Security : Forensic Signal Analysis

Video eavesdropping- RF

Y.K. Roland Tai

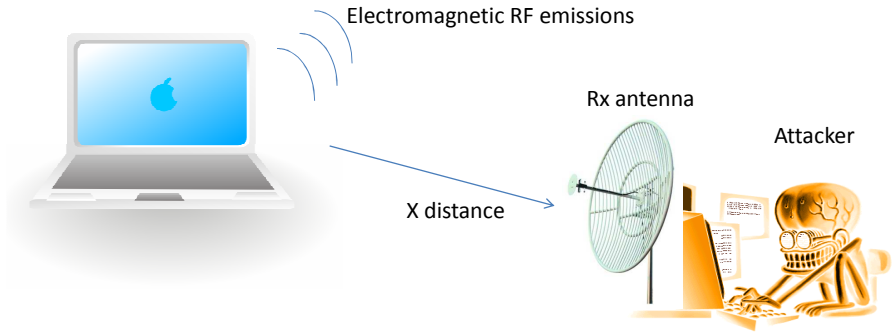
UNIVERSITY OF CAMBRIDGE

1. Introduction
2. History of TEMPEST
3. Type of RF leakages
4. Counter-measures.
5. Experiment & Demo

UNIVERSITY OF CAMBRIDGE

Phenomenon of video eavesdropping

1. All electronics equipment emit RF emissions
2. Classified information may ride onto these emission and be rebroadcasted.



Security : Forensic Signal Analysis: MPHIL ACS 2009

History

- MI5 used in the late 1950s compromising emanations of French and Russian embassy equipment in London for counter-intelligence operations
- First civilian discussion in the early 1980s; public awareness of VDU emanation threats after van Eck paper in 1985
- Further studies in 1990 by Smulders on RS-232 cables and Möller on VDUs
- US "Tempest" programme started in the late 1950s to study the problem and to define anti-emanation test procedures and standards
- All Tempest standards such as NACSIM 5100A (US) and AMSG 720B (NATO) are still classified and conforming equipment is export controlled
- Civilian EMI and safety standards (ISO/IEC, MPR, TCO) are not applicable
- Over 50 vendors supply multi-billion US$ market, practically exclusively military, diplomatic and government agency customers

* Information extracted from paper Soft Tempest: Hidden data Transmission Using Electromagnetic emanations.

UNIVERSITY OF CAMBRIDGE

Prying eyes on your PC secrets

By B. Sreejan

Kochi, Dec 29: Don't be under the misconception that the highly confidential document you are preparing at the iron-walled office cabin or the controversial video sleaze you are gleefully watching are as safe and secure as your soul.

Unless you have a radiation-proof monitor, all these data can be hacked by any tech-wiz, using a small antennae and by positioning himself within a specific range of one or two kilometers.

The academic project submitted by four engineering students of the Kasargod LBS Engineering College has become 'the talk' among technocrats. Abdulla Hisham, Arvind G.S., Viswajith A and Unnikrishnan Koroth, Semester 7, Electronics & Telecommunication students have surprised their teachers with their project, UVAH (Universal Video Display Authentic Hacking box), which would enable them to eavesdrop on any computer or television monitor that emit electronic or electromagnetic radiation.

Unnikrishnan Koroth, Abdulla Hisham, Viswajith.A and Aravind G.S.

By virtue of the uniqueness of their project and its amazing conclusion, the teachers awarded 98 percent marks for the project, which is a record in the college scrolls. Three of the four whiz kids have already secured placements in Infosys and IBS.

The students, who were motivated by the idea 'Van eck phreaking', imported an antenna from the US and assembled the hacking unit. Dr Markus Kuhn of Cambridge University also helped them to complete the project.

With their miniature project, they could collect data from the radiations emitted by PC monitors within 10-metre radius and reproduce it on their own monitor in a matter of seconds.

The idea of 'Van eck phreaking' originated decades ago. Spy instruments are made in the US, based on this concept. But the sale of which is strictly restricted inside the country.

■ Engg whiz kids develop a hacking device, P 5

http://img393.imageshack.us/i/b28ck.jpg/

UNIVERSITY OF CAMBRIDGE

Passive Attack

Attacks use available electromagnetic RF signal.

1. Leakage through **conduction**. E.g Pipes, signal cables. (Near field coupling)

2. Leakage through **RF** signal.(Far field radiation)

UNIVERSITY OF CAMBRIDGE

Leakage Through RF

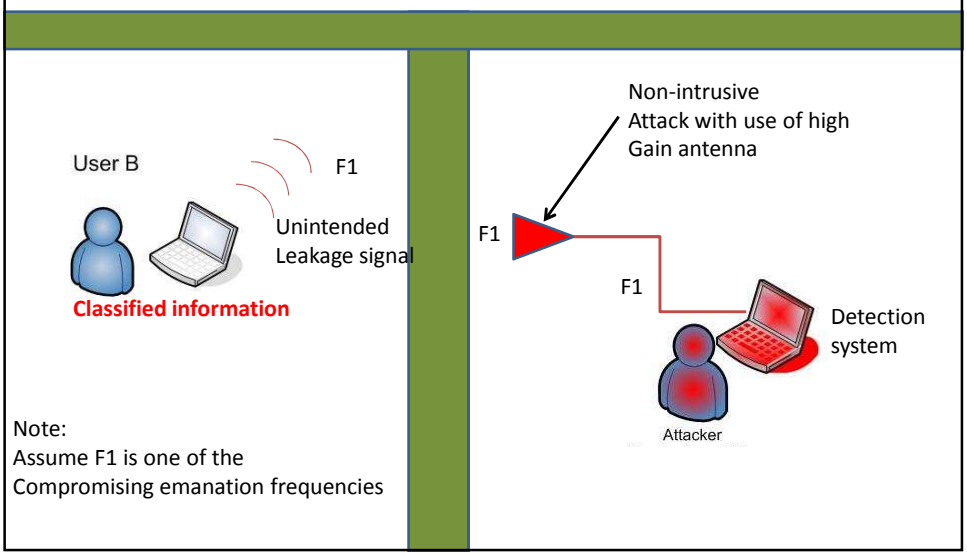
All monitors emit weak TV signal

1. UHF or VHF radio modulated with distorted version of displayed image
2. Emissions can be reconstructed using a good broadband receiver
3. LCD monitors are also vulnerable
4. Serial cable (acts as radiating antenna) from LCD carries video signal

UNIVERSITY OF CAMBRIDGE

3. Leakage through RF (Direct radiation leakage)

Typical Attack scenario

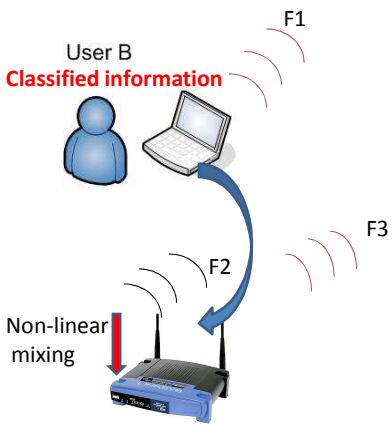


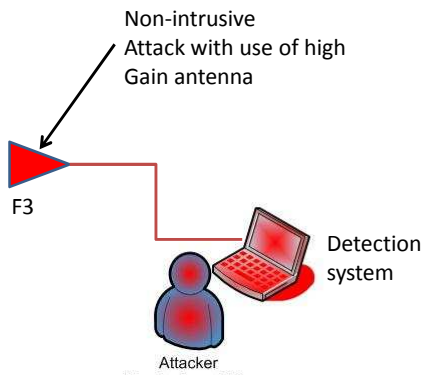
Note:
Assume F1 is one of the Compromising emanation frequencies

UNIVERSITY OF CAMBRIDGE

4. Leakage through RF

(Non-linear intermodulation radiation leakage)





Where F3 is the intermod frequency.
F3= F2+F1 or F3 = F2-F1

UNIVERSITY OF CAMBRIDGE

Leakage Through Conduction

1. **Equipment based**
- fax
- Ethernet cables
- RS-232

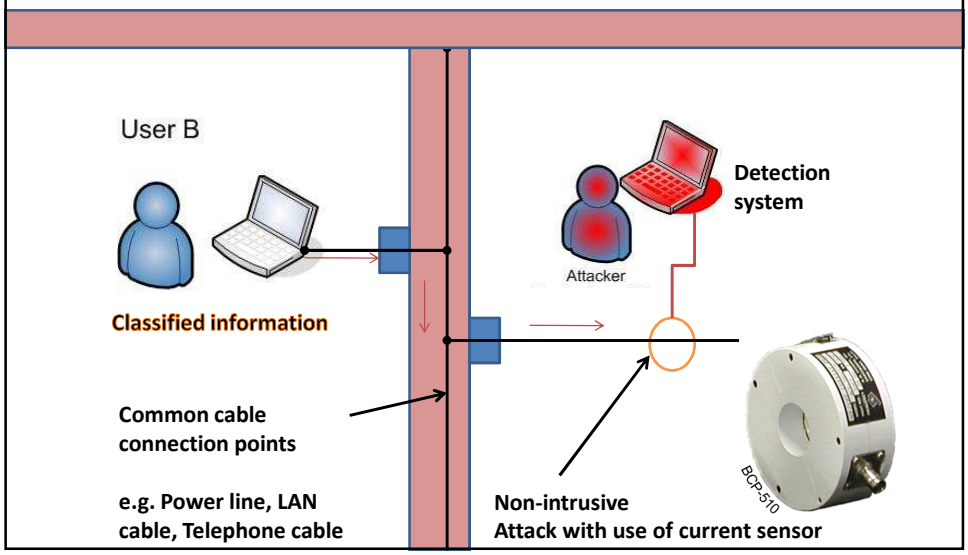
2. **Infrastructure based (Buildings)**

1. Power cables
2. Telephone lines
3. Metallic piping

UNIVERSITY OF CAMBRIDGE

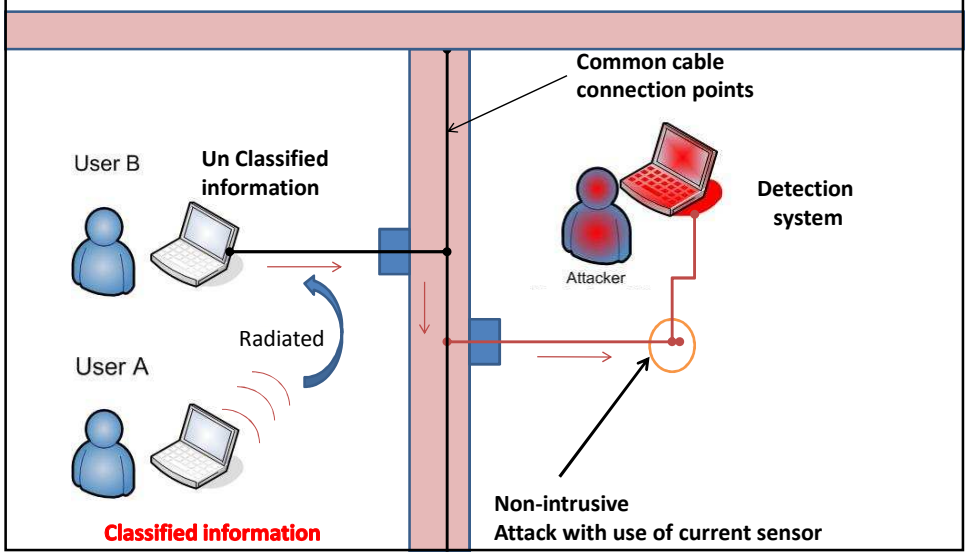
1. Leakage through conduction
(Direct conduction leakage)

Typical Attack scenario



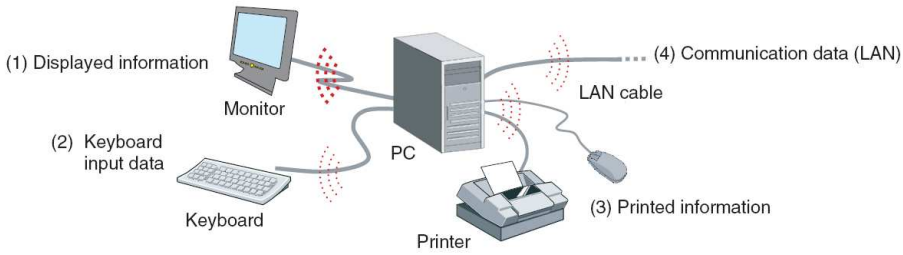
UNIVERSITY OF CAMBRIDGE

2. Leakage through conduction
(Radiated conduction leakage)



UNIVERSITY OF CAMBRIDGE

Vulnerability levels of Computer equipment



Information hidden in leaking emissions	Importance and quantity of the information	Difficulty of regenerating original information	Strength of emissions	Total threat of information leakage
(1) Displayed information	High (displayed information)	Easy	Strong	High
(2) Keyboard input data	Low to medium (only text)	Hard (need to decipher code assigned to each key)	Weak	Low to medium
(3) Printed information	Low (only printed information)	Hard (need to demodulate printer interface signal)	Weak	Low
(4) Communication data	Medium to high (communicated information)	Hard (need to demodulate LAN interface signal)	Weak	Medium

Note: Quote from paper: Countermeasures to Prevent Eavesdropping on Unintentional Emanations from Personal Computers

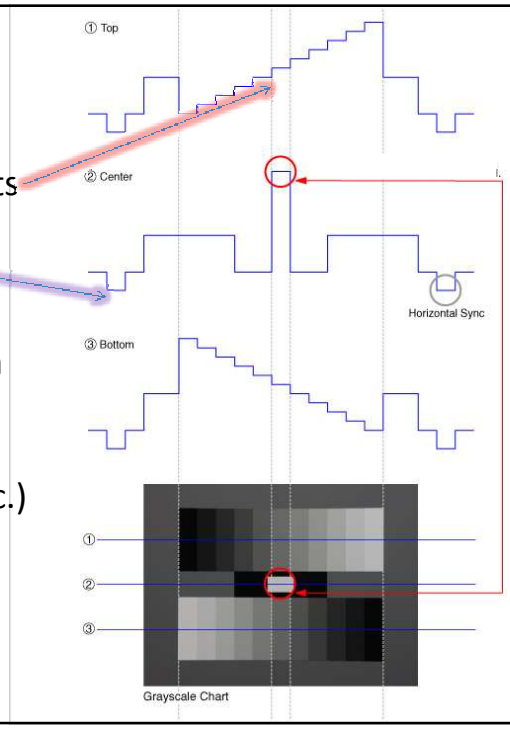
UNIVERSITY OF CAMBRIDGE

Video timing

1. Actual video contents

2. H-Sync pulses
(48kHz, 80kHz etc)
One line of information

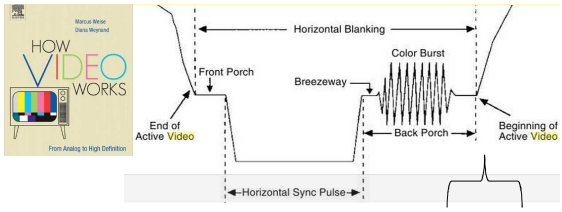
3. Vertical sync pulses
(60Hz, 75Hz, 100Hz etc.)
Entire frame



UNIVERSITY OF CAMBRIDGE

Video timing of Display monitor

Blanking pulses
Front porch
Back porch



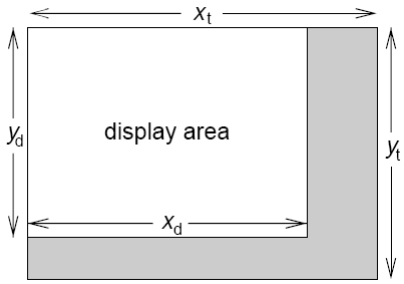
* Pixel frequency: f_p

Deflection frequencies:

$$f_h = \frac{f_p}{x_t}, \quad f_v = \frac{f_p}{x_t \cdot y_t}$$

Pixel refresh time:

$$t = \frac{x}{f_p} + \frac{y}{f_h} + \frac{n}{f_v}$$

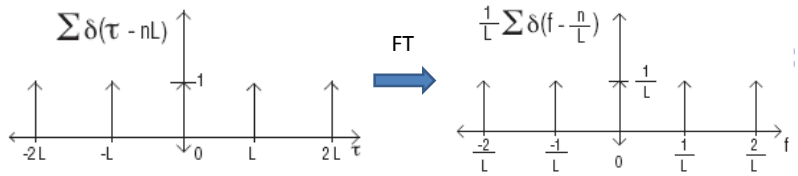


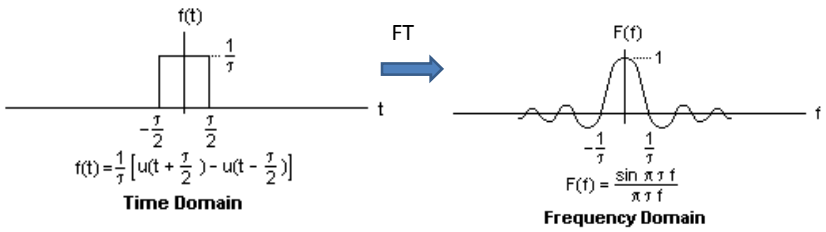
*Extracted : presentation slides "Electromagnetic eavesdropping on computers", Markus Kuhn

UNIVERSITY OF CAMBRIDGE

Series of Equidistant Dirac

Series of Equidistant Dirac with reciprocal distance



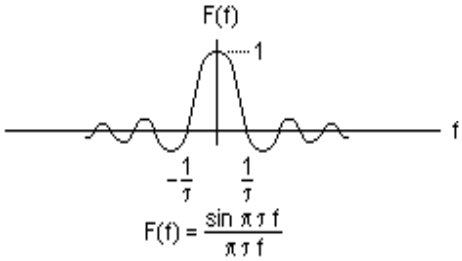


Single pixel
Rectangular pulse

Sinc function

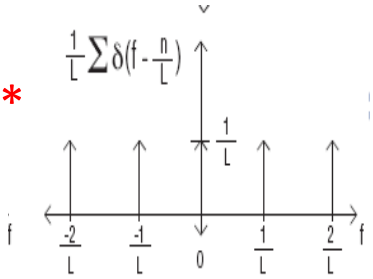
UNIVERSITY OF CAMBRIDGE

Video pixel information



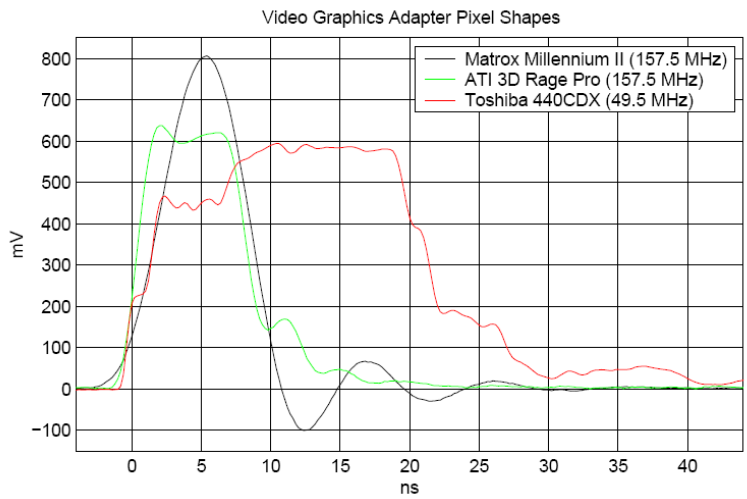
*

Sampling at rate of *fp*



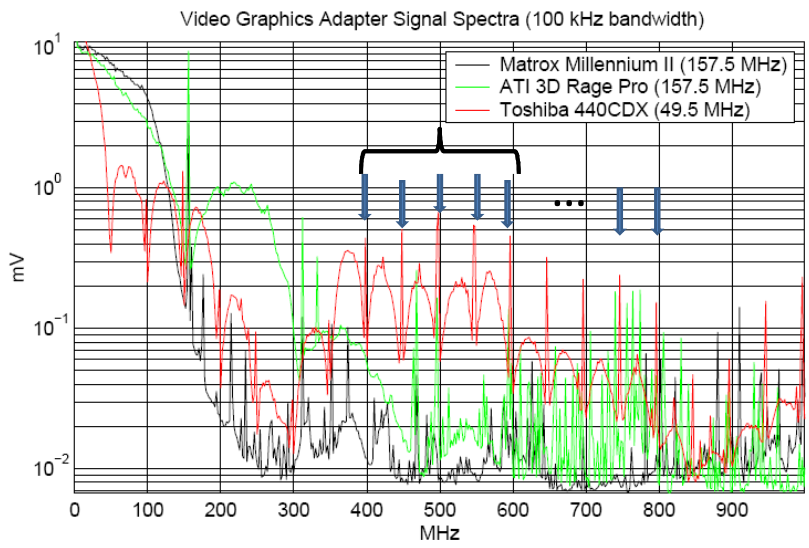
Samples of video information appearing across the entire spectrum **<u>at very *fp* frequency</u>**.

UNIVERSITY OF CAMBRIDGE



*Extracted : presentation slides "Electromagnetic eavesdropping on computers", Markus Kuhn

UNIVERSITY OF CAMBRIDGE

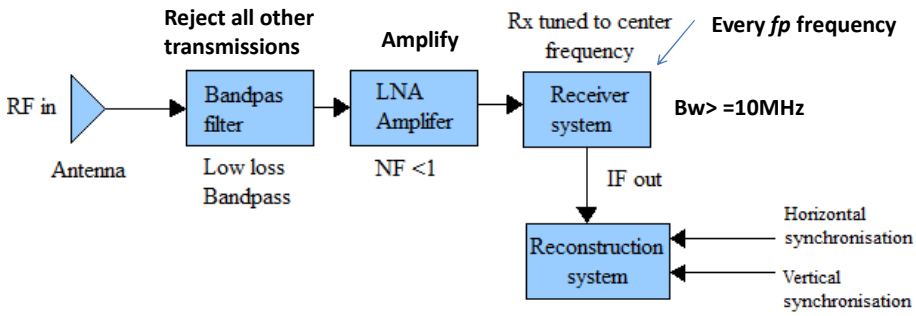


*Extracted : presentation slides "Electromagnetic eavesdropping on computers", Markus Kuhn

UNIVERSITY OF CAMBRIDGE

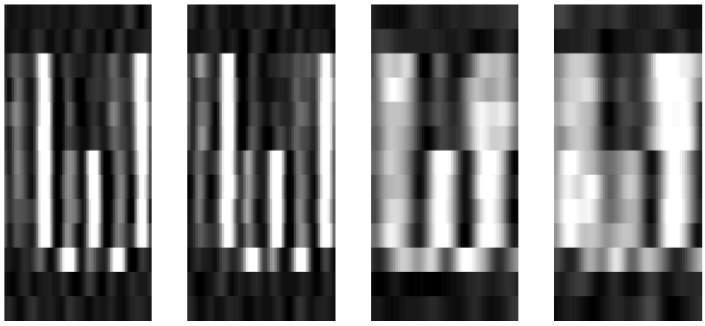
Video Detection System

1. Receive antenna
2. Receiver of at least 10MHz



UNIVERSITY OF CAMBRIDGE

- Trade off between image reconstruct quality with receiver Bandwidth.
- Higher bandwidth will have higher noise level.

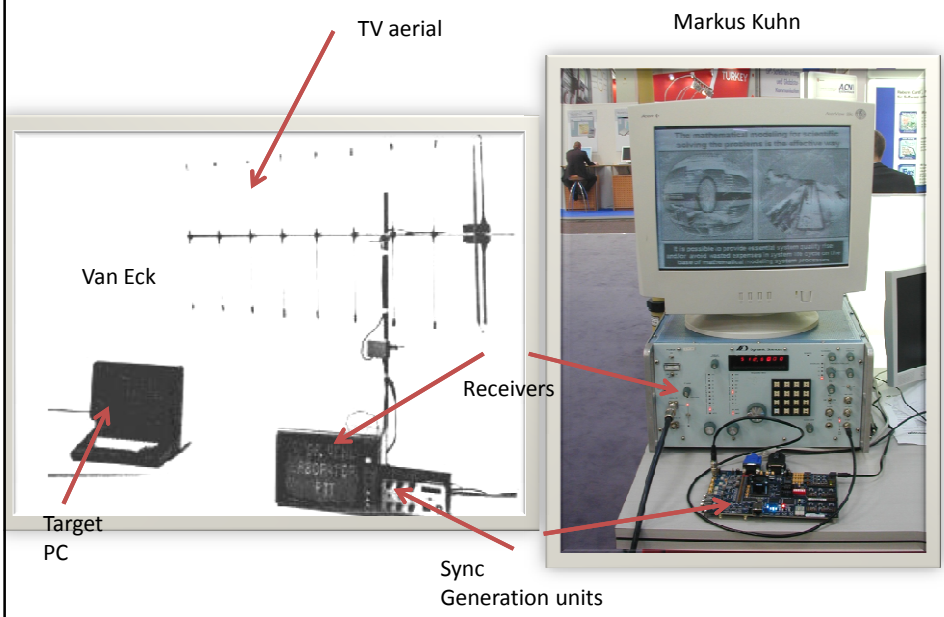


200 MHz BW 50 MHz BW

*Electromagnetic eavesdropping on computers, Markus Kuhn

UNIVERSITY OF CAMBRIDGE

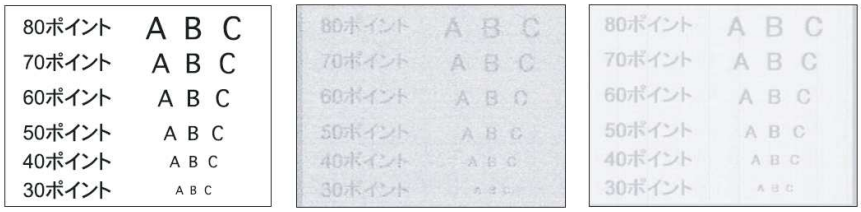
Detection System built in the past



UNIVERSITY OF CAMBRIDGE

Actual Detection System

- Detection is a challenge in the fully occupied radio spectrum.
- Random noise from the external environment.
- Requires at least S/N ratio of 10dB.
- Periodic averaging to improve S/N of the video image

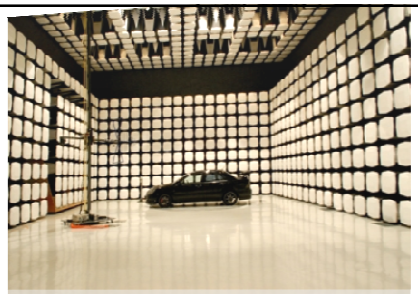


(a) Original display image on PC monitor (b) Image reconstructed from emanations (not averaged) (c) Image reconstructed from emanations (average of 32 frames)

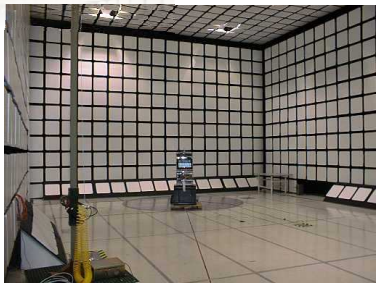
http://www.youtube.com/watch?v=YcTM0dqVz14&feature=related

UNIVERSITY OF CAMBRIDGE

Semi-Anechoic chamber to provide a clean spectrum for detailed analysis Measurement of TEMPEST signals



EMRL chamber in NTU 10m 9kHz to 18GHz



UNIVERSITY OF CAMBRIDGE

Effective radiator

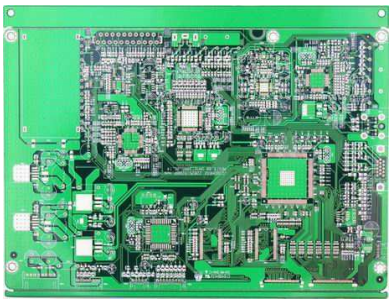
Every traces on the PCB carries current.

The amount of radiation depends:-

1.Speed of transitions

2. The length of the traces.

e.g. for 30MHz the length must be at least 2.5m for it to emit effectively.



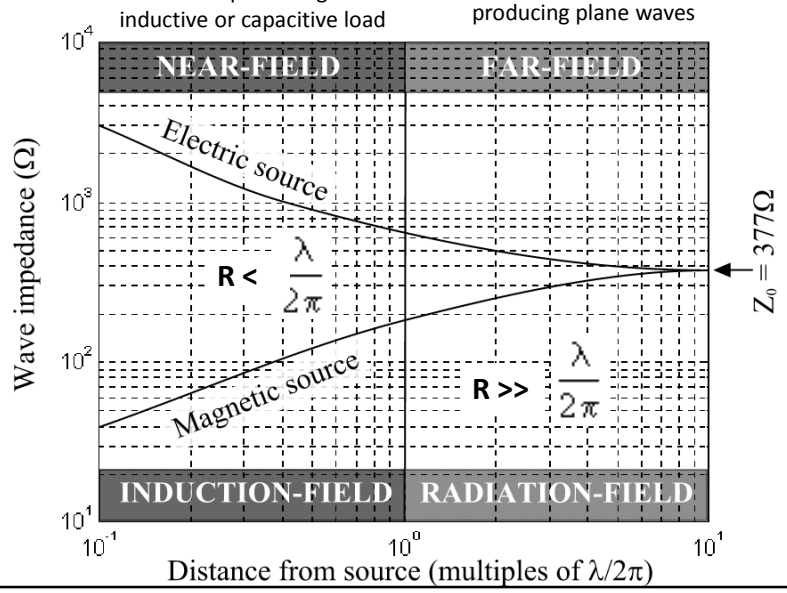
$$\lambda = \frac{c}{f}$$

Where :
c = speed of light
f= frequency
λ = lamda

UNIVERSITY OF CAMBRIDGE

The *E* and the *H* fields are not in phase and orthogonal to each other producing inductive or capacitive load

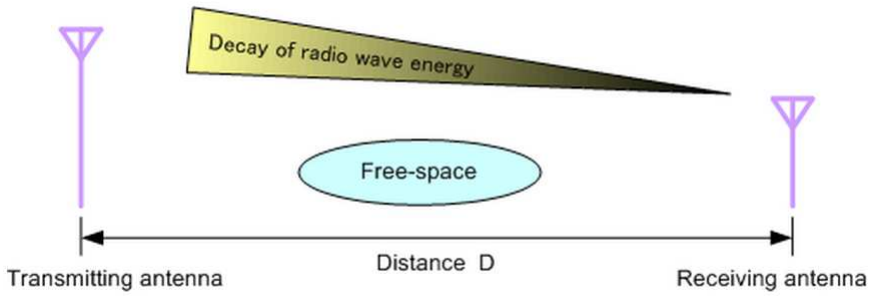
The *E* and the *H* fields will then be in phase and orthogonal to each other producing plane waves



UNIVERSITY OF CAMBRIDGE

RF attenuation over distance

Calculation of free space basic propagation loss



Attenuation of electric field intensity in free-space

1/r

UNIVERSITY OF CAMBRIDGE

RF attenuation over distance

$$\boxed{\begin{aligned}\mathrm{FSPL} &= \left(\frac{4\pi d}{\lambda}\right)^2 \\ &= \left(\frac{4\pi df}{c}\right)^2\end{aligned}}$$

$$\begin{aligned}\mathrm{FSPL(dB)} &= 10\log_{10}\left(\left(\frac{4\pi}{c}df\right)^2\right) \\ &= 20\log_{10}\left(\frac{4\pi}{c}df\right) \\ &= 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right) \\ &= 20\log_{10}(d) + 20\log_{10}(f) - 147.55\end{aligned}$$

Free Space Loss = 32.45 + 20log(d) + 20log(f)dB
(where d is in km and f is in MHz)

FSPL is a function of d and f

***For every twice in distance increase we will have 6dB of RF attenuation.**

UNIVERSITY OF CAMBRIDGE

Security Mitigation measures

Do we have to work inside a shielded box???

Laptop inside

Shielded fabric

Both hands inside to prevent keyboards emission

Source image from :
http://rayannelutenerblog.files.wordpress.com/2008/06/body-laptop-interface-lorax.jpg

UNIVERSITY OF CAMBRIDGE

Mitigation measures

Shielded fabric tent

Wide band jammer

Shielded PC or laptop

UNIVERSITY OF CAMBRIDGE

Mitigation measures

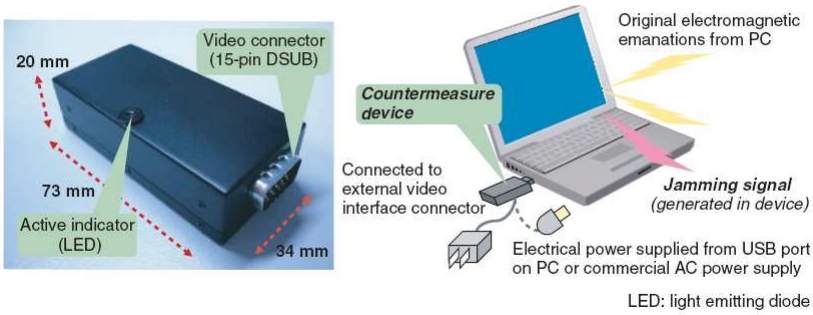
Architectural shielding

3M shielded film

UNIVERSITY OF CAMBRIDGE

Mitigation measures

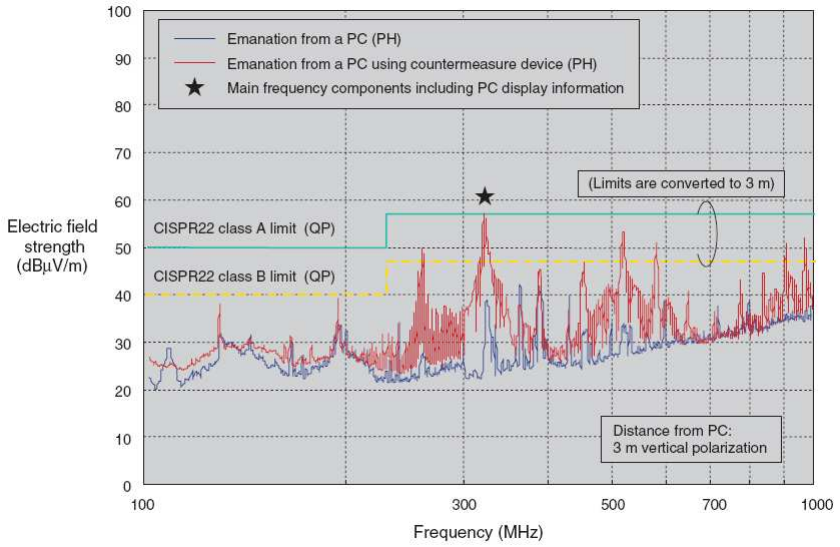
Signal Jamming ??



*Countermeasures to prevent eavesdropping on Unintentional Emanations from personal computer

UNIVERSITY OF CAMBRIDGE

Mitigation measures



UNIVERSITY OF CAMBRIDGE

Mitigation measures

Software

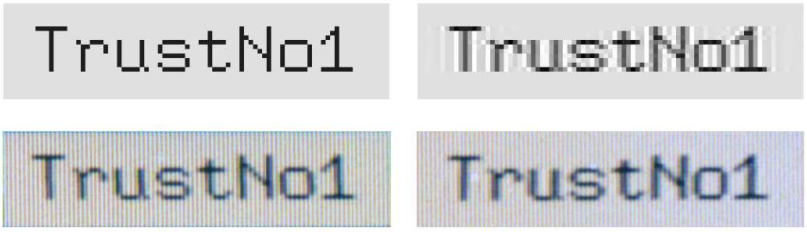
1. Soft fonts
2. Message hiding (Dithering)

UNIVERSITY OF CAMBRIDGE

Mitigation measures

1.Soft fonts (Low pass Filtering)

Markus Kuhn and Ross Anderson, University of Cambridge



Conventional fonts Filtered (30% of horizontal spectrum)

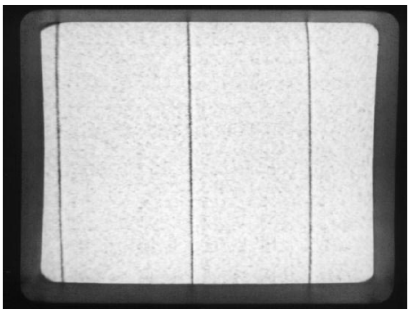
*Soft Tempest: Hidden Data Transmission
Using Electromagnetic Emanations, Markus Kuhn and Ross Anderson.
University of Cambridge

UNIVERSITY OF CAMBRIDGE

Mitigation measures

1.Soft fonts

Normal text



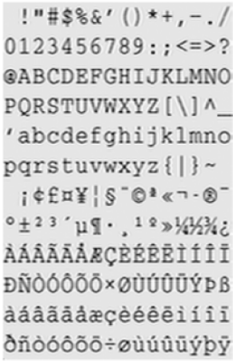
With Soft-fonts

*Soft Tempest: Hidden Data Transmission
Using Electromagnetic Emanations, Markus Kuhn and Ross Anderson.

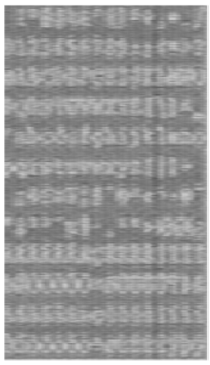
UNIVERSITY OF CAMBRIDGE

Mitigation measures

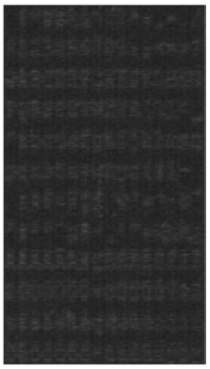
1.Soft fonts (Gaussian and Low Pass Filters)



Original Text



SONY VAIO PCG-V505 notebook



21 inch CRT NANAO FlexScan 77F

*Evaluation and Improvement of the Tempest Fonts
Hidema Tanaka, Osamu Takizawa, and Akihiro Yamamura
National Institute of Information and Communications Technology

UNIVERSITY OF CAMBRIDGE

Mitigation measures

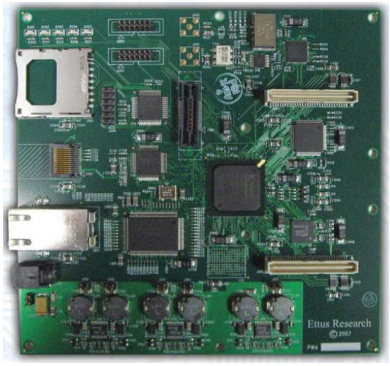
2.Message hiding (Dithering)

1. High frequency BLACK/WHITE dither pattern creates strongest signal with highest emission.

2. Constant color provide the minimize emissions

UNIVERSITY OF CAMBRIDGE

Miniaturize Detection system



Software Define Radio (SDR)

- Advancement in digital electronics

Where hardware like ADC, mixer , modulator and demodulator can be implemented in Software.

Gnuradio provides some available software .

UNIVERSITY OF CAMBRIDGE

Technical specifications

- Two 100 MS/s 14-bit analog to digital converters
- Two 400 MS/s 16-bit digital to analog converters
- Digital downconverters with programmable decimation rates
- Digital upconverters with programmable interpolation rates
- Gigabit Ethernet Interface
- 2 Gbps high-speed serial interface for expansion
- Capable of processing signals up to 100 MHz wide
- Modular architecture supports a wide variety of RF daughterboards
- Auxiliary analog and digital I/O support complex radio controls such as RSSI and AGC
- Fully coherent multi-channel systems (MIMO capable) with up to 8 antennas
- 1 Megabyte of on-board high-speed SRAM

UNIVERSITY OF CAMBRIDGE

Experiment using the ETTus USRP2

UNIVERSITY OF CAMBRIDGE

Target

IF out

Extract to Matlab

LAN Port

UNIVERSITY OF CAMBRIDGE

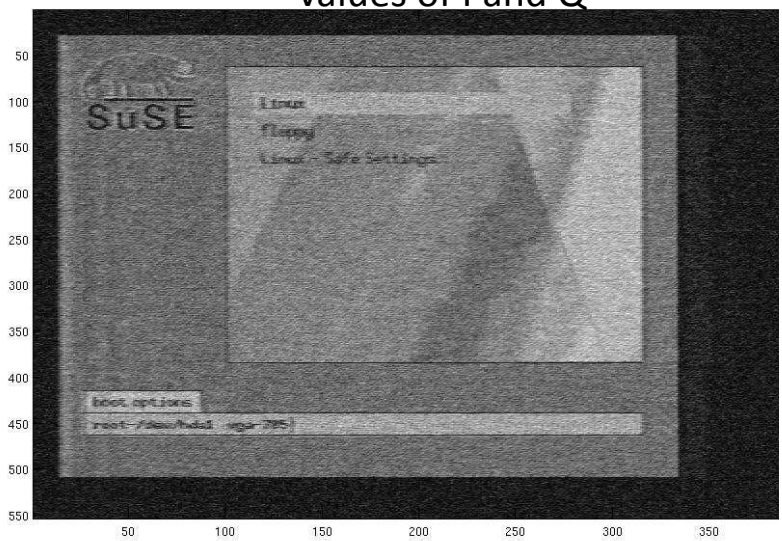
Target laptop : Toshiba CDX 440
Display resolution: 800 x 600
Xt = 1056 and yt =628

Dynamic science receiver
Center frequency = 350 MHz
Bandwidth = 20MHz

SDR was set to capture the IF output signal at frequency of 30MHz with sampling rate of about 25Msamples/sec.

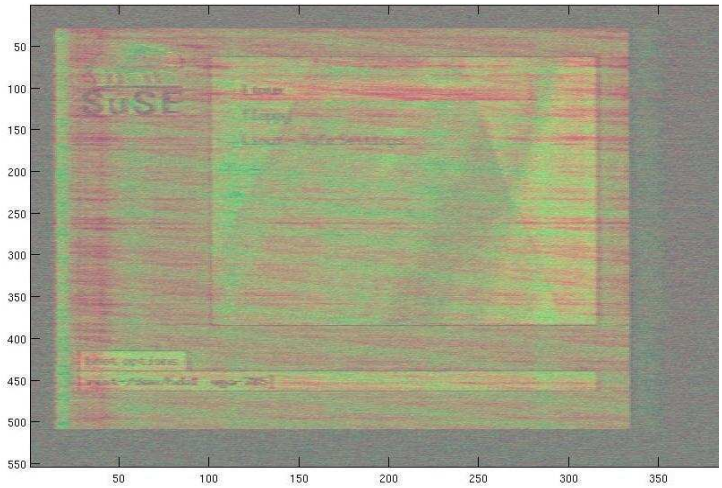
UNIVERSITY OF CAMBRIDGE

Raster the image using the absolute values of I and Q



UNIVERSITY OF CAMBRIDGE

Raster the image using the complex I and Q



UNIVERSITY OF CAMBRIDGE

DEMO