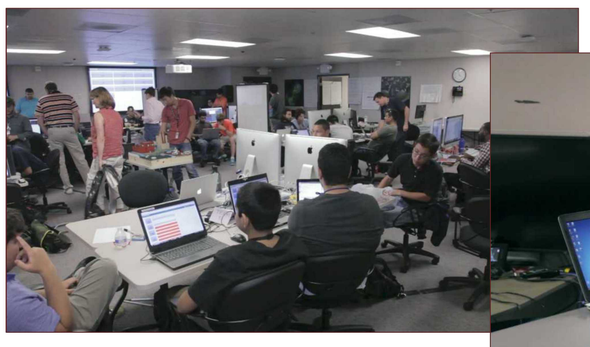
SAND2015-2961D

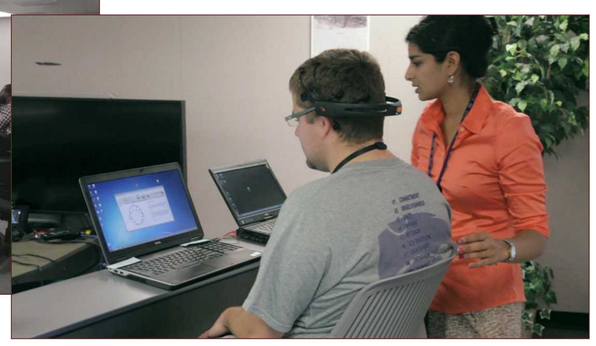
Measuring Human Performance within Computer Security Incident Response Teams

Sandia National Laboratories
J. McClain, A. Silva, G. Emmanuel, K. Nauer, A. Speed, R. Abbott, L. Matzen, M. Haass, D. Trumbo
Albuquerque, New Mexico

Problem

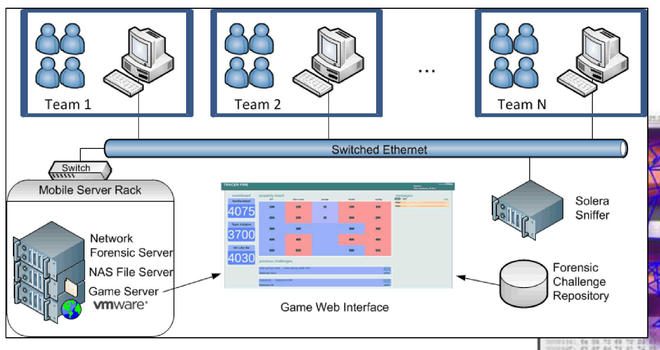
Computer Security Incident Response (IR) teams are key to our nation's strategy for addressing cyber threats. Current IR team training focuses on software tool skillsets with less effort devoted to understanding cognitive skills that both distinguish experts from novices and promote effective team performance. **This project seeks to test the hypothesis that we can differentiate between expert and novice IR individuals through behavioral and physiological measures in the RECOIL* environment.**





Approach

This project seeks to quantify novice/expert differences through empirical testing. We have instrumented RECOIL with validated measures to quantify cognitive/behavioral processes. Variables measured include human-machine transaction monitoring, EEG, eye-tracking, and psychological assessments.



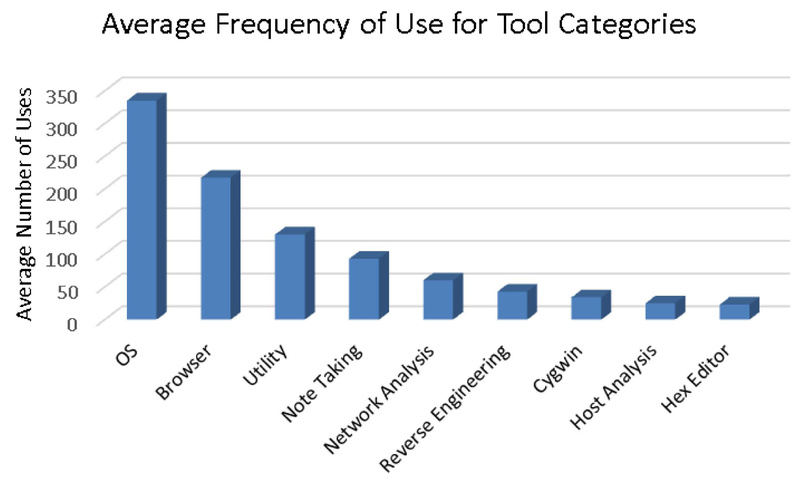
* Research and Engineering for Cyber-Operations Intelligence Laboratory

Results

Frequent switching between tools was significantly predictive of incorrect submissions, r=0.877, $F(1,9)$=26.601, p<0.001. For every increase in total switches, incorrect submissions increased by .877 units.

More frequent use of general-purpose tools significantly predicted more successful answers, r=.810, $F(1, 9)$=15.291, p=.004, as well as earned points, r=.740, $F(1,9)$=9.689, p=.014. For every unit increase in general purpose tools, successful answers increased by .810, and earned points increased by .740.

The use of hex editor significantly predicted incorrect answers, r=.749, $F(1, 9)$=10.206, p=.013. As use of hex editor increased by one unit, incorrect answers increased by .749 units.



Significance

Characterization of high performing individuals and teams in cyber security would allow for the ability to identify individuals with a high aptitude for cyber security tasks. This would allow for enhanced teaming and informed recruiting, as well as accelerated training through targeted interventions based on observed performance and cognitive metrics.

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

SAND 2010-xxxP