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

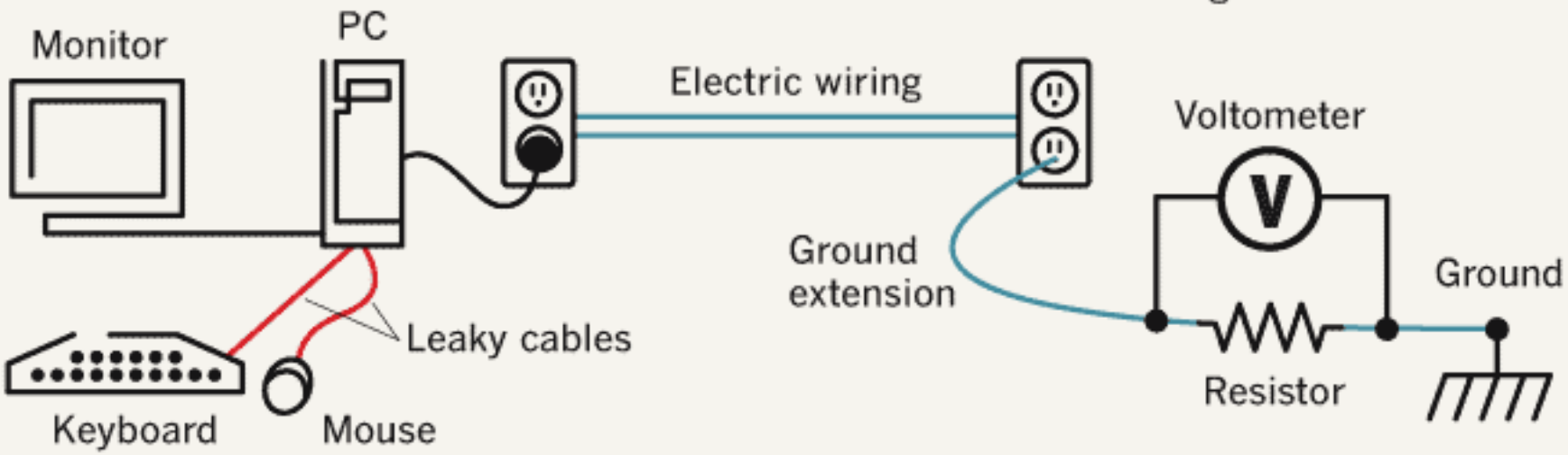
Stealing keystrokes through electric lines

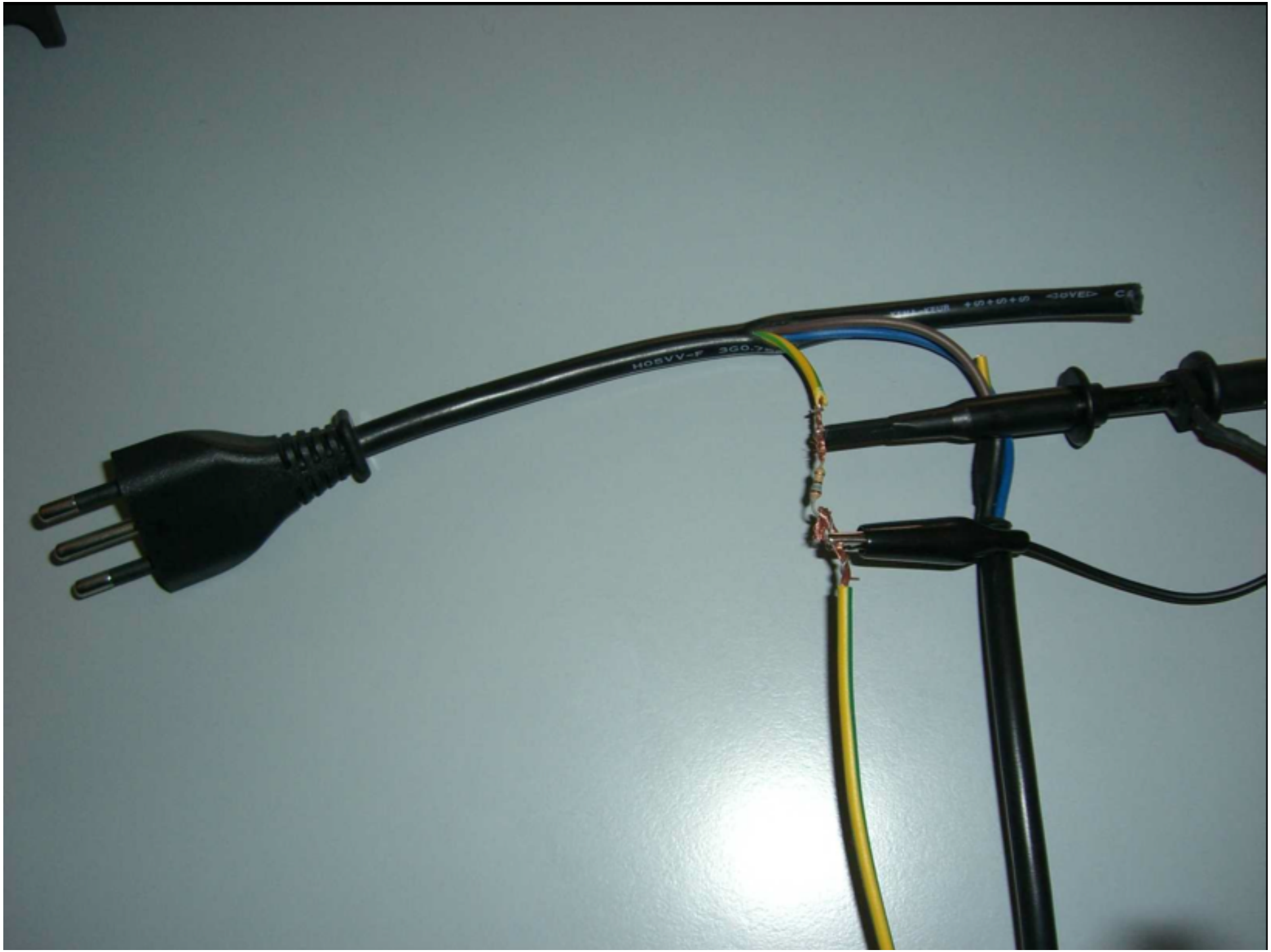
Relatively simple equipment can tap power lines to intercept what is being typed on nearby keyboards.

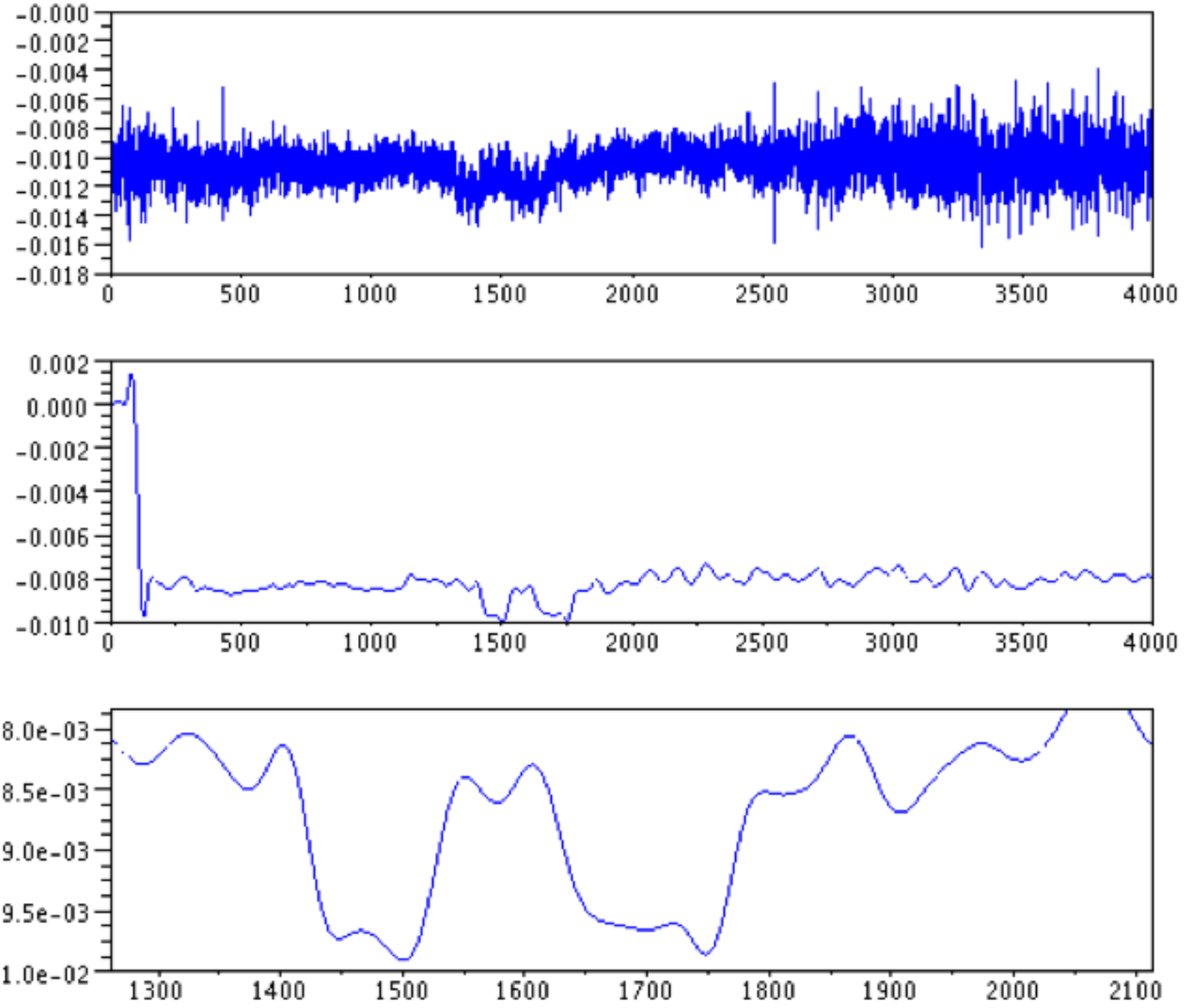
1. Unshielded wires in keyboard cables leak keystroke signals into the cable ground.

2. The signals continue along the ground wire of the electrical service feeding the PC.

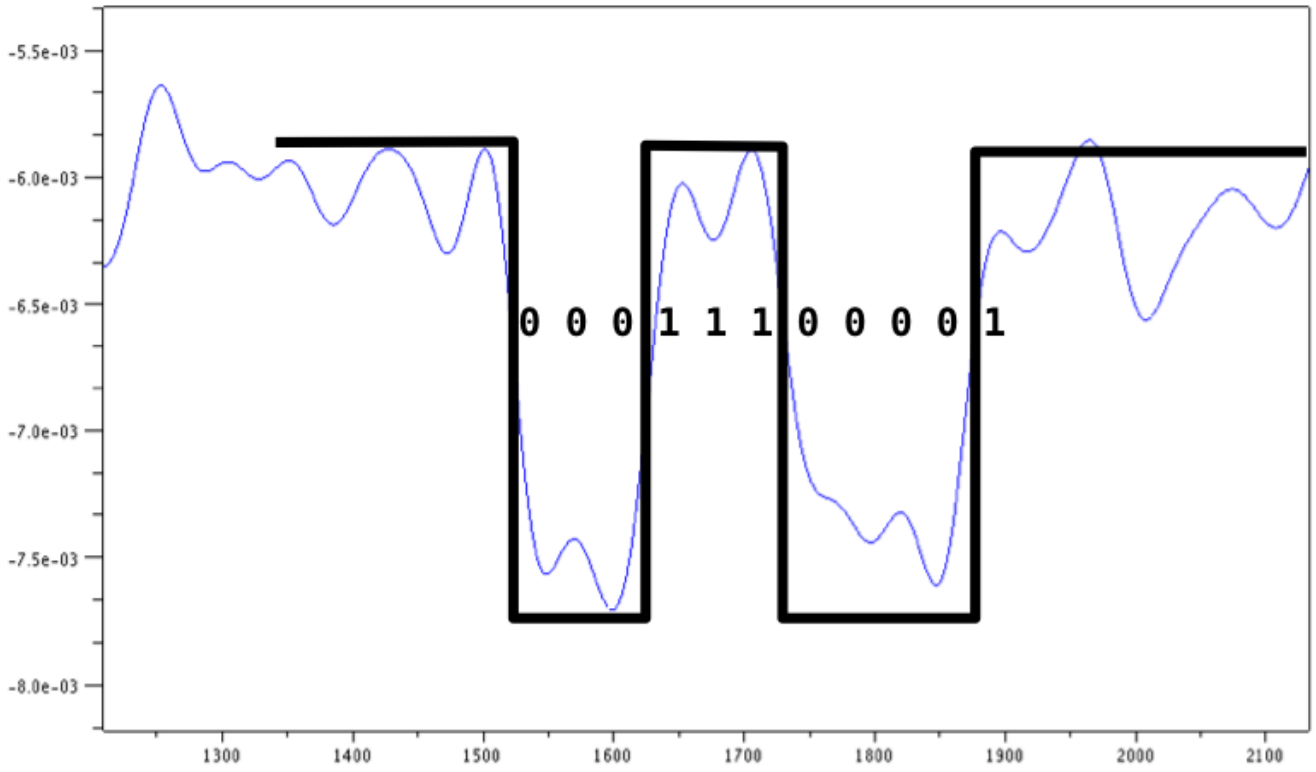
3. Measuring voltage shifts across an extension of the electric-system ground reveals what keys are being struck.




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

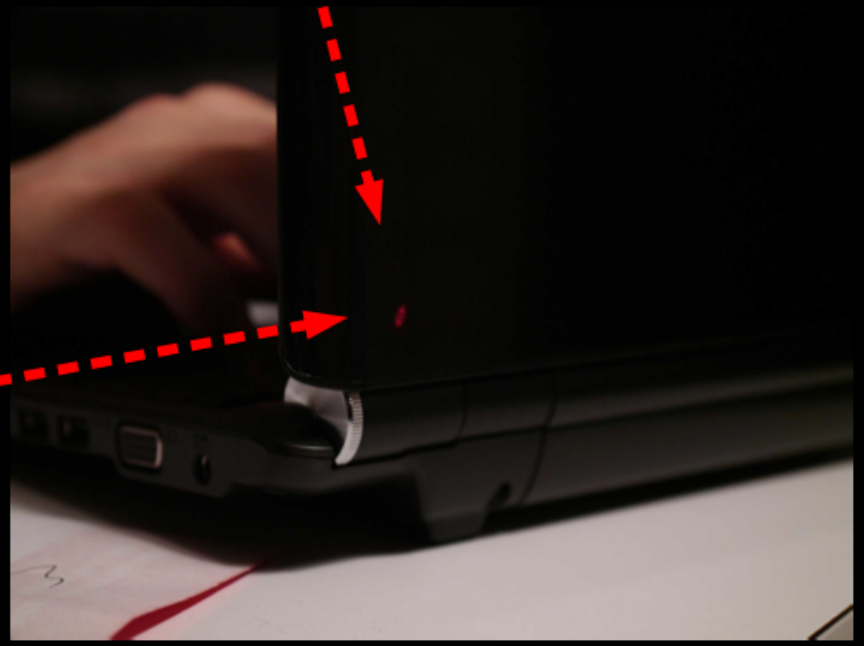
- | **0** | **00111000** | **0** | **1** | = letter 'a'



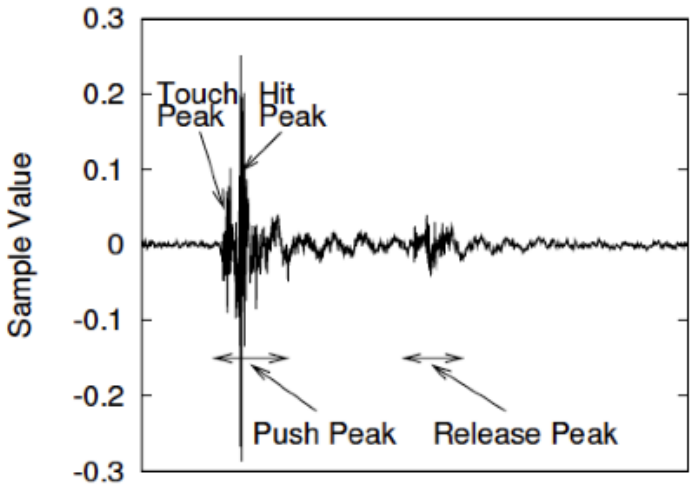
UI Side Channel Snooping

- 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” from a distance using laser + telescope!

Reflective Plastic Case



PWNED!



Sniffing Keystrokes With Lasers/Voltmeters

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.

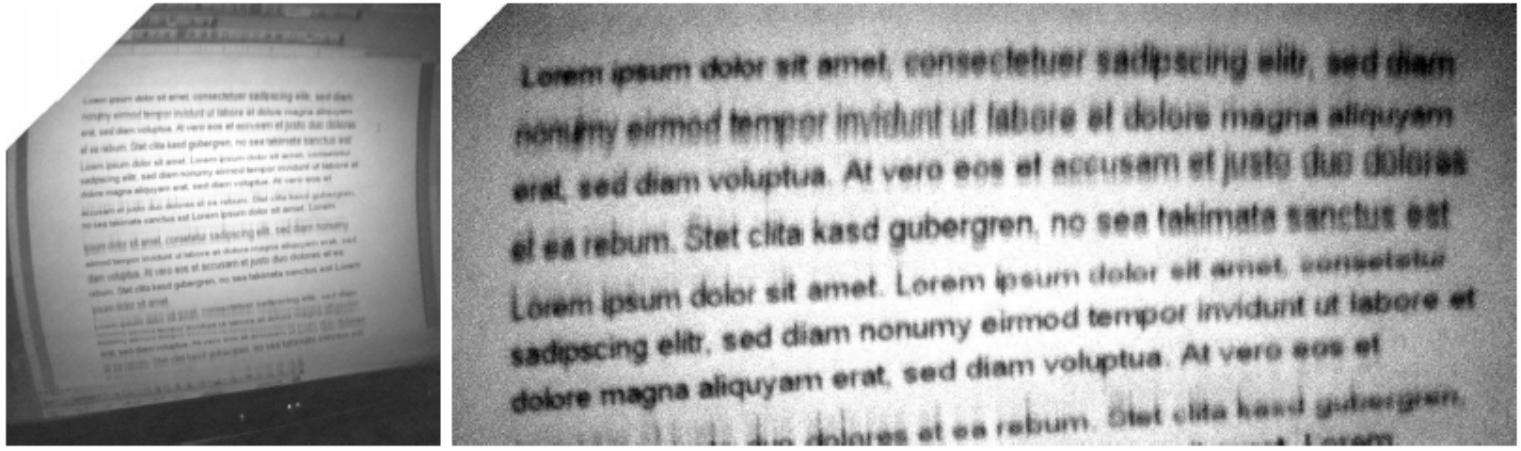


Figure 7. Reflection of a Word document with small 12pt font size in a tea pot, taken from a distance of 5m. The 12pt font is readable from the reflection.

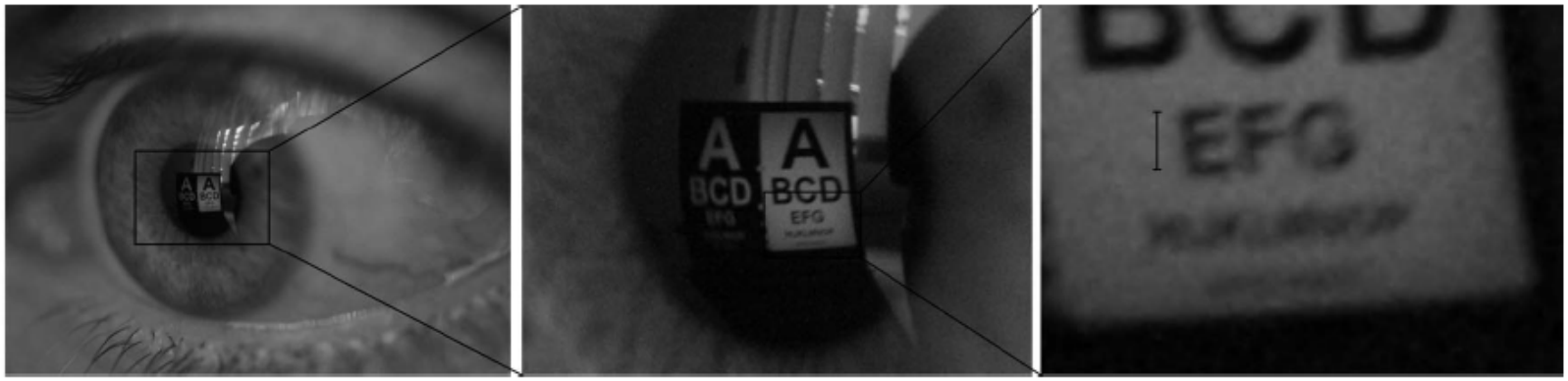


Figure 9. Image taken with a macro lens from very short distance, with realistic distance between the monitor and the eye. Readability is limited by the resolution of the camera.

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.