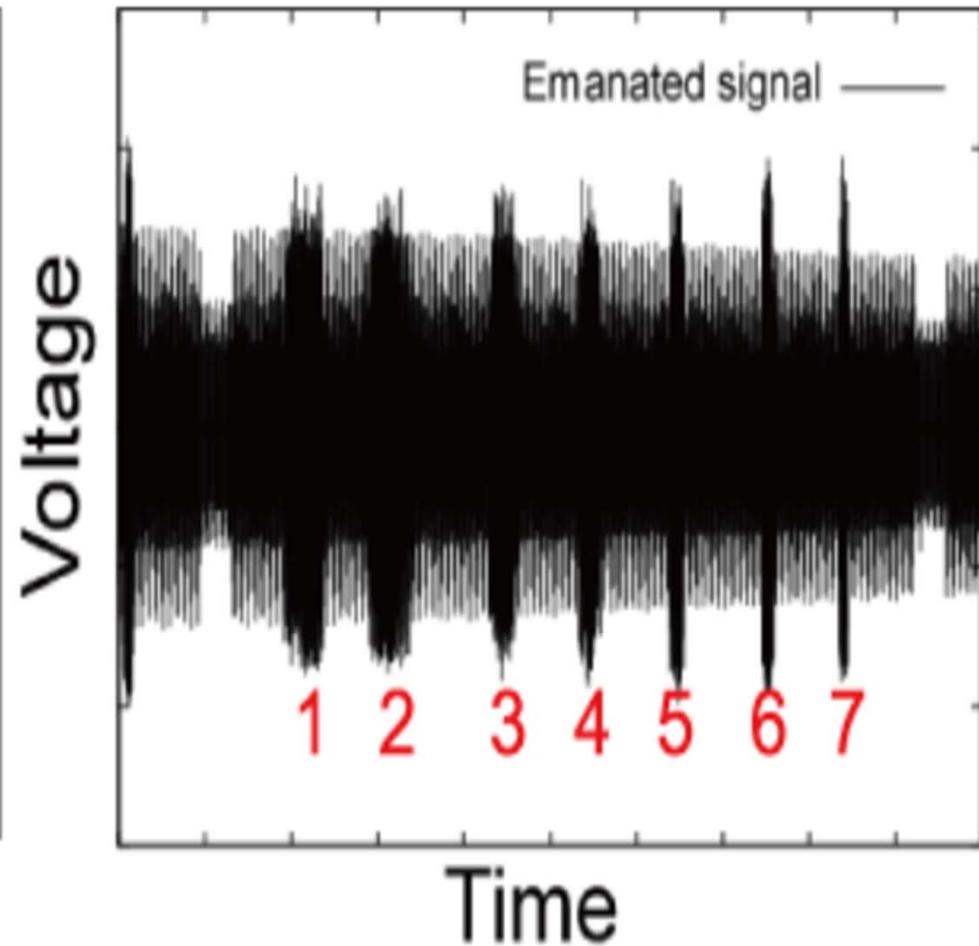
Tempest – Impulsive Emanations

- **Impulsive Emanations**
 - Mark 신호 (ex. '+', 1, etc.)
 - Space 신호 (ex. '-', 0, etc.)
(Mark, Space 신호는 통신 방식에 따라 달라짐)
 - Mark  Space 간의
매우 빠른 신호 전환으로 발생하는 신호

Impulsive Emanations – example

1	画面表示文字 認識テスト
2	36 pt たていすか qwert
3	24 pt ちとしあき asdfg
4	18 pt つぞぞひこ zxcvb
5	12 pt あなにうせ jklnç
6	10pt (未記入)
7	7pt (未記入)

モニタ表示画像



글자의 크기 or 두께에 의해 신호의 발생빈도가 다름

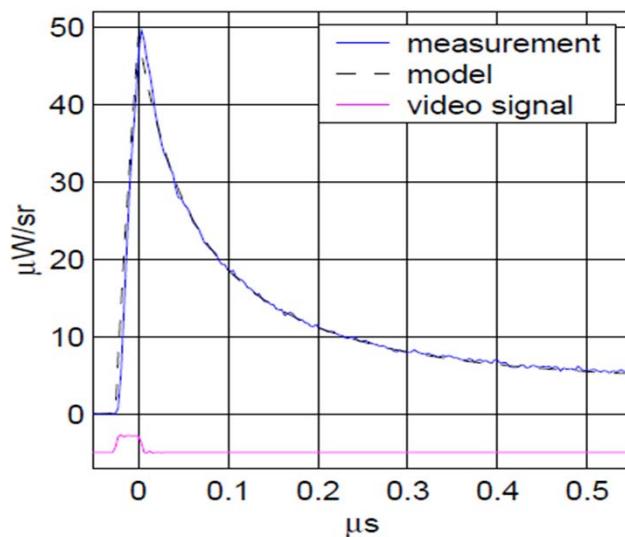
Tempest – CRT

- **CRT**
 - 전자 빔을 형광면에 도포되어 있는 형광체에 충돌시켜 그 에너지로 광을 발생
- **형광체 분석**
 - Pixel
 - RGB
 - Frequency

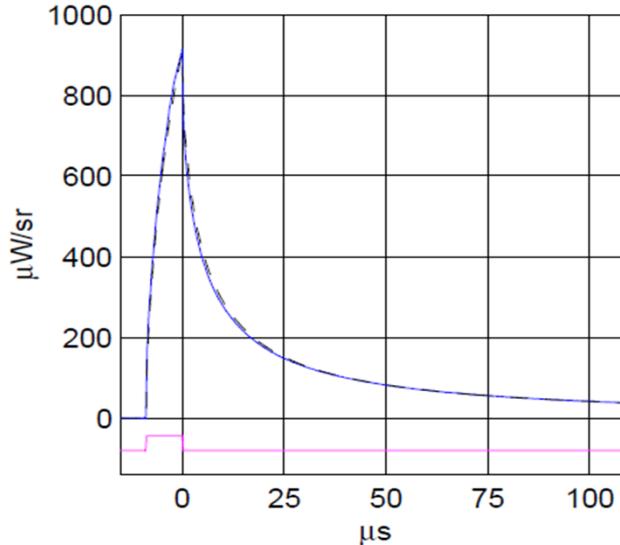
Tempest – Pixel

- 형광체 통과 곡선에 따른 pixel의 배출 감소

(a) Emission decay of a single pixel ($f_p = 36 \text{ MHz}$)



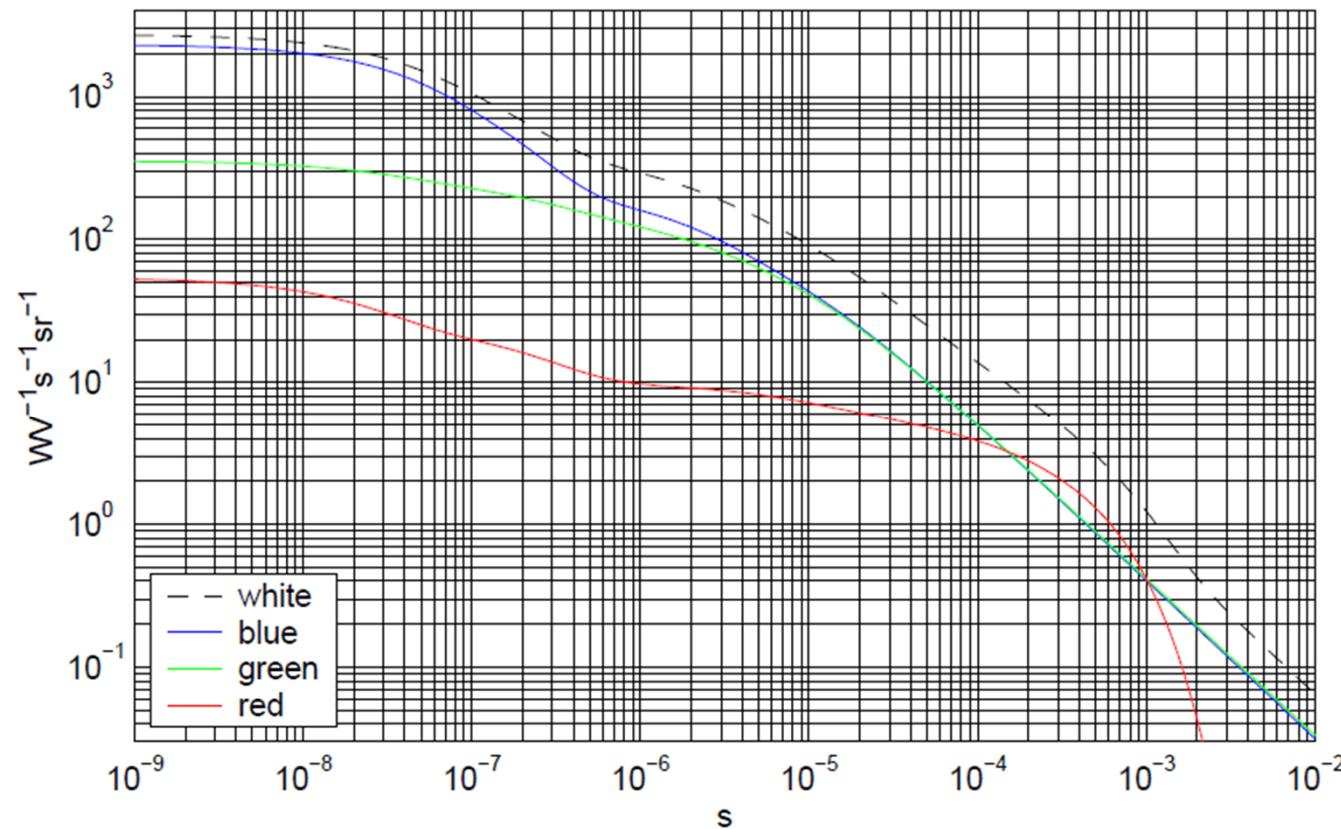
(b) Emission decay of a 320-pixel line



$$\begin{aligned} P_{P22R}(t) / \frac{\text{W}}{\text{V} \cdot \text{s} \cdot \text{sr}} = & \\ 4 \times e^{-2\pi t \times 360 \text{ Hz}} + 1.75 \times e^{-2\pi t \times 1.6 \text{ kHz}} + & \\ 2 \times e^{-2\pi t \times 8 \text{ kHz}} + 2.25 \times e^{-2\pi t \times 25 \text{ kHz}} + & \\ 15 \times e^{-2\pi t \times 700 \text{ kHz}} + 29 \times e^{-2\pi t \times 7 \text{ MHz}} & \end{aligned}$$

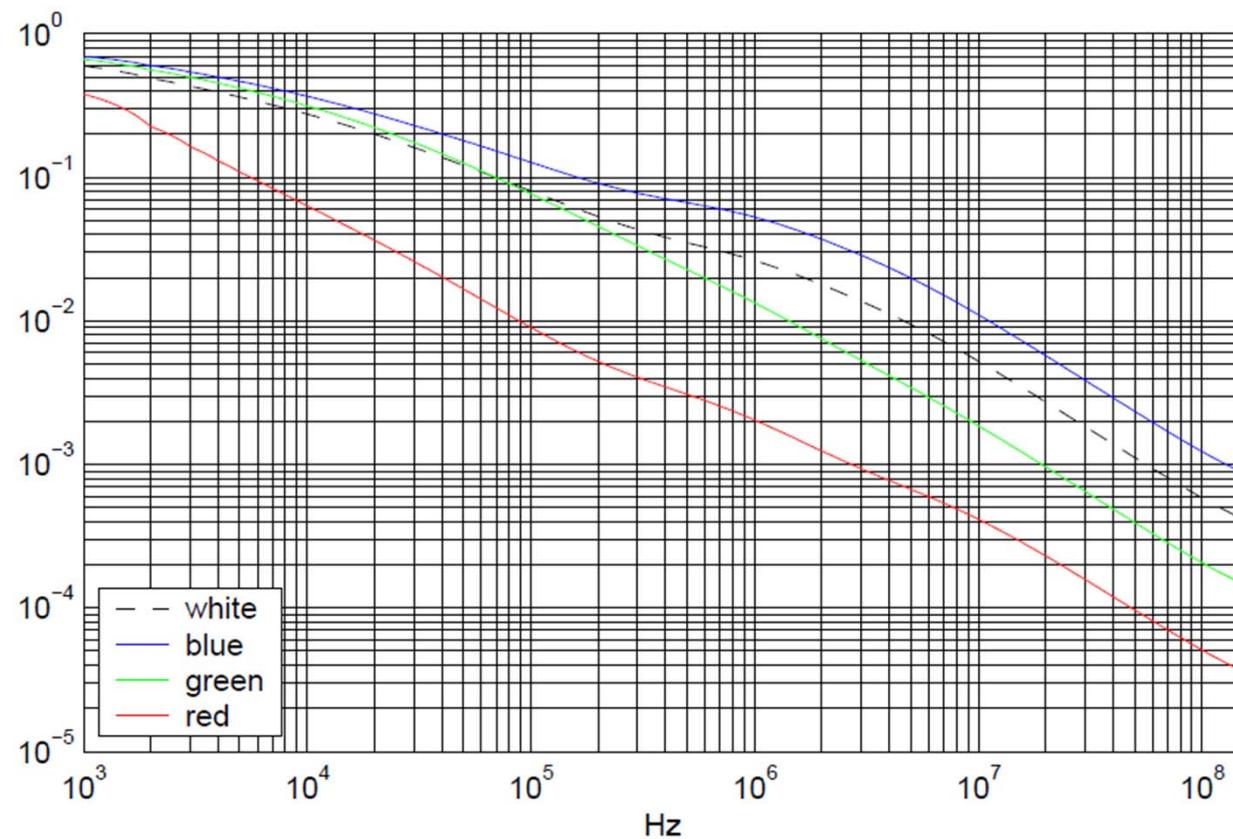
Tempest – RGB

- 형광체 통과 곡선에 따른 RGB



Tempest – Frequency

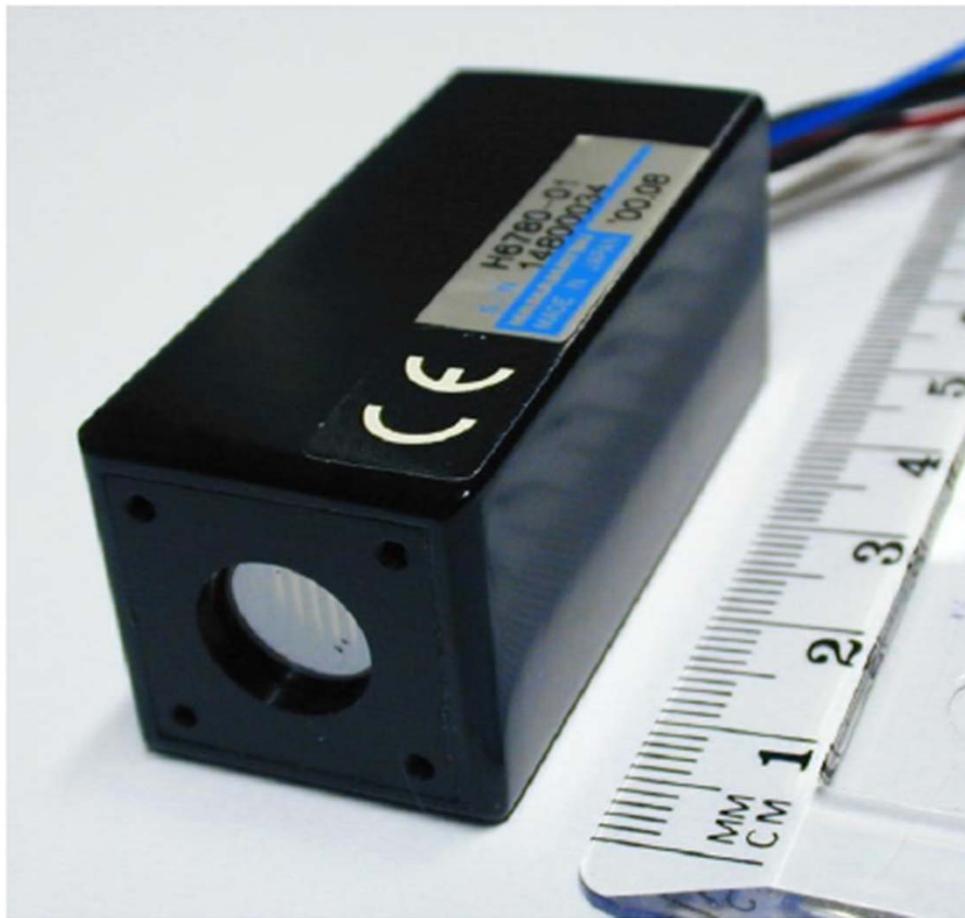
- 주파수에 따른 RGB 형광체



Tempest – Device

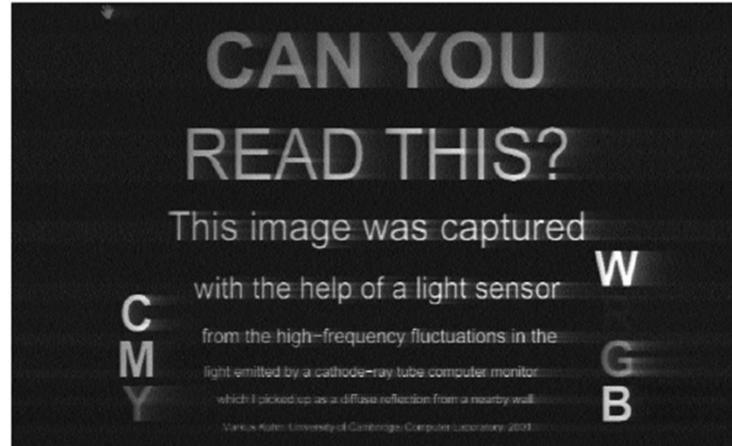
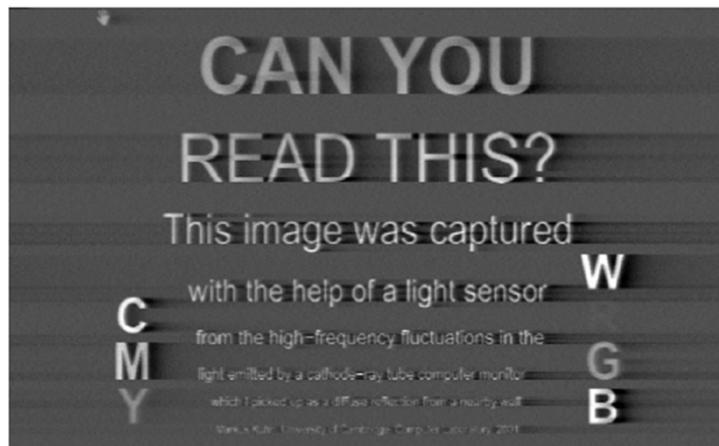
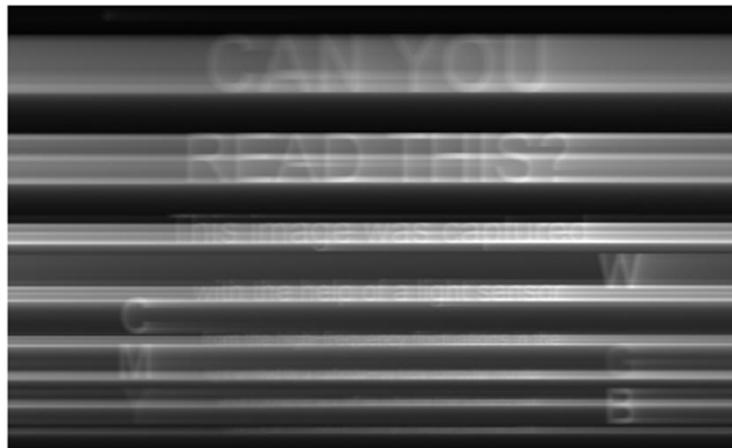
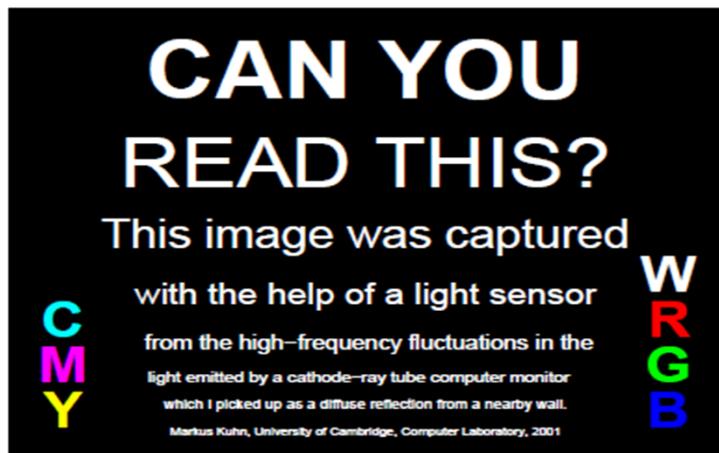
- **CRT Tempest Device**
 - Pixel 수에 따른 형광체 봉괴곡선 고려
 - 한 라인당 Pixel 수
 - 해상도
 - RGB에 따른 형광체 봉괴곡선 고려
 - 주파수에 따른 RGB 형광체 값 고려
 - Pixel Clock

Device – example



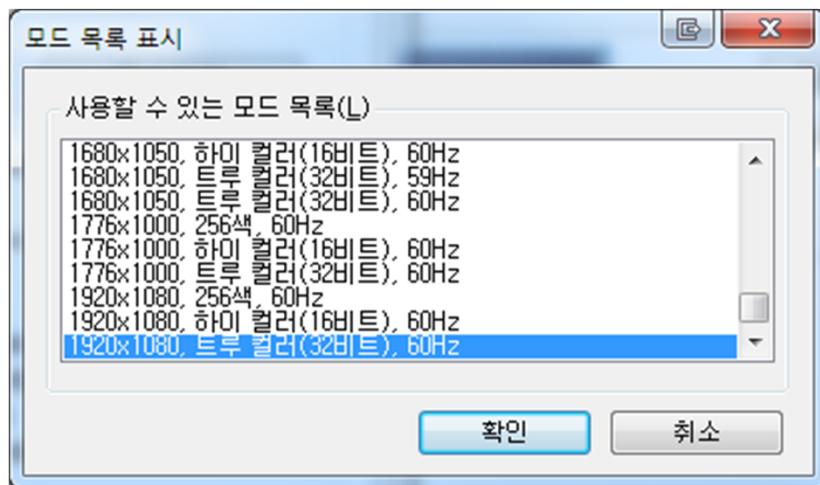
CRT Tempest 장비

Tempest – Progress



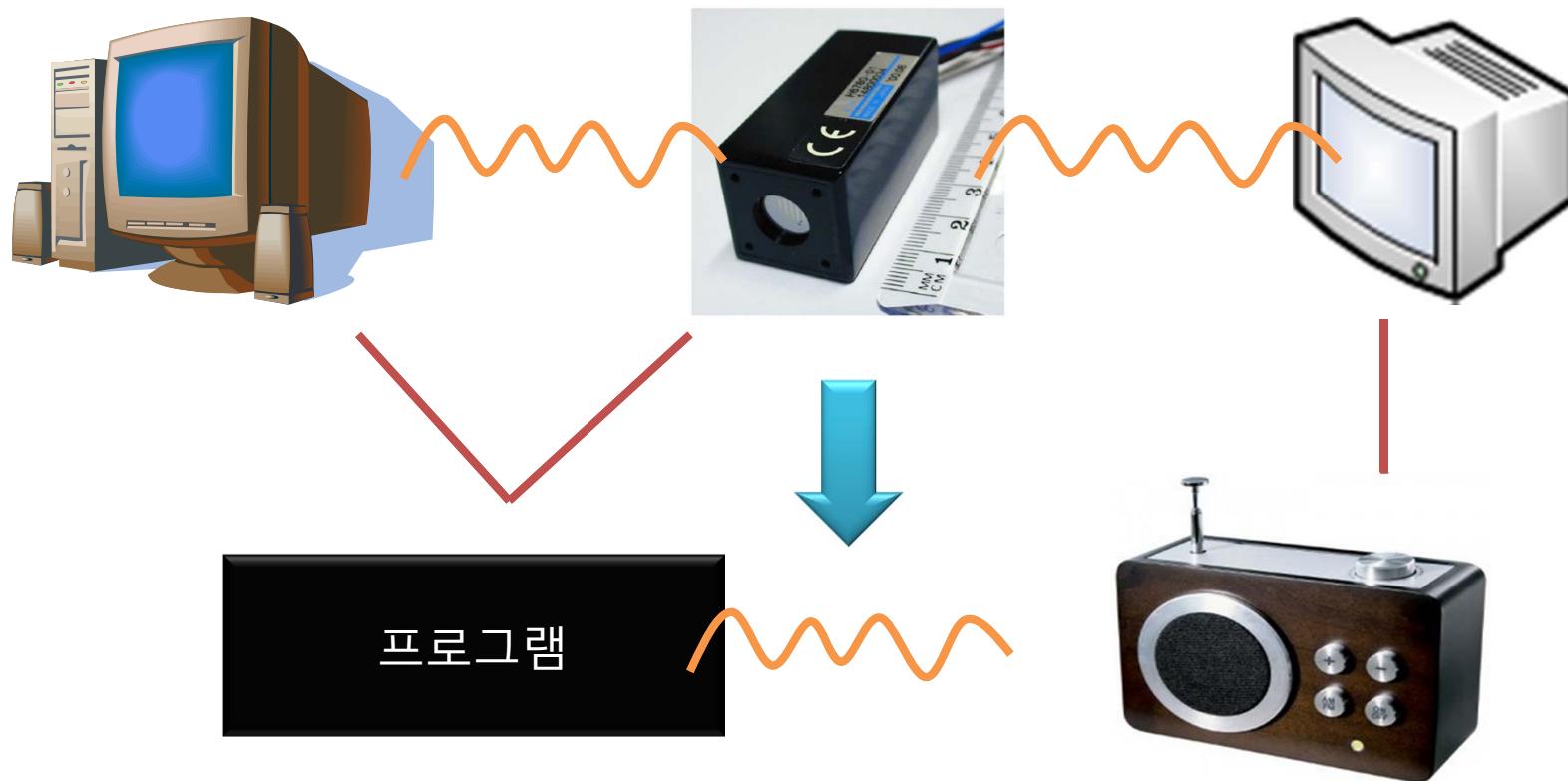
Tempest – CRT Tempest Attack

- CRT Tempest Attack 고려할 점
 - 해상도
 - 픽셀 수
 - Pixel Clock
 - 정보를 모니터로 어떤 속도로 내보낼지 결정



시연 - 구성

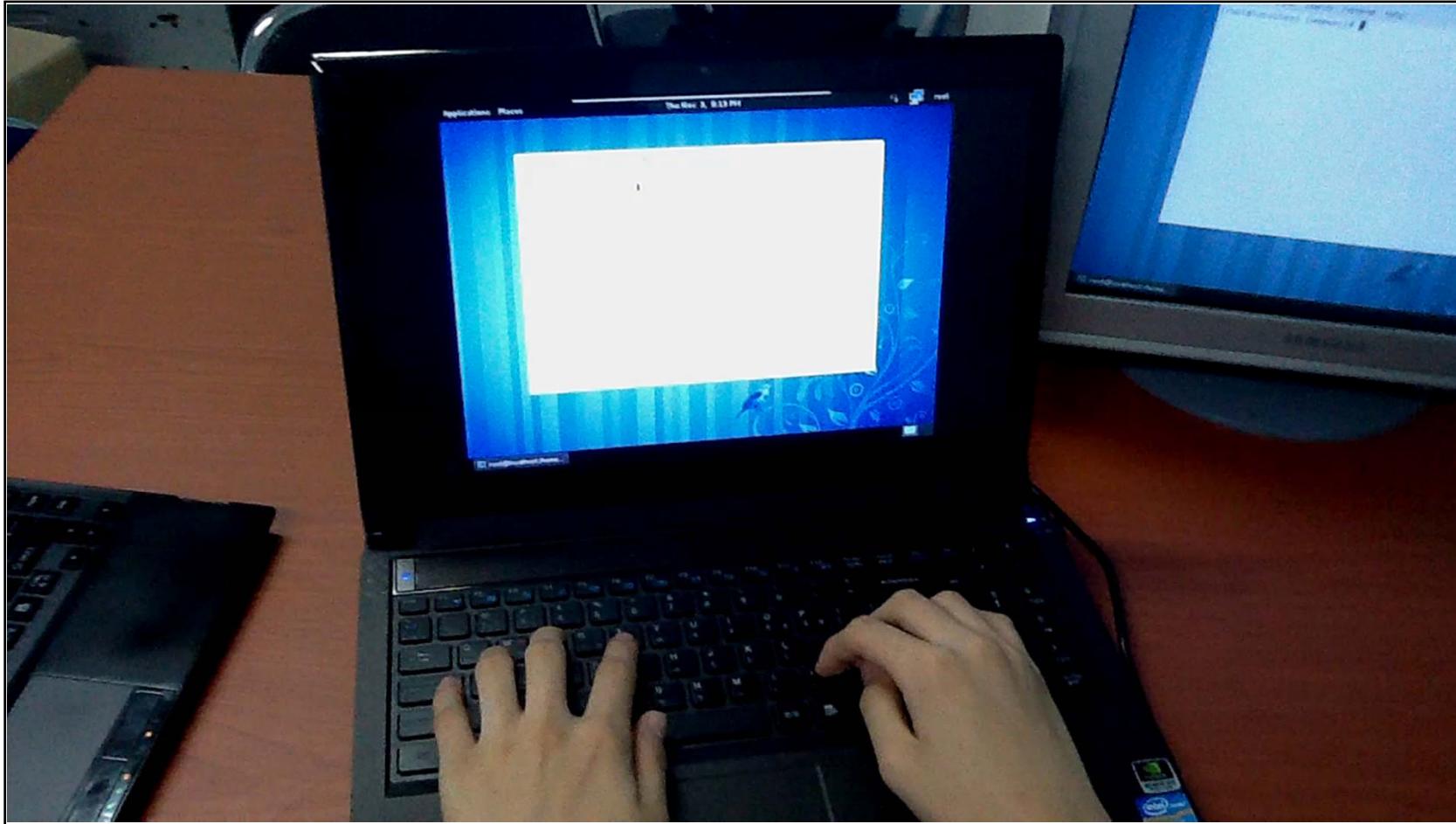
- 환경



시연 – 설명

- **프로그램의 역할(수신했다고 가정)**
 - 모니터에서 전자기파 발산 (CRT)
 - 발산된 전자기파를 수신 (Tempest Device)
 - 수신한 전자기파를 라디오 신호로 전파
- **라디오의 역할**
 - 재생된 라디오 신호를 받아 재생

시연



./tempest_for_eliza PixelClock 해상도 픽셀수(1 line) 라디오주파수 곡명 25

대응방안

- 건물 내부를 구리로 감싸 전파가 외부로 세어나가지 못하도록 보호
- 방사되는 전자기를 도청하지 못하도록 특수 제작된 컴퓨터, 모니터, 키보드, 마우스 등 전자기기를 사용

참조

- **Optical Time–Domain Eavesdropping Risks of CRT Displays**
 - Markus G. Kuhn
 - *University of Cambridge, Computer Laboratory*
 - mgk25@cl.cam.ac.uk
- **The Complete, Unofficial TEMPEST Information Page**
 - www.eskimo.com/~joelm/