# Information Leakage from Optical Emanations

JOE LOUGHRY
Lockheed Martin Space Systems
and
DAVID A. UMPHRESS
Auburn University

A previously unknown form of compromising emanations has been discovered. LED status indicators on data communication equipment, under certain conditions, are shown to carry a modulated optical signal that is significantly correlated with information being processed by the device. Physical access is not required; the attacker gains access to all data going through the device, including plaintext in the case of data encryption systems. Experiments show that it is possible to intercept data under realistic conditions at a considerable distance. Many different sorts of devices, including modems and Internet Protocol routers, were found to be vulnerable. A taxonomy of compromising optical emanations is developed, and design changes are described that will successfully block this kind of "Optical TEMPEST" attack.

Categories and Subject Descriptors: C.2.0 [**Computer Systems Organization**]: COMPUTER-COMMUNICATION NETWORKS—*General, Security and protection (e.g., firewalls)*; D.4.6 [**Software**]: OPERATING SYSTEMS—*Security and Protection, Invasive software (e.g., viruses, worms, Trojan horses)*; E.3 [**Data**]: DATA ENCRYPTION—*Code breaking*; K.6.5 [**Computing Milieux**]: MANAGEMENT OF COMPUTING AND INFORMATION SYSTEMS—*Security and Protection, Unauthorized Access (e.g., hacking, phreaking)*

General Terms: Compromising emanations, Emissions security, Experimentation

Additional Key Words and Phrases: Information displays, light emitting diode, LED, fiber optics, encryption, compromising emanations, covert channel, communication, COMINT, COMSEC, EMSEC, SIGINT, TEMPEST

## 1. INTRODUCTION

Can optical radiation emitted from computer LED (light emitting diode) status indicators compromise information security? Data communication equipment, and even data encryption devices, sometimes emit modulated optical signals that carry enough information for an eavesdropper to reproduce the entire data stream being

Much of this work was done while the first author was a graduate student in the Department of Computer Science and Software Engineering at Seattle University.
Authors' addresses: Joe Loughry, Lockheed Martin Space Systems, Dept. 3740, Mail Stop X3741, P.O. Box 179, Denver, Colorado 80122 USA, email joe.loughry@applied-math.org; David A. Umphress, Auburn University, Department of Computer Science and Software Engineering, 215 Dunstan Hall, Auburn University AL 36849 USA, email umphress@eng.auburn.edu.
Permission to make digital/hard copy of all or part of this material without fee for personal or classroom use provided that the copies are not made or distributed for profit or commercial advantage, the ACM copyright/server notice, the title of the publication, and its date appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee.

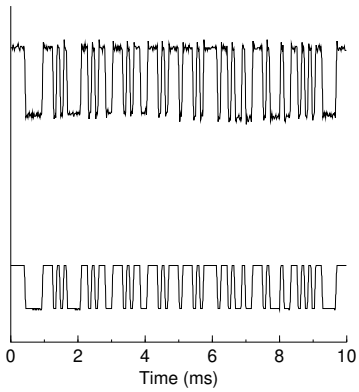


Fig. 1. Compromising optical emanations. The lower trace shows the ±15V EIA/TIA-232-E input signal (at 9600 bits/second); the upper trace shows optical emanations intercepted 5 m from the device.

processed by a device. It requires little apparatus, can be done at a considerable distance, and is completely undetectable. In effect, LED indicators act as little free-space optical data transmitters, like fiber optics but without the fiber.

Experiments conducted on a wide variety of devices show evidence of exploitable compromising emanations in 36% of devices tested. With inexpensive apparatus, we show it is possible to intercept and read data under realistic conditions from at least across the street. In Figure 1, the lower trace shows the ±15V EIA/TIA-232-E waveform of a serial data signal at 9600 b/s. The upper trace shows modulated optical radiation intercepted 5 m from the device. A high correlation is evident.

We have successfully recovered error-free data at speeds up to 56 kb/s; the physical principles involved ought to continue to work up to about 10 Mbits/s. Protecting against the threat is relatively straightforward, but may require design changes to vulnerable equipment.

### 1.1 Paper Organization

The first part of this paper reviews the idea of compromising emanations, and gives an overview of what information is to be found in the literature. Next comes a technical explanation of why compromising optical emanations exist, together with some of their properties. A series of experiments is then described, along with results that were found. Finally, some possible countermeasures are discussed, along with directions for future work. Related work on active attacks using optical emanations is presented in the appendices.

## 2. EMSEC, TEMPEST, AND COMPROMISING EMANATIONS

> **Compromising Emanations** [National Computer Security Center 1988]: "Unintentional data-related or intelligence-bearing signals that, if intercepted and analyzed, disclose the information transmi[tted], received, handled, or otherwise processed by any information processing equipment. See *TEMPEST*."

Thorough discussion of compromising emanations and EMSEC (emissions security) in the open literature is limited. The information that is available tends to exhibit a strong bias toward radio frequency (RF) emanations from computers and video displays. Because of the high cost of equipment and the difficulty of intercepting and exploiting RF emanations, reports of successful attacks against emanations have been limited primarily to high-value sources of information such as military targets and cryptologic systems. A significant problem is that much important information on compromising emanations is classified [Russell and Gangemi 1991], although some documents have recently been declassified [National Security Agency 1992; 1995; 1994].

### 2.1 Related Work

The ability to compromise signals emanating from computers has been known for some time. For instance, Smulders [1990] found RF emanations in unshielded or poorly shielded serial cables, and van Eck [1985] showed that cathode-ray tube video displays can be read at a distance by intercepting and analyzing their RF emanations. Others have noted RF compromise, including more contemporary research showing ways to hide information in signals emitted by video devices as well as specialized fonts that minimize compromising RF emanations [Kuhn and Anderson 1998]. Wright [1987] described, anecdotally, the discovery of electrically conducted compromising emanations from cipher machines as early as 1960. For an excellent overview of the current state of emanations security research, the interested reader is referred to the book by Anderson [2001] and a related paper by Kuhn and Anderson [1998].

Until recently, little mention of signals in the optical spectrum was found in the literature. Kuhn [2002] has demonstrated remotely reading CRT displays from diffuse optical emanations, without requiring line-of-sight access. Other related topics include security of fiber optics [Hodara 1991; EXFO Electro-Optical Engineering, Inc. 1999] and optical communications [Wilkins 1641]. Social engineering attacks such as "shoulder surfing" and visual surveillance of video displays are well covered in [Fites and Kratz 1993]. Free-space optical data links are prone to interception, and for this reason wireless data links (both laser and RF) are typically encrypted [Lathrop 1992]. But with the exception of a work of fiction, in which one character uses the LEDs on a computer keyboard[1] to send information in Morse code [Stephenson 1999], and inferences from redacted sections of partially declassified documents [National Security Agency 1992], a thorough search of the literature revealed no direct mention of the risk of interception of data from optical emanations of LED status indicators.

## 3. COMPROMISING OPTICAL EMANATIONS

> *"The [IBM] 360 had walls of lights; in fact, the Model 75 had so many that the early serial number machines would blow the console power supply if the 'Lamp Test' button was pressed."* [Morris 1996]

[1]See also Appendix A.

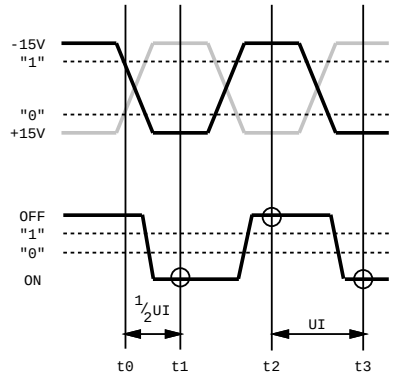


Fig. 2. EIA/TIA-232-E serial data waveform and typical LED response.

### 3.1 Light-Emitting Diodes

Light-emitting diodes are cheap, reliable, bright, and ubiquitous. They are used in nearly every kind of electronics, anywhere a bright, easy-to-see indicator is needed. They are especially common in data communication equipment. Every year, some 20–30 billion LEDs are sold [Perry 1995].

LEDs are very fast; that is, they exhibit a quick response to changes in the applied drive voltage (tens of nanoseconds). In fact, common visible LEDs are fast enough that a close cousin is used as a transmitter in fiber optic data links at speeds in excess of 100 Mbits/s [Hewlett–Packard Company 1993b].

Although fast response time is oftentimes a desirable quality in a display, LEDs are fast enough to follow the individual bit transitions of a serial data transmission. Herein lies the problem: if certain LED indicators are visible to an attacker, even from a long distance away, it becomes possible for that person to read all of the data going through the device.

One of the advantages of LED displays is that they can be read from across a room. The disadvantage may be that they can be read from across the street.

### 3.2 Rationale for the Existence of Compromising Optical Emanations

The brightness of LED displays would not be a problem if it were not for the way they interact with serial data transmissions. Consider the idealized EIA/TIA-232-E waveform and associated LED response curve depicted in Figure 2. The upper waveform shows the EIA/TIA-232-E serial data signal; the lower waveform illustrates the optical output of an LED indicator monitoring that signal. As long as the rise time of the LED is less than $\frac{1}{2}$ of the unit interval $t_{\mathrm{UI}}$, the LED will accurately enough mirror the EIA/TIA-232-E data signal at the critical points shown by the small circles in the diagram to enable recovery of the original data.

The EIA/TIA-232-E standard (formerly known as RS-232) defines a bit-serial format using bipolar encoding and non-return-to-zero–level (NRZ–L) signaling [Electronic Industries Association, Engineering Department 1991]. As illustrated in Figure 3, bits are transmitted asynchronously, with framing bits embedded in the serial data stream for synchronization between sender and receiver. During peri-

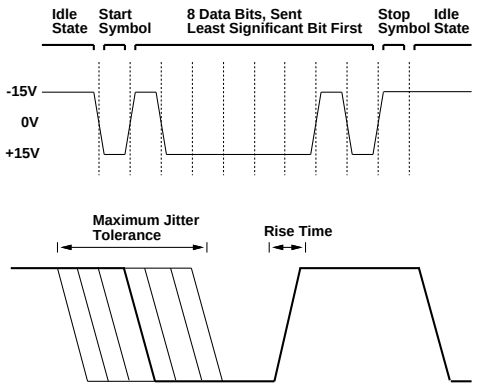


Fig. 3. EIA/TIA-232-E serial data waveform and maximum jitter tolerance from TIA/EIA-404-B.

ods when no data are being transmitted, the transmitter remains in the logical "1" state. The start of a new symbol is indicated by a momentary excursion to the logical "0" state for one unit interval, called the *start bit*. This is followed by a serial waveform consisting of a mutually agreed-upon number of data bits, sent least significant bit first. Following the last data bit, the transmitter returns to the logical "1" state for at least one unit interval, called the *stop bit*, in order to provide necessary contrast for the receiver to recognize the beginning of the next start bit. (Another way of looking at this is that the channel is required to return to the idle state for at least one unit interval between characters.)

EIA/TIA-232-E uses bipolar encoding, with a negative voltage signifying logical "1" and a positive voltage used for logical "0" [Black 1996]. Usually, LEDs are wired to light up for a logical "0" so that they flicker when bits are transmitted, and remain dark when the channel is idle. The fact that the original signal is bipolar is immaterial. As long as the LED is fast enough to faithfully reproduce the timing of bit transitions, the optical output will contain all of the information in the original EIA/TIA-232-E signal.

LEDs cannot be connected directly to logic circuits, as they would draw too much power from the signal source. For reasons of cost, however, the very same high-speed gates (usually TTL or CMOS inverters) typically used to construct logic circuits are also employed to power the LEDs [Lancaster 1980]. The result is a direct path allowing information to flow from the serial data channel to the optical output of the LED. Because the monitoring circuit was not designed for the purpose, the resulting optical signal may exhibit noise or other degradation, but LEDs and their associated driver circuitry are generally more than fast enough to reproduce a serial data signal at normal data rates.

3.2.1 *Characteristics of the Optical Signal.* NRZ–L signals are susceptible to noise, which is why other signaling methods, such as differential Manchester encoding, are most often used in long-distance digital communication systems. To overcome the noise sensitivity of NRZ–L, additional redundancy is often introduced into the communication channel in the form of *channel encoding* [Proakis and Salehi 1994]. Parity checks, cyclic redundancy checking (CRC), and other error detection

Table I. Proposed classification system for optical emanations.

| Type | Correlated to | Associated Risk Level |
|---|---|---|
| Class I | State of the device | Low |
| Class II | Activity level of the device | Medium |
| Class III | Content (data) | High |

and correction methods may be used to increase the reliability of the system. But it should be noted that these features are also available to an eavesdropper, who may use them to overcome the effects of a poor optical signal.

As optical communication systems go, it must be recognized that LED status displays are highly sub-optimal. There are no beam-forming optics on the transmitting LED. The radiant flux available is extremely limited. Buffer circuits used to drive LED indicators, while more than fast enough for their intended purpose, are not optimized for high-speed data transmission in the way that special-purpose circuits used in fiber optic transmitters are. Practical optical data communication systems use laser transmitters, sophisticated encoding schemes, and coherent detectors that greatly improve signal recovery under noisy conditions [Gagliardi 1995]. Our hypothetical eavesdropper would likely have to deal with off-axis aiming errors, high levels of optical background noise from artificial lighting, and lack of a priori knowledge of the specific bit rate and word length used by the target. Nevertheless, our experiments show that with a sensitive detector and telescopic optics, it is possible for an eavesdropper to recover a noisy analog waveform closely approximating the original digital data stream. Once the received optical signal has been amplified, cleaned of noise, and fed to a USART (Universal Synchronous-Asynchronous Receiver-Transmitter)—an inexpensive chip which serves as a ready-made solution to the problem of decoding a noisy signal—the original data stream is easily recovered.

3.2.2 *Insensitivity to the Modulation Scheme Employed.* High-speed modems employ a variety of complicated modulation schemes, including frequency, amplitude, and phase modulation to maximize available bandwidth on voice-grade telephone lines. But this makes no difference—it is the relatively simple NRZ–L waveform of the EIA/TIA-232-E data signal that is modulated onto the LED.

3.2.3 *Nonsusceptibility of Other Light Sources.* Questions remain as to the susceptibility of non-LED sources to interception of compromising optical emanations. Liquid crystal (LCD) displays, in particular, exhibit a relatively slow impulse response, typically on the order of tens of milliseconds, making these displays relatively poor sources of compromising optical emanations, except at fairly low data rates. Cathode ray tube (CRT) displays, however, at the pixel level, are very fast, and have been shown to be vulnerable even to non-line-of-sight optical emanations [Kuhn 2002].

### 3.3 Classification of Optical Emanations

It is useful to consider a division of optical emanations into three broad classes according to the amount of information potentially carried to an adversary. The

proposed taxonomy is shown in Table I. In the list that follows, LED indicators that exhibit Class $n$ behavior are called Class $n$ indicators.

The classifications are:

—**Class I** indicators, which are unmodulated. The optical emanations put out by this type of display are constant, and correlated with the *state* of a device or communication channel. Class I indicators communicate at most one bit of information to an observer. An example would be a power-on indicator.

—**Class II** indicators are time-modulated, and correlated with the *activity level* of a device or communication channel. Class II indicators provide an adversary with considerably more information than Class I indicators do. On face value, while the content of the data being processed by a device is not known, the fact that something is being transmitted, and a rough idea of where and how much, together make possible *traffic analysis* of interesting targets. Examples of Class II indicators include the `Work Station Active` light on an IBM 5394 Control Unit, activity indicators on Ethernet interfaces, and the front-panel lights of a Cisco router. It is important to note that by affecting the activity level of a device, and hence modulating the output of a Class II indicator, it is possible for an attacker to implement a covert timing channel.

—**Class III** optical emanations are modulated optical signals that are strongly correlated with the *content* of data being transmitted or received. If the correlation is sufficiently good, then from analysis of Class III optical emanations it is possible to recover the original data stream. Examples of Class III emanations are surprisingly common; the "Transmitted Data" and "Received Data" indicators on modems are usually Class III.

Devices having at least one Class II indicator, but no Class III indicators, are called Class II devices; any device having at least one Class III indicator is a Class III device. Class III devices are the most interesting.

Note that in both the Class I and Class II cases, the adversary gets no more information than the operator does; the indicator is being used in the manner for which it was intended, except that the eavesdropper is unauthorized, and reading the information at a distance.

Class III devices may arise when the designer of a device inadvertently specified a Class III indicator where a Class II indicator was needed. It is not clear whether there is *any* situation in which a Class III indicator would be warranted, except in the case of an extremely low-speed communication channel, where individual bit transitions could be observed by eye and decoded. In most cases the activity of a data communication channel occurs too fast for the human eye to follow. In the real world, an oscilloscope is a much more useful tool than a Class III indicator.

Potentially dangerous Class III indicators can be converted to the safer and more useful Class II type by the addition of a pulse stretching circuit, as described in Section 6 on Countermeasures below.

## 4. EAVESDROPPING EXPERIMENTS

Three series of experiments were run. First, a survey was made of a large number of devices, looking for evidence of Class III behavior. Then, long-range testing was done on a selection of devices, to prove the feasibility of interception under realistic

conditions. Finally, examination was made of the internals of several devices, in an attempt to understand why these emanations occur.

### 4.1 Hypothesis

The null hypothesis was stated as follows: "It is not possible to recover data from optical emanations." The null hypothesis was disproved by experiment.

### 4.2 Experimental Design and Methodology

A total of 39 devices containing 164 unique LED indicators were identified for this study. The devices selected for testing were chosen to represent a wide variety of information processing technology, including low-speed and high-speed communication devices, local-area network (LAN) and wide-area network (WAN) devices, PC and mainframe computers, mass storage devices, and peripherals.

Prior to commencement of measurements, radiometric readings were taken on an optical bench of a standard red LED driven by a square wave signal. These measurements were used to establish a baseline. Following this step, each of the 164 LED indicators identified in the survey was examined for evidence of Class III behavior.

Measurements were made of individual LED indicators by placing a hooded detector in contact with each LED. A dual-trace oscilloscope was used to observe the signal from the detector. To visualize the corresponding data stream, a breakout box was inserted into the data path, with the original data displayed alongside the optical signal from the detector.

The detector used was a high-speed, large-area silicon PIN (Positive–Intrinsic–Negative) photodiode with an active area of 1 $mm^2$. The responsivity of this detector is 0.45 A/W at a nominal wavelength of 830 nm, with a spectral response of 350–1100 nm. The photocurrent from the detector was amplified by a transimpedance photodiode amplifier operated in zero-bias mode. Signals were observed with a 200 MHz digital oscilloscope, and captured for later analysis.

The bandwidth of the photodiode amplifier is inversely proportional to its gain setting; at a gain factor of $10^7$ V/A, the bandwidth of the detector–amplifier system is only 10 KHz. Therefore, for most measurements, the amplifier was operated at a gain setting of $10^4$ V/A, yielding an overall detector–amplifier system bandwidth of 45 KHz, which was marginal, but adequate. For higher-speed measurements, the photodiode was connected directly to the input amplifier of the oscilloscope and operated in the quadrant IV (photovoltaic) region. Limited sensitivity in this configuration is what necessitated placing the detector directly in contact with the LED. However, the greatly increased bandwidth of the detector–amplifier system in this configuration allowed for examination of very high speed devices for evidence of signals in the MHz range.

4.2.1 *Long-Range Testing.* Long-range optical eavesdropping experiments were conducted with a small number of representative devices. The ANP Model 100 short-haul modem, Hayes Smartmodem OPTIMA 9600 and 14400, and a Practical Peripherals PM14400FXMT fax modem were all examined.

The same photodetector and amplifier system described in the previous section was used. The detector was mounted at the focus of an optical system consisting of

a 100 mm diameter, $f/2.5$ converging lens, an aperture stop, and a 650 nm optical bandpass filter, chosen to match the spectral output of a standard visible red LED [Agilent Technologies 1999].

The device under test was placed a measured distance away, and connected to an identical unit at the test station through a length of unshielded twisted pair cable. The image from a single LED on the device under test was adjusted to completely cover the detector's active area. Test transmissions were made to each device, and the EIA/TIA-232-E waveform and resulting optical signals captured for analysis.

4.2.2 *Experimental Methodology.* Three independent variables and one dependent variable were identified. The independent variables were: (1) the separation distance between the detector and the device under test, (2) the data transmission rate, and (3) ambient lighting conditions on the test range. The dependent variable was the correlation between the received optical signal and the original EIA/TIA-232-E waveform captured at the same time. The independent variables were varied according to a formal test matrix. Separation distance was varied from 5 m to 38 m (the maximum dimension of the laboratory) in increments of 5 m during the test. At each measured distance, test transmissions were made at data rates of 300, 600, 1200, 2400, 4800, 9600, and 19 200 bits/s.

For simplicity, symbols in the optical signal were detected by observing the signal's amplitude at one-half of the unit interval after the NRZ–L transition. Because this was a proof-of-concept experiment, actual bit-error rates were not measured. The optical waveform from the detector amplifier was compared to the original EIA/TIA-232-E signal waveform obtained from a breakout box inserted in the data path between the data generator and the device under test. After each series of measurements over the full range of distances, the ambient lighting conditions on the test range were changed. Lighting conditions tested included daylight office conditions (i.e., sunlight coming through windows, plus artificial light), normal fluorescent office lighting, nighttime office lighting (scattered fluorescent lights plus some light entering through windows from the streetlights outside), and a darkened, windowless conference room. An optical bandpass filter was used in some tests in an attempt to reduce the level of background radiation and determine if detector overload was an important factor. All tests were conducted indoors.

### 4.3 Experimental Results

Results of the survey of devices are shown in Table II. Of 39 devices tested, 14 showed evidence of Class III optical emanations at the tested bit rate.

4.3.1 *Results of the Survey of Devices.* Dial-up and leased-line modems were found to faithfully broadcast data transmitted and received by the device. Only one device of this type did not exhibit Class III emanations: the Practical Peripherals PM14400FXMT fax modem. The shortest pulse duration measured from this device was 20 ms, even at high data rates.

None of the LAN interface cards tested, including 10 Mbits/s Ethernet and 16 Mbits/s Token Ring adapters, were found to broadcast any recognizable data. Examination of the data sheet for a chipset used in fiber optic Ethernet devices reveals a possible reason for this finding. According to [Hewlett–Packard Company 1993a], LED drivers for `transmit`, `receive`, and `collision` indicators are filtered through

Table II. Results of a survey of 39 devices.

| *LED Indicator* | *Class I* | *Class II* | *Class III* |
|---|---|---|---|
| **Modems and Modem-Like Devices** | | | |
| ANP Model 100 short-haul modem, `TD` indicator | | | • |
| ANP SDLC card, `TD` indicator | | | • |
| CASE/Datatel DCP3080 CSU/DSU, `TD` indicator | | | • |
| Hayes Smartmodem OPTIMA 14400, `SD` indicator | | | • |
| Hayes Smartmodem OPTIMA 9600, `SD` indicator | | | • |
| Motorola Codex 6740 `Hex TP` card, `TD` indicator | | | • |
| Motorola Codex 6740 `TP Proc` card, `TD` indicator | | | • |
| MultiTech MultiModem V32, `TD` indicator | | | • |
| Practical Peripherals PM14400FXMT fax modem, `TX` and `RX` indicators | | • | |
| SimpLAN IS433-S printer sharing device, front panel LEDs | | | • |
| Telemet SDR-1000 Satellite Data Receiver, `Data` indicator | | | • |
| V.32bis modem simulator, `TD` indicator | | | • |
| **LAN Devices** | | | |
| 3Com TokenLink III Token Ring LAN card, `Link` indicator | • | | |
| Cabletron TRXI-24A Token Ring hub, `Activity` indicator | | • | |
| Ethernet NIC, unknown manufacturer, backplane LED | • | | |
| Ethernet AUI, unknown manufacturer, `Link` indicator | | • | |
| Ethernet AUI, unknown manufacturer, `Receive` indicator | | • | |
| Ethernet AUI, unknown manufacturer, `Transmit` indicator | | • | |
| Synoptics 2715B Token Ring hub, `Link` indicator | • | | |
| **WAN Devices** | | | |
| Cisco 4000 IP router, Fast Serial `TD` indicator | | | • |
| Cisco 4000 IP router, front panel LED | | • | |
| Cisco 7000 IP router, Fast Serial `TD` indicator | | | • |
| Cisco 7000 IP router, front panel LED | | • | |
| Stratacom IPX SDP5080A, `RXD` indicator | | • | |
| Verilink FT1 DSU/CSU, `Pulses` indicator | | • | |
| Westel 3110-30 DS1 Connector, `Pulses` indicator | | • | |
| **Storage Devices** | | | |
| 2x CD-ROM drive, unknown manufacturer, activity LED | | • | |
| Compaq Proliant hot-swappable disk array, activity LED | | • | |
| Compaq Proliant server, floppy drive LED | | • | |
| IBM 4702 controller, $5\frac{1}{4}$-inch floppy drive LED | | • | |
| IBM 4702 controller, hard disk activity LED | | • | |
| IBM 8580 computer, disk activity indicator | | • | |
| PC, unknown manufacturer, hard disk LED | | • | |
| **Miscellaneous Devices** | | | |
| Hewlett-Packard LaserJet 4 laser printer, `Ready` indicator | | • | |
| IBM 3745 Front-End Processor, console LEDs | • | | |
| IBM 4019 Laser Printer, `Buffer` indicator | | • | |
| IBM 5394-01B Control Unit, `Work Station Active` LED | | • | |
| IBM AS/400 Model 9406, `Processor Activity` indicator | | • | |
| WTI POLLCAT III PBX Data Recorder, `PBX Input A, B` indicators | | | • |

pulse stretching circuits to make their activity more visible. The pulse stretcher extends the *on*-time of LED indicators to a minimum of several milliseconds. This makes short pulses easier to see, but severely limits the bandwidth of the LED from the perspective of compromising optical emanations. All of the Ethernet and Token Ring devices examined showed similar behavior in this regard.

Both of the routers tested (Cisco Series 4000 and 7000 routers equipped with Token Ring, Fast Serial and FDDI Interface Processors) were found to broadcast Class III emanations from the Fast Serial LEDs on their back panels. Front-panel activity indicators, while suggestive of data leakage, typically exhibited a typical minimum pulse width on the order of 20 ms, indicating that the front-panel indicators are merely Class II. None of the LAN devices tested showed any evidence of Class III emanations from LAN traffic.

Two T1 (1.554 Mbits/s) CSU/DSU (Channel Service Unit/Data Service Unit) devices were tested. Neither unit showed evidence of Class III emanations. Lower-speed CSU/DSU devices, however, on 56 kbits/s leased circuits, behaved similarly to dialup modems. All showed usable Class III emanations in both synchronous and asynchronous operation.

Intelligent serial data switches (i.e., printer sharing devices), a satellite data receiver, and a PBX call data recorder behaved similarly to the modems in this test. Data from attached devices showed up in the form of Class III optical emanations on the front panels of all these devices.

Mass storage devices such as hard disks and tape transports are usually equipped with device activity indicators. It was hypothesized that the optical output of these LEDs might be related to data transfers to or from the storage device. A variety of PC and minicomputer hard disk drives, floppy diskette drives, CD-ROM drives and tape transports were tested. None were found to emit anything other than Class II optical emanations.

Miscellaneous devices tested included the `Processor Activity` indicator on an IBM AS/400 computer, the `Work Station Active` indicator on an IBM 5394 terminal controller, and control panel indicators on IBM and Hewlett-Packard laser printers. All of these devices were found to be Class II at most.

No significant difference was found between the observability of 5 mm standard-sized LEDs and the much smaller surface-mount components used in newer devices. The absolute brightness levels of these LEDs are comparable.

4.3.2 *Long-Range Testing.* Results of long-range testing are shown in Figure 4. Note the increasing signal degradation as the distance was varied from 10 m to 30 m from the detector. There is a high correlation evident between the EIA/TIA-232-E waveform and the received optical signal, as shown in Figure 5. For comparison, the correlation between the upper trace of the first part of Figure 4 and a random signal of similar amplitude to the optical signal was found to be $-0.02558$.

No difference was seen at faster bit rates. Interestingly, several devices continued to emit a recognizable optical signal at data rates exceeding the rated capability of the device. Despite high noise levels in the recorded waveforms, due apparently to a combination of detector shot noise and thermal noise in the amplifier, signals were intercepted and properly decoded at a distance.

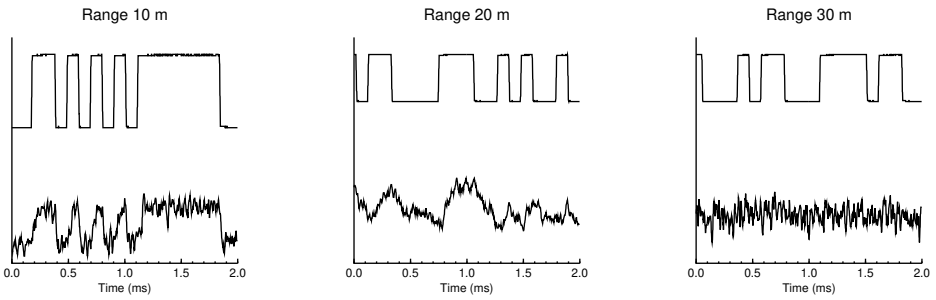


Fig. 4. Degradation of the optical signal with increasing distance from the target Data rate was 9600 bits/s.

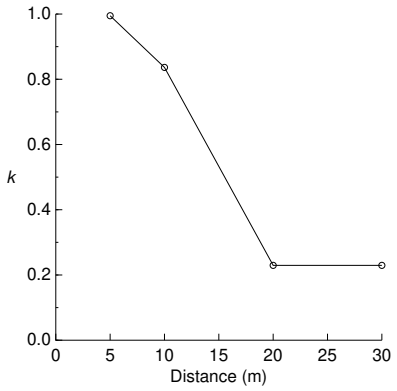


Fig. 5. Observed correlation $k$ between the original EIA/TIA-232-E data signal (9600 bits/s) and the received optical signal for distances of 5 m, 10 m, 20 m, and 30 m. This is from the data of Figures 1 and 4.

4.3.3 *Reverse Engineering of Devices.* It appears that some types of data encryption devices, in particular standalone data encryptors and modems with built-in link encryption capability, may emit optical signals in unencrypted form.

Figure 6 is a detail taken from the *Installation and Operation Manual* for the Paradyne InfoLock model 2811-11 DES encryptor. The InfoLock 2811 is a standalone DES (Data Encryption Standard) link encryptor of the type used by financial institutions to encrypt data on their wire transfer and ATM (automated teller machine) networks [Paradyne Corporation 1985].

The figure shows a portion of the data path between the DTE connector (Data Terminal Equipment—the side of the encryptor that connects to a computer) through the encryption function, to the DCE connector (Data Communications Equipment—the side that connects to a modem). The DTE, or *red* side is unencrypted; the DCE, or *black* side is encrypted [United States Department of Defense 1987]. It is clear from this diagram that LED indicators on the `TXD` and `RXD` (transmitted and received data, respectively) are on the red side of the InfoLock 2811. This is a serious design flaw. The LEDs will display all of the data passing through the device (in either direction) in its unencrypted, or plaintext form.

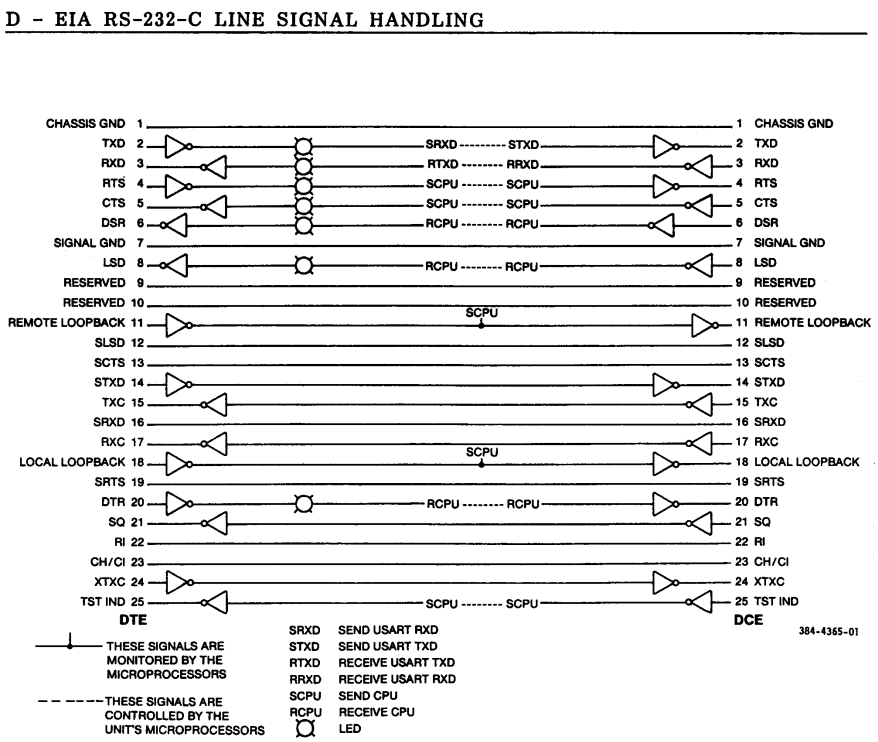


**Figure D-1. RS-232-C Line Signal Handling Level-One Signals**

Fig. 6. Detail from *Installation and Operation Manual* for the InfoLock 2811-11 DES encryptor.

It is believed that any link encryption device with LED indicators may potentially contain this flaw. Modems with built-in link encryption are probably vulnerable as well. Stand-alone data encryptors like the InfoLock 2811 will protect downstream equipment on the black side, but are vulnerable to compromising optical emanations themselves. The failure mode results in leakage of cleartext. The determination of whether or not a particular encryption unit is vulnerable will require examination of the internals of each device.

## 5. INTERPRETATION OF RESULTS

The null hypothesis was disproved.

Class III emanations were found only in data communication devices, but not all data communication devices examined were found to be Class III. In particular, none of the LAN cards tested were found to exhibit Class III behavior (although most of them were Class II). No data storage device was found to be Class III. The design flaw in the InfoLock 2811 encryption device is particularly interesting.

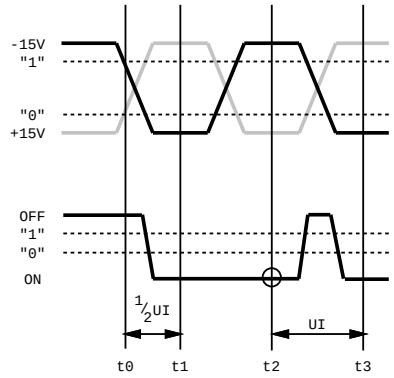


Fig. 7. Effect of a pulse stretcher between the data source and LED. Vertical lines are decision points; the small circle indicates the point at which an eavesdropper would incorrectly read the optical signal.

Optical background noise from artificial sources proved to be a significant problem. Sources of low-frequency noise (120 Hz and below) include incandescent, fluorescent, mercury vapor and sodium vapor lamps; high-frequency noise sources include industrial fluorescent lighting and compact fluorescent lights. Sunlight, while dwarfing in brightness the artificial sources, contributes only a DC component, and is much easier to filter out. Artificial lighting sources proved to be a pervasive and difficult-to-eliminate source of problems, because they contribute large amounts of amplitude-modulated noise containing strong harmonics in precisely the range of interest. In the United States, the standard 60 Hz alternating current electrical power supply leads to a characteristic noise component at 120 Hz. Most common data transmission rates are multiples of this frequency, complicating recovery of the data.

Digital signal processing techniques can help. By using a low-pass filter to isolate the 120 Hz component of the received optical signal, low-frequency noise can be isolated and subtracted from the optical signal, yielding a new signal without the 120 Hz component. Results of experiments in this area were very encouraging. Experiments using analog electronic filters were also encouraging.

The limiting factors in long-range interception seem to be the optics and the detector–amplifier system. Both a larger aperture and a narrower field of view are required. It is believed that, out to a range of at least several hundred meters, the optical flux available from a single LED is well within the capability of our detector. The response time of a typical LED suggests a practical upper limit on the order of 10 Mbits/s. Clearly, however, interception of data at longer ranges and higher speeds is feasible.

## 6. COUNTERMEASURES

A contributing factor to the threat of optical interception is a historical tendency to locate computers and data communication equipment in environmentally controlled "glass houses" which provide no barrier to the escape of optical radiation. Clearly this must now be considered a threat.

Examination of lighted windows of high-rise office buildings in the evening hours reveals a rich variety of equipment racks with LED indicators in view. Line-of-sight access is surprisingly easy to find. Fortunately, optical emanations are easier to contain than RF; opaque materials will shield the radiation effectively.

Black tape over the LEDs is effective, but inelegant. The best solution to the problem is a design change. Status displays could be designed to be deactivated when not in use (effectively making them Class I), or alternative display technologies could be employed, such as LCD and displays, which can be made inherently Class II due to their relatively slow impulse response. But many of these other technologies (such as CRT displays) are more expensive. LEDs are fast, cheap, and relatively low power indicators that can be read from across a room (a significant weakness of liquid crystal displays). It is preferable to retain these desirable properties.

A better solution is presented in Figure 7. The key here is a violation of the worst-case jitter tolerance of the serial data communication transmission scheme in use [Telecommunications Industry Association 1996]. If the minimum *on*-time of an LED indicator is greater than 1.5 times the unit interval of the current data rate[2], then an attacker will be unable to recover sufficient information to decode the signal. The effect is to convert a Class III indicator to Class II. The resulting low-pass filter removes a sufficient amount of information from the optical signal that an attacker cannot recover the original data from the emanations. The LED will flicker in response to a random data signal, and hence will still be useful as a Class II activity indicator, but the risk of significant information leakage is reduced.

More conservatively, the minimum *on*-time of the LED could be made to be at least twice the unit interval; even more conservatively, the minimum *off*-time could be similarly controlled as well. Most conservatively of all, the minimum *on*-time of the LED should be made to equal the nominal character interval of the current data rate, or of the slowest data rate expected. This will guarantee that an attacker cannot derive any information from the optical signal other than that a symbol was transmitted.

Even though it appears that at least one device (the PM14400FXMT fax modem) already incorporates pulse stretching functionality on its status LEDs, it is believed that this was done to make the display easier to read, not for reasons of blocking compromising emanations [Johnson 1995].

Of course, even in the presence of the aforementioned hardware modification, a patient attacker might simply time-modulate the asynchronous data stream in such a way as to effect a covert channel at a rate of $(\frac{t_{\mathrm{UI}}}{t_{\mathrm{character}}})^{-1}$ bits/s. This is an illustration of the general principle that it is difficult to completely eliminate the possibility of covert timing channels in multilevel systems [Proctor and Neumann 1992].

## 7. SUMMARY AND CONCLUSIONS

Modulated optical radiation from LED status indicators appears to be a previously unrecognized source of compromising emanations. This vulnerability is exploitable at a considerable distance. Primarily, data communication equipment is affected,

[2]or alternatively, the slowest data rate expected

although data encryption devices also pose a high risk of information leakage, potentially leading to loss of plaintext and encryption keys.

A taxonomy of optical emanations was developed according to the amount of "useful" information available to an attacker. Experiments showed that Class III optical emanations, which should never be permitted, were present in 36% of devices tested, and data could be read from these devices at a distance of at least 20 m. Countermeasures are possible that will convert a vulnerable Class III indicator into the safer (but still useful) Class II variety, by means of inserting a pulse stretcher into the LED driver circuitry.

### 7.1 Conclusions

Theft of information by interception of optical emanations is necessarily limited to one-way—the intruder can only receive information. However, login IDs and reusable passwords obtained in this fashion could be used to support a conventional attack. As mentioned before, parity checking, CRC values, and other error detection and correction features embedded in the data stream are available to the eavesdropper too, and can be of great benefit in helping to overcome the effects of a low-quality optical signal.

Ironically, it may be the simplest devices—low-speed, obsolete, insignificant parts of a network—that provide a gateway for intruders. In our experiments, it was low-speed modems, routers, line drivers, data loggers, and a printer sharing device that were found to be the most enthusiastic broadcasters of data. Class III optical emanations have been observed in the wild from devices as diverse as TTY-equipped payphones in airports and the digital control box of a player piano. Like the Purloined Letter, they hide in plain sight: a tangle of remote office connections in the corner, a modem sitting next to a PC by the window, or a call-accounting system on the PBX.

### 7.2 Summary of Contributions

—The existence of compromising optical emanations was proved.

—Successful exploitation, under realistic conditions, was demonstrated.

—A taxonomy of compromising optical emanations was developed.

—Some possible countermeasures were presented.

## 8. DIRECTIONS FOR FUTURE RESEARCH

Much work remains to be done. While we have shown that it is possible to intercept data at realistic data rates out to a few tens of meters, the maximum distance at which this can be accomplished remains unknown. Improved signal detection techniques, optics, and detectors would go a long way toward quantifying the effective limits on distance and bit error rate.

Other possible areas of investigation include the exploitation of Class II devices (especially disk drive and LAN card activity indicators) by covert channels; methods for dealing with extremely low-level optical emanations; exploitation of non–line-of-sight, or diffuse, emanations; several interesting aspects of fiber optics, including dark fiber; and the opportunities afforded by stimulated emanations (Appendix A).

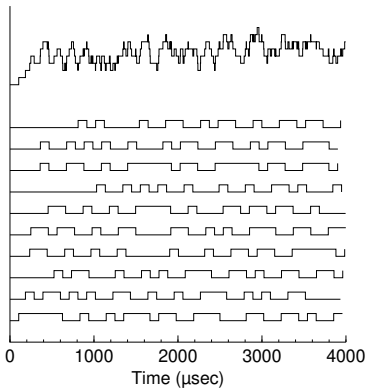


Fig. 8. Optical sum of ten random but correctly formatted data signals. **SIMULATION**

### 8.1 Low-Level Optical Emanations

While no evidence was found of Class III emanations from data storage devices, more investigation is needed to verify that disk and tape drive activity indicators experience no second-level effects due to (for instance) insufficient power supply regulation. And the wide variety and distribution of LAN cards suggests the possibility that at least one might show more than just Class II activity on the LEDs[3].

Other possible sources of compromising optical emanations include leakage from improperly terminated fiber optics or unconnected fiber optic ports. Alternative forms of attack are possible, including active attacks via optically emitting bugs operating outside of the visible spectrum that would be missed by conventional (RF) countersurveillance scanners. A passive collection system could operate over dark fiber; an accidental passive fiber optic tap would result if the end of a fiber strand were exposed to optical emanations from other devices in the room.

### 8.2 The Possibility of Non–Line-of-Sight Interception

Still unresolved is the question of whether diffuse emanations from multiple commingled or non–line-of-sight sources can be profitably unraveled. Optical signals sum linearly; the optical sum of $n$ linearly independent sources results in an extremely complicated signal (Figure 8). A room full of LED status indicators, even if individual sources are not directly observable, nevertheless can be seen to fill an entire area with a diffuse red glow. Light leakage around a door, or a passive fiber optic tap[4], might provide an adversary with enough optical flux to begin to analyze it.

8.2.1 *Experiments with Non–Line-of-Sight Access.* Sometimes things that are impossible in theory turn out to be feasible in practice. While it is true that in the

[3]LAN cards on PCs are particularly interesting, given that the LEDs are on the back panel; when the computer is conventionally oriented on a desk by a window, the LEDs are clearly visible from outside.

[4]A passive fiber optic tap might consist of as little as an unused strand of fiber, terminated at a patch panel inside the room but reserved for future use. Consequently, unused fiber optic ports should be capped when not in use.

Table III. Decoding of diffuse emanations from state transitions. **SIMULATION**

| $t_{\text{event}}\,(\mu\text{s})$ | *Transition* | *Interpretation* | $t_{\text{next}-\text{event}}\,(\mu\text{s})$ | *What can be deduced?* |
|---|---|---|---|---|
| $104.1\overline{6}$ | ↑ | $\phi_1$ start bit | $208.\overline{33}$ | |
| $184.1\overline{6}$ | ↑ | $\phi_2$ start bit | $288.\overline{33}$ | At least two signals exist. |
| $208.\overline{33}$ | none | $\phi_1$ $\text{data}_0 = 1$ | 312.50 | |
| $235.1\overline{6}$ | ↑ | $\phi_3$ start bit | $339.\overline{33}$ | ...three signals ... |
| $248.1\overline{6}$ | ↑ | $\phi_4$ start bit | $352.\overline{33}$ | ...four signals ... |
| $288.\overline{33}$ | ↓ | $\phi_2$ $\text{data}_0 = 0$ | 392.50 | |
| 312.50 | none | $\phi_1$ $\text{data}_1 = 1$ | $416.\overline{66}$ | |
| $339.\overline{33}$ | none | $\phi_3$ $\text{data}_0 = 1$ | 443.50 | |
| $352.\overline{33}$ | none | $\phi_4$ $\text{data}_0 = 1$ | 456.50 | |
| $359.1\overline{6}$ | ↑ | $\phi_5$ start bit | $463.\overline{33}$ | ...five signals ... |
| $362.1\overline{6}$ | ↑ | $\phi_6$ start bit | $466.\overline{33}$ | ...six signals ... |
| 392.50 | ↑ | $\phi_2$ $\text{data}_1 = 1$ | $496.\overline{66}$ | |
| $416.\overline{66}$ | none | $\phi_1$ $\text{data}_2 = 1$ | $520.8\overline{3}$ | |
| 443.50 | ↓ | $\phi_3$ $\text{data}_1 = 0$ | $547.\overline{66}$ | |

general case of $n$ random square wave signals—whose amplitude, pulse width, and pulse repetition rate are unknown—that a unique decomposition may not exist, in the real world, however, data signals are *not* random. EIA/TIA-232-E in particular is full of known values: start symbols, stop symbols, the number of data bits following a start symbol, and the guaranteed minimum and maximum duration of all symbols (the unit interval). Because the signals are not entirely random, but contain a small number of known values at certain fixed locations, it becomes possible to identify individual components ($\phi_1$ through $\phi_n$) with high probability. The left-hand side of Table III gives the timing and direction of state transitions during the first few hundred $\mu$s of the simulation shown in Figure 8. The algorithm works by scanning the received optical waveform from left to right until the first positive-going transition is found. The optical signal should be sampled at a rate at least three to five times the reciprocal of the smallest time difference between successive level transitions [McCarthy 2001]. Once a candidate transition is identified in the aggregate optical sum, any further activity on that particular component ($\phi_i$) can be ruled out for at least one unit interval. Any transitions seen in the meantime must be the result of another, heretofore unknown signal ($\phi_{i+1}$). By an iterative process of elimination, each individual signal in turn is teased out of the jumble.

The unit interval is not difficult to guess from the Fourier spectrum of the times of transitions in the received signal (Figure 9). The peak in the curve, at 104 $\mu$s, corresponds to the most likely unit interval. In any case, the range of possible data formats is small enough simply to try all of the various possibilities until one of them yields intelligible data. Even an ambiguous solution might be of some value to an attacker, if the result were a data stream having some non-zero, but not catastrophic, bit error rate[5]. As long as the individual signal components are not precisely aligned in time—which leads to ambiguous solutions—the analysis

[5]For example, if the most-significant bit of an 8-bit data word is not always 0, the data stream is not ASCII. Similarly, there are many disallowed values in EBCDIC that could be used to rule out this encoding as well.

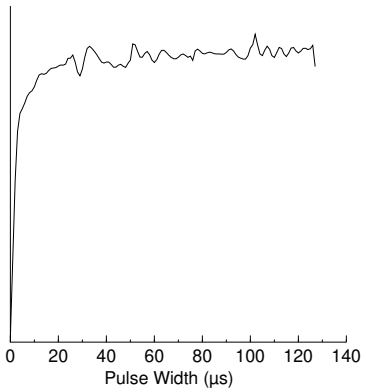


Fig. 9. Fourier spectrum (real part) of the interval between transitions in the optical sum in Figure 8. The peak in the curve, at approximately 104 $\mu$s, corresponds to the most likely unit interval.

appears to be tractable. More work is clearly needed, on real signals, as a follow-on to the unrealistically low-noise simulation presented here.

## REFERENCES

Agilent Technologies 1999. *T-1$\frac{3}{4}$ (5 mm) Diffused LED Lamps Technical Data.* Agilent Technologies. Data sheet 5968-4161E (2/99).

Anderson, R. J. 2001. *Security Engineering: A Guide to Building Dependable Distributed Systems.* John Wiley & Sons, New York, New York.

Anderson, R. J. and Kuhn, M. G. 1999. Soft tempest—an opportunity for NATO. In *Protecting NATO Information Systems in the 21st Century.* NATO Research & Technology Organisation, Washington, D.C.

Black, U. 1996. *Physical Layer Interfaces and Protocols*, 2nd ed. IEEE Computer Society Press, Los Alamitos, California.

Common Criteria Project Sponsoring Organizations 1999. *Common Criteria for Information Technology Security Evaluation.* Common Criteria Project Sponsoring Organizations. CCIMB-99-031, Version 2.1.

Electronic Industries Association, Engineering Department 1991. *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange.* Electronic Industries Association, Engineering Department. EIA/TIA-232-E.

EXFO Electro-Optical Engineering, Inc. 1999. *LFD-100 Live Fiber Detector.* EXFO Electro-Optical Engineering, Inc. Data sheet SPLFD100.4AN.

Fites, P. and Kratz, M. P. 1993. *Information Systems Security: A Practitioner's Reference.* Van Nostrand Reinhold, New York, New York.

Gagliardi, R. 1995. *Optical Communications*, 2nd ed. John Wiley & Sons, New York, New York.

Garfinkel, S. 1994. *PGP: Pretty Good Privacy.* O'Reilly & Associates, Sebastopol, California.

Hewlett–Packard Company 1993a. *HFBR-4663 Single Chip 10BASE–FL Transceiver Technical Data.* Hewlett–Packard Company. Data sheet 5091-7391E.

Hewlett–Packard Company 1993b. *Low-Cost Fiber-Optic Links for Digital Applications up to 155 MBd.* Hewlett–Packard Company. Application Bulletin 78, 5091-9102E.

Hodara, H. 1991. Secure fiberoptic communications. In *Proceedings of Symposium on Electromagnetic Security for Information Protection.* Fondazione Ugo Bordoni, Rome, Italy.

Johnson, P. 1995. Circuit adapts signals for visual perception. *Electronic Design News 40,* 21 (12 October), 104.

KUHN, M. G. 2002. Optical time-domain eavesdropping risks of CRT displays. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*. IEEE Computer Society, Oakland, California.

KUHN, M. G. AND ANDERSON, R. J. 1998. Soft tempest: Hidden data transmission using electromagnetic emanations. In *Proceedings of Information Hiding, Second International Workshop*, D. Aucsmith, Ed. Springer–Verlag, Portland, Oregon, 15–17.

LAMPSON, B. W. 1973. A note on the confinement problem. *Comm. ACM 16,* 10 (October), 613–615.

LANCASTER, D. 1980. *TTL Cookbook*. Howard W. Sams, Indianapolis, Indiana.

LATHROP, D. L. 1992. Security aspects of wireless local area networks. *Computers & Security 11*, 421–426.

MCCARTHY, D. C. 2001. Faster vs. denser: Networks reach another crossroad. *Photonics Spectra 35,* 9 (September), 110–118.

MORRIS, J. 1996. Re: blinking lights on computers. Article ⟨55ni3a$bm3top.mitre.org⟩, in USENET newsgroup alt.folklore.computers.

National Computer Security Center 1988. *Glossary of Computer Security Terms*. National Computer Security Center. NCSC-TG-004, Version 1.

National Computer Security Center 1993. *A Guide to Understanding Covert Channel Analysis of Trusted Systems*. National Computer Security Center. NCSC-TG-030, Version 1.

National Security Agency 1992. *NACSIM 5000 TEMPEST Fundamentals*. National Security Agency, Fort George G. Meade, Maryland. `http://cryptome.org/nacsim-5000.htm`.

National Security Agency 1994. *Specification NSA No. 94-106, Specification for Shielded Enclosures*. National Security Agency, Fort George G. Meade, Maryland. `http://cryptome.org/nsa-94-104.htm`.

National Security Agency 1995. *TEMPEST/2-95 Red/Black Installation Guidance*. National Security Agency, Fort George G. Meade, Maryland. `http://cryptome.org/tempest-2-95.htm`.

Paradyne Corporation 1985. *InfoLock Model 2811-11 Installation and Operation Manual*, 1st ed. Paradyne Corporation. 2811-A2-GN32-00.

PERRY, T. S. 1995. M. George Craford. *IEEE Spectrum 32,* 2 (February), 52–55.

PETITCOLAS, F. A., ANDERSON, R. J., AND KUHN, M. G. 1999. Information hiding—a survey. *Proceedings of the IEEE 87,* 7 (July), 1062–1078.

PROAKIS, J. G. AND SALEHI, M. 1994. *Communication Systems Engineering*. Prentice-Hall, Englewood Cliffs, New Jersey.

PROCTOR, N. E. AND NEUMANN, P. G. 1992. Architectural implications of covert channels. In *Proceedings of the Fifteenth National Computer Security Conference*. National Institute of Standards and Technology, National Computer Security Center, Baltimore, Maryland, 28–43.

RUSSELL, D. AND GANGEMI, G. 1991. *Computer Security Basics*. O'Reilly & Associates, Sebastopol, California.

SMULDERS, P. 1990. The threat of information theft by reception of electromagnetic radiation from RS-232 cables. *Computers & Security 9,* 1, 53–58.

STEPHENSON, N. 1999. *Cryptonomicon*. Avon Books, New York, New York.

Telecommunications Industry Association 1996. *Standard for Start–Stop Signal Quality for Non-Synchronous Data Terminal Equipment*. Telecommunications Industry Association. TIA/EIA-404-B.

UMPHRESS, D. AND WILLIAMS, G. 1985. Identity verification through keyboard characteristics. *Int. J. Man–Machine Studies 23*, 263–273.

United States Department of Defense 1985. *Trusted Computer System Evaluation Criteria*. United States Department of Defense. DOD 5200.28-STD.

United States Department of Defense 1987. *Red/Black Engineering–Installation Guidelines*. United States Department of Defense. MIL-HDBK-232A.

VAN ECK, W. 1985. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security 4*, 269–286.

VAN GILLUWE, F. 1994. *The Undocumented PC*. Addison–Wesley Publishing Company, Reading, Massachusetts.

WILKINS, J. 1641. *Mercury, or the Secret and Swift Messenger*. I. Norton, London.

WRAY, J. C. 1991. An analysis of covert timing channels. In *Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy*. IEEE Computer Society, Oakland, California, 2–7.

WRIGHT, P. 1987. *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer*. Viking Press, New York, New York.

## A. STIMULATED EMANATIONS

Not all sources of compromising optical emanations are naturally occurring. We describe two implementations of a Trojan horse that manipulates the LEDs on a standard keyboard to implement a high-bandwidth covert channel [Wray 1991]. This is an example of an *active attack*, mounted by an adversary against a device that is not normally vulnerable to compromising optical emanations.

### A.1 The Keyboard Considered as an Output Device

Ever since the standardization of computer keyboards to the IBM layout, most computer keyboards have three LED indicators, for Caps Lock, Num Lock, and Scroll Lock, respectively. Interestingly, these LEDs are not directly connected to their associated keys—the lights, in fact, are software controlled.

The PC keyboard is an intelligent device that communicates with the host computer over a bi-directional, synchronously clocked serial interface at approximately 10 000 bits/s[6].

The capacity of the keyboard interface channel far exceeds the requirements of even the fastest typist. So long as the amount of data sent to the keyboard is limited, and does not interfere with processing of keystrokes, the excess bandwidth can be profitably employed by an attacker.

A *covert channel* is a means of extracting data from a computer system in violation of the system security policy [Lampson 1973; National Computer Security Center 1993]. A *high-bandwidth* covert channel is considered to be one capable of transmitting data faster than 100 bits/s [Common Criteria Project Sponsoring Organizations 1999; United States Department of Defense 1985]. The covert channel described here has been demonstrated to work at speeds from 150 to 10 000 bits/s.

### A.2 Related Work

The fact that keyboard LEDs can be manipulated has been known for a long time. Some operating systems provide the capability to control the keyboard indicators from a shell script; if not, then it is a relatively simple matter to program directly to the keyboard interface [van Gilluwe 1994].

A more recent paper describes another possible method for remotely monitoring the electrical signals inside a PC keyboard, together with some countermeasures. [Anderson and Kuhn 1999]. The only other published description of a covert channel employing keyboard LEDs appears in a work of fiction [Stephenson 1999], in which a character employs a similar technique to extract a small amount of critical information from his computer despite being under continuous surveillance.

[6]The exact speed was found to vary among different manufacturers.

### A.3 A Covert Channel in Software

A successful covert channel running at up to 450 bits/s was demonstrated on the IBM PC/AT, several different Compaq ProLineas, and the Sun Microsystems SPARCstation 20 and Ultra 1 workstations. The attack was successful under MS-DOS, Microsoft Windows 3.1, Windows 95, and Windows 98, Windows NT 3.5 and 4.0, and Sun Microsystems Solaris 2.5, 2.5.1, Solaris 7, and Trusted Solaris 2.5 and 2.5.1. A handful of machines could not be made to work, among them a Compaq LTE Lite 486/25E notebook.

We found that activity on a single keyboard LED at 150 bits/s was not particularly noticeable during interactive use. Employing more than one LED at a time increases the probability of discovery but offers some compelling advantages. If all three LEDs are modulated identically, the optical output of the transmitter is tripled, greatly increasing the useful range. Alternatively, two or even three bits could be transmitted in parallel, increasing the bandwidth of the covert channel to approximately 450 bits/s. Experiments were run with (1) asynchronous parallel transmission using three LEDs, (2) synchronous serial transmission using single and biphase clocking, and (3) differential Manchester encoding. The latter yielded high reliability at the receiving end, but with all the activity on three LEDs, it was noticeable to the operator that something strange was going on.

Appendix B contains example code implementing the covert channel under Solaris version 2.$x$ [7].

### A.4 Attacking the Hardware

Even better results can be obtained through modification of the keyboard hardware. Depending on the details of a particular keyboard, the modifications may be as simple as moving a single wire. An IBM PC/AT keyboard was modified as an experiment. The Scroll Lock LED was cross-connected to the `keyboard data` signal, as shown in Figure 10. It was necessary to invert the `keyboard data` signal so that the LED would remain dark when the covert channel was idle. Fortunately, IBM provided a ready-made solution in the form of an unused gate on one of the chips. The optical output of the LED is now modulated directly by the 10 000 bits/s serial data stream in the keyboard cable. The Scroll Lock LED can be seen to flicker momentarily with keyboard activity, but the effect is not very noticeable. No software is required.

Normal operation of the Scroll Lock LED is prevented, but the Scroll Lock function is not used very often. By a fortuitous coincidence, the normal behavior of the keyboard LEDs during the power-on self test (POST) function is unaffected; the functionality of the Scroll Lock key itself is also unchanged (except of course that the LED does not appear to work anymore.)

Figure 11 shows the optical waveform obtained from a keyboard with the modifications of Figure 10. The upper trace of Figure 11 shows the intercepted optical signal; the lower two traces are the electrical signals on the keyboard data interface and the keyboard data clock. The bandwidth of the resulting covert channel is greater than that of a software-only attack, but the information is in the form of keyboard scan codes, not ASCII. It requires a bit of translation on the receiving

[7] The authors demonstrated this technique privately in 1996.

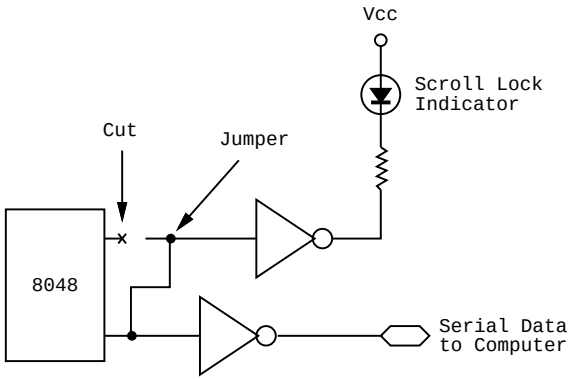


Fig. 10. Modifications to the IBM PC/AT keyboard.

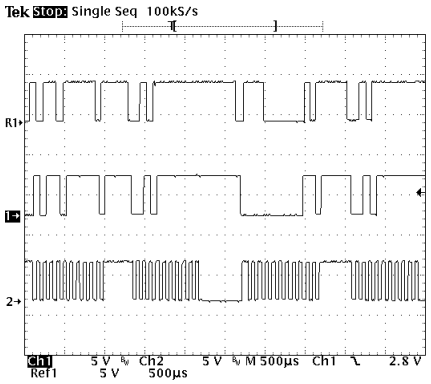


Fig. 11. Optical signal (top) obtained from a keyboard with the modifications of Figure 10.

end, but also yields more information. Since accurate timing of both key-down and key-up events are reported, this method may provide enough information to compromise identity verification systems based on typing characteristics [Umphress and Williams 1985] or the generation of cryptographic keys [Garfinkel 1994].

A.4.1 *Improving the Bandwidth of the Covert Channel.* It is not difficult to imagine how a small investment in additional hardware could vastly improve the chances of a successful attack. An infrared (IR) LED chip could be co-encapsulated with a visible LED in the same package. If the two LEDs were connected back-to-back internally, only two leads would be required, and the Trojan LED would be indistinguishable from a standard component except under high magnification. Modification to the keyboard controller circuitry would be required to utilize the IR capability; as long as this is being done anyway, the following "improvements" might be made to the controller's firmware at the same time:

—Increasing the drive current to the IR emitter for correspondingly increased range

—Use of more sophisticated channel encoding to reduce transmission errors and support higher speeds

—A timer and buffer memory to allow for a delay in sending until the keyboard has been idle for a while

—Encryption and compression of the covert channel data

—Sender identification, to support multiple units in a single location

—Pattern matching capability, to look for specific information in the keyboard data stream

—Preserving the normal functionality of the visible LED indicator.

All but the first of these have been successfully demonstrated in software. Given that access to the hardware or surreptitious replacement would be necessary in order to emplace a hardware Trojan horse, concurrent implementation of all the above features would seem to pose little trouble. Modifications to firmware would be nearly undetectable, barring a close examination of the microcontroller object code.

### A.5 Conclusions

This vulnerability potentially affects hundreds of millions of devices. It might be argued that keyboard LEDs lack sufficient brightness to be successfully exploited from a long distance. However, the authors once encountered a Compaq PC whose keyboard LEDs were bright enough to throw shadows on the ceiling. When tested, this keyboard was able to handle 450 bits/s communication on all three LEDs simultaneously without noticeably affecting response time. The software presented in Appendix B is small enough to be included in a computer virus, as described in [Petitcolas et al. 1999].

### A.6 Summary

It has been shown that it is possible to cause the emission of compromising optical emanations in devices not normally vulnerable, by taking advantage of software-controlled LED indicators. The covert channel thereby created has a bandwidth of several hundred bits/second at least, and is compatible with standard techniques for exploiting compromising optical emanations described in the previous paper.

## B. SENDING DATA THROUGH THE KEYBOARD

The following C program implements the software version of the covert channel under Solaris version 2.$x$. It transmits ASCII data by modulating the Caps Lock LED with serial data at 50 bits/s. A similar program, written in Intel x86 assembly language and incorporating additional functionality[8], required less than 1500 bytes of memory.

```
/*
// sl.c -- a covert channel using the Caps Lock LED.
//
```

[8]The program installed itself as an interrupt handler and hooked the keyboard interrupt. It copied all keyboard activity while waiting for the keyboard to become idle. After four hours of no keyboard activity, the contents of the buffer were transmitted. If any keyboard activity was detected while the program was busy transmitting, it immediately stopped sending, restored the state of the keyboard LEDs, and resumed waiting.

```
// For Solaris 2.x on SPARC; compile with ${CC} sl.c -lposix4
*/

#include <fcntl.h>
#include <stdio.h>
#include <stdlib.h>
#include <sys/kbio.h>
#include <sys/kbd.h>
#include <time.h>
#include <unistd.h>

#define SPEED 50 /* data transmission speed (bits per second) */

void set_led (int fd, char *data);
void time_led (int fd, char *data);
void perror_exit (char *function_name);

/* set up a 20 millisecond intersymbol delay */

struct timespec min, max = { 0, 1000000000 / SPEED };

int
main (void)
{
    char message[] = "My credit card number is 1234 5678 910 1112.";
    char restore_data;
    char *p = &message[0];
    int  fd;

    /* open the keyboard device */
    if ((fd = open ("/dev/kbd", O_RDONLY)) < 0)
        perror_exit ("open");

    /* save the state of the keyboard LEDs */
    if (ioctl (fd, KIOCGLED, &restore_data) < 0)
        perror_exit ("ioctl");

    while (*p) {
        char data = LED_CAPS_LOCK;
        int  i;

        /* start bit is a "1" */
        time_led (fd, &data);

        /* send 8 bits, least significant first */
        for (i = 0; i < 8; i++) {
            data = *p >> i & 1 ? LED_CAPS_LOCK : 0;
            time_led (fd, &data);
        }

        /* stop bit is a "0" */
```

```
        data = 0;
        time_led (fd, &data);

        /* next character of message */
        p++;
    }
    /* restore state of the keyboard LEDs */
    set_led (fd, &restore_data);

    return (close (fd));
}

/* turn keyboard LEDs on or off */

void
set_led (int fd, char *data)
{
    if (ioctl (fd, KIOCSLED, data) < 0)
        perror_exit ("ioctl");
}

/* transmit one bit */

void
time_led (int fd, char *data)
{
    set_led (fd, data);
    nanosleep (&min, &max);
}

/* display an error message and quit */

void
perror_exit (char *function_name)
{
    perror (function_name);
    exit (1);
}
```

ACKNOWLEDGMENTS

The authors wish to thank the anonymous reviewers; their careful reading and insightful comments helped catch a number of errors that otherwise would have crept into publication. Annie Cruz of Washington Mutual Bank, and Eduard Telders of PEMCO Financial Services, also provided valuable assistance and encouragement with the preparation of this paper.

Received April 2001; revised February 2002; accepted March 2002