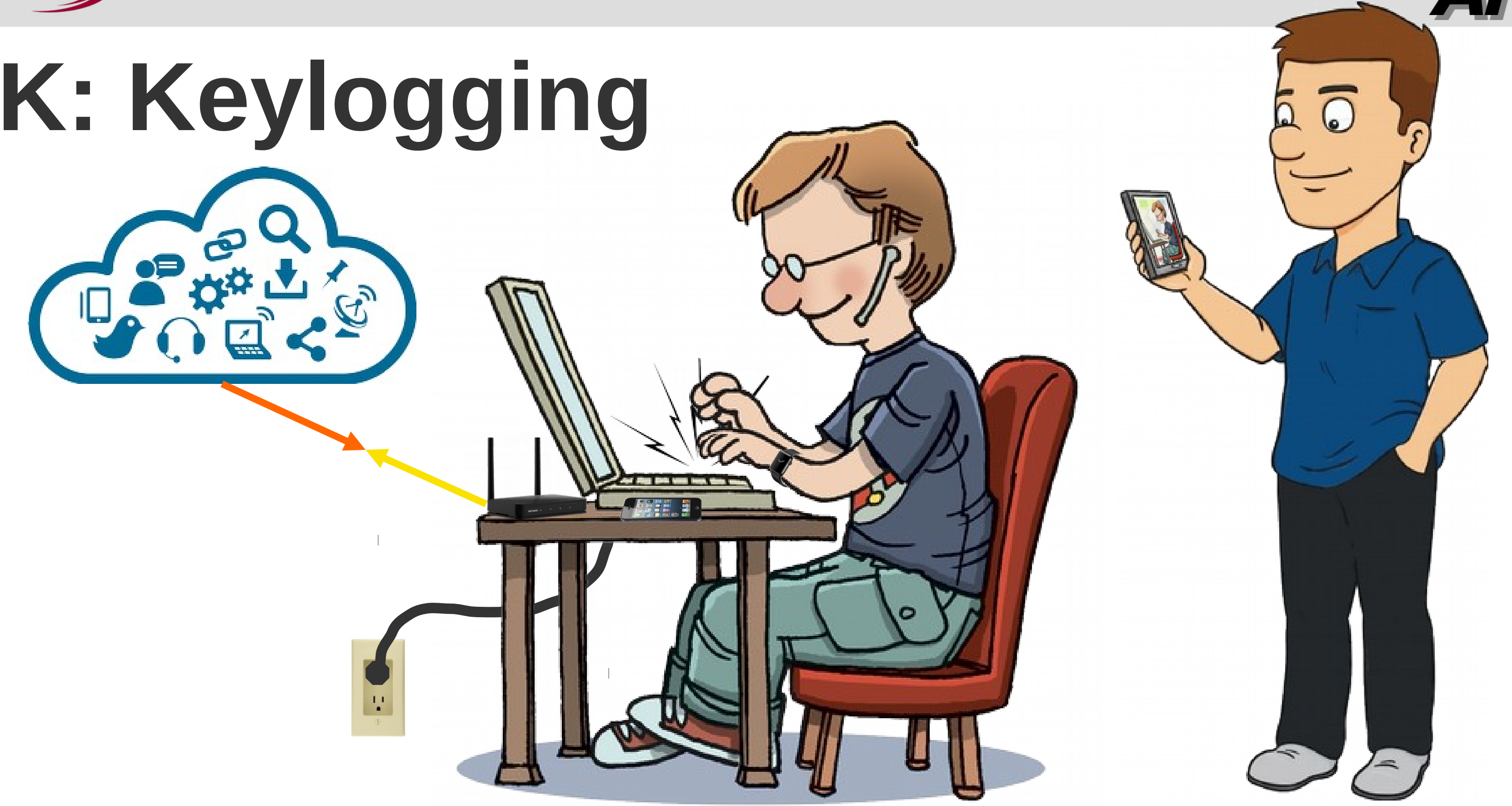
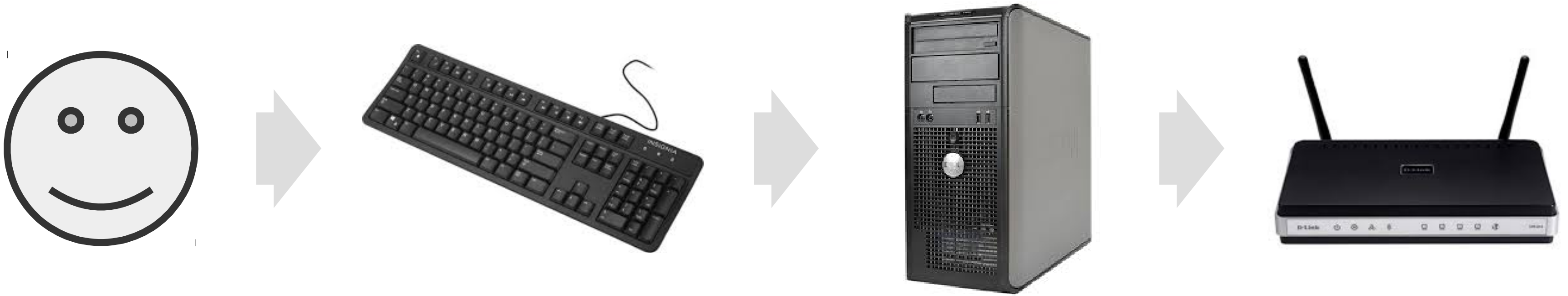
SoK: Keylogging Side Channels



John “Vinnie” Monaco / U.S. Army Research Laboratory

What’s in a keystroke?



User

+ Hand motion
+ Key travel

Keyboard

+ Matrix scan
+ Debouncing
+ Encoding

Host

+ USB polling
+ Process scheduling

Network

+ Transmission
+ Routing

Keylogging metrics

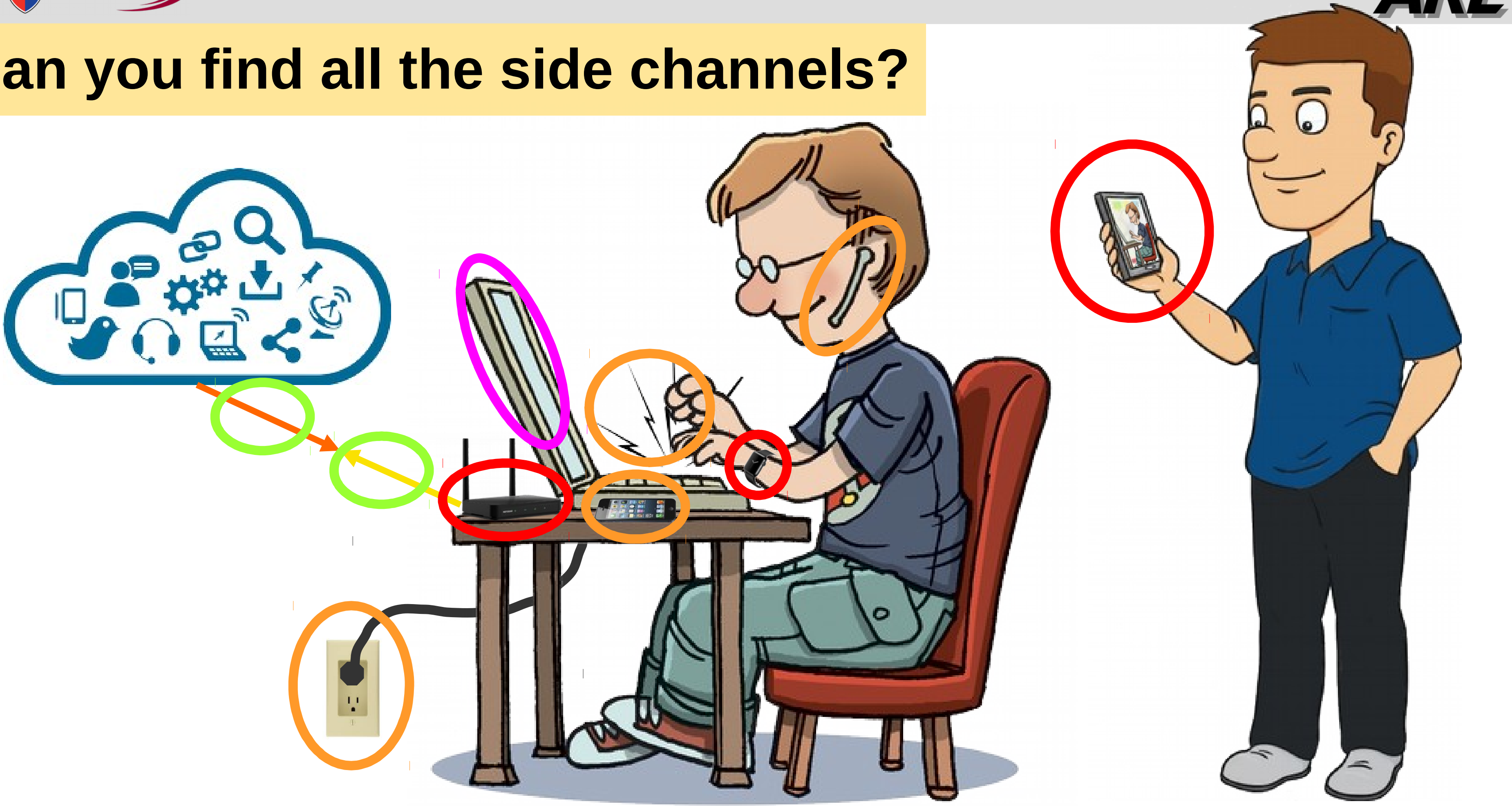
- **Detection**
  - Establish the presence/absence of a keystroke
  - Precision/recall, ROC analysis
- **Identification**
  - Determine which keyboard key was pressed
  - Information gain, classification accuracy

Early attacks

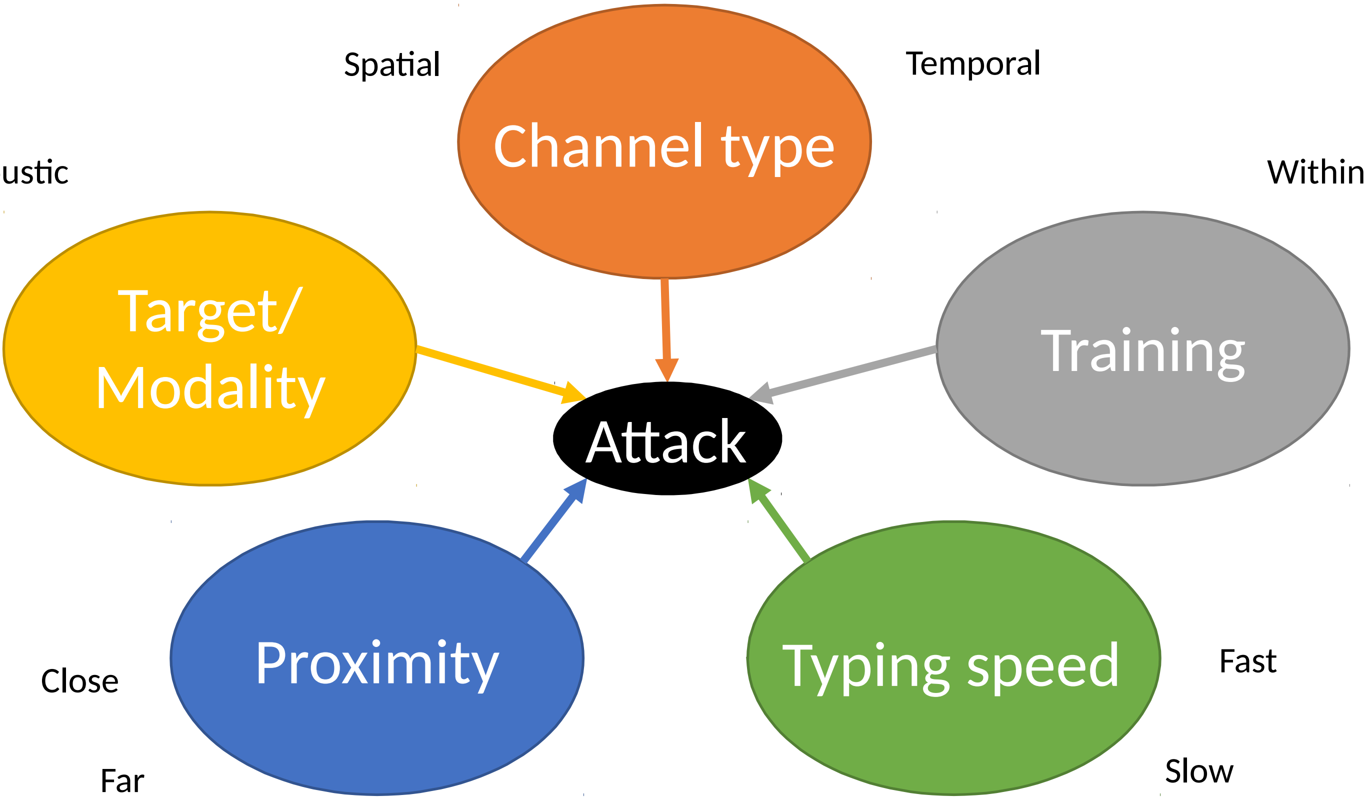
1943
TEMPEST

1984
Project GUNMAN

Can you find all the side channels?



Attack taxonomy



Spatial

Temporal

Acoustic

Electromagnetic

CPU

Cache

Within-subject

Between-subject

None

Close

Far

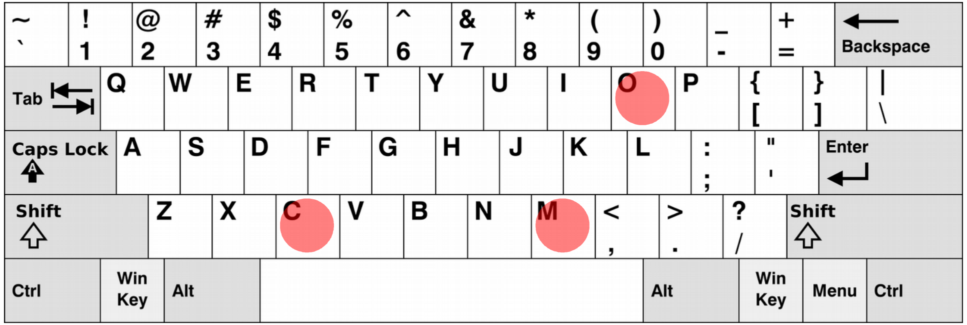
Fast

Slow

Spatial side channels

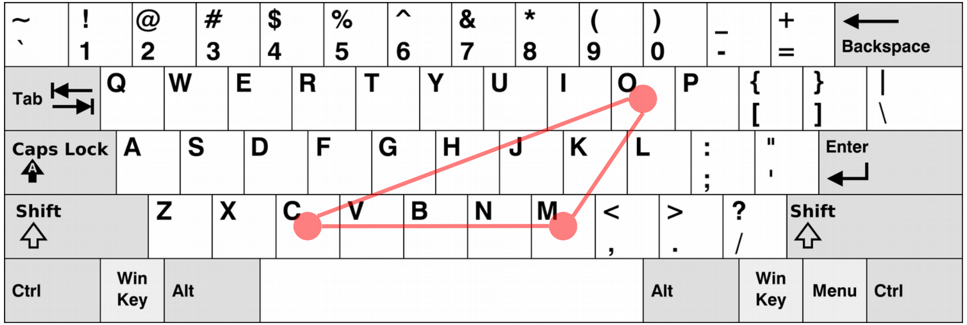
First order

Key locations

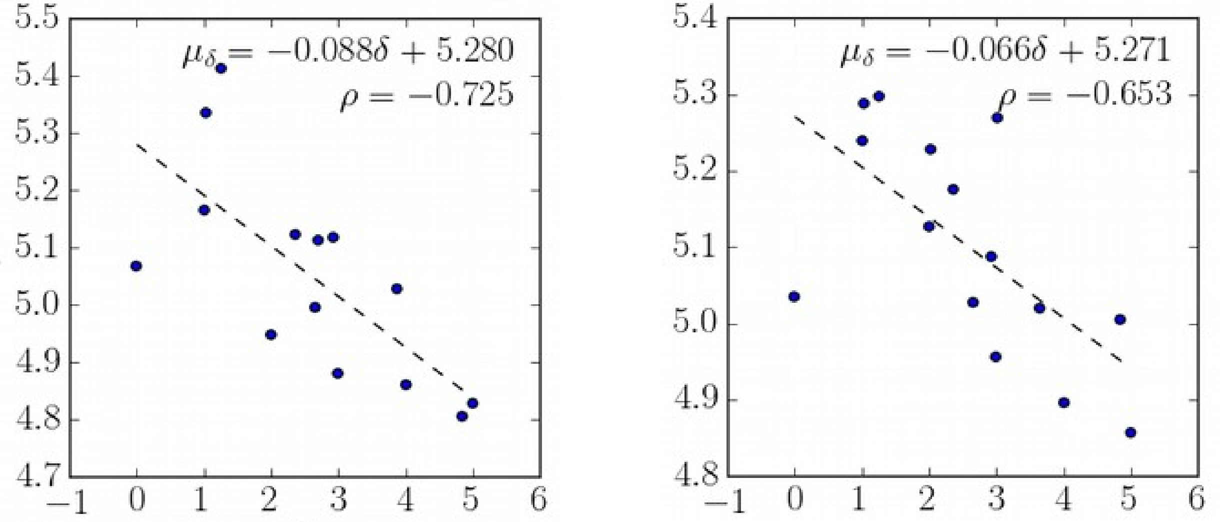

~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + = Backspace
Tab Q W E R T Y U I O P { [}] | \
Caps Lock A S D F G H J K L : ; " ' Enter
Shift Z X C V B N M < , > . ? / Shift
Ctrl Win Key Alt Alt Win Key Menu Ctrl

Second order

Key distances


~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + = Backspace
Tab Q W E R T Y U I O P { [}] | \
Caps Lock A S D F G H J K L : ; " ' Enter
Shift Z X C V B N M < , > . ? / Shift
Ctrl Win Key Alt Alt Win Key Menu Ctrl

Temporal side channels


User A

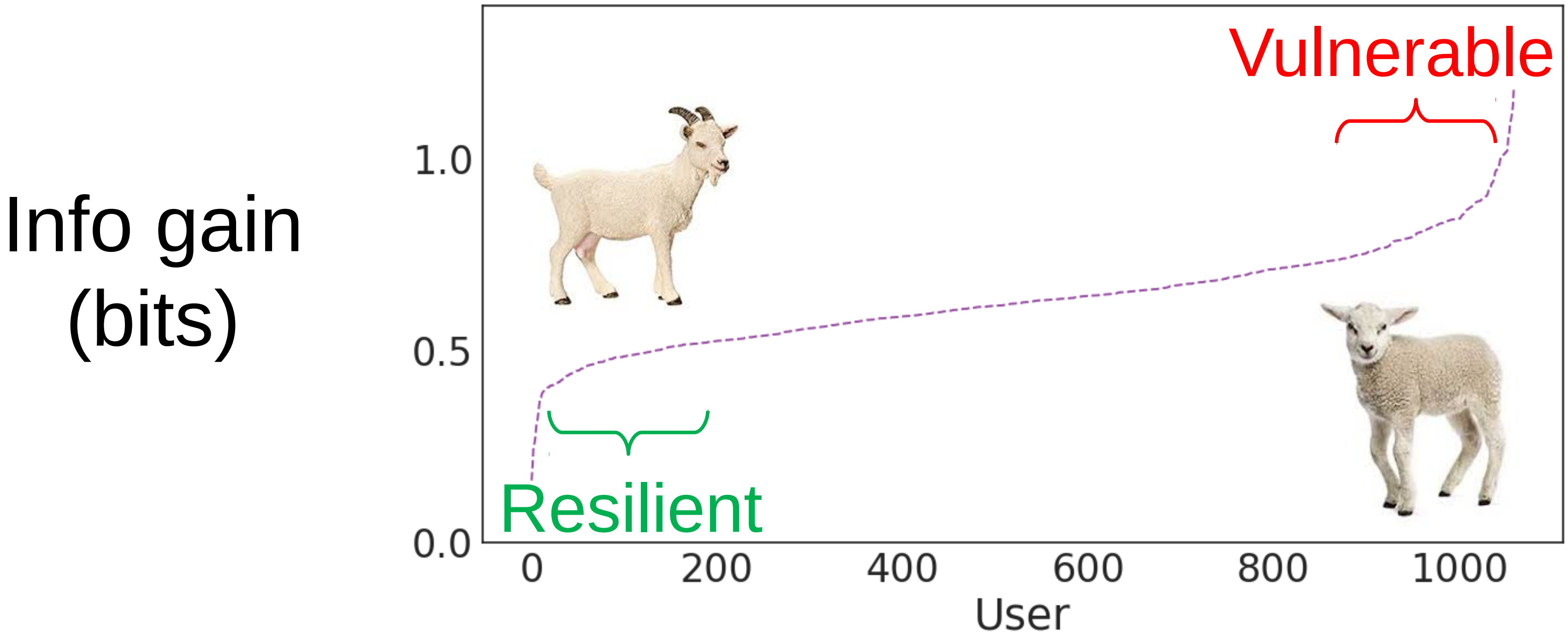
User B

Key-press latency

Inter-key distance

The “side channel menagerie”

A phenomenon reminiscent of the *biometric menagerie*



Homogeneity as an **indicator** for side channel attack **severity**

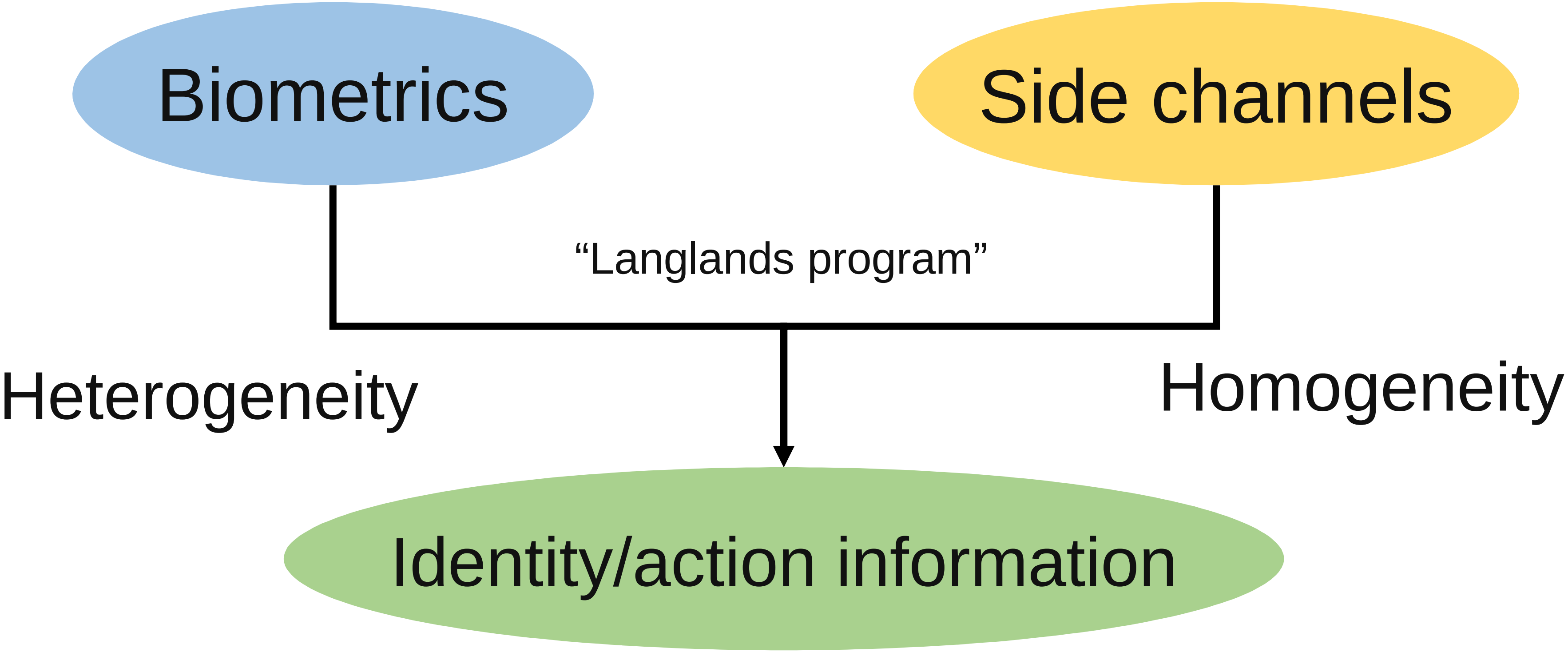
Very similar

High risk

Somewhat similar

Medium risk

Linking two fields


Biometrics

Side channels

“Langlands program”

Heterogeneity

Homogeneity

Identity/action information

Summary/prediction

- 75 years of keylogging side channels
- Behavior **heterogeneity** vs **homogeneity**
- Temporal attacks will improve

Contact:

www.vmonaco.com