


## Chapter 7

# Optical TEMPEST

HE leakage of information from a system through a channel of modulated light is a vulnerability. The operative terms are ‘leakage’, ‘information’, ‘channel’, and ‘modulated light’. The *leakage* might be accidental or it might be caused on purpose by an adversary, but it is not supposed to be there. *Information* can be anything from a single bit to large volumes of information; it might be extremely valuable information like cryptographic keys. *Channels* in the Shannon sense (Shannon 1948) have a bandwidth-delay product, and noise; both of these are important to understand the risk of optical TEMPEST. And finally, *modulated light* carries the signal. Light can be modulated in time or in space—here we think of light modulated in the time domain. Light modulated in the space domain is an *image*; ‘shoulder surfing’ is a real risk but not the one we are concerned with here.<sup>1</sup>

Further in the time domain, light can be amplitude-modulated, or frequency-modulated, or phase-modulated. Of the three possibilities, amplitude modulation (AM) is the most plausible for optical TEMPEST (from a physical standpoint) because optical TEMPEST vulnerabilities most often depend on the accidental or improvised existence of a modulated—or modulatable—channel, and AM is likely the simplest and most straightforward to implement. On-off keying (OOK) is the simplest AM method and the most likely to occur accidentally; in OOK, light *on* means a binary 0 or 1, and light *off* means the other kind. OOK is not self-clocking: the receiver must know *a priori* or be able to figure out the sender’s intended *bit interval* to decode the signal; there are better *line codes* than OOK that a deliberate sender inside the target system may be able to use—Manchester coding, for example—but most often the adversary is limited to exploiting sources and methods that are already there.

### Light Sources

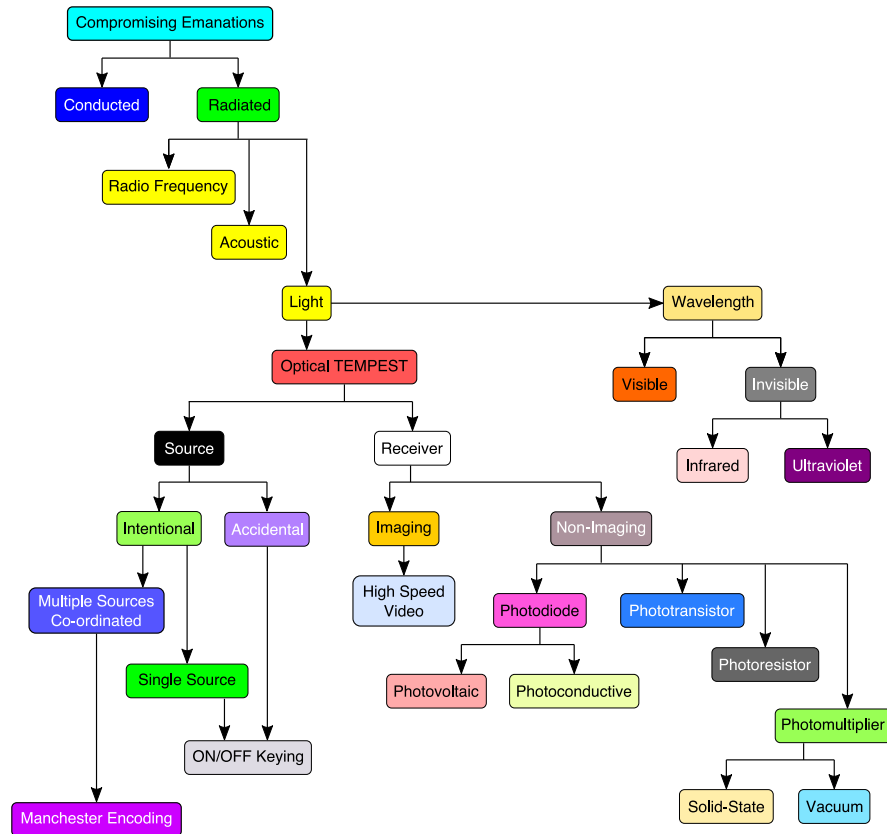
Compromising emanations take one of two paths: they may be *conducted* or *radiated*. Light sources vulnerable to optical TEMPEST include visual indicators—a subset of which are video displays—and discrete indicators. If

---

<sup>1</sup> *Shoulder surfing* is the clandestine surveillance of display screens or keyboard activity for the purpose of stealing secrets. It might be done visually or through a video camera; it can even be done without line-of-sight, by deconvoluting a distorted reflection off a shiny object in the optical path (Backes et al. 2008, 2009, Raguram et al. 2011, Jenkins & Kerr 2013, Xu et al. 2013).

controlled automatically, indicators are not as useful as if they may be set by the adversary.

Figure 7.1 shows the taxonomy of optical TEMPEST in the larger context of vulnerabilities due to *compromising emanations*—exploitable leakage of measurable physical phenomena out of a system that can be interpreted by an adversary to gain information about the internal state of the system.



Taxonomy continues here

Figure 7.1: Taxonomy of compromising emanations.

## Sensors

Given these sources of compromising emanations (accidental or intentional), to have a communication channel there must be a receiver. Many kinds of optical sensors will suffice, but what is needed particularly is an optical sensor with a fast response time. Photodiodes, photomultipliers (solid state or otherwise), phototransistors, photoresistors, or even some video cameras might be used. Still cameras are not suitable.

## Induced Emanations

### The clock recovery problem

(Figure from 2002 paper)

Depending on the nature of the leakage, information leakage through optical emanations may or may not be a covert channel. By the classical definition, due to (Lampson 1973), a covert channel is made of a pair of communicating processes, but in many cases, the source of compromising optical emanations is in hardware, not a programme running on the CPU.

electromagnetic but in the optical spectrum; we consider that to include at least infrared (wavelengths longer than 700 nm) because of the ubiquitousness of light emitting diode (LED) sources in that range and their convenient invisibility to humans.

Cite (Allain 2019).

## 7.1 History

The U.S. National Security Agency (NSA) named TEMPEST, as far as we know. We don't even know for sure that the word is not an acronym. It is believed to be a code name, TEMPEST<sup>2</sup> but evidence in the open literature is scarce; the only clear original source is one declassified document dating from 1972 in which everything related to emanations other than RF is redacted (National Security Agency 1972).

## Information Leakage

### Electromagnetic

Field telephones in WWI; *funkspiel* in WWII; electromechanical cypher machines in West Berlin. (This topic is covered well elsewhere in the book.)

## TEMPEST

The protection of information from remote eavesdropping; air gaps; control zones; protected distribution systems (PDS)<sup>3</sup> The inclusion of acoustic but overlooking of optical, with the exception of shoulder surfing. Contextual blindness?

<sup>2</sup>Evidence for it is shaky but there was supposedly another programme called TEAPOT dealing with stimulated RF compromising emanations (Anderson 2008, p. 539) and partially corroborated in December of 2013 by Edward Snowden (NSA ANT catalogue).

<sup>3</sup>Visibility, stories of poison gas, flammable gas, pressure gauges—reference Anderson (2001).

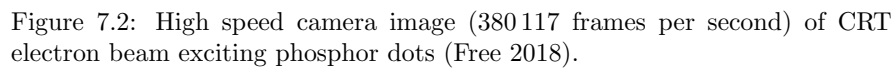
## How dangerous?

**Class I** optical emanations are correlated only minimally with the state of a device; they tell if it is on or off. **Class II** emanations leak information about the activity level of a device—is it busy or idle? **Class III** optical emanations are correlated with the contents of data, and are extremely hazardous.

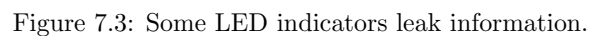
## Video Cameras

It is tempting to think of using video cameras to capture an entire rack of LED indicators at once, but that won't work. The reason is because video cameras have a relatively low *frame rate*—usually 30–240 frames per second—and this is not fast enough to capture the transitions we're interested in.

LEDs and CRTs—Figure 7.2.



Photons, energy, generation atmospheric absorption. Recent development of high efficiency LEDs (and the unexpected effect that had on reversing LEDs). Telescopic optics, fibreoptic collection.



One surprising thing, to anyone unfamiliar with digital signal processing, is how effectively it can pull a usable signal out of what appears to be hopelessly noisy data. An example may be seen in Fig. 4 of (Loughry & Umphress 2002).

Need a new figure here.