

Identifying Malicious Insiders through Mouse Cursor Movements

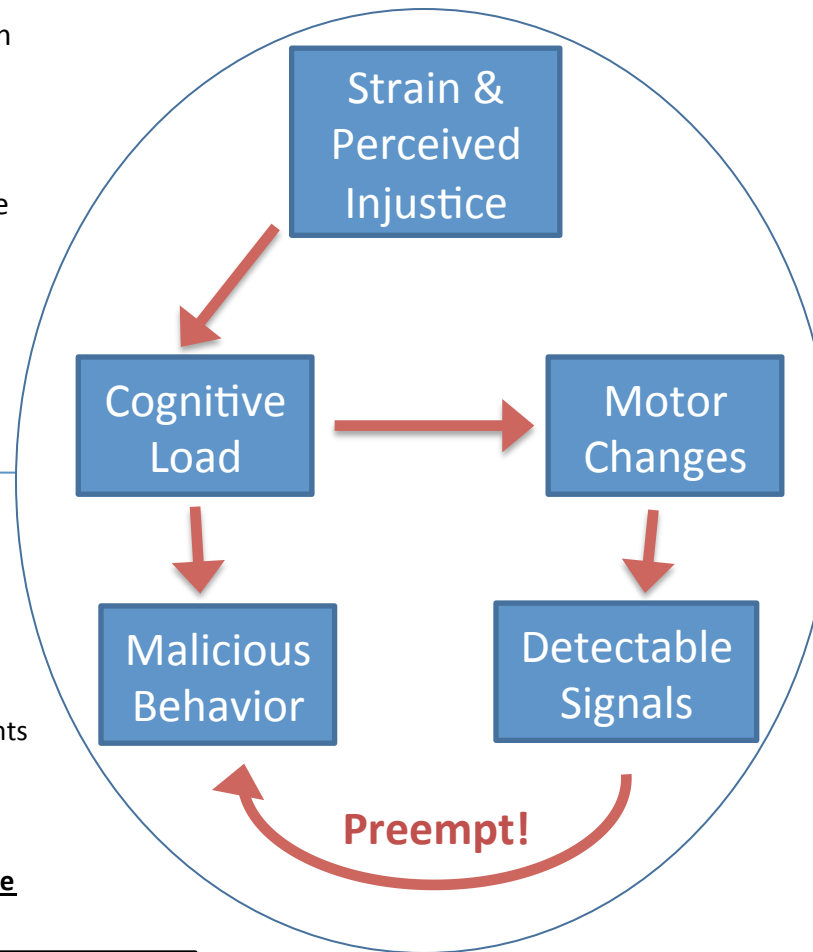


Challenge:

- Insider threats are a top concern for government agencies and corporations
- Difficult to detect using existing methods and often only possible after the event
- Need a way to preemptively assess internal mental states at scale

Solution:

- Malicious activities increase cognitive load
- Motor movements change under increased cognitive load
- Detect changes in motor movements using standard HCI devices (mice, touch, etc.)
- Signals can predict potential malicious behavior during or before it occurs



Scientific Impact:

- Objective mechanism for measuring internal mental states
- Reduce bias from self-report measures
- Scalable, using widely available and deployed HCI hardware
- General Strain Theory for Insider Threat Detection

Broader Impact:

- Broad applicability to insider threat identification and intervention
- Scalable, software driven approach with great commercialization potential
- Quickly resolve false positives in existing monitoring systems without human intervention
- Approach can be used in a broad range of fraud contexts