# Side Channels

EECS 388

Monday, April 13, 2015

# Covert Channels

- Communication between two cooperating parties that uses a hidden (secret) channel
- Main requirement is agreement between sender and receiver (established in advance)
- Example: suppose (unprivileged) program **A** wants to send 128 bits of secret data to (unprivileged) program **B** ...
  - But can't use pipes, sockets, signals, shared memory, or network connections; can only read files, can't write them
  - How can they cooperate to achieve this?

# Covert Channels

- Method #1: Divide time up into 128 time slots. In *i*th time slot, **A** either runs heavy computation or idles, to communicate 0 or 1 bit. **B** monitors CPU usage.
- Method #2: Pick 128 files in advance. **A** reads *i*th file, for each *i* where secret has a 1-bit. **B** observes access time on each file.
- There are so many other possibilities...

# Covert Channels

- How do we stop covert channels?
- Answer: We can't. Attacker always wins.
- The only alternative is: don't let **A** know anything secret. i.e., don't let untrusted programs ever learn anything secret, because they can exfiltrate it.

# Side Channels

- Unintended information leakage from **A** to **B**.
- Crucially, here **A** and **B** are not cooperating. Instead, **B** is exploiting some aspect of how system is structured to learn something about **A** that **A** would not want to have revealed.
- Can be difficult to recognize because often system builders "abstract away" seemingly irrelevant elements of system structure

# Inferring Password via Side Channel

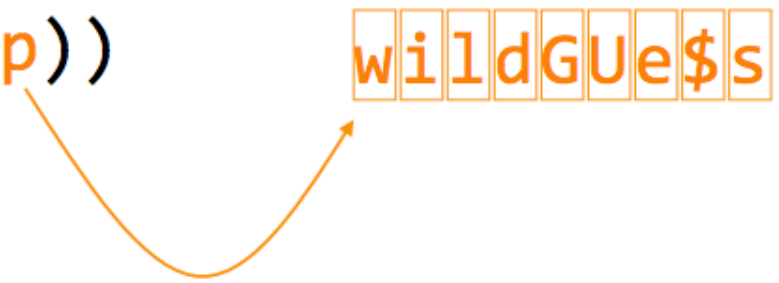
```
/* Returns true if the password from the
 * user, 'p', matches the correct master
 * password. */

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];
}
```

Attacker knows code, but not this value

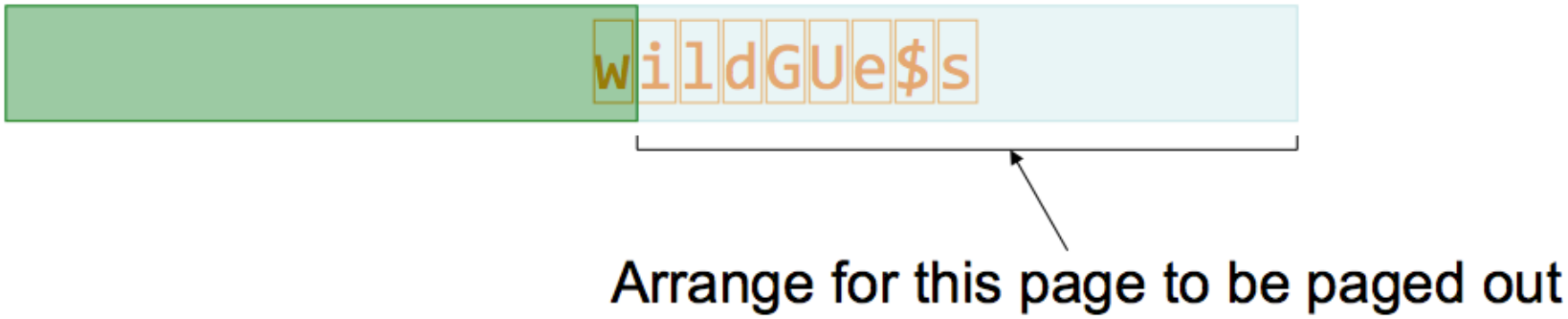
# Inferring Password via Side Channel

- Suppose the attacker's code can call **check_password()** many times (but not billions/trillions)
  - 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();
...
```



- Spread p across different memory pages:

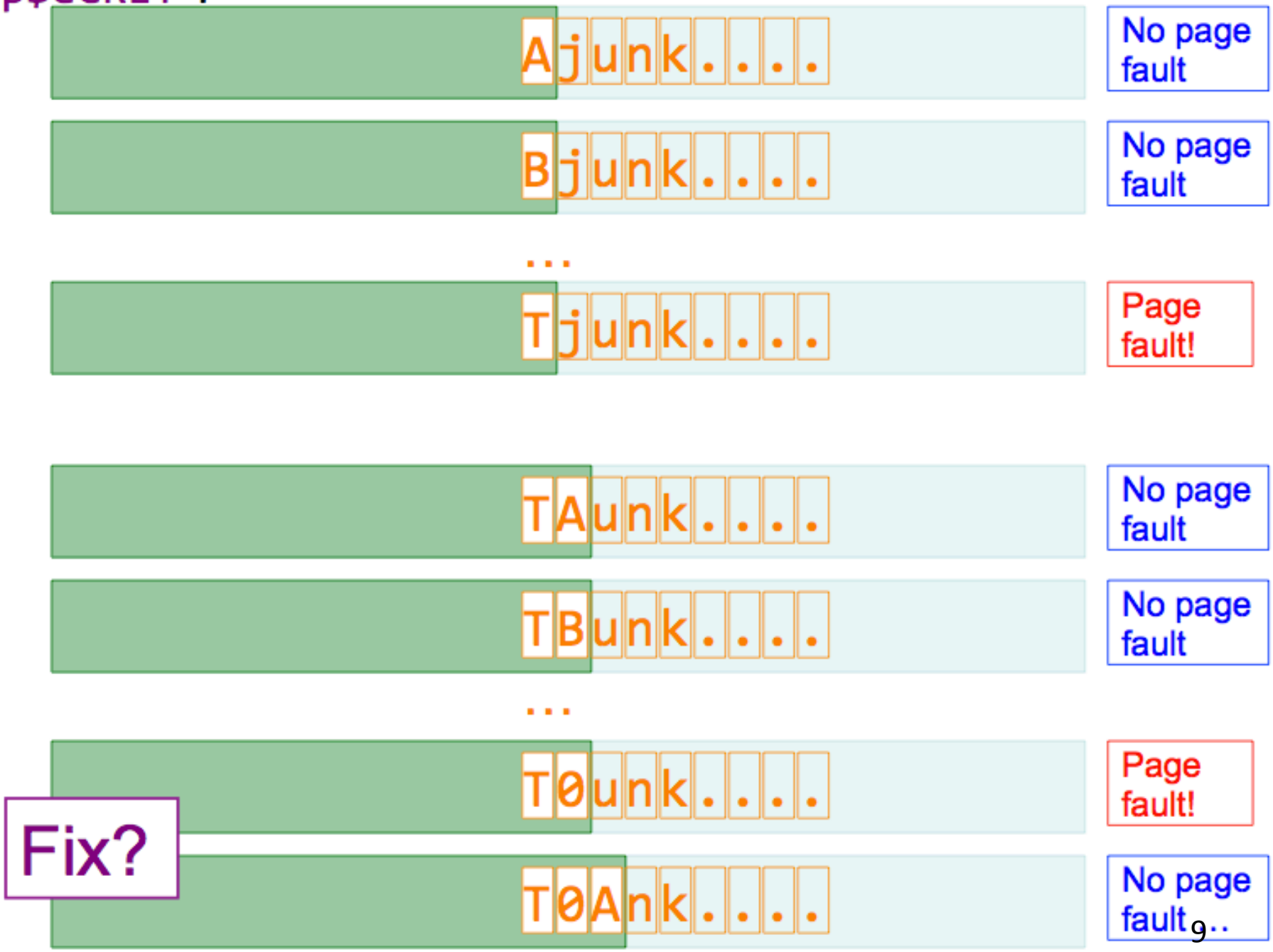



- If master password doesn't start with 'w', then loop exits on first iteration (i=0):

```
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 ?




Fix?

```
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**

**Note: total time correlated to number of matches**

```
bool check_password3(uchar *p)
{
  static uchar *master_pw = "T0p$eCRET";
  int i;
  int diff = 0;
  for(i=0; p[i] && master_pw[i]; ++i)
     diff |= p[i] ^ master_pw[i];
  diff |= p[i] ^ master_pw[i];
  return diff == 0;
}
```

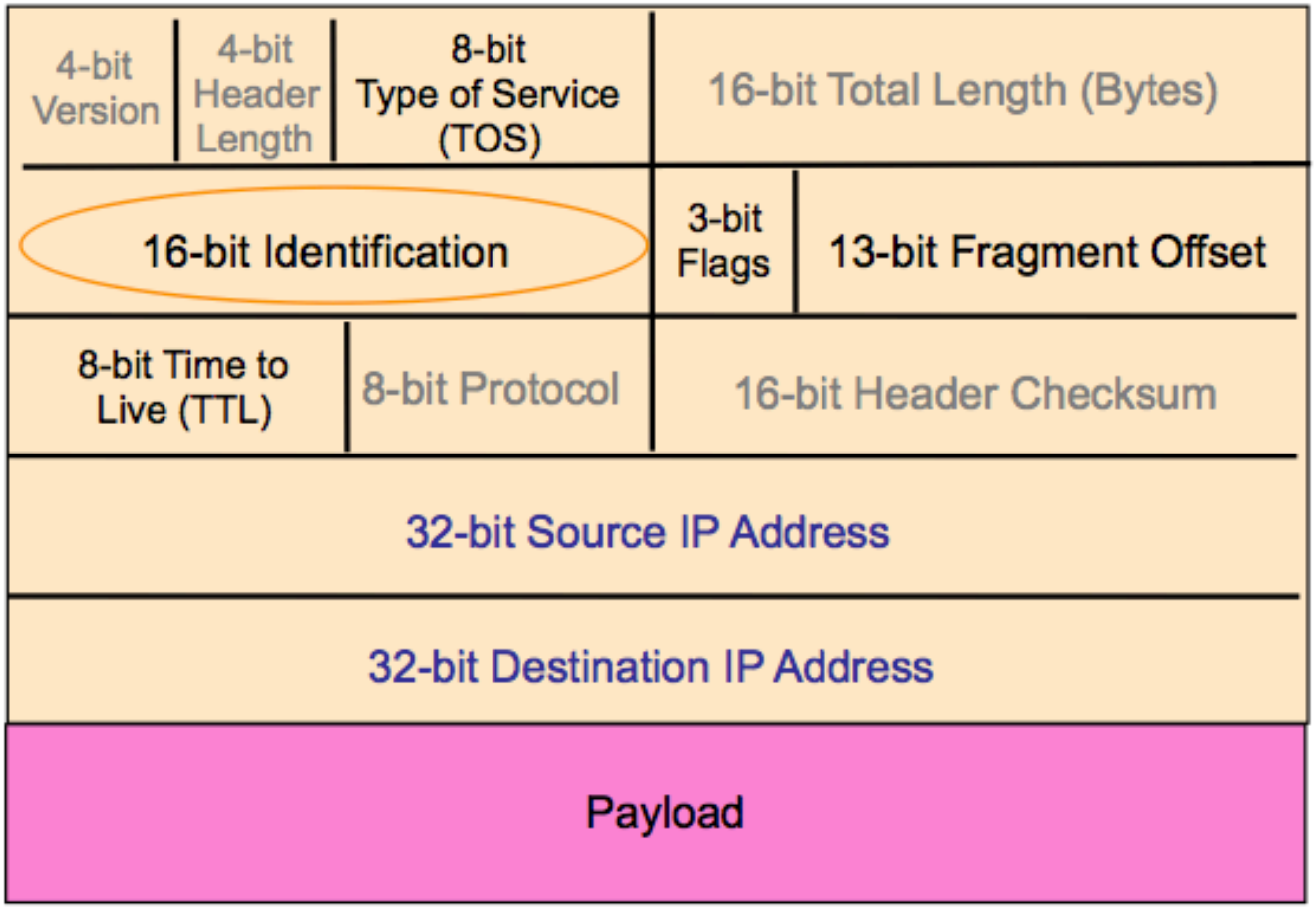
**Constant-time equality check.**
**Important in crypto (e.g., checking MAC tag).**

# Exploiting Side Channels For Stealth Scanning

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

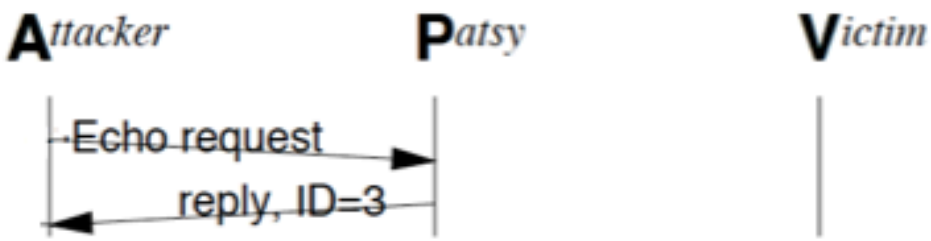
- Seems impossible: how can **A** receive the results of probes **A** sends to **V**, unless probes include **A**'s IP address for **V**'s replies?

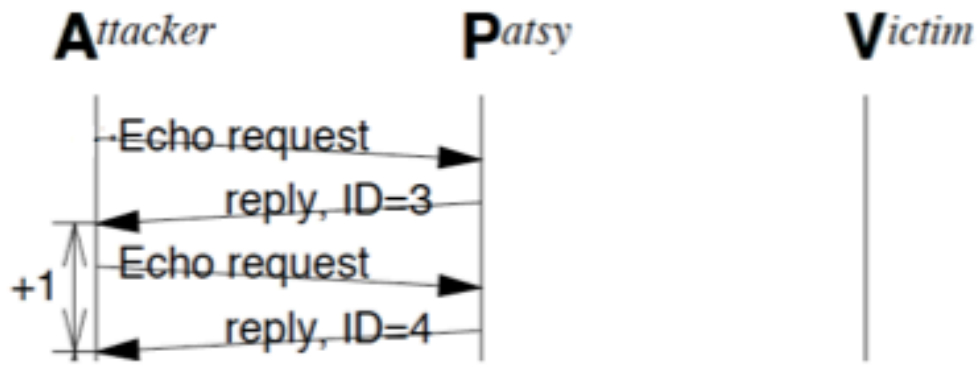
# IP Header Side Channel

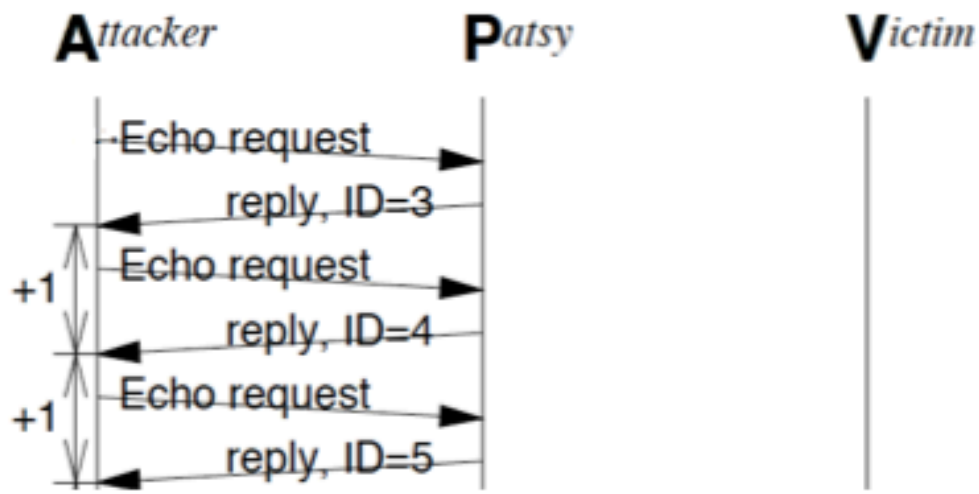


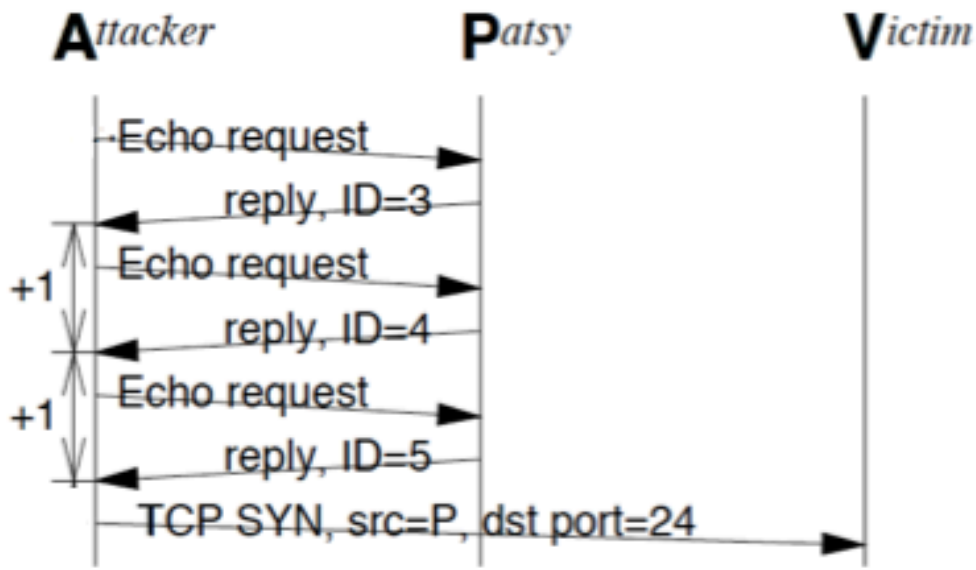

ID field is supposed to be unique per IP packet.

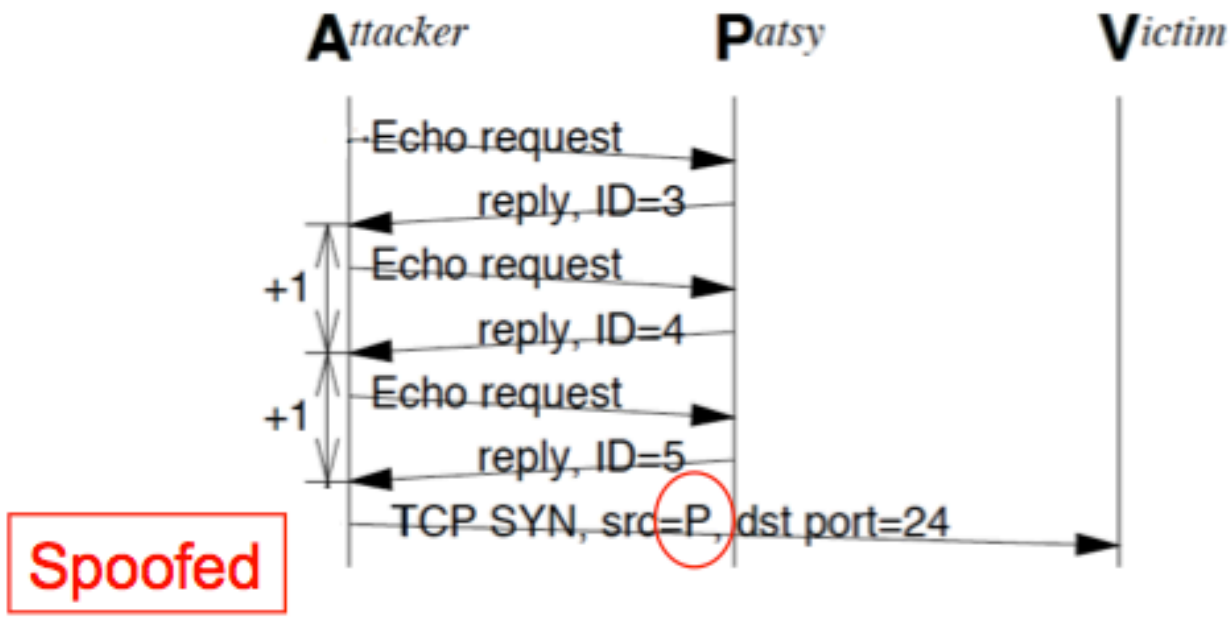
One easy way to do this: increment it each time system sends a new packet.

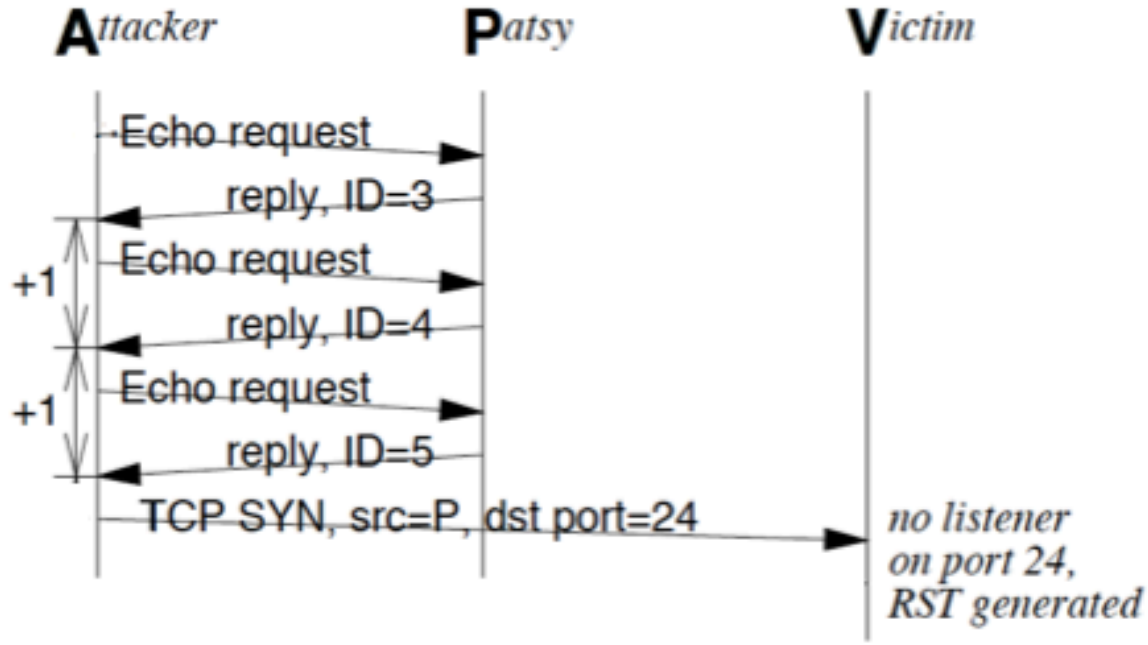

Attacker
Patsy
Victim
Echo request
reply, ID=3

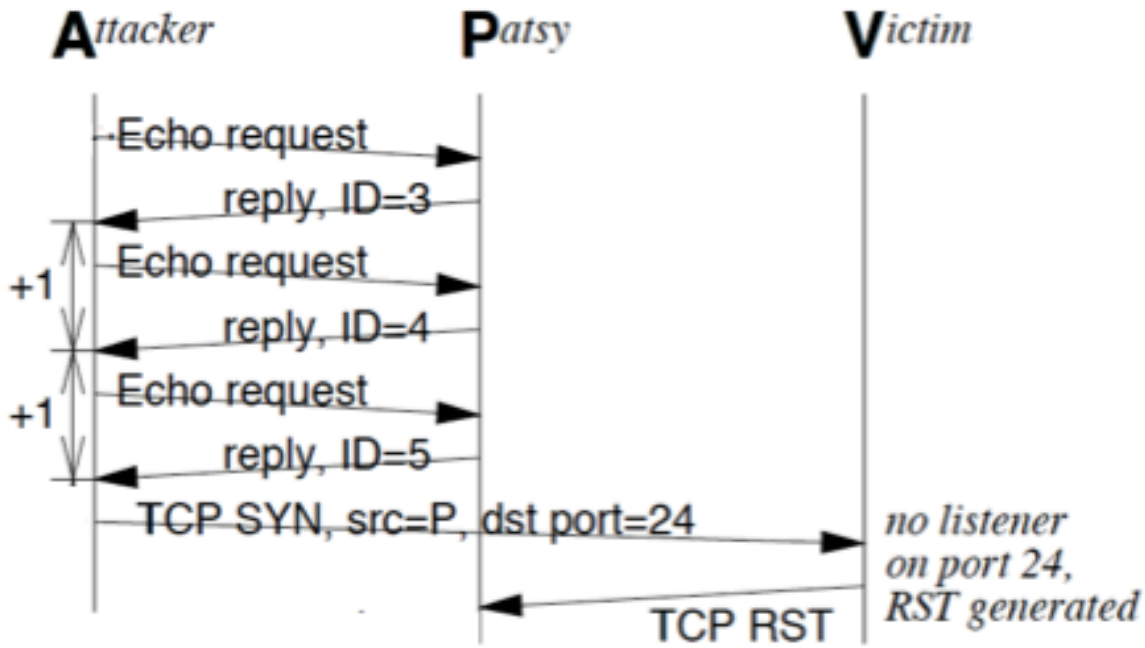

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
reply, ID=4
+1

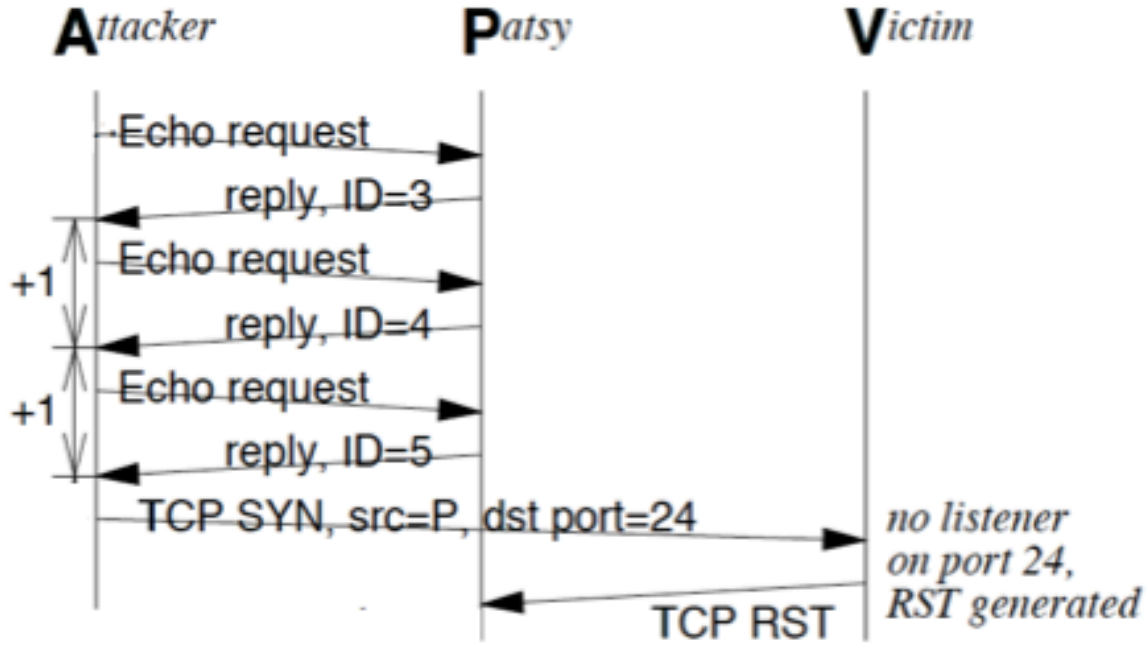

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5


Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5
TCP SYN, src=P, dst port=24

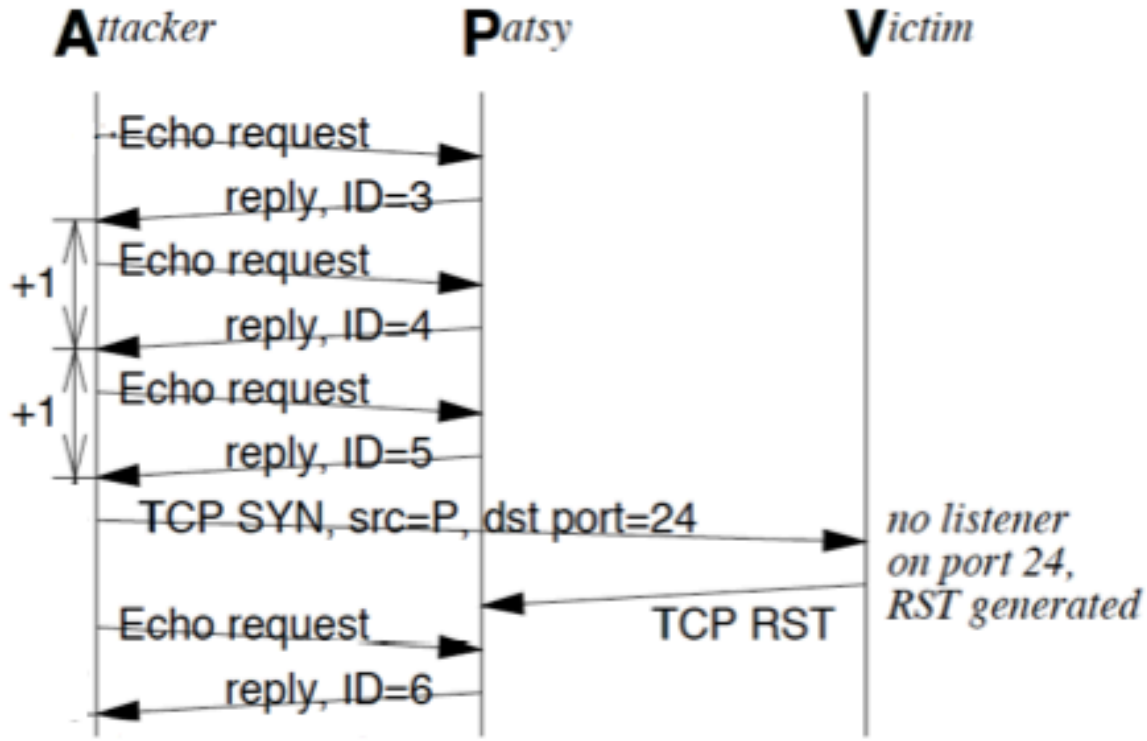

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5
TCP SYN, src=P, dst port=24
Spoofed

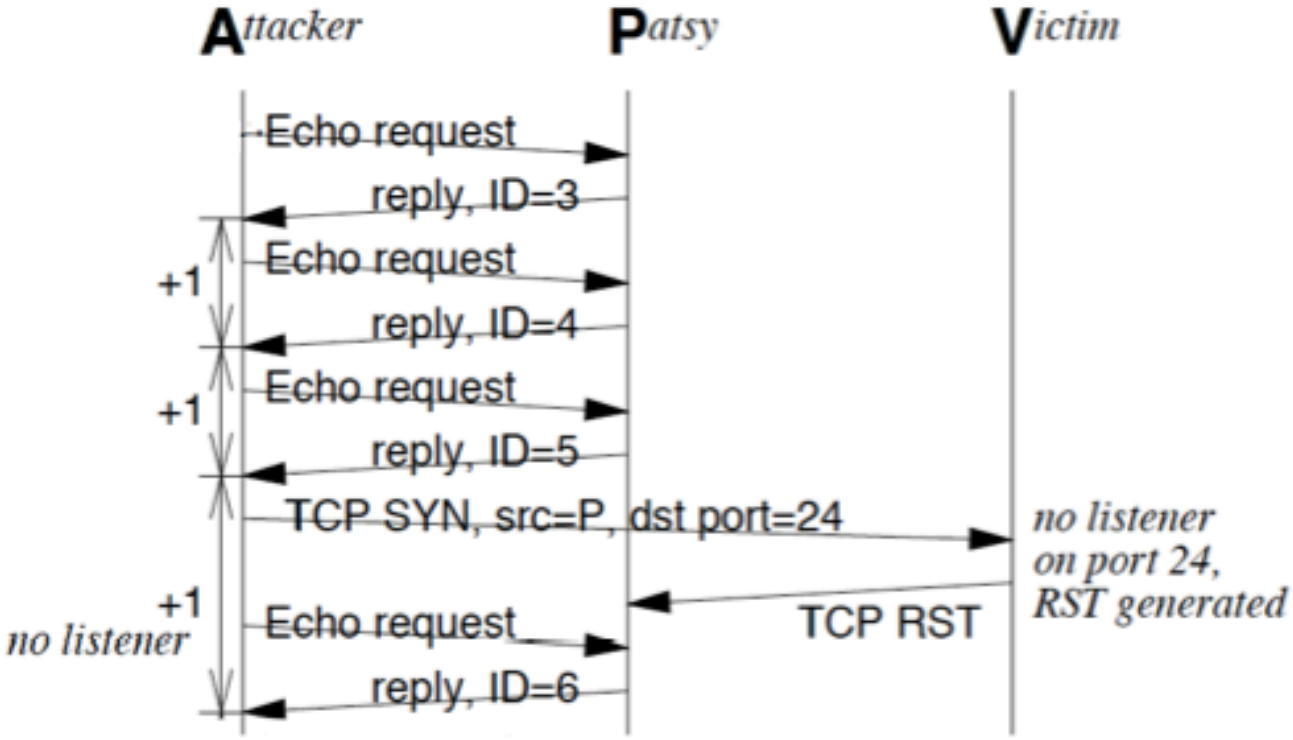

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated

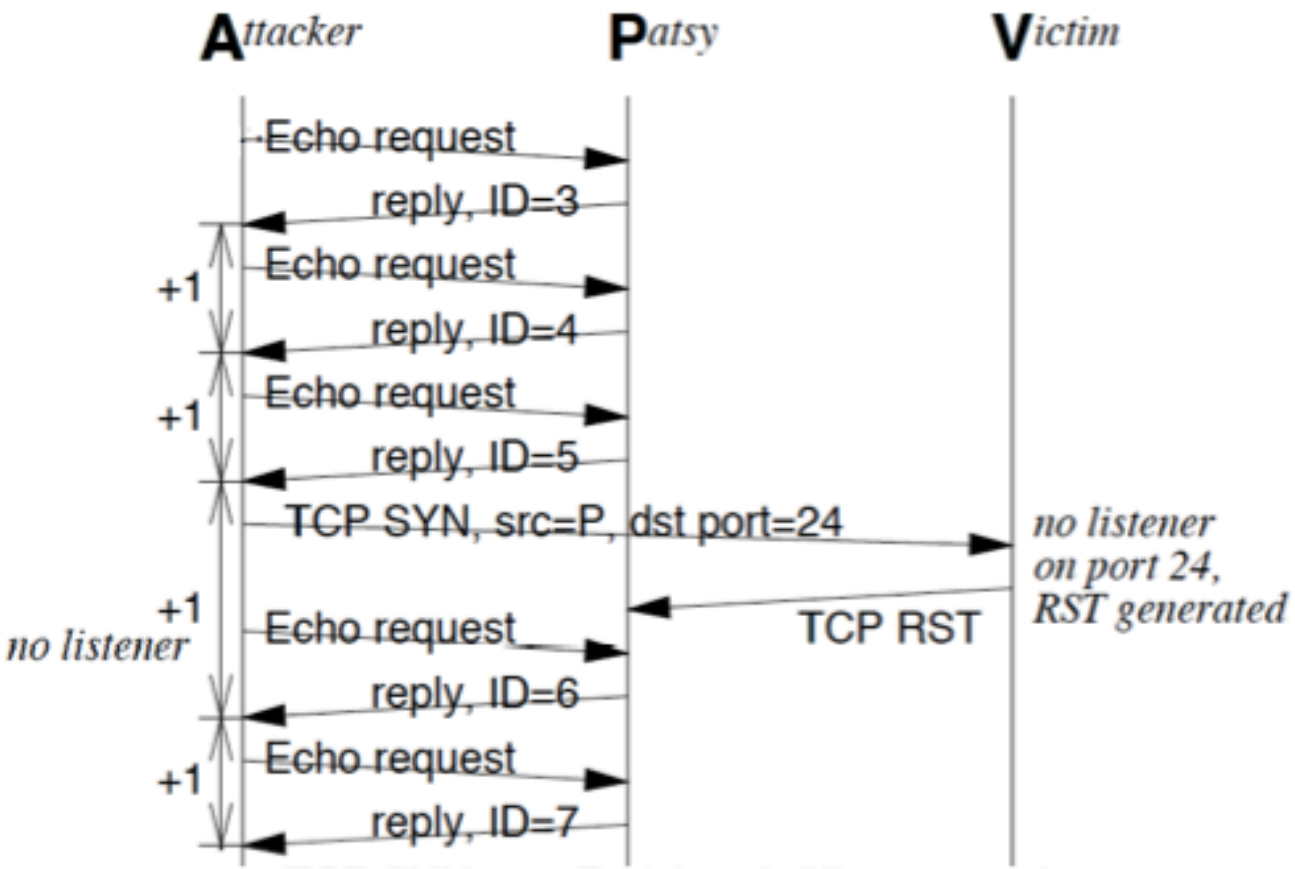

Attacker
Patsy
Victim
Echo request
reply, ID=3
Echo request
+1
reply, ID=4
Echo request
+1
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST

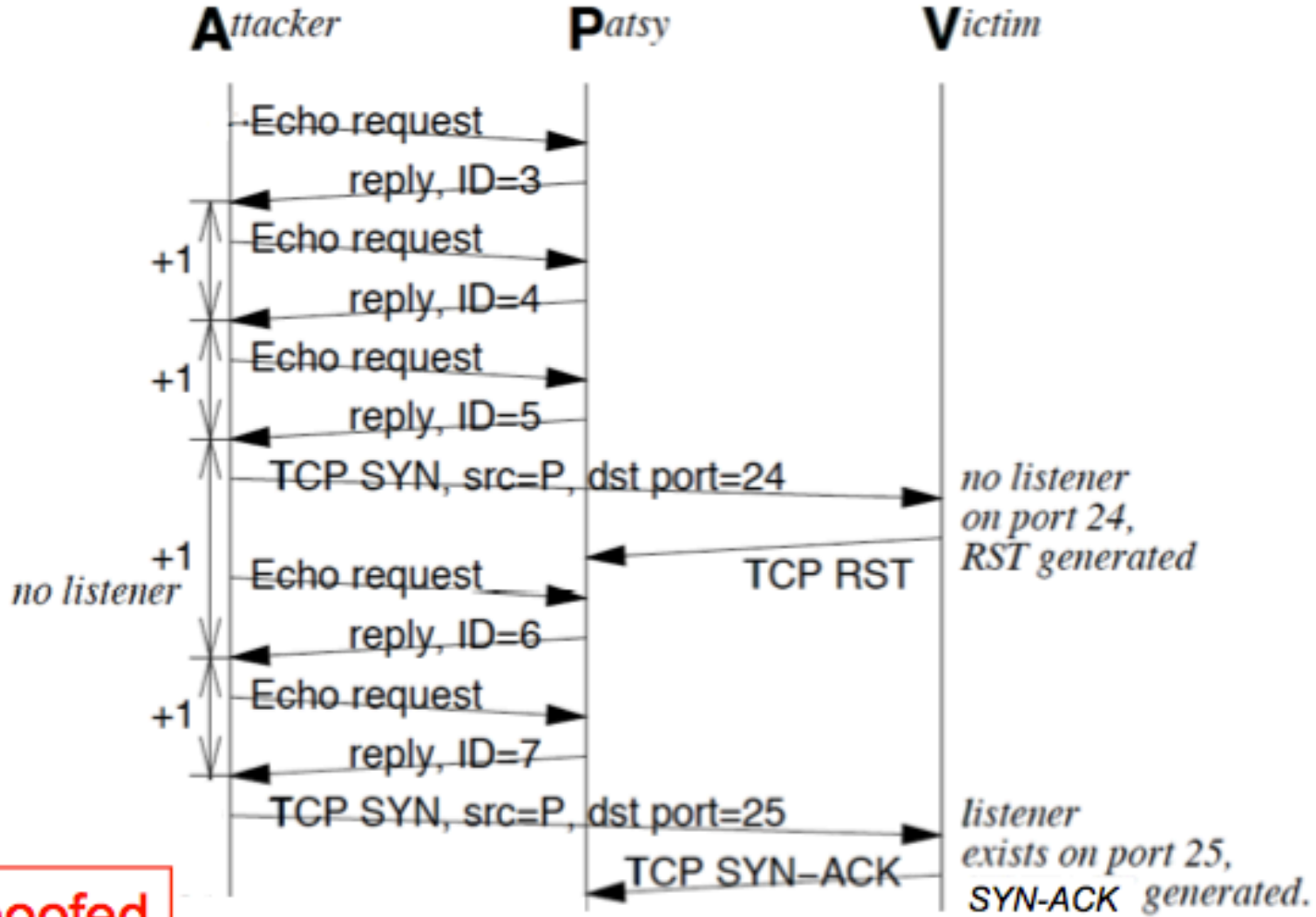


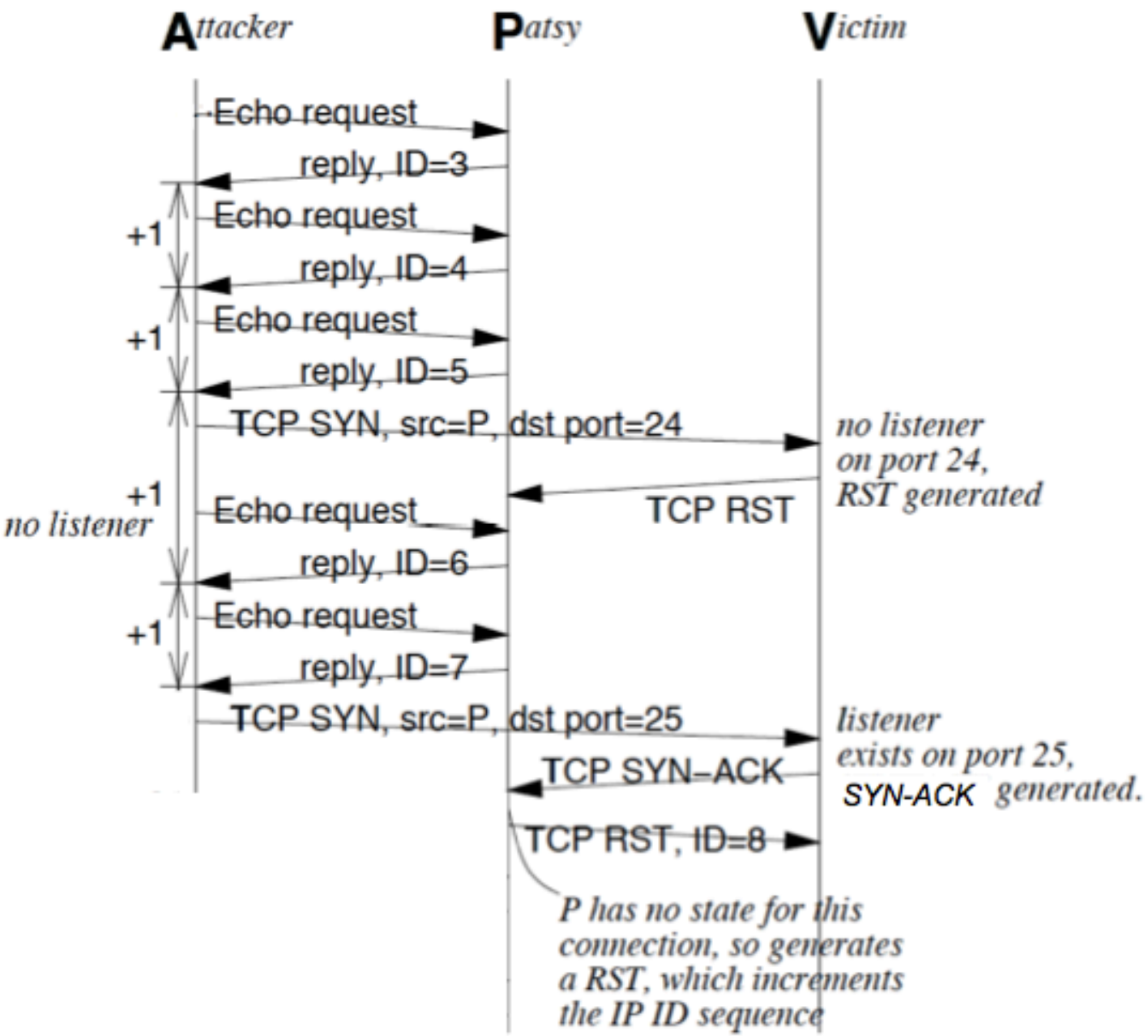

Upon receiving RST, Patsy ignores it and does nothing, per TCP spec.

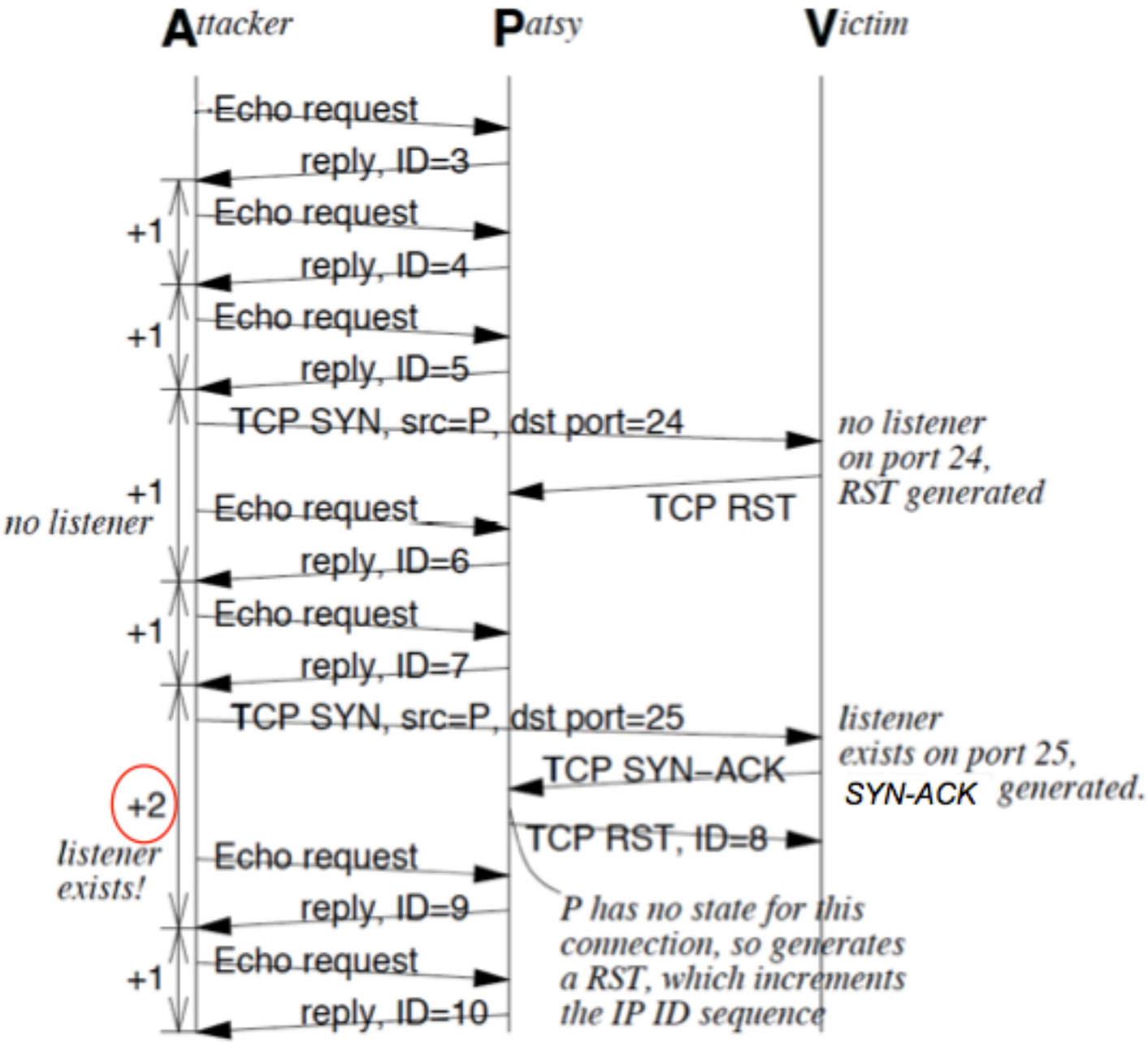

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener
on port 24,
RST generated
TCP RST
Echo request
reply, ID=6


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
+1
no listener
Echo request
TCP RST
reply, ID=6


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
+1
no listener
Echo request
TCP RST
reply, ID=6
+1
Echo request
reply, ID=7


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
+1
no listener
Echo request
TCP RST
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
listener
exists on port 25,
TCP SYN–ACK
SYN-ACK generated.
Spoofed


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
+1
no listener
Echo request
TCP RST
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
listener
exists on port 25,
TCP SYN–ACK
SYN-ACK generated.
TCP RST, ID=8
P has no state for this
connection, so generates
a RST, which increments
the IP ID sequence

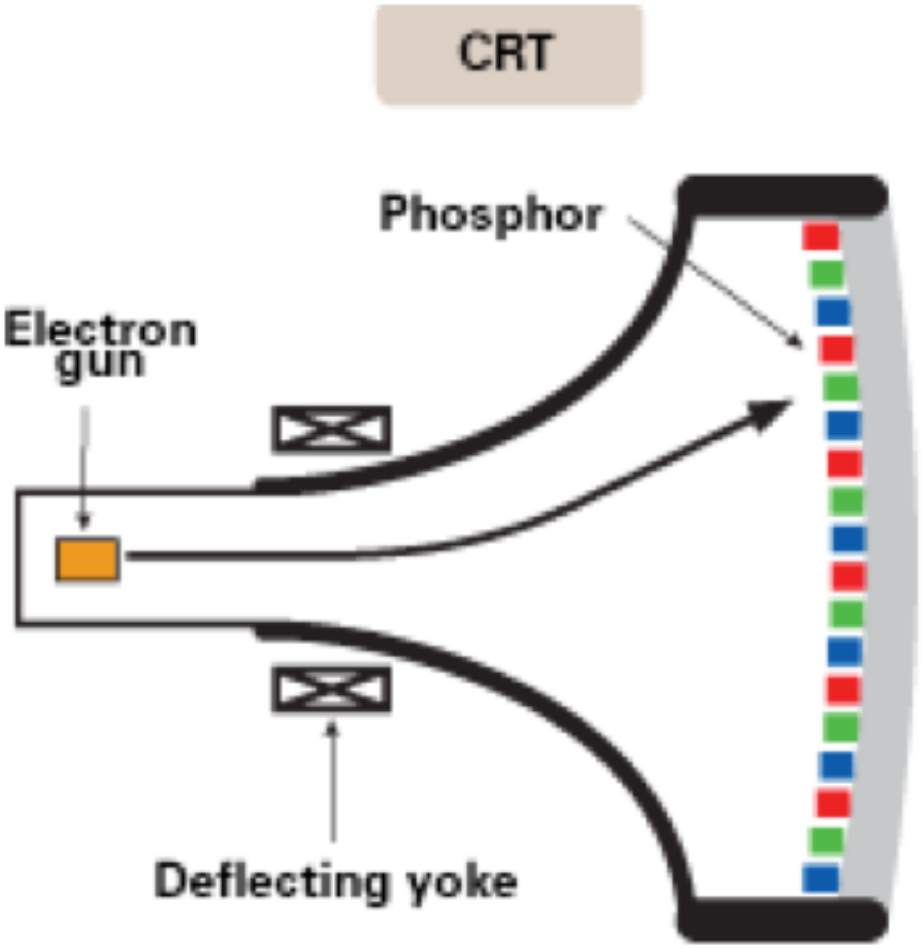

Attacker
Patsy
Victim
Echo request
reply, ID=3
+1
Echo request
reply, ID=4
+1
Echo request
reply, ID=5
TCP SYN, src=P, dst port=24
no listener on port 24, RST generated
TCP RST
+1
no listener
Echo request
reply, ID=6
+1
Echo request
reply, ID=7
TCP SYN, src=P, dst port=25
listener exists on port 25, SYN-ACK generated.
TCP SYN–ACK
+2
TCP RST, ID=8
listener exists!
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

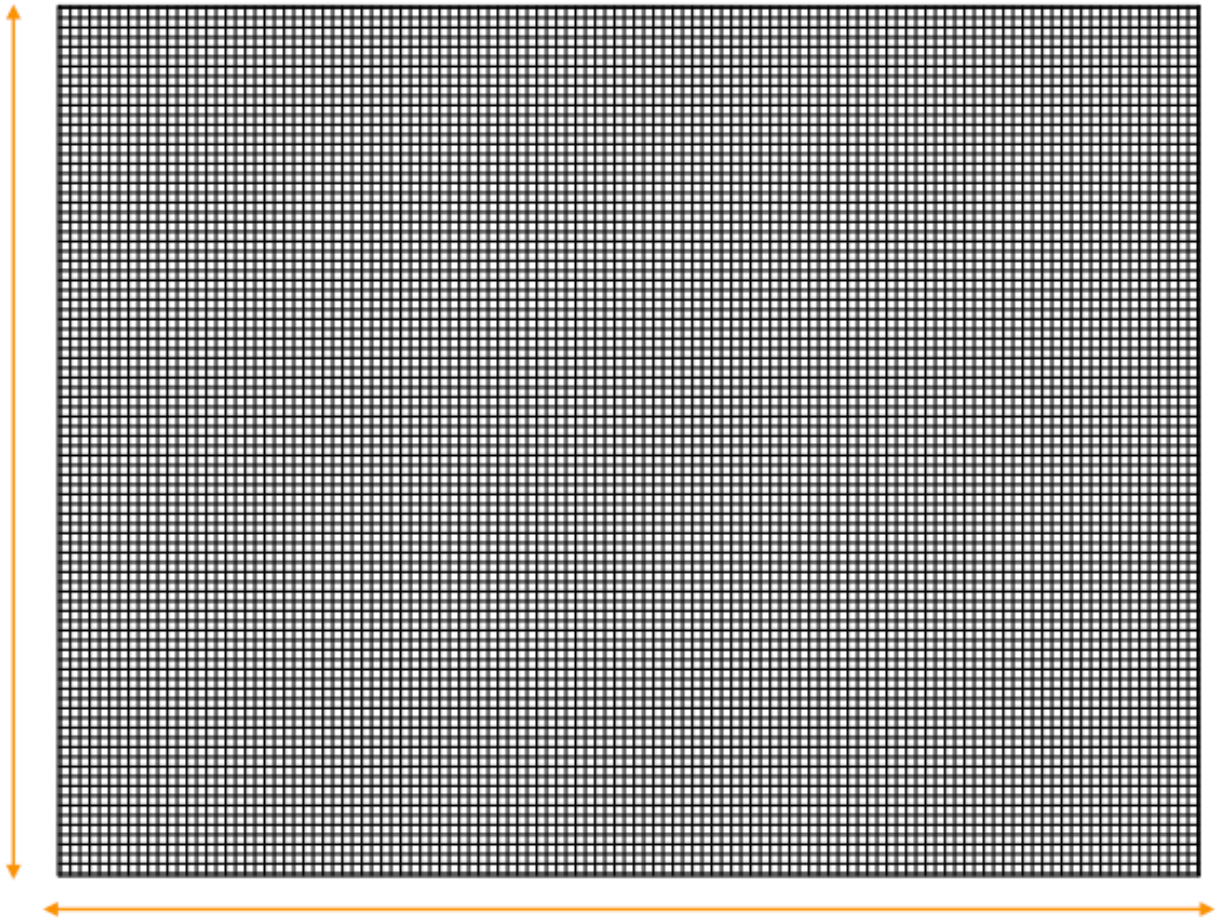
- Scenario: Ann the Attacker works in a building across the street from Victor the Victim. Late one night Ann can see Victor hard at work in his office, but can't see his CRT display, just the glow of it on his face.

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

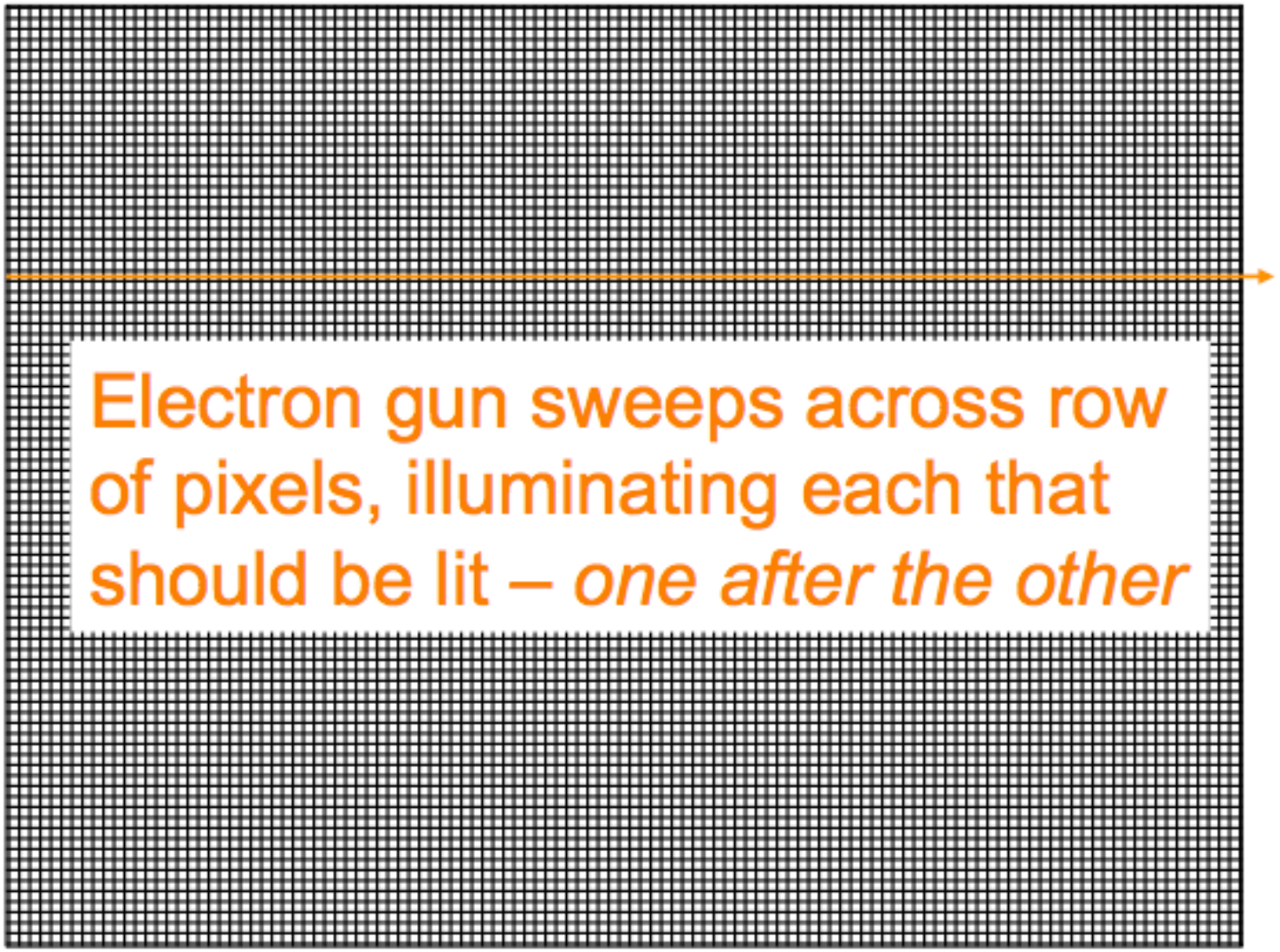
# Cathode Ray Tube (CRT)

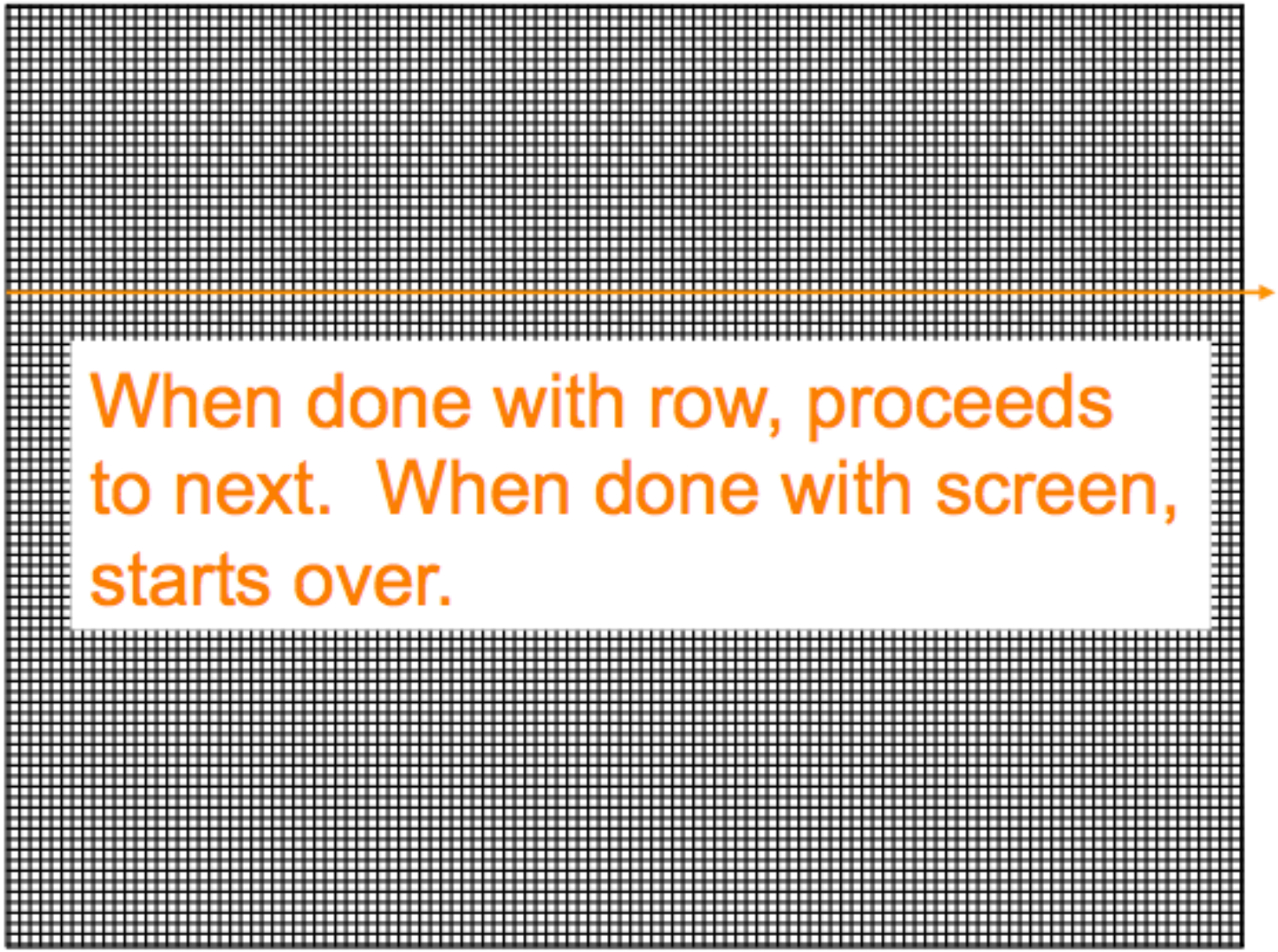


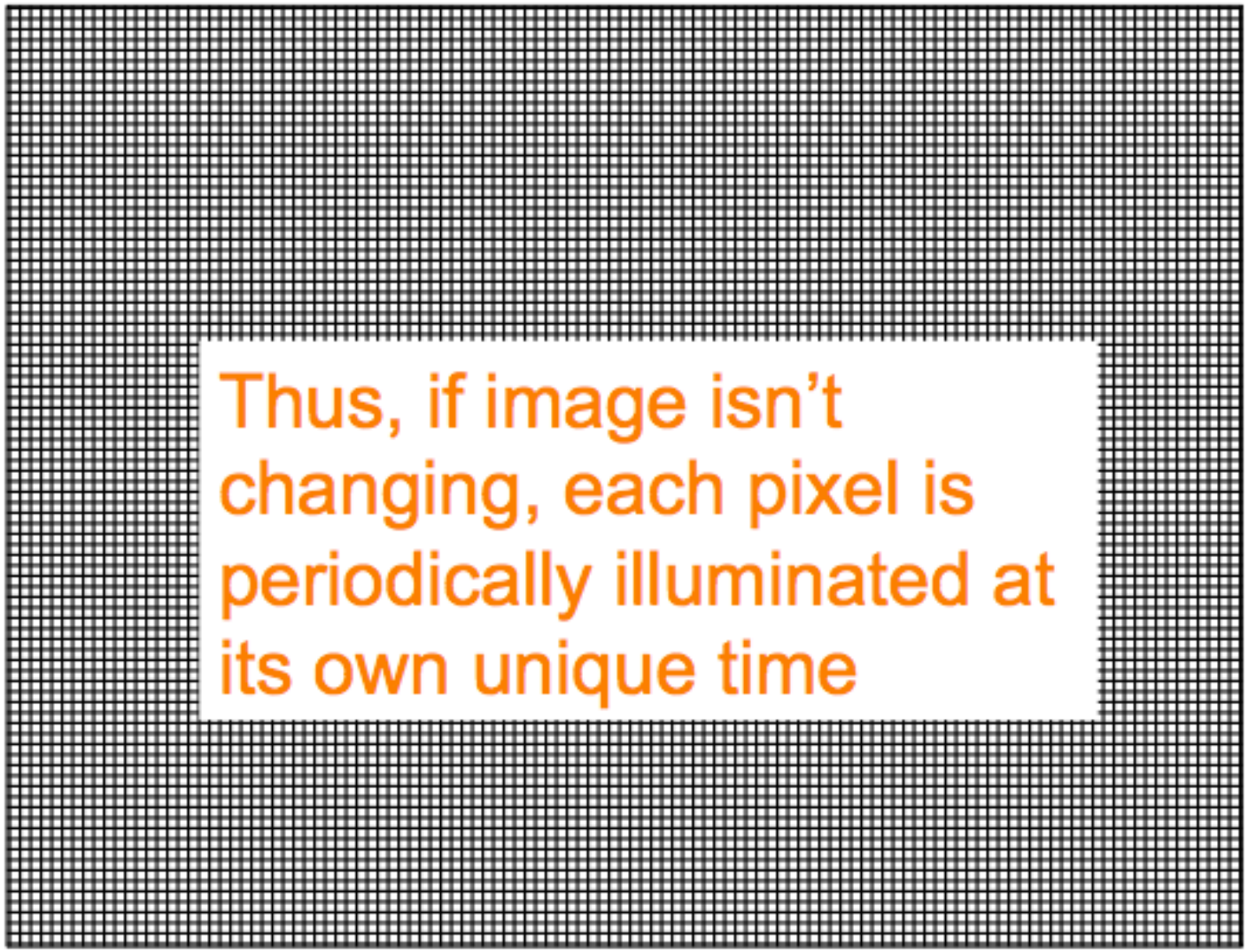
# CRT display is made up of an array of phosphor pixels



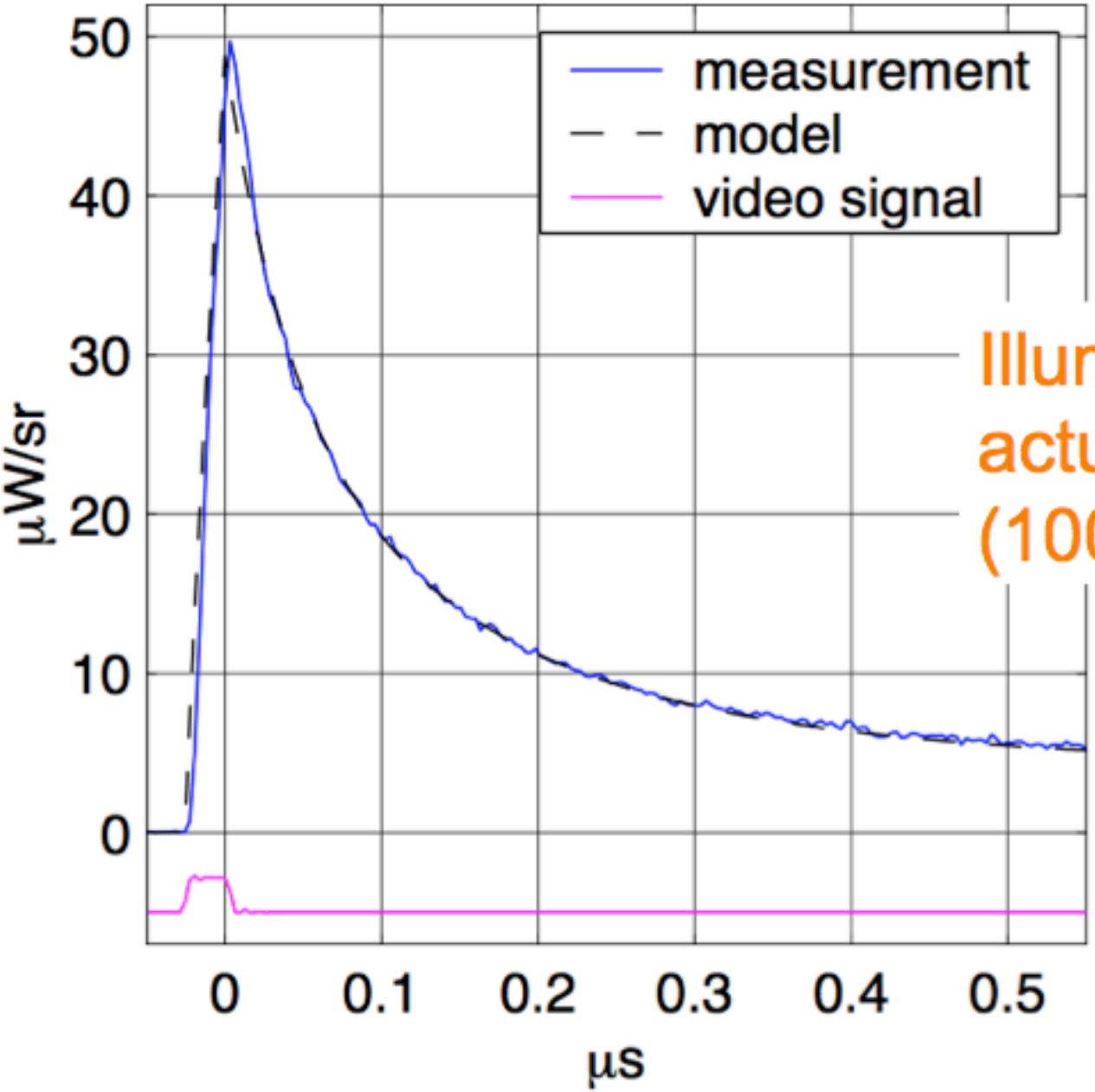
640x480 (say)


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

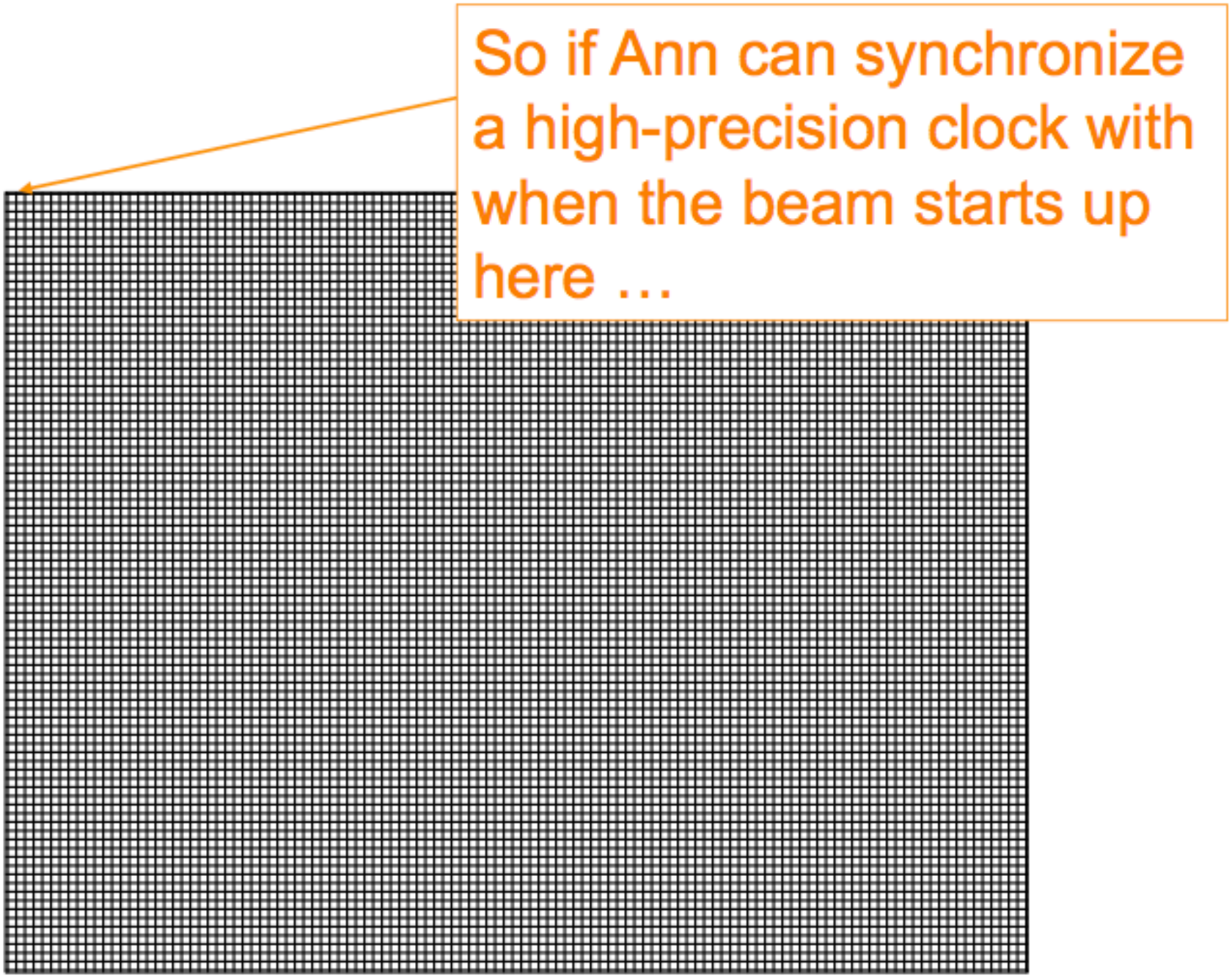

When done with row, proceeds to next. When done with screen, starts over.

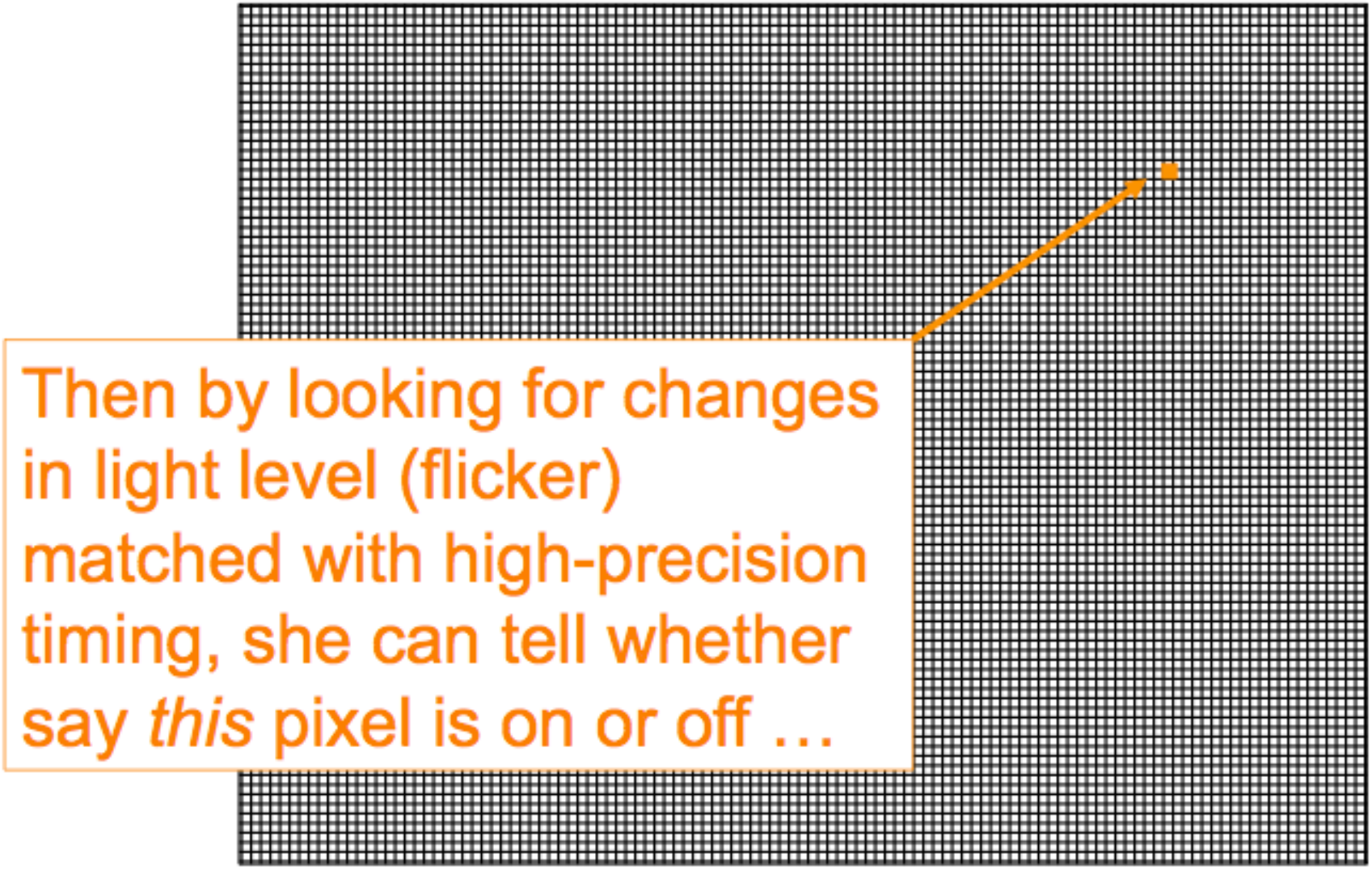

Thus, if image isn't changing, each pixel is periodically illuminated at its own unique time

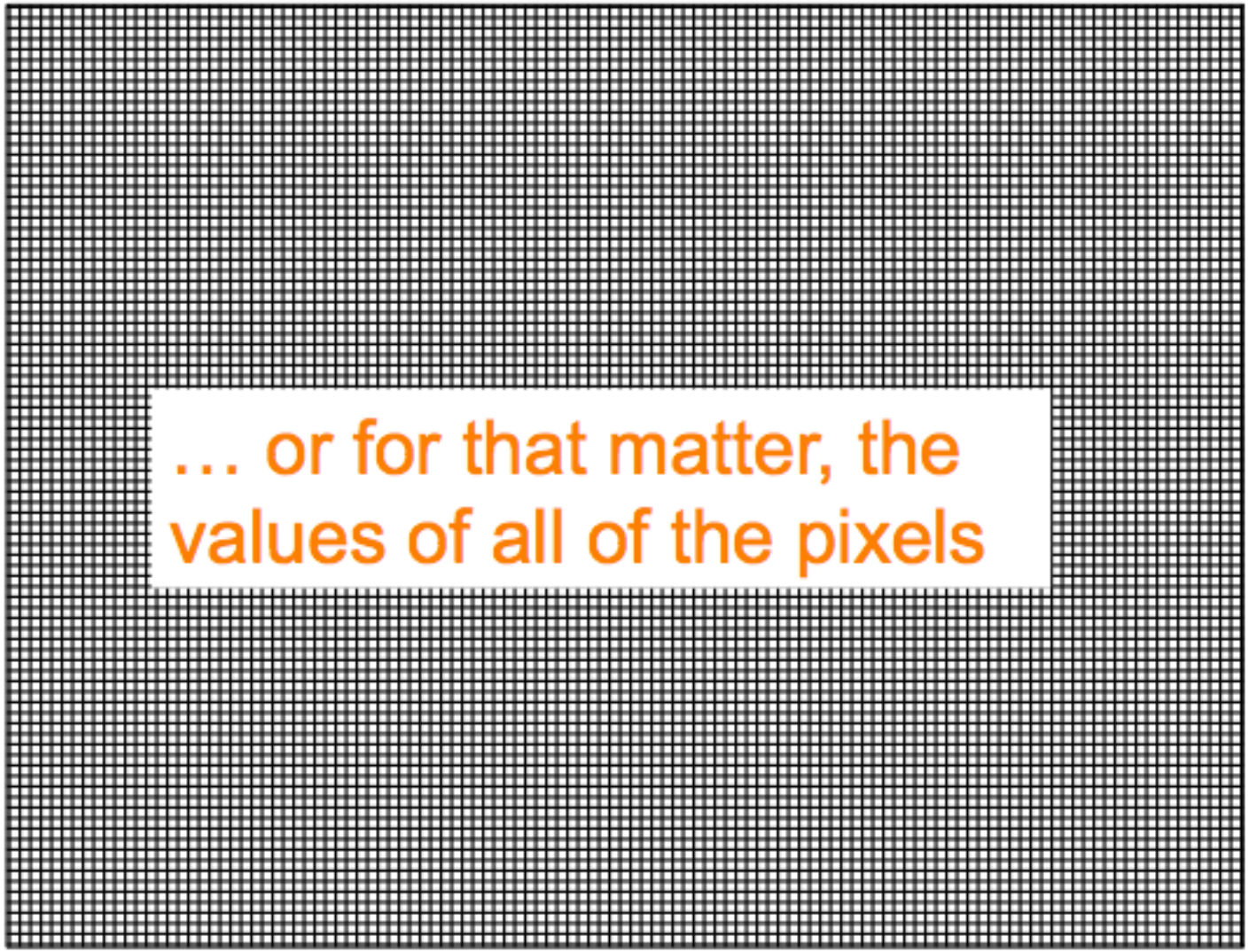
(a) Emission decay of a single pixel ($f_p$ = 36 MHz)

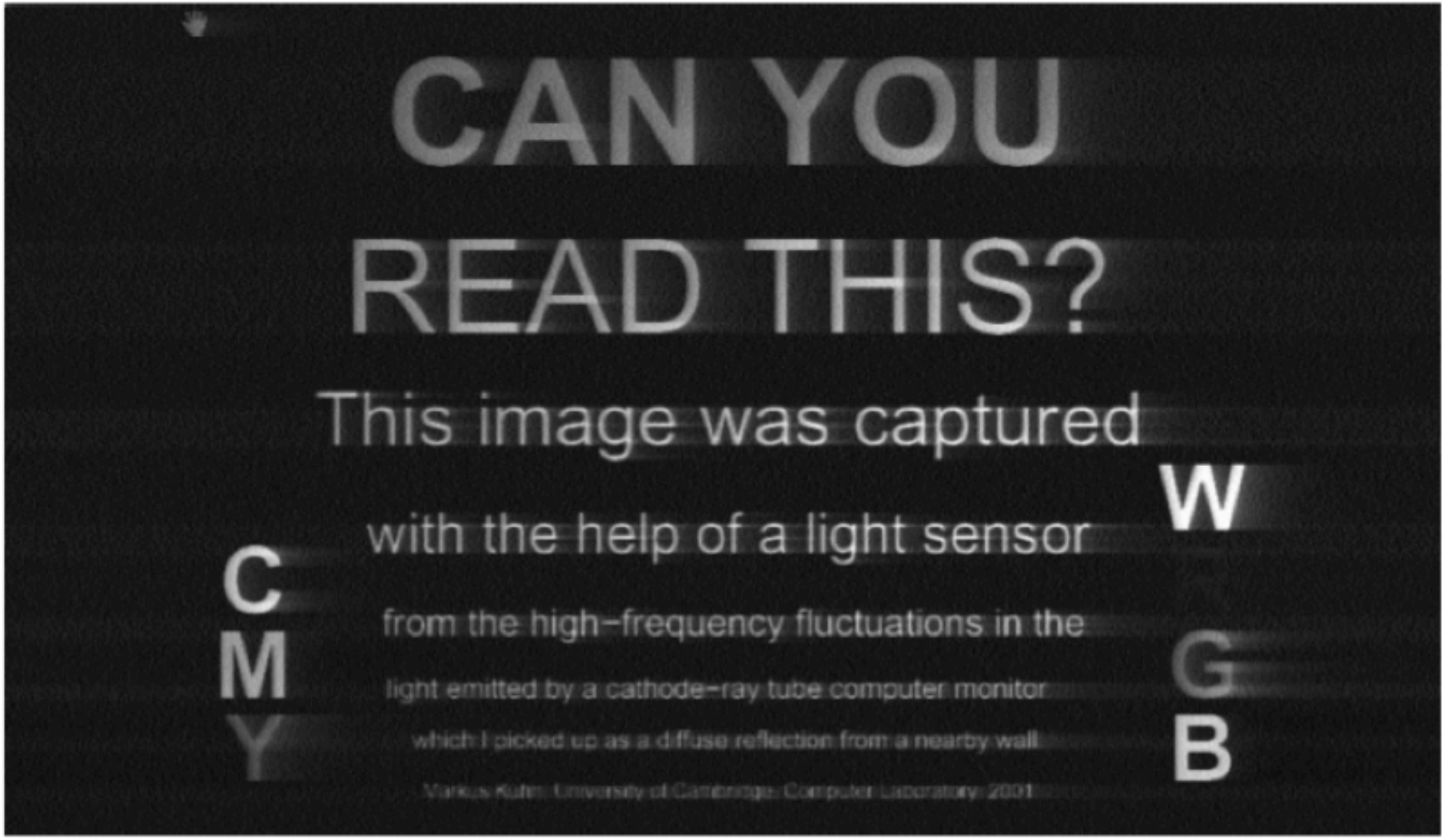



Illumination is actually short-lived (100s of nsec).

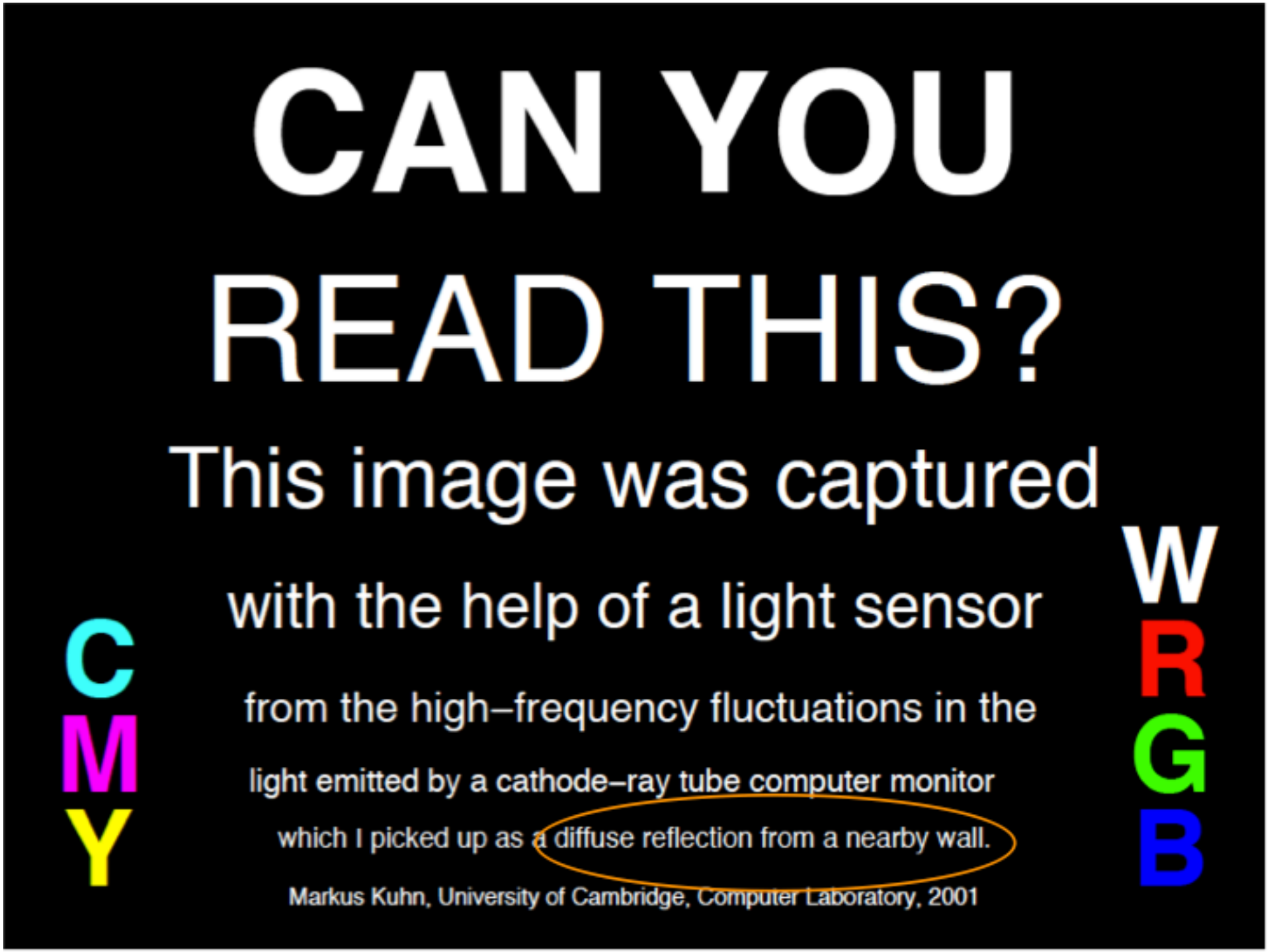

So if Ann can synchronize a high-precision clock with when the beam starts up here …


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

# 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

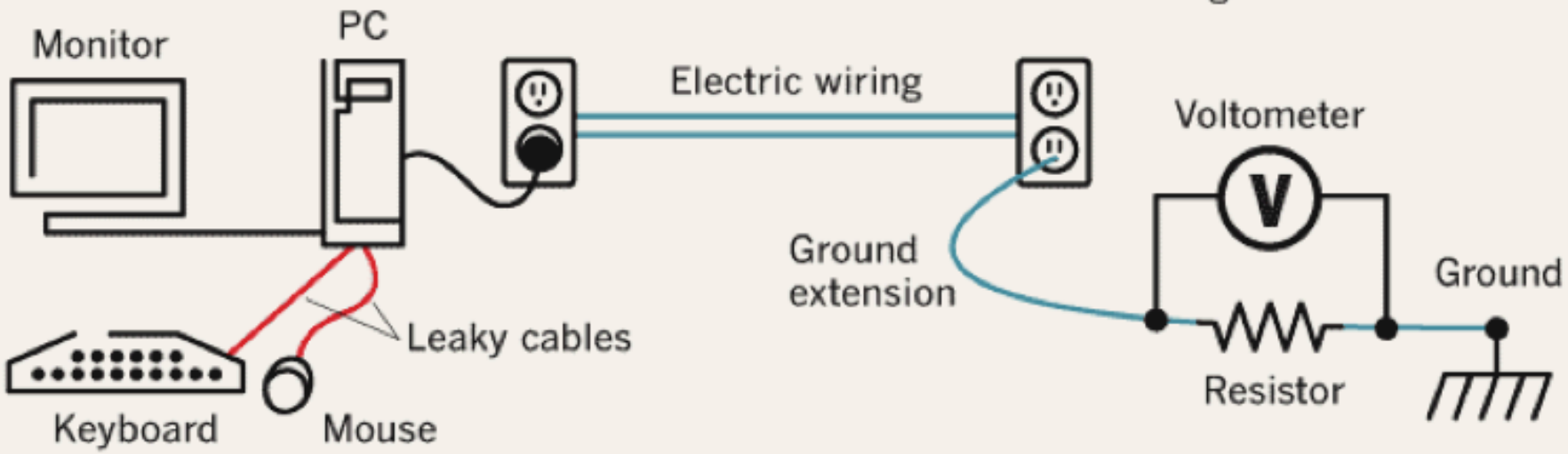
# Stealing keystrokes through electric lines

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.



# UI Side Channel Snooping

- 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!


**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.**

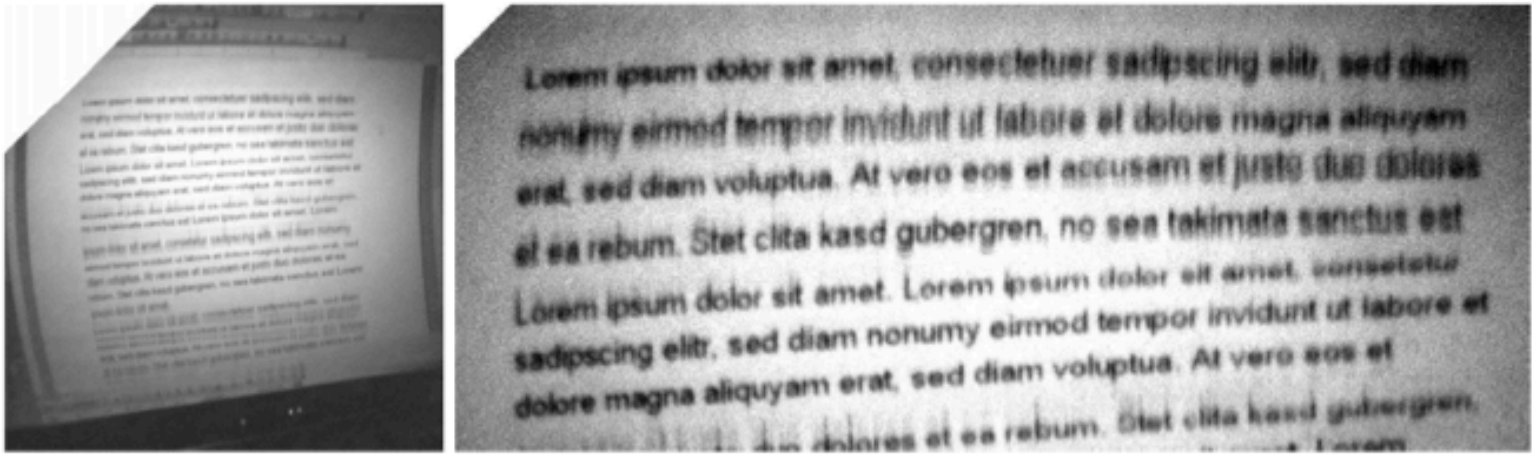



**Figure 7. Reflection of a Word document with small 12pt font size in a tea pot, taken from a distance of 5m. The 12pt font is readable from the reflection.**

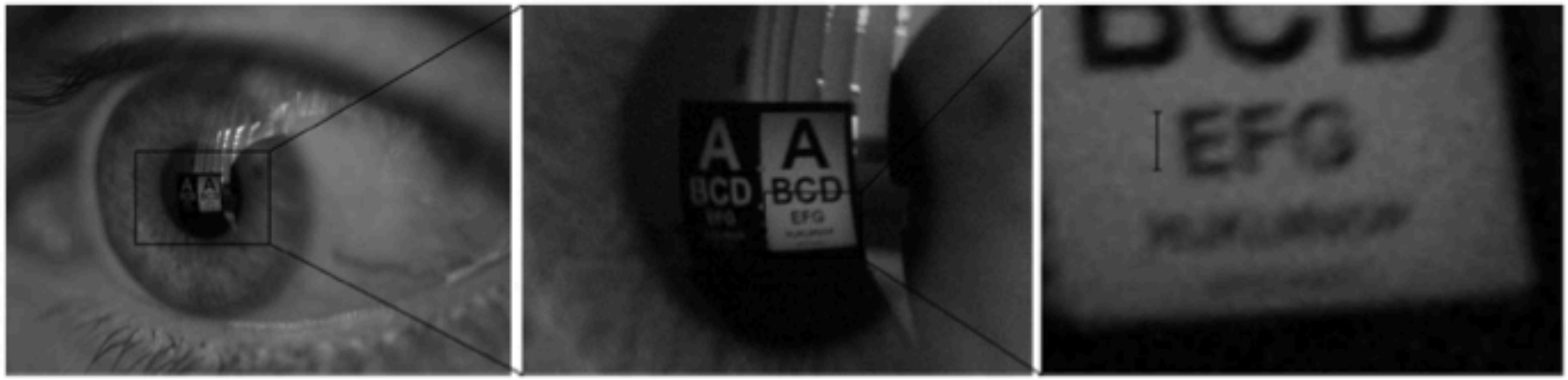



**Figure 9. Image taken with a macro lens from very short distance, with realistic distance between the monitor and the eye. Readability is limited by the resolution of the camera.**


**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

Fox News | Fox Business | uReport | Fox News Radio | Fox News Latino | Fox Nation | Fox News Insider

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

Home | Video | Politics | U.S. | Opinion | Entertainment | Tech | Science | Health | Travel | Lifestyle | World | Sports | On Air

# 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

FOXBUSINESS

| | | | |
|---|---|---|---|
| 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

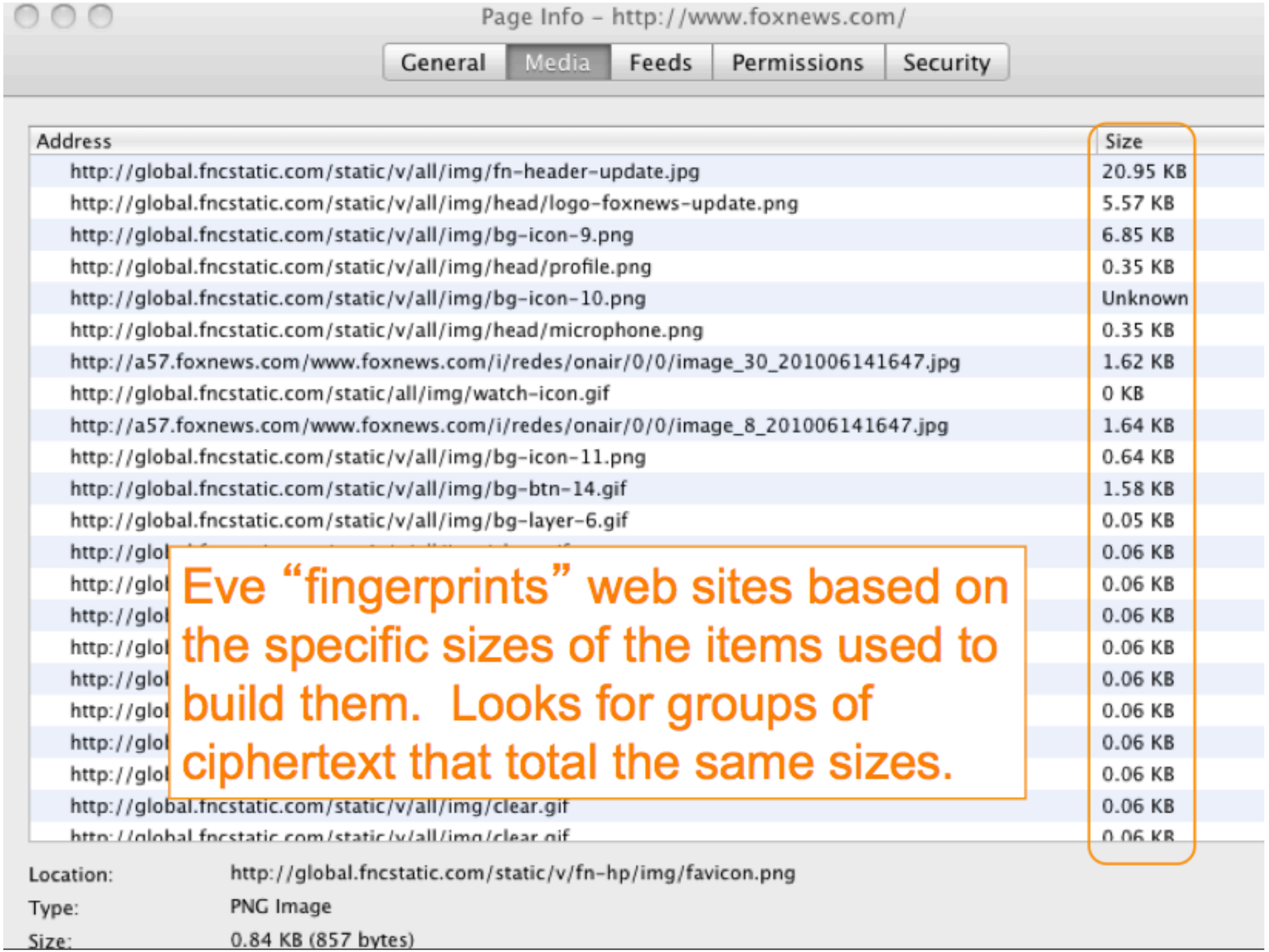
## WATCH NOW

Does the president have an 'image problem'?

High schooler doesn't regret asking Miss America to prom

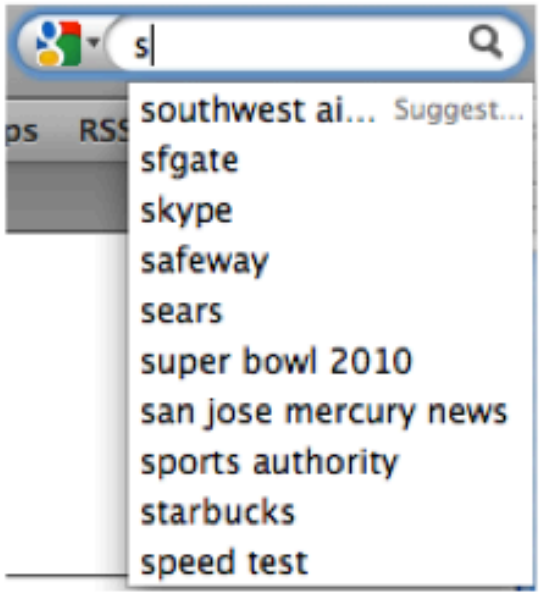
Leopard attacks villagers, causes panic

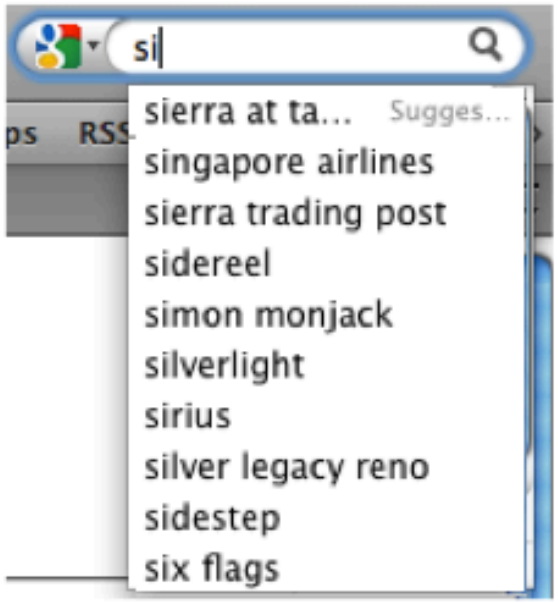
Teen stowaway's adventure raises security concerns

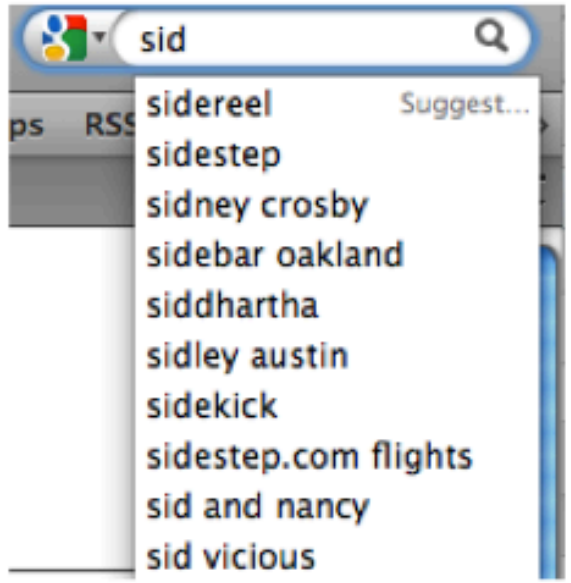

Page Info – http://www.foxnews.com/
General
Media
Feeds
Permissions
Security
Address
Size
http://global.fncstatic.com/static/v/all/img/fn-header-update.jpg 20.95 KB
http://global.fncstatic.com/static/v/all/img/head/logo-foxnews-update.png 5.57 KB
http://global.fncstatic.com/static/v/all/img/bg-icon-9.png 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
0.06 KB
0.06 KB
0.06 KB
0.06 KB
0.06 KB
0.06 KB
0.06 KB
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)

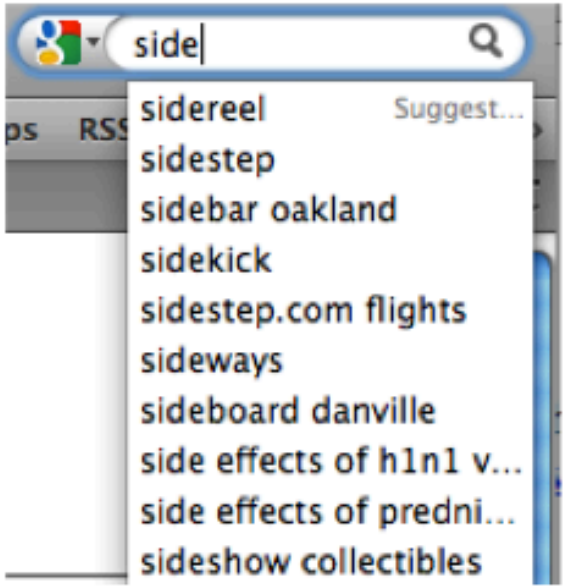
# Side Channels in Web Surfing

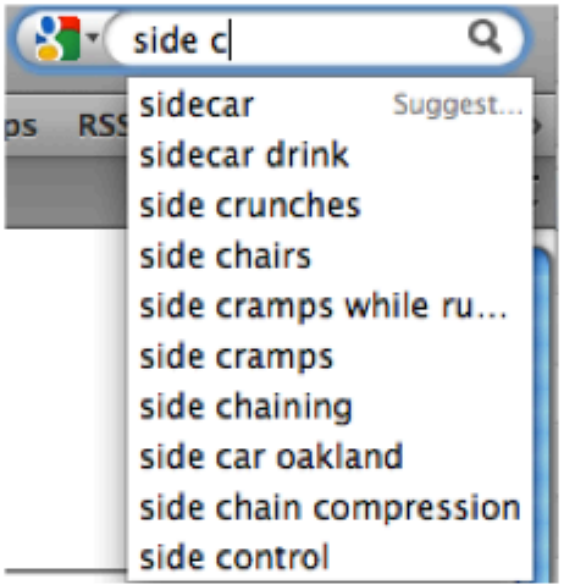
- Suppose Alice is surfing the web and all of her traffic is encrypted and running through an anonymizer
- Eve can observe the presence of Alice's packets & their size, but can't read their contents or ultimate destination
- How can Eve deduce that Alice is visiting FoxNews (say)?
- What about inferring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

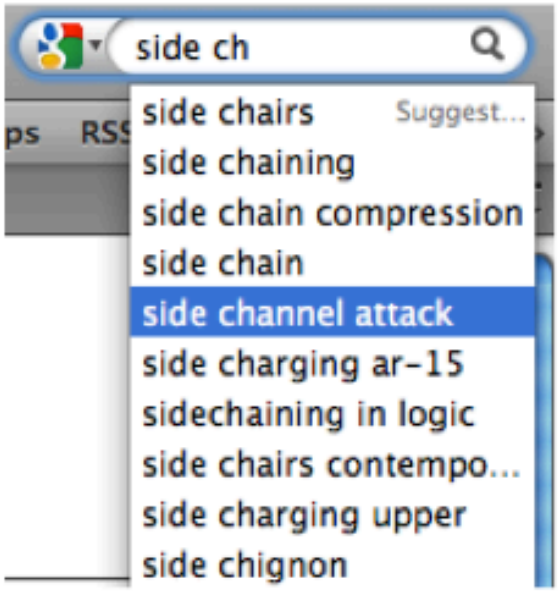

s
southwest ai... Suggest...
sfgate
skype
safeway
sears
super bowl 2010
san jose mercury news
sports authority
starbucks
speed test

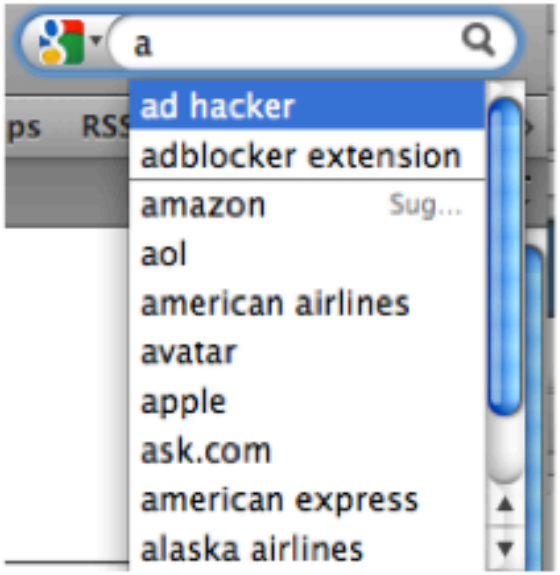

si
sierra at ta... Sugges...
singapore airlines
sierra trading post
sidereel
simon monjack
silverlight
sirius
silver legacy reno
sidestep
six flags


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

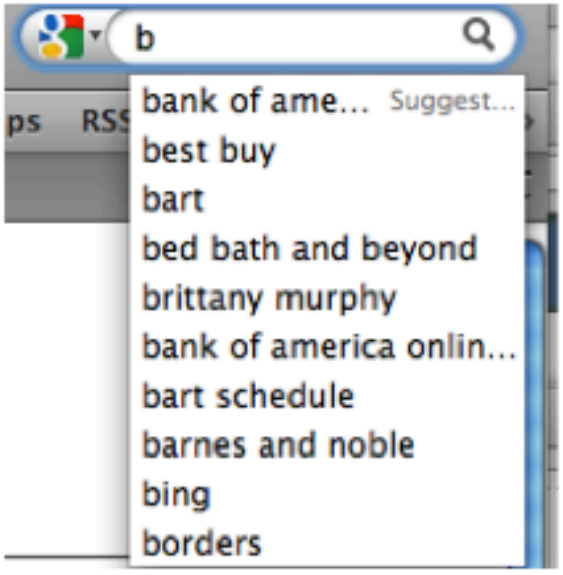

side
sidereel Suggest...
sidestep
sidebar oakland
sidekick
sidestep.com flights
sideways
sideboard danville
side effects of h1n1 v...
side effects of predni...
sideshow collectibles


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

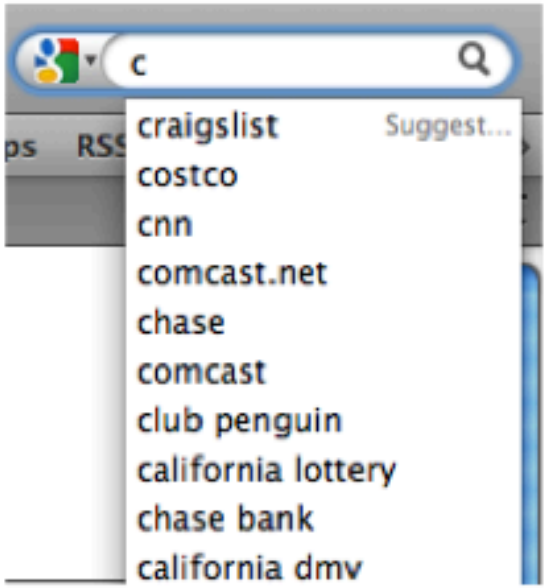

side ch
side chairs Suggest...
side chaining
side chain compression
side chain
side channel attack
side charging ar-15
sidechaining in logic
side chairs contempo...
side charging upper
side chignon




102 chars.

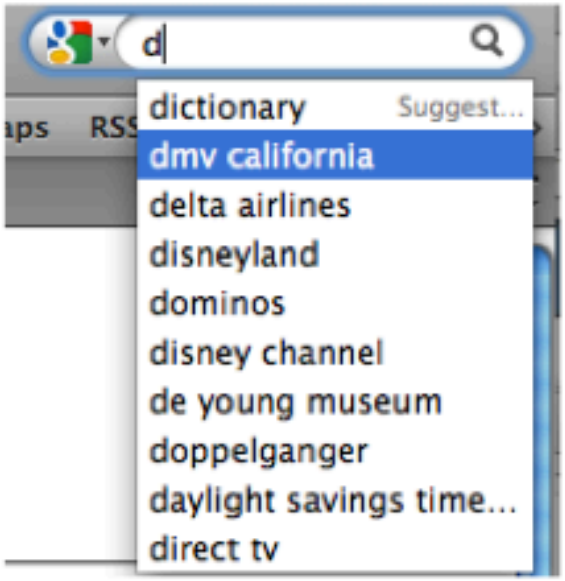



125 chars.

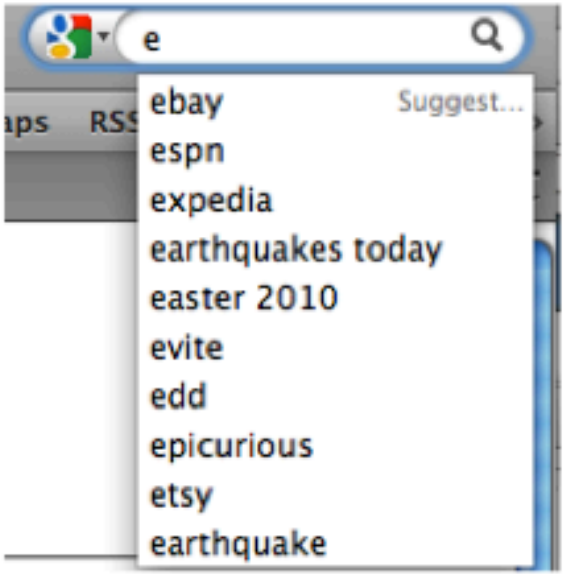



107 chars.

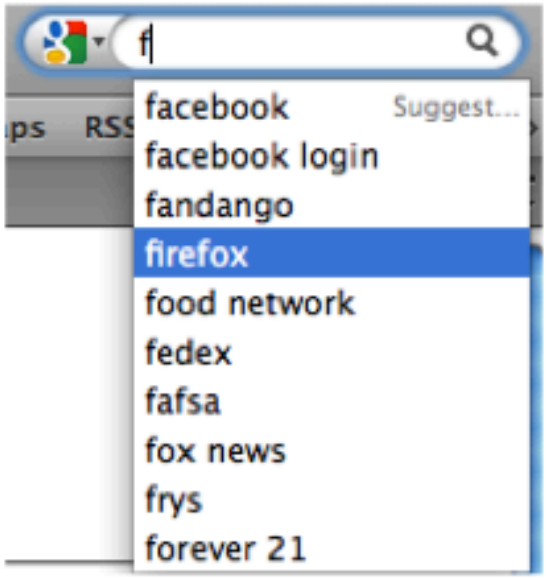
136 chars.




101 chars.




102 chars.



# Other examples of timing attacks

modular exponentiation: m = c^d mod n (d is k bits)

```
m = 1
for i = 0 ... k-1:
    if d(i) = 1:
        m = c*m mod n (might be slow b/c modular reduction)
    m = m^2 mod n
```

Running time leaks Hamming weight (the number of 1's) of private key!

# How to turn into a full attack?

- Suppose attacker can cause victim to decrypt arbitrary ciphertexts and time them.
  (e.g., TLS RSA key exchange mode)
  1. Choose test decryption ciphertexts c_1, ..., c_R, decryption times t_1, ..., t_R
  2. Iteratively guess bits of d
  3. Variance of decryption times decreases linearly if guess correctly.

# Timing Analysis of Keystrokes and Timing Attacks on SSH

- 2001: Song, Wagner, Tian
- Observation: Interactive SSH -- individual keystrokes sent in separate packets

1. Build model of inter-keystroke delays by finger, key pair
2. Measure packet timing off network, apply model to find most likely combinations

# Cache Timing Attacks

- Example: "s-boxes" (map byte->byte, implemented as lookup table)
- faster to look up nearby array values (table loaded into L1 cache)
  - if value far away or page evicted:
    - cache miss, extra time
    - info to attacker about sequence of addresses (leaks key or ciphertext)
- Bernstein 2005: remote cache-timing attacks on AES
- Zhang Juels Reiter Ristenpart 2012: cross-VM cache-timing attacks

# Power Analysis Attacks

- simple power analysis: plot power consumption over time
- differential power analysis: statistical correlations between many power traces

# Memory Remanence

- Gutman 1996: hard drives require multiple passes to secure erase data
  - inexact positioning - magnetic tracks of old writes
  - "overwrite 7 times" -- questionable advice
  - SSD story more complicated (see forensics lecture)
- SRAM: Static RAM
  - "burn in" phenomenon: tends to flip bit to "remembered" state
- DRAM: Cold Boot Attack

# 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.).