2002 IEEE Symposium on Security and Privacy

Proceedings

2002 IEEE Symposium on

Security and Privacy

12–15 May 2002 • Berkeley, California

Sponsored by

IEEE Computer Society Technical Committee on Security and Privacy

江苏工业学院图书馆
藏书章

IEEE COMPUTER SOCIETY

IEEE

Los Alamitos, California

Washington • Brussels • Tokyo

Copyright © 2002 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number PR01543
ISBN 0-7695-1543-6
ISSN 1081-6011

Additional copies may be ordered from:

IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 714 821 8380
Fax: + 1 714 821 4641
http://computer.org/
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
http://shop.ieee.org/store/
customer-service@ieee.org

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Editorial production by A. Denise Williams

Cover art production by Joseph Daigle/Studio Productions

Printed in the United States of America by The Printing House

Proceedings

2002 IEEE Symposium on

Security and Privacy

Program Committee

Program Co-Chairs

Martín Abadi
University of California at Santa Cruz, USA

Steve Bellovin
AT&T Research, USA

Program Commitee

Ross Anderson, *University of Cambridge, UK*
Andrew Appel, *Princeton University, USA*
William Arbaugh, *University of Maryland, USA*
Dominique Bolignano, *Trusted Logic, France*
Simon Foley, *University College Cork, Ireland*
Cédric Fournet, *Microsoft Research, UK*
Dan Geer, *@Stake, USA*
Ian Goldberg, *Zero-Knowledge Systems, Canada*
Stephen Kent, *BBN, USA*
Hugo Krawczyk, *Technion, Israel*
Wenke Lee, *Georgia Institute of Technology, USA*
Vern Paxson, *ACIRI, USA*
Greg Rose, *Qualcomm, Australia*
Fred Schneider, *Cornell University, USA*
Dan Simon, *Microsoft Research, USA*
Leendert Van Doorn, *IBM Research, USA*
Avishai Wool, *Lumeta, USA*

此为试读,需要完整PDF请访问: www.ertongbook.com

Message from the Program Chairs

These Proceedings contain the 21 papers that were presented at the 2002 IEEE Symposium on Security and Privacy, held May 12-15 at the Claremont Resort, in Berkeley, California, USA. The papers were selected from 95 submissions on the basis of their scientific excellence by a program committee of experts. We wish to thank all authors of submissions for offering their papers for consideration.

The submissions were received in response to an open call for papers. The call for papers requested anonymous submissions, so the reviewers were usually not aware of the identity of the authors. However, we treated anonymity as a privilege rather than a duty; we accepted some papers for which the identity of the authors was to various degrees apparent or easy to guess.

Each submission was assigned to three members of the program committee. We are grateful to the members of the program committee for their diligence and insight in reviewing the submissions. The programme committee sometimes resorted to the advice of outside colleagues; we are also grateful to those outside colleagues, in particular Dave Aitel, Tuomas Aura, Josh Benaloh, Hal Burch, Ran Canetti, Brian Carrier, Pau-Chen Cheng, Don Davis, Yair Frankel, Alex Gantman, Dieter Gollman, Andrew Gordon, Peter Gutmann, Shai Halevi, Amir Herzberg, Philip Homburg, Jon Howell, Paul Karger, Aram Khalili, John McLean, Arunesh Mishra, Kobbi Nissim, Panos Papadimitratos, Bryan Payne, Adrian Perrig, Fabien Petitcolas, Nick Petroni, Benny Pinkas, Tal Rabin, Josyula R. Rao, Mike Roe, Reiner Sailer, Andrei Serjantov, Narendar Shankar, Alex Shvartsman, Gün Sirer, Jessica Staddon, Mark Tuttle, Wietse Venema, David Walker, Avi Wigderson, Steve Zdancewic, and Lidong Zhou. A meeting of the program committee took place at AT&T Research in Menlo Park on January 11, 2002, and the selection of the papers was concluded soon after that.

In addition to these 21 papers, the Symposium included a session of short presentations and two invited talks, by Udi Manber and by Bob Blakley.

Bob Blakley also served as conference vice chair, seconding Heather Hinton who served as general chair. It is a pleasure to thank both of them for the arrangements for the Symposium.

Program Co-Chairs

Martín Abadi
Steven Bellovin

Symposium Committee

General Chair

Heather Hinton
Tivoli Systems, USA

Vice Chair

Bob Blakley
Tivoli Systems, USA

Program Co-Chair

Martín Abadi
University of California at Santa Cruz, USA

Program Co-Chair

Steve Bellovin
AT&T Research, USA

Treasurer

Terry Hall
Boeing, USA

Table of Contents

2002 IEEE Symposium on Security and Privacy

Program Committee

Program Co-Chairs

Martín Abadi
University of California at Santa Cruz, USA

Steve Bellovin
AT&T Research, USA

Program Commitee

Ross Anderson, *University of Cambridge, UK*
Andrew Appel, *Princeton University, USA*
William Arbaugh, *University of Maryland, USA*
Dominique Bolignano, *Trusted Logic, France*
Simon Foley, *University College Cork, Ireland*
Cédric Fournet, *Microsoft Research, UK*
Dan Geer, *@Stake, USA*
Ian Goldberg, *Zero-Knowledge Systems, Canada*
Stephen Kent, *BBN, USA*
Hugo Krawczyk, *Technion, Israel*
Wenke Lee, *Georgia Institute of Technology, USA*
Vern Paxson, *ACIRI, USA*
Greg Rose, *Qualcomm, Australia*
Fred Schneider, *Cornell University, USA*
Dan Simon, *Microsoft Research, USA*
Leendert Van Doorn, *IBM Research, USA*
Avishai Wool, *Lumeta, USA*

Optical Time-Domain Eavesdropping Risks of CRT Displays

Markus G. Kuhn
University of Cambridge, Computer Laboratory
JJ Thomson Avenue, Cambridge CB3 0FD, UK
mgk25@cl.cam.ac.uk

Abstract

A new eavesdropping technique can be used to read cathode-ray tube (CRT) displays at a distance. The intensity of the light emitted by a raster-scan screen as a function of time corresponds to the video signal convolved with the impulse response of the phosphors. Experiments with a typical personal computer color monitor show that enough high-frequency content remains in the emitted light to permit the reconstruction of readable text by deconvolving the signal received with a fast photosensor. These optical compromising emanations can be received even after diffuse reflection from a wall. Shot noise from background light is the critical performance factor. In a sufficiently dark environment and with a large enough sensor aperture, practically significant reception distances are possible. This information security risk should be considered in applications with high confidentiality requirements, especially in those that already require "TEMPEST"-shielded equipment designed to minimize radio-frequency emission-security concerns.

1. Introduction

Classic techniques for unauthorized remote access to private and confidential information – tapping communication links, code breaking, impersonation – become increasingly difficult as the use of modern cryptographic protection techniques proliferates. Those in the business of obtaining information from other people's computers without their consent or knowledge – from law enforcement and intelligence service technicians through criminals to market researchers – are continuously looking for alternative means of access.

Military organizations have been aware of compromising acoustic and radio-frequency emanations from information processing equipment since the early 1960s and established *emission security (EMSEC)* test standards with shielding requirements for computers that process classified information [1, 2, 3]. A larger community became aware of the radio-frequency information leakage of video displays and other computer peripherals through van Eck's eavesdropping demonstration with modified TV sets [4] and subsequent research on related phenomena [5, 6, 7]. Optical emission security has been discussed for fiber-optic cables [8].

The available open emission-security literature on displays has so far only focused on the threat of information carried in the radio-frequency bands (primarily 3 MHz–3 GHz). We must not forget, however, that the very purpose for which display devices are designed is the emission of information suitable for human perception in the optical bands (385–790 THz frequency or 780–380 nm wavelength). As we will see, the overall light emitted by a commonly used cathode-ray tube computer monitor is a broadband information carrier that transmits via light-intensity modulation the low-pass filtered video signal. It is feasible to reconstruct screen contents from this information channel, even if the eavesdropper cannot position a sensor within a direct line-of-sight to the target display surface and receives the light only after diffuse reflection, for instance from an office wall.

An upper bound for the possible signal quality and eavesdropping distance is set by the shot noise from other light sources. Such an analysis can not only be applied to video screens but also to any other optical displays that might be targeted by an eavesdropper, for instance status indicators of serial ports.

2. Projective observation with telescopes

It has of course not escaped the attention of security experts in the past that any video display surface that is within a line of sight to an eavesdropper's hiding place could be read with the help of a telescope. Many organizations dealing with critical information have security policies concerning the orientation and visibility of documents, computer monitors, and keyboards relative to windows that are visible from uncontrolled spaces such as nearby streets, parking lots, or buildings.

Proceedings of the 2002 IEEE Symposium on Security and Privacy (S&P'02)
1081-6011/02 $17.00 © 2002 **IEEE**

IEEE COMPUTER SOCIETY

此为试读,需要完整PDF请访问: www.ertongbook.com

With high-quality optics, the limiting factor for the angular resolution of a telescope is the diffraction at its aperture. For an aperture (diameter of the first lens or mirror) D, the achievable angular resolution as defined by the Rayleigh criterion is

$$\theta = \frac{1.22 \cdot \lambda}{D}, \tag{1}$$

where $\lambda \approx 500$ nm is the wavelength of light. Typical modern office computer displays have a pixel size $r = 0.25$ mm (for example in the form of the 320×240 mm display area on a 43 cm CRT, divided into 1280×1024 pixels). If the observer is located at distance d and her viewing direction differs by an angle α from a perpendicular view onto the display surface, she will see a single pixel under a viewing angle $\theta = \frac{r}{d} \cdot \cos\alpha$. She will therefore need a telescope with an aperture of at least

$$D = \frac{1.22 \cdot \lambda \cdot d}{r \cdot \cos\alpha}. \tag{2}$$

A simple amateur astronomy telescope ($D = 300$ mm) will be sufficient for reading high-resolution computer display content from up to 60 m distance under $\alpha < 60°$, even with very small font sizes.

3. Time-domain observation of CRT light

The direct projection of a video display surface onto the image plane of a camera with a good telescope is not the only way in which optical emanations of cathode-ray tubes can be used to read the screen content at a distance.

Most computer video displays used today are raster scan devices. As in a television receiver, the image is transmitted and updated as a sequence of scan lines that cover the entire display area with constant velocity. The pixel luminosity values in this sequence are a function of the video signal voltage. Vector displays are an alternative technique, in which not only the intensity but also the path of a cathode-ray tube electron beam is controlled by the displayed data, however they are hardly used any more.

The timing of a raster-scan video signal is first of all characterized by the pixel clock frequency f_p, which is the reciprocal of the time in which the electron beam travels from the center of one pixel to the center of its right neighbor. The pixel clock is an integer multiple of both the horizontal and vertical deflection frequency, that is the rate $f_\mathrm{h} = f_\mathrm{p}/x_\mathrm{t}$ at which lines are drawn and the rate $f_\mathrm{v} = f_\mathrm{h}/y_\mathrm{t}$ at which complete frames are built on the screen. Here, x_t and y_t are the total width and height of the pixel field that we would get if the electron beam needed no time to jump back to the start of the line or frame. The actually displayed image on the screen is only $x_\mathrm{d} < x_\mathrm{t}$ pixels wide and $y_\mathrm{d} < y_\mathrm{t}$ pixels high to leave time to transmit synchronization pulses to the monitor and for the electron-beam flyback.

In order to facilitate the correct factory adjustment of the monitor image geometry over the wide range of different video timings used today, the *Video Electronics Standards Association (VESA)* has standardized a collection of exact timing parameters [9]. These include the 20–30 settings used by most personal computer displays today. An eavesdropper who has no access to the synchronization impulses from a video signal can use these standard timings as a first guess of the exact deflection frequencies. Careful additional frequency adjustment will be necessary, because the VESA timings are specified with a tolerance of 5%, whereas an eavesdropper has to match the correct frequency with a relative error of less than 10^{-7} to get a stable image.

The light emitted by all of the pixels of a CRT together is a weighted average of the luminosity of the last few thousand pixels that the electron beam addressed. More precisely, the intensity $I(t)$ of the light emitted is equivalent to the (gamma corrected[1]) video signal $v_\gamma(t)$ convolved with the impulse response $P(t)$ of the screen phosphor:

$$I(t) = \int_0^\infty v_\gamma(t - t')\, P(t')\, \mathrm{d}t'. \tag{3}$$

So even if an observer can pick up only the current average luminosity of a CRT surface, for example by observing with a telescope the diffuse light reflected from nearby walls, furniture, or similar objects, this provides her access to a low-pass filtered version of the video signal. Not even curtains, blinds, or windows with etched or frosted glass surfaces – as are frequently used to block views into rooms – are necessarily an effective protection, as the average luminosity inside a room can still leak out.

As with radio-frequency eavesdropping, an attacker utilizes the fact that displayed pixels are updated sequentially, and again the periodic nature of the process can be used to reduce noise and to address individual display units out of several in a room via periodic averaging.

The light emitted by a cathode-ray tube is generated when the electron beam hits a luminescent substance, called the *phosphor* (not to be confused with the chemical element phosphorous). The measurements described in the next section show that when the electron beam hits the phosphor of a bright pixel, the emitted light intensity reaches its maximum within a single pixel period, and even though the

[1] The intensity of the light emitted by the phosphor is up to a saturation limit proportional to the electron beam current $i(t)$, which is typically linked to the video-signal voltage $v(t)$ by a power-law relationship $i(t) \sim (v(t) - v_0)^\gamma$. The "gamma corrected" video voltage $v_\gamma(t) \sim i(t)$ used here is strictly speaking not the actual video voltage supplied by a graphics adapter to the monitor. It is a hypothetical voltage that is proportional to the beam current and $v_\gamma(t) = 1$ V shall represent the maximum intensity. This way, we can quantify the phosphor impulse response of a monitor without having to measure the beam current.

IEEE COMPUTER SOCIETY

overall afterglow of the phosphor lasts typically more than a thousand pixel times, a noticeable drop of luminosity also occurs within a single pixel time. This preserves enough high-frequency content of the video signal in the emitted light to allow for the reconstruction of readable text.

4. Characterization of phosphor decay times

The exact shape of the decay curve of the phosphors used in the CRT is an important factor for the image quality that the eavesdropper can obtain:

- It determines the frequency characteristic of the phosphor, which shows how much the high-frequency content of the video signal will be attenuated before appearing in the emitted light.
- It determines the initial luminosity during the first pixel time, which is a characteristic parameter for estimating how strong the received signal will be against the shot noise due to background light.
- It is needed as a parameter for the deconvolution operation that the eavesdropper can use to reconstruct the original image.

Every bright pixel of a CRT surface is hit by an electron beam of typically up to 100 μA for time $t_\mathrm{p} = f_\mathrm{p}^{-1}$, and this refresh is repeated once each time interval f_v^{-1}, where f_p and f_v are the pixel-clock and vertical-deflection frequency, respectively. The beam electrons push other electrons in the phosphor material to higher energy levels. As they fall back into their original position, they emit stored energy in the form of photons. The time delay in this process causes an afterglow for several milliseconds after the electron beam has passed by.

The user manual of the VGA CRT color monitor [10] that I used in the measurements described in the following identifies its phosphor type simply as "P22". This is an old and obsolete designation referring to an entry in an early version of the *Electronic Industries Alliance (EIA)* phosphor type registry. It merely describes the entire class of phosphors designed for color TV applications.

The more modern *Worldwide Type Designation System (WTDS)* for CRTs [12] calls the old P22 family of phosphors "XX" instead and distinguishes subclasses. The most recent EIA TEP-116-C phosphor type registry [13] lists seven different color TV RGB phosphor type triples designated XXA (P22 sulfide/silicate/phosphate), XXB (P22 all-sulfide), XXC (P22 sulfide/vanadate), XXD (P22 sulfide/oxysulfide), XXE (P22 sulfide/oxide), XXF (P22 sulfide/oxide modified) and XXG. In addition, it contains partial information on composition, emission spectrum, decay curves and color coordinates for at least 15 further RGB phosphor-type triplets designated XBA, XCA, etc. that were developed for data-display applications and that differ somewhat from the TV standards in their color. Unfortunately, the original manufacturer of the tested monitor has not yet been able to answer my question on which exact P22 variant was used.

CRT screen phosphors are usually based on the sulfides of zinc and cadmium or rare-earth oxysulfides and are activated by additions of dopant elements to determine the color. Most EIA registered XX and X phosphor type triplets use for the red phosphor yttrium oxysulfide doped with europium (Y_2O_2S:Eu), often blended with zinc phosphate doped with manganese ($Zn_3(PO_4)_2$:Mn). The green phosphor is often zinc sulfide doped with copper (ZnS:Cu) and sometimes also with aluminium and/or gold, or zinc silicate doped with manganese and silver (Zn_2SiO_4:Mn,Ag). The blue phosphor is usually zinc sulfide doped with silver (ZnS:Ag) and in some cases also aluminium or gallium.

Like many physical decay processes (e.g., radio activity), the luminosity of a typical excited phosphorescent substance follows an exponential law of the form

$$I_\mathrm{e}(t) = I_0 \cdot \mathrm{e}^{-\frac{t}{\tau}} \tag{4}$$

where I_0 is the initial luminosity right after the excitation ceases and the time constant τ is the time in which the luminosity drops by a factor e ($= 2.718$). Such decays can be identified easily in a plot of the logarithm of the luminosity over time as a straight line. For

$$\tau = \frac{1}{2\pi f} \tag{5}$$

the above exponential decay is also the impulse response of a first-order Butterworth low-pass filter consisting of a single resistor and capacitor, with a 3-dB cut-off frequency f. As the phosphor decay can be seen as a low-pass filter applied to the video signal before we can receive it with a photosensor, describing the decay in terms of the cut-off frequency is perhaps more illustrative than the time constant.

Zinc-sulfide based phosphors show instead a power-law decay curve of the form

$$I_\mathrm{p}(t) = \frac{I_0}{(t+\alpha)^\beta}. \tag{6}$$

Such a decay behavior can be identified on a plot of the logarithm of the luminosity versus the logarithm of the time since excitation has ceased as an asymptotically straight line that flattens somewhat near $t = 0$. The condition $\beta > 1$ must be fulfilled, otherwise the integral

$$\int_0^\infty \frac{1}{(t+\alpha)^\beta}\,\mathrm{d}t = \frac{\alpha^{1-\beta}}{\beta - 1} \tag{7}$$

which is proportional to the total number of photons emitted would not be positive and finite.

IEEE COMPUTER SOCIETY

Since commonly used phosphors are mixtures of various substances and different excitation modes occur (resulting in various wavelengths), actual decay curves have to be modeled as the sum of several exponential and power-law curves.

The TEP116-C standard provides decay curves for most phosphor types, but these are plotted on a linear time scale extending over many milliseconds. These curves give no indication about the detailed decay during the first microsecond and they are therefore not suitable for estimating the frequency characteristic of the phosphors above 1 MHz. The decay curves published in TEP116-C were measured primarily to provide information about how the phosphor type might affect the perceived flicker caused by the frame refresh. Since suitable fast decay curves or even closed form approximations were not available from the existing CRT phosphor literature, I performed my own measurements on a typical example monitor.

4.1. Instrumentation

We are primarily interested in the rapid decay within a time interval not much longer than t_p, therefore we need a very sensitive light sensor with, ideally, more than 100 MHz bandwidth or less than 5 ns rise and fall time.

One fast light sensor is the PIN photodiode in photoconductive mode, in which a reverse bias voltage is applied and the resulting current is measured. The PIN photodiode has an undoped "intrinsic" layer between the p- and n-doped regions (hence the name). Compared with normal photodiodes, PIN diodes have reduced capacity and can be used with a higher bias voltage, which increases their response time. For example, a PIN diode with a "rise and fall time of about 20 μs" was used in [14] to evaluate the luminance decay of the P31 phosphor in a CRT used in vision research.

Photodiodes are now available with down to 1 ns response time for applications such as optical Gbit/s communication links and laser range finding. However their low sensitivity of typically 0.5 A/W makes significant additional amplification necessary, which would lead to additional noise and further limit the bandwidth. Avalanche photodiodes (APDs) provide greater sensitivity (10^2 A/W) and are also available with 1 ns response times.

Photomultiplier tubes (PMTs) are evacuated electron tubes with a photocathode. Received photons can trigger the emission of electrons, which are then accelerated with high voltage and multiplied in a cascade of further electrodes. A single received photon results in an entire cloud of electrons hitting the anode, contributing to the measured current. Photomultiplier tubes have response times in the nanosecond range and their sensitivity can be adjusted easily over many orders of magnitude.

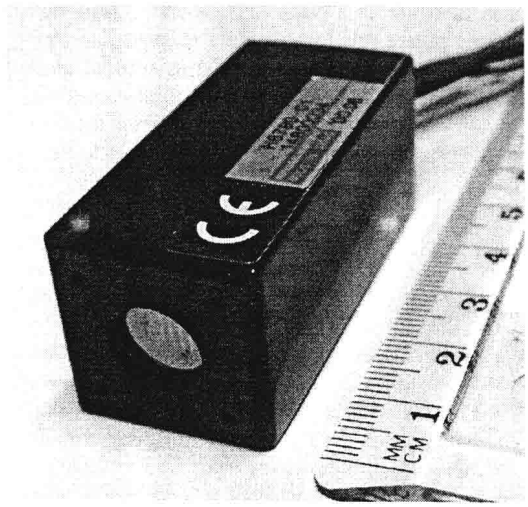

Figure 1. Photomultiplier tube module.

I used a Hamamatsu H6780-01 photosensor module (Fig. 1), which can be operated with radiant sensitivity levels in the 10^1–10^5 A/W range [15]. It can therefore be used under a quite wide range of light conditions. This device consists of a small robust metal package containing a photomultiplier tube and a high-voltage generating circuit. It can be operated conveniently from a 12 V lab power supply. A separately applied 0.25–0.90 V control voltage U_c adjusts the radiant sensitivity of the sensor to

$$1.5 \times 10^5 \text{ A/W} \cdot \left(\frac{U_c}{1 \text{ V}}\right)^{7.2}.$$

The radiant sensitivity is the quotient of the output current generated by the sensor and the radiant energy received by the sensor on its aperture (8 mm diameter). When operated within the specified parameters, a photomultiplier is a highly linear light-controlled current source. To prevent damage to the sensor, care must be taken to ensure that the maximum allowed average output current of 100 μA is not exceeded, by selecting the control voltage appropriately.

According to the data sheet, the anode-current rise time of the H6780 photomultiplier module is 0.78 ns, an order of magnitude faster than the pixel time t_p of commonly used video modes. Its high sensitivity allowed me to connect it directly to the 50 Ω input of a digital storage oscilloscope with a resolution of 40 μV.

4.2. Measurement method

In order to characterize phosphor response times, I used several test video signals that showed either a single pixel or a 320-pixel-long horizontal line, each in full intensity red,

IEEE COMPUTER SOCIETY

green, blue, or white on a black background. Using both short and long pulses provides the data necessary to characterize very fast (tens of nanoseconds) as well as much slower (millisecond) features. The signal timing used was the VESA 640×480@85Hz video mode, in which the electron beam traverses a 320 mm wide screen with 18 km/s.

The decay curves of zinc-sulfide based phosphors can vary significantly under different drive conditions [16]. The EIA standard for the characterization of CRT phosphor decay times [11] therefore requires for measurements a fixed beam current of 100 μA. Lacking the equipment to measure such a current directly at the high-voltage anode connection, I simply used a default setting of monitor controls (100% contrast, 50% brightness, color temperature 6500 K, monitor powered up for at least 30 min) and the full intensity color combinations that are most frequently used for text display. The resulting luminosity measurement is therefore with respect to a known video signal voltage, not a beam current.

Placed 0.25 m in front of the center of the screen surface with an aperture of 50 mm^2, the photosensor, as seen from a pixel, covered a solid angle of around 0.8 msr. The oscilloscope that recorded the photosensor signal was triggered from the vertical sync signal on pin 12 of the feature connector of the driving VGA card. It recorded with 8-bit resolution at a sampling rate of 5 GHz over 40 μs the single-pixel signal and with 125 MHz over 2 ms the 320-pixel line. Averaging each signal over 256 frame repetitions reduced noise.

4.3. Results

Taking into account the solid angle covered by the photo sensor, its exact control voltage and resulting radiant sensitivity, as well as the input impedance of the oscilloscope, the recorded voltage can be converted into a radiant intensity (power per solid angle). The radiant sensitivity used is the one given in the sensor data sheet for 420 nm (blue) and can vary for up to a factor of two for other wavelengths. Because of this, and since no calibration source for radiant intensity was available, the resulting absolute values should only be seen as estimates. Figure 2 shows as an example the measured light output of the blue phosphor as well as the video input signal.

For further theoretical analysis as well as for optimizing the processing of signals for best readability, it is helpful to have a simple closed-form approximation of the phosphor impulse response. I manually adjusted the coefficients and number of terms in a sum of several exponential and power-law decay functions until the convolution of the resulting function with the video signal closely fitted the recorded photosensor output on a number of linear, logarithmic and double-logarithmic plots. This semi-manual fitting process

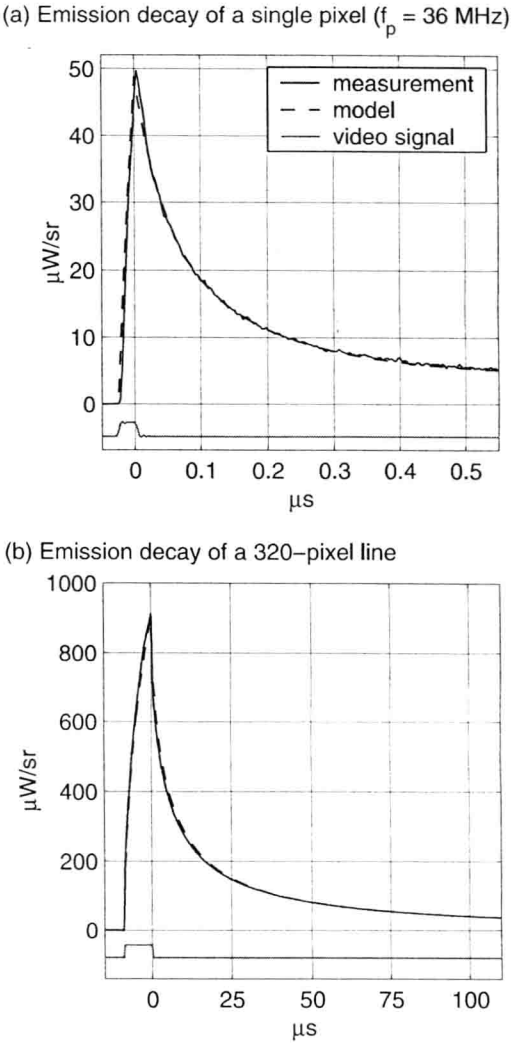

Figure 2. Blue phosphor decay measurement.

led to compacter and more accurately fitting impulse response functions than various parameter fitting algorithms that I tried.

I ended up with the following closed form approximation for the impulse response of the three phosphors:

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

IEEE COMPUTER SOCIETY

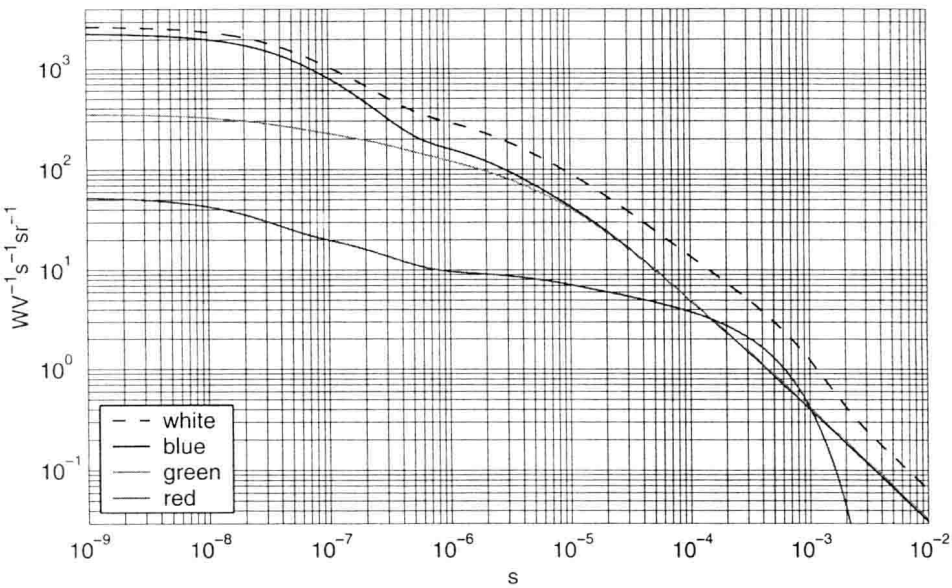

Figure 3. The numeric model of the measured P22 phosphor impulse response.

$$P_{\mathrm{P22G}}(t) \,/\, \frac{\mathrm{W}}{\mathrm{V}\cdot\mathrm{s}\cdot\mathrm{sr}} = 210\times10^{-6}\times\left(\frac{t+5.5\ \mu\mathrm{s}}{1\ \mathrm{s}}\right)^{-1.1} + 37\times\mathrm{e}^{-2\pi t\times 150\ \mathrm{kHz}} + 100\times\mathrm{e}^{-2\pi t\times 700\ \mathrm{kHz}} + 90\times\mathrm{e}^{-2\pi t\times 5\ \mathrm{MHz}} \quad (9)$$

$$P_{\mathrm{P22B}}(t) \,/\, \frac{\mathrm{W}}{\mathrm{V}\cdot\mathrm{s}\cdot\mathrm{sr}} = 190\times10^{-6}\times\left(\frac{t+5\ \mu\mathrm{s}}{1\ \mathrm{s}}\right)^{-1.11} + 75\times\mathrm{e}^{-2\pi t\times 100\ \mathrm{kHz}} + 1000\times\mathrm{e}^{-2\pi t\times 1.1\ \mathrm{MHz}} + 1100\times\mathrm{e}^{-2\pi t\times 4\ \mathrm{MHz}} \quad (10)$$

$$P_{\mathrm{P22}} = P_{\mathrm{P22R}} + P_{\mathrm{P22G}} + P_{\mathrm{P22B}} \quad (11)$$

After convolution with the 1 V video signal according to (3) and a delay of 29 ns (transmission times in electron tubes and signal cables), these impulse response functions lead to the excellently matching dashed lines in Fig. 2.

All three phosphors show a very noticeable relative drop of radiant intensity in the first tenth of a microsecond. Figure 3 shows that of all three phosphors, the blue one has with $-1500\ \mathrm{W}/(\mathrm{V}\cdot\mathrm{s}\cdot\mathrm{sr})$ by far the largest drop in absolute intensity in the first 100 ns and therefore will provide the strongest high-frequency signal, while the red phosphor has with $-34\ \mathrm{W}/(\mathrm{V}\cdot\mathrm{s}\cdot\mathrm{sr})$ the smallest absolute drop.

The Fourier transforms of the impulse response curves in Fig. 5 show that the blue phosphor applies to the video signal a low-pass filter in which for example a 10 MHz component is less than 40 dB more attenuated than a 1 kHz signal. Only for frequencies above around 5–10 MHz, the phosphors show the continuous 20 dB per decade roll-off typical for a first order low-pass filter.

Figure 4 shows as continuous lines the impulse response curves on a logarithmic time scale. Their amplitudes have been normalized to $P(0) = 1$ in this representation in order to make the curve forms more comparable. The dashed lines represent the integrals of the decay functions and show which fraction of the totally emitted energy after stimulation ceased has already been given off at any point in time.

The red phosphor, which decays purely exponentially, emits practically all of its stored energy within 1–2 ms, but it still has not lost a significant part of its energy within the first 10 μs. The blue and green phosphors show a far more heavy-tailed behavior, thanks to the power-law component in their impulse response. Even long after the stimulus, they still have not emitted all of their stored energy and as a result, even an unaided human observer with fully adapted scotopic vision can notice an afterglow on a CRT screen in an otherwise completely dark room for several minutes.

It might be worth noting that the integral of $P_{\mathrm{P22G}}(t)$ shows even hours after the excitation some unreleased energy in this phosphor type. Although this measurement was not designed to estimate the here significant parameter β

IEEE COMPUTER SOCIETY

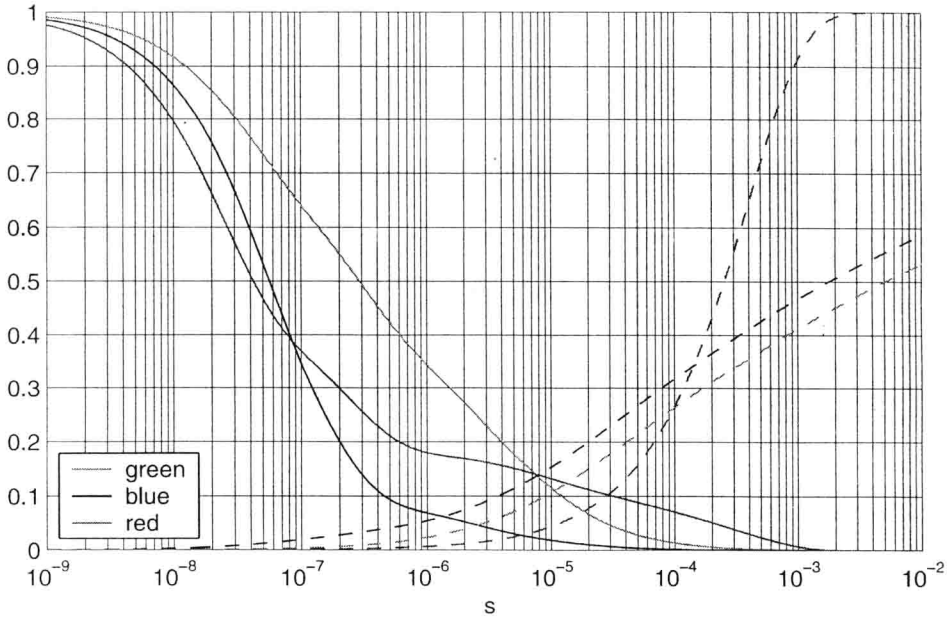

Figure 4. Normalized linear intensity impulse response curves and corresponding integrals (dashed).

in (6) with good accuracy, this observation still leads to the question whether CRT phosphors could leak confidential information not only via instantaneous compromising emanation, but also via data remanence.

5. Optical eavesdropping demonstration

Perhaps more interesting than a theoretical discussion of phosphor decay frequency characteristics is a visually convincing actual reconstruction of a displayed image from an out-of-sight CRT surface.

In the following experiment, the same monitor (Dell D1025HE) faces a white office wall at around a meter distance. The photomultiplier is now located behind the monitor, facing the same wall at around 1.5 m distance. There is no direct line of sight between the sensor and the screen surface.

As the wall illuminated by the monitor covers a large solid angle as seen from the photosensor, no additional optical elements such as a focusing lens are needed in this demonstration. The experiment was performed at night with the room lights switched off, however the room was far from completely dark, being illuminated by several computer displays and stray light from outside lamps.

Figure 6 shows a simple readability test chart with text in various sizes, which the monitor displayed as the target video signal during the test. This test image was displayed in the same video mode as before (VESA 640 × 480@85Hz). The text is in full white on black, and additional test letters show all full intensity combinations of the three phosphor colors. The oscilloscope averaged 256 frames (or equivalently 3 s of signal) at a sampling frequency of 250 MHz. (These exact parameters are not critical and quite acceptable readability of small text can also be achieved with lower sampling rates and numbers of averaged frames as well as higher video modes.)

Figure 7 shows the recorded and averaged photocurrent as a gray-scale image, much like a monitor driven with appropriate sync pulses would present it. The largest font sizes are readable, though the slow decay smears the luminosity of each white pixel along the path of the electron beam across the rest of the line and further. The gray values of all the rastered signals shown here were adjusted such that the values of the 0.1% highest and 0.1% lowest pixels in a histogram are all mapped to full white or full dark respectively, and the remaining values are linearly mapped to the corresponding points on a gray scale.

The raw photomultiplier current in Fig. 7 clearly has to be processed further in order to make text readable. Analog preprocessing has the advantage that it can improve significantly the signal-to-noise ratio before any amplification and quantization steps limit the dynamic range of the sig-

IEEE COMPUTER SOCIETY

此为试读,需要完整PDF请访问: www.ertongbook.com