Emission security (i drugi sporedni kanali)

Dimitrije Erdeljan

Matematička gimnazija

Nedelja informatike

27. mart 2018.

Sporedni kanali

Da bi napravili bezbedan sistem, dobar softver i dokazano bezbedni algoritmi nisu dovoljni

Implementacija dobrog kriptografskog algoritama može da odaje neočekivane informacije – sporedni kanal ("*side channel*")

Sistemi za koje ne očekujemo da komuniciraju sa svetom mogu da slučajno šalju informacije

Neki stari primeri

Komunikacioni kablovi u Prvom svetskom ratu su koristili zemlju umesto druge žice – signal se vidi u zemlji na ≈ 100 metara

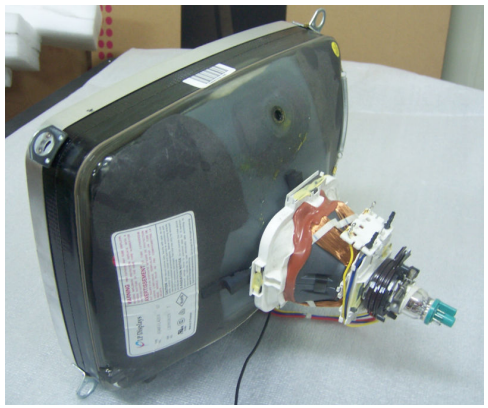
Originalni podaci su nađeni kao slab signal u šifrovanoj komunikaciji francuske ambasade u UK 1960.

Mainframe računari su proizvodili radio-šum – radio-prijemnik kao alat za debagovanje

CRT monitori

CRT (*cathode ray tube*) monitori iscrtavaju sliku pomoću elektronskog topa:

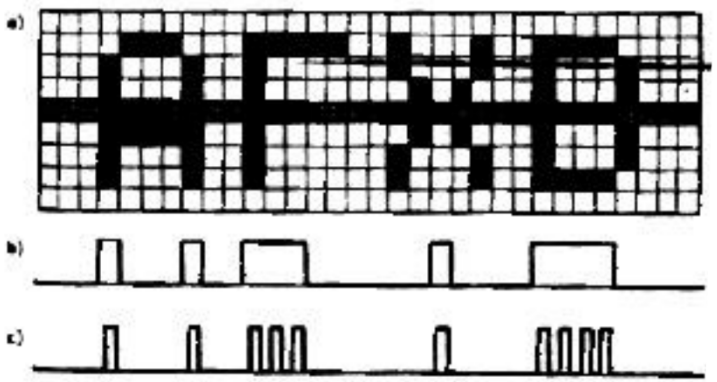
- Ekran je ploča prekrivena “fosforima” (različita jedinjenja, ne sadrže fosfor) koji svetle kada ih udari elektron
- Zrak elektrona iz topa prelazi preko cele slike, piksel po piksel
- Za svaki piksel, top se na kratko pali (puls) ako ga treba nacrtati



http://commons.wikimedia.org/file/Crt14.jpg

Signal koji opisuje sliku (na ulazu u top) je “opis slike” pomnožen sa četvrtkom fiksne frekvencije:

$$f = \frac{f_r}{w \cdot h} \approx 50\text{–}100 \text{ MHz}$$



Veliko pojačanje na ulazu u top $\rightarrow$ monitor emituje jak signal

Analogni TV signal je veoma sličan (ista tehnologija), osim sto sadrži sinhronizacione impulse ("kraj reda" i "kraj slike")

Uz minimalno nestandardne opreme, slika sa monitora se može videti sa nekoliko desetina metara ("*Van Eck Phreaking*")[1]:

- TV prijemnik
- Elektronika koja generiše sinhronizacione impulse
- Direkciona antena

[1] Van Eck, Wim. "Electromagnetic radiation from video display units: An eavesdropping risk?." Computers & Security 4.4 (1985): 269-286.

Sa rastojanja od tri metra, prosek 256 frejmova[2]:

[2]Kuhn, Markus Guenther. Compromising emanations: eavesdropping risks of computer displays. Diss. University of Cambridge, 2002.

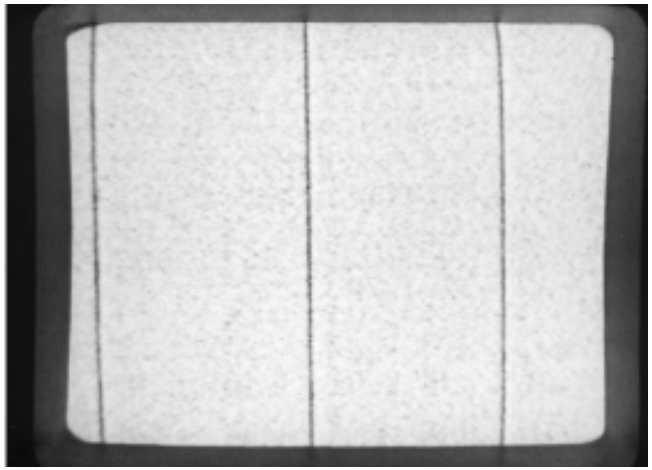
In February, 1985, we carried out an eavesdropping experiment in London, in cooperation with the British Broadcasting Corporation. Part of the results were shown in the programme "Tomorrow's World." A small van was equipped with a 10 metre high pump mast to which a VHF band III antenna wa clamped (10 dB gain). The received signal was fed through an antenna, amplified (18 dB) and displayed on a television screen inside the van. For obvious reasons we cannot give information on the data picked up during the experiment. The results can be summarized as follows:

- *It is possible to eavesdrop on the video display units or terminals in buildings from a large distance, using a car fitted up for the purpose.*
- *Although the experiment was carried out in broad daylight and many people watched us, nobody asked what we were doing.*

Ovakav signal mnogo bolje prenosi komponente visoke frekvencije. Filtriranjem možemo napraviti font koji se vidi lošije[3]:

TrustNo1 TrustNo1

TrustNo1 TrustNo1



Obrnuto takođe važi: virus koji koristi monitor da bi slao informacije?

[3] Kuhn, Markus G., and Ross J. Anderson. "Soft tempest: Hidden data transmission using electromagnetic emanations." International Workshop on Information Hiding. Springer, Berlin, Heidelberg, 1998.

LCD monitori

LCD monitori ne emituju signal kao CRT:

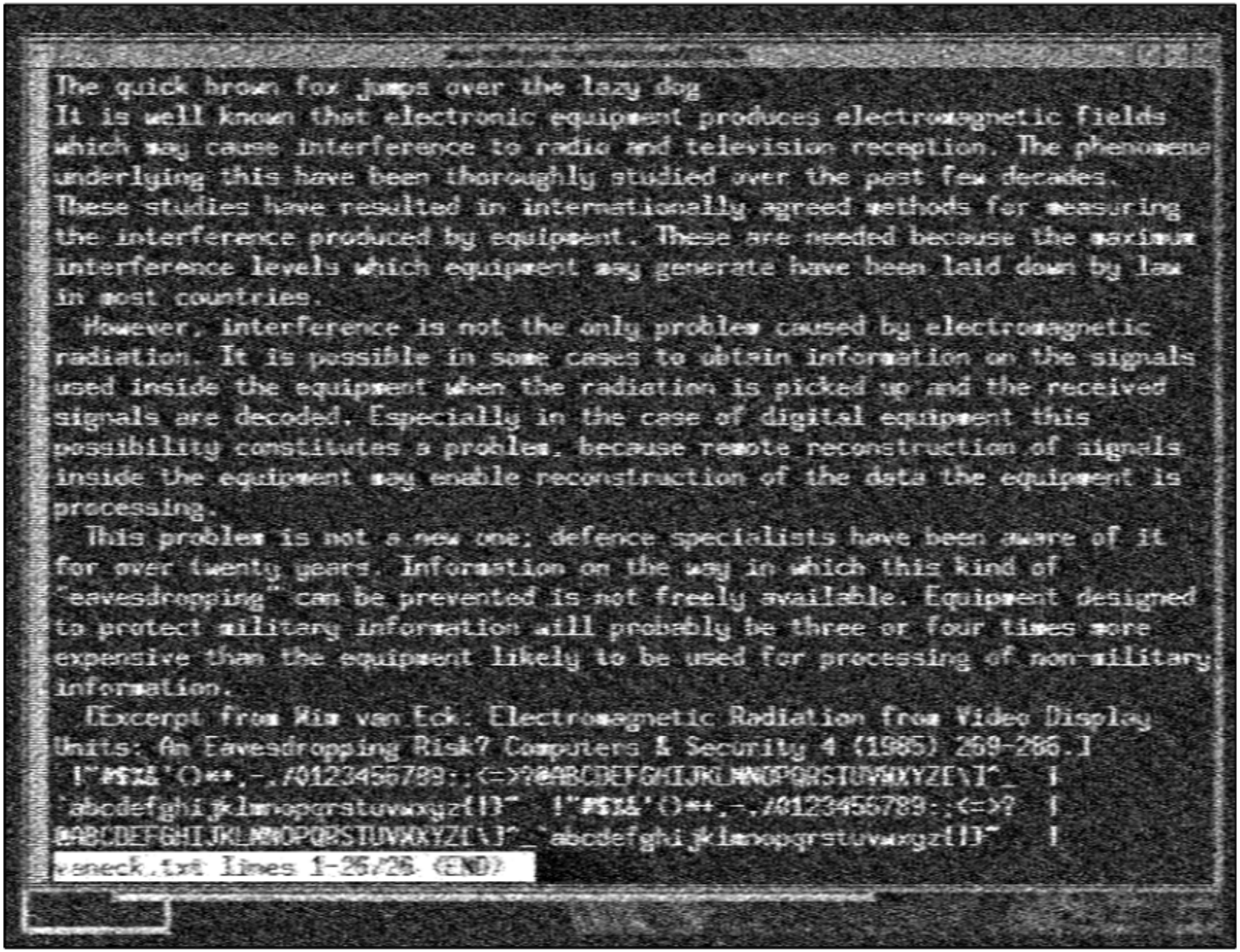
- Slika se crta red po red, ne piksel po piksel
- Nema delova velike snage (elektronski top)

Monitor nema dovoljno memorije za celu sliku – video kontroler "šalje" celu sliku svaki frejm

Kabl kontroler–monitor se ponaša kao antena

Signal nije jednostavan kao na CRT monitorima, ali sadrzi dovoljno informacija o slici[4]

[4] Kuhn, Markus G. "Electromagnetic eavesdropping risks of flat-panel displays." International Workshop on Privacy Enhancing Technologies. Springer, Berlin, Heidelberg, 2004.


The quick brown fox jumps over the lazy dog
It is well known that electronic equipment produces electromagnetic fields
which may cause interference to radio and television reception. The phenomena
underlying this have been thoroughly studied over the past few decades.
These studies have resulted in internationally agreed methods for measuring
the interference produced by equipment. These are needed because the maximum
interference levels which equipment may generate have been laid down by law
in most countries.
However, interference is not the only problem caused by electromagnetic
radiation. It is possible in some cases to obtain information on the signals
used inside the equipment when the radiation is picked up and the received
signals are decoded. Especially in the case of digital equipment this
possibility constitutes a problem, because remote reconstruction of signals
inside the equipment may enable reconstruction of the data the equipment is
processing.
This problem is not a new one; defence specialists have been aware of it
for over twenty years. Information on the way in which this kind of
"eavesdropping" can be prevented is not freely available. Equipment designed
to protect military information will probably be three or four times more
expensive than the equipment likely to be used for processing of non-military
information.
[Excerpt from Wim van Eck: Electromagnetic Radiation from Video Display
Units: An Eavesdropping Risk? Computers & Security 4 (1985) 269-286.]
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_
`abcdefghijklmnopqrstuvwxyz{|}~
!"#$%&'()*+,-./0123456789:;<=>?
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
veneck.txt Lines 1-26/26 (END)

Izbori

Na parlamentarnim izborima u Danskoj 2006. planirano je glasanje na mašinama

Kontroler koji iscrtava tekst podržava ASCII i osam ne-ASCII karaktera

Specijalni karakteri usporavaju kontroler:

- samo ASCII $\rightarrow$ 72 Hz
- bar jedan specijalni karakter $\rightarrow$ 58 Hz

Displej emituje signal na ovoj frekvenciji – možemo razlikovati glasanje za *Christen Democratisch Appèl* od ostalih[5]

[5] Gonggrijp, Rop, and Willem-Jan Hengeveld. "Studying the Nedap/Groenendaal ES3B voting computer: A computer security perspective." Proceedings of the USENIX workshop on accurate electronic voting technology. USENIX Association, 2007.

CRT monitori (opet)

CRT monitori crtaju sliku piksel po piksel

Snimak osvetljenja u sobi visoke vremenske rezolucije omogućava da u svakom trenutku vidimo da li je “trenutni” piksel svetao

Teleskop + fotodioda $\rightarrow$ slika[6]

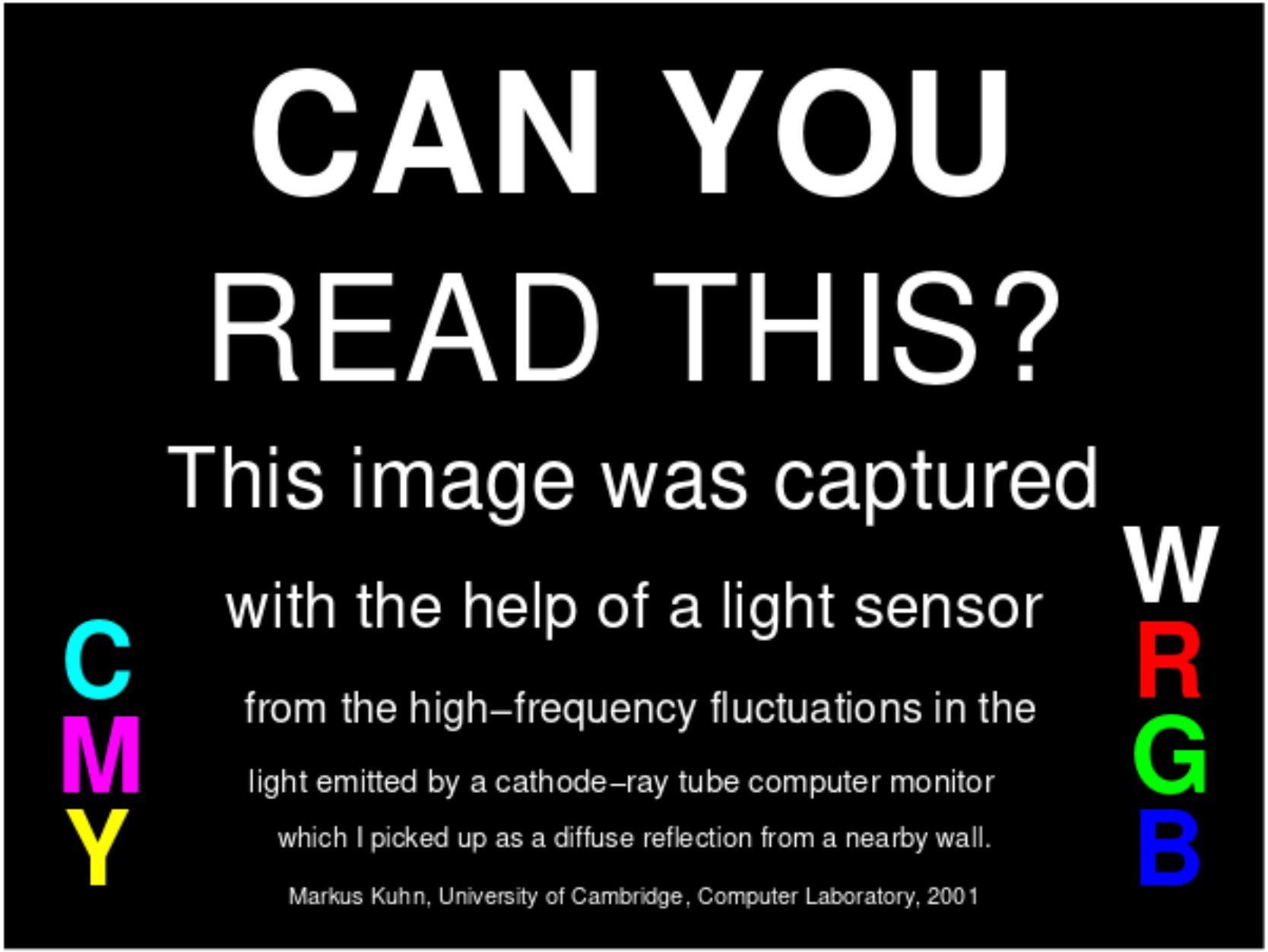
[6] Kuhn, Markus G. “Optical time-domain eavesdropping risks of CRT displays.” Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on. IEEE, 2002.

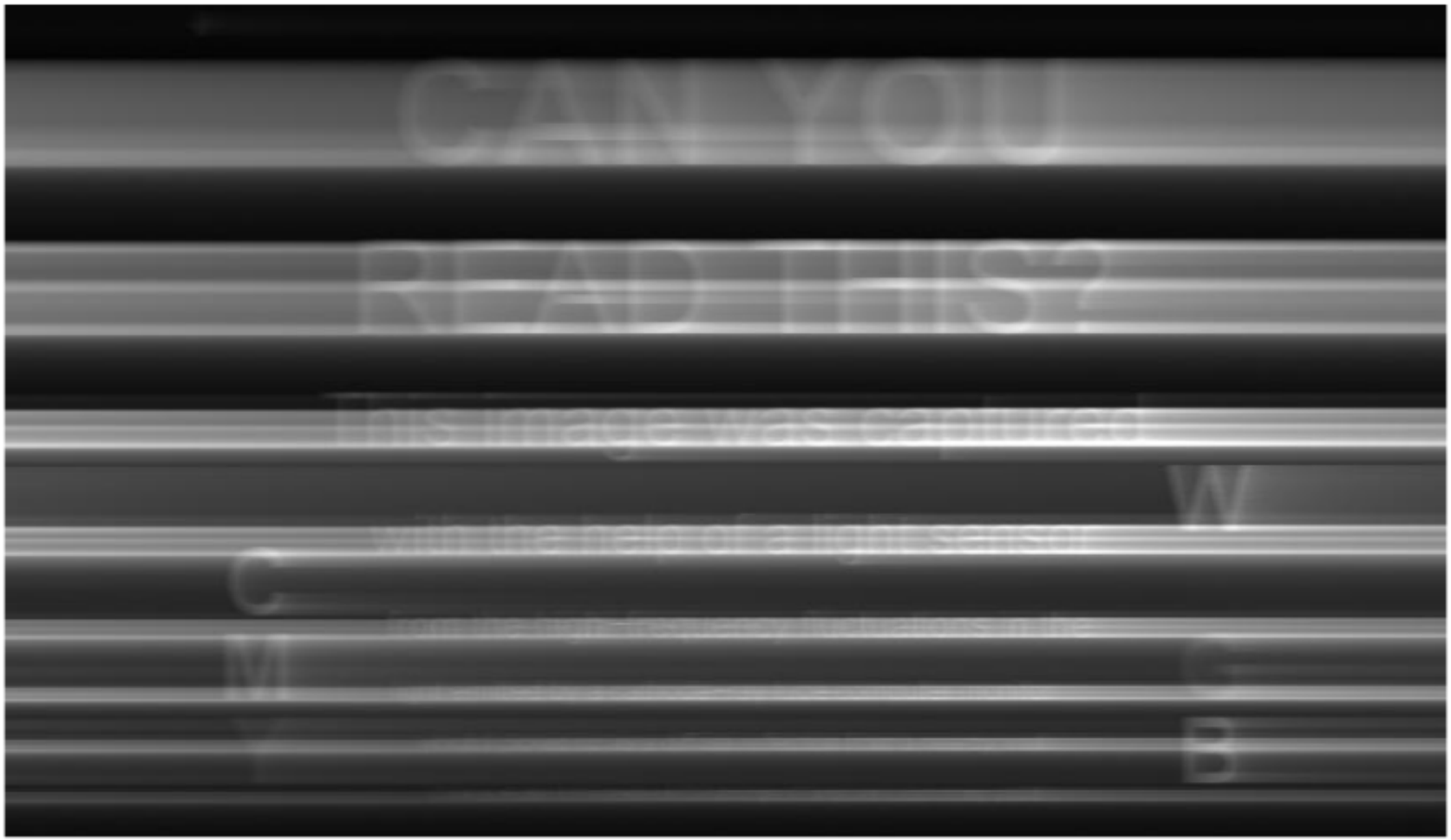
U praksi ovo nije tako jednostavno – fosfor se nece “ugasiti” odmah

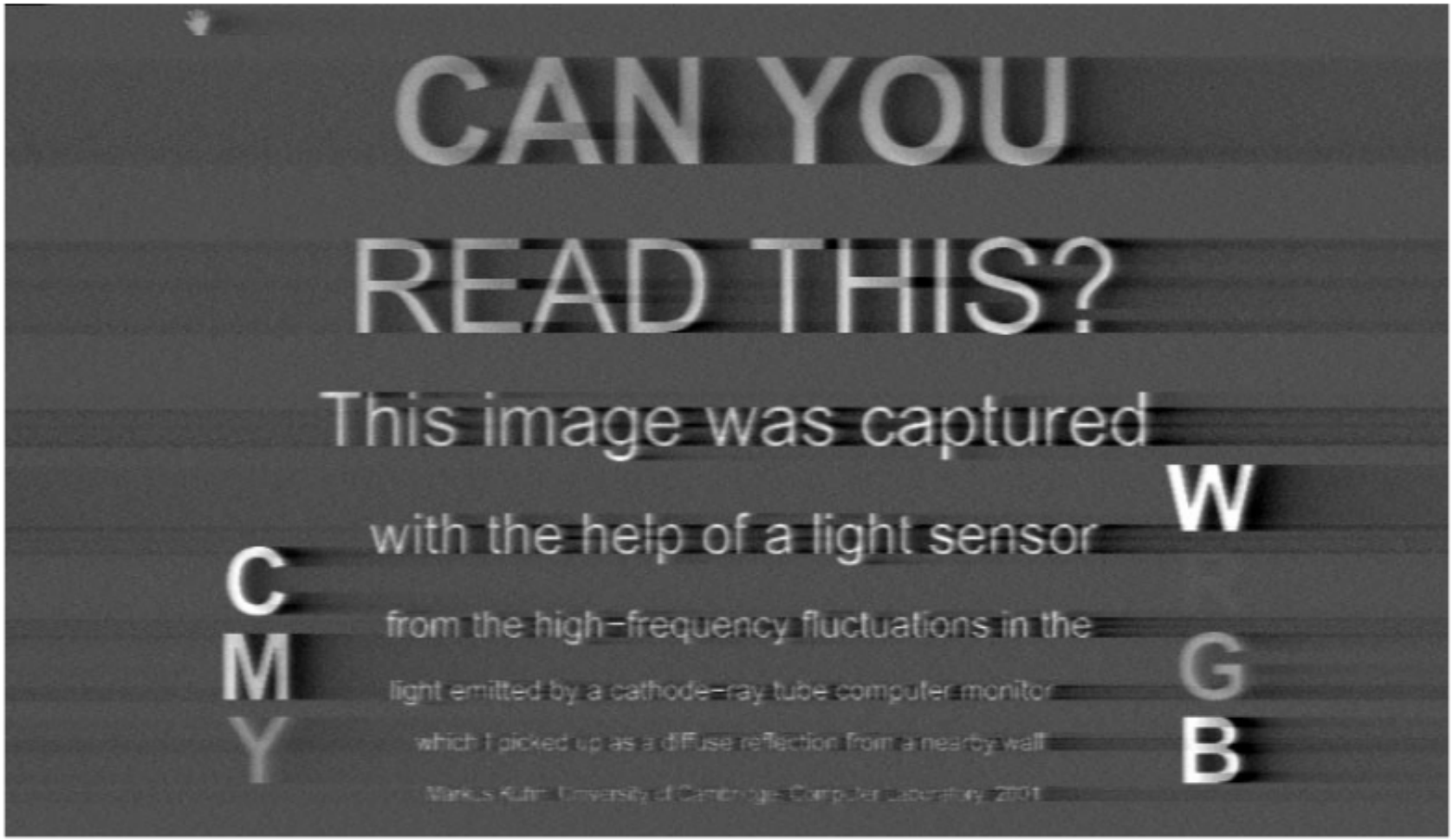
Signal koji dobijamo je suma prethodnih piksela $p(t)$, pomnoženih (opadajućim) težinama $d(t)$:

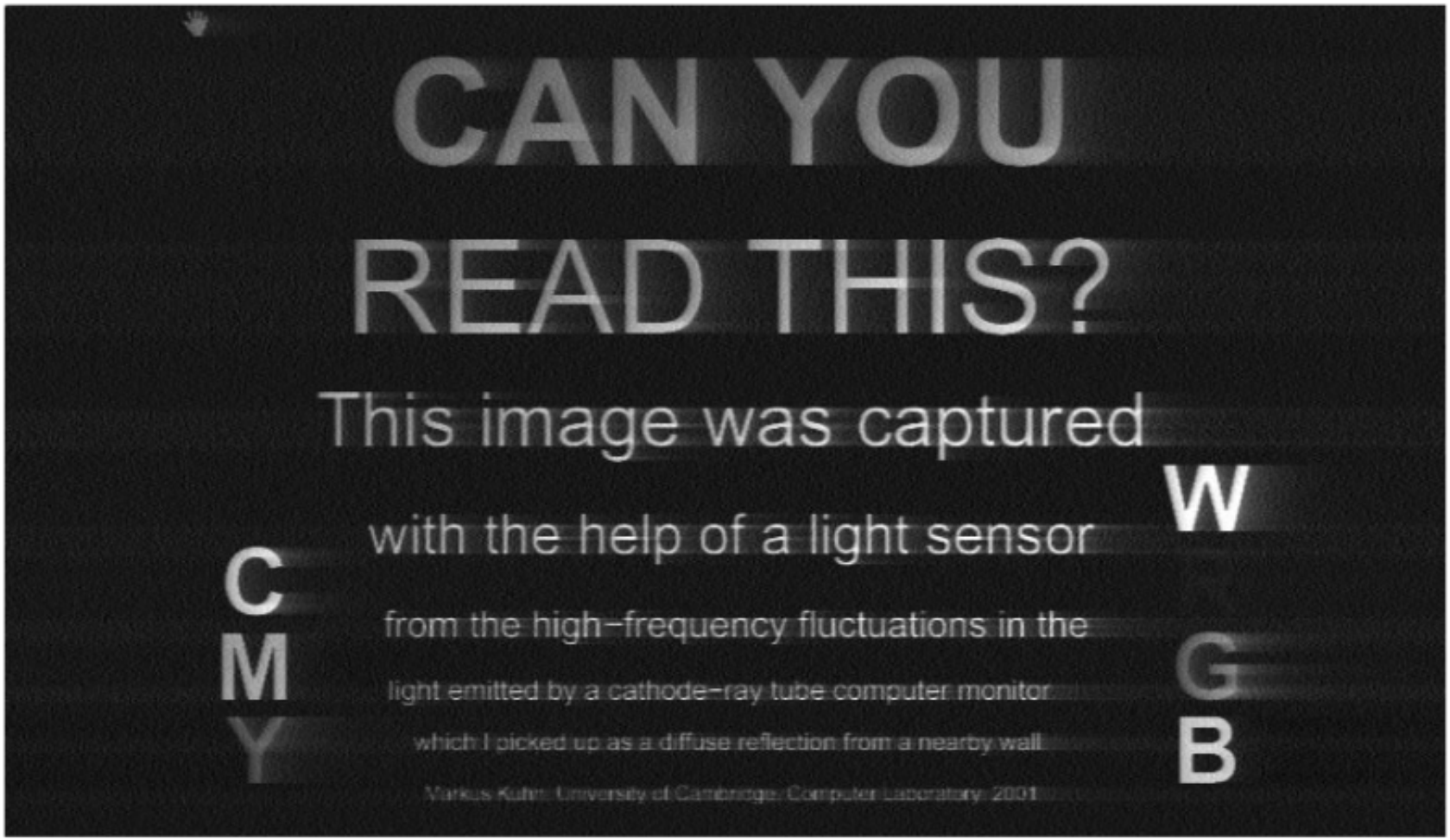
$$s(t) = d(0) \cdot p(t) + d(1) \cdot p(t-1) + d(2) \cdot p(t-2) + \ldots$$

Znamo kako $d(x)$ izgleda – možemo rekonstruisati vrednosti p_i (dekonvolucija)


CAN YOU
READ THIS?
This image was captured
with the help of a light sensor
from the high–frequency fluctuations in the
light emitted by a cathode–ray tube computer monitor
which I picked up as a diffuse reflection from a nearby wall.
Markus Kuhn, University of Cambridge, Computer Laboratory, 2001
C
M
Y
W
R
G
B




CAN YOU
READ THIS?
This image was captured
with the help of a light sensor
from the high-frequency fluctuations in the
light emitted by a cathode-ray tube computer monitor
which I picked up as a diffuse reflection from a nearby wall
C
M
Y
W
G
B


CAN YOU
READ THIS?
This image was captured
with the help of a light sensor
from the high-frequency fluctuations in the
light emitted by a cathode-ray tube computer monitor
which I picked up as a diffuse reflection from a nearby wall
Markus Kuhn, University of Cambridge, Computer Laboratory, 2001
C
M
Y
W
G
B

Optički mikrofon

Zvuk prenose vazdušne vibracije (20 Hz – 20 kHz)

Vibracije se prenose na predmete $\rightarrow$ mogu se rekonstruisati iz slike[7]

Dva problema:

- Pomeraji su veoma mali ($\approx 1/100$ px) – posmatramo celu sliku, ne samo jedan piksel
- Potreban je velik frame-rate – kamere ne snimaju sve piksele istovremeno ("*rolling shutter*"), tako da imamo više tačaka po frejmu

[7] Davis, Abe, et al. "The visual microphone: passive recovery of sound from video." (2014).

Power analysis

Merenje struje koju čip na (staroj) kreditnoj kartici troši daje informacije o kodu koji se izvršava – dovoljno za kloniranje

Različit signal za tačan i netačan karakter u password-u
$\rightarrow$ pogađanje slovo po slovo

Kompleksniji napadi na kriptografske čipove ("*differential power analysis*") – sakupi signale za slične ulaze i traži razlike da bi otkrio deo internog stanja

Glitching

Unošenje grešaka ("*glitch*") u sistem može da izazove korisne posledice

Neki stari čipovi na karticama izvršavaju `NOP` ako se dovede impuls na *clock* signal

Brisanje ROM-a zahteva visok napon (u poređenju sa čitanjem) – prelepi kontakt izolir-trakom i TV dekoder više nije moguće deaktivirati

...

Provera password-a

```
bool check_password(char pwd[], char in[]) {
    for(int i = 0; i < strlen(pwd); i++)
        if(pwd[i] != in[i]) return false;
    return true;
}
```

Vreme izvršavanja `check_password` je srazmerno sa brojem ispravnih karaktera u `in`

Ako možemo da precizno merimo vreme, nalazimo tačan password u $\mathcal{O}(nc)$ umesto $\mathcal{O}(c^n)$

Ovo nije preterano korisno u softveru, ali jeste u hardveru

Stepenovanje

```
int pow(int x, int n) {
    int res = 1;
    for(; n > 0; n >>= 1) {
        if(n & 1) res = (res * x) % MOD;
        x = (x * x) % MOD;
    }
    return res;
}
```

Stenpenovanje po modulu je osnovna operacija RSA enkripcije ($C = M^e$)

Naivna implementacija brzog stepenovanja zahteva $L + O$ množenja, gde je L duzina e u bitima, a O broj 1-bita u $e \rightarrow$ vreme izvršavanja daje broj 1-bita

```
int pow(int x, int n) {
    int res = 1;
    for(; n > 0; n >>= 1) {
        if(n & 1) res = (res * x) % MOD;
        x = (x * x) % MOD;
    }
    return res;
}
```

Ako možemo da nađemo x takvo da $res \cdot x$ traje dugo, možemo rekonstruisati e:

- Ako ovo x traje jednako dugo kao bilo koje drugo, donji bit e je 0 (inace je 1)
- Sada znamo `res` u sledećoj iteraciji – možemo odabrati x takvo da je $res \cdot x^2$ sporo
- ...

Keševi

Vreme potrebno za pristup memoriji pokazuje da li je ta vrednost u kešu ili ne

AES koristi velike *lookup* tabele ("*S-box*") – vreme pristupa daje informacije o internom stanju algoritma

Ovo je dovoljno za pronalaženje ključa u (starom) OpenSSL-u na drugom računaru koji enkriptuje podatke na zahtev[8]

Kombinacija sa out-of-order izvršavanjem u modernim procesorima $\rightarrow$ Meltdown, Spectre

[8] Bernstein, Daniel J. "Cache-timing attacks on AES." (2005): 3.