Human Factors – rok 2018, roč. 60

Číslo 5 (August)

SPECIAL SECTION: 2017 HUMAN FACTORS PRIZE FOR EXCELLENCE IN HUMAN FACTORS/ERGONOMICS RESEARCH: CYBERSECURITY

HUMAN FACTORS PRIZE WINNER

Ben D. Sawyer, Peter A. Hancock. *Hacking the Human: The Prevalence Paradox in Cybersecurity*. pp. 597–609.

Objective: This work assesses the efficacy of the "prevalence effect" as a form of cyberattack in human-automation teaming, using an email task. **Background:** Under the prevalence effect, rare signals are more difficult to detect, even when taking into account their proportionally low occurrence. This decline represents diminished human capability to both detect and respond. As signal probability (SP) approaches zero, accuracy exhibits logarithmic decay. Cybersecurity, a context in which the environment is entirely artificial, provides an opportunity to manufacture conditions enhancing or degrading human performance, such as prevalence effects. Email cybersecurity prevalence effects have not previously been demonstrated, nor intentionally manipulated. **Method:** The Email Testbed (ET) provides a simulation of a clerical email work involving messages containing sensitive personal information. Using the ET, participants were presented with 300 email interactions and received cyberattacks at rates of either 1%, 5%, or 20%. **Results:** Results demonstrated the existence and power of prevalence effects in email cybersecurity. Attacks delivered at a rate of 1% were significantly more likely to succeed, and the overall pattern of accuracy across declining SP exhibited logarithmic decay. **Application:** These findings suggest a "prevalence paradox" within human-machine teams. As automation reduces attack SP, the human operator becomes increasingly likely to fail in detecting and reporting attacks that remain. In the cyber realm, the potential to artificially inflict this state on adversaries, hacking the human operator rather than algorithmic defense, is considered. Specific and general information security design countermeasures are offered.

- **Keywords:** human-computer interaction, internet, information security, messages, signal detection, vigilance, risk, antivirus, virus, antimalware, malware, design

SPECIAL SECTION: 2017 HUMAN FACTORS PRIZE FOR EXCELLENCE IN HUMAN FACTORS/ERGONOMICS RESEARCH: CYBERSECURITY

HUMAN FACTORS PRIZE FINALISTS

Kevin B. Bennett, Adam Bryant, Christen Sushereba. *Ecological Interface Design for Computer Network Defense*. pp. 610–625.

Objective: A prototype ecological interface for computer network defense (CND) was developed. **Background:** Concerns about CND run high. Although there is a vast literature on CND, there is some indication that this research is not being translated into operational contexts. Part of the reason may be that CND has historically been treated as a strictly technical problem, rather than as a socio-technical problem. **Methods:** The cognitive systems engineering (CSE)/ecological interface design (EID) framework was used in the analysis and design of the prototype interface. A brief overview of CSE/EID is provided. EID principles of design (i.e., direct perception, direct manipulation and visual momentum) are described and illustrated through concrete examples from the ecological interface. **Results:** Key features of the ecological interface include (a) a wide variety of alternative visual displays, (b) controls that allow easy, dynamic reconfiguration of these displays, (c) visual highlighting of functionally related information across displays, (d) control mechanisms to selectively filter massive data sets, and (e) the capability for easy expansion. Cyber attacks from a well-known data set are illustrated through screen shots. **Conclusion:** CND support needs to be developed with a triadic focus (i.e., humans interacting with technology to accomplish work) if it is to be effective. Iterative design and formal evaluation is also required. The discipline of human factors has a long tradition of success on both counts; it is time that HF became fully involved in CND. **Application:** Direct application in supporting cyber analysts.

- **Keywords:** cybersecurity, ecological interface design, cognitive task analysis/cognitive work analysis, ecological approaches, computer interface, graphical user interface, display design, design strategies, perception action

Prashanth Rajivan, Nancy J. Cooke. *Information-Pooling Bias in Collaborative Security Incident Correlation Analysis*. pp. 626–639.

Objective: Incident correlation is a vital step in the cybersecurity threat detection process. This article presents research on the effect of group-level information-pooling bias on collaborative incident correlation analysis in a synthetic task environment. **Background:** Past research has shown that uneven information distribution biases people to share information that is known to most team members and prevents them from sharing any unique information available with them. The effect of such biases on security team collaborations are largely unknown. **Method:** Thirty 3-person teams performed two threat detection missions involving information sharing and correlating security incidents. Incidents were predistributed to each person in the team based on the hidden profile paradigm. Participant teams, randomly assigned to three experimental groups, used different collaboration aids during Mission 2. **Results:** Communication analysis revealed that participant teams were 3 times more likely to discuss security incidents commonly known to the majority. Unaided team collaboration was inefficient in finding associations between security incidents uniquely available to each member of the team. Visualizations that augment perceptual processing and recognition memory were found to mitigate the bias. **Conclusion:** The data suggest that (a) security analyst teams, when conducting collaborative correlation analysis, could be inefficient in pooling unique information from their peers; (b) employing off-the-shelf collaboration tools in cybersecurity defense environments is inadequate; and (c) collaborative security visualization tools developed considering the human cognitive limitations of security analysts is necessary. **Application:** Potential applications of this research include

development of team training procedures and collaboration tool development for security analysts.

- **Keywords:** cybersecurity, threat detection, teamwork, hidden profile paradigm, security visualization

ACCIDENTS, HUMAN ERROR

Meghan Leaver, Alex Griffiths, Tom Reader. *Near Misses in Financial Trading: Skills for Capturing and Averting Error*. pp. 640–657.

Objective: The aims of this study were (a) to determine whether near-miss incidents in financial trading contain information on the operator skills and systems that detect and prevent near misses and the patterns and trends revealed by these data and (b) to explore if particular operator skills and systems are found as important for avoiding particular types of error on the trading floor. **Background:** In this study, we examine a cohort of near-miss incidents collected from a financial trading organization using the Financial Incident Analysis System and report on the nontechnical skills and systems that are used to detect and prevent error in this domain. **Method:** One thousand near-miss incidents are analyzed using distribution, mean, chi-square, and associative analysis to describe the data; reliability is provided. **Results:** Slips/lapses (52%) and human–computer interface problems (21%) often occur alone and are the main contributors to error causation, whereas the prevention of error is largely a result of teamwork (65%) and situation awareness (46%) skills. No matter the cause of error, situation awareness and teamwork skills are used most often to detect and prevent the error. **Conclusion:** Situation awareness and teamwork skills appear universally important as a "last line" of defense for capturing error, and data from incident-monitoring systems can be analyzed in a fashion more consistent with a "Safety-II" approach. **Application:** This research provides data for ameliorating risk within financial trading organizations, with implications for future risk management programs and regulation.

- **Keywords:** accidents, human error, situation awareness, cognition, team collaboration, teams and groups, social processes, safety culture and behavior change

HUMAN-COMPUTER INTERACTION, COMPUTER SYSTEMS

Kevin Juang, Joel Greenstein. *Integrating Visual Mnemonics and Input Feedback With Passphrases to Improve the Usability and Security of Digital Authentication*. pp. 658–668.

Objective: We developed a new authentication system based on passphrases instead of passwords. Our new system incorporates a user-generated mnemonic picture displayed during login, definition tooltips, error correction to reduce typographical errors, a decoy-based input masking technique, and random passphrase generation using either a specialized wordlist or a sentence template. **Background:** Passphrases exhibit a greater level of security than traditional passwords, but their wider adoption has been hindered by human factors issues. Our assertion is that the added features of our system work particularly well with passphrases and help address these shortcomings. **Method:** We conducted a study to evaluate our new system with a customized 1,450-word list and our new system with a 6-word sentence structure against the control conditions of a user-created passphrase of at least 24 characters and a system-generated passphrase using a 10,326-word list. Fifty participants completed two sessions so that we could measure the usability and security of the authentication schemes. **Results:** With the new system conditions, memorability was improved, and security was equivalent to or better than the control conditions. Usability and overall ratings also favored the new system conditions over the control conditions. **Conclusion:** Our research presents a new authentication

system using innovative techniques that improve on the usability and security of existing password and passphrase authentication systems. **Application:** In computer security, drastic changes should never happen overnight, but we recommend that our contributions be incorporated into current authentication systems to help facilitate a transition from passwords to usable passphrases.

- **Keywords:** cybersecurity, usability, passwords, passphrases, mnemonics

HUMAN-ROBOT INTERACTION

Hossein Mirinejad, Paramsothy Jayakumar, Tulga Ersal. *Modeling Human Steering Behavior During Path Following in Teleoperation of Unmanned Ground Vehicles*. pp. 669–684.

Objective: This paper presents a behavioral model representing the human steering performance in teleoperated unmanned ground vehicles (UGVs). **Background:** Human steering performance in teleoperation is considerably different from the performance in regular onboard driving situations due to significant communication delays in teleoperation systems and limited information human teleoperators receive from the vehicle sensory system. Mathematical models capturing the teleoperation performance are a key to making the development and evaluation of teleoperated UGV technologies fully simulation based and thus more rapid and cost-effective. However, driver models developed for the typical onboard driving case do not readily address this need. **Method:** To fill the gap, this paper adopts a cognitive model that was originally developed for a typical highway driving scenario and develops a tuning strategy that adjusts the model parameters in the absence of human data to reflect the effect of various latencies and UGV speeds on driver performance in a teleoperated path-following task. **Results:** Based on data collected from a human subject test study, it is shown that the tuned model can predict both the trend of changes in driver performance for different driving conditions and the best steering performance of human subjects in all driving conditions considered. **Conclusions:** The proposed model with the tuning strategy has a satisfactory performance in predicting human steering behavior in the task of teleoperated path following of UGVs. **Application:** The established model is a suited candidate to be used in place of human drivers for simulation-based studies of UGV mobility in teleoperation systems.

- **Keywords:** human performance modeling, teleoperation, driver behavior, ACT-R cognitive architecture, computational modeling

INDIVIDUAL DIFFERENCES

Monique Frances Crane, Sue Brouwers, Mark William Wiggins, Thomas Loveday, Kirsty Forrest, Suyin Giselle Marianne Tan, Allan Michael Cyna. *"Experience Isn't Everything": How Emotion Affects the Relationship Between Experience and Cue Utilization*. pp. 685–698.

Objective: This research examined whether negative and positive arousal emotions modify the relationship between experience level and cue utilization among anesthetists. **Background:** The capacity of a practitioner to form precise associations between clusters of features (e.g., symptoms) and events (e.g., diagnosis) and then act on them is known as *cue utilization*. A common assumption is that practice experience allows opportunities for cue acquisition and cue utilization. However, this relationship is often not borne out in research findings. This study investigates the role of emotional state in this relationship. **Method:** An online tool (EXPERTise 2.0) was used to assess practitioner cue utilization for tasks relevant to anesthesia. The experience of positive and negative arousal emotions in the previous three days was measured, and emotion clusters were

generated. Experience was measured as the composite of practice years and hours of practice experience. The moderating role of emotion on the relationship between experience and cue utilization was examined. **Results:** Data on 125 anesthetists (36% female) were included in the analysis. The predicted interaction between arousal emotions and the experience level emerged. In particular, post hoc analyses revealed that anxiety-related emotions facilitated the likelihood of high cue utilization in less experienced practitioners. **Conclusion:** The findings suggest a role for emotions in cue use and suggest a functional role for normal range anxiety emotions in a simulated work-relevant task. **Application:** This research illustrates the importance of understanding the potentially functional effects common negative arousal emotions may have on clinical performance, particularly for those with less experience.

- **Keywords:** arousal, cues, emotion, cognition, anesthetists, decision making

MANUFACTURING, PROCESS CONTROL SYSTEMS

Hao Wang, Nathan Lau, Ryan M. Gerdes. *Examining Cybersecurity of Cyberphysical Systems for Critical Infrastructures Through Work Domain Analysis*. pp. 699–718.

Objective: The aim of this study was to apply work domain analysis for cybersecurity assessment and design of supervisory control and data acquisition (SCADA) systems. **Background:** Adoption of information and communication technology in cyberphysical systems (CPSs) for critical infrastructures enables automated and distributed control but introduces cybersecurity risk. Many CPSs employ SCADA industrial control systems that have become the target of cyberattacks, which inflict physical damage without use of force. Given that absolute security is not feasible for complex systems, cyberintrusions that introduce unanticipated events will occur; a proper response will in turn require human adaptive ability. Therefore, analysis techniques that can support security assessment and human factors engineering are invaluable for defending CPSs. **Method:** We conducted work domain analysis using the abstraction hierarchy (AH) to model a generic SCADA implementation to identify the functional structures and means–ends relations. We then adopted a case study approach examining the Stuxnet cyberattack by developing and integrating AHs for the uranium enrichment process, SCADA implementation, and malware to investigate the interactions between the three aspects of cybersecurity in CPSs. **Results:** The AHs for modeling a generic SCADA implementation and studying the Stuxnet cyberattack are useful for mapping attack vectors, identifying deficiencies in security processes and features, and evaluating proposed security solutions with respect to system objectives. **Conclusion:** Work domain analysis is an effective analytical method for studying cybersecurity of CPSs for critical infrastructures in a psychologically relevant manner. **Application:** Work domain analysis should be applied to assess cybersecurity risk and inform engineering and user interface design.

- **Keywords:** cybersecurity, cyberphysical system, work domain analysis, supervisory control, cognitive work analysis, ecological approaches, system analysis

SIMULATION AND VIRTUAL REALITY

Sami Mecheri, Régis Lobjois. *Steering Control in a Low-Cost Driving Simulator: A Case for the Role of Virtual Vehicle Cab*. pp. 719–734.

Objective: The aim of this study was to investigate steering control in a low-cost driving simulator with and without a virtual vehicle cab. **Background:** In low-cost simulators, the lack of a vehicle cab denies driver access to vehicle width, which could affect steering control, insofar as locomotor adjustments are known to be based on action-scaled visual

judgments of the environment. **Method:** Two experiments were conducted in which steering control with and without a virtual vehicle cab was investigated in a within-subject design, using cornering and straight-lane-keeping tasks. **Results:** Driving around curves without vehicle cab information made drivers deviate more from the lane center toward the inner edge in right (virtual cab = 4 ± 19 cm; no cab = 42 ± 28 cm; at the apex of the curve, $p < .001$) but not in left curves. More lateral deviation from the lane center toward the edge line was also found in driving without the virtual cab on straight roads (virtual cab = 21 ± 28 cm; no cab = 36 ± 27 cm; $p < .001$), whereas driving stability and presence ratings were not affected. In both experiments, the greater lateral deviation in the no-cab condition led to significantly more time driving off the lane. **Conclusion:** The findings strongly suggest that without cab information, participants underestimate the distance to the right edge of the car (in contrast to the left edge) and thus vehicle width. This produces considerable differences in the steering trajectory. **Application:** Providing a virtual vehicle cab must be encouraged for more effectively capturing drivers' steering control in low-cost simulators.

- **Keywords:** driving simulator, vehicle cab, steering control, lateral position, curve