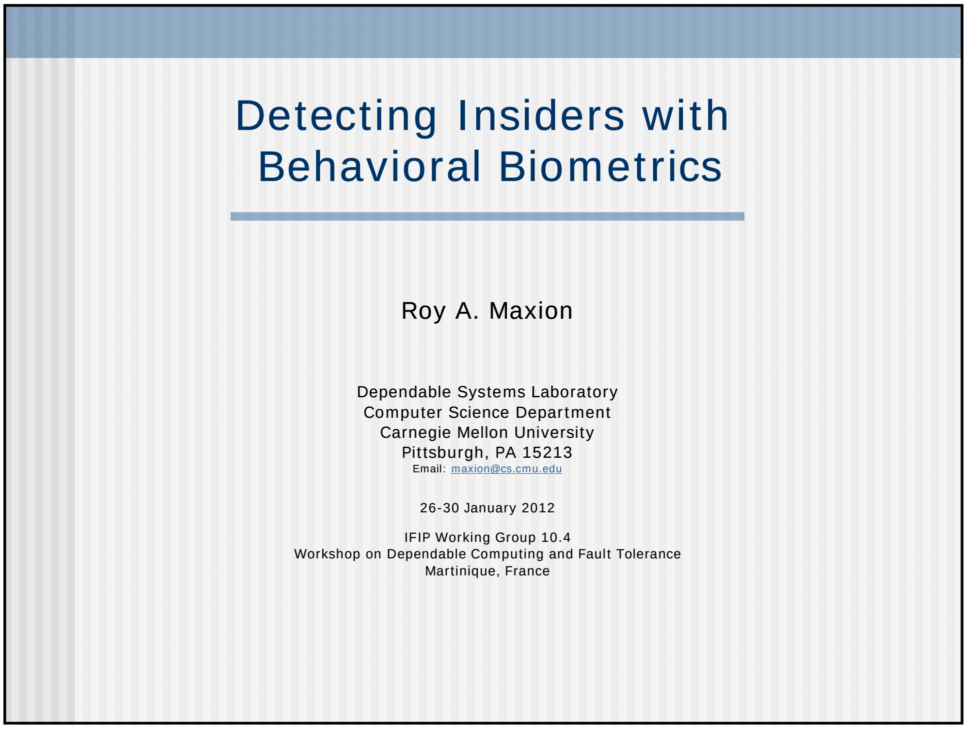


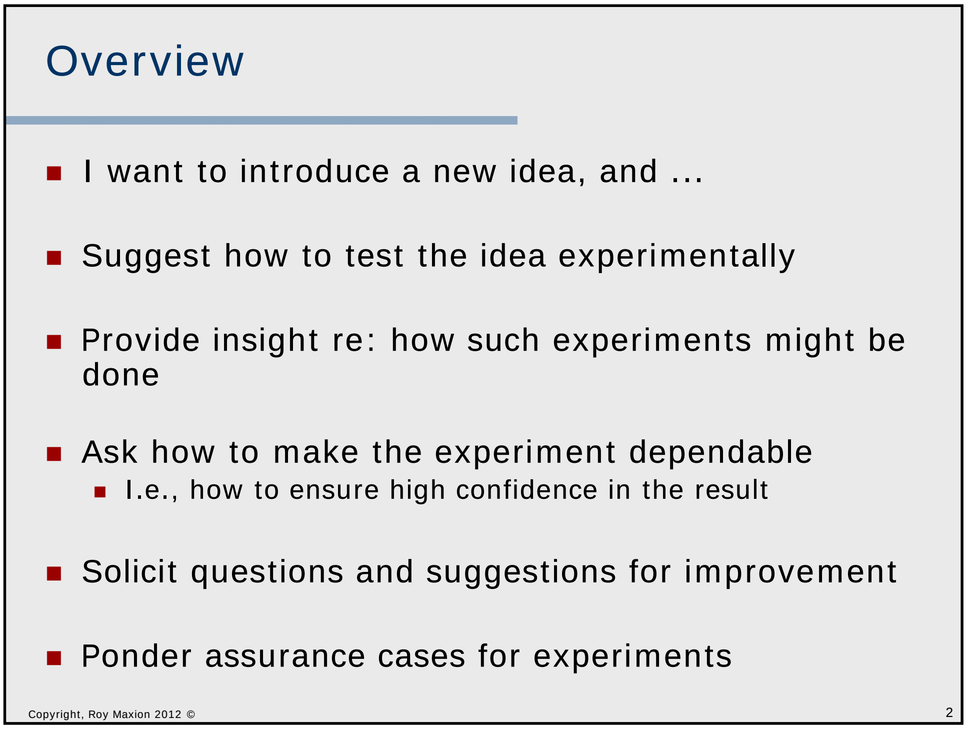
Detecting Insiders with Behavioral Biometrics

Roy A. Maxion

Dependable Systems Laboratory
Computer Science Department
Carnegie Mellon University
Pittsburgh, PA 15213
Email: maxion@cs.cmu.edu

26-30 January 2012

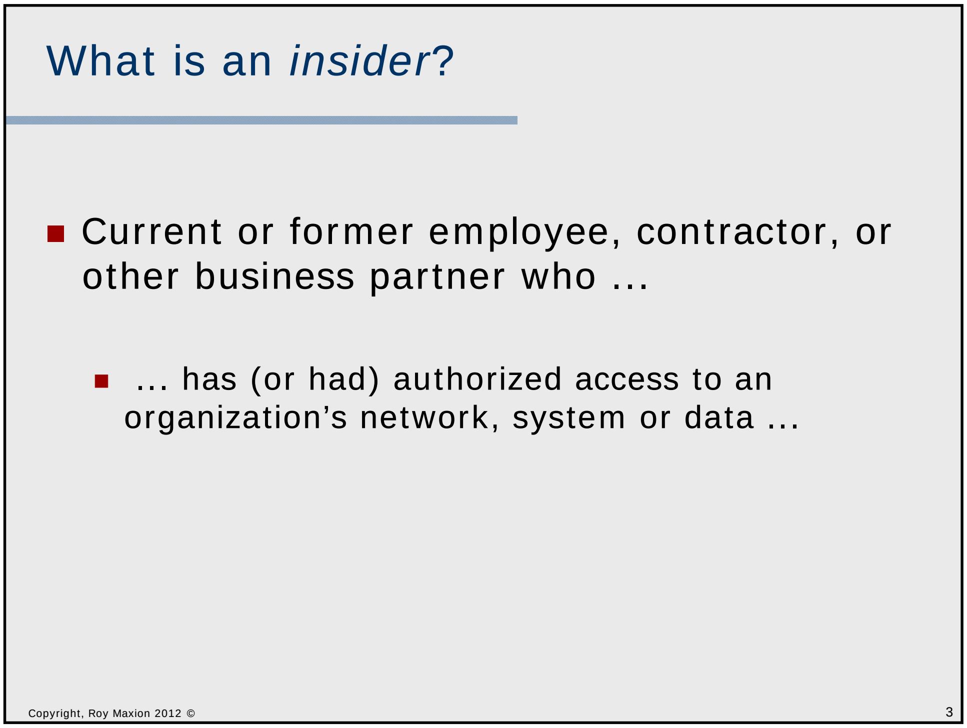
IFIP Working Group 10.4
Workshop on Dependable Computing and Fault Tolerance
Martinique, France



Overview

- I want to introduce a new idea, and ...
- Suggest how to test the idea experimentally
- Provide insight re: how such experiments might be done
- Ask how to make the experiment dependable
  - I.e., how to ensure high confidence in the result
- Solicit questions and suggestions for improvement
- Ponder assurance cases for experiments

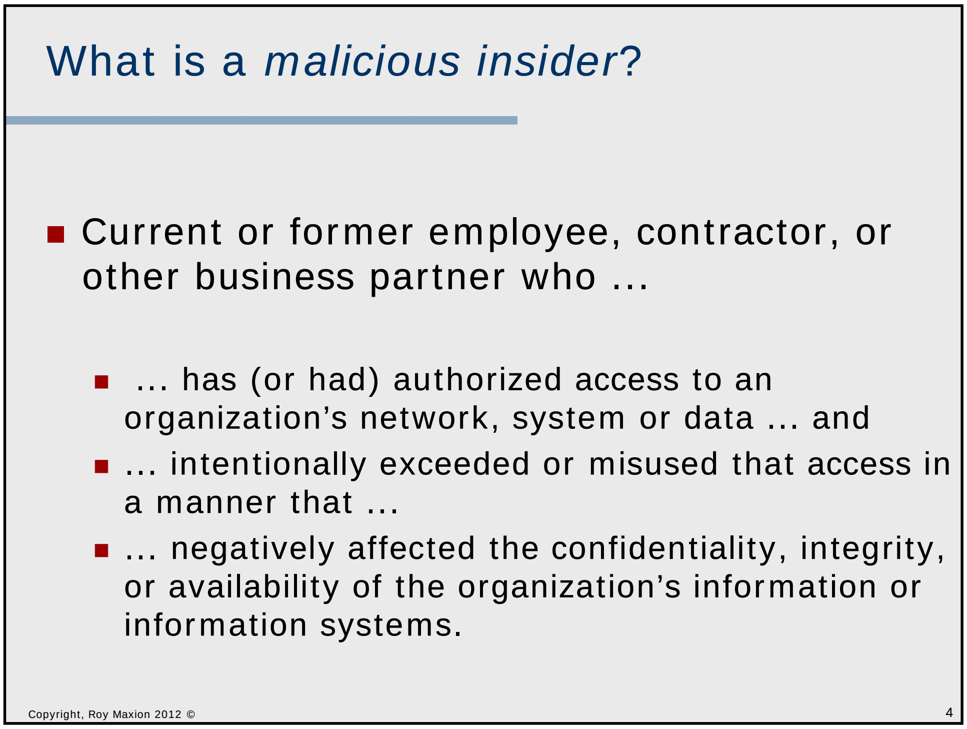
Copyright, Roy Maxion 2012 ©



What is an *insider*?

- Current or former employee, contractor, or other business partner who …
  - … has (or had) authorized access to an organization’s network, system or data …

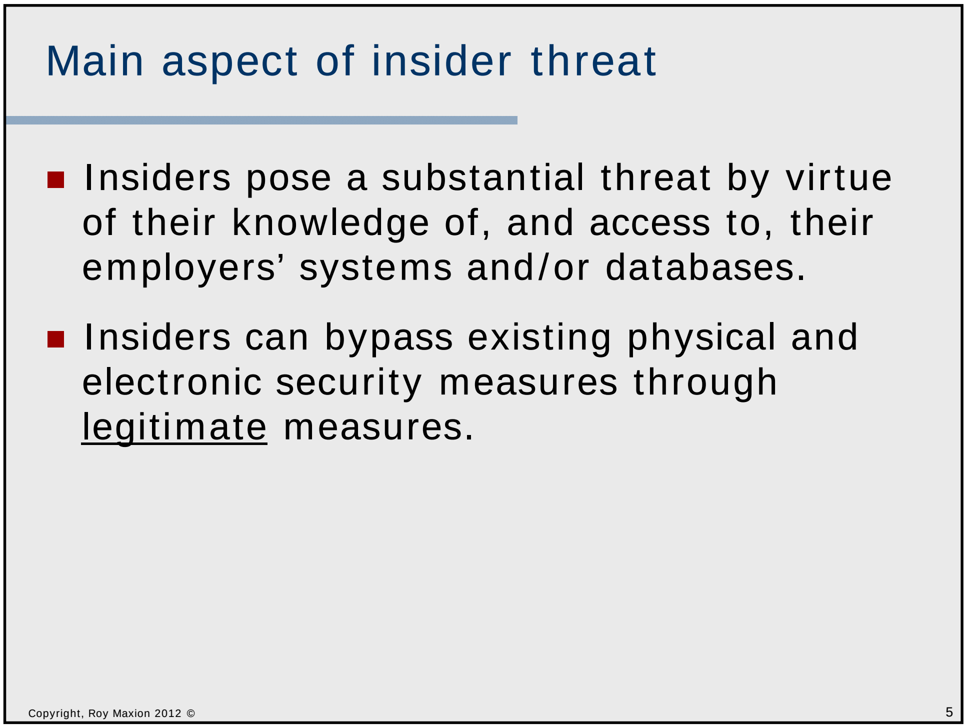
Copyright, Roy Maxion 2012 ©



What is a *malicious insider*?

- Current or former employee, contractor, or other business partner who …
  - … has (or had) authorized access to an organization’s network, system or data … and
  - … intentionally exceeded or misused that access in a manner that …
  - … negatively affected the confidentiality, integrity, or availability of the organization’s information or information systems.

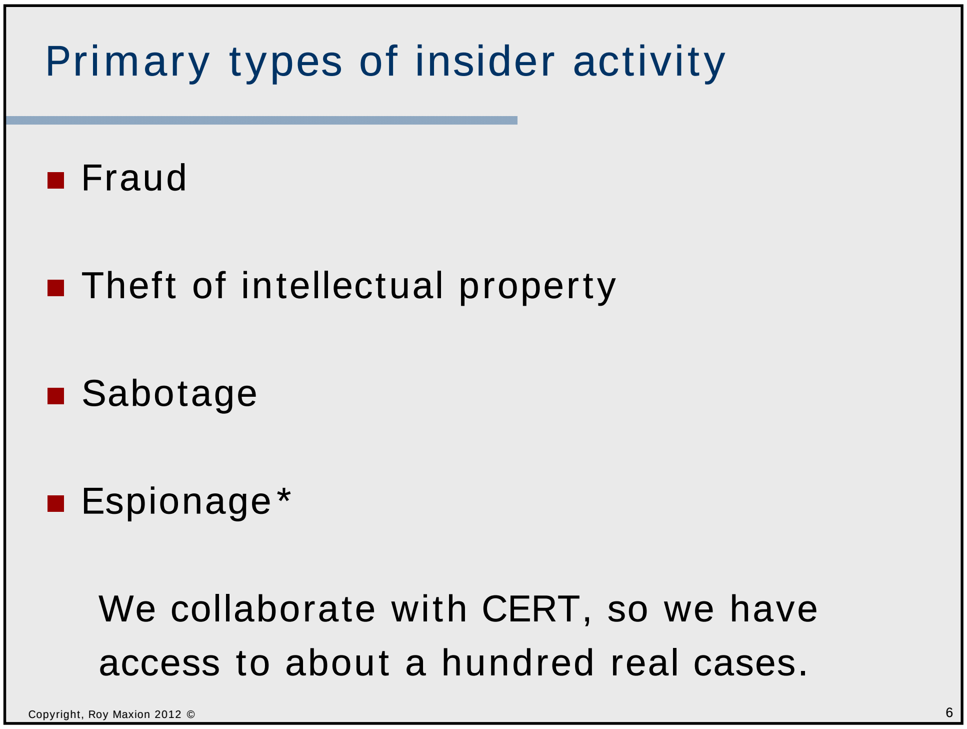
Copyright, Roy Maxion 2012 ©



Main aspect of insider threat

- Insiders pose a substantial threat by virtue of their knowledge of, and access to, their employers' systems and/or databases.
- Insiders can bypass existing physical and electronic security measures through <u>legitimate</u> measures.

Copyright, Roy Maxion 2012 ©

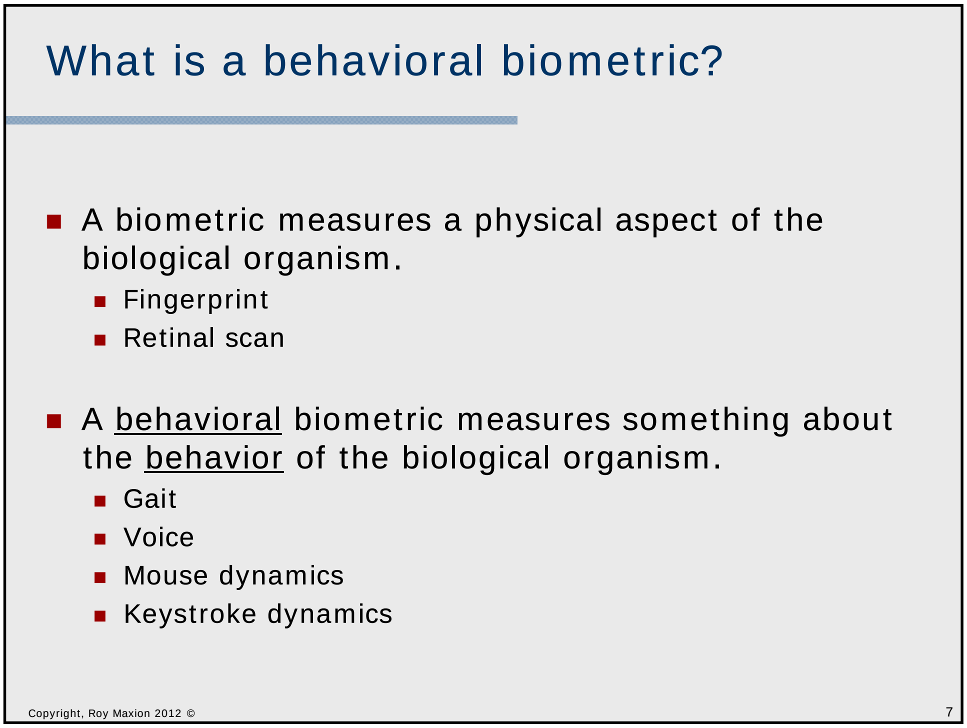


Primary types of insider activity

- Fraud
- Theft of intellectual property
- Sabotage
- Espionage*

We collaborate with CERT, so we have access to about a hundred real cases.

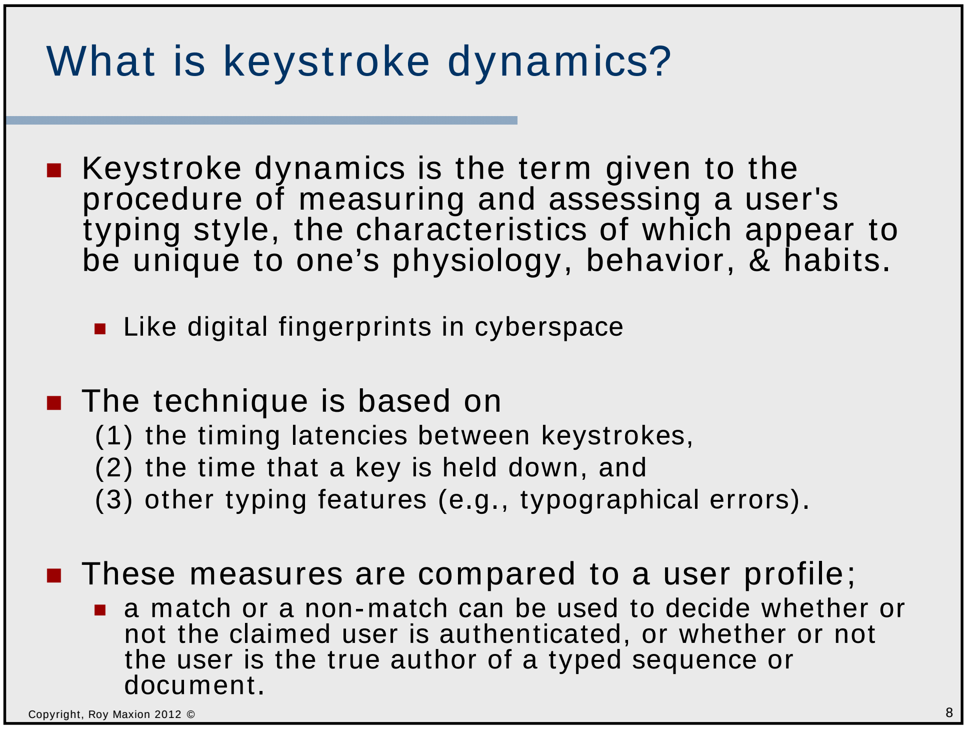
Copyright, Roy Maxion 2012 ©



What is a behavioral biometric?

- A biometric measures a physical aspect of the biological organism.
  - Fingerprint
  - Retinal scan
- A behavioral biometric measures something about the behavior of the biological organism.
  - Gait
  - Voice
  - Mouse dynamics
  - Keystroke dynamics

Copyright, Roy Maxion 2012 ©

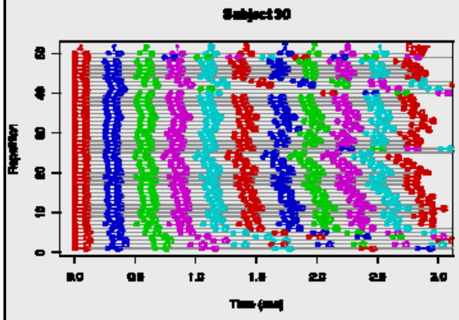


What is keystroke dynamics?

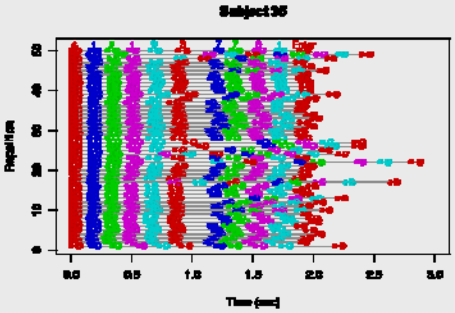
- Keystroke dynamics is the term given to the procedure of measuring and assessing a user's typing style, the characteristics of which appear to be unique to one’s physiology, behavior, & habits.
  - Like digital fingerprints in cyberspace
- The technique is based on
  (1) the timing latencies between keystrokes,
  (2) the time that a key is held down, and
  (3) other typing features (e.g., typographical errors).
- These measures are compared to a user profile;
  - a match or a non-match can be used to decide whether or not the claimed user is authenticated, or whether or not the user is the true author of a typed sequence or document.

Copyright, Roy Maxion 2012 ©

Compare: differences between two typists



Times between keystrokes are spread out and reasonably even.



Times between keystrokes are tighter and more consistent.

Two different users typed the passcode 412 193 7761 50 times each.
Their typing patterns are remarkably different and unique.

Closed circles on the timeline indicate key-down events; open circles represent key-up events.

Copyright, Roy Maxion 2012 ©

Results

Metric	Achieved	Target
Hits	**99.97%**	**99.999%**
Misses	**.03%**	**.001%**
False alarms	**1.51%**	**1.000%**
EER	**1.00%**	**.001%**

Task: Single-finger, 10-digits

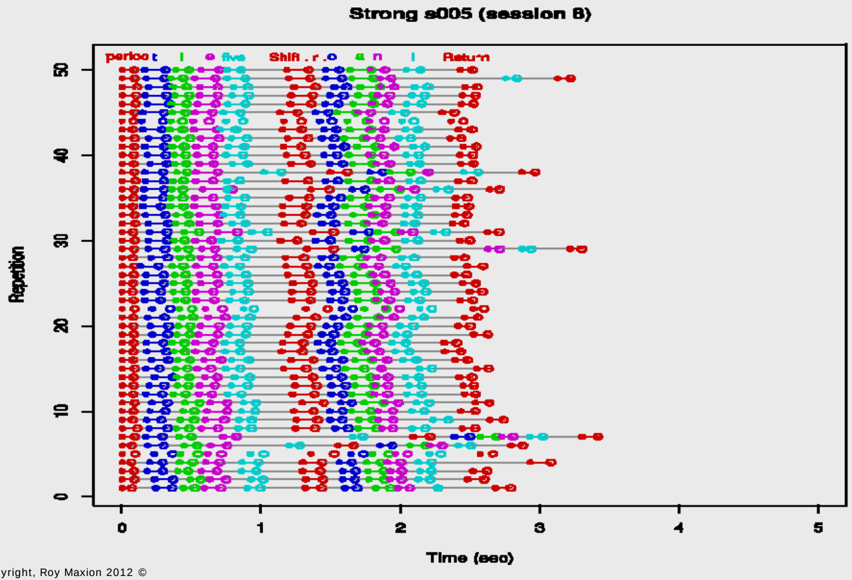
Copyright, Roy Maxion 2012 ©

But one day in the lab …

- We noticed something odd
- We'd been leafing through a stack of experiment results …
- … which looked mostly like this …

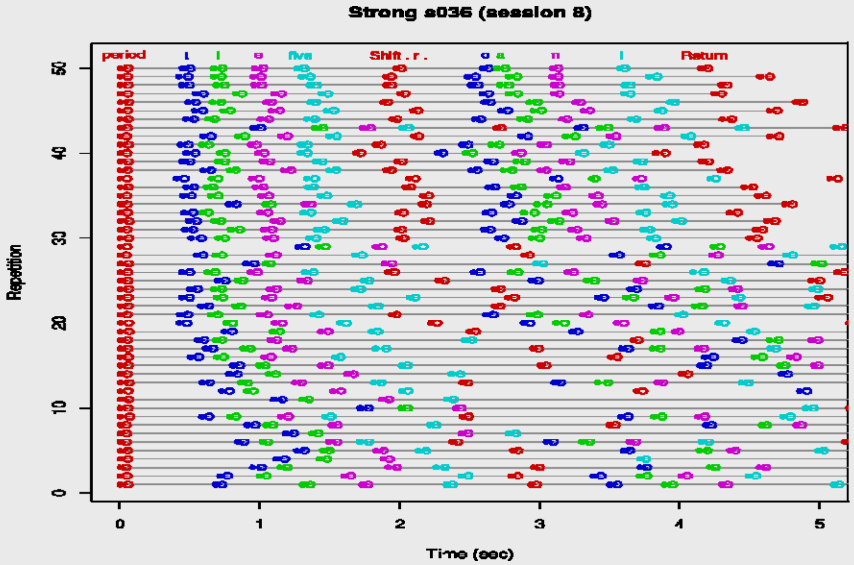
Copyright, Roy Maxion 2012 ©

Subject 005



Copyright, Roy Maxion 2012 ©

But not like this: Subject 036 – Yow!

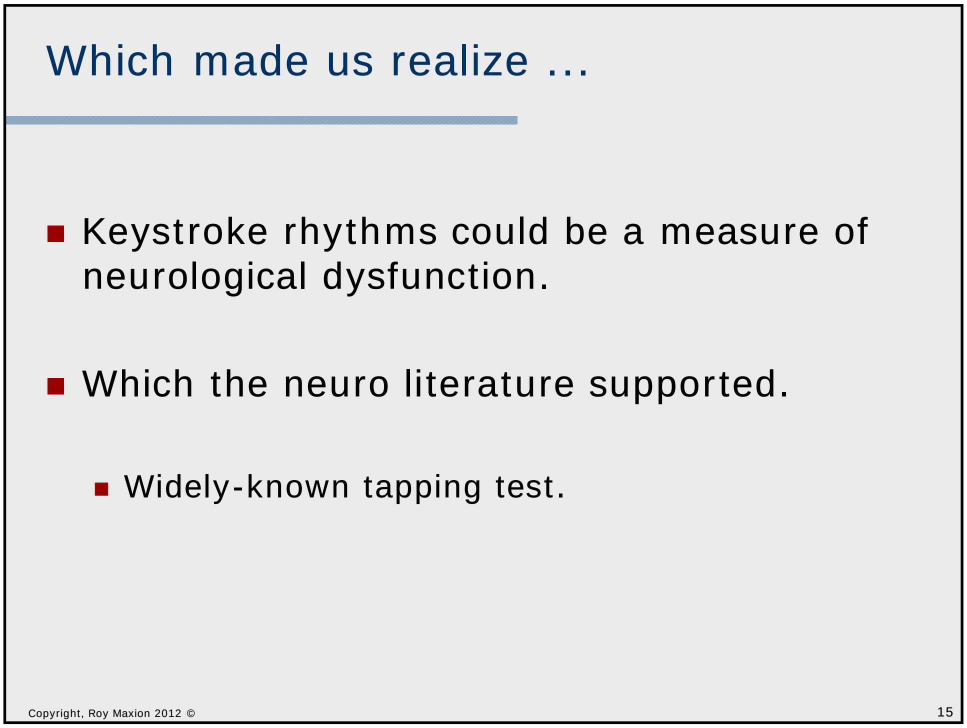


Copyright, Roy Maxion 2012 ©

What made S036's behavior so strange?

- Looked in the logs
- Knew who the subject was
- No reason to think anything was amiss
- Until … the demographic survey revealed …
- The subject suffered from temporal lobe epilepsy

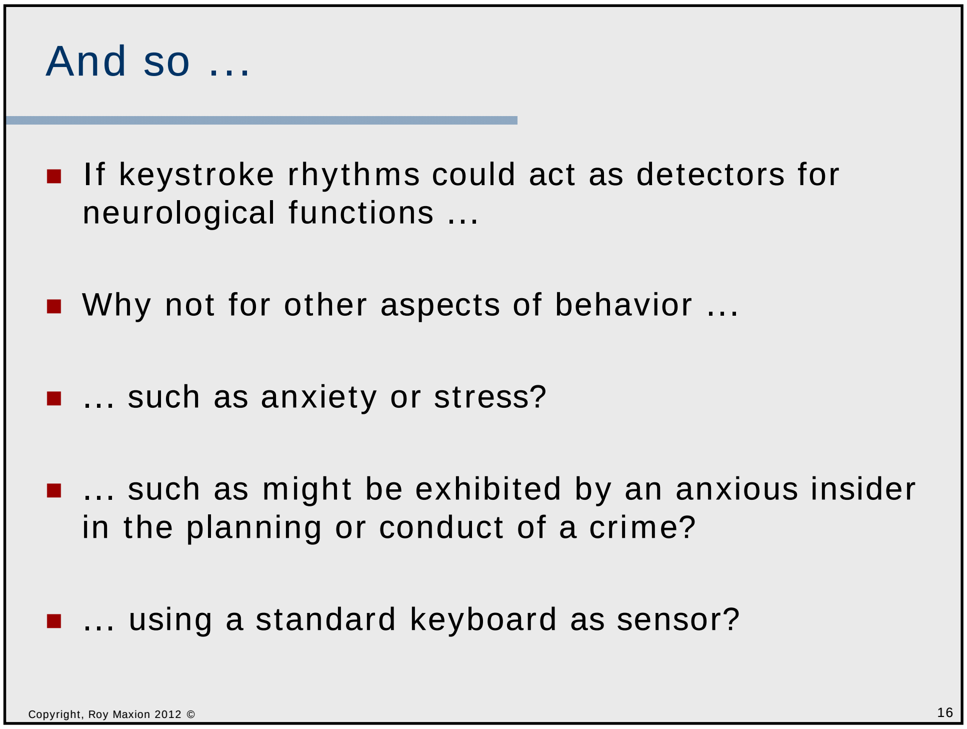
Copyright, Roy Maxion 2012 ©



Which made us realize …

- Keystroke rhythms could be a measure of neurological dysfunction.
- Which the neuro literature supported.
  - Widely-known tapping test.

Copyright, Roy Maxion 2012 ©



And so …

- If keystroke rhythms could act as detectors for neurological functions …
- Why not for other aspects of behavior …
- … such as anxiety or stress?
- … such as might be exhibited by an anxious insider in the planning or conduct of a crime?
- … using a standard keyboard as sensor?

Copyright, Roy Maxion 2012 ©

And then …

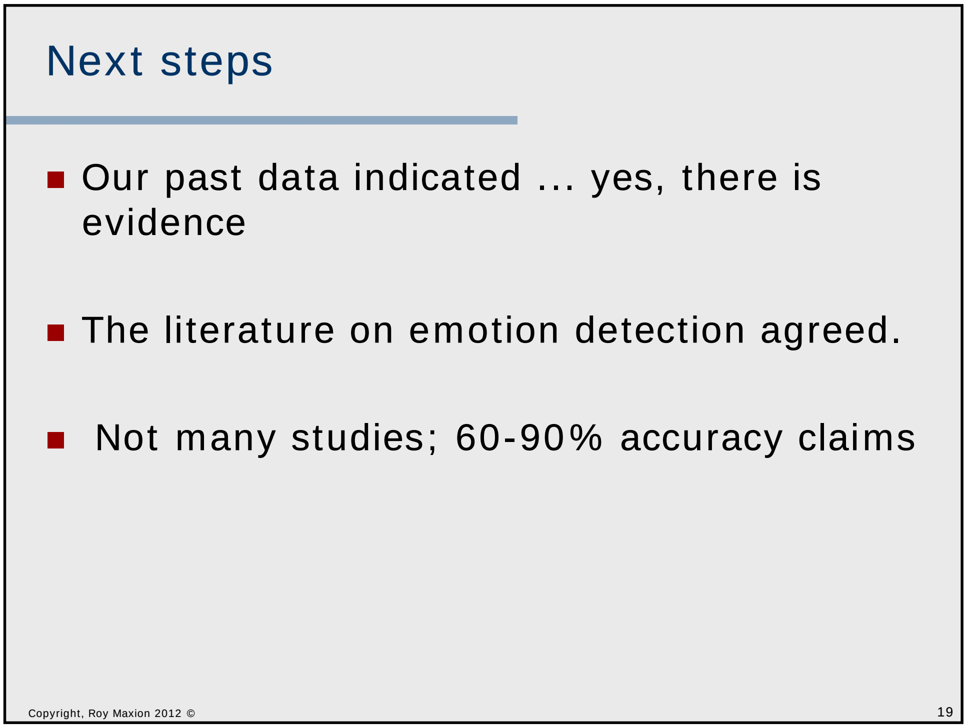
- Such a keyboard-based stress detector could be coupled with systems like Raytheon’s SureView, which already …
  - Monitors 50,000 users
  - Checks their email (e.g., sentiment analysis)
  - Checks their data access and transfers
  - Checks their hours
  - Checks their printing habits
  - Checks various aspects of their <u>behaviors</u>
- … with the goal of catching insiders.

Copyright, Roy Maxion 2012 ©

Of course …

- None of the previously-mentioned behaviors is a completely-reliable indicator of insider activity when used alone.
- But used in concert with one another, convergent evidence builds to the point at which your friendly security officer might explore a few off-line details …
- … and hence be forewarned of malicious activity.

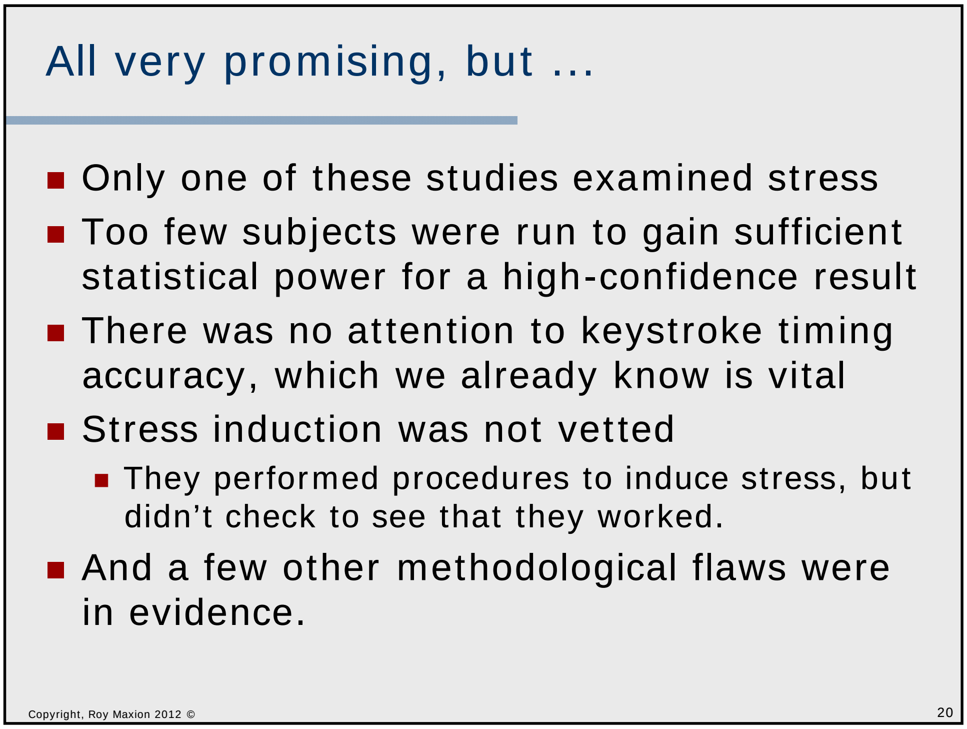
Copyright, Roy Maxion 2012 ©



Next steps

- Our past data indicated … yes, there is evidence
- The literature on emotion detection agreed.
- Not many studies; 60-90% accuracy claims

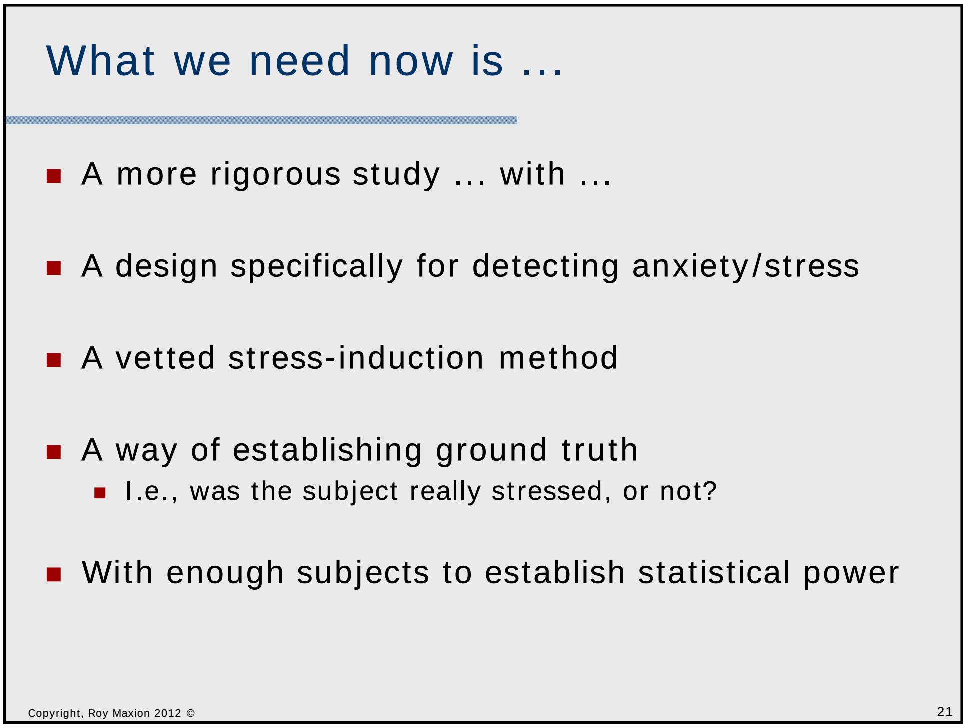
Copyright, Roy Maxion 2012 ©



All very promising, but …

- Only one of these studies examined stress
- Too few subjects were run to gain sufficient statistical power for a high-confidence result
- There was no attention to keystroke timing accuracy, which we already know is vital
- Stress induction was not vetted
  - They performed procedures to induce stress, but didn’t check to see that they worked.
- And a few other methodological flaws were in evidence.

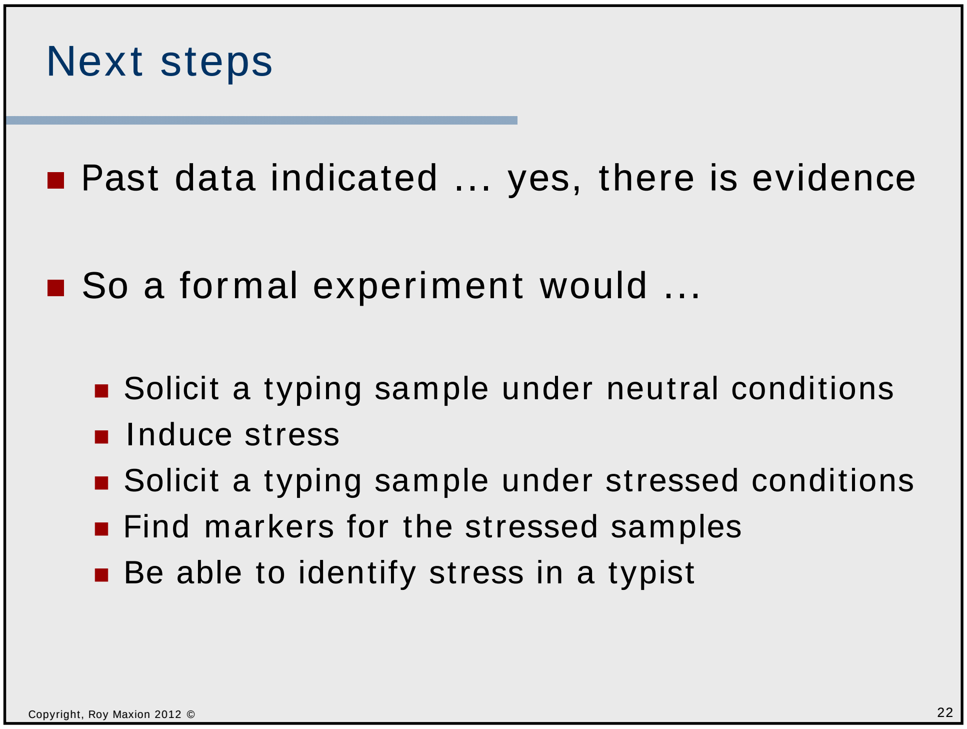
Copyright, Roy Maxion 2012 ©



What we need now is …

- A more rigorous study … with …
- A design specifically for detecting anxiety/stress
- A vetted stress-induction method
- A way of establishing ground truth
  - I.e., was the subject really stressed, or not?
- With enough subjects to establish statistical power

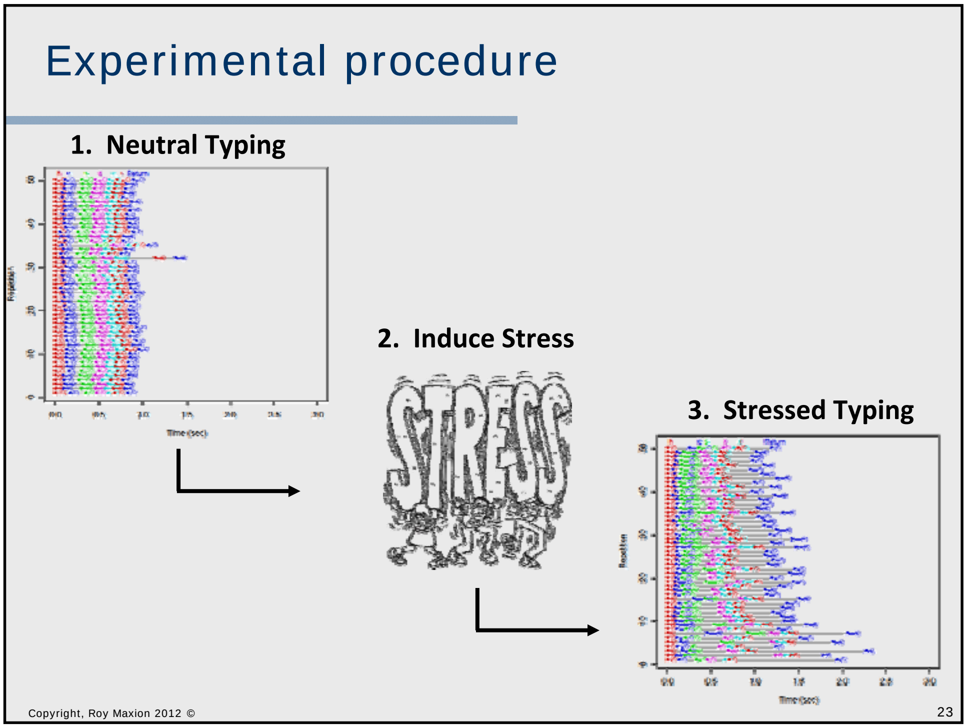
Copyright, Roy Maxion 2012 ©



Next steps

- Past data indicated … yes, there is evidence
- So a formal experiment would …
  - Solicit a typing sample under neutral conditions
  - Induce stress
  - Solicit a typing sample under stressed conditions
  - Find markers for the stressed samples
  - Be able to identify stress in a typist

Copyright, Roy Maxion 2012 ©



Experimental procedure

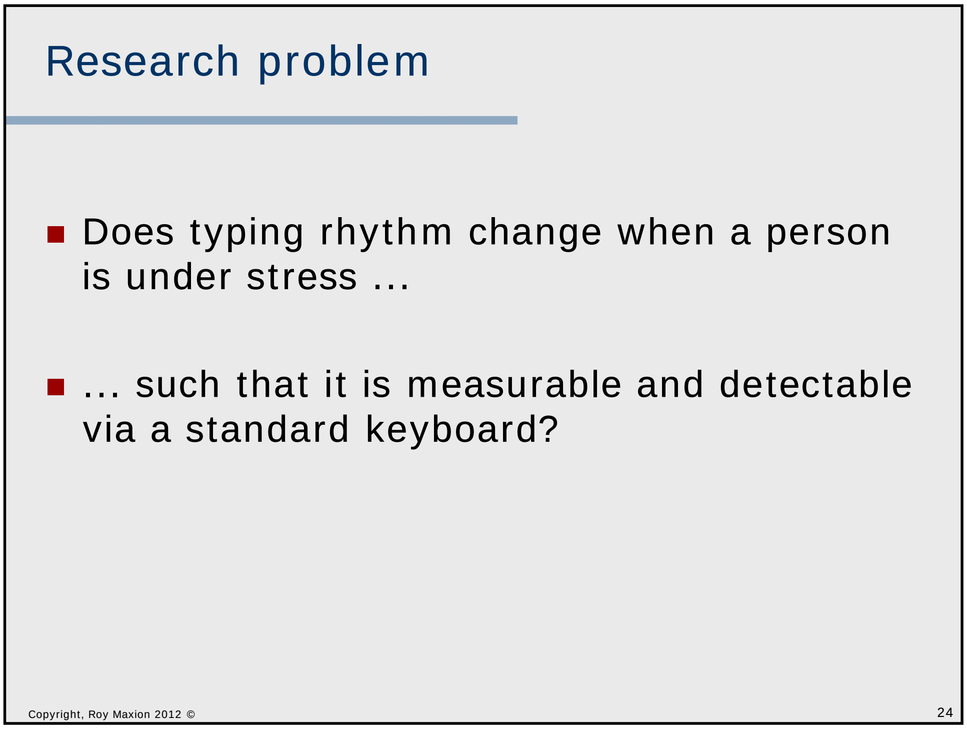
1. Neutral Typing

2. Induce Stress

3. Stressed Typing

Time (sec)
STRESS
Repetition
Time (sec)

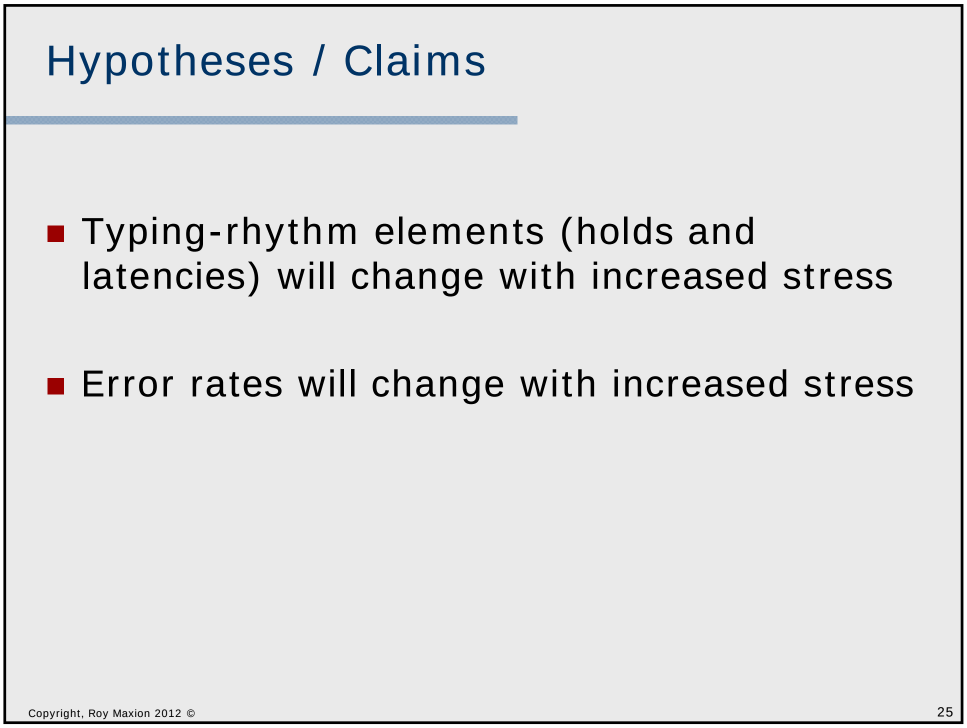
Copyright, Roy Maxion 2012 ©



Research problem

- Does typing rhythm change when a person is under stress …
- … such that it is measurable and detectable via a standard keyboard?

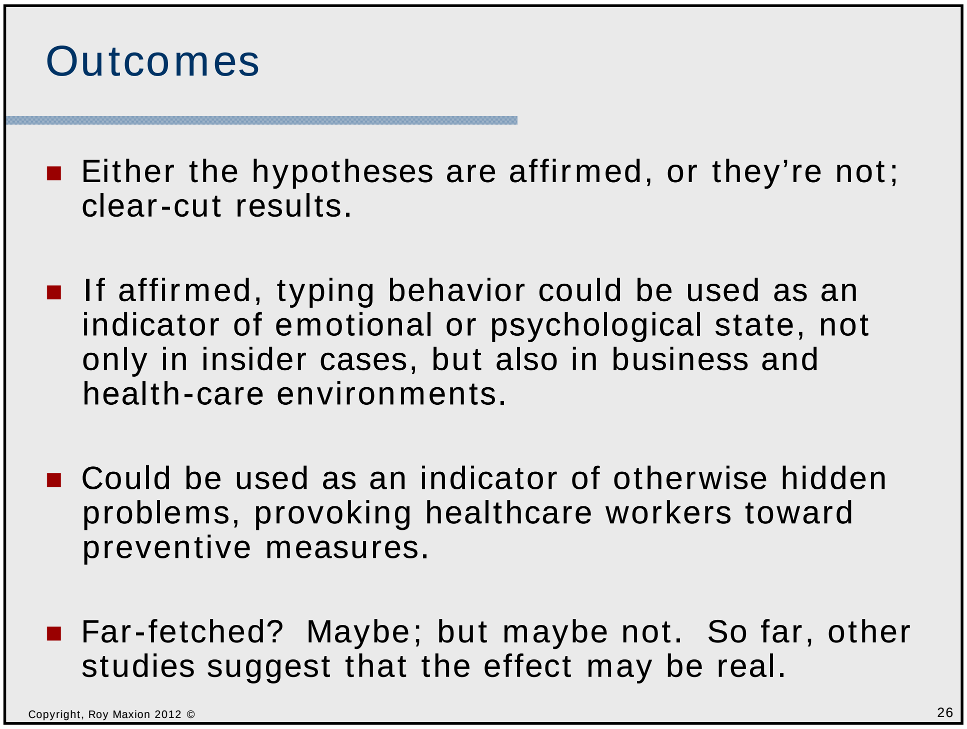
Copyright, Roy Maxion 2012 ©



Hypotheses / Claims

- Typing-rhythm elements (holds and latencies) will change with increased stress
- Error rates will change with increased stress

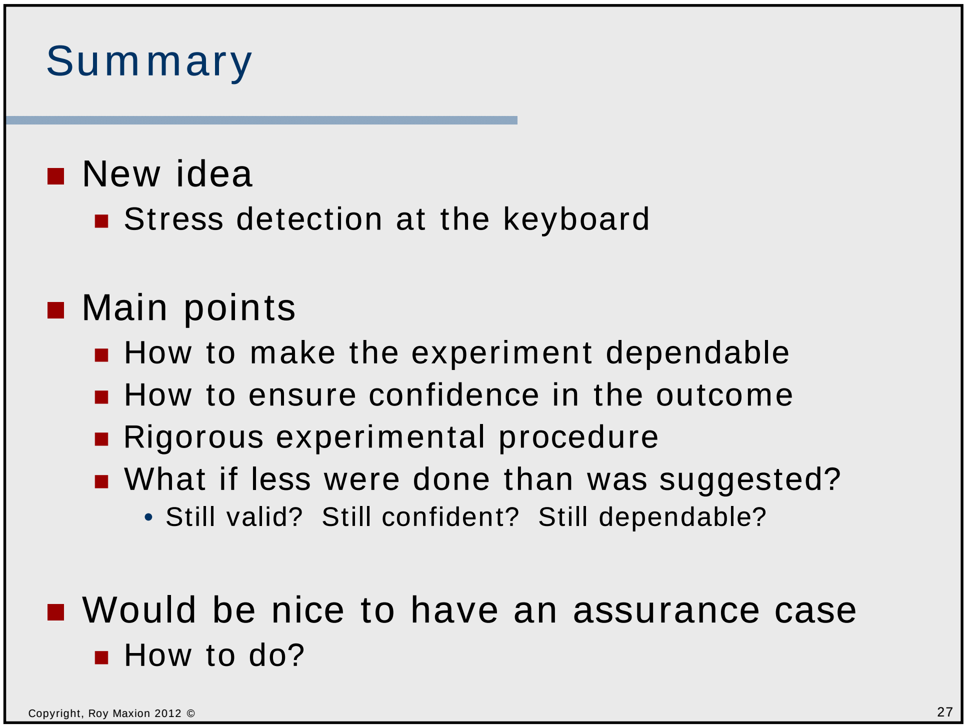
Copyright, Roy Maxion 2012 ©



Outcomes

- Either the hypotheses are affirmed, or they're not; clear-cut results.
- If affirmed, typing behavior could be used as an indicator of emotional or psychological state, not only in insider cases, but also in business and health-care environments.
- Could be used as an indicator of otherwise hidden problems, provoking healthcare workers toward preventive measures.
- Far-fetched? Maybe; but maybe not. So far, other studies suggest that the effect may be real.

Copyright, Roy Maxion 2012 ©



Summary

- New idea
  - Stress detection at the keyboard
- Main points
  - How to make the experiment dependable
  - How to ensure confidence in the outcome
  - Rigorous experimental procedure
  - What if less were done than was suggested?
    - Still valid? Still confident? Still dependable?
- Would be nice to have an assurance case
  - How to do?

Copyright, Roy Maxion 2012 ©