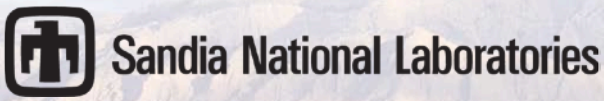
SANDIA REPORT
SAND2015-9030
Unlimited Release
September 2015

Measuring Human Performance within Computer Security Incident Response Teams

Jonathan McClain, Austin Silva, Glory Emmanuel Aviña, and Chris Forsythe

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.



Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: http://www.ntis.gov/search

SAND2015-9030
Unlimited Release
September 2015

Measuring Human Performance within Computer Security Incident Response Teams

Jonathan McClain
Data-Driven and Neural Computing

Austin Silva
Cognitive Science and Systems

Glory Emmanuel Aviña
Cognitive Science and Systems

Chris Forsythe
Human Factors

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-MS1327

Abstract

Human performance has become a pertinent issue within cyber security. However, this research has been stymied by the limited availability of expert cyber security professionals. This is partly attributable to the ongoing workload faced by cyber security professionals, which is compounded by the limited number of qualified personnel and turnover of personnel across organizations. Additionally, it is difficult to conduct research, and particularly, openly published research, due to the sensitivity inherent to cyber operations at most organizations. As an alternative, the current research has focused on data collection during cyber security training exercises. These events draw individuals with a range of knowledge and experience extending from seasoned professionals to recent college graduates to college students. The current paper describes research involving data collection at two separate cyber security exercises. This data collection involved multiple measures which included behavioral performance based on human-machine transactions and questionnaire-based assessments of cyber security experience.

ACKNOWLEDGMENTS

The research team would like to thank Kevin Nauer, Ben Anderson, and those who supported TracerFIRE and the RECOIL lab, both which were the means for data collection. We also acknowledge and are grateful for the various government agencies and the individuals from them who participated in this research study.

CONTENTS

FIGURES

TABLES

NOMENCLATURE

DOE	Department of Energy
EEG	Electroencephalogram
FIRE	Forensic Incident Response Exercise
SNL	Sandia National Laboratories

1. INTRODUCTION

The human dimension of cyber security has been described from the perspective of the computer user reliant on information technologies and systems, the organization with its policies and management practices and the cyber security analysts responsible for defending information networks from cyber threats (Kraemer, Carayon & Clem, 2009; Forsythe et al., 2013). The current paper focuses on behavioral performance of cyber security analysts, and in particular, analysts for whom cyber forensic analysis is a primary component of their job assignments. Previous research has provided a descriptive account of the tasks (Erbacher et al., 2010), workflow (Erbacher et al., 2010; Reed et al., 2014) and cognitive demands (DiAmico et al., 2005) associated with cyber security analysis. Related studies have described cyber security analysis from the perspective of situation awareness (Barford et al., 2010; Stevens-Adams et al, 2013) and teamwork considerations (Jariwala et al., 2010).

Different organizations conceptualize the job of cyber security analysts differently and consequently, the tasks, responsibilities, expectations and levels of discretion assigned to individuals and teams vary. In many organizations, cyber security professionals primarily focus on assuring compliance (e.g., operating system and software version management, virus protection updates). Individuals in these settings rarely have the knowledge and expertise to respond to a significant incident and when an incident does occur, there is need to call on the services of other organizations. In other settings, cyber security professionals receive alerts from sources including automated intrusion detection systems, user reports, correspondence with other cyber security professionals, community bulletin boards, etc. and the primary responsibility involves performing triage on these alerts (Reed et al., 2014). The ability to effectively assess and prioritize alerts is critical to these operations and has been the subject of research (Dutt, Ahn & Gonzalez, 2013). Individuals working in these settings often do not perform investigations that go beyond identifying appropriate means of mitigating vulnerabilities, with more extensive analysis referred to other organizations. Finally, in more sophisticated cyber operations, analysts conduct forensic analysis to investigate incidents deemed to represent a threat to the organization to gain a better understanding of the perpetrators and their capabilities (e.g., sophistication of phishing attacks, malware employed), enabling the organization's cyber defense to adapt and evolve.

Cyber forensic analysis involves problem solving skills that extend beyond those associated with criminal forensic analysis. Specifically, analysts must possess a basic understanding of computer hardware and software systems, computer networking, and the tactics and techniques employed by cyber criminals. Problem solving often involves parallel analysis undertaken at more than one level of detail. For instance, low level analysis of network logs may provide insights into the origin and paths taken by an intruder, while higher level analysis will consider the capabilities of the adversary, their target and presumed objectives, and affiliations and motivations. Through low level analysis, clues are attained and through higher level analysis, these clues are stitched together to construct a story of the who, what, why and how underlying a cyber incident.

Through the Tracer FIRE (Forensic Incident Response Exercise) program, a platform has been developed that provides training that encompasses both the low-level and high-level analysis

skills required by cyber forensic analyst. Participants work as teams of 4-6 individuals and are provided essential software tools (e.g., Wireshark, PDF dissector). The exercise is a competitive event with teams awarded points for successfully solving challenges. Individual challenges require that participants exercise various computer forensic analysis skills (e.g., review server logs to identify a suspicious entry). Once solved, challenges unlock other challenges, while providing clues to the overall scenario. As participants work through the individual challenges, a CNN-like news server provides updates regarding events related to the cyber-crimes (e.g., public statement from hacktivist group) and supply additional clues to the overall scenario. The ultimate objective is to accurately determine the overall scenario, and specifically, identify the perpetrators, and ascertain their motives and objectives.

While serving as a training platform, Tracer FIRE also provides a laboratory for conducting human performance research for cyber security operations. Instrumentation allows data to be collected non-intrusively regarding participant human-computer transactions. This data includes opening and closing of files and software tools, window contents and transitions between windows, and keyboard and mouse activities. These data are synched with data from the game server indicating the challenges accessed and answer submissions, and the news server showing news articles that were accessed. Finally, techniques have been developed for the analysis of logs to parse entries into blocks of activity and decompose blocks of activity into distinct tasks (Abbott et al., 2015).

Previous research conducted in a similar setting found that the most successful students were those that committed the longest blocks of time to individual challenges and combined the use of specialized cyber security software tools (e.g., Encase Enterprise, Wireshark) with general purpose software tools (e.g., Microsoft Excel, Cygwin) (Silva et al., 2014). The current research extends these findings with consideration of a larger group of participants and more detailed consideration of participant human-machine transactions. The objective was to determine if differences exist in the use of software tools by experienced cyber security professionals, as compared to their less experienced counterparts.

2. RESEARCH METHODOLOGY

The current report describes analysis of human-machine transactions and self-reported cyber security experience. Additional questionnaire-based measures were collected which included the Big Five Personality Inventory (Dingman, 1990), the Need for Cognition Scale (Cacioppo & Petty, 1984) and the General Decision-Making Style Inventory (Scott & Bruce, 1995). Additionally, EEG and eye-tracking data collection occurred for a subset of participants as they performed tasks outside the context of the Tracer FIRE training exercise, with results of the eye-tracking reported in Silva et al. (2015). The purpose of these measures is to determine not only what tools are being used in the cyber context but how cyber defenders utilize various cognitive attributes to approach cyber-based problems.

2.1 Subjects

Subjects consisted of a total of 26 Tracer FIRE participants who consented to data collection during two separate training exercises. There were 11 subjects from the first event which occurred during the spring of 2014 and 15 subjects from the second event that occurred in the summer of 2014.

2.2 Materials

Subjects were asked to complete multiple questionnaire measures of cyber security experience, personality characteristics and cognitive style.

2.2.1 Cyber Security Experience Questionnaire

This assessment consisted of two parts. The first part asked participants to report their professional and student experience with six types of cyber security forensics analysis topics on a six-point scale (0=No Experience; 1=One Month or Less; 2=Three Months or Less; 3=Six Months or Less; 4=One Year or Less; 5=Three Years or Less; and 6=More than Three Years). The second part of the assessment used the same six-point scale and asked subjects to report their experience with each of 8 cyber security software tools.

2.2.2 Big Five Personality Inventory

The Big Five Personality Inventory, (BFI; Benet-Martinez & John, 1998) consists of items used to measure neuroticism, agreeableness, conscientiousness, and openness to experience as well as characteristics of extraversion and introversion. Respondents are asked on a Likert scale of 1 to 5 to state how strongly they disagree (1) or agree (5) with a statement about themselves. Example statements are: “Is outgoing, sociable,” “Is talkative,” and “Is sometimes shy, inhibited.”

2.2.3 Need for Cognition Scale

The Need for Cognition Scale is an assessment instrument that quantitatively measures "the tendency for an individual to engage in and enjoy thinking" (Cacioppo & Petty, 1982, p. 116). Cacioppo and Petty created the Need for Cognition Scale in 1982. The original scale included 34 questions. Two years later, Cacioppo and Petty collaborated with Chuan Feng Kao to shorten the scale to the 18-item format, which is used in the Wabash National Study of Liberal Arts Education. Based on previous research, the Need for Cognition Scale appears to be a valid and reliable measure of individuals’ tendencies to pursue and enjoy the process of thinking—that is,

of their "need for cognition" (Cacioppo & Petty, 1982; Cacioppo, Petty, Feinstein, & Jarvis, 1996; Cacioppo et al., 1984; Sadowski, 1993; Sadowski & Gulgoz, 1992b). Need for Cognition scores are not influenced by whether an individual is male or female, or by differences in the individual's level of test-taking anxiety or cognitive style (the particular way that an individual accumulates and merges information during the thinking process). In general, scores on the Need for Cognition Scale also are not impacted by whether or not the individuals are trying to paint a favorable picture of themselves (Cacioppo & Petty, 1982).

2.2.4 General Decision-Making Style Inventory

The General Decision-Making Style Inventory (GDMS; Scott & Bruce, 1995) measures five different decision-making styles: rational, intuitive, dependent, avoidant and spontaneous. The instrument has 25 questions (5 items for each dimension) rated on a 5-point Likert-type scale ranging from "strongly disagree" to "strongly agree". The following headings were used: "Listed below are statements describing how individuals go about making important decisions". The GDMS has been shown to be a reliable and valid scale for assessing decision-making. Reliability (Cronbach's alphas) for the different dimensions vary between 0.62 and 0.87 and patterns of correlations with values, measure of social relations, work conditions and other variables provided convergent validity support for the GDMS (Loo, 2000, Scott and Bruce, 1995, Spicer and Sadler-Smith, 2005 and Thunholm, 2004).

2.3 Procedure

The Tracer FIRE exercise consisted of a multi-day event that combined classroom instruction in the use of cyber security software tools, forensic analysis techniques, and adversary tactics and techniques with a team competition exercise. At the beginning of the competition, there was an announcement concerning the study and those willing to consent to data collection underwent the informed consent process. Date collection regarding human-machine transactions occurred non-intrusively through automated data logging as subjects participated in the exercise.

The exercise presented teams a multi-level challenge. At a low level, there was a series of puzzles that allowed participants to exercise their cyber forensic analysis skills, as well as the cyber security software tools. At a higher level, there was a complex scenario partially based on real-world events that involved multiple adversaries with differing objectives operating individually and in collaboration with one another. As participants solved the individual puzzles they received points that were tallied on a scoreboard and unlocked more puzzles. Additionally, by solving individual puzzles, participants obtained clues to the overall scenario that would be helpful in solving subsequent puzzles. At the conclusion, each team presented their interpretation of the overall scenario and the ultimate outcome hinged upon how closely the team interpretations corresponded with the ground truth of the actual events.

2.4 Instrumentation

Each student was provided with a laptop computer on which essential cyber security software tools had been installed which included Encase Enterprise, Wireshark, PDF Dissector and Volitility. Laptops also offered the basic tools available with the Microsoft Windows and Microsoft Office products. Students were free to download additional software tools and install them on computers used for the exercises. A web-based game server provided the basis for participants to access individual challenges, submit their answers and receive feedback indicating

if their answers were correct. Additionally, a news server provided periodic announcements regarding events relevant to the overall scenario (e.g., press release from Hacktivist group).

A Sandia National Laboratories software tool known as Hyperion was used to capture human-machine transactions. This included the use of software applications, Internet accesses, windows events, and keystrokes and mouse clicks. The data collected from Hyperion was combined and synchronized with the game server logs and logs from of the news server to provide a combined record encompassing the activities of each individual participant.

The logs generated from the Tracer FIRE exercise consisted of a time synchronized record combining multiple sources of data. For each human-machine transaction, the data included:

- Participant UserID
- Timestamp
- Interval since previous transaction (i.e., duration)
- Challenge ID, for transactions involving the game server
- Event Type, for transactions involving game server
- Submission, answer submitted for transactions involving submitting answer to game server
- Points Awarded, for transactions involving submitting answers to the game server
- Software Tool, for transaction involving software tools
- Class of Event (Windows, Game Server or News Server)
- Article ID, for transactions involving the News Server

Data logs from the Tracer FIRE exercise were parsed into meaningful blocks of time in which participants were focused on a specific mid-level to high-level goal. The techniques for parsing the logs and a descriptive analysis of the resulting blocks of activity are discussed in Abbott et al. (2015) and a validation of these techniques in Abbott et al. (in press).

3. RESULTS

3.1 Behavioral Observations and Self-Reported Experience

The current section provides a comparison of behavioral observations and self-reported experience with cyber security topics and software tools.

3.1.1 Self-Reported Experience

Table 1 provides a summary of the self-reported experience of the participants. On average, participant experience in most areas ranged between 1-3 months. However, there were a couple of noteworthy exceptions: Network Analysis and Wireshark. While the participants included several individuals with significant cyber security experience, in general, participants had little professional experience with the cyber security topics and cyber security software tools incorporated into the exercise. Nonetheless, teams successfully completed many of the challenges suggesting that the materials were difficult, yet not impossible, given the experience of the participants.

Table 1. Self-reported experience of participants with cyber security topics and software tools.

Survey Item	Mean Response	Standard Deviation	Maximum
Cyber Security Topics			
Memory Forensics	1.3	1.8	5
Disk Forensics	1.5	1.9	6
Reverse Engineering PDF	1.0	1.4	5
Reverse Engineering Java	0.8	1.2	4
Reverse Engineering Binary	1.3	1.8	5
Network Analysis	3.2	2.2	6
Cyber Security Software Tools			
Encase Enterprise	0.6	1.3	5
Volatility	0.6	1.2	4
Autopsy	0.6	1.3	5
Wireshark	3.3	1.8	6
IDA Pro	0.7	1.4	6
Java Decompiler	0.9	1.3	4
PDF Dissector	0.5	1.1	4
Hex Editor	2.2	2.1	6

* Scale values correspond to: 0=No Experience; 1=One Month or Less; 2=Three Months or Less; 3=Six Months or Less; 4=One Year or Less; 5=Three Years or Less; and 6=More than Three Years

** The minimum of all items was 0.

The behavioral activity of relatively experienced and inexperienced participants was compared. Two measures of experience were considered. The sum experience of participants involved adding together the ratings of a participant on all 14 items from the experience survey. A second measure, highest rating, was based on the highest rating a given subject offered for any one of

the 14 items. While the two measures of experience were correlated (r=0.657; p<0.001), this approach addressed the situation where an individual might have extensive experience in one area (e.g., network analysis), yet little or no experience in other areas (e.g., memory forensics).

Correlation analyses were calculated for the two measures of experience and the following behavioral measures: (1) total duration of blocks of activity; (2) number of actions observed within blocks of activity; (3) number of different software tools used within blocks of activity; (4) number of transitions between different software tools within blocks of activity; and (5) number of times returned to a previously utilized software tool within a block of activity. The correlation results are presented in Table 2. The absence of statistically significant correlations suggests that there are no relationships between the levels of self-reported experience of participants in the current study and the behavioral measures of activity. It is noted that an additional analysis considering the relationship between the total number of different tools used by each participant and self-reported experience did not yield a statistically significant relationship (Sum of Ratings, *r*=0.238; NS; Highest Rating, *r*=0.180; NS). Thus, it appears that at a general level, the behavioral activity of experienced and inexperienced participants is comparable.

Table 2 . Correlations between ratings of experience and behavioral measures of activity

	Sum of experience ratings	Highest experience rating
Duration blocks	*r*=0.051	*r* =-0.149
	NS	NS
Number actions	*r*=0.054	*r*=-0.198
	NS	NS
Number tools	*r*=-0.043	*r*=-0.106
	NS	NS
Number transitions	*r*=0.230	*r*=-0.022
	NS	NS
Number returns	*r*=0.253	*r*=-0.013
	NS	NS

Next, the use of specific software tools was considered. Across all the participants, there was a total of 62 unique software applications used during the exercise. This included both general use tools (e.g., Internet Explorer, Notepad) and specialized tools (e.g., Wireshark, Scalpel). Figure 1 and Figure 2 provide descriptive statistics for the overall tool use by the participants (Abbott et al., 2015). Correlations were calculated to identify relationships between self-reported experience and the level of use for specific software tools. This analysis revealed several interesting relationships. First, there was a positive relationship between experience and the use of certain general purpose software tools. Those with more experience, tended to make greater use of the Chrome Internet browser (Number of Actions, *r*=0.565; p<0.003; Number of Instances, *r*=0.555; p<0.003). This relationship appeared to be restricted to the Chrome Internet browser, as there was no relationship with use of the Firefox Internet browser (Number of Actions, *r*=-0.044; NS; Number of Instances, *r*=0.065; NS).

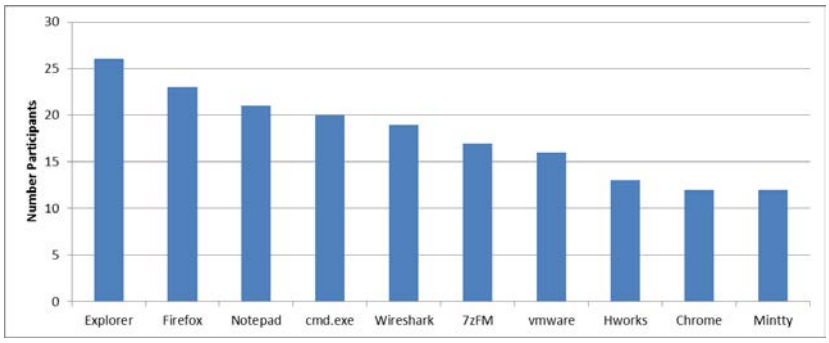


Figure 1. Software applications utilized by the most participants.

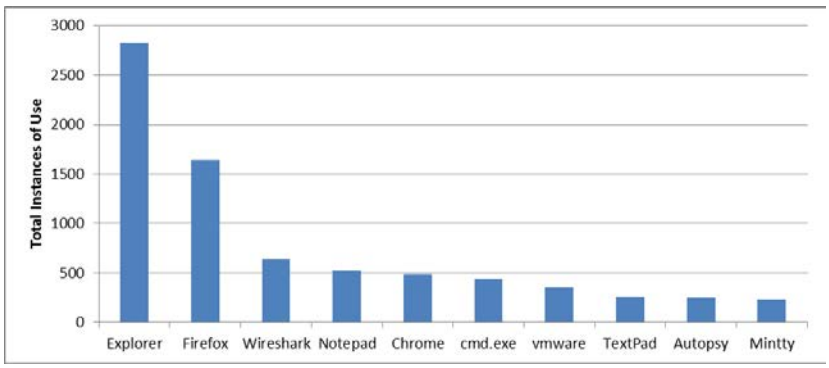


Figure 2. Total number of instances software applications were used summed across subjects.

A positive relationship was also observed between self-reported experience and the use of four general purpose tools: (1) the Windows command line or the cmd.exe process (Number of Actions, r=0.484; p<0.05; Number of Instances r=0.352; p<0.10); (2) Windows Task Manager (Number of Actions, r=0.769; p<0.001; Number of Instances, r=0.773; p<0.001); (3) the Windows Explorer file directory (Number of Actions, r=0.398; p<0.05; Number of Instances, r=0.352; p<0.10) and (4) vmware (Number of Actions, r=0.668; p<0.001; Number of Instances, r=0.673; p<0.001). A consideration of the specialized cyber security software tools found only one statistically significant relationship in that there was a positive relationship between experience and the use of the software tool Autopsy (Number of Actions, r=0.374; p<0.10; Number of Instances, r=0.464; p<0.05).

As discussed in earlier publications (Stevens-Adams et al., 2013; Silva et al., 2014), measures of performance based on transactions with the game server can be misleading. Often, participants work as a team to solve challenges, but only the member of the team that submits a response to the game server receives direct credit. Additionally, while point values assigned to different challenges vary in relation to the estimated difficulty of the challenge, these are only estimates and do not reflect an empirically established measure of difficulty, or achievement.

Only 12 of the 26 participants in the current study made submissions to the game server. While there was no relationship between the sum of experience ratings and whether or not subjects made submissions (r=0.108; NS), the greatest experience rating of subjects was significantly correlated with submissions (r=0.540; p<0.001), with those having substantial experience in at least one area being more likely to make submissions. The greatest experience rating was also significantly correlated with the total number of points (r=0.501; p<0.01), but not the sum of experience ratings (r=-0.007; NS). Similarly, those with the greatest experience rating made their first submission significantly sooner (r=0.536; p<0.01) and entered correct submissions sooner following their opening a challenge (r=0.551; p<0.01), with the relationship with the sum of experience scores not obtaining statistical significance for either of these measures (r=-0.023; NS and r=0.038; NS, respectively). These findings reflect upon the measures of experience and suggest that whereas the sum of experience across areas does not relate to performance within the competitive exercise, having experience in at least one area is sufficient to perform somewhat better than participants who have relatively little experience across all areas.

Additionally, it was noted that those who used more tools over the course of the competitive exercise did better than those who used fewer tools. The total number of tools used correlated with whether subjects submitted answers (r=0.510; p<0.01), the number of successful submissions (r=0.438; p<0.05) and the total number of points (r=0.493; p<0.01). The latter relationships are illustrated within Figure 3. However, the relationship between the number of tools used during the exercise was not significantly correlated with the sum of experience ratings (r=0.238; NS) or the greatest experience rating (r=0.180; NS).

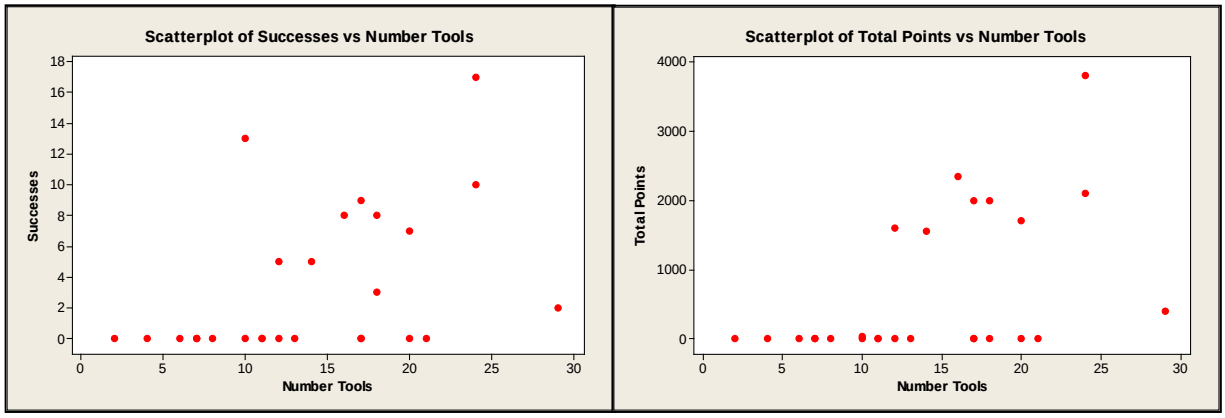


Figure 3. Scatterplots illustrating relationships between the overall Number of Tools used by participants during the competitive exercise, and the number of successful answers submitted for challenges and the overall number of points that were earned.

A stepwise regressions was calculated in which each of the topics and tools for which subjects provided ratings were considered as predictors of the total points earned. The resulting model accounted for 73.4% of the variance (R^2 (Adj) = 69.80) using three predictors: Wireshark (t=6.68; p<0.001); reverse engineering binary (t=-2.44; p<0.05); and reverse engineering java (t=1.99; p<0.06).

Finally, the transitions to and from software tools was analyzed. Figure 4 shows the resulting transition diagrams for the 12 most frequently used software tools for the 11 subjects with the least self-reported experience and the 11 subjects with the most self-reported experience. It is evident that for the more experienced participants, there were more transitions to and from Windows Explorer, Firefox and Wireshark. However, TextPad was used more extensively by the more experienced participants with there being frequent transitions from Firefox to TextPad.

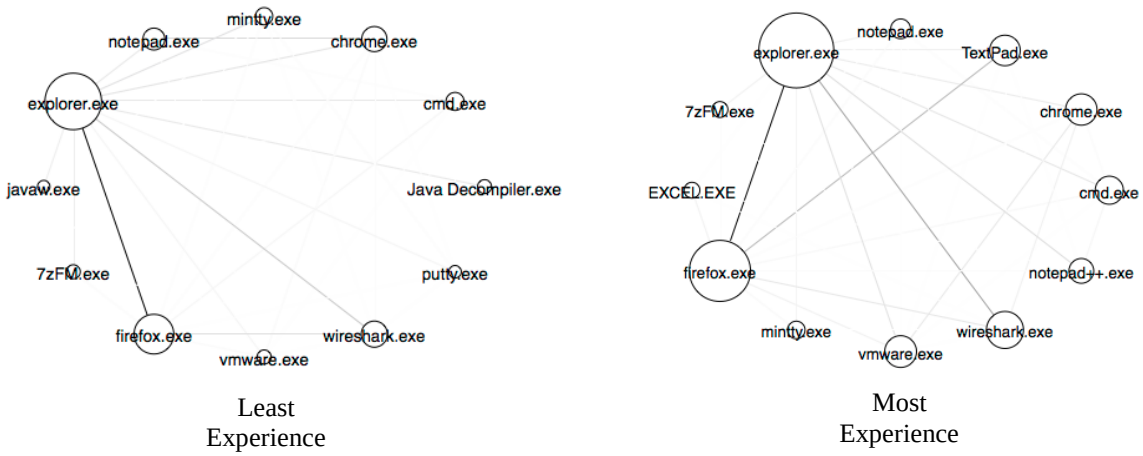


Figure 4. Transitions to and from software applications for most frequently used software tools.

4. DISCUSSION

The current results are consistent with a significant finding from analysis of activity during an earlier cyber security training exercise (Silva et al., 2014). Specifically, the previous study found that the participants who submitted the most correct answers to the challenges made more use of general purpose software tools. It was suggested that while specialized cyber security software tools may provide essential features enabling participants to accomplish tasks that would not be possible otherwise, they are not sufficient in themselves for the overall task of cyber security forensic analysis. Instead, the more successful participants combined the use of specialized software with general purpose software tools (e.g., Notepad, Microsoft Excel, Cygwin). Similarly, in the current study, participants with more professional cyber security experience, made greater use of certain general purpose software tools. These included the Windows command line, Windows Task Manager, vmware, and the Firefox and Chrome Internet browsers.

As noted earlier, success in completing challenges is a crude measure of performance within current cyber security competitive exercises. A more effective measure may entail comparing the behavior of novices to that observed with experts. The current study showed that novices and experts behaved comparably with regard to the overall structure of their activities. There was no apparent difference in the duration of blocks of activity, or the number of actions, the number of software tools used, the number of transitions between software tools and the number of returns to a previously used software tool within blocks of activity. Instead, experts differed in their use of general purpose software tools and their integration of the use of general purpose and specialized cyber security software tools. While the current analysis describes behavior at a fairly high level (e.g., instances using a specific software tool), the next step must be to consider the specific content accessed and actions taken. With this level of detail, opportunities may be created to understand both conceptually and procedurally how expert and novice performance differs.

5. REFERENCES

Abbott, R.G., McClain, J., Anderson, B., Nauer, K., Silva, A. & Forsythe, C. (2015). Log analysis of cyber security training exercises. Proceedings of the Applied Human Factors and Ergonomics Conference, Las Vegas, NV.

Cacioppo, J. T., Petty, R. E., & Feng Kao, C. (1984). The efficient assessment of need for cognition. Journal of Personality Assessment, 48(3), 306-307.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, SAGE Publications, 229-233.

Digman, J. M. (1990). Personality structure: Emergence of the five-factor model. Annual Review of Psychology, 41(1), 417-440.

Dutt, V., Ahn, Y. S., & Gonzalez, C. (2013). Cyber situation awareness modeling detection of cyber attacks with instance-based learning theory. Human Factors: The Journal of the Human Factors and Ergonomics Society, 55(3), 605-618.

Erbacher, R. F., Frincke, D. A., Wong, P. C., Moody, S., & Fink, G. (2010). A multi-phase network situational awareness cognitive task analysis. Information Visualization, 9(3), 204-219

Forsythe, C., Silva, A., Stevens-Adams, S., & Bradshaw, J. (2013). Human dimension in cyber operations: Research and development priorities. In Foundations of Augmented Cognition (pp. 418-422). Springer Berlin Heidelberg.

Jariwala, S., Champion, M., Rajivan, P., & Cooke, N. J. (2012). Influence of team communication and coordination on the performance of teams at the iCTF competition. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, SAGE Publications, 458-462.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28(7), 509-520.

Reed, T., Abbott, R., Anderson, B., Nauer, K. & Forsythe, C. (2014). Simulation of workflow and threat characteristics for cyber security incident response teams. Proceedings of the 2014 International Annual Meeting of the Human Factors and Ergonomics Society, Chicago, IL.

Scott, S. G., & Bruce, R. A. (1995). Decision-making style: The development and assessment of a new measure. Educational and Psychological Measurement, 55(5), 818-831.

Silva, A., Emmanuel, G., McClain, J.T., Matzen, L. & Forsythe, C. (2015). Measuring expert and novice performance within computer security incident response teams. Proceedings of the Human-Computer Interaction International Conference, Los Angeles, CA.

Silva, A., McClain, J., Reed, T., Anderson, B., Nauer, K., Abbott, R. & Forsythe, C. (2014). Factors impacting performance in competitive cyber exercises. Proceedings of the Interservice/Interagency Training, Simulation and Education Conference, Orlando FL.

Stevens-Adams, S., Carbajal, A., Silva, A., Nauer, K., Anderson, B., Reed, T. & Forsythe. C. (2013). Enhanced training for cyber situational awareness. Proceedings of the Human-Computer Interactional International Conference, Las Vegas, NV.

DISTRIBUTION

1	MS9671	G. Aviña	1463
1	MS1327	P. Bennett	1463
1	MS1327	J. Forsythe	431
1	MS1327	J. McClain	1462
1	MS1327	A. Silva	1463
1	MS1327	J. Wagner	1462
1	MS0899	Technical Library	9536 (electronic copy)
1	MS0359	D. Chavez, LDRD Office	1911


Sandia National Laboratories