Electromagnetic eavesdropping risks of flat-panel displays

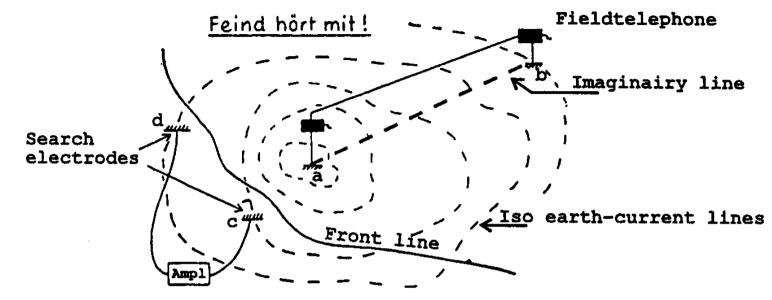
Markus G. Kuhn



Computer Laboratory

http://www.cl.cam.ac.uk/~mgk25/

Early use of compromising emanations





The German army started in 1914 to use valve amplifiers for listening into ground return signals of distant British, French and Russian field telephones across front lines [Bauer, 1999].

Military history of side-channel attacks

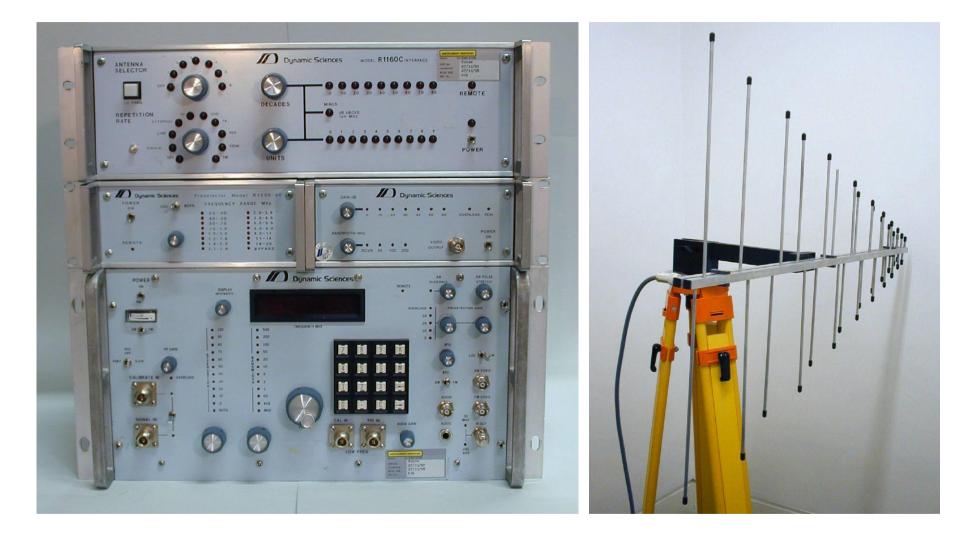
- \rightarrow 1915: WW1 ground-return current tapping of field telephones.
- → 1960: MI5/GCHQ find high-frequency plaintext crosstalk on encrypted telex cable of French embassy in London.
- → Since 1960s: Secret US government "TEMPEST" programme investigates electromagnetic eavesdropping on computer and communications equipment and defines "Compromising Emanations Laboratory Test Standards" (NACSIM 5100A, AMSG 720B, etc. still classified today).
- → Military and diplomatic computer and communication facilities in NATO countries are today protected by
 - "red/black separation"
 - shielding of devices, rooms, or entire buildings.

US market for "TEMPEST" certified equipment in 1990: over one billion dollars annually.

Open literature on compromising emanations

- \rightarrow 1985: Wim van Eck demonstrates eavesdropping on video displays with a modified TV set in BBC's "Tomorrow's World".
- → 1990: Peter Smulders investigates electromagnetic eavesdropping on RS-232 cables.
- → 1988/1991: Two Italian conferences on electromagnetic security for information protection.
- → 1998: We demonstrate steganographic forms of compromising video emanations.
- → 1999: Paul Kocher et al. demonstrate reconstruction of DES keys from power supply fluctuations in smartcard microcontrollers.

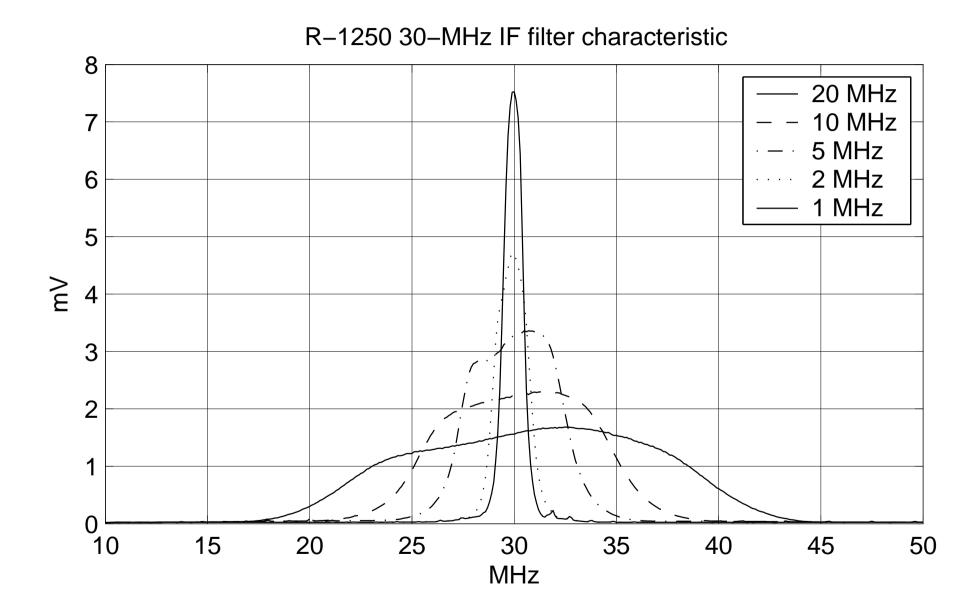
R1250 wideband Tempest receiver



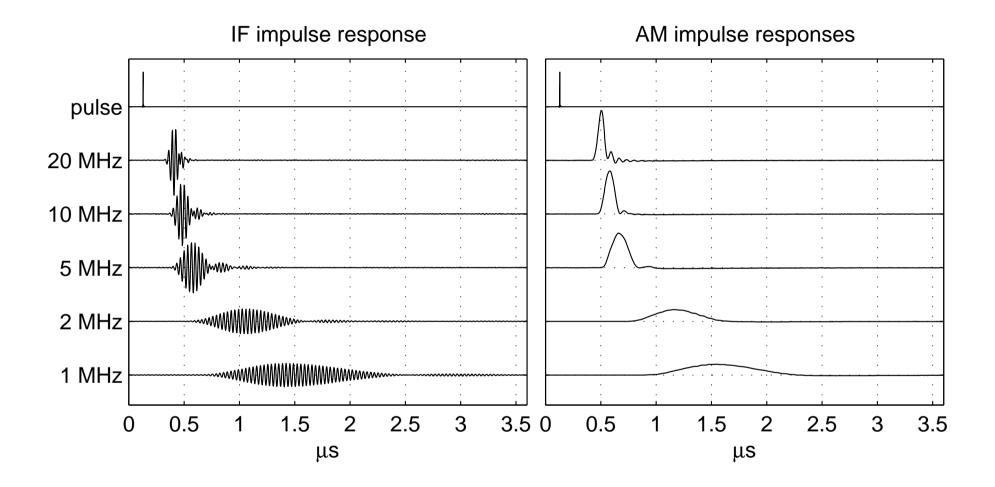
R1250 wideband Tempest receiver

- \rightarrow Can be tuned continuously from 100 Hz to 1 GHz.
- → Offers 21 bandwidths from 50 Hz to 200 MHz (1-2-5 steps). For comparison:
 - AM radio: 2–10 kHz
 - FM radio: 200 kHz
 - TV set: 6 MHz
- \rightarrow Especially robust antenna input (for listening on power lines).
- \rightarrow Gain adjustable by a factor of 10^9 .
- \rightarrow Automatic gain control can be deactivated.
- \rightarrow Demodulators: AM linear, AM logarithmic, FM, BFO.
- → Export controlled products, $\approx 30-100 \text{ k} \pounds$ Second hand offers on Internet for < 1 k \pounds

Intermediate frequency bandwidth



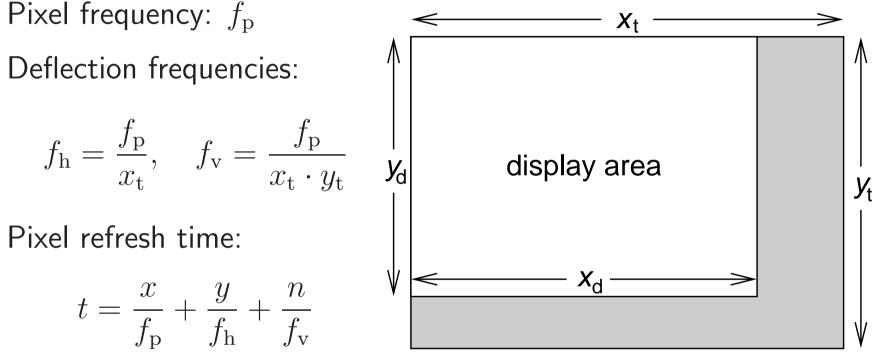
Receiving impulse signals



impulse width = $\frac{1}{\text{bandwidth}}$

Video timing

The electron beam position on a raster-scan CRT is predictable:



The 43 VESA standard modes specify $f_{\rm p}$ with a tolerance of $\pm 0.5\%$.

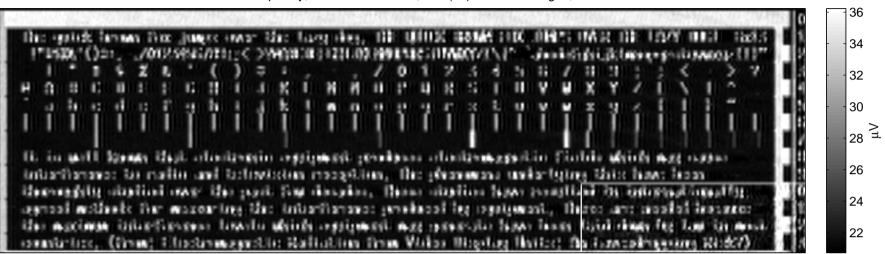
ModeLine "1280x1024@85" 157.5 1280 1344 1504 1728 1024 1025 1028 1072 Image mostly stable if relative error of $f_{\rm h}$ below $\approx 10^{-7}$.

Eavesdropping of CRT Displays

Cathode-ray tube monitors amplify with $\gg 100$ MHz bandwidth the video signal to ≈ 100 V and applies it to the control grid in front of the cathode to modulate the e-beam current. All this acts, together with the video cable, as a (bad) transmission antenna.

Test text used in the following experiments:

The quick brown fox jumps over the lazy dog. THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG! 6x13 !"#\$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~ 2 3 3 5 R R Q S 5 6 8 It is well known that electronic equipment produces electromagnetic fields which may cause 9 interference to radio and television reception. The phenomena underlying this have been thoroughly studied over the past few decades. These studies have resulted in internationally Ô agreed methods for measuring the interference produced by equipment. These are needed because the maximum interference levels which equipment may generate have been laid down by law in most 2 3 countries, (from: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?) 0123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901

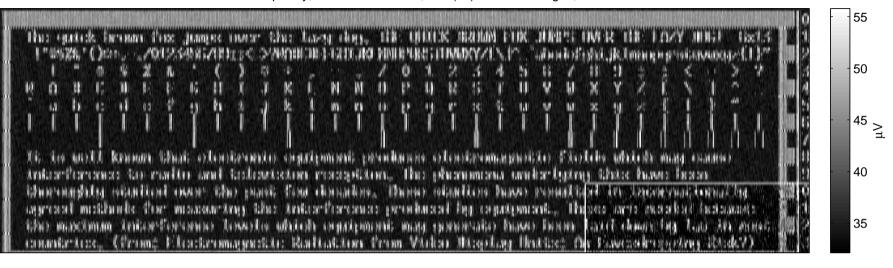


292 MHz center frequency, 20 MHz bandwidth, 256 (16) frames averaged, 3 m distance

292 MHz center frequency, 10 MHz bandwidth, 256 (16) frames averaged, 3 m distance



Too low bandwidths blur the recovered image and limit readability.



480 MHz center frequency, 50 MHz bandwidth, 256 (16) frames averaged, 3 m distance

480 MHz center frequency, 50 MHz bandwidth, magnified image section



AM receiver bandwidth equal to eavesdropped pixel rate distinguishes individual pixels.

Magnified example of eavesdropped text

Test text on targeted CRT:

The quick brown fox

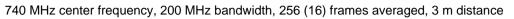
Rasterized output of AM demodulator at 480 MHz center frequency:

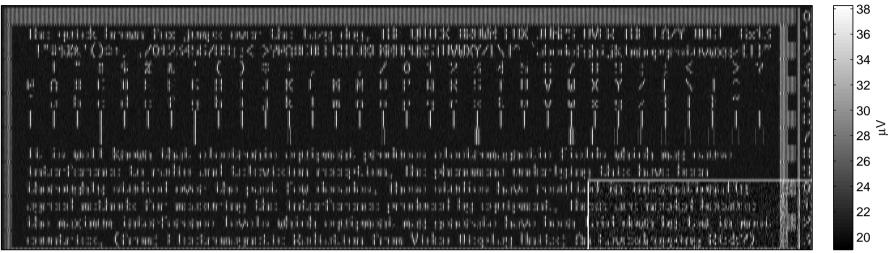


Characteristics:

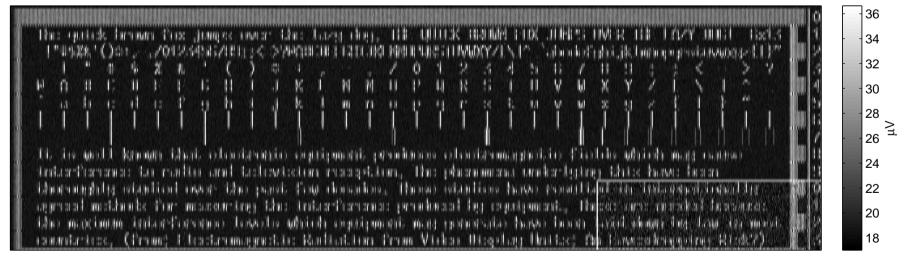
- \rightarrow Vertical lines doubled
- \rightarrow Horizontal lines disappear (reduced to end points)
- \rightarrow Glyph shapes modified, but still easily readable unaided

Pixel frequency: 50 MHz, IF bandwidth: 50 MHz, AM baseband sampling frequency: 500 MHz, measured peak e-field at 3 m: 46 dB μ V/m, corresponds to 12 nW EIRP. [Kuhn, 2003]





700 MHz center frequency, 100 MHz bandwidth, 256 (16) frames averaged, 3 m distance



Higher bandwidths provide sharper impulses, but no further information about pixel data.

Filtered fonts as a protection measure

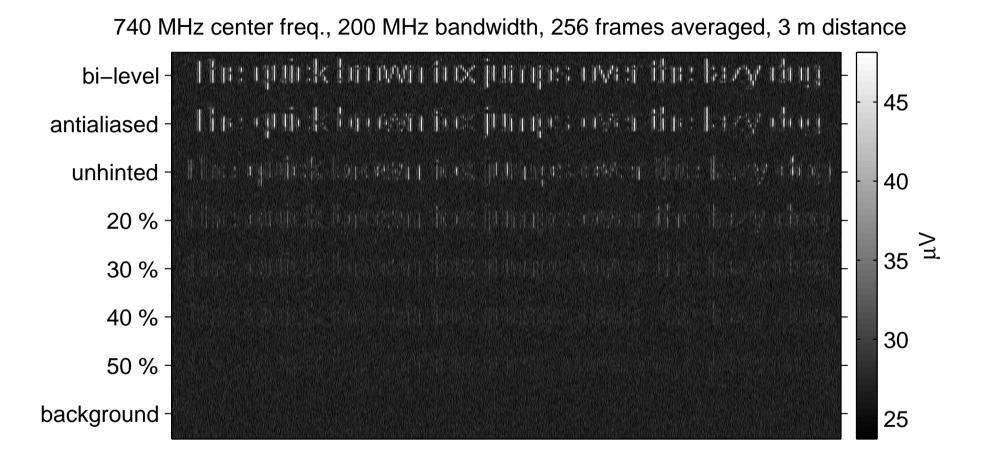
- (1) The quick brown fox jumps over the lazy dog
- (2) The quick brown fox jumps over the lazy dog
- (3) The quick brown fox jumps over the lazy dog
- (4) The quick brown fox jumps over the lazy dog
- (5) The quick brown fox jumps over the lazy dog
- (6) The quick brown fox jumps over the lazy dog
- (7) The quick brown fox jumps over the lazy dog(8)

The above lines show (1) bi-level text, (2) anti-aliased text, (3) anti-aliased text without "hinting", (4–7) anti-aliased text lowpass filtered to remove to 20, 30, 40, and 50 % of the spectrum $[0, f_{\rm p}/2]$, respectively. Font: Microsoft's Arial (TTF), rendered at 12 pixels-per-em. [Kuhn, 2003]

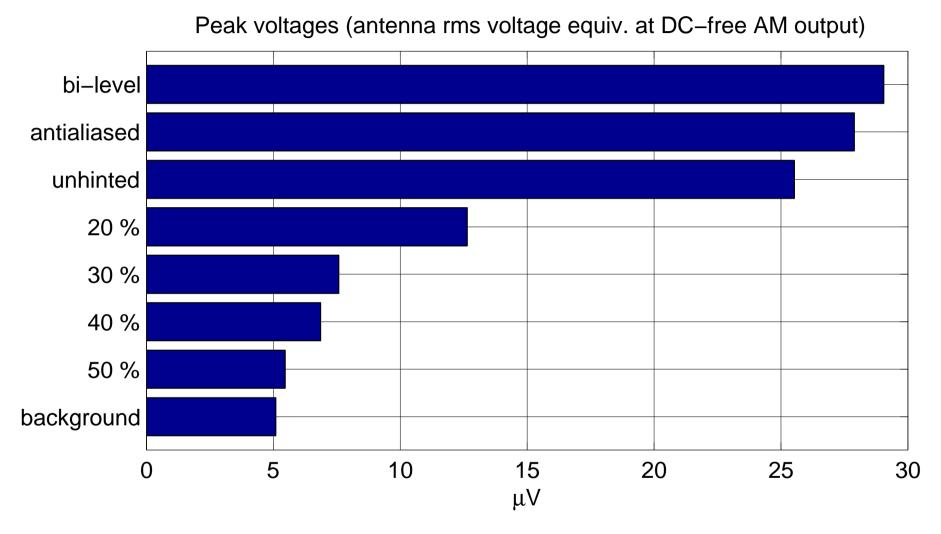
Filtered fonts on the CRT screen

- (1) The quick brown fox jumps over the lazy dog
- (2) The quick brown fox jumps over the lazy dog
- (3) The quick brown fox jumps over the lazy dog
- (4) The quick brown fox jumps over the lazy dog
- (5) The quick brown fox jumps over the lazy dog
- (6) The quick brown fox jumps over the lazy dog
- (7) The quick brown fox jumps over the lazy dog
- (8)

Received radio signal



Filtered fonts peak-amplitude comparison



Removing the top 30 % of the spectrum reduces peak emissions by 12 dB, without significantly affecting user comfort. This means the eavesdropper has to come $3 \times$ closer, into a $10 \times$ smaller area.

Eavesdropping on flat panel displays

350 MHz center frequency, 50 MHz bandwidth, 16 (1) frames averaged, 3 m distance

Enabling syn flood pertection Disabling UP forwarding Boot bogging started on -dearthylic-dearconsule) at Sun fyr 28 22:19:44 2002 Moster Resource Control: previous ronlewel: N. switching to rombewel: Storting personal-firewall (Enittal) For active! Initializing remote generator Storting States Losh 1 Storting Systeme: Storting systeme: Storting systeme: Storting systeme: Coding expressions: Coding expression: Coding keyner generator Storting service: Coding keyner generator Storting service: Storting service: Storting service: Storting service: Storting service: Storting service: Storting none Service: Storting service: Storti			
Host Engine Started on Adamstry U-demonstrate) at Sum Apr 28 22:19:41 2862 Naster Resource Control: premious contenel: N. switching to combasel: Starting personal-firewall (initial) End active) Initializing random number generator Starting soft daeman: Starting systed account: Starting systed services I ush 1 Starting service at daeman: Loading compose table winkeys shifter I latin1.add Loading console form lat29-16.psfu Loading servenes trivial Starting us console thys Starting none Service Cache Baeman Starting console thys Starting console thys Starting none Services support (gpm): Starting services in runbewel 3 has Stipped services in runbewel 3: Naster Resource Control: runbewel 3: Netern Stipped services in runbewel 4: Netern Stipped services in runbewel 4: Netern Stipped services in runbewel 5: Netern Stipped services in runbewel 5: Starting Stipped service			
Master Resource Control: previous runlewel: N. switching to runlewel: Starting personal-firewall Cinitial) Cont active: Initializing random number generator dome Starting Sill daemon: dome Starting supp services: dome Starting supp services: dome Starting supp service at domain: dome Starting service at domain: dome Conding compose to ble winkeys shiftetrl Latin1.add dome Loading compose to ble winkeys shiftetrl Latin1.add dome Loading compose to ble winkeys shiftetrl Latin1.add dome Starting op console func dome Starting service: dome Loading compose to ble winkeys shiftetrl Latin1.add dome Starting op console func dome Starting service coche Doewon dome Starting sound driver: cs4231 dome Restoring the previous sound setting octive: t Starting services in runlewel 3 has herew dome Skipped services in runlewel 3: dome Meleowe to SuBE Linux 7.3 (GB65) - Remet 2.4, 18-468 (ttyp):			- 120
Starting personal-firewall (initial) funct active! dome Initializing random number generator dome Starting hatplugging services I ush 1 dome Starting SSH daemon: dome Starting upd dome Starting version of FONCIA (using scheme: cl) dome Starting service at daemon: dome Inading compuse table winkeps shiftctr1 latin1.add dome Inading console fout latter is support (ggm): dome Starting versionel force is support (ggm): dome Starting the previous sound setting active i Starting the previous in runlewell 3: active i Master Resource Control: runlewell 3: been Nethome to SuSE Linux 7.3 (1386) - Nermel 2.4.18-468 (ttypt).			
Initializing rondom number generator dome dom		lon - innorm Dieswoer D 🗧	
Starting hatplugging serwices [ush] dame da			
Starting SSH daeman: dame 100 Skarting syslog serwices: dame dame Starting ind dame dame Starting syslog serwices: cline dame Starting service at daeman: dame dame Loading keynap querts/de-latinf-nodeadkeys.map.gs dame dame Loading compuse table winkeys shiftctrl latinf.add dame dame Loading compuse table winkeys shiftctrl latinf.add dame dame Loading screenmap trivial dame dame dame Starting vocusale fromt lat9w-16.psfu dame dame dame Loading screenmap trivial dame dame dame dame Starting vocusale tags dame dame<			
Starting sysling services dome		doomesaaa	
Starting lyd done done <td></td> <td></td> <td>F - 100</td>			F - 100
Starting external FCMCIA fusing scheme: cl) done		domession	
Starting service at daeman: dome		dennermente	
Loading keynap quertz-de-latint-modeadkeys.map.gz done done done done done done done done			
Loading compose table winkeys shiftctrl latini.add done done done done done done done do		donmerstan	
Laading compuse table wonkeys shiftered latonil.add done Laading consule fort lat9w-16.psfu Laading screenwap trivial deve Setting up consule thys Starting None Service Cache Daemon Starting consule mouse support (gpm): Starting sound driver: cs4231 Restoring the previous sound setting Starting personal-firewall (final) (not Naster Resource Control: runlewell 3 has Skipped services in runlewell 3: Welcome to SuSE Linux 7.3 (i386) - Remet 2.4.10-468 (ttyp):			80
Loading screenmap trivial Setting up console thys Starting Name Service Cache Daemon Starting console mouse support (gpm): Starting sound driver: cs4234 Restoring the previous sound setting Starting personal-firewall (final) (not Master Resource Control: runlewell 3 has Skipped services in runlewell 3: Melcome to SuSE Linux 7.3 (1386) - Kernel 2.4.18-468 (rtyp):			
Setting up console thys Starting Name Service Cache Daeman Starting console mouse support (gpm): Starting sound driver: cs4230 Restoring the previous sound setting Starting personal-firewall (final) foot Master Resource Control: runlewell 3 has Skipped services in runlewell 3: Welcome to SuSE Linux 7.3 (6386) - Remet 2.4.18-468 (ttyp):		NET VALUE AND ADDRESS AND ADD	
Starting Name Service Cache Doeman Starting consule mouse support (gpm): Starting sound driver: cs4230 Restarting personal-firewall (fimal) (mot Naster Resource Control: runlewed 3 has Skipped services in runlewed 3: Welcome to SuSE Linux 7.3 (i386) - Kernel 2.4.16-468 (rtyg):			그.
Starting console mouse support (gpm): deve 60 Starting sound driver: cs4230 deve deve Restoring the previous sound setting devie devie Starting personal-firewall (final) Inct active) devie Naster Resource Control: runlewell 3 hos heem 40 Welcome to SuSE Linux 7.3 (i386) - Rermet 2.4.16-468 (ttyp): 40			
Starting sound driver: cs4230 Restoring the previous sound setting Starting personal-firewall (final) (not Naster Resource Control: runlewell 3 has Skipped services in runlewell 3: Welcome to SuSE Linux 7.3 (1386) - Remet 2.4.10-468 (ttyf):		2019년 1월 1949년 1949년 2019년 2019년 1월 1949년 1949년 1949년 1967년 1967년 1967년 1967년 1967년 1967년 1967년 1967년 1967년 19	
Hestoring the previous sound setting Starting personal-firewall (final) (not active) Naster Resource Control: runlewell 3 has been Skipped services in runlewell 3: Welcome to SuSE Linux 7.3 (1386) - Remell 2.5.18-068 (ttyp).		のたいだだい ないがん ちゅうえい おとうかい かいしょう ひかい かいかい ないない ひかい かいかい ちゃく ちょう ストリン ちょうかい ひょうかい ないしない	60
Starting personal-firewall (final) (not active) Naster Resource Control: rombewell 3 has Skipped services in rombewell 3: Welcome to 303E Linux 7.3 (1386) - Rernet 2.4.10-968 (rtyp):			
Naster Resource Control: runlewel 3 has ficen Skipped services in runlewell 3: Welcome to SuSE Linux 7.3 (1386) - Remel 2.3.10 568 (Rtyp).	Restaring the previous sound setting	denie a stational de la companya de	
Skipped serwices in runbewell 3: Welcome to SuSE Linux 7.3 (1386) - Kernelf 2.3.10-368 (ttyp):			
Velaame ta SuSE Lünum 7.3 Cü3860 - Reemel 2.5.18-468 Cttyd).			
Nelaame ta SuSE Limux 7.3 (ij386) - Reemel 2.5.18-468 (ttyl):.	3kipped services in runlewel 3:		10
			40
nuk ^{se} n Dronim.	Welcome to SuSE Limux 7.3 (i386) - Reemet 2.4.10-468 Cttyt	đe.	
= 20	ngk25. Dogim:		20

0-40000-4000-40

-980,980,980,980

ogkæs bogins

magnified image section

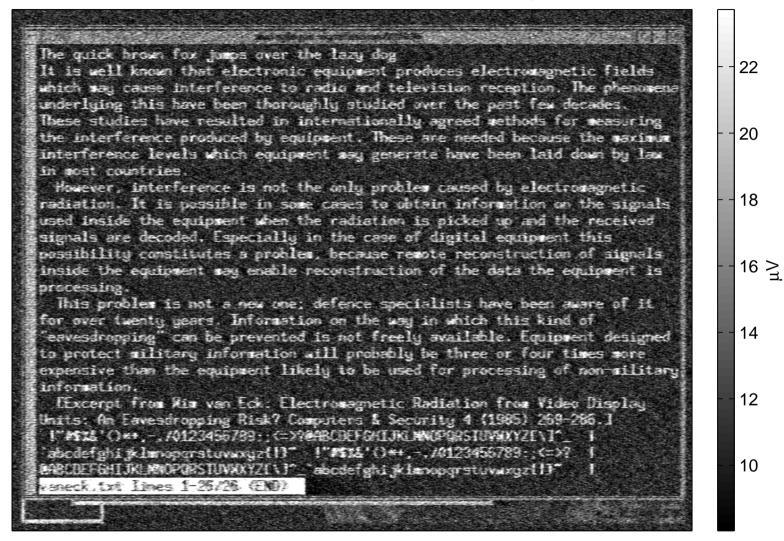


- \rightarrow Horizontal lines intact (\rightarrow no analog video signal)
- \rightarrow Horizontal resolution reduced
- \rightarrow 100 μ V signal amplitude at receiver input (rms equiv.)
- \rightarrow 57 dB μ V/m (50 MHz BW) field strength at 3 m distance

 \rightarrow equivalent isotropic radiated power (EIRP) about 150 nW Target display: Toshiba 440CDX laptop, 800×600@75Hz, $f_{\rm p} = 50$ MHz

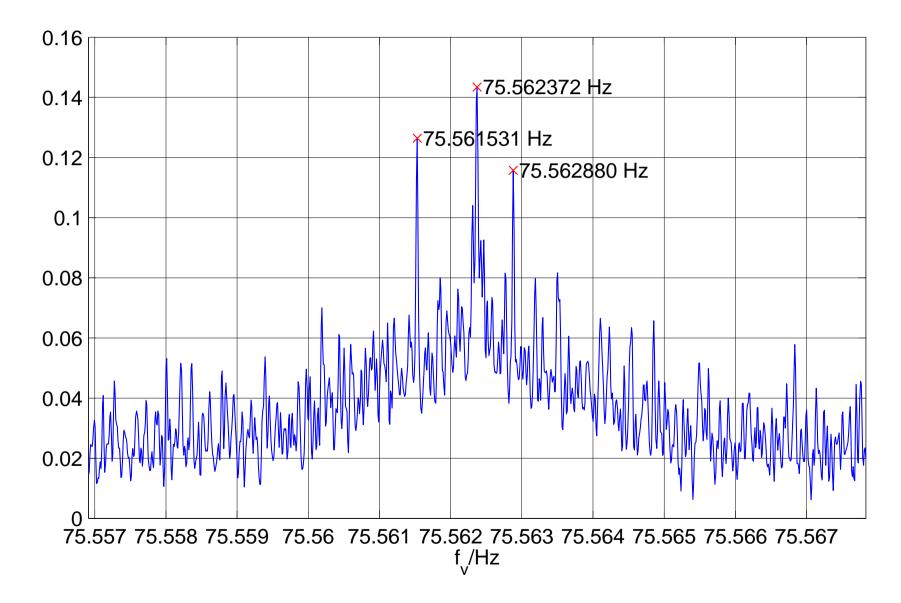
Eavesdropping across two office rooms

350 MHz, 50 MHz BW, 12 frames (160 ms) averaged



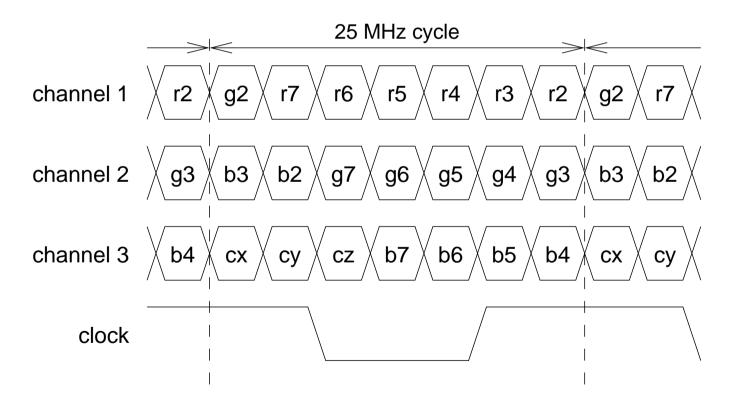
Target and antenna in a modern office building 10 m apart, with two other offices and three plasterboard walls (-2.7 dB each) in between. Single-shot recording of 8 megasamples with storage oscilloscope at 50 Msamples/s, then offline correlation and averaging of 12 frames.

Remote video timing estimation via cross-correlation



FPD-Link – a digital video interface

LCD module and video controller are connected in Toshiba 440CDX laptop by eight twisted pairs (each 30 cm long), which feed the 18-bit RGB parallel signal through the hinges via low-voltage differential signaling (LVDS, EIA-644).



FPD-Link chipset: NEC DS90CF581

FPD link parameters of example target

- \rightarrow pixel frequency: 50 MHz
- \rightarrow bits per pixel: 18
- \rightarrow parallel FPD-Links: 2
- \rightarrow FPD clock frequency: 25 MHz
- \rightarrow FPD bit rate: 7 × 25 MHz = 175 MHz
- \rightarrow total bit rate: $2 \times 3 \times 175$ MHz = 1.05 Gbit/s

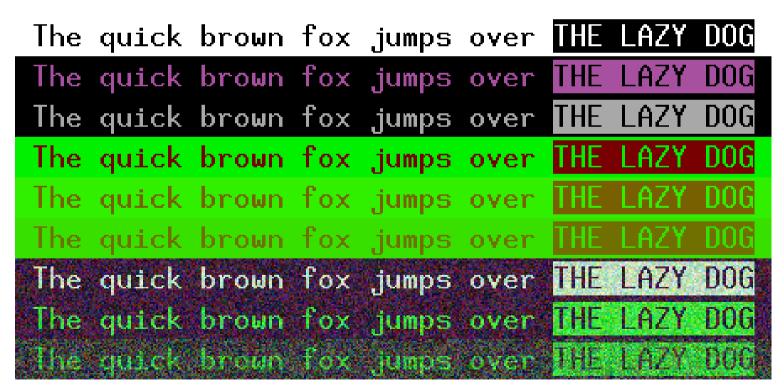
Therefore:

- → 01010101...signal would broadcast harmonics at multiples of 87.5 MHz
- \rightarrow constant-color signal spectrum repeats every 25 MHz

Minimal/maximal reception contrast

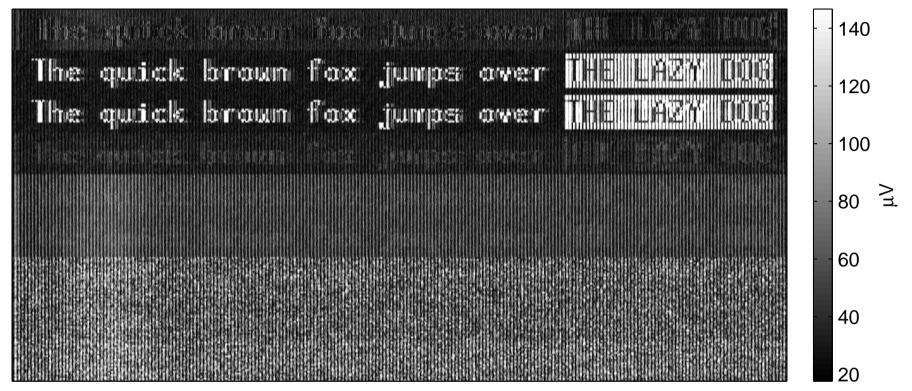
		foreground		back	ground
line	description	RGB	signal	RGB	signal
1	black on white	00 00 00	x000000	ff ff ff	111111X
			0x00000		1X11111
			xxx0000		xxx1111
2	maximum contrast	a8 50 a0	010101x	00 00 00	x000000
			0x01010		0x0000x0
			xxx1010		xxx0000
3	maximum contrast	a8 a8 a8	010101x	00 00 00	000000x
	(gray)		1x10101		0x0000x0
			xxx1010		xxx0000
4	minimum contrast	78 00 00	001111x	00 f0 00	000000x
			0x00000		0x11110
			xxx0000		xxx0000
5	minimum contrast	78 60 00	001111x	30 f0 00	000110x
			0x01100		0x11110
			xxx0000		xxx0000
6	minimum contrast	70 70 00	001110x	38 e0 00	000111x
	(phase shift)		0x01110		0x11100
			xxx0000		xxx0000

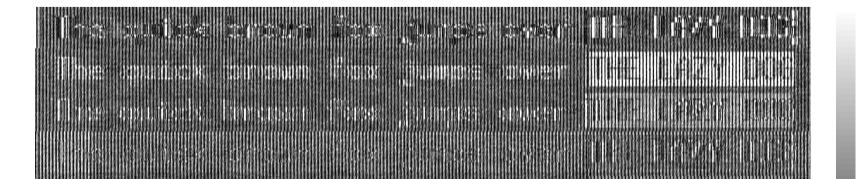
		foreground		ba	ckground
line	description	RGB	signal	RGB	signal
7	text in most significant		r1rrrx		r0rrrrx
	bit, rest random		rx1rrrr		rx0rrrr
			xxx1rrr		xxx0rrr
8	text in green two msb,		rrrrrx		rrrrrx
	rest random		rx11rrr		rx00rrr
			xxxrrrr		xxxrrrr
9	text in green msb, rest	—	rrrrrx	—	rrrrrx
	random		rx1rrrr		rx0rrrr
			xxxrrrr		xxxrrrr



Minimal/maximal reception contrast

350 MHz center frequency, 50 MHz bandwidth, 16 frames averaged, 3 m distance







285 MHz center frequency, 50 MHz bandwidth, 16 frames averaged, 3 m distance



Transition Minimised Differential Signaling (TMDS)

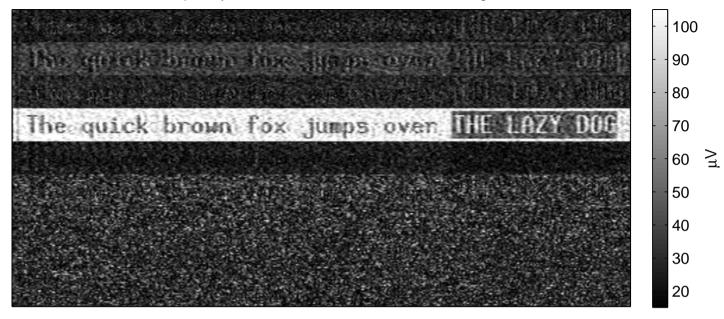
Now industry standard (DVI) for connecting desktop flat-panel displays.

- \rightarrow Differential Gbit/s signaling on three twisted pair channels.
- \rightarrow Converts byte stream into sequence of 10-bit words.
- \rightarrow Attempts to reduce number of bit transitions.
- \rightarrow Balances the total number of 0 and 1 bits transmitted.
- \rightarrow Embeds sync signals using special words.

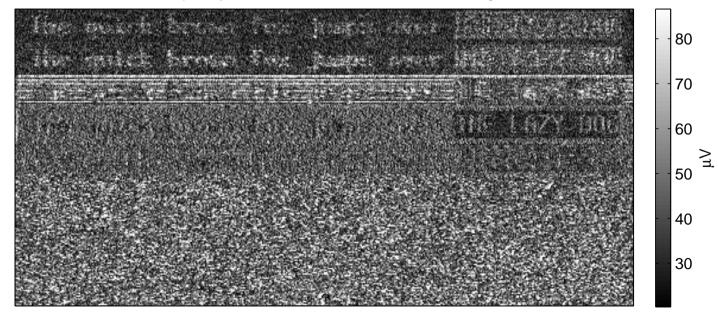
The DC balancing step adds encoding state and only 52 byte values lead to balanced words that are immune against the balancing algorithm. High-contrast pair:

		foreground	background
line	description	RGB	RGB
1	black on white	00 00 00	ff ff ff
2	maximum bit transition contrast	00 00 00	aa aa aa
3	half bit transition contrast	00 00 00	cc cc cc
4	balanced word, max contrast	10 10 10	55 55 55
5	minimum signal contrast	ff 00 00	00 ff 00
6	low nybble random	Or Or Or	fr fr fr
7	text in msb, rest random		
8	text in green two msb, rest random		
9	text in green msb, rest random		

The	quick	brown	fox	jumps	over	THE	Lazy	DOG
The	quick	brown	fox	jumps	over	THE	LAZY	DOG
The	quick	brown	fox	jumps	over	THE	LAZY	DOG
The	quick	brown	fox	jumps	over	THE	LAZY	DOG
The	quick	brown	fox	jumps	over	THE	LAZY	DOG
The	quick	brown	fox	jumps	over	THE	LAZY	DOG
The	quick	brown	fox	jumps	over	THE	LAZY	DOG
The	quick	brown	fox	jumps	over	THE	LAZY	DOG
The	quick	brown	fox	Jumps	over	THE	LAZY	DOG



648 MHz center frequency, 100 MHz bandwidth, 5 frames averaged, 3 m distance



324 MHz center frequency, 50 MHz bandwidth, 5 frames averaged, 3 m distance

Random LSB jamming

Random bits can be added to a text image to generate a phase-locked jamming signal that cannot be averaged away by an attacker. Considerations:

- \rightarrow Foreground/background colors with equal number of bit transitions.
- \rightarrow Randomize less significant bits of each color channel.
- \rightarrow These random bits must *only* be changed when the text changes:
 - Changing the random bits continuously (like TV noise) would help the attacker to average away the jamming signal.
 - Not changing the random bits when the text changes would help the attacker to average away the text and obtain this way a copy of the random signal that can then be subtracted from the received signal.
- → Independent noise bits must be used for *each* occurrence of a character. Beware of glyph caches from which the same bitmap might be used several times.

Open research question: How to jam without leaking update rate of displayed text?

Structure of compromising video signals Mathematical tools:

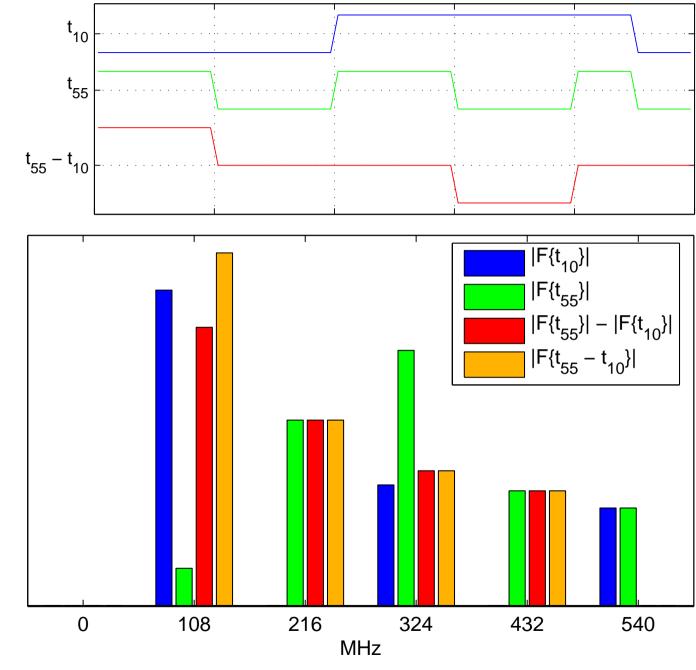
- \rightarrow Fourier transform: time domain \leftrightarrow frequency domain
- → Convolution theorem: multiplication in time domain is convolution in frequency domain, and vice versa.
- → Sampling theorem: Sampled time-domain signal is periodic in the frequency domain, and vice versa.

Result:

- \longrightarrow Symmetric spectrum of digital 2-color video signal repeats itself at frequency intervals $f_{\rm p}$
- → Amplitudes of the individual repetitions of the spectrum are predicted by the difference between the DFTs of the two color code words used.

 \Rightarrow Eavesdropping colors can be optimized to place signal energy into quiet part of UHF radio spectrum.

Details: M. Kuhn, Technical Report UCAM-CL-TR-577, 2003.



DVI signal in 1280×102460Hz video mode with $f_{\rm p}=108$ MHz.

Conclusions

- → Digital video interfaces used with flat-panel displays can emit significantly stronger and better to decode signals than CRTs.
- → An understanding of the exact digital transmission format can be used for attack and defense, especially with stateful balanced codes.
- → High RF-contrast colors can be maliciously configured to simplify RF eavesdropping.
- → The selection of low RF-contrast colors is possible, but can have limited effectiveness with simple codes.
- → An effective low-cost software countermeasure are randomized less-significant bits as a correlated jamming signal.
- → Emission security remains a valid concern in applications with very high confidentiality requirements, predictable device usage, and easy longterm outsider access to nearby rooms/buildings.