Side Channels

CS 161: Computer Security

Prof. David Wagner

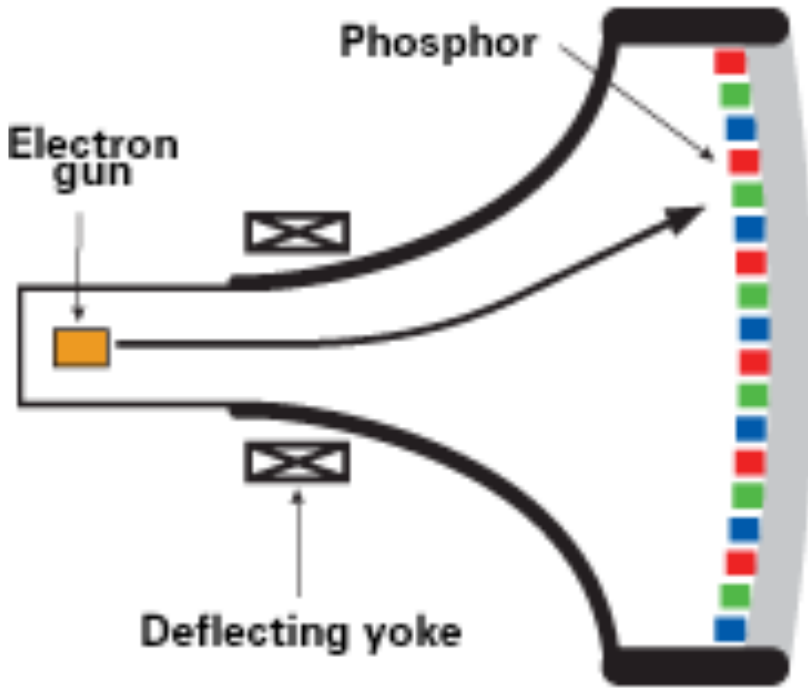
April 23, 2013

UI Side Channel Snooping

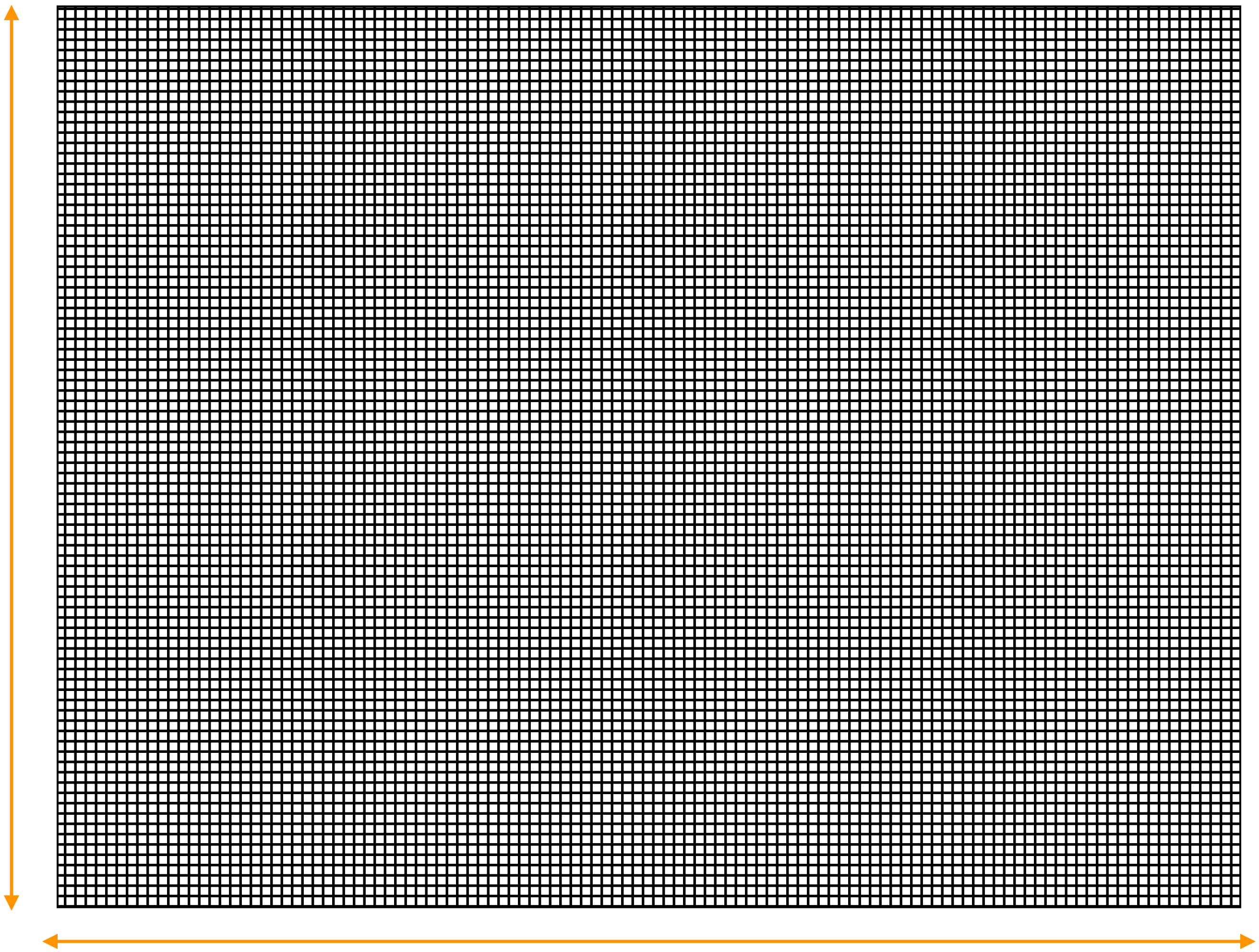
- Scenario: Ann the Attacker works in a building across the street from Victor the Victim. Late one night Ann can see Victor hard at work in his office, but can't see his CRT display, just the glow of it on his face.

- Can Ann still somehow snoop on what Victor's display is showing?

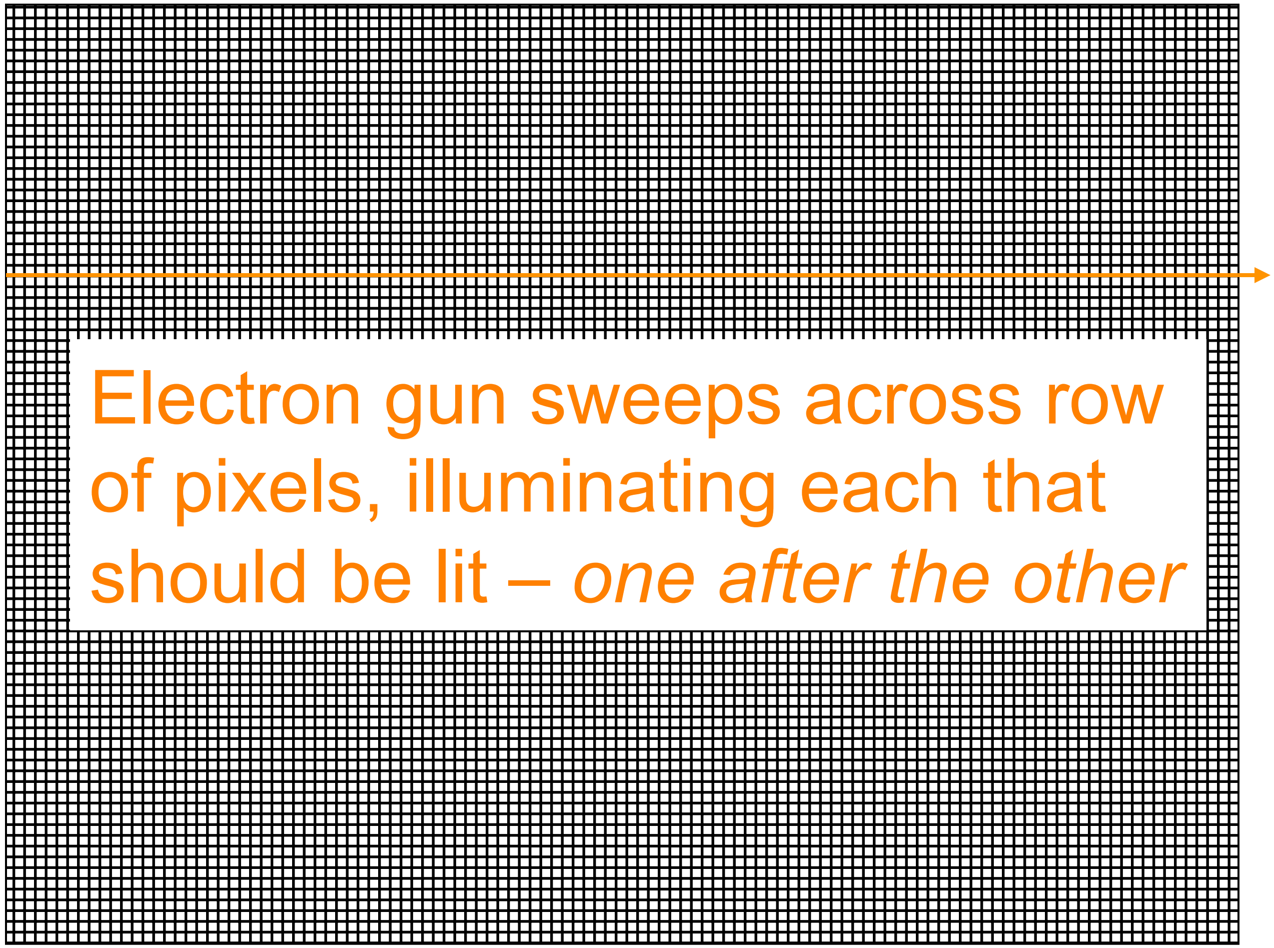
CRT

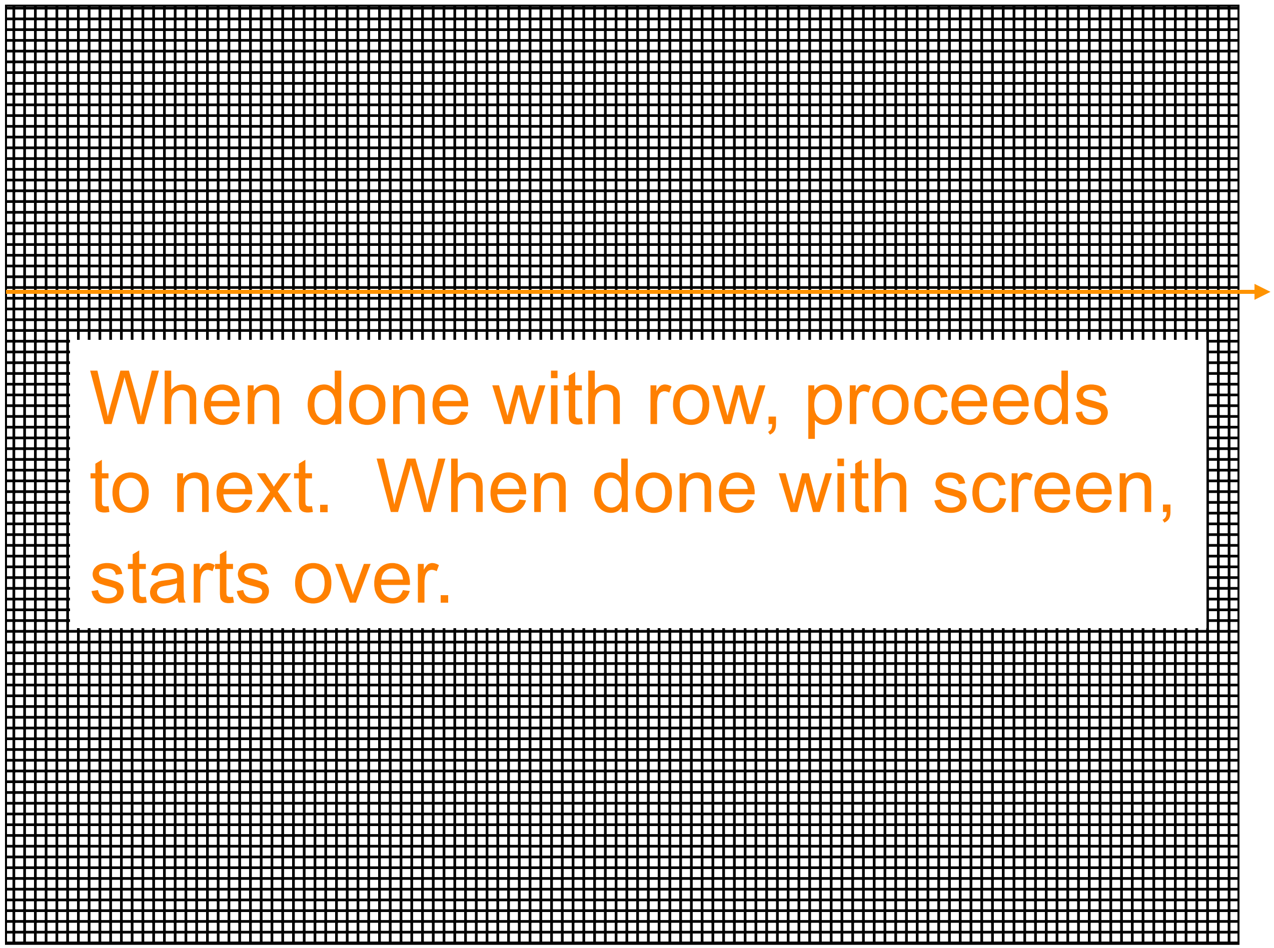


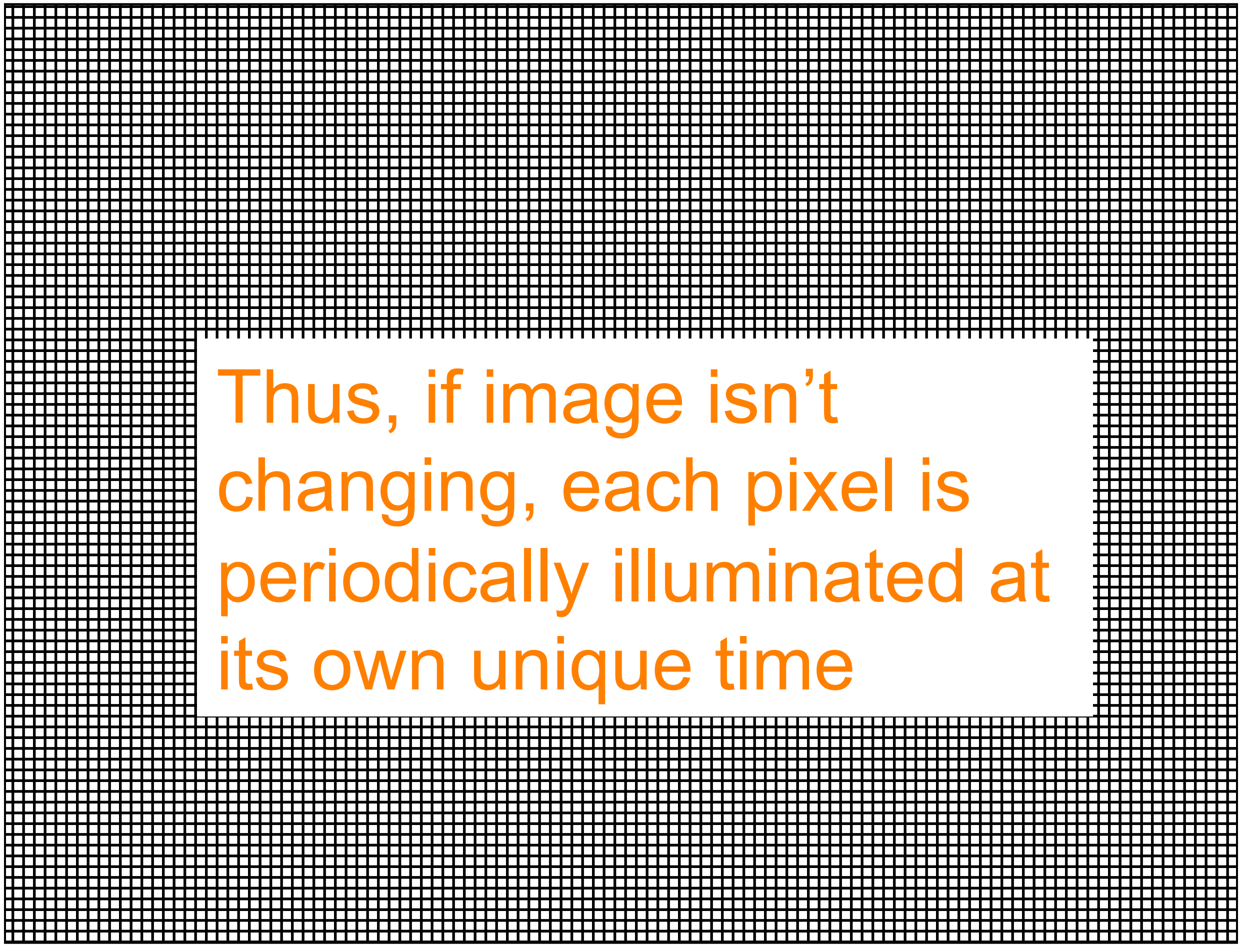
CRT display is made up of
an array of phosphor pixels



640x480 (say)

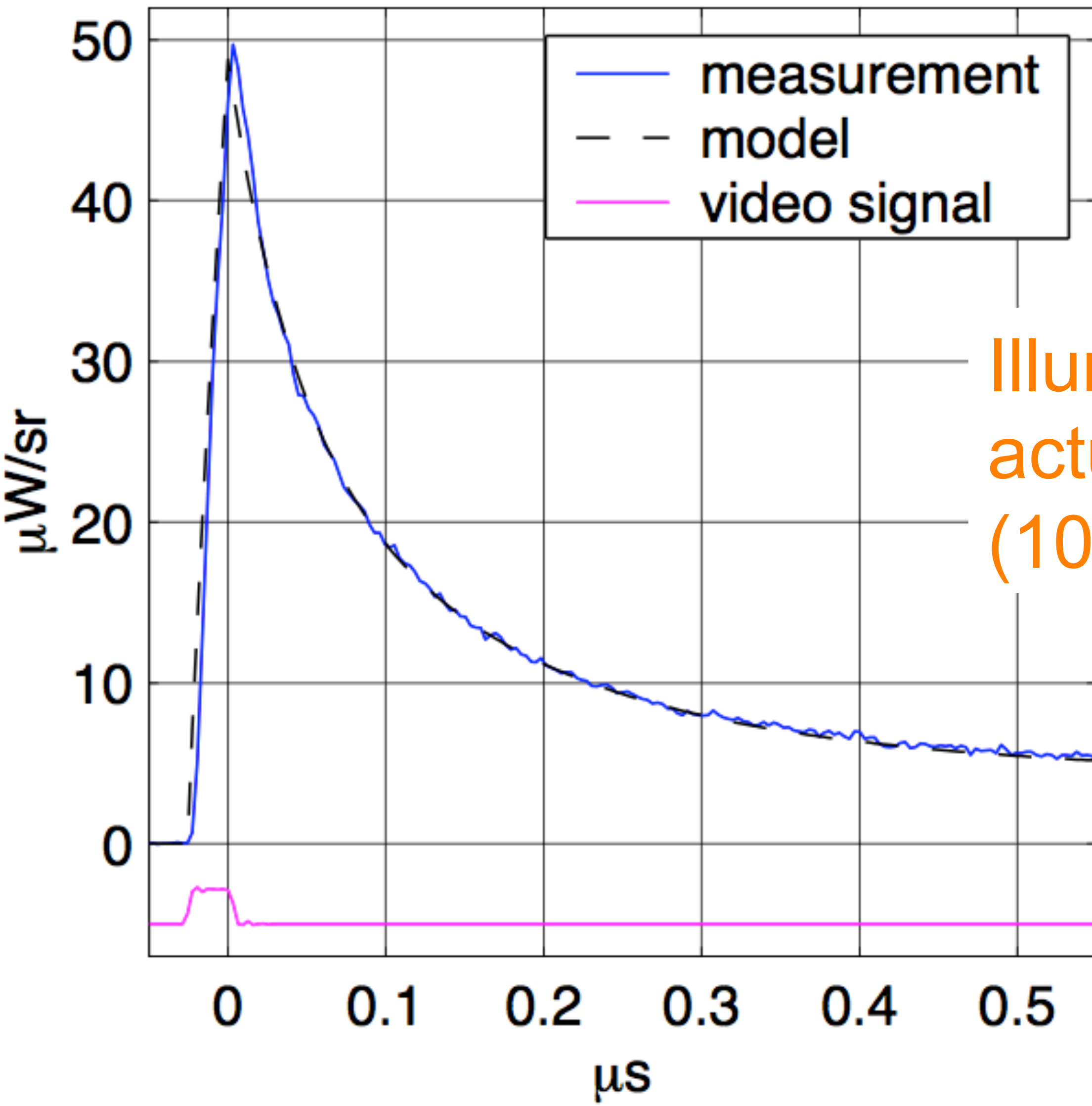

Electron gun sweeps across row of pixels, illuminating each that should be lit – *one after the other*


When done with row, proceeds to next. When done with screen, starts over.



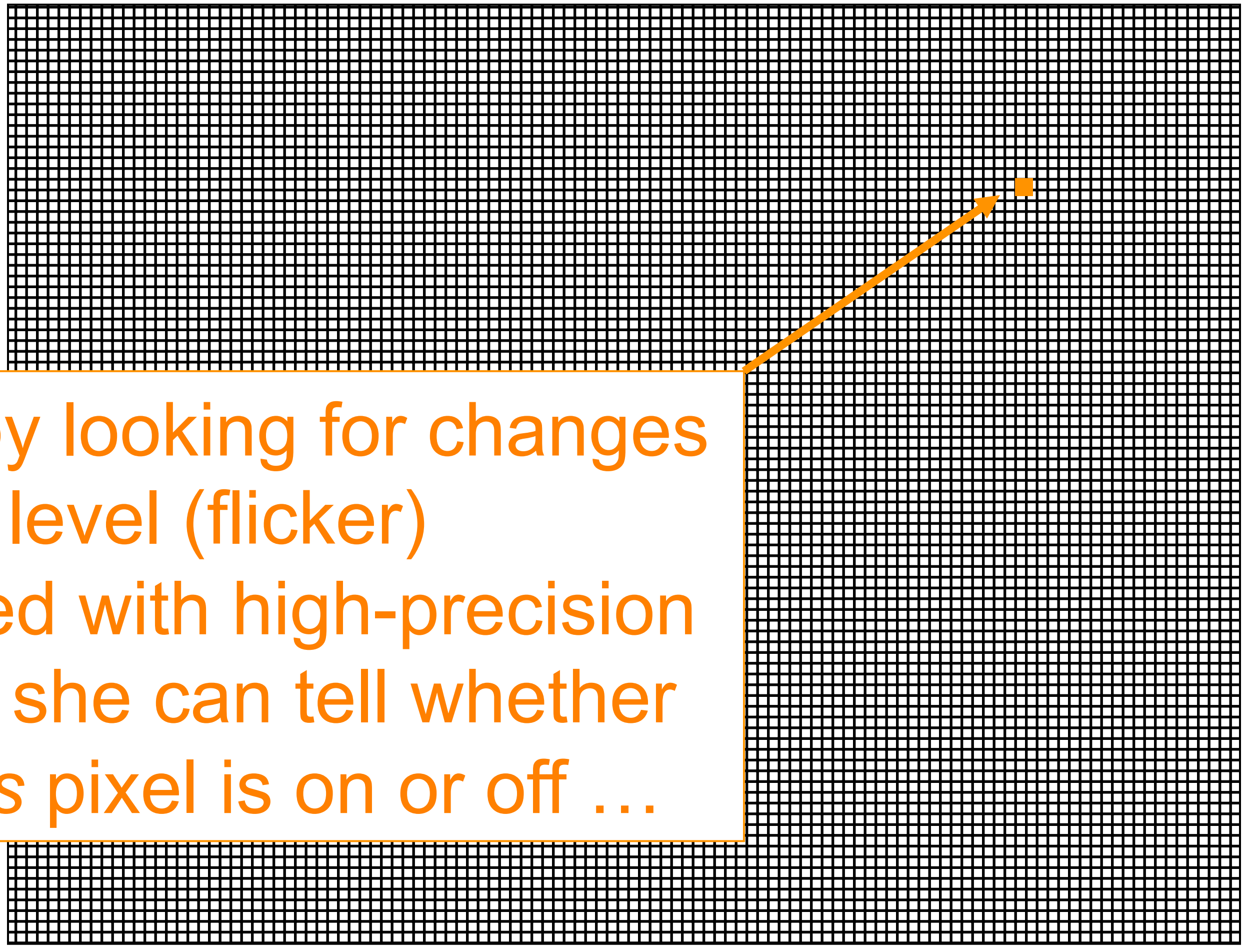
Thus, if image isn't changing, each pixel is periodically illuminated at its own unique time

(a) Emission decay of a single pixel (f_p = 36 MHz)

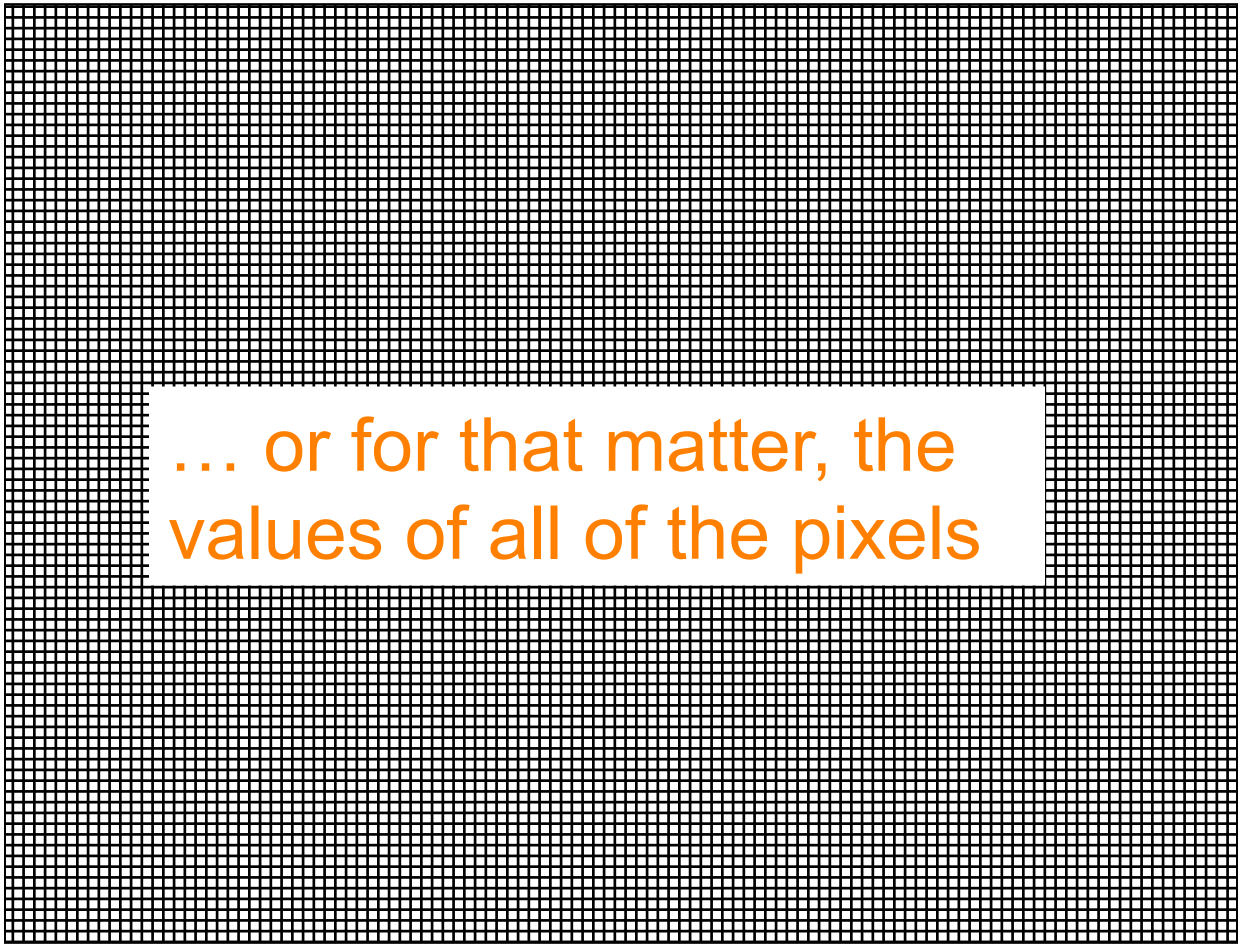


Illumination is actually short-lived (100s of nsec).

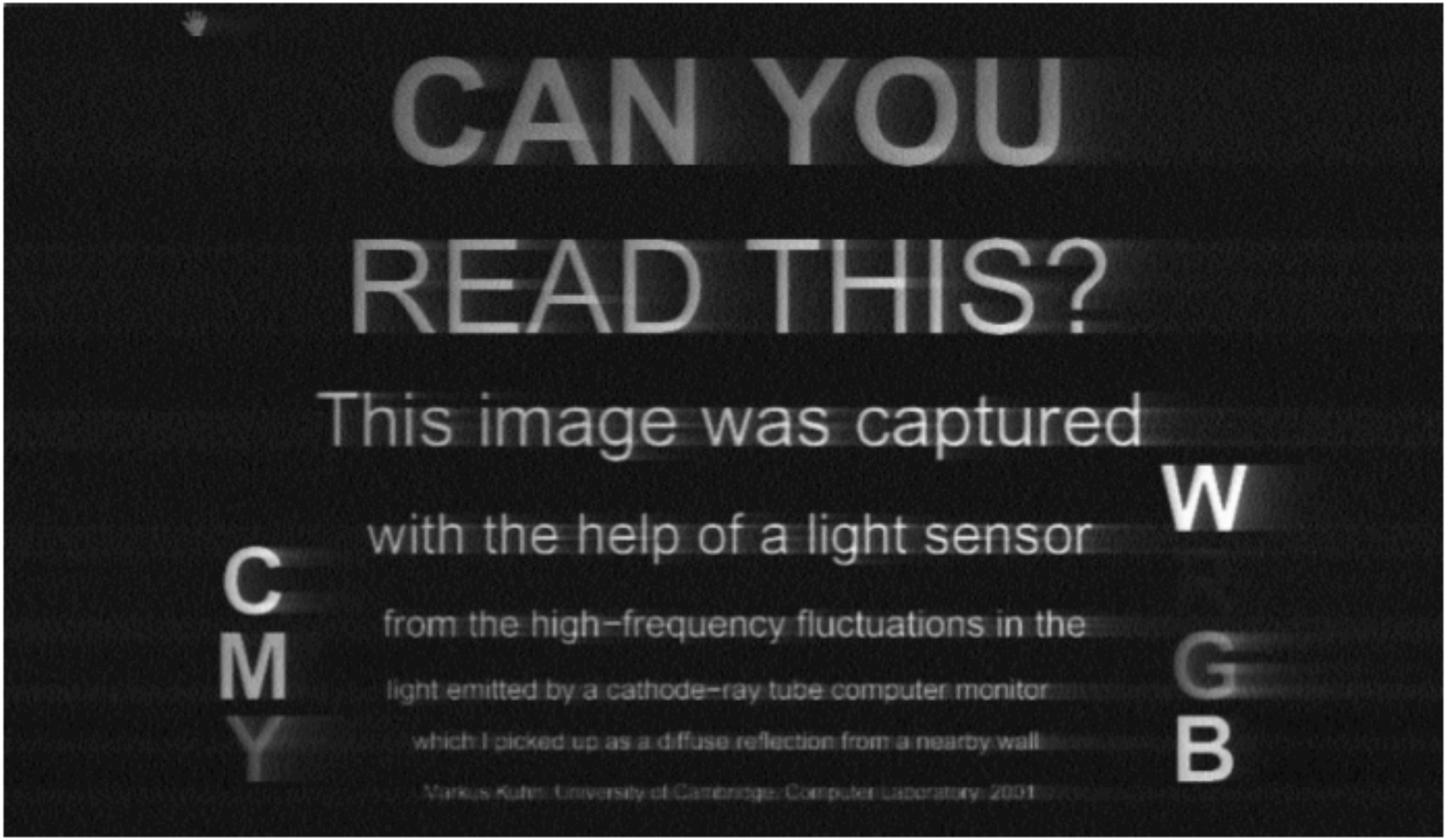
So if Ann can synchronize a high-precision clock with when the beam starts up here …



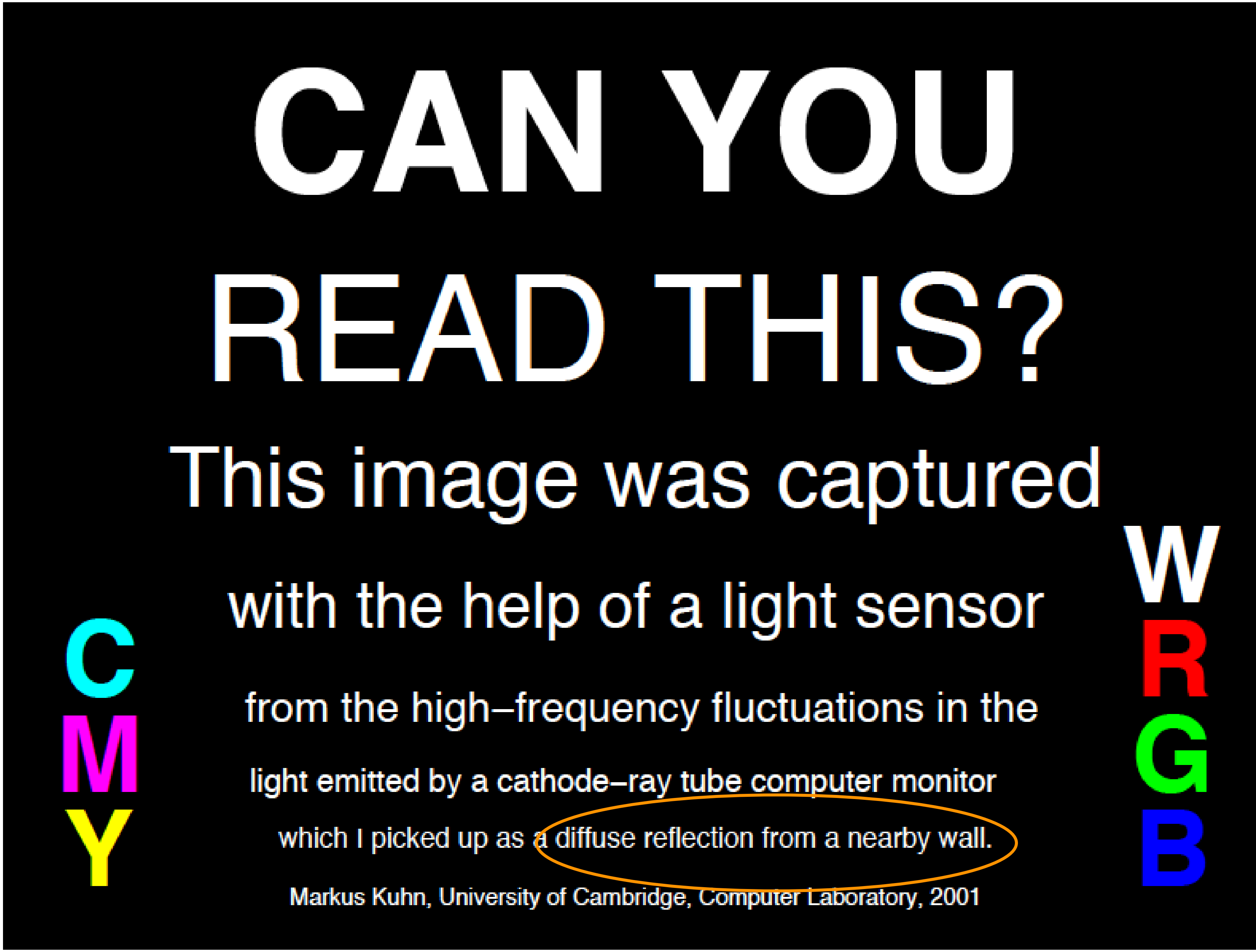
Then by looking for changes in light level (flicker) matched with high-precision timing, she can tell whether say *this* pixel is on or off …



… or for that matter, the values of all of the pixels



Photomultiplier + high-precision timing + deconvolution to remove noise


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

NIGHTWATCH

ANT Product Data

(TS//SI//REL TO USA,FVEY) NIGHTWATCH is a portable computer with specialized, internal hardware designed to process progressive-scan (non-interlaced) VAGRANT signals.

24 Jul 2008

(U) Capability Summary

(TS//SI//REL TO USA,FVEY) The current implementation of NIGHTWATCH consists of a general-purpose PC inside of a shielded case. The PC has PCI digitizing and clock cards to provide the needed interface and accurate clocking required for video reconstruction. It also has:

- horizontal sync, vertical sync and video outputs to drive an external, multi-sync monitor.
- video input
- spectral analysis up to 150 kHz to provide for indications of horizontal and vertical sync frequencies
- frame capture and forwarding
- PCMCIA cards for program and data storage
- horizontal sync locking to keep the display set on the NIGHTWATCH display.
- frame averaging up to 2^16 (65536) frames.

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The video output from an appropriate collection system, such as a CTX4000, PHOTOANGLO, or general-purpose receiver, is connected to the video input on the NIGHTWATCH system. The user, using the appropriate tools either within NIGHTWATCH or externally, determines the horizontal and vertical sync frequencies of the targeted monitor. Once the user matches the proper frequencies, he activates "Sync Lock" and frame averaging to reduce noise and improve readability of the targeted monitor. If warranted, the user then forwards the displayed frames over a network to NSAW, where analysts can look at them for intelligence purposes.

Unit Cost: N/A

Status: This system has reached the end of its service life. All work concerning the NIGHTWATCH system is strictly for maintenance purposes. This system is slated to be replaced by the VIEWPLATE system.

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

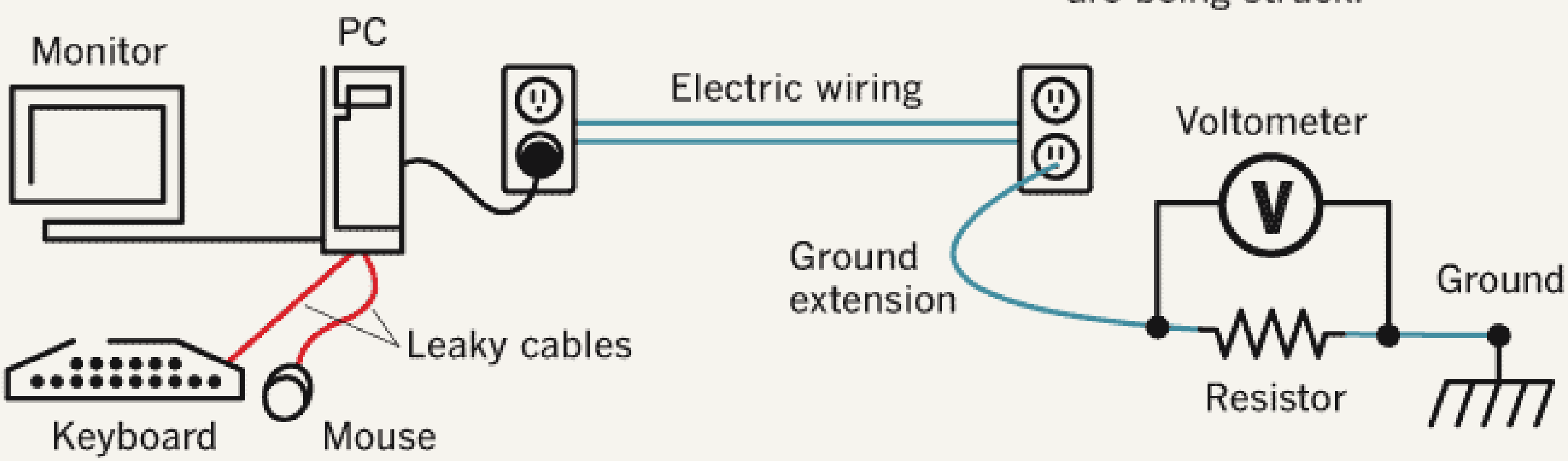
UI Side Channel Snooping

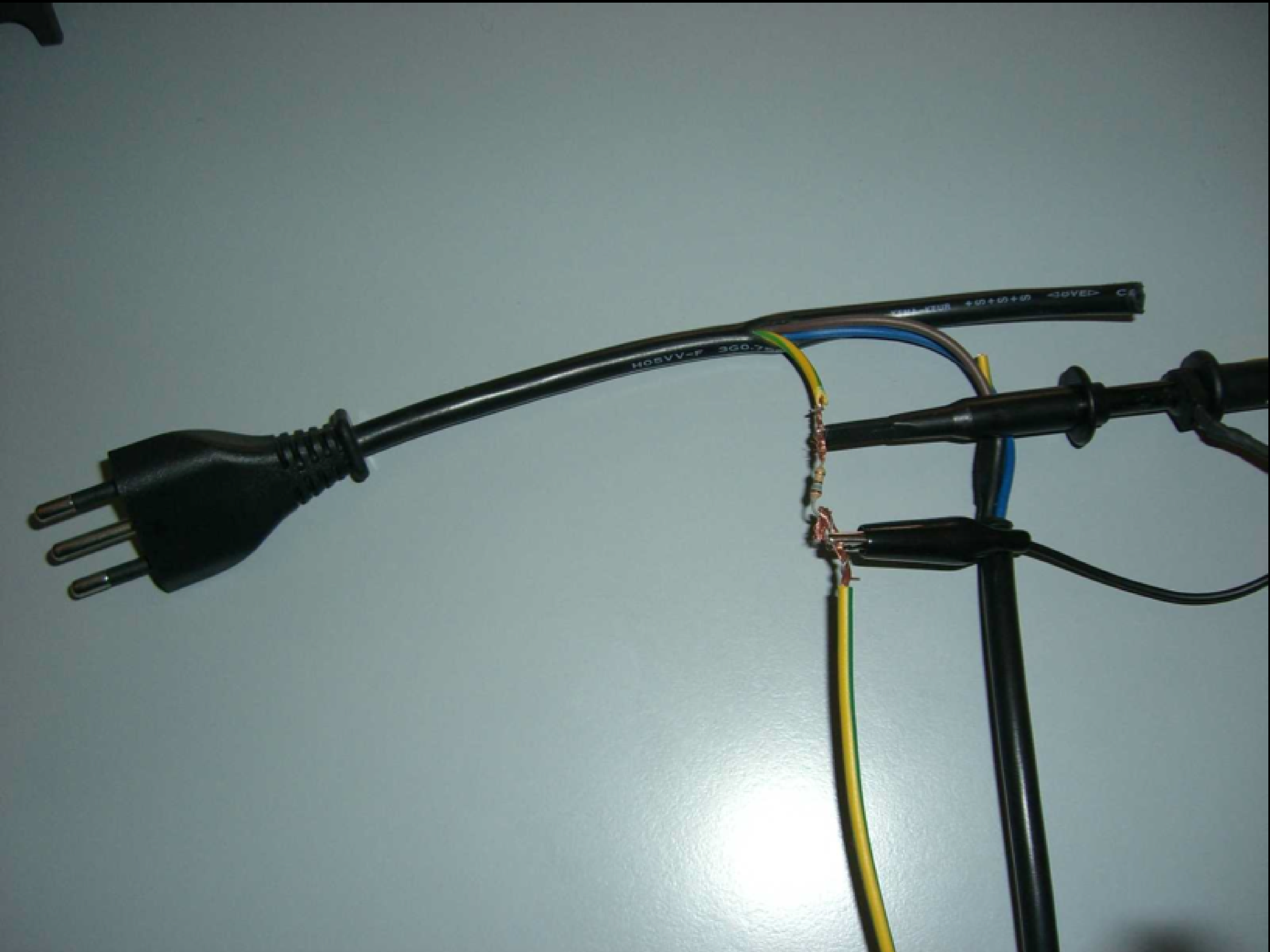
- Victor switches to an LCD display. Any other ways Ann can still steal his display contents or his keystrokes?
- Cables from computer to screen & keyboard act as crude antennas!
  - Broadcast weak RF signals corresponding to data streams (as does a CRT's operation – "Tempest")
  - Even induce faint voltage fluctuations in power lines

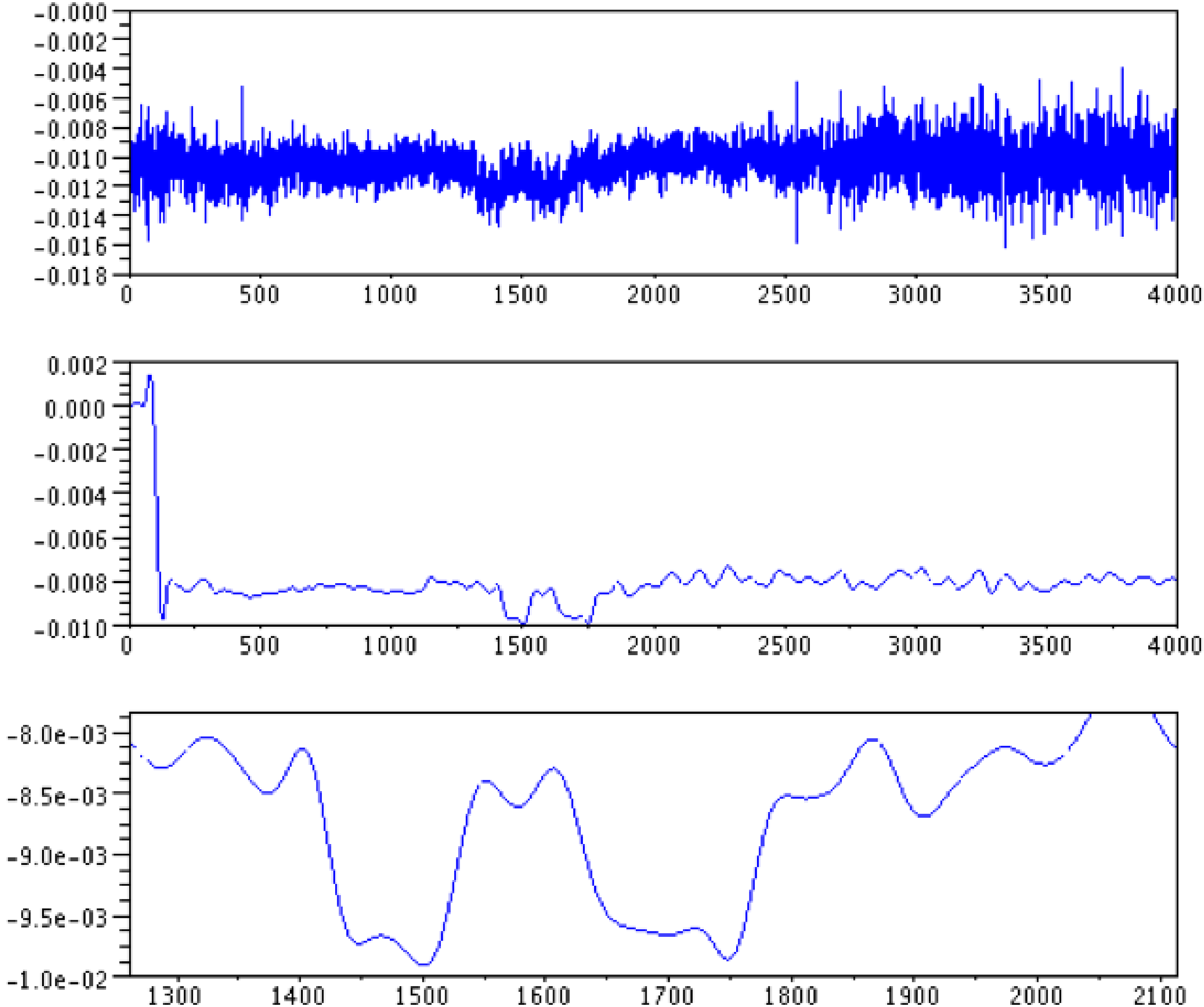
Stealing keystrokes through electric lines

Relatively simple equipment can tap power lines to intercept what is being typed on nearby keyboards.

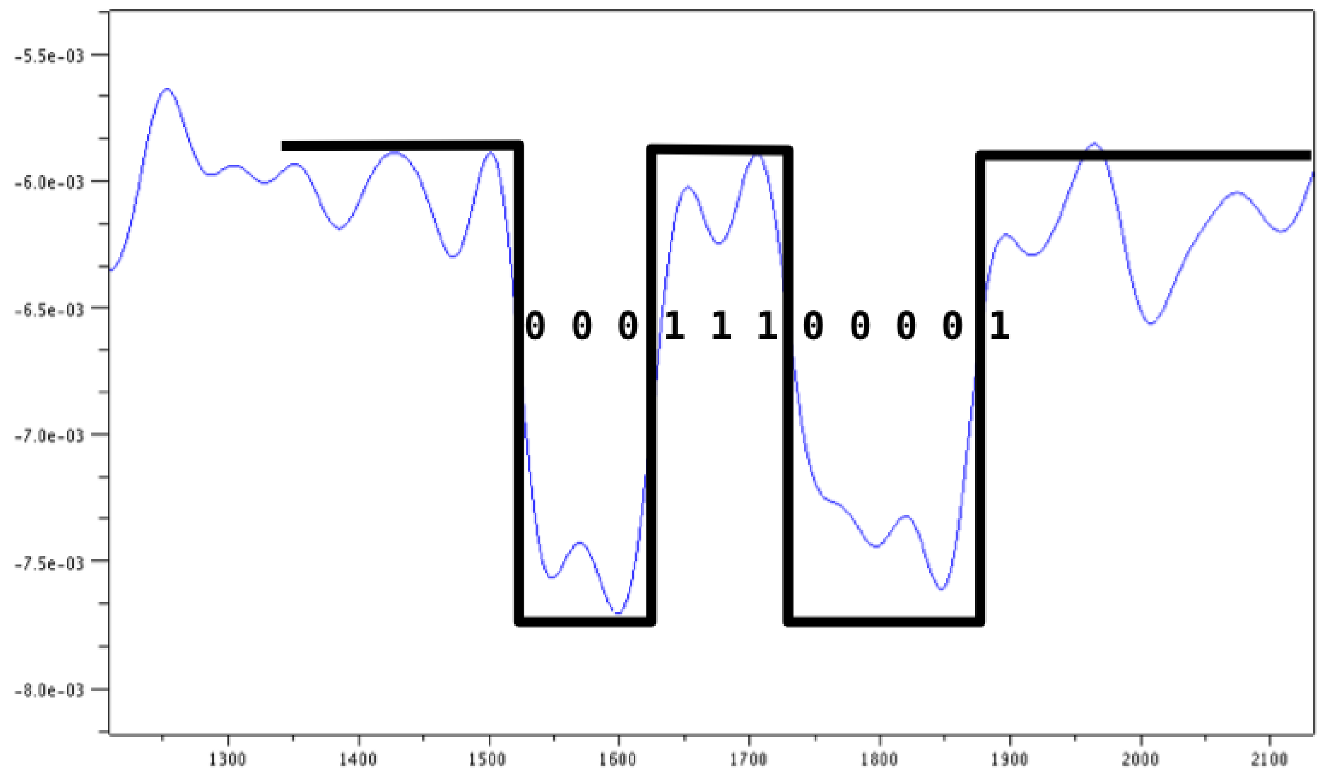
1. Unshielded wires in keyboard cables leak keystroke signals into the cable ground.
2. The signals continue along the ground wire of the electrical service feeding the PC.
3. Measuring voltage shifts across an extension of the electric-system ground reveals what keys are being struck.




H05VV-F


-0.000
-0.002
-0.004
-0.006
-0.008
-0.010
-0.012
-0.014
-0.016
-0.018
0 500 1000 1500 2000 2500 3000 3500 4000
0.002
0.000
-0.002
-0.004
-0.006
-0.008
-0.010
0 500 1000 1500 2000 2500 3000 3500 4000
-8.0e-03
-8.5e-03
-9.0e-03
-9.5e-03
-1.0e-02
1300 1400 1500 1600 1700 1800 1900 2000 2100

- | 0 | 00111000 | 0 | 1 | = letter 'a'



Copyright 2009 Inverse Path Ltd.

UI Side Channel Snooping

- Victor switches to an LCD display. Any other ways Ann can still steal his display contents or his keystrokes?
- Cables from computer to screen & keyboard act as crude antennas!
  – Broadcast weak RF signals corresponding to data streams
  – Even induce faint voltage fluctuations in power lines
- Keystrokes create sound
  – Audio components unique per key
  – Timing reflects key sequencing / touch typing patterns
    - If language known, can employ spell-checking to clean up errors
  – Can listen w/ any convenient microphone (e.g, telephone!)
  – Can “listen” from a distance using laser + telescope!

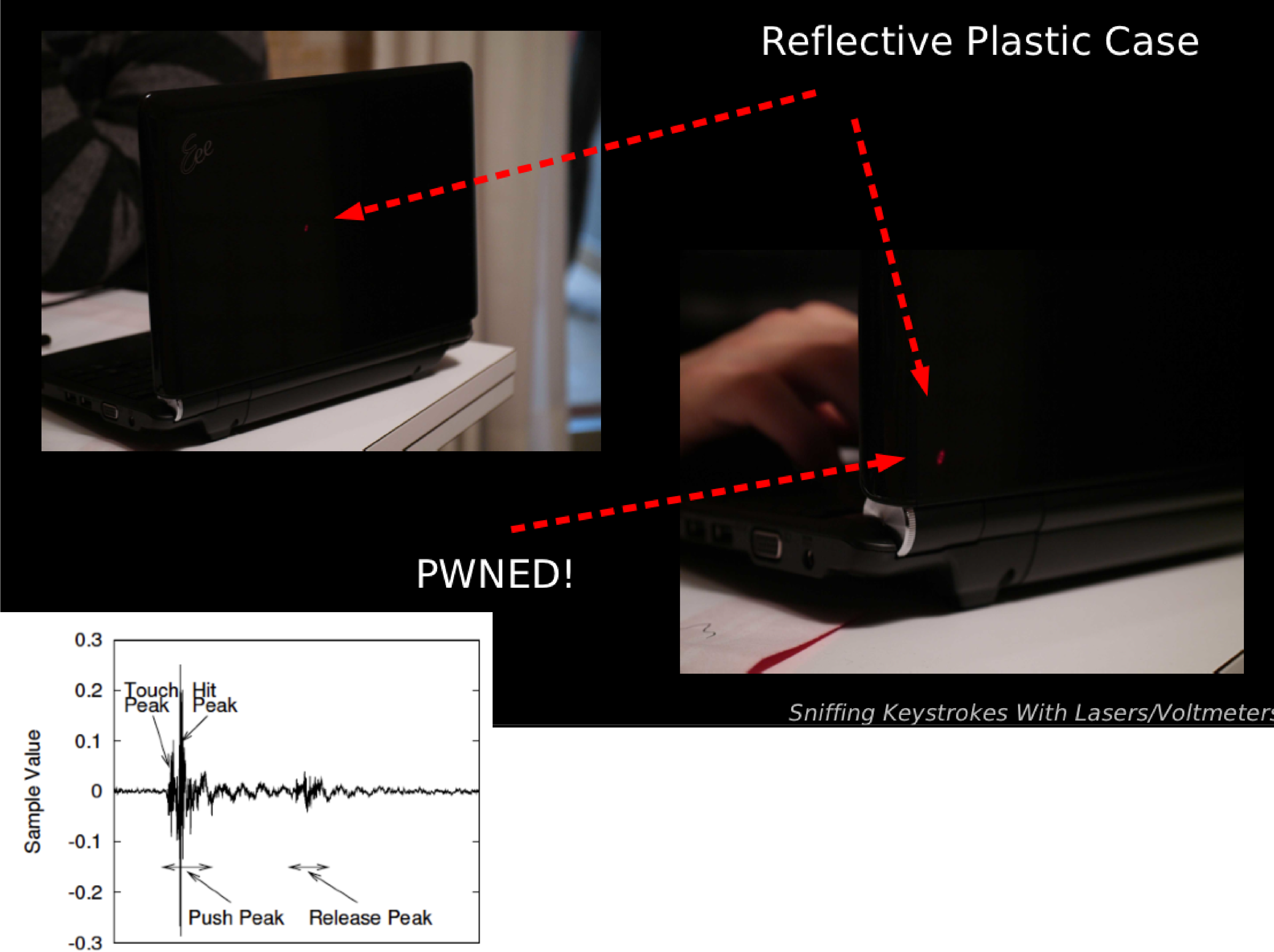

Reflective Plastic Case
PWNED!
Sniffing Keystrokes With Lasers/Voltmeters
Sample Value
0.3
0.2
0.1
0
-0.1
-0.2
-0.3
Touch Peak
Hit Peak
Push Peak
Release Peak

Figure 6. Reflections in two other tea pots, taken from a distance of 5m. The 18pt font is readable from the reflection in the left picture, and almost readable in the right picture.

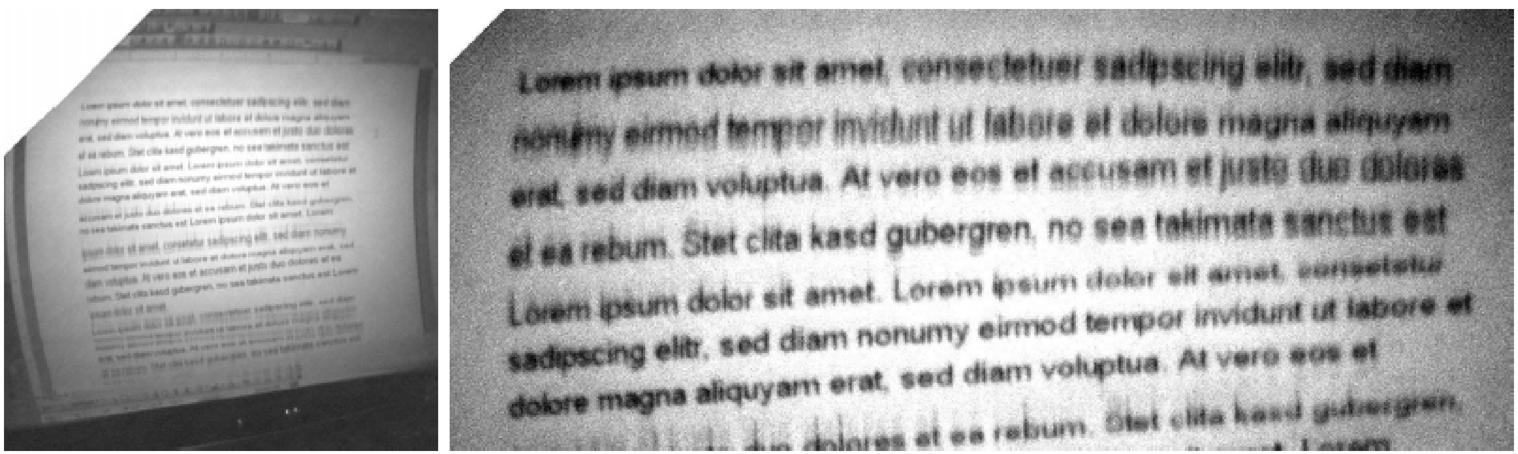


Figure 7. Reflection of a Word document with small 12pt font size in a tea pot, taken from a distance of 5m. The 12pt font is readable from the reflection.

Figure 9. Image taken with a macro lens from very short distance, with realistic distance between the monitor and the eye. Readability is limited by the resolution of the camera.

Figure 10. Reflections in two different pairs of glasses, taken from a distance of 5m. Both the inner side and the outer side of glasses produce reflections. The 18pt font is readable from the reflection.

Side Channels in Web Surfing

- Suppose Alice is surfing the web and all of her traffic is encrypted and running through an anonymizer
- Eve can observe the presence of Alice's packets & their size, but can't read their contents or ultimate destination
- How can Eve deduce that Alice is visiting FoxNews (say)?

www.foxnews.com

Reader

FOX NEWS .com Fair & Balanced

April 21, 2014 -- Updated at 4:30 PM ET

Search

Listen to Fox News Radio Live ›

ON AIR NOW ›

5p et The Five

WATCH LIVE

On Air Personalities ›

6p et Special Report w/ Bret Baier

Hosted by Bret Baier

End of train line for small-town USA?

AMTRAK SAYS CUSTOMERS along a 600-mile stretch of a famous line that runs from Chicago to Los Angeles will lose service in 2016 unless the states they live in cough up enough cash to upgrade aging track.

- VIDEO: Amtrak service pulling out of small towns?

SNEAKY FUNDRAISING? White House solicited $$ for ObamaCare group

- David Axelrod: 'Angry' ObamaCare opponents are 'more mobilized' for the 2014 elections
- FOX NEWS FIRST: Jeb gets

CHEM WEAPONS USE? 'Indications' of new attack in Syria — but whose?

- Assad reportedly visits Christian village

A FEW GOOD MEN Marines issue casting call for 'terrorist' training

- Drone strike in Yemen kills 55 Al Qaeda militants
- Federal court: Administration must release memos allowing drone strikes on Americans

61°

New York, NY

Detailed Forecast ›

MARKETS

FOX BUSINESS

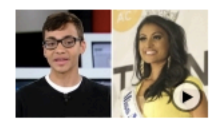
DJIA	16,449.25	+40.71	+0.25%
Nasdaq	4,121.55	+26.03	+0.64%
S&P 500	1,871.89	+7.04	+0.38%

Enter Stock Symbol | Get Quote

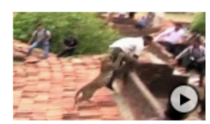
- Pershing, Valeant Team Up to Buy Allergan
- Did Square Really Hold Acquisition Talks?
- Netflix Logs 1Q EPS Beat

WATCH NOW

Does the president have an 'image problem'?



High schooler doesn't regret asking Miss America to prom



Leopard attacks villagers, causes panic

Teen stowaway's adventure raises security concerns

Page Info – http://www.foxnews.com/

General | Media | Feeds | Permissions | Security

Address	Size
http://global.fncstatic.com/static/v/all/img/fn-header-update.jpg	20.95 KB
http://global.fncstatic.com/static/v/all/img/head/logo-foxnews-update.png	5.57 KB
http://global.fncstatic.com/static/v/all/img/bg-icon-9.png	6.85 KB
http://global.fncstatic.com/static/v/all/img/head/profile.png	0.35 KB
http://global.fncstatic.com/static/v/all/img/bg-icon-10.png	Unknown
http://global.fncstatic.com/static/v/all/img/head/microphone.png	0.35 KB
http://a57.foxnews.com/www.foxnews.com/i/redes/onair/0/0/image_30_201006141647.jpg	1.62 KB
http://global.fncstatic.com/static/all/img/watch-icon.gif	0 KB
http://a57.foxnews.com/www.foxnews.com/i/redes/onair/0/0/image_8_201006141647.jpg	1.64 KB
http://global.fncstatic.com/static/v/all/img/bg-icon-11.png	0.64 KB
http://global.fncstatic.com/static/v/all/img/bg-btn-14.gif	1.58 KB
http://global.fncstatic.com/static/v/all/img/bg-layer-6.gif	0.05 KB
http://glo	0.06 KB
http://glo	0.06 KB
http://glo	0.06 KB
http://glo	0.06 KB
http://glo	0.06 KB
http://glo	0.06 KB
http://glo	0.06 KB
http://glo	0.06 KB
http://global.fncstatic.com/static/v/all/img/clear.gif	0.06 KB
http://global.fncstatic.com/static/v/all/img/clear.gif	0.06 KB

Eve "fingerprints" web sites based on the specific sizes of the items used to build them. Looks for groups of ciphertext that total the same sizes.

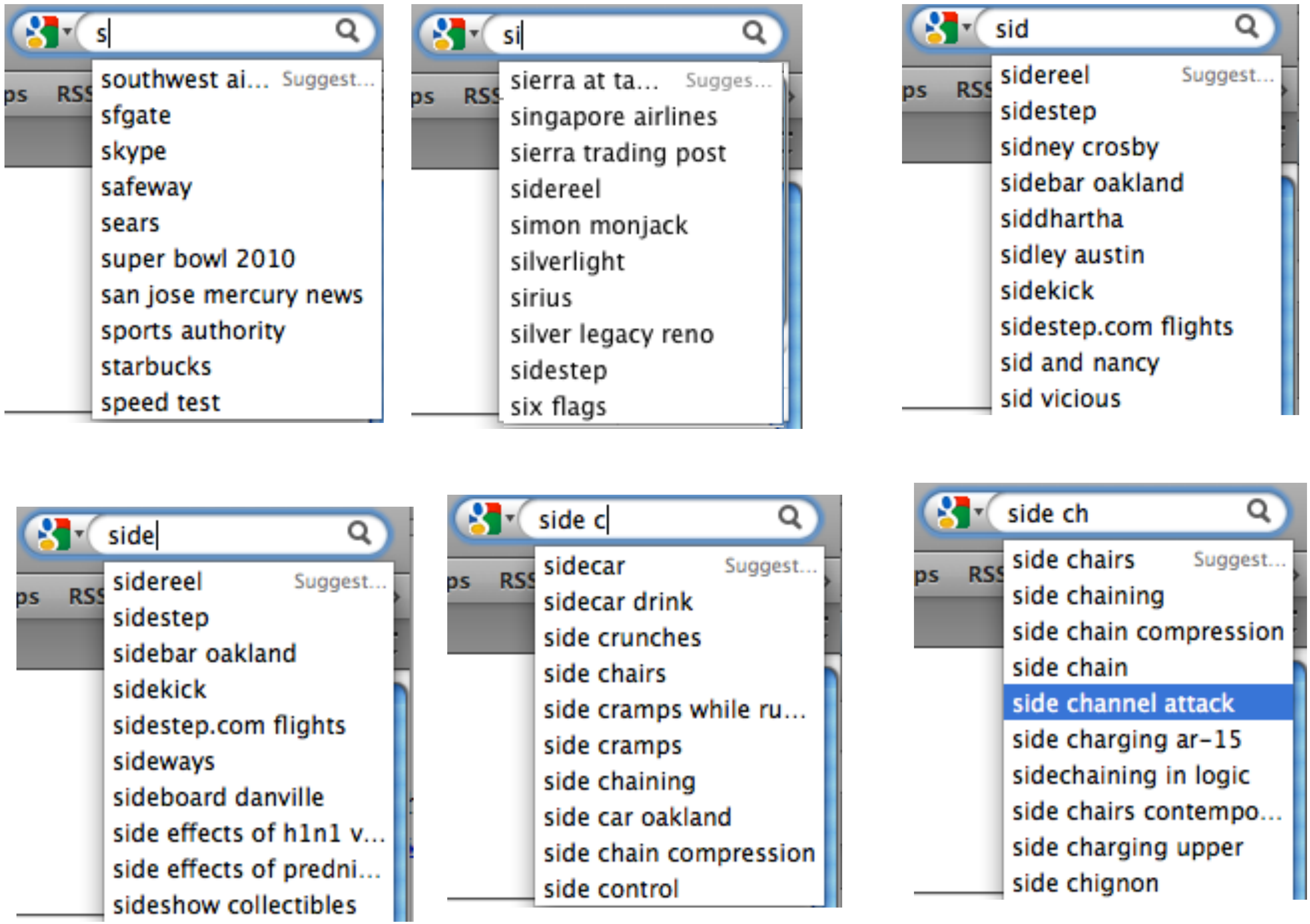
Location: http://global.fncstatic.com/static/v/fn-hp/img/favicon.png

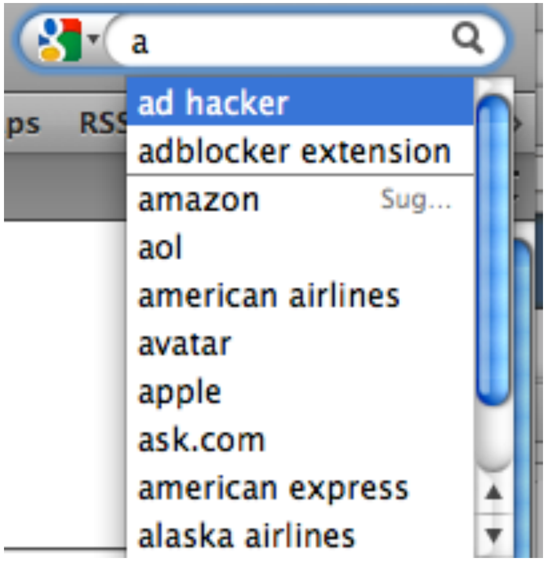
Type: PNG Image

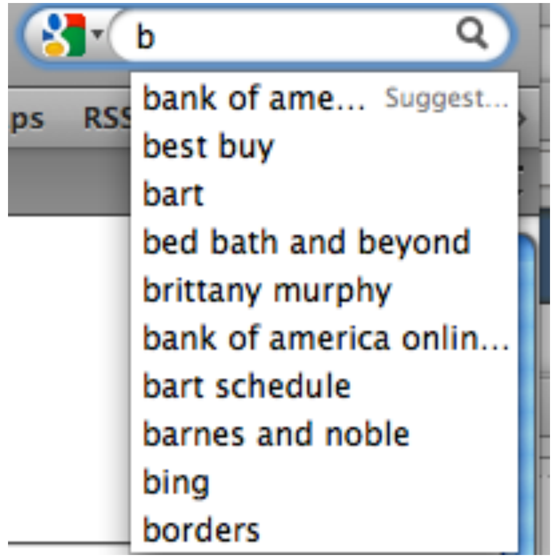
Size: 0.84 KB (857 bytes)

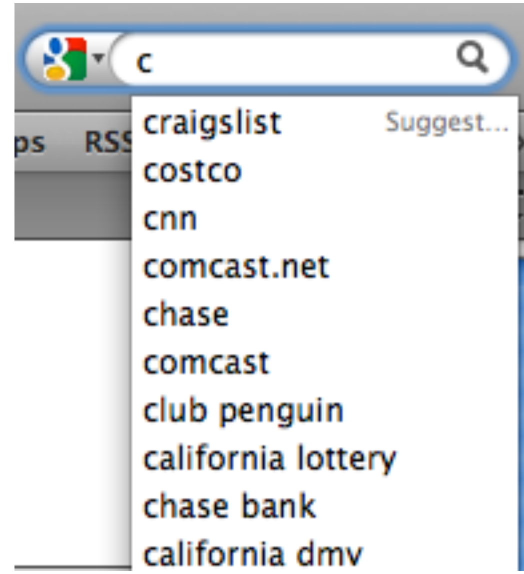
Side Channels in Web Surfing

- Suppose Alice is surfing the web and all of her traffic is encrypted and running through an anonymizer
- Eve can observe the presence of Alice’s packets & their size, but can’t read their contents or ultimate destination
- How can Eve deduce that Alice is visiting FoxNews (say)?
- What about inferring what terms Alice is searching on?


s
southwest ai... Suggest...
sfgate
skype
safeway
sears
super bowl 2010
san jose mercury news
sports authority
starbucks
speed test
si
sierra at ta... Sugges...
singapore airlines
sierra trading post
sidereel
simon monjack
silverlight
sirius
silver legacy reno
sidestep
six flags
sid
sidereel Suggest...
sidestep
sidney crosby
sidebar oakland
siddhartha
sidley austin
sidekick
sidestep.com flights
sid and nancy
sid vicious
side
sidereel Suggest...
sidestep
sidebar oakland
sidekick
sidestep.com flights
sideways
sideboard danville
side effects of h1n1 v...
side effects of predni...
sideshow collectibles
side c
sidecar Suggest...
sidecar drink
side crunches
side chairs
side cramps while ru...
side cramps
side chaining
side car oakland
side chain compression
side control
side ch
side chairs Suggest...
side chaining
side chain compression
side chain
side channel attack
side charging ar-15
sidechaining in logic
side chairs contempo...
side charging upper
side chignon







102 chars.

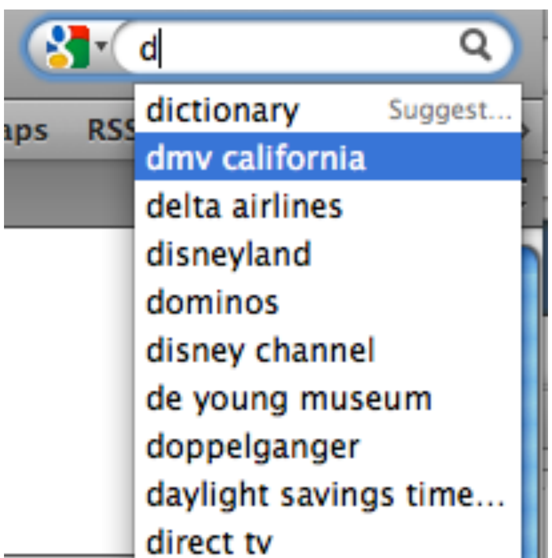
125 chars.

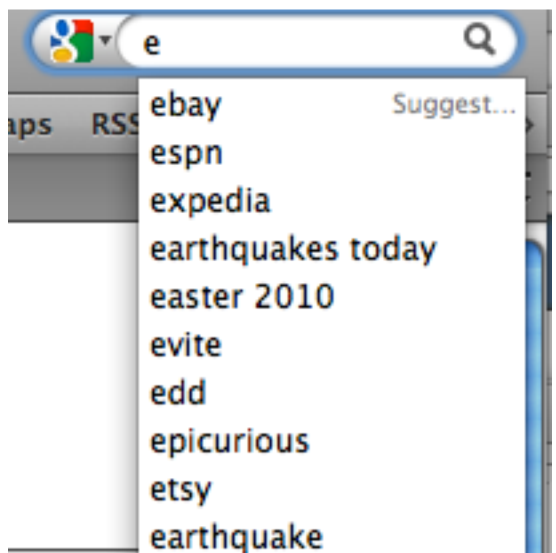
107 chars.

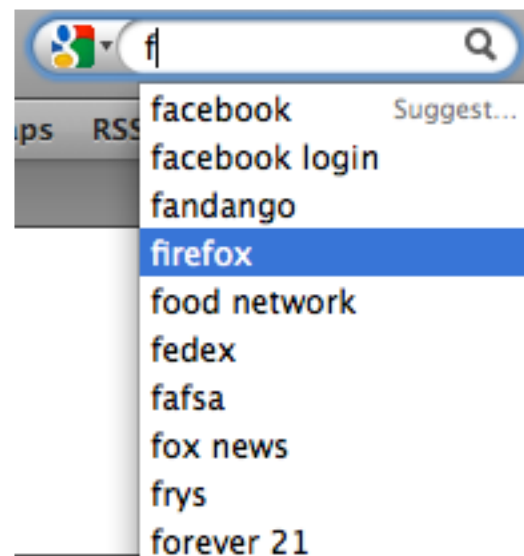
136 chars.

101 chars.

102 chars.

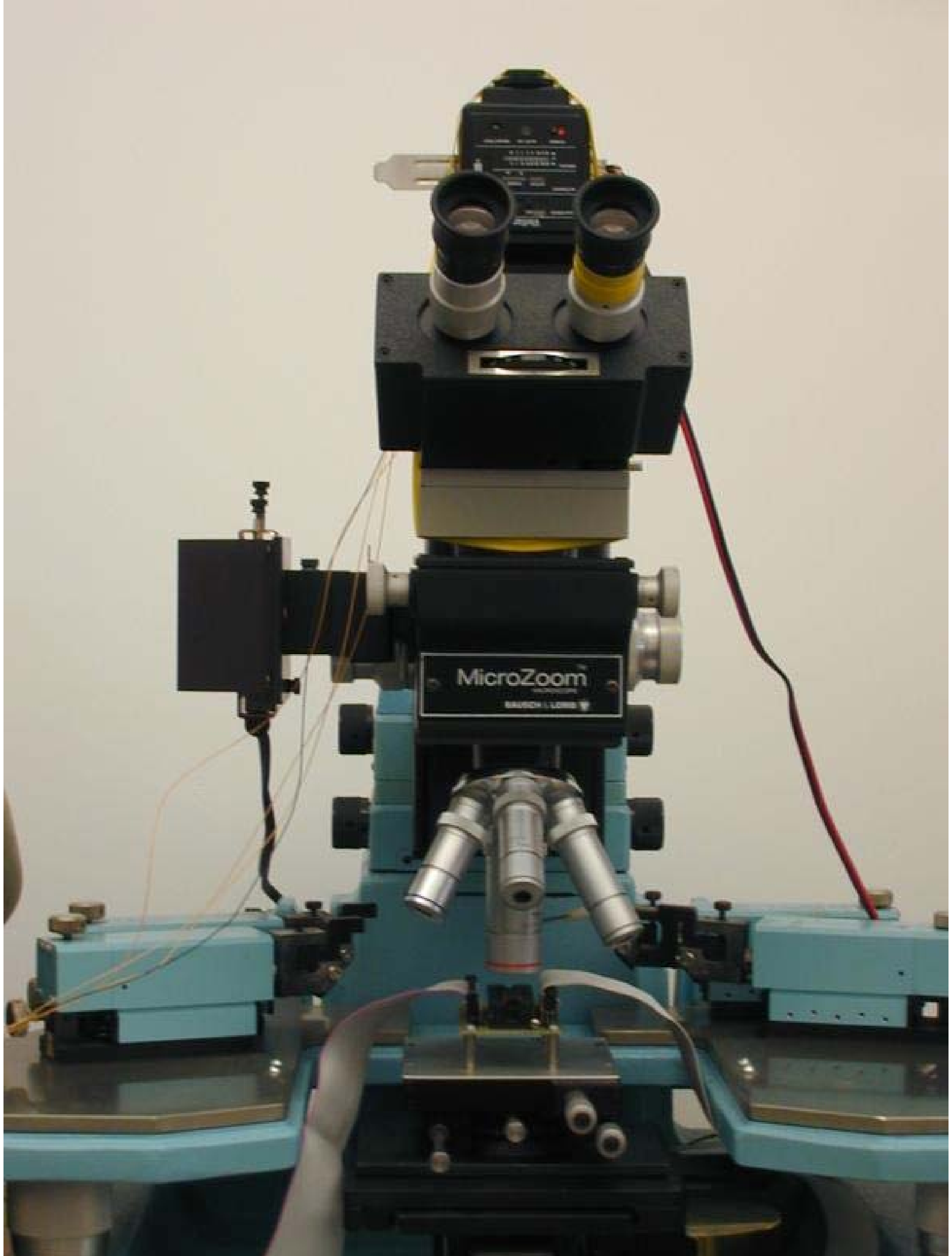






```
void out(char *p, size_t n)
{
	while (n > 0) {
		send_to_output(*p);
		p++; n--;
	}
}
```

Given the ability to trigger a fault (“glitch”) at any instruction, how would you induce this code to output something it shouldn’t?


MicroZoom

Fault Attacks

- Smartcard stores your BART balance. When you go through turnstile, turnstile sends “Debit account by $3.80” and smartcard replies “Done.” plus an AES-CMAC tag, using key *K* stored on smartcard.
- Suppose Mallory can zap any bit of the memory where *K* is stored, permanently clearing that bit of *K*. How can she recover the 128-bit AES key *K*?

One Solution

- Answer: Observe M = “Done.”, T = CMAC_K(M). Now zap the last 127 bits; let K^* be the resulting key. Observe M = “Done.”, T* = CMAC_{K^*}(M). Check whether T = T*. Notice that we will have T = T* if and only if first bit of K is 0.
- Now do it again with a new smartcard to learn second bit of K, third bit, etc.
- Better attack: Zap the first bit, to learn K_1. Zap the second bit (using the same smartcard), and you can learn K_2. Repeat. You learn the entire key. At the end, all bits of the key have been zapped to 0 and smartcard is useless; throw it away.

Alternative Solution

- Answer: Zap the last 127 bits, to get K^*. Now there are only two possibilities for K^*, since last 127 bits of K^* are all zero. Observe M = "Done.", T = $\mathrm{CMAC}_{K^*}(\mathrm{M})$ and try both possibilities for K^*. You learn K^* and thus learn the first bit of K. Now do this with 128 smartcards, to learn all 128 bits of K.
- Better attack: Zap the last bit, to get K_1. Observe M_1, $\mathrm{T}_1 = \mathrm{CMAC}_{K1}(\mathrm{M}_1)$. Zap the next-to-last bit, to get K_2. Observe M_2, $\mathrm{T}_2 = \mathrm{CMAC}_{K2}(\mathrm{M})$. Repeat 128 times. From M_{127}, T_{127}, we can learn first bit of K. From M_{126}, T_{126}, we learn next bit. etc.

Take-away on Side Channels

- Very challenging to identify all the ways that code might leak secrets.
- Defenses: prove that what attacker can observe does not depend upon anything secret (e.g., code is constant-time, etc.).

Extra Material

Information Leakage via Inducing Faults

- Suppose there's a sealed black box that performs RSA decryption:
  - $X \rightarrow \boxed{} \rightarrow Y$ $\qquad Y = X^d \bmod N$ $\quad (N = pq)$
- Attacker gets access to box, can play with it freely
  - Knows N …. but not d, p or q
  - Can repeatedly feed it X's, observe corresponding Y's
- Suppose for efficiency box computes $X^d \bmod N$ using Chinese Remainder Theorem (CRT)
  - Number theory trick that's faster than repeated exponentiation
  - (Note, this is a common performance approach)

Fault Attacks on RSA

- CRT works by first computing:
  - $y_1 = (X \bmod p)^{d \bmod (p-1)}$
  - $y_2 = (X \bmod q)^{d \bmod (q-1)}$
- Given that, CRT provides a cheap function f so that for $Y = f(y_1, y_2)$ we have:
  - $Y = y_1 \bmod p$; $Y = y_2 \bmod q$
- … and that gives us our goal, $Y = X^d \bmod N$
- Suppose now attacker repeatedly feeds the same X into the box, observing resulting Y …
  - … but can induce the box to sometimes glitch (causes one computation step to *work incorrectly*)

Fault Attacks on RSA

- Assume glitch induces a random fault
- Most likely it occurs during computation of either $y_1 = (X \bmod p)^{d \bmod (p-1)}$ or $y_2 = (X \bmod q)^{d \bmod (q-1)}$
- Attacker tell glitch occurs since will observe box produce $Y' \neq Y$
- Suppose glitch occurs when computing y_1 …
- Then Y' is incorrect mod p …
  - … but correct mod q (since y_2 okay)

Fault Attacks on RSA

- Attacker has Y' ≠ Y mod p, Y' = Y mod q
  - Y-Y' is a multiple of q but not p
- Attacker computes Z = gcd(Y-Y', N) (fast!)
- Z = ?
  - Well, must be either 1, p, q, or N (since N = pq)
  - But Y-Y' is a multiple of q, so it's *either* q or N
  - But Y-Y' is not a multiple of p, so it's q
- **Whoops!**
  - Attacker just factored N!
- Fix?
  - Box could check that Y^e mod N = X