Surreptitious Communication

CS 161 - Computer Security

Profs. Vern Paxson & David Wagner

TAs: John Bethencourt, Erika Chin, Matthew Finifter, Cynthia Sturton, Joel Weinberger

http://inst.eecs.berkeley.edu/~cs161/

April 26, 2010

Steganography

- Transmitting hidden messages using a known communication channel
  - Or hiding extra data inside known storage
- Goal: Sneak past a reference monitor (“warden”)
- Examples?
  - Zillions: tattooed heads of slaves, least-significant bits of image pixels, extra tags in HTML documents, …
  - All that’s necessary is agreement between writer of message & reader of message
- Security?
  - Brittle: relies on *security-by-obscurity*
    - Warden can extract/block messages if they know the trick

Covert Channels

- Communication between two parties that uses a hidden (secret) channel
- Goal: evade reference monitor inspection entirely
  - Warden doesn't even realize communication is possible
- Example: suppose (unprivileged) process **A** wants to send 128 bits of secret data to (unprivileged) process **B** …
  - But can't use pipes, sockets, signals, or shared memory; and can only read files, can't write them

Covert Channels, con’t

- Method #1: **A** *syslog*’s data, **B** reads via /var/log/…
- Method #2: select 128 files in advance. **A** opens for read only those corresponding to 1-bit’s in secret.
  - **B** recovers bit values by inspecting access times on files
- Method #3: divide **A**’s running time up into 128 slots. **A** either runs CPU-bound - or idle - in a slot depending on corresponding bit in the secret. **B** monitors **A**’s CPU usage.
- Method #4: Suppose **A** can run 128 times. Each time it either exits after 2 seconds (0 bit) or after 30 seconds (1 bit).
- Method #5: …
  - There are zillions of Method #5’s!

Covert Channels, con't

- Defenses?
- As with steganography, #1 challenge is identifying the mechanisms
- Some mechanisms can be very hard to completely remove
  - E.g., duration of program execution
- Fundamental issue is the covert channel's capacity
  - Bits (or bit-rate) that adversary can obtain using it
- Crucial for defenders to consider their threat model

Side Channels

- Inferring information meant to be hidden / private by exploiting how system is structured
  - Note: unlike for steganography & covert channels, here we do *not* assume a cooperating sender / receiver
- Can be difficult to recognize because often system builders "abstract away" seemingly irrelevant elements of system structure
- Side channels can arise from physical structure …


ACCEPT
PROG
1
2
3
4
5
6
7
8
9
ENTER
0
CLEAR

Side Channels

- Inferring information meant to be hidden / private by exploiting how system is structured
  - Note: unlike for steganography & covert channels, here we do not assume a cooperating sender / receiver
- Can be difficult to recognize because often system builders “abstract away” seemingly irrelevant elements of system structure
- Side channel can arise from physical structure …
  - … or higher-layer abstractions

```
/* Returns true if the password from the
 * user, 'p', matches the correct master
 * password. */
bool check_password(char *p)
{
     static char *master_pw = "T0p$eCRET";
     int i;
     for(i=0; p[i] && master_pw[i]; ++i)
          if(p[i] != master_pw[i])
               return FALSE;

     /* Ensure both strings are same len. */
     return p[i] == master_pw[i];
}
```

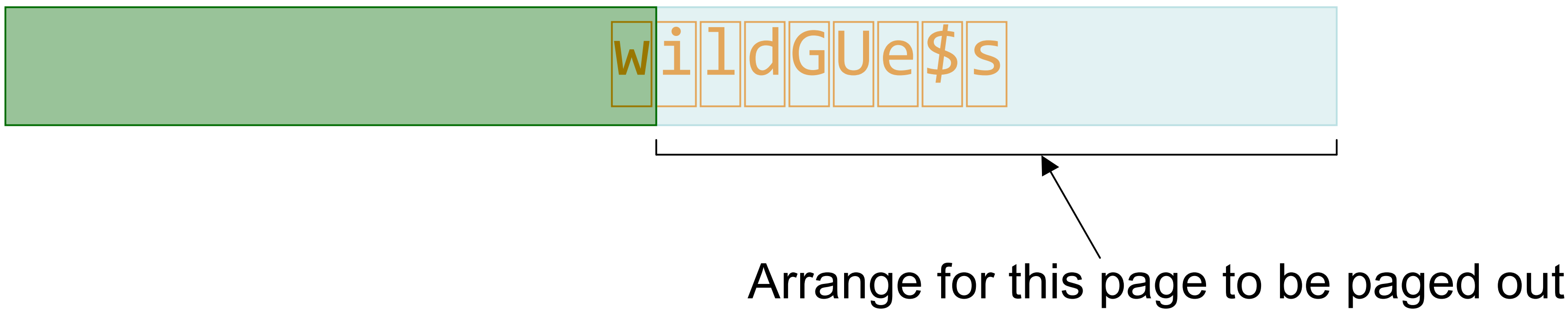
Inferring Password via Side Channel

- Suppose the attacker's code can call **`check_password`** many times (but not millions)
  - But attacker can't breakpoint or inspect the code
- How could the attacker infer the master password using side channel information?
- Consider layout of **`p`** in memory:

```
...
if(check_password(p))
     BINGO();
...
```

w	i	l	d	G	U	e	$	s

Spread **p** across different memory pages:

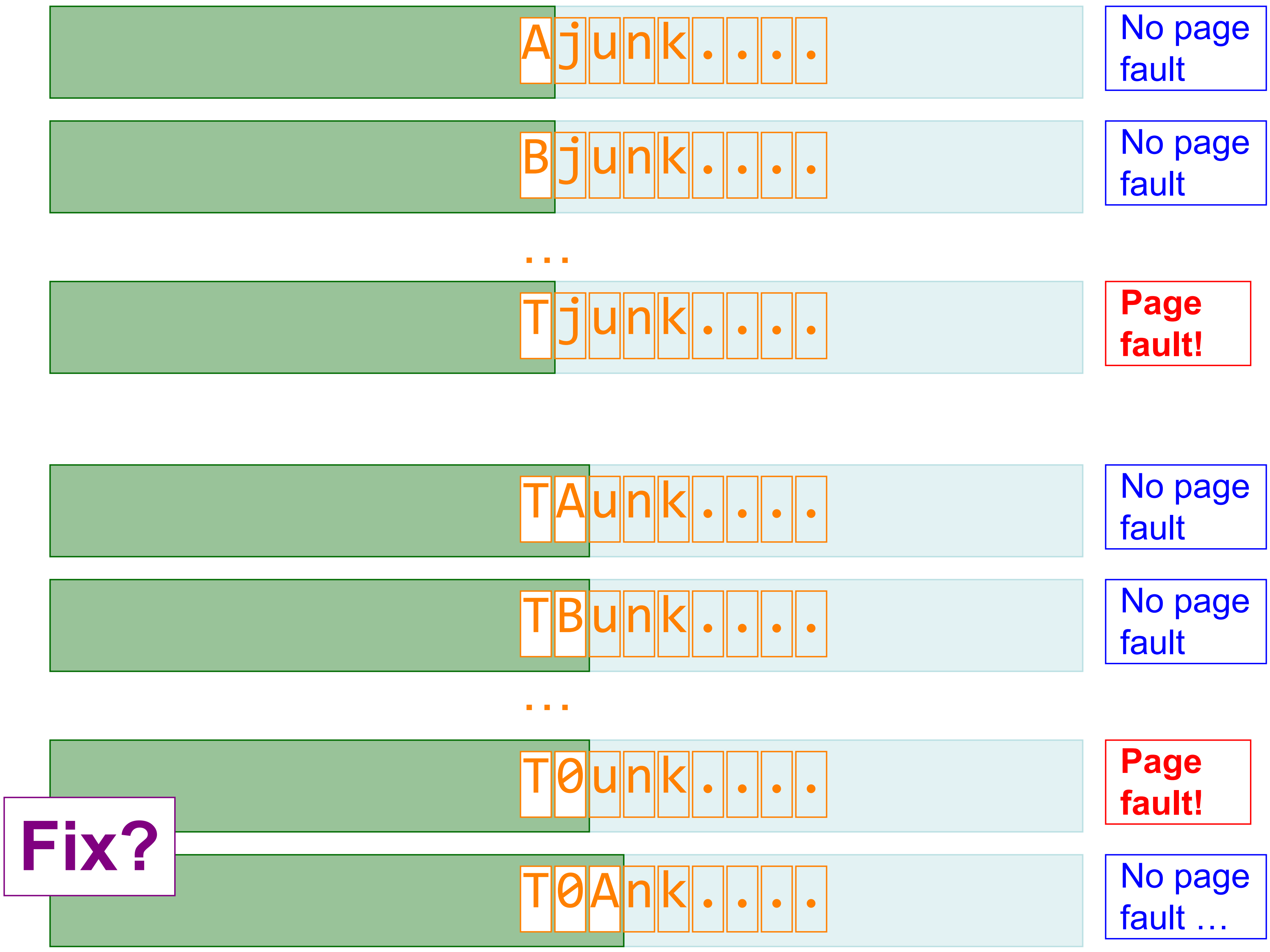


If master password doesn't start with 'w', then loop exits on first iteration (`i=0`):

```
for(i=0; p[i] && master_pw[i]; ++i)
    if(p[i] != master_pw[i])
        return FALSE;
```

If it *does* start with 'w', then loop proceeds to next iteration, generating a page fault that the caller can observe

T0p$eCRET ?


Ajunk....
No page fault
Bjunk....
No page fault
...
Tjunk....
Page fault!
TAunk....
No page fault
TBunk....
No page fault
...
T0unk....
Page fault!
Fix?
T0Ank....
No page fault …

```c
bool check_password2(char *p)
{
    static char *master_pw = "T0p$eCRET”;
    int i;
    bool is_correct = TRUE;

    for(i=0; p[i] && master_pw[i]; ++i)
        if(p[i] != master_pw[i])
            is_correct = FALSE;

    if(p[i] != master_pw[i])
        is_correct = FALSE;
    return is_correct;
}
```

Note: still leaks length of master password

Side Channels in Web Surfing

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

Breaking News | Latest News | Current News – FOXNews.com

http://www.foxnews.com/

Most Visited · Getting Started · Latest Headlines

Breaking News | Latest News | Cu...

VIDEO RADIO MOBILE U-REPORT

FOX NEWS .com Fair & Balanced

Search

Full Coverage · It's Your Land · It's All Your Money · Road to Recovery

Watch Live · White House Briefing · NYC Mayor on Salt Reduction

HOME · U.S. · WORLD · BUSINESS · POLITICS · ENTERTAINMENT · LEISURE · HEALTH · SCITECH · OPINION · SPORTS · ON AIR

Live Coverage · White House Press Briefing

FoxNews.com Meets iPhone

Don't Talk to Aliens, Warns Stephen Hawking

The No. 1 name in news — in the palm of your hand. Download the Fox News iPhone app for latest news, streaming video, and radio — and it's all free.

- The Five Best Apple iPad Apps
- SLIDESHOW: Killer Apps for the Apple iPad

Wall Street Battle Brews

Democrats are resisting Republican appeals for a broad compromise on a financial overhaul bill as vote nears

- SEC to Investigate Timing of Goldman Suit | VIDEO
- FoxBusiness: Goldman Stands Behind 'Fabulous Fab'
- Buffett Presses for Eased Curbs on Derivatives

GOP Urges Border Insecurity Solution

Republican lawmakers and Arizona residents call on Capitol Hill to put immigration aside and secure the border

- Arizona Lawmaker: U.S. Should Fight Immigration Law
- Mexico: Cartels Turning Attacks on Authorities

Wrong Guy, Place to Tell a Jewish Joke?

URGENT: National Security Adviser James Jones issues apology for joke told in front of pro-Israeli group

- YOU DECIDE: Was Jones' Joke Inappropriate?

FOX BUSINESS

- EXCLUSIVE: Blankfein Says Trader 'Fab' is Immature, but Not a Crook
- DC Report: Small Business Tax Breaks in the Mail?

Sponsored By Scottrade · Get Quote · Business Traveler

Latest News – Today's Top Stories · Most Read – Most Popular Stories · Live Shots – Fox News in the Field · The Strategy Room – Watch Live on the Web

Armed Man Arrested at N.C. Airport as Obama Departs

Desperate Rush to Cap Gulf Oil Spill | SLIDESHOW

Remarkable Tales of Survival After Southern Tornado - VIDEO | SLIDESHOW | LIVESHOTS

Chicago Lawmakers: Call In National Guard | VIDEO

ADVERTISE

FOX NEWS VIDEOS

TOP VIDEOS

National Guard to stop Chicago violence?

Left to die: When empathy is ignored

Media boosting Tea Party anger?

- Kardashian explains nude Bazaar shoot
- Teen drinking related to R-rated movies?
- Ex-Geico adman defends Tea Party rant
- Workers rush to rescue trapped girl

MORE VIDE

ON FOX NEWS CHANNEL

SCHEDULE | FOX FAN | BIOS

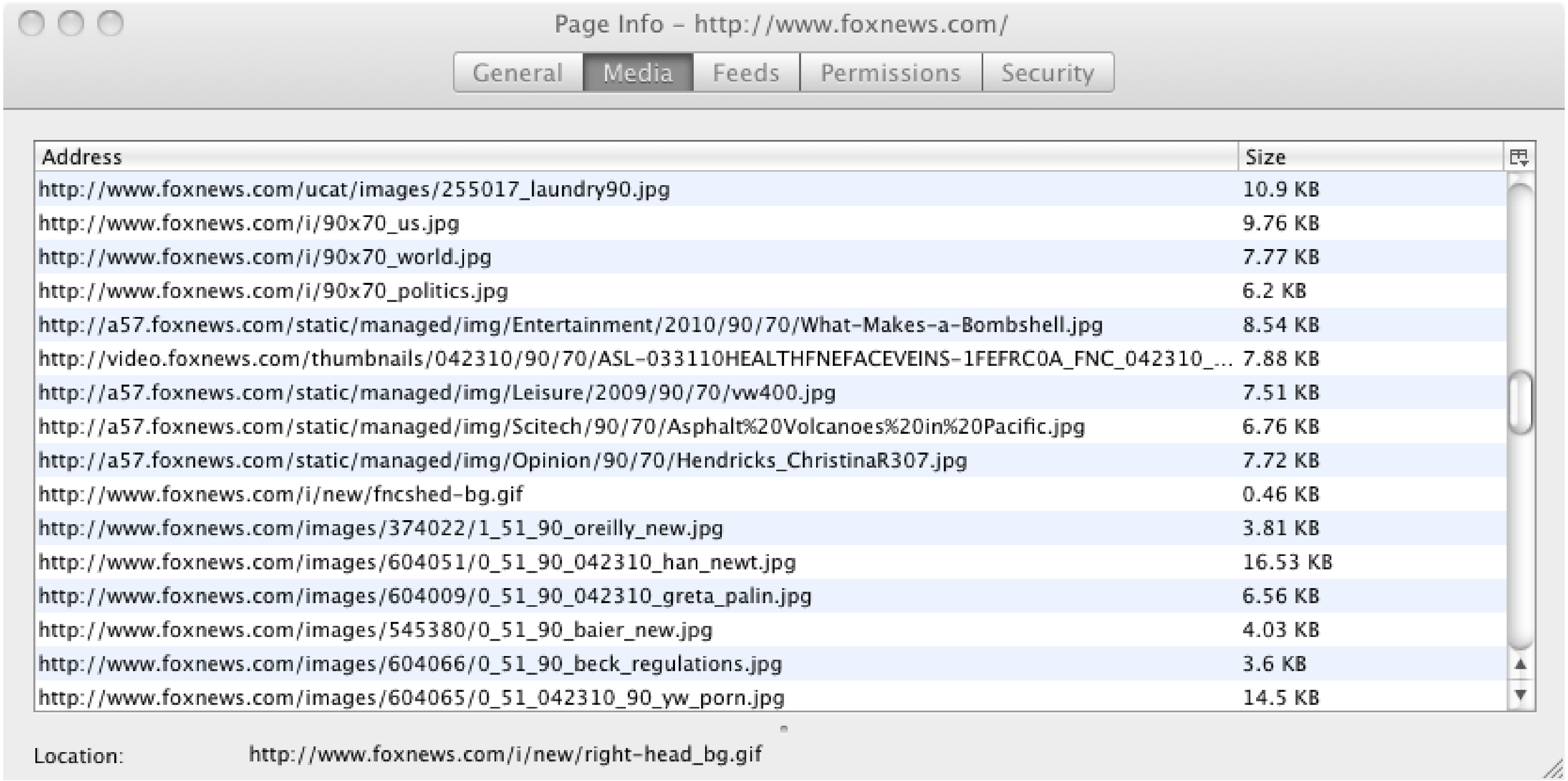
IMAG LIFESTYLE SECTION

Bold Tuna Burger – A tasty and nutritious dinner!

Your Date Did What? – The most unbelievable dating horro stories.

Pretty Prints – Check out the hottest style trend for

Done



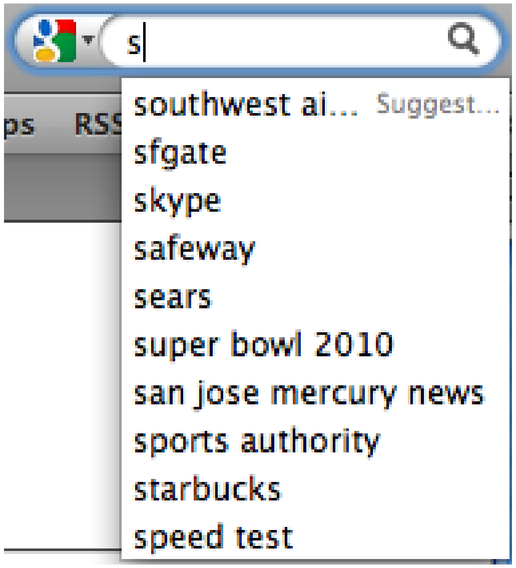
Address	Size
http://www.foxnews.com/ucat/images/255017_laundry90.jpg	10.9 KB
http://www.foxnews.com/i/90x70_us.jpg	9.76 KB
http://www.foxnews.com/i/90x70_world.jpg	7.77 KB
http://www.foxnews.com/i/90x70_politics.jpg	6.2 KB
http://a57.foxnews.com/static/managed/img/Entertainment/2010/90/70/What-Makes-a-Bombshell.jpg	8.54 KB
http://video.foxnews.com/thumbnails/042310/90/70/ASL-033110HEALTHFNEFACEVEINS-1FEFRC0A_FNC_042310_...	7.88 KB
http://a57.foxnews.com/static/managed/img/Leisure/2009/90/70/vw400.jpg	7.51 KB
http://a57.foxnews.com/static/managed/img/Scitech/90/70/Asphalt%20Volcanoes%20in%20Pacific.jpg	6.76 KB
http://a57.foxnews.com/static/managed/img/Opinion/90/70/Hendricks_ChristinaR307.jpg	7.72 KB
http://www.foxnews.com/i/new/fncshed-bg.gif	0.46 KB
http://www.foxnews.com/images/374022/1_51_90_oreilly_new.jpg	3.81 KB
http://www.foxnews.com/images/604051/0_51_90_042310_han_newt.jpg	16.53 KB
http://www.foxnews.com/images/604009/0_51_90_042310_greta_palin.jpg	6.56 KB
http://www.foxnews.com/images/545380/0_51_90_baier_new.jpg	4.03 KB
http://www.foxnews.com/images/604066/0_51_90_beck_regulations.jpg	3.6 KB
http://www.foxnews.com/images/604065/0_51_042310_90_yw_porn.jpg	14.5 KB

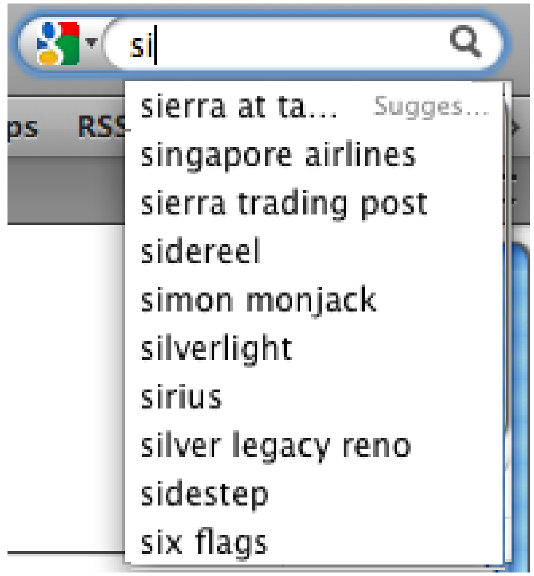
Location: http://www.foxnews.com/i/new/right-head_bg.gif

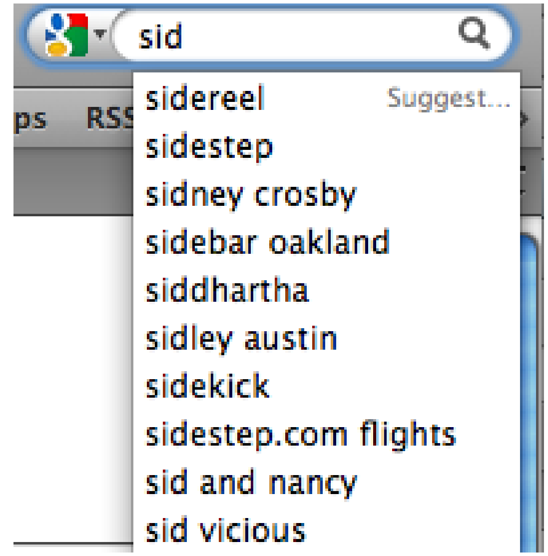
Eve "fingerprints" web sites based on the specific sizes of the items used to build them

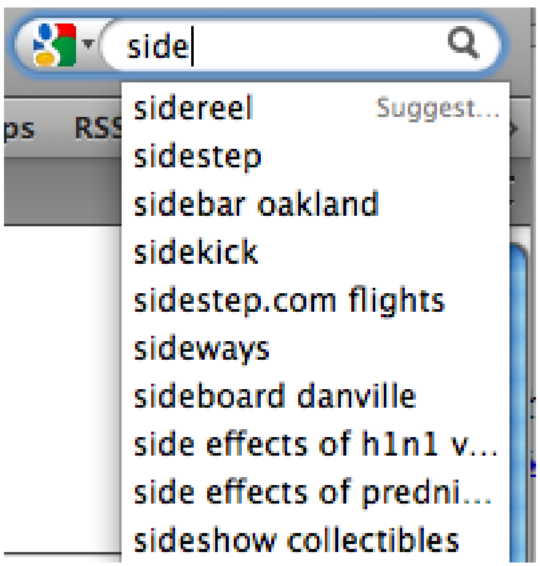
Side Channels in Web Surfing

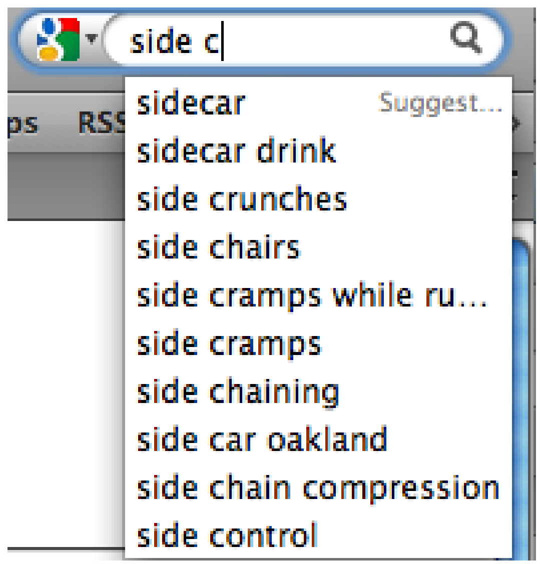
- Suppose Alice is surfing the web and all of her traffic is encrypted
- Eve can observe the presence of Alice’s packets but can’t read their contents or destination
- How can Eve deduce that Alice is visiting FoxNews (say)?
- What about inferring what terms Alice is searching on?

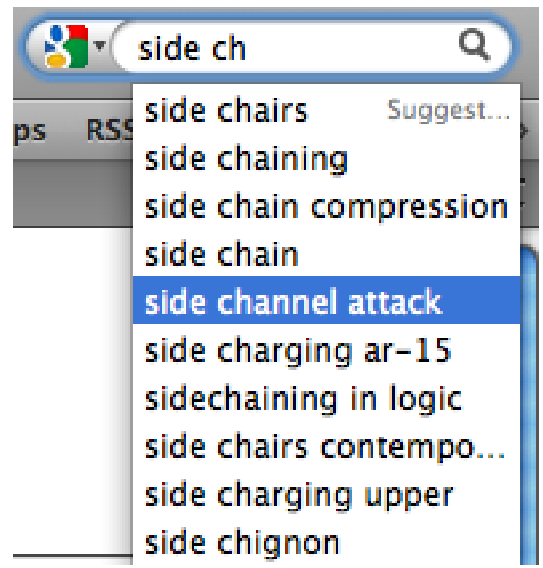

s
southwest ai... Suggest...
sfgate
skype
safeway
sears
super bowl 2010
san jose mercury news
sports authority
starbucks
speed test

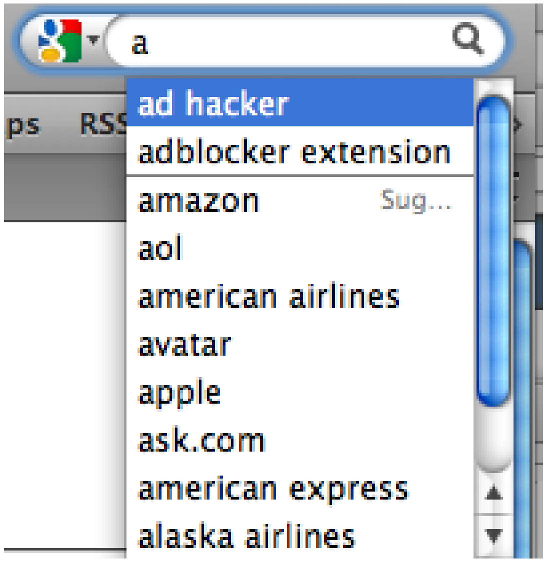

si
sierra at ta... Sugges...
singapore airlines
sierra trading post
sidereel
simon monjack
silverlight
sirius
silver legacy reno
sidestep
six flags

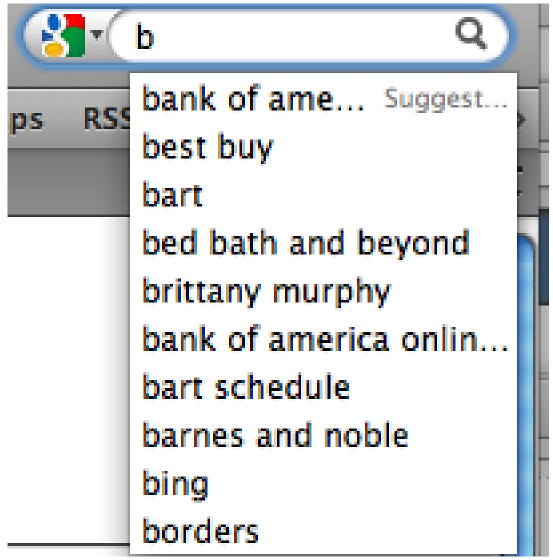

sid
sidereel Suggest...
sidestep
sidney crosby
sidebar oakland
siddhartha
sidley austin
sidekick
sidestep.com flights
sid and nancy
sid vicious

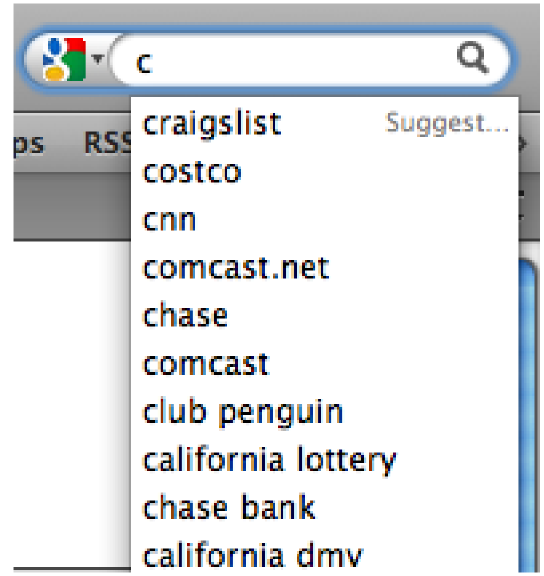

side
sidereel Suggest...
sidestep
sidebar oakland
sidekick
sidestep.com flights
sideways
sideboard danville
side effects of h1n1 v...
side effects of predni...
sideshow collectibles


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.

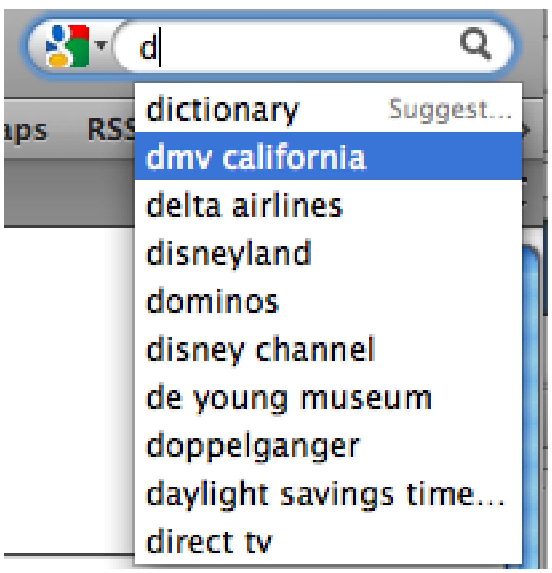
125 chars.

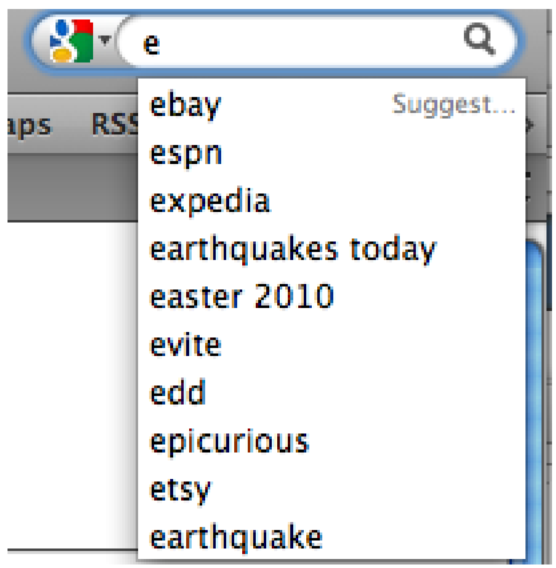
107 chars.

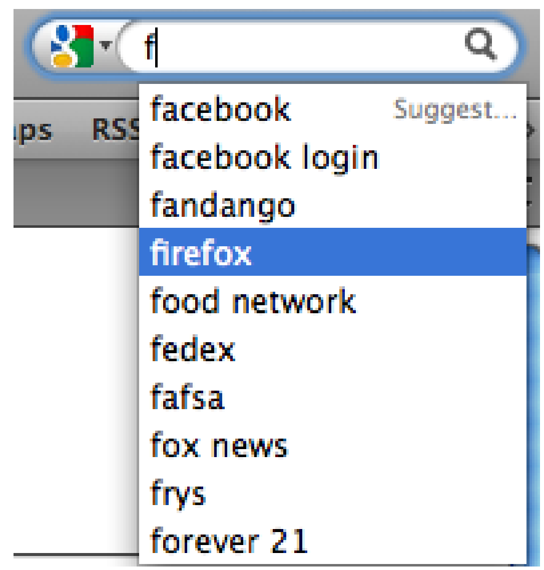
136 chars.

101 chars.

102 chars.





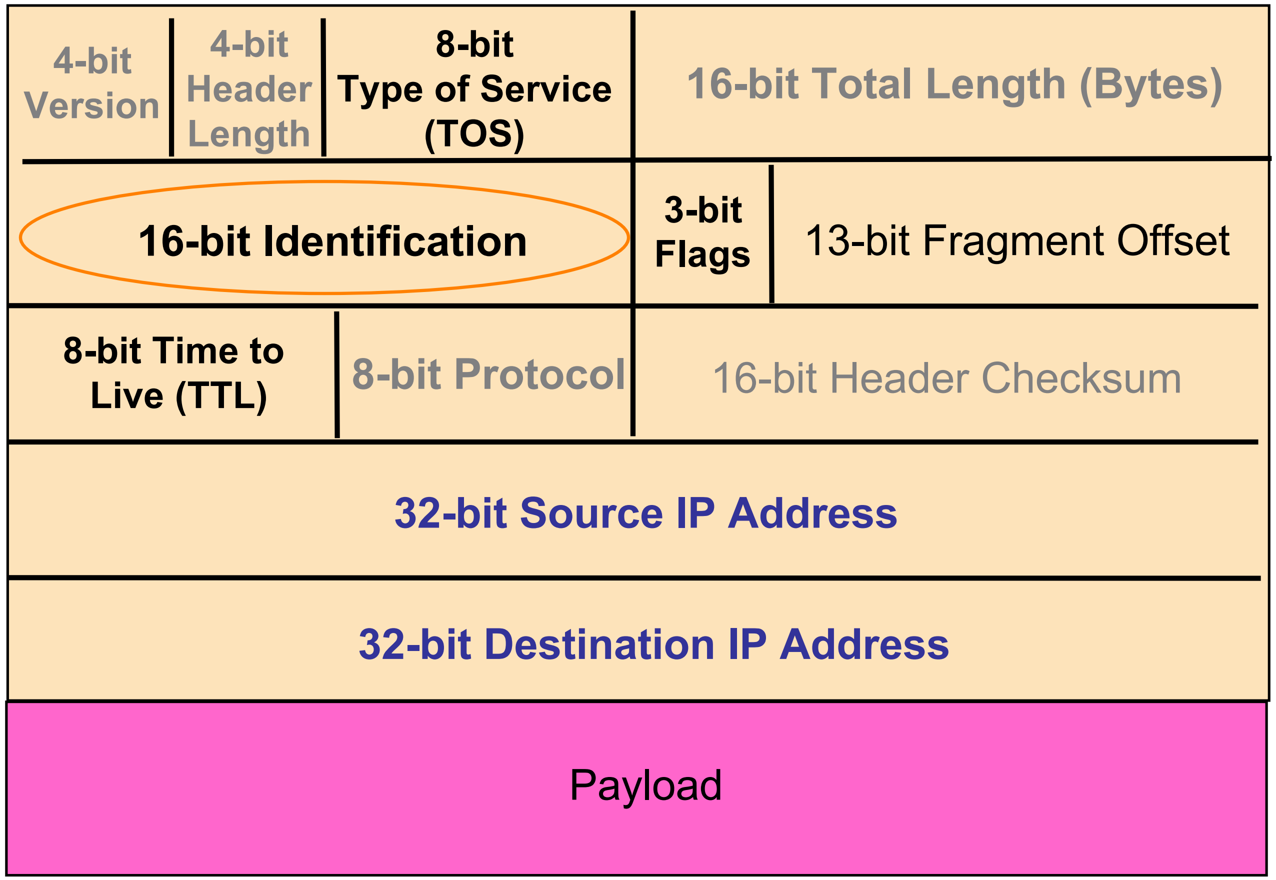


Exploiting Side Channels For Stealth Scanning

- Can attacker using system **A** scan the server of victim **V** to see what services **V** runs …
- … without **V** being able to learn **A**'s IP address?

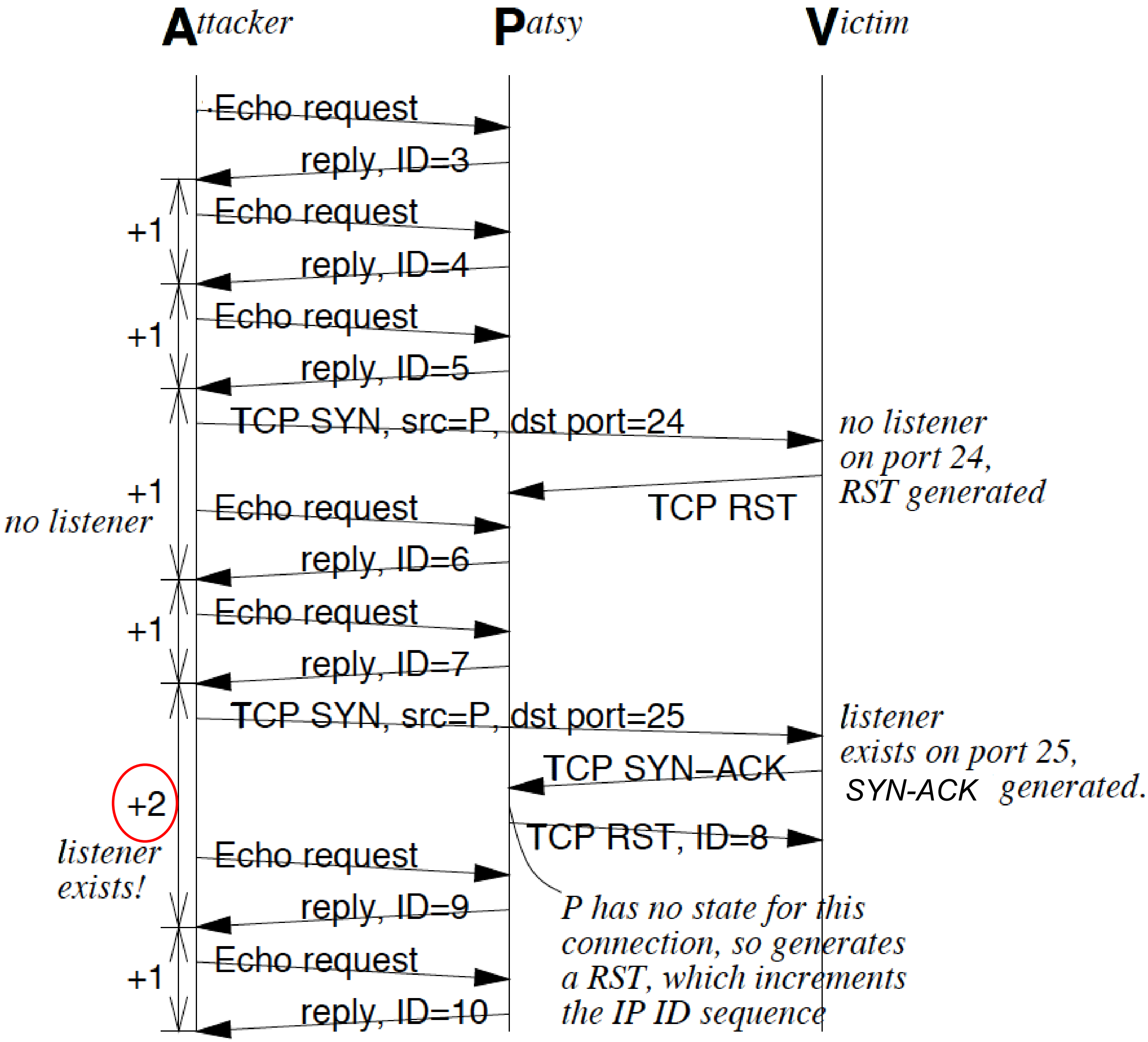
- Seems impossible: how can **A** receive the results of probes **A** sends to **V**, unless probes include **A**'s IP address for **V**'s replies?

IP Header Side Channel



ID field is supposed to be unique per IP packet.

One easy way to do this: **increment** it each time system sends a new packet.

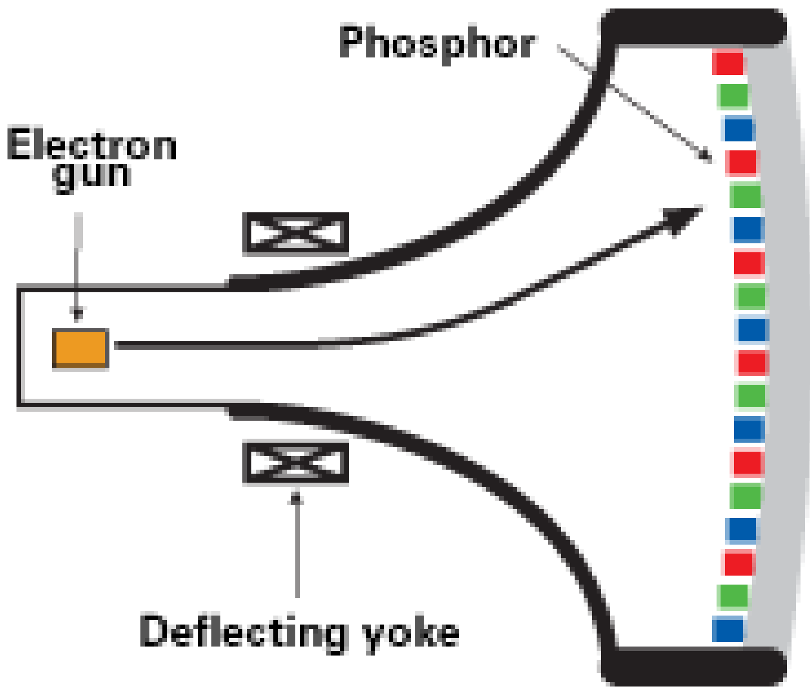

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
listener
exists on port 25,
SYN-ACK generated.
TCP SYN–ACK
+2
listener
exists!
TCP RST, ID=8
Echo request
reply, ID=9
P has no state for this
connection, so generates
a RST, which increments
the IP ID sequence
+1
Echo request
reply, ID=10

UI Side Channel Snooping

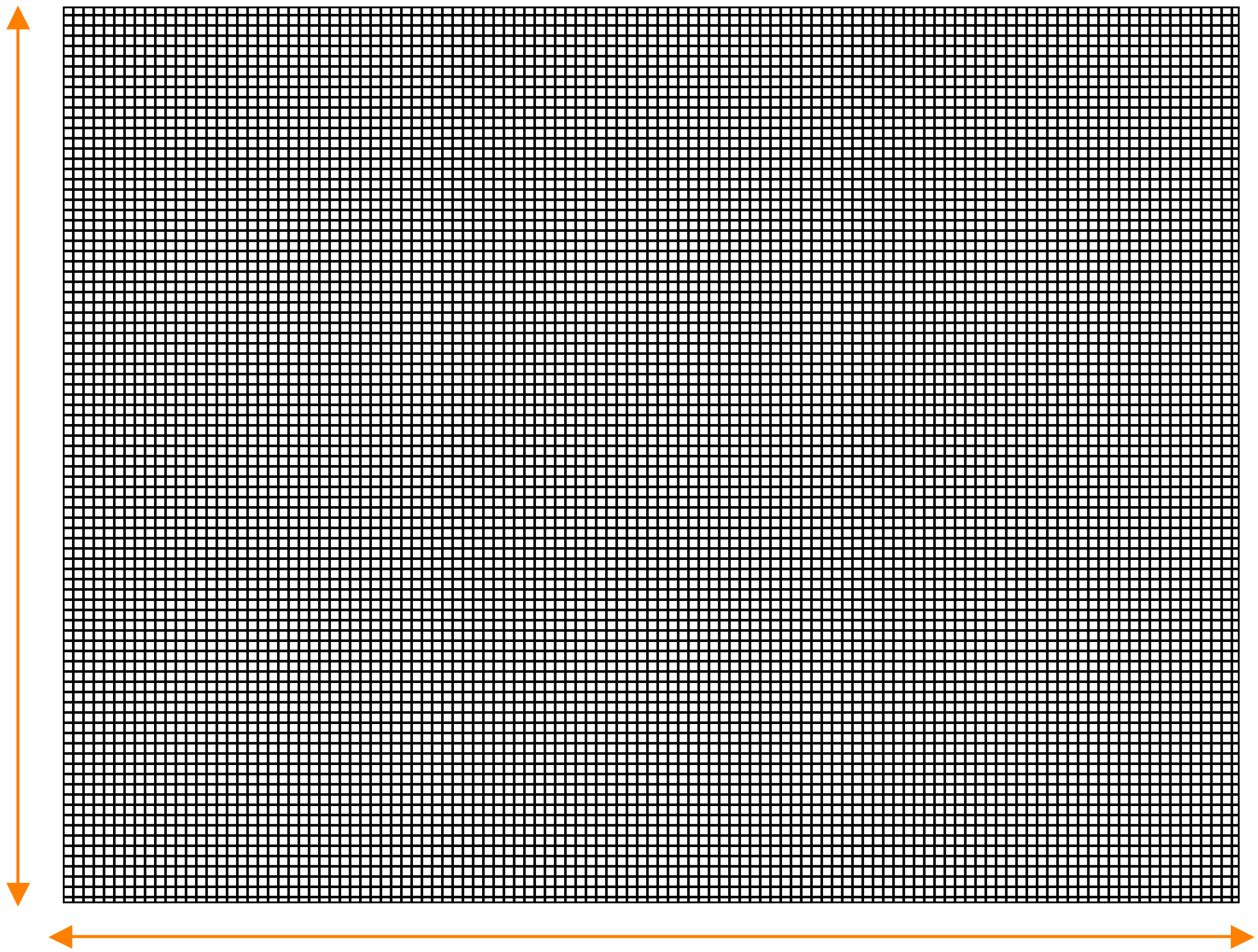
- Scenario: Ann the Attacker works in a building across the street from Victor the Victim. Late one night Ann can see Victor hard at work in his office, but can't see his CRT display, just the glow of it on his face.

- How might Ann snoop on what Victor's display is showing?

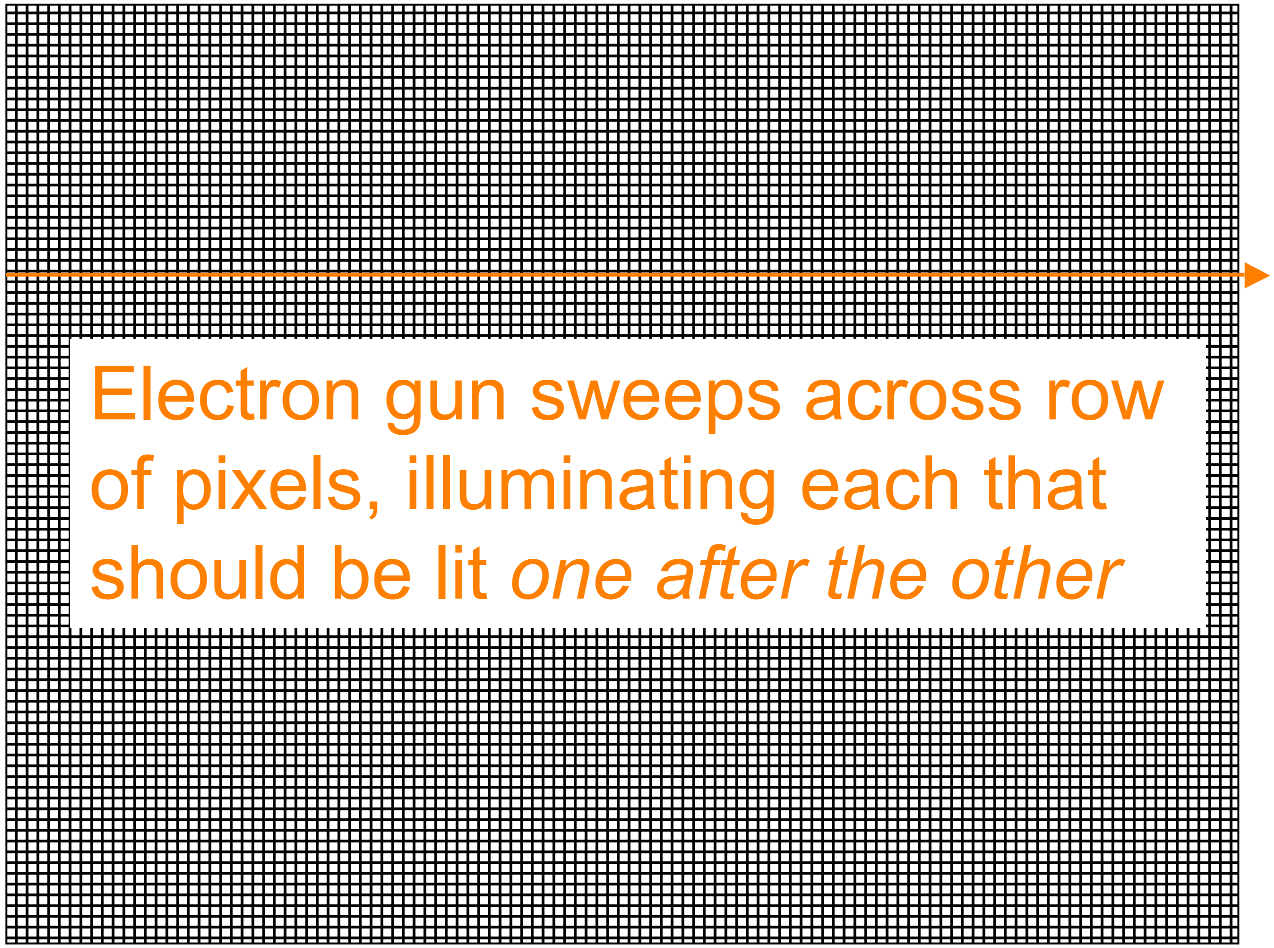
CRT

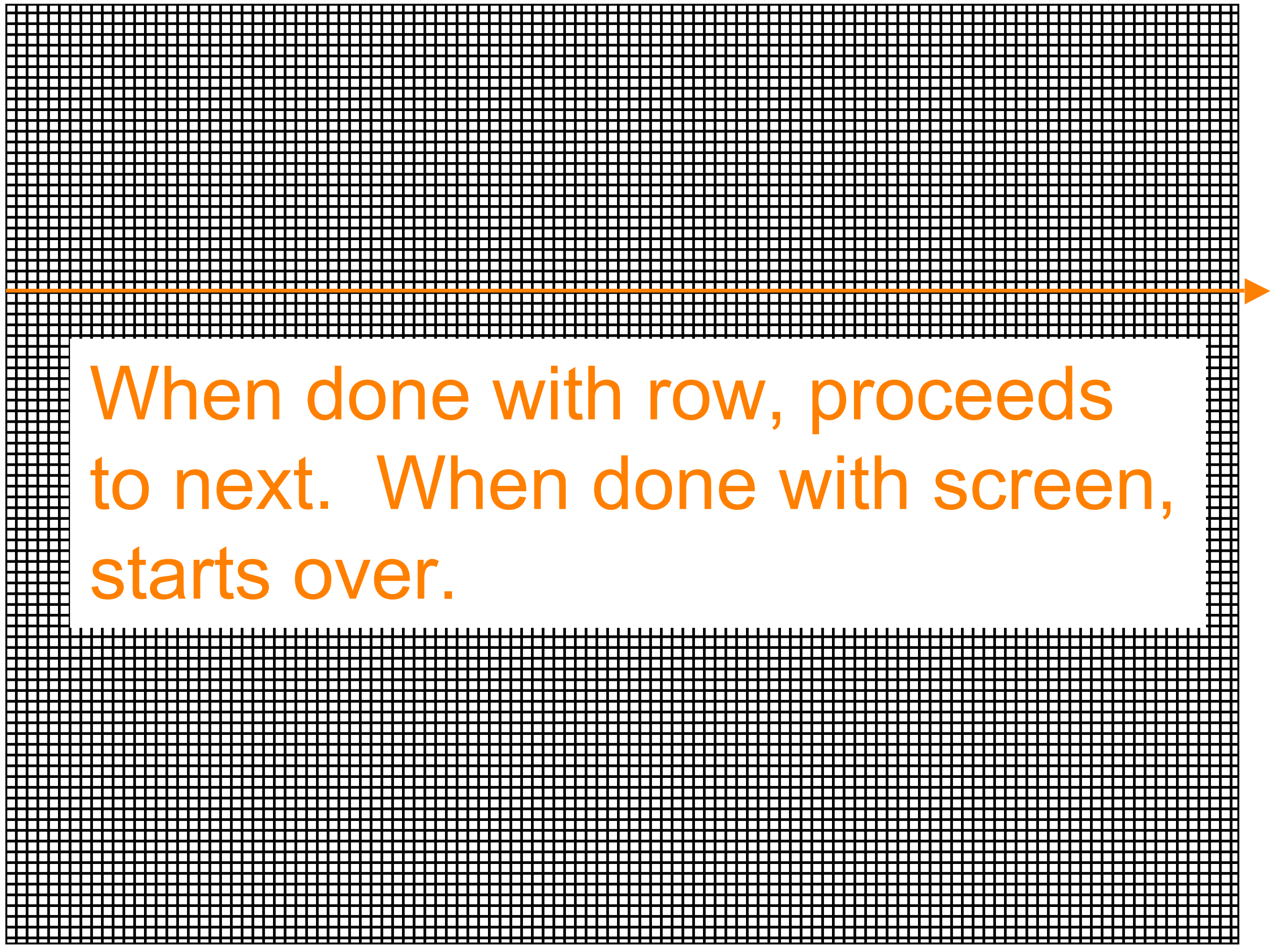


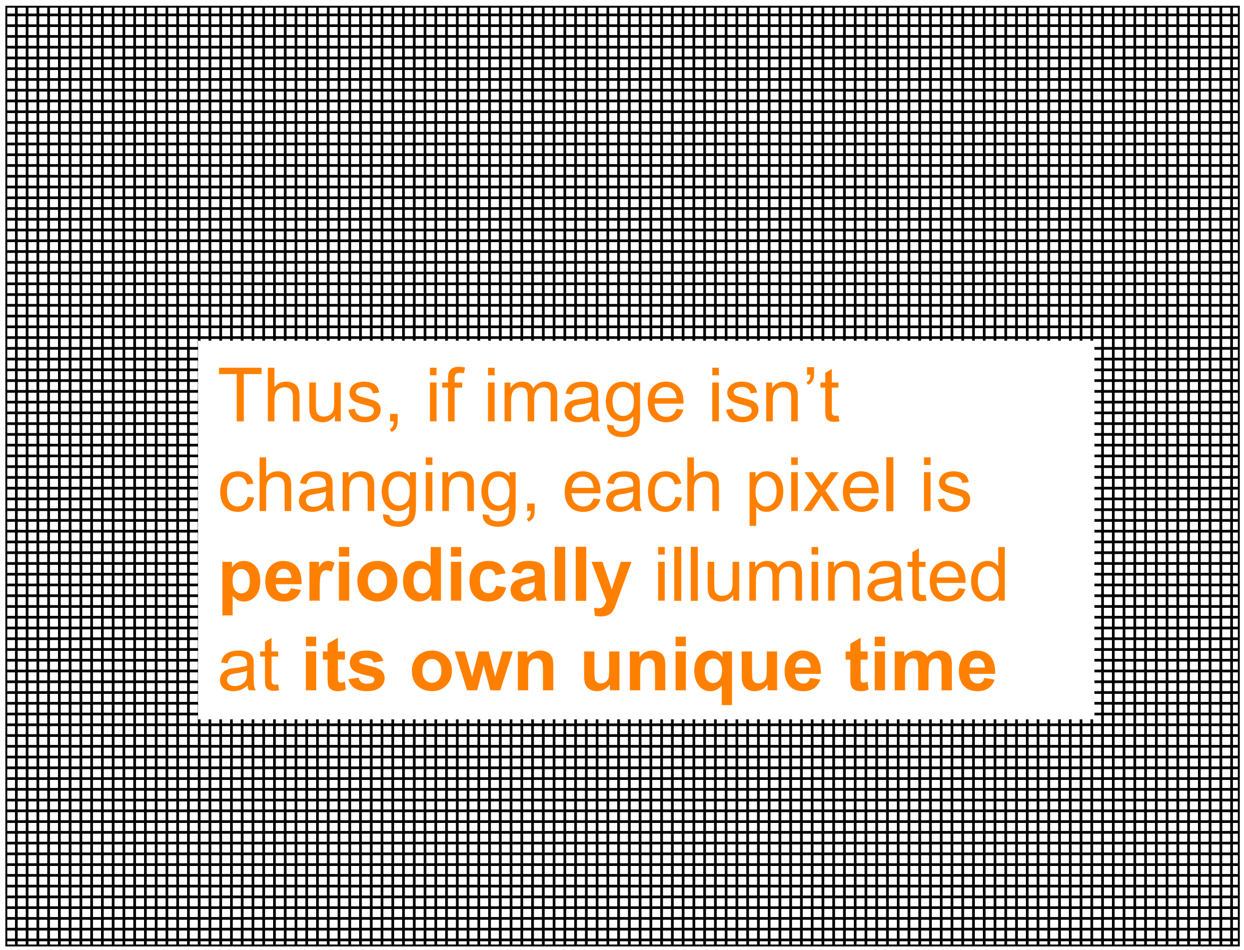
CRT display is made up of
an array of phosphor pixels

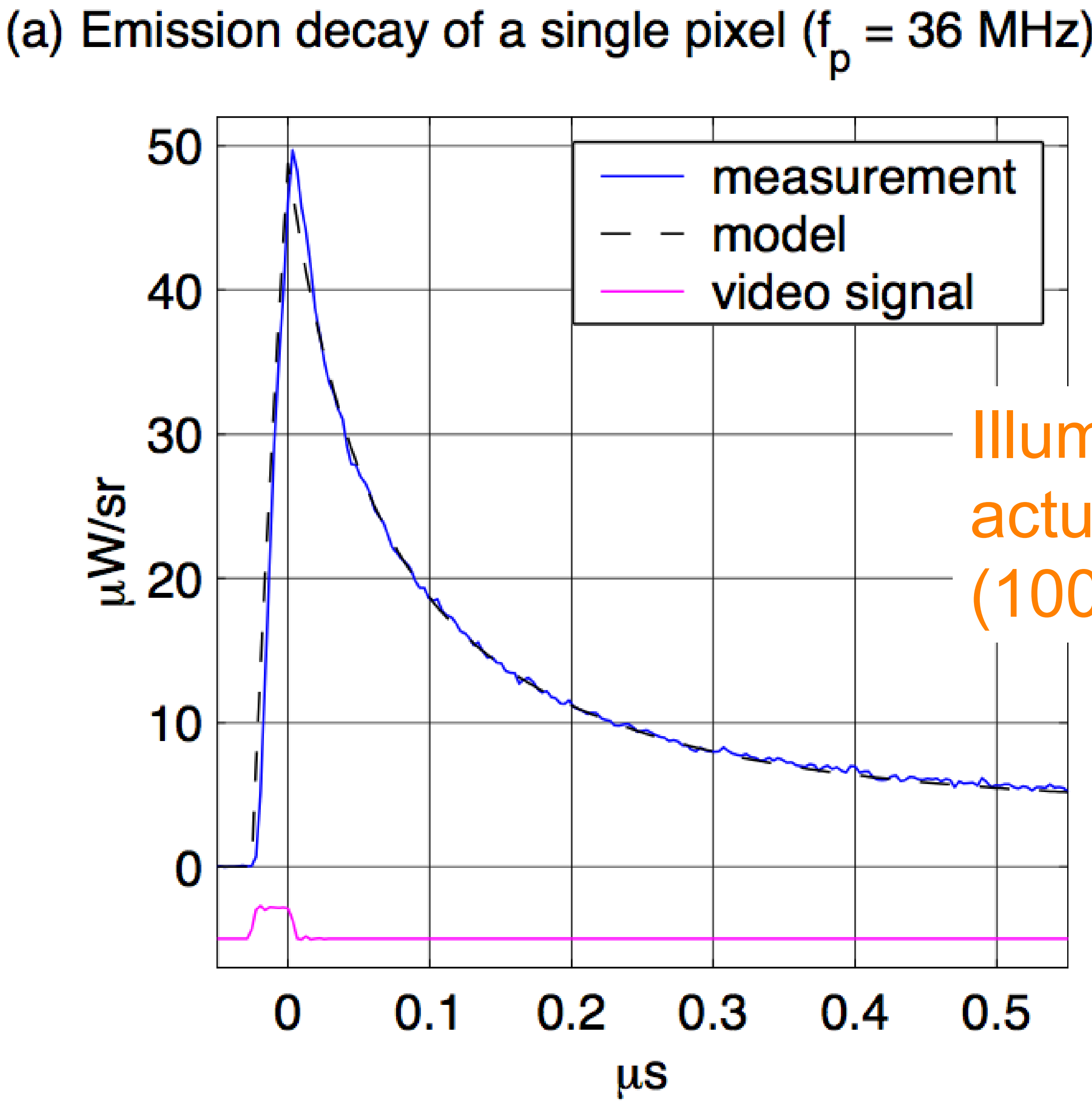


640x480 (say)

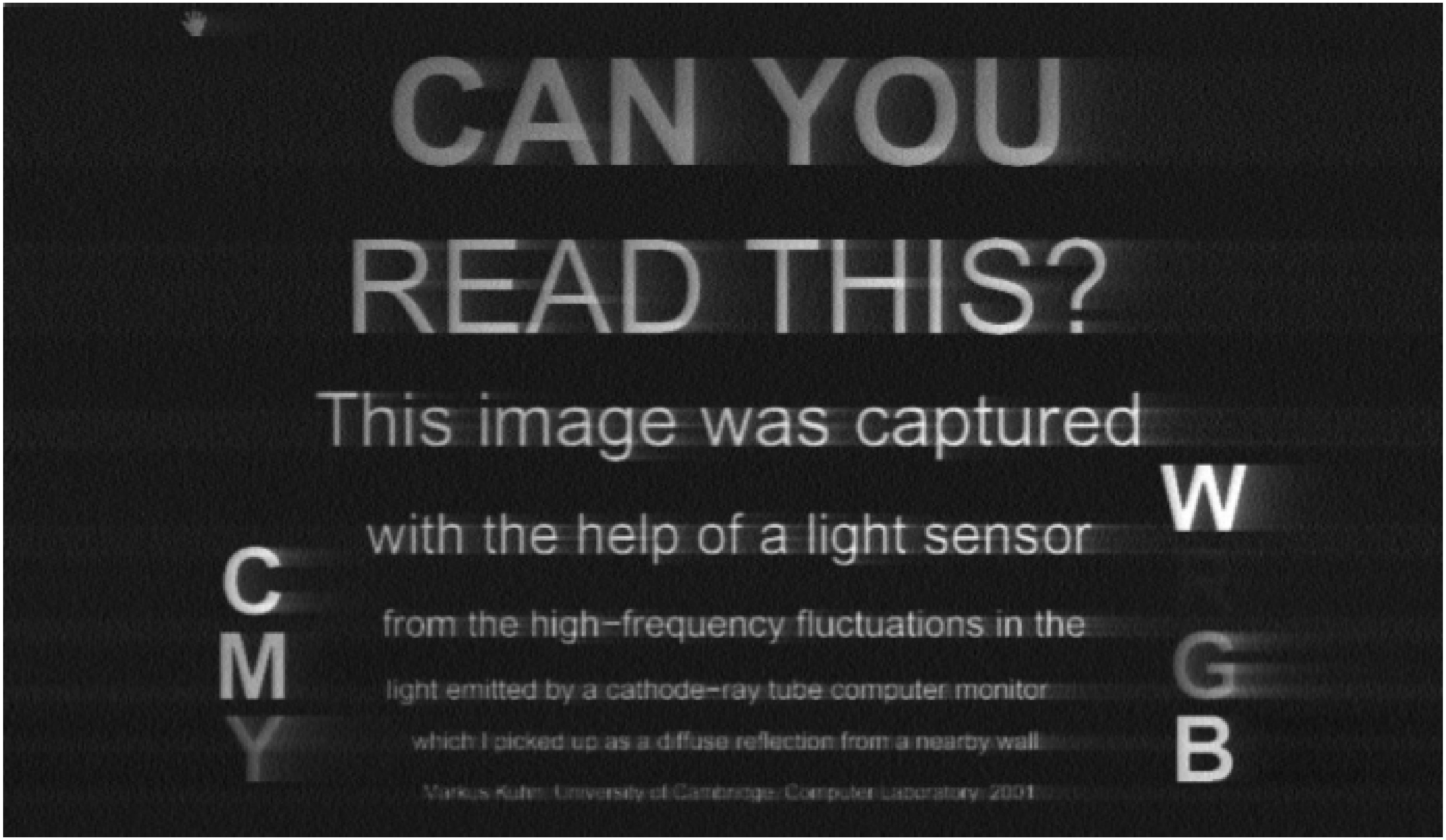

Electron gun sweeps across row of pixels, illuminating each that should be lit *one after the other*


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

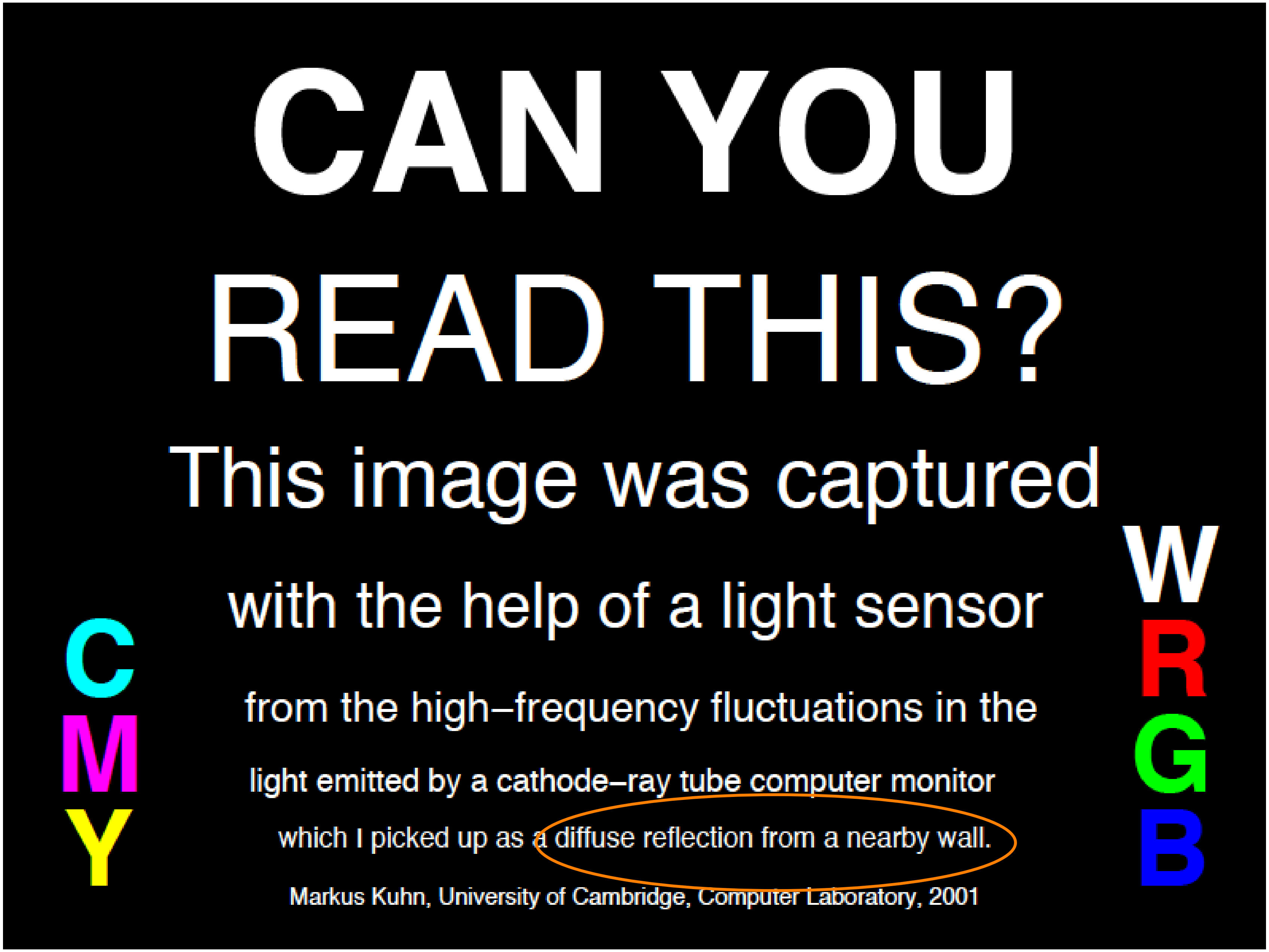

Thus, if image isn't changing, each pixel is **periodically** illuminated at **its own unique time**



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



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