# Electromagnetic eavesdropping on computers

Markus Kuhn

2002-06-12



**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.

# 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.



#### Cross-correlation detection of weak binary signals in noise

# **Video Timing**

The electron beam position on a raster-scan CRT is predictable: Pixel frequency:  $f_{\rm p}$ Xt Deflection frequencies:  $f_{\rm h} = \frac{f_{\rm p}}{x_{\rm t}}, \quad f_{\rm v} = \frac{f_{\rm p}}{x_{\rm t} \cdot y_{\rm t}} \quad \begin{vmatrix} \\ \end{matrix} \Big|_{\mathsf{M}}$ display area *Y*<sub>t</sub> Pixel refresh time: Xd  $t = \frac{x}{f_{\rm p}} + \frac{y}{f_{\rm h}} + \frac{n}{f_{\rm y}}$ 

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  $\approx 10^{-7}$ .

# AM audio broadcast from CRT displays

$$s(t) = A \cdot \cos(2\pi f_{\rm c} t) \cdot [1 + m \cdot \cos(2\pi f_{\rm t} t)]$$

#### 300 and 1200 Hz tones at $f_{\rm c} = 1.0$ MHz:



Play your MP3 music at home via CRT emanations in your AM radio: http://www.erikyyy.de/tempest/

# **Eavesdropping of CRT Displays**

CRT Monitor amplifies with  $\gg 100$  MHz bandwidth the video signal to  $\approx 100 V$  and applies it to the screen 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:

																																			Û
l l	The	; qu	uicl	k E	յոօս	in 1	fox	(j	ump	28	ove	in t	:he	laz	уd	log₊	Tŀ	IE Q	UIC	ЖE	3ROW	N F	ΟX	JUÞ	IPS	OVE	RT	ΉE	LAZY	DC	)G !	- 6×	:13 🕴	<b>.</b>	1
l	ļ"	#\$%	28.1	()*	(+ , -	$\cdot_*/0$	012	234	567	789	::<	=>	?@AF	CDE	FGH	IJK	ĽMM	40PQ	RST	Ս۷և	JXYZ	$[ \]$	^_`	abo	def	ghi	jkl	mno	pgrs	tu	/wxy	Jz{I	}~ }		2
Î		ļ	н	#	\$	2	8	5	I	(	)	*	+	,	-	+	1	0	1	2	3	4	5	6	7	8	9	‡	;	<	=	>	?	8	3
Î	0	Ĥ	В	С	D	Е	F	: 1	G	Η	Ι	J	K	L	М	Ν	0	Р	Q	R	S	Т	U	V	ω	Х	Y	Z	[	١.	]	~	_ }		4
Î	•	ą	Þ	ç	ġ	ę	f	: .	9	h	i	j	ķ	1	M	ņ	ò	P	9	r	ş	ţ	ų	Ŷ	Ŵ	X	y	Ż	-{	Į	}	N .		8	5
ļ																					ļ						J	J		1	1	1			6
Ĭ																																			7
ļ	It	iε	we	11	knc	)wn	tŀ	nat	e!	lec	tro	nic	ec ec	puip	nen	nt p	roc	luce	sе	lec	tro:	mag	net	ic	fie	lds	: wh	ich	n may	Cā	ause	3	}		8
ĺ	int	erf	Per	enc	;e t	:o t	rac	lio	ar	٦d	tel	ev:	isic	n r	все	pti	on,	, Th	e F	her	nome	na	unc	ler]	yir	g t	his	: ha	ive b	eer	1			8	9
	the	prou	.gh	ly	stu	die	ed	ΟV	er	th	e p	ast	: fe	w di	вса	ides	: <b>,</b> 1	ihes	e s	tuc	lies	ha	ive	res	ult	ed	in	int	erna	tic	pnal	.ly			Q
Į	agr	eec	d m	eth	iods	; f(	or	Мe	ast	uri	ng	the	e ir	nter	fer	enc	e p	prod	uce	ed b	у е	qui	.pme	nt,	Tŀ	ese	an	e n	eede	d b	)eca	ause	!	8	1
Î	the	e Ma	axi	mum	ı ir	iter	rfe	re	nce	e 1	eve	ls	whi	ch i	equ	ipm	ient	: ma	y je	ene	erat	e h	nave	; Бе	en	lai	d d	lown	ьу	lau	J_ir	) MC	ist 🕴		2
	COL	intr	<u>rie</u> :	S.	(fr	'OM)	÷E	le	ctr	rom	agn	et:	ic R	ladi	ati	on	fro	jm V	ide	o I	lisp	lay	į Ur	nits	;‡ Ĥ	in E	ave	sdr	oppi	ng	Ris	:k?)		<b></b>	3
																																			4
)12	345	678	<u> 190</u>	123	345E	;789	901	.23	45f	378	901	.234	1567	'890	123	456	:789	1012	345	i678	1901	234	1567	'89(	123	456	789	1012	3456	789	4012	2345	6789	901	X



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

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





### **Automatic Radio Character Recognition**

#### Example Results (256 frames averaged):

The quick brown fox jumps over the lazy dog. THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG! 6x13 !"#\$%&'()\*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^\_'abcdefghijklmnopqrstuvwxyz{|}~ It is well known that electronic equipment produces electromagoetic fields which may cause 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 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 countries. (from: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?)

#### With only 16 frames averaged:

Ihc quick bcown fox\_jumps-evec-toe Iazg dsg\_=TOE\_QHICK-DROWM-EHX JUHPS Q?ER iUE LOZY DH6! -6zi3= !"#\$%&'()\* ,-=ZO!?3'56709:;< >?@ADcDEFCHIJKLHNcPQRHTHVQ%YZ[\]^='abedcBg6Ijkimndpqcstuvw:yz{|}" it Ic weII=kocwn=tHat-clectroric=cguipmcnt e\_dduces-electrpmugmctic\_fidlde\_whico-may euuse \_-. = icce-feceaee tc-radic-and teIcvisicn ceccpticc=-|6e phcncmcna uedcrlyigg tcic=have=bcec\_= \_= \_-tncceughIy ctuHicd=dvcc the eust few=decudes, ihcsc stvdics'have =ecuItcd io\_inteceutiocu\_iy \_ \_ ugrceH=mct6edc=foc meacuciny t6c icterfcsesce pcoduccd\_bg eeuipmcnt. Tbese are-nccded bccouse toc=meximum intcrfercncc ievcls which-eguipmcnt may gesc-atc-6ave oecn la7d=dewc=by law in mcsc ceuntricc=-(fcem: Flectromegnctic-Radiatibn f\_om Video Dispiey\_Hsitc:=Hn Eavcsdcc=pimg-Risk?)-

# **Steganographic transmission of images**

#### The user sees on her screen:

My De	The Computer Laboratory - Microsoft Internet Explorer	×
I	→ Back • → · ⊗ <ul> <li></li></ul>	39
My	General Security Content Connections Programs Advanced	-1
My	Vou can change which page to use for your home page. Addgess: BH/DOCORGERCEMENT 255/2755222 HTML Use Current Use Default Use Blank UNIVERSITY OF CAMBRIDGE	
Re	Temporary Internet files       Computer Laboratory         Pages you view on the Internet are stored in a special folder for quick viewing later.       Delete Files         Delete Files       Settings	
	History          History         The History folder contains links to pages you've visited, for quick access to recently viewed pages.         Days to keep pages in history:         20         Clear History	
Ado	Colors       Fonts       Languages       Accessibility       ticns, and Lab seminars.         OK       Cancel       Accessibility       Iticns, and Lab seminars.	
1	The set of	1
1	Start 🙆 😂 🧊 🕼 The Computer Labora	

#### The radio frequency eavesdropper receives instead:

445 MHz center frequency, 10 MHz bandwidth, 1024 frames averaged, 3 m distance



# **Amplitude modulation of dither patterns**



Cover image  $C_{x,y,c}$ , embedded image  $E_{x,y}$ , all normalized to [0,1]. Then screen display is

$$S_{x,y,c} = \left(C_{x,y,c}^{\tilde{\gamma}} + \min\{\alpha E_{x,y}, C_{x,y,c}^{\tilde{\gamma}}, 1 - C_{x,y,c}^{\tilde{\gamma}}\} \cdot d_{x,y}\right)^{1/\tilde{\gamma}}$$

with dither function  $d_{x,y} = 2[(x+y) \mod 2] - 1 \in \{-1, 1\}$ and  $0 < \alpha \le 0.5$ .

### Filtered fonts as a protection measure

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

### **Received radio signal**



### **Eavesdropping across two office rooms**

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



Target in room GE16 and antenna in room GE10 of the William Gates building, with two offices and three plasterboard walls (-2.7 dB each) in between.

## **FPD-Link – a digital video interface**

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



# Minimal/maximal reception contrast

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

