

Cognitive Foundations of Cyber Analysts

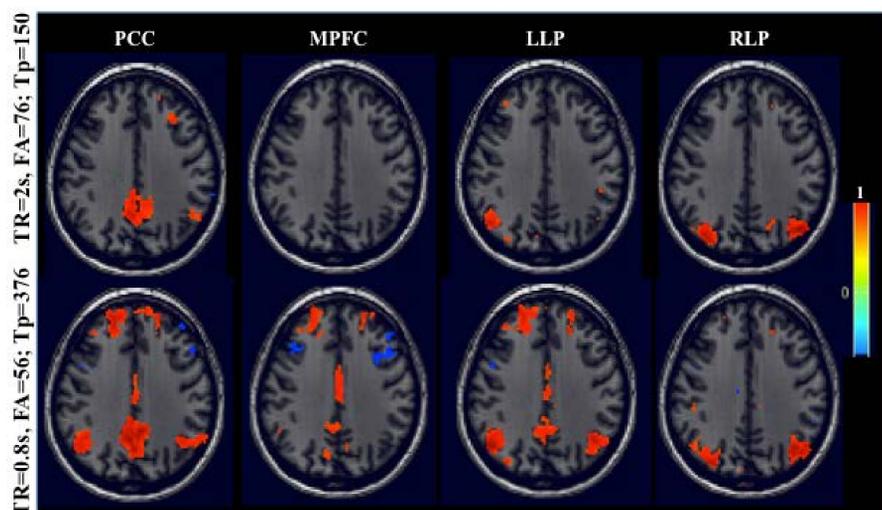


S&T Campaign: Information Sciences
Science of Cyber Security

Dr. Robert F. Erbacher, (301) 394-1674
Robert.F.Erbacher.civ@mail.mil

Research Objective

- Quantitatively compare the performance of expert cyber analysts with a baseline tabular display and two alternative displays
- Measure the effectiveness of students as surrogates for expert cyber analysts in user studies
- Develop cognitive models of expert cyber analysts and users to foster the development of new, more effective and cognitively efficient, techniques and capabilities



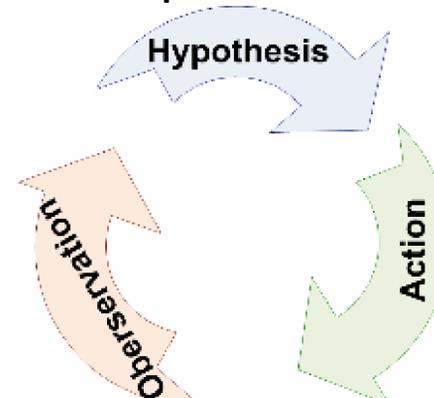
fMRI studies will aid analysis of cognitive load, impact of learning styles, and identification of characteristics correlated with increased effectiveness

Challenges

- Unavailability of real-world data and expert cyber analysts on which to perform quantitative user studies and limited knowledge of analyst needs, biases, and processes. This is exacerbated by the need for a significant number of subjects for a valid quantitative user study
- Lack of empirical evidence that alternative displays are effective
- Lack of empirical evidence that students are effective surrogates for expert cyber analysts

ARL Facilities and Capabilities Available to Support Collaborative Research

- Leverage ARL's Computer Network Defense Service Provider, i.e., expert analysts and real-world data
- Novel AOH model to aid analysis of process models
 - Zhong et al., "RankAOH: Context-driven similarity-based retrieval of experiences in cyber analysis," CogSIMA, pp.230,236, 3-6 March 2014.
 - Yen et al., "Systematic Capture of Cognitive Reasoning Process of Cyber Analyst Toward Agile Cyber Defense" Springer Cyber Defense and Situational Awareness.
- Unique ARL and related displays
- T Tests: surrogates perform poorer than experts; parallel coordinates performed poorest; node-link display performed nominally better but completed tasks 22+% faster



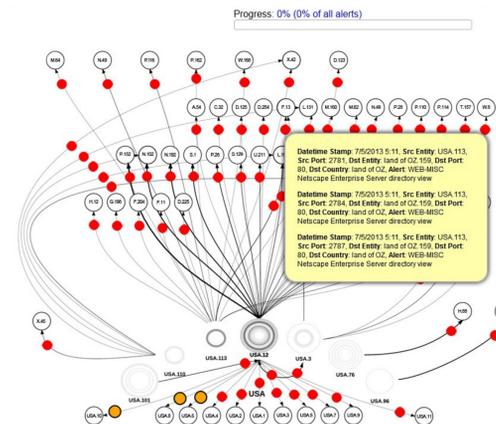
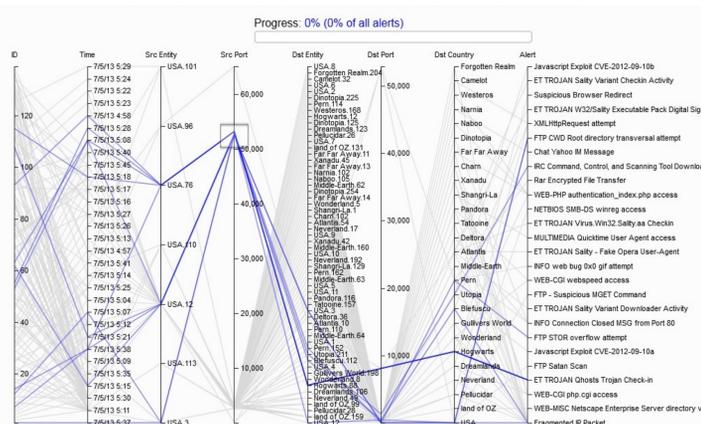
AOH model employed to aid analysis of analyst process models

Complementary Expertise/ Facilities/ Capabilities Sought in Collaboration

- Comparative analysis with subjects of varying expertise
- Development of models of users
- Comparative analysis of models of experts across domains
- Quantitative study across the breadth of VizSec displays
- Novel analysis and process model paradigms to increase the depth and sophistication of the models and derived understanding from user studies

Progress: 17.3% (4.3% of all alerts)

ID	Time	Src Entity	Src Port	Dst Entity	Dst Port	Dst Country	Alert
10	7/5/13 9:12	USA.12	2852	USA.4	21	USA	FTP Satan Scan
14	7/5/13 9:38	USA.12	52870	Penn.152	21	Penn	FTP STOR overflow attempt
16	7/5/13 9:12	USA.12	2859	USA.1	21	USA	FTP Satan Scan
24	7/5/13 9:14	USA.12	2948	USA.11	21	USA	FTP Satan Scan
25	7/5/13 9:12	USA.12	2853	USA.5	21	USA	FTP Satan Scan
32	7/5/13 9:13	USA.12	2909	USA.10	21	USA	FTP Satan Scan
38	7/5/13 9:12	USA.12	2889	USA.9	21	USA	FTP Satan Scan
49	7/5/13 9:12	USA.12	2858	USA.3	21	USA	FTP Satan Scan
62	7/5/13 9:15	USA.12	52614	USA.3	21	USA	FTP CWD Root directory transversal attempt
78	7/5/13 9:12	USA.12	2871	USA.7	21	USA	FTP Satan Scan
108	7/5/13 9:21	USA.12	52643	USA.3	21	USA	FTP CWD Root directory transversal attempt
114	7/5/13 9:12	USA.12	2857	USA.2	21	USA	FTP Satan Scan
117	7/5/13 9:16	USA.12	20	USA.3	52621	USA	FTP - Suspicious MGET Command
118	7/5/13 9:12	USA.12	2868	USA.6	21	USA	FTP Satan Scan
170	7/5/13 9:13	USA.12	2842	USA.8	21	USA	FTP Satan Scan



Baseline tabular display and alternative displays, parallel coordinates and node-link.