Modeling Cognitive Workload and Fatigue for Defensive Cyber Security Operations

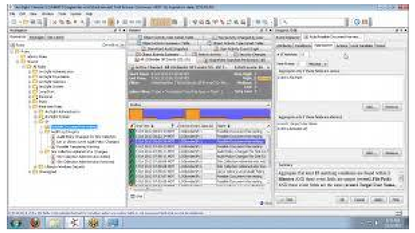
Authors: Jayson Boubin, SOCHE Capt. Christina Rusnock, Ph.D., Air Force Institute of Technology
Contact: boubinjg@miamioh.edu christina.rusnock@afit.edu

Introduction

Cyber defense is an ever growing topic concentrating on the security of computer networks. Human operators are employed to detect and neutralize security threats. These operators use th program ArcsightESM to defen our military networks. We have set out to understand the tasks involved in using ArcsightESM and its alternative to understand the workload and performance of these cyber operators as well as the fatigue they experience to gain a higher understanding of which user interfaces are most optimal for cyber defense. To gain this understanding, we used IMPRINT, a discrete event simulation software tool, to create a realistic simulation to capture fatigue and vigilance decrement, experienced by cyber operators while examining and interpreting alerts.

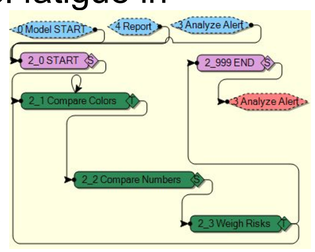
Questions

How do cyber operators experience workload while using interfaces like ArcsightESM



The ArcsightESM Interface

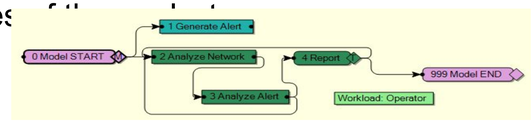
How can we properly model fatigue in IMPRINT?



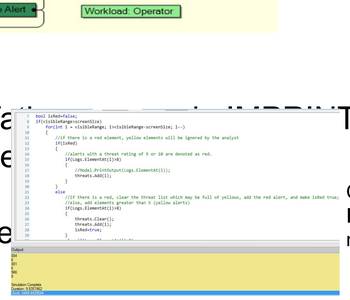
An IMPRINT Task Network

Methods

We used known information about ArcsightESM and other similar software packages to construct a task network. We turned this task network into a discrete event simulation in IMPRINT. We used the IMPRINT's task nodes and logical statements written in the C# language to simulate the cognitive processes



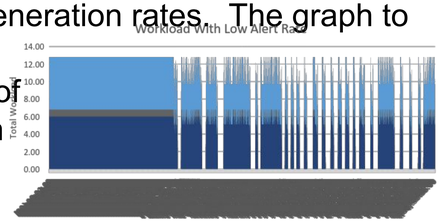
Next, we created our own fa T using mathematical models derive from previous research to accurately represent fatigue experienced by analysts.

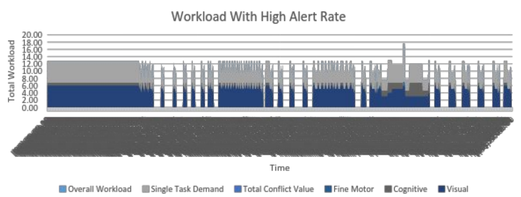


C# Code in an IMPRINT task node

Workload Results

Our workload results have shown us not only the most cognitively intense aspects of cyber analysis, but the differences between workload in certain situations, such as periods of high or low alert generation rates. The graph to the right shows the workload experienced during a period of low alerts. It clearly shows an extended period of constant vigilance. The graph to the left contains a higher rate of alerts, thus the shorter period of vigilance, interspersed with fluctuating workload, signifying periods of analysis.

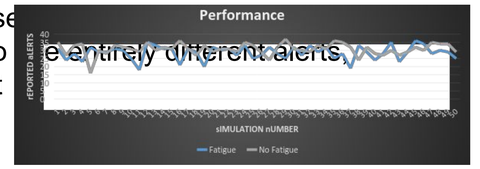




Fatigue Results

In order to accurately models the fatigue experienced by cyber operators in situations under vigilance tasks, we incorporate the fatigue function derived by Giambra & Quilter(1987). The variable y represents the increase in reaction time, the variable t represents the length of the vigilance task in minutes, e is the base of the natural logarithm. $y = 0.6419\left(\left(1 - e^{-0.05319t}\right) + \left(1 - \frac{1}{1 + e^{-0.04633t}}\right)\right)$

Below are the results showing the performance based on total alerts reported by cyber operators when experiencing fatigue (blue) and not experiencing fatigue (gray). It shows that, though the difference in time between the tasks is negligible (only a few se can cause operators to e entirely different alerts. Leading to reports that are vastly different. On average, cyber operators report 20.5



Broader Impact

Our project has provided the IMPRINT community with an easy to use method for incorporating fatigue into human performance models. This will allow for more realistic IMPRINT models in the future.

Our work with interface workload and performance will allow us to understand which interface paradigms will allow cyber security operators to perform as best as possible with little workload. This will allow us to catch more alerts and threats over time without

Acknowledgements

This work was supported in part by the Air Force Research Laboratory, Applied Neuroscience Branch. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied. Special thanks to Giambra and Quilter for their research, Dr. Brett Borghetti, Greg Dye, and Dr. Glenn Gunzelmann.

Giambra, L. M. L., & Quilter, R. E. (1987, December). A two-term exponential functional description of the time course of sustained attention. Human Factors: The Journal of the Human Factors and Ergonomics Society, 0(6).